CloakLoRa: A Covert Channel over LoRa PHY

Ningning Hou, Yuanqing Zheng
The Hong Kong Polytechnic University, Hong Kong, China
ningning.hou@connect.polyu.hk, yqzheng@polyu.edu.hk

***Abstract*—This paper describes our design and implementation of a covert channel over LoRa physical layer (PHY). 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). Our study 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. To demonstrate the feasibility of building a covert channel, we implement `CloakLoRa`. `CloakLoRa` embeds covert information into a regular LoRa packet by modulating the amplitudes of LoRa chirps while keeping the frequency intact. As amplitude modulation is orthogonal to CSS, a regular LoRa node receives the LoRa packet as if no secret information is embedded into the packet. Such an embedding method is transparent to all security mechanisms at upper layers in current LoRaWAN. As such, an attacker can create an amplitude modulated covert channel over LoRa without being detected by current LoRaWAN security mechanism. We conduct comprehensive evaluations with COTS LoRa nodes and receive-only software defined radios and experiment results show that `CloakLoRa` can send covert information over $250m$.**

***Index Terms*—Covert communication, LoRa**

I. Introduction

Internet-of-things (IoT) envisions ubiquitous communication and enables innovations in government public services, smart cities, and industrial manufacturing. Low Power Wide Area Network (LPWAN) is an emerging network technology which is expected to boost the next-generation IoT. There are several LPWAN technologies (*e.g.*, NB-IoT, LTE-M, SigFox, *etc.*), among which Long Range Wide Area Network (LoRaWAN) is designed to provide communication over a long distance at extremely low power consumption. LoRaWAN now has been deployed to enable innovative applications and pilot studies in the field.

The security of IoT devices is one of the most important problems which may impede the wide adoption of LoRaWAN. Current LoRaWAN secures application layer and network layer with symmetric encryption. However, we observe that the LoRaWAN security mechanism does not examine physical layer communication parameters (*e.g.*, amplitude, phase, and waveform), which leaves the LoRa PHY vulnerable to information leakage. For example, in a smart home where LoRa-enabled IoT sensors are employed for door access [28], smart electricity and water meter, a malicious attacker (Carol in Fig. 1) can compromise a sensor node (*e.g.*, Alice) and build a *covert channel* by modulating the neglected PHY parameters (*e.g.*, amplitude) to secretly collect the sensory data of Alice without affecting the normal communication between Alice and Bob (who are legitimate transmitter and receiver). By synthesizing the sensory data of multiple IoT nodes (*e.g.*, building access records, electricity and water metering, *etc.*), Carol can learn daily routines of the residents (such as the time of home leaving/arriving), and broke in during the residents' absent time. This example raises security risks and privacy concerns of building a covert channel over LoRa PHY. We note that in real scenarios, the IoT devices can be compromised by attackers either before delivering to users or after deployment as reported in previous works [17, 34].

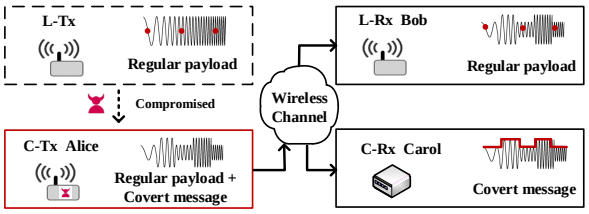


Fig. 1: Covert communication scenario. Alice transmits regular LoRa packets to Bob and the malware on Alice embeds covert information by modulating the amplitude of transmitted LoRa signal. Bob does not check the amplitude of received signal. Only Carol will decode the covert AM information.

In this paper, we demonstrate the feasibility of building a covert channel over LoRa PHY by designing and implementing a covert channel named `CloakLoRa`. `CloakLoRa` uses amplitude modulation (AM) to embed covert information. The key insight is that AM is orthogonal to the CSS modulation scheme of LoRa PHY. We can modulate the amplitude of LoRa chirps while maintaining normal LoRa communication. As a result, AM modulated LoRa chirps carry both original CSS information and AM covert information. The legitimate receiver(Bob) 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.

We note that the AM modulated LoRa chirps can be detected and decoded by a receiver (*e.g.*, Carol), but totally transparent and covert to current LoRaWAN security mechanism. That is because LoRaWAN only protects the end-to-end communication at the network layer and above, while many physical layer parameters including the amplitude variations are largely ignored by current security mechanisms.

We design and implement a prototype to demonstrate the feasibility of such a covert channel over LoRa. Our hardware prototype of `CloakLoRa` uses passive components and a COTS LoRa node as the covert transmitter and a low-cost receive-only SDR dongle (*i.e.*, RTL-SDR) as the covert receiver. Attackers can also implant the AM components into

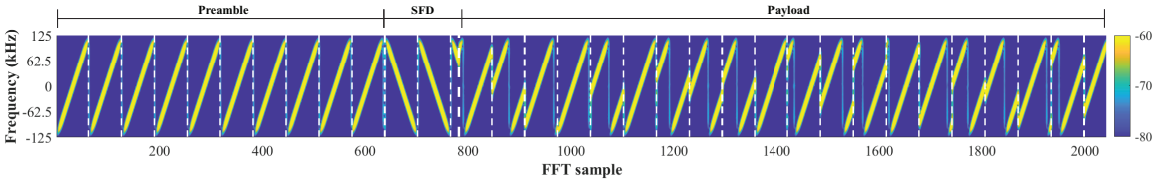


Fig. 2: LoRa packet structure.

LoRa-enabled sensors or install malware to modulate the amplitude of LoRa chirps before delivering bugged sensors to users.

We conduct comprehensive evaluations with both COTS LoRa devices and software defined radios in various experiment settings. The results demonstrate that our prototype can build a covert channel and achieve a high communication accuracy of 99.47% when Alice (Tx) and Carol (C-Rx) are separated by 250 m. These results indicate that it is feasible to build a covert channel with COTS LoRa devices and communicate effectively without being detected. In addition, we also evaluate the impact of covert channel on regular LoRa channel with extensive trace-driven simulations with GNU radio in various parameter settings and channel conditions. The results show that a covert channel does not affect regular LoRa channel, since the regular LoRa channel can inherently tolerate channel variations and noise by design.

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.

The key contributions of this paper are as follows:

- We investigate the vulnerability of current LoRaWAN physical layer where the legacy end-to-end security mechanisms fail to protect. By designing and implementing `CloakLoRa` with COTS LoRa devices, we expose the risk of leaking secret information over LoRa. To the best of our knowledge, we are the first to build a covert channel over LoRa PHY.
- We prototype a covert channel transceiver with simple passive components that can be secretly embedded into sensor nodes. We design and implement a simple yet effective covert channel decoder using a low-cost software defined radio.
- We conduct comprehensive experiments with the COTS LoRa nodes as well as software defined radios under various experiment settings. The experiment results validate the feasibility of building a covert channel over LoRa.

II. LoRa Physical Layer

LoRa PHY. The physical layer (PHY) of LoRaWAN adopts a unique chirp spread spectrum modulation (CSS), which trades data rate for sensitivity and improves the robustness against interference in the crowded Industrial, Scientific, and Medical (ISM) bands. A LoRa chirp is a signal whose frequency increases (upchirp) or decreases (downchirp) linearly

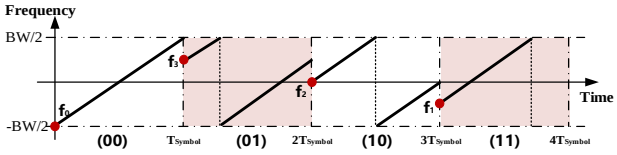


Fig. 3: Example of CSS modulation.

at a constant rate over time. The chirp sweeps through and wraps around a predefined bandwidth. Fig. 2 shows the PHY samples of a LoRa packet collected with low-cost software defined radios (SDR). The packet starts with a preamble consisting of 10 up-chirps followed a synchronization frame consisting of 2.25 down-chirps and payload.

LoRa uses different initial frequencies to modulate symbols. Fig. 3 illustrates the CSS modulation scheme used in LoRa. The symbol duration is denoted as (T_{symbol}). Assume we need to modulate 2 bits ('00', '01', '10', '11') with each symbol (*i.e.*, spreading factor = 2). We need 4 different symbols with different initial frequencies (*e.g.*, f_0, f_1, f_2, f_3). An upchirp with the initial frequency of $f_0 = -BW/2$ is named base chirp, which modulates '00' as shown in Fig. 3. In practice, depending on the spreading factor SF ($7 \leq SF \leq 12$), the number of possible symbols is 2^{SF}. Upon the reception of a LoRa chirp, a receiver examines the initial frequency of the chirp and thereby demodulates the chirp. A LoRa receiver thus largely overlooks the amplitude changes of the symbols in the demodulation process.

Security mechanism. Current LoRaWAN mainly adopts message encryption to ensure the security of end-to-end communication. For instance, symmetric key algorithms (*e.g.*, AES-128) are adopted at network layer and application layer to encrypt messages. This message encryption is only implemented at the upper layers. In physical layer, CSS modulation only exploits the initial frequencies of chirps to differentiate symbols and ignores other parameters such as amplitude, phase, and waveform which can be modulated by potential attackers or malware to leak sensitive information. Our proof-of-concept experiment builds a covert channel over LoRa PHY by modulating amplitude of LoRa chirps.

III. Covert Channel over LoRa PHY

A. System Model and Assumptions

Fig. 1 depicts the system model which consists of three devices: a compromised transmitter (Tx) Alice, a legitimate LoRa receiver (L-Rx) Bob, and a covert channel receiver (C-Rx) Carol. Alice and Bob can be COTS LoRa devices (*e.g.*, LoRa nodes, LoRa gateways) in practice. In this scenario, the LoRa packets transmitted by the compromised LoRa node

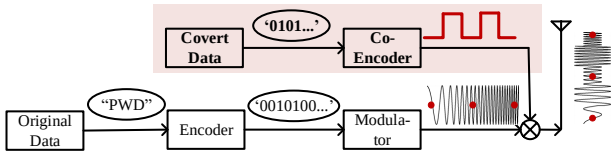


Fig. 4: Workflow of covert channel transmitter.

Alice contain two kinds of information: the CSS modulated LoRa message and the covert information. The three devices in the model have distinct objectives. Alice transmits regular CSS modulated LoRa packets to Bob and, after being compromised, the malware on Alice also sends covert data to Carol through the covert channel. Bob aims to receive the regular LoRa packets. Carol would like to receive covert information from Alice's transmission. Carol only extracts the embedded covert information and does not need to decode a LoRa packet. The goal of building a covert channel is to stealthily get information out without affecting the performance of regular LoRa channel and avoid being detected by LoRaWAN security mechanisms.

We assume that an attacker has compromised a LoRa node Alice. This can be done by either software-based attack or hardware based attack. For example, an attacker can be an insider who aims to secretly send out sensitive information without being detected. An attacker can also be a LoRa node manufacturer who can modify the firmware of sensor node or add micro hardware components in the PCB board to enable covert communication before delivering the bugged sensor node to users. We assume that only Carol knows the implementation details of covert channel. Therefore, Carol can leverage the knowledge of covert channel implementation to detect the existence of a covert channel and secretly receive the covert information.

B. Design Requirements

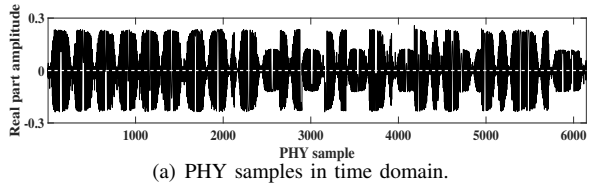
We summarize the key design requirements to build covert channel over LoRa PHY:

R-1) Ideally, the covert channel should not substantially affect the communication performance between Alice and Bob (*e.g.*, packet reception rate, bit error rate, *etc.*). Alice modulates covert information by making changes to a regular LoRa packet.

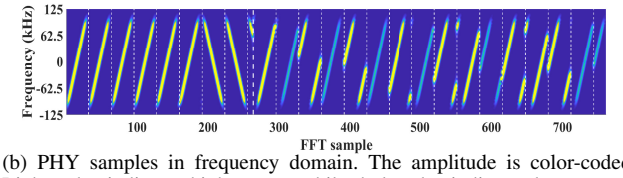
R-2) We aim to improve the efficiency (information rate) of covert channel such that the covert channel can leak more information. It turns out, however, this design requirement inherently conflicts with the first requirement R-1. We need to strike a balance.

IV. Covert Channel Design and Implementation

In this section, we first conduct a proof-of-concept with software defined radios to demonstrate the feasibility of building a covert channel. Then we describe the design and implementation of Tx with a COTS LoRa and C-Rx with an SDR dongle, respectively. Finally, we introduce the covert packet structure and packet reception process.



(a) PHY samples in time domain.



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

Fig. 5: Covert channel signals captured by a software defined radio. The amplitude of LoRa chirps are modulated to carry covert information.

A. Proof-of-concept with Software Defined Radio

We test the feasibility of building a covert channel over LoRa PHY by implementing a proof-of-concept based on GNU Radio and GR-LoRa projects [18, 19]. We add an amplitude-modulated (AM) component as shown in Fig. 4, which modulates the amplitude of LoRa chirps and thus embeds covert information. As such, the AM LoRa chirps contain two kinds of information: the CSS modulated LoRa message and the covert information.

We use a software defined radio (acting as Alice) to generate and transmit AM LoRa chirps. We use two receivers to extract different information: a COTS LoRa node (acting as Bob) for CSS modulated LoRa packets and a low-cost SDR receiver (acting as Carol) for covert information. In the experiment, both Carol and Bob are kept close to Alice with a good channel quality only for the proof-of-concept purpose. Fig. 5 shows the PHY samples collected by Carol. In both time domain (Fig. 5(a)) and frequency domain (Fig. 5(b)), we can observe alternating amplitudes of chirps in payload. The signal strength is color coded in Fig. 5(b), *i.e.*, brighter color indicates stronger 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 frequencies of chirps remain unchanged, Bob can still decode the payload even though the amplitudes of chirps have been intentionally modulated.

In summary, the preliminary experiment results show 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 LoRa chirps.

B. Covert Transmitter with COTS LoRa

In the proof-of-concept, we use an SDR (*e.g.*, USRP N210) to build a covert channel over LoRa PHY. In the following,

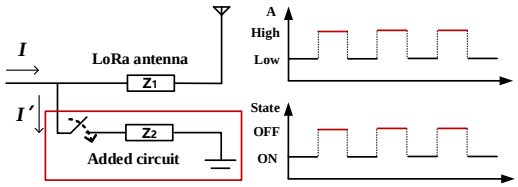


Fig. 6: Circuit design. The ON/OFF state of the switch controls the amplitude of the outgoing signals. As a result, covert information can be conveyed to the receiver.

we present the implementation of a simple covert channel with COTS LoRa node. The key idea is to use COTS LoRa devices to generate chirps (serving the purpose of carrier waves) and use passive components to modulate the amplitude of those chirps, thereby transmitting covert information.

A Strawman Approach: Packet-level Amplitude Modulation. One straightforward yet inefficient way of modulating the amplitude is to configure the transmission power of a LoRa node before every packet transmission. HopeRF RFM95 module [15] and Semtech sx1276 chip [29] allow users to configure the RF output before sending a packet. A covert channel receiver may measure the received RSSI to infer the covert information. However, the packet-level amplitude modulation approach cannot provide sufficient data rate for practical covert channel applications, failing to meet the design requirement R-2. Instead, we aim to modulate the amplitude of each chirp to achieve higher data rate as in the proof-of-concept experiment.

Our Approach: Chirp-level Amplitude Modulation. Our prototype uses simple passive components to modulate the amplitude of LoRa chirps. We use a switch to control the electric current through the antenna load. As shown in Fig. 6, a new branch (consisting of a switch and an impedance Z_2) is added to control the amplitude of LoRa chirps. As illustrated in the figure, when the state of the switch is OFF, the current (denoted as I) flows through 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 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. As a LoRa packet takes a relatively long time to transmit, by changing the state of the switch (*e.g.*, 200 bps), we can modulate the amplitude at chirp-level. In this way, a stream of covert data can be embedded into a LoRa packet.

Fig. 7 shows our hardware prototype. 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. 6. In practice, attackers can embed the components in sensor node and hide the components on the board before delivering the node to user. 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.

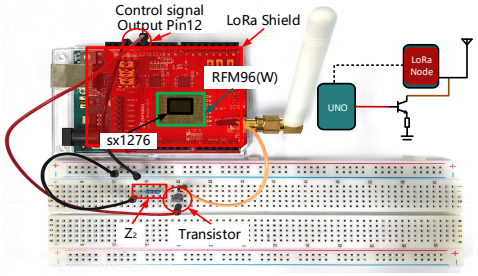


Fig. 7: Hardware implementation of transmitter. The LoRa node is compromised to leak information. A low-cost transistor is used as a switch to directly modulate the amplitude of LoRa chirps.

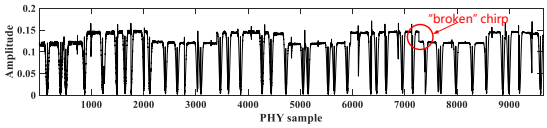
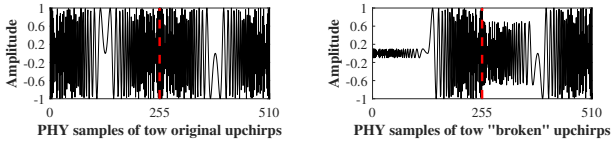


Fig. 8: Physical samples of covert message with LoRa node.

In the experiment, we configure the bit duration of output pin (*i.e.*, pin 12) 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 $BW = 250K$). That means every 5 LoRa chirps are used to encode 1-bit covert information. Fig. 8 shows the received PHY samples after AM modulation. We can observe that every five chirps share the same power level. The amplitude profile of these samples alternates corresponding to the ON/OFF state of the transistor. The receiver can reveal the covert message by measuring the profile.

However, from Fig. 8, we find that some of the LoRa symbols are "broken" (the amplitude profile within one chirp has a sudden change). In the previous SDR-based proof-of-concept experiment, we change the amplitude of chirps alternatively yet the amplitude of each LoRa chirp remains stable. To see whether a "broken" chirp can be correctly demodulated, we conduct another experiment. As shown in Fig. 9, we first generate two complete up-chirps (Fig. 9(a)) and use the demodulated results as the ground truth. We then intentionally vary the amplitude within one chirp severely to "break" it as shown in Fig. 9(b). In Fig. 9(b), the first half parts of the two up-chirps are shrank to 0.1 and 0.7 (normalized amplitude is 1), respectively. The result shows that even the the symbol is broken, the receiver can still demodulate it correctly. In this prototype, we use another COTS LoRa node as regular receiver. The COTS receiver also decodes the regular LoRa message correctly.

The prototype (Fig. 7) is used to demonstrate the feasibility of hardware implementation and can be optimized. For example, a few passive components used to control the power level can be hidden among many electronic components in sensor nodes. Attackers can even sandwich the components between the PCB layers of sensor nodes before delivering the compromised nodes to regular users.



(a) original up-chirps. (b) broken up-chirps.

Fig. 9: Original up-chirps and broken up-chirps.

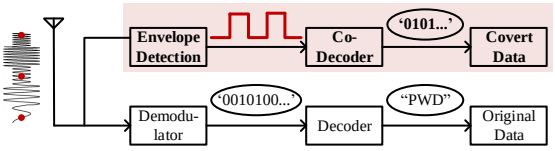


Fig. 10: Workflow of covert channel receiver and regular LoRa receiver.

C. Covert Receiver with Receive-only SDR

We use a receive-only SDR as Carol to collect PHY samples and extract covert information from the PHY samples. In specific, we use an RTL-SDR dongle as the low-cost SDR receiver.

Fig. 10 shows the demodulation and decoding process of LoRa packets as well as the covert information extraction process. The PHY samples collected by the receive-only SDR can be processed in parallel in two processing chains to demodulate the LoRa packet and to extract the covert information, respectively. To demodulate the LoRa packet, the demodulator measures the initial frequency of each LoRa chirp and sends the demodulated symbols to the decoder. The decoder then implements Hamming decoding, de-interleaving, and de-whitening to decode the LoRa message [18].

As for covert receiver, Carol does not need to decode the LoRa message. Therefore, we only focus on the covert information extraction process. Note that the covert information is embedded in the variation of the amplitude, the covert information extraction process essentially implements the AM demodulation process. We describe this process in the following section.

D. Covert packet reception

In our implementation, we use FM0 as an example to encode the covert data. FM0 uses a state (power level) transition within a symbol duration to encode '0' and no state transition to encode '1'. Thanks to its simplicity and efficiency, FM0 is widely used to support communication for lightweight devices (*e.g.*, RFID backscatter communication). Developers can also use other encoding methods according to their specific design requirements.

Packet structure. Fig. 11 illustrates the packet structure of a covert message. We use the pilot tone and the preamble which resemble those of tag-to-reader messages in commodity RFID communication [6]. In particular, we use 8 alternating chips (*i.e.*, four "0"s of FM0) as the leading pilot tone, which is followed by the preamble (*i.e.*, "1011" of FM0). The length of the payload can be adjusted according to different design requirements.

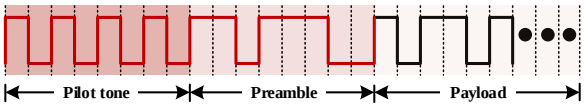


Fig. 11: Covert packet structure.

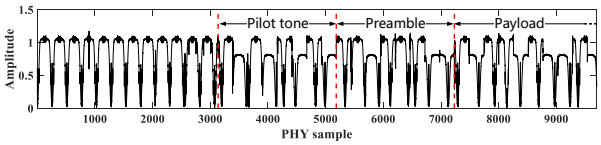


Fig. 12: Physical samples of covert message.

Packet reception. At the receiver side, the RTL-SDR records the received PHY samples. Fig. 12 shows the physical samples containing ON/OFF amplitude variations. Covert bits in the packet can then be extracted in the following three steps.

1. Pilot tone detection. We use 8 alternating chips as the leading pilot tone. The covert transmitter and receiver have prior knowledge about covert packet structure. Therefore, the same pilot tone can be generated at the covert receiver and used to do self-correlation with the received physical samples. We choose the duration of three symbol (*i.e.*, 6 chips) as the self-correlation window and move forward in steps of one symbol.The covert receiver uses an empirical threshold of two standard deviation (*i.e.*, 95% confidence level) to detect a covert packet. In particular, a covert packet is detected if the self-correlation value is higher than the threshold and presents twice. In case of the payload bits may also contain four consecutive symbol "0"s, we buffer the physical samples for one packet length and treat every four "0"s as the pilot tone of a covert packet. False positive cases can be differentiated by checking the checksum in the end of the payload data.

2. Synchronization. Similar to synchronization process of FM0 method in RFID communication, a violation symbol in the preamble is used to help with synchronization and boundary detection. Since a covert receiver has prior knowledge of the preamble, it calculates the correlation between the received signal and the predefined preamble template and detects the correlation peak for synchronization.

3. Payload extraction. After the previous steps, we can detect the starting point of the payload. Then we need to detect whether there is a state transition of power level within a symbol duration to determine the covert bits. However, due to signal attenuation and interference from nearby wireless transmissions, the amplitude transition would be minute, which is challenging for receiver to detect the occurrence of transition. In our case, we use FM0 to encode covert data, where each symbol contains two chips. Therefore, we tackle this problem by first determining the chip state of each chip and then compare the chip states of two chips with in a symbol. In specific, we first slice the remaining samples into chips and calculate the average power of each chip. Then, we determine the power level state of each chip by comparing its average power level to a reference threshold *th*. *th* is configured as the average power of the leading pilot tone.

V. Covert Channel Analysis

In this section, we analyze LoRa PHY covert channel in terms of efficiency and we discuss its impact on regular LoRa communication.

Efficiency. We quantify the efficiency of covert channel as the information rate that transmitted through this covert channel [8, 10]. Specifically, assuming that the channel is an Additive white Gaussian noise (AWGN) channel, the information rate of covert channel (I_c) can be calculated as:

$$I_c = K \times \frac{1}{2}\log_2\left(1+\frac{S}{N}\right) \quad (1)$$

where K is the amplitude changing rate of the transmitted signal. K is determined by the changing rate of switch in Fig. 7. $\frac{S}{N}$ is the SNR at the receiver side, while N is the power of noise of AWGN channel and S is the signal strength of covert signal (*i.e.*, amplitude variation of carrier waves in amplitude modulation).

We use *modulation depth (D)* to represent signal variations of carrier wave. 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. For example, if $M = 0.3$, the carrier amplitude varies by 30% above and (below) its unmodulated level. A larger D indicates a larger change of amplitude thus a higher SNR for covert channel. Due to signal attenuation, the received signal strength of Carol is inversely proportional to the square of the distance r from Alice (*i.e.*, inverse square law). Therefore, we represent the received signal power S_r as:

$$S_r \propto \frac{(AD)^2}{r^2} = \frac{D^2}{r^2}P_{Tx} \quad (2)$$

The above discussion simplifies the path loss of RF signal so as to focus on the influence of modulation depth D and distance r. According to Eq. 1 and Eq. 2, we can improve the covert channel efficiency by using a larger D (*e.g.*, 0.9) and a smaller r. Fig. 14 shows the amplitude of signal recorded by Carol at different distances. We denote the distance from Alice to Carol as r_{AC}. As illustrated in Fig. 13, r_1 is the largest distance for Carol (*i.e.*, covert channel receiver) to correctly decode the covert data from Alice (*i.e.*, covert channel transmitter). If Carol is placed further, *i.e.*, $r_1 < r_{AC} < r_2$, it can only correctly receive a portion of covert information. If Carol moves further away from Alice ($r_{AC} > r_2$), it cannot reliably receive even one-bit information, indicating that even the existence of covert channel cannot be determined. r_3 is the largest distance for a legitimate LoRa receiver to correctly decode the CSS modulated data. In practice, r_2 is much shorter than r_3.

Impact on regular LoRa communication. In our prototype, we vary the amplitude of regular LoRa signal to embed covert information. This operation will reduce the signal strength of part of the regular LoRa chirps. As a result, the regular LoRa communication may be impacted.

Modulation depth (D) indicates the degree of amplitude change. For LoRa covert channel, a larger D is preferred as it indicates a higher SNR at covert channel receiver. However, for Bob, the legitimate LoRa receiver, a larger D means weaker signal strength of part of the regular LoRa chirps. As a result, the largest communication distance r_3 of a compromised LoRa node will be shorter.

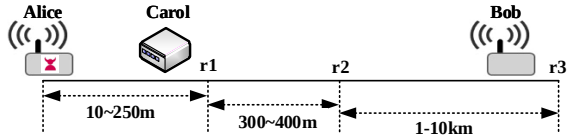
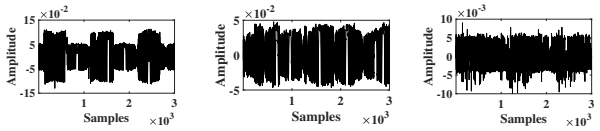


Fig. 13: Efficiency versus distance.



(a) $r_{AC} < r_1$. (b) $r_1 < r_{AC} < r_2$. (c) $r_{AC} > r_2$.

Fig. 14: Amplitude of signals recorded by SDR at different distances.

Besides D, channel condition also influences the regular LoRa communication. Since LoRa receiver has very high sensitivity, there is a large SNR margin to tolerate the reduction in chirp amplitude. AM modulated LoRa packets can be still received and decoded correctly when the amplitude change is within this margin. However, when the SNR of LoRa communication is close to the sensitivity, the performance of LoRa communication will deteriorate. We evaluate the impact of D and channel condition on regular LoRa communication at VI-D. In practice, Alice can actively adjust its transmission power and modulation depth to make sure the covert information can be received by Carol while regular LoRa packets can be correctly decoded by BoB.

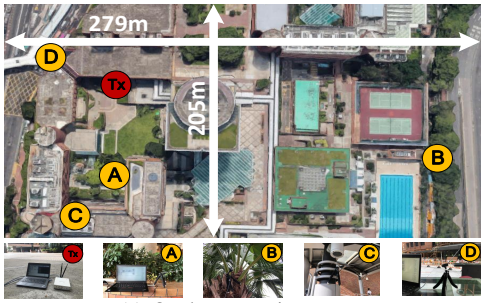
In summary, to achieve higher efficiency, we need a larger modulation depth D. However, a larger D may impact the regular LoRa communication performance. In fact, the two design goals are inherently conflicting with each other. We need to strike a balance between these tow goals. As illustrated in Fig. 13, in practice, Alice can adjust the transmission power and modulation depth so that Carol can receive within a range (*e.g.*, between $10m$ to $250m$).

VI. Evaluation

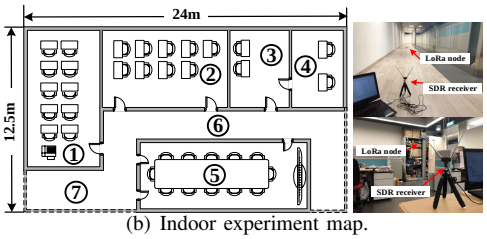
In the evaluation, we explore the following research questions: First, what is the maximum covert communication range? Next, what is the impact of modulation depth on both covert channel and regular channel communication. What is the performance of covert communication when coexisting with other regular LoRa signals? Finally, how do different environments influence the covert communication performance?

A. Experiment setting

Equipment and experiment layout. In the experiment, we use both COTS LoRa node and USRP to act as Alice and transmit covert messages. An RTL-SDR is used as Carol. We conduct experiments in the outdoor and indoor scenarios as



(a) Outdoor experiment map.



(b) Indoor experiment map.

Fig. 15: Experiment layout.

shown in Fig. 15. Outdoor field spans 279×205 m^2 (Fig. 15(a)) while a typical office building with the size of 12.5×24 m^2 (Fig. 15(b)).

Default parameters: carrier waves. LoRa chirps work as carrier waves of covert message and we configure the carrier waves by setting spreading factor, code rate, and bandwidth of the LoRa chirp signal to 8, $4/8$, and 250 KHz, respectively. We use implicit header mode and low data rate mobile node mode. The default parameters of regular LoRa transmitter and receiver are shown in Table I(a).

Default parameters: covert channel. We present the key parameters of covert channel transmitter and receiver in Table I(b). In specific, the symbol duration of covert message is set to 5 ms for LoRa node transmitter and 2 ms for USRP transmitter, respectively. The default transmission power of Alice is set to 5 dBm and the default receive gain is set to 20 dB. We set the default sampling rate of covert channel receiver as 500 KS/s. We set the payload of a covert message to 30 bits. Since the pilot tone and preamble before payload last 8 bits, the total length of a covert message is 38 bits. We note that the maximum size of a LoRa packet can be up to 255 bytes, thus a typical LoRa packet is sufficient to carry a 38-bit covert packet. The default modulation depth (D) is set to 0.1 empirically.

In each scenario, we conduct over 100 measurements and we send 30 packets in each measurement.The payload of each covert packet as well as the regular LoRa packet is randomly generated. We use Bit Error Rate (BER) to measure the covert channel communication performance and we use Symbol Error Rate (SER) to measure the performance of regular LoRa communication performance.

B. Effective range of covert communication

We conduct this experiment in outdoor field (Fig. 15(a)). We keep the Tx Alice (red dot) stationary and move the C-Rx Carol to four different positions (*i.e.*, yellow dots: A, B, C, and D). This outdoor scenario is non-line-of-sight (NLOS). The transmission power of USRP is set to 30 dBm and the receive gain is set to 60 dB. We set D to 0.3 to enable longer communication range in NLOS outdoor environment. We then measure the BER at each position and thus estimate the maximum covert channel communication range.

TABLE I: Default parameter settings.

(a) Default parameter settings of regular LoRa transmitter and receiver

Freq.	SF	BW	Code Rate	Header Mode	MN Mode
$915MHz$	8	$250KHz$	$4/8$	Implicit	Low Data Rate

(b) Default parameter settings of covert channel transmitter and receiver

Tx Power	Rx gain	Sampling Rate	Payload	D
$5(5-30)dBm$	$20dB$	$500KS/s$	$30bits$	0.1

Fig. 16 shows the average and one standard deviation of BER at different positions. A is 68 m away from covert channel transmitter and the BER is 0, which means the covert channel receiver can reliably decode all the covert information. Receivers at B (approximately 250 m away from Tx) and C (102 m) can also decode the covert information with average BER 0.43% and 0.42%, respectively. D is the closest to Tx, however, the performance at D is the worst. This is because the covert signal need to penetrate 5 to 6 concrete walls and mental scaffold to arrive at the covert channel receiver, which makes the signal too weak to be decoded correctly by the SDR dongle. By increasing the receiver gain and using a larger modulation depth, Tx can send covert message to covert channel receiver separated by even longer distance. Better channel quality (line-of-sight) can also extend the covert channel communication range. We investigate the impact of modulation depth in the next subsection.

We note that the communication distance between Alice and Carol is around 250 m in our experiment. This shows covert channel's capability of communicating within 250 m. This is a small range, however, compared with the long communication range between regular LoRa transmitter and regular LoRa receiver ($\sim$ 10 km). The result implies that C-Rx needs to be placed within 250 m in order to correctly receive the covert message.

C. Covert communication performance

Modulation depth $D = M/A$, where M is the peak-to-peak changes and A is the carrier amplitude. Thus, modulation depth quantifies the difference in the power levels between ON state and OFF state when Tx uses the amplitude modulation to embed covert data.

We use the USRP as Tx and use the low-cost receive-only RTL-SDR dongle as C-Rx. In this experiment, we set the transmission power of USRP to the lowest 5 dBm for convenience of receiving. We set the sampling rate of USRP sink to 1 M/s. The distance between Tx and C-Rx is fixed at 3 m and receiver gain of C-Rx is set to 10 dB. The other key parameters are set as the default values specified in Table I.

Fig. 17 shows the average BER and standard deviation of covert channel with different modulation depths of Tx ranging

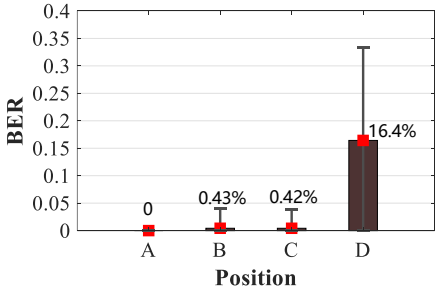


Fig. 16: Outdoor performance at different positions.

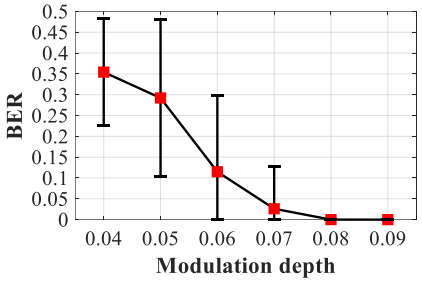


Fig. 17: BER of covert channel using different modulation depths.

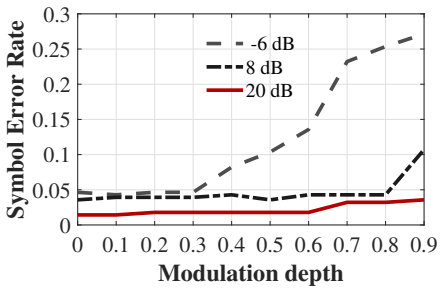


Fig. 18: Symbol error rate of regular LoRa packets with different modulation depth.

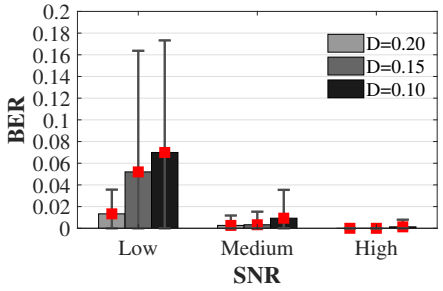


Fig. 19: Performance of covert channel coexisting with other regular LoRa signals.

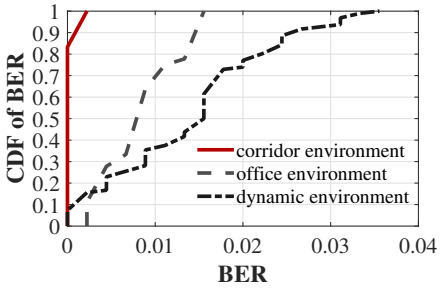


Fig. 20: BER of covert channel under various environments.

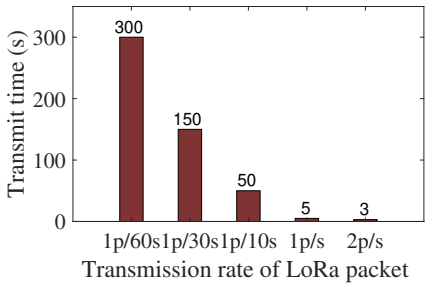


Fig. 21: The time to leak 128-bit sensitive information (*e.g.*, NwkSKey).

from 0.04 to 0.09. We only present the results with $0.04 \leq D \leq 0.09$. That is because the performance is most sensitive to D in such a range in this experiment setting. We notice that when $D = 0.04$, BER is very high (0.35), getting closer to a BER of 0.5 (*i.e.*, random guess). That is because with $D = M/A = 0.04$, it becomes difficult to differentiate the ON state and the OFF state, since the power levels of ON/OFF states become quite similar. BER starts to decrease as the modulation depth increases. The BER is nearly 0 when D increase to 0.09.

We note that a larger modulation depth (*i.e.*, substantial difference between ON state and OFF state) can benefit covert *packet decoding* process. However, it also *increases the risk of being detected* by a covert channel detector. We see that efficiency and covertness are inherently conflicting goals. Covert channel transceivers need to strike a balance between the efficiency and the covertness according to application requirement. In practice, Tx adjusts D and transmission power to enable correct decoding at C-Rx while avoid being detected by covert channel detector. We empirically set D to 0.1 in most experiments if not specified otherwise.

D. Impact on regular LoRa communication

In this subsection, we evaluate the impact of different modulation depth D on regular LoRa communication. Since we want to control the modulation depth and get sufficient data at different channel conditions (*i.e.*, low, medium, and high SNR), we use GNU Radio to simulate such different conditions. In this experiment, we add AWGN noise to generate different SNR conditions. We vary D from 0 (without embedding covert information) to 0.9 at the step of 0.1. In this experiment, we measure symbol error rate (SER). The initial frequencies of LoRa chirps before AM modulation are used as ground truth. We demodulate the received signal (which contains covert information and noise) at the receiver side. If the initial frequency of a chirp at the receiver side are not the same with the corresponding ground truth, we regard it as a symbol error. We use 168 symbol in each case.

Fig. 18 shows the results. We have two observations in this figure. 1) When $D = 0$, which means we do not change the amplitude of LoRa chirps, LoRa achieves less than 5% SER even when the SNR is -6 dB. This result demonstrates that LoRa is resilient to noise and can communicate below the noise. 2) Modulation depth D has bigger influence on SER when the SNR is low while it slightly influences SER when the SNR is high. When SNR is -6 dB, the SER starts to increase as D is larger than 0.3. SER reaches 25% when $D = 0.9$. However, for $SNR = 8$ dB and $SNR = 20$ dB, SER are less than 5% even when D is 0.8. In low SNR condition, when D becomes larger, chirps with low amplitude will become weaker, which make it hard for regular LoRa receiver to demodulate them correctly. When SNR is high, the frequency information can still be extracted correctly even with a larger D. In the above experiments, we evaluate the symbol error rates. To mitigate the impact of symbol errors, LoRa adopts forward error correction scheme (*e.g.*, Hamming code). As such, the symbol error rates of around 5% can be corrected in practice.

E. Coexisting with other regular LoRa nodes

Covert channel transmitter and receiver may coexist with other regular LoRa nodes. As a result, the LoRa transmission of coexisting regular nodes may influence the performance of a covert channel. In the following, we evaluate the performance

of a covert channel with presence of coexisting regular LoRa nodes.

The USRP Tx and the RTL-SDR C-Rx are positioned inside of a meeting room ⑤ in Fig. 15(b). We placed other regular LoRa nodes to different positions (*e.g.*,①-④, ⑥ and ⑦) and control them to transmit packets at different transmission power levels. We also change the modulation depth ($D = 0.10$, 0.15, and 0.20) of the covert channel transmitter. We categorize the measured results into low, medium and high SNR regimes according to the SNR of covert channel.

In Fig. 19, the experiment results show that the covert channel achieves better performance with higher SNR. The average BER is less than 0.2% in the high SNR regime. The BER as well as standard deviation decreases as the channel condition improves. The results also indicate that the modulation depth plays an important role in the covert channel communication. Specifically, covert signals with $D = 0.20$ achieves $BER = 1.3\%$ even when the SNR is low, while BER increases to around 7.5% when the modulation depth is set to $D = 0.10$.

In practice, the duty cycle of LoRa is 1%. Although there may coexist several LoRa nodes, the probability of two nodes nearby transmit at the same time is very low. Therefore, the attacker still has chance to leak information out. Besides, attackers can adopt a larger D to increase the covert signal strength to resist interference.

F. Performance in various environments

In this experiment, we evaluate the impact of different environments on BER. We consider three typical environments (1) empty corridor with the line-of-sight path (Fig. 15(b), corridor ⑥ and ⑦), (2) multipath-rich office (Fig. 15(b), room ①-⑤) and (3) dynamic environment with people walking nearby (Fig. 15(b), room ①). We use COTS LoRa device as Tx by adding a transistor and an impedance as shown in Fig. 7. The receiver is still the low-cost SDR. In each environment, we configure the covert channel transceiver by using default setting parameters in Table I.

Fig. 20 shows the CDF of BER in these three different environments. In corridor environment with the line-of-sight(LOS) path, the payload of the package can be accurately decoded with a BER of less than 0.5% even with the lowest transmission power. In the office environment with rich-multipath, the performance of covert channel communication becomes diverse due to the multipath effect. We observe that 90% of the covert packets are decoded with BER less than 1.5% and with the medium BER of around 0.78%. In the dynamic environment, people walking around Tx make the performance worse, since they may weaken the signal and block the LOS path between the transmitter and the receiver. We find that the BER in dynamic environment is still less than 4% and can be used to transmit covert information.

We notice that the BER of COST LoRa device as Tx is relatively high than that of USRP. The reason is that we use very simple external circuit to change the transmission power of LoRa chirps. This prototype is used to test the feasibility of building a covert channel with commodity LoRa nodes. Future design of covert channel can be sophisticated. Attackers can install malware or implant a tiny spy chip in LoRa nodes before delivering the product to users.

G. Time overhead of information leakage

We evaluate the time to transmit some sensitive information through covert channel. Suppose a LoRa node is compromised, we estimate the time to leak sensitive information (*e.g.*, encryption keys). The security keys in LoRaWAN are used to secure the end-to-end communication. For example, Network Session Key (NwkSKey 128 bits) is used for interaction between the Node and the Network Server. Suppose we transmit a secret key of 128 bits over a covert channel. We adopt FM0 with 2 chips and the payload size is of 30 bits. In this case, we need to transmit 5 regular LoRa packets to transmit the 128-bit secret key. As we use LoRa packets as the carrier waves of covert packets, the transmission time of such sensitive information depends on the transmission rate of regular LoRa packets. Assuming that a regular LoRa node sends 1 packet every 10 seconds (*i.e.*, 1p/10s), it takes 50 seconds to transmit the 128-bit sensitive information.

We also plot the transmission time of security keys in LoRaWAN (*i.e.*, 128 bits) with different regular LoRa packet transmission rates in Fig. 21. We observe that the transmission time of sensitive data decreases as the transmission rate of regular LoRa packet increases. The transmission time of sensitive information can also be decreased by increasing the payload size and and increasing the alternating rate of on-off states of covert packets.

VII. Related work

Covert channel was first introduced by Lampson [20]. Many works point out the potential covert channels in computer networks and different communication systems. [39] surveys the covert channels and countermeasures in computer network protocols. Recent work NICScatter [38] uses NIC to backscatter radio signals and builds a covert channel to leak information. NICScatter switches NIC between ON/OFF states to modulate incident RF signals generated by signal helper. The NICScatter receiver then extracts information from the transmitter by analyzing the amplitude of the reflected signals. DC-MAC [36] generates intended interference patterns in wireless communication to build an in-band covert channel without degrading the effective throughput of main channel.

Covert channels in OFDM, WiMax, and LTE systems are introduced in [11, 12, 31]. Those works build covert channels by padding frames or packets. Other covert channels in OFDM and Wi-Fi systems are introduced in [2, 3, 13, 41]. Shadow Wi-Fi [27] embeds covert information by pre-filtering Wi-Fi frames prior to transmission. The receiver then extracts embedded information by analyzing CSI. PN-ASK-WiFi [4] and Dolphinattack [40] are the most similar work. PN-ASK-WiFi [4] uses pseudo-noise asymmetric shift keying (PN-ASK) modulation to embed secret information into Wi-Fi signals while Dolphinattack [40] utilizes amplitude modulation

to embed voice commands in ultrasonic sound. Unlike those works, we leverage AM to build covert channel over LoRa.

LoRa is one of the most promising technologies to boost LPWAN development. A survey of LoRaWAN [14] gives an overview of recent research works in this field, including existing security and reliability mechanisms. [1, 16, 23, 24, 26, 32, 35] conduct real world experiments and report measurement studies. PLoRa [25] builds a prototype that backscatters LoRa chirps. Recent works [5, 33, 37] aim to enable parallel transmission of multiple LoRa nodes. LoRaBee [30] enables the cross technology communication from LoRa to ZigBee. Symphony [22] achieves concurrent transmissions from heterogeneous radios (*i.e.*, BLE, ZigBee and LoRa) to a LoRaWAN base station. Some works aim to optimize parameter settings (*e.g.*, spreading factor [21], frequency selection [7]) to achieve higher throughput and lower power consumption. A recent work [9] aims to support CSMA in LoRaWAN.

Unlike those works, `CloakLoRa` builds a covert channel over LoRa PHY. As LoRa PHY only examines frequency changes while ignoring amplitude variations, a regular LoRa receiver cannot receive or detect covert messages. On the other hand, a covert channel receiver can receive the covert message embedded using the amplitude modulation.

VIII. Limitation and future work

Prior knowledge of covert channel and countermeasures: We note that if LoRaWAN has the prior knowledge of our covert channel design (*i.e.*, AM-based covert channel embedding), one may design and implement a countermeasure to detect such a covert channel. For example, the legitimate receiver Bob (*i.e.*, base station) can monitor amplitude changes and check if any covert information has been embedded. We note that current LoRaWAN does not detect the existence of such a covert channel and is totally oblivious of such an AM-based embedding method. The key contribution of our work is that it reveals the venerability of current LoRa PHY.

Data rate and power adaptation: Our work does not explicitly consider the power adaptation (*e.g.*, Adaptive Data Rate (ADR) mechanism) and its impact on communication range. ADR optimizes the energy consumption in the network by automatically adjusting data rate. If the node uses a smaller spreading factor and reduce the transmit power, the distance r_1 for Carol to correctly decode the covert data will become shorter. The largest LoRa communication distance r_3 will also decrease. When SNR is low, if the LoRa Rx cannot receive regular LoRa message due to low SNR, the regular LoRa Tx will adapt the transmission power according to current LoRaWAN standard. In the power adaption process, the covert Tx does not need to collect feedback from the LoRa Rx. The power adaption is automatically done by regular LoRa Rx and regular LoRa Tx in case that modulation depth affect the regular LoRa packet reception.

Other covert information embedding approaches: Besides amplitude modulation, there are other ways to build covert channels over LoRa PHY. For example, one can embed covert data in the initial phases of chirps or phase shifts. However, we note that the implementation of phase based covert information embedding can be more challenging especially with passive components. In the future, we plan to explore other ways of building covert channels.

Generality of our approach: We focus on building a covert channel over LoRa PHY, which uses chirp spreading spectrum (CSS). For the generality of our approach, we believe our approach can be generalized to wireless technologies that use CSS as physical layer modulation scheme (*e.g.*, Low-Rate Wireless Personal Area Networks (LR-WPAN) in IEEE 802.15.4a). Generally, our intuition of building covert channels over PHY is to send covert information using a modulation scheme that is orthogonal to the existing modulation scheme. Although we have not tested the feasibility, our approach should be applicable to frequency modulation (FM) and phase modulation (PM) as well, since FM and PM also only examine frequency and phase, and overlook amplitude changes in demodulation process. In contrast, our approach cannot be generalized to amplitude modulation (AM) or quadrature amplitude modulation (QAM), because these two schemes examine amplitude changes in demodulation process.

Ethical aspects of our work: We hope our work can reveal the vulnerability so that LoRa PHY can be better protected from being abused to leak sensitive information by malicious attackers. To detect and defend against AM-based covert channels, LoRa nodes can be enhanced to examine amplitude changes in the CSS demodulation process. In practice, LoRa gateways could collaborate in covert channel detection.

IX. Conclusion

This paper presents `CloakLoRa`, the first covert channel over LoRa PHY. `CloakLoRa` embeds covert information into LoRa packets by changing the amplitude of LoRa chirps while keeping the frequency intact. The insight behind the covert channel design is that we use a modulation scheme that is orthogonal to LoRa PHY. Thereby, the embedded information is decodable to covert receiver while cannot be perceived by current LoRaWAN security mechanism. The key innovation is that we implement a prototype covert channel over LoRa PHY with commodity LoRa nodes and SDRs. 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.

Acknowledgements

We would like to thank our shepherd Dr Ashwin Ashok and anonymous reviewers for their constructive feedback and valuable comments for improving the quality of this paper. 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. Centenaro, L. Vangelista, A. Zanella, and M. Zorzi. Long-range communications in unlicensed bands: The rising stars in the iot and smart city scenarios. *IEEE Wireless Communications*, 23(5):60–67, 2016.

[2] J. Classen, M. Schulz, and M. Hollick. Practical covert channels for wifi systems. In *2015 IEEE Conference on Communications and Network Security (CNS)*, pages 209–217. IEEE, 2015.

[3] A. Dutta, D. Saha, D. Grunwald, and D. Sicker. Secret agent radio: Covert communication through dirty constellations. In *International Workshop on Information Hiding*, pages 160–175. Springer, 2012.

[4] S. D'Oro, F. Restuccia, and T. Melodia. Hiding data in plain sight: undetectable wireless communications through pseudo-noise asymmetric shift keying. In *IEEE INFOCOM 2019-IEEE Conference on Computer Communications*, pages 1585–1593. IEEE, 2019.

[5] R. Eletreby, D. Zhang, S. Kumar, and O. Yağan. Empowering low-power wide area networks in urban settings. In *Proceedings of the Conference of the ACM Special Interest Group on Data Communication*, pages 309–321. ACM, 2017.

[6] G. EPCglobal. Epc radio-frequency identity protocols generation-2 uhf rfid; specification for rfid air interface protocol for communications at 860 mhz–960 mhz. *EPCglobal Inc., November*, 2013.

[7] A. Gadre, R. Narayanan, A. Luong, S. Kumar, A. Rowe, and B. Iannucci. Frequency configuration for low-power wide-area networks in a heartbeat. In *USENIX NSDI 2020*.

[8] R. G. Gallager. *Information theory and reliable communication*, volume 588. Springer, 1968.

[9] A. Gamage, J. C. Liando, C. Gu, R. Tan, and M. Li. Lmac: Efficient carrier-sense multiple access for lora. In *The 26th Annual International Conference on Mobile Computing and Networking (MobiCom'20)*, 2020.

[10] V. Gligor. Covert channel analysis of trusted systems. a guide to understanding. Technical report, NAVAL COASTAL SYSTEMS CENTER PANAMA CITY FL, 1993.

[11] I. Grabska and K. Szczypiorski. Steganography in wimax networks. In *2013 5th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, pages 20–27. IEEE, 2013.

[12] I. Grabska and K. Szczypiorski. Steganography in long term evolution systems. In *2014 IEEE Security and Privacy Workshops*, pages 92–99. IEEE, 2014.

[13] S. Grabski and K. Szczypiorski. Steganography in ofdm symbols of fast ieee 802.11 n networks. In *2013 IEEE Security and Privacy Workshops*, pages 158–164. IEEE, 2013.

[14] J. Haxhibeqiri, E. De Poorter, I. Moerman, and J. Hoebeke. A survey of lorawan for iot: From technology to application. *Sensors*, 18(11):3995, 2018.

[15] HopeRF. Rf95. https://www.hoperf.com/modules/lora/RFM95, 2019.

[16] S. Hosseinzadeh, H. Larijani, K. Curtis, A. Wixted, and A. Amini. Empirical propagation performance evaluation of lora for indoor environment. In *2017 IEEE 15th International Conference on Industrial Informatics (INDIN)*, pages 26–31. IEEE, 2017.

[17] K. M. in San Francisco. Decoding the Chinese Super Micro super spy-chip super-scandal: What do we know – and who is telling the truth?, url = https://bit.ly/2NlY9lS, year=2018, lastaccessed = Oct 4, 2018.

[18] M. Knight. Gr-lora. https://github.com/BastilleResearch/gr-lora, 2019.

[19] M. Knight and B. Seeber. Decoding lora: Realizing a modern lpwan with sdr. In *Proceedings of the GNU Radio Conference*, volume 1, 2016.

[20] B. W. Lampson. A note on the confinement problem. *Communications of the ACM*, 16(10):613–615, 1973.

[21] Y. Li, J. Yang, and J. Wang. Dylora: Towards energy efficient dynamic lora transmission control. In *IEEE INFOCOM 2020*.

[22] Z. Li and Y. Chen. Achieving universal low-power wide-area networks on existing wireless devices. In *2019 IEEE 27th International Conference on Network Protocols (ICNP)*, pages 1–11. IEEE, 2019.

[23] J. C. Liando, A. Gamage, A. W. Tengourtius, and M. Li. Known and unknown facts of lora: Experiences from a large-scale measurement study. *ACM Transactions on Sensor Networks (TOSN)*, 15(2):16, 2019.

[24] G. Pasolini, C. Buratti, L. Feltrin, F. Zabini, C. De Castro, R. Verdone, and O. Andrisano. Smart city pilot projects using lora and ieee802. 15.4 technologies. *Sensors*, 18(4):1118, 2018.

[25] Y. Peng, L. Shangguan, Y. Hu, Y. Qian, X. Lin, X. Chen, D. Fang, and K. Jamieson. 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*, pages 147–160. ACM, 2018.

[26] J. Petäjäjärvi, K. Mikhaylov, R. Yasmin, M. Hämäläinen, and J. Iinatti. Evaluation of lora lpwan technology for indoor remote health and wellbeing monitoring. *International Journal of Wireless Information Networks*, 24(2):153–165, 2017.

[27] M. Schulz, J. Link, F. Gringoli, and M. Hollick. Shadow wi-fi: Teaching smartphones to transmit raw signals and to extract channel state information to implement practical covert channels over wi-fi. In *Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services*, pages 256–268. ACM, 2018.

[28] Semtech. Home security system with lora technology. https://www.semtech.com/uploads/technology/LoRa/app-briefs/, 2019.

[29] Semtech. Lora transceivers semtech sx1276. https://www.semtech.com/products/wireless-rf/lora-transceivers/sx1276, 2019.

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

[31] K. Szczypiorski and W. Mazurczyk. Hiding data in ofdm symbols of ieee 802.11 networks. In *2010 International Conference on Multimedia Information Networking and Security*, pages 835–840. IEEE, 2010.

[32] F. Van den Abeele, J. Haxhibeqiri, I. Moerman, and J. Hoebeke. Scalability analysis of large-scale lorawan networks in ns-3. *IEEE Internet of Things Journal*, 4(6):2186–2198, 2017.

[33] X. Wang, L. Kong, L. He, and G. Chen. mlora: A multi-packet reception protocol in lora networks. In *2019 IEEE 27th International Conference on Network Protocols (ICNP)*, pages 1–11. IEEE, 2019.

[34] Wired. 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/, 2019.

[35] A. J. Wixted, P. Kinnaird, H. Larijani, A. Tait, A. Ahmadinia, and N. Strachan. Evaluation of lora and lorawan for wireless sensor networks. In *2016 IEEE SENSORS*, pages 1–3. IEEE, 2016.

[36] K. Wu, H. Tan, Y. Liu, J. Zhang, Q. Zhang, and L. M. Ni. Side channel: Bits over interference. *IEEE Transactions on Mobile Computing*, 11(8):1317–1330, 2012.

[37] X. Xia, Y. Zheng, and T. Gu. Ftrack: parallel decoding for lora transmissions. In *Proceedings of the 17th Conference on Embedded Networked Sensor Systems*, pages 192–204, 2019.

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

[39] S. Zander, G. Armitage, and P. Branch. A survey of covert channels and countermeasures in computer network protocols. *IEEE Communications Surveys & Tutorials*, 9(3):44–57, 2007.

[40] G. Zhang, C. Yan, X. Ji, T. Zhang, T. Zhang, and W. Xu. Dolphinattack: Inaudible voice commands. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 103–117. ACM, 2017.

[41] E. Zielinska and K. Szczypiorski. Direct sequence spread spectrum steganographic scheme for ieee 802.15. 4. In *2011 Third International Conference on Multimedia Information Networking and Security*, pages 586–590. IEEE, 2011.