SECURITY THREATS AND COUNTERMEASURES OF LORA PHYSICAL LAYER

HOU NINGNING

PhD

The Hong Kong Polytechnic University

2021

The Hong Kong Polytechnic University
Department of Computing

Security Threats and Countermeasures of LoRa Physical Layer

Hou Ningning

A thesis submitted in partial fulfilment of the requirements

for the degree of Doctor of Philosophy

May 2021

CERTIFICATE OF ORIGINALITY

I hereby declare that this thesis is my own work and that, to the best of my knowledge and belief, it reproduces no material previously published or written, nor material that has been accepted for the award of any other degree or diploma, except where due acknowledgement has been made in the text.

_____ (Signed)

HOU Ningning (Name of student)

Abstract

LoRa is a popular Low Power Wide Area Networking (LPWAN) technology that is expected to boost the next generation IoT for its capability to provide long-range ubiquitous connectivity for everyday objects with an AA battery. Despite the popularity, there exists a growing concern about the security of LoRa communication. Current LoRaWAN systems are susceptible to security attacks due to the inherent features of LoRa communication. Specifically, LoRa operates at unlicensed frequency bands under public standards, which makes it vulnerable to active attack and information leakage. Besides, LoRa packets have a long transmission window compared with traditional wireless technologies (*i.e.*, Wi-Fi, Bluetooth), which leaves sufficient time for attackers to launch attacks. Meanwhile, the large scale of LoRa deployment with low-cost and low-power devices makes it an ideal target for large-scale cyber attacks.

In this thesis, we investigate security threats and countermeasures of LoRa physical layer. Specifically, we explore the possible security attack at both the transmitter side (covert channel) and receiver side (jamming attack) and propose corresponding countermeasures against such attacks.

The first work 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. Since 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 build the covert channel using a COTS LoRa node (Tx) and a low-cost receive-only software-defined radio (Rx). Comprehensive evaluations show that `CloakLoRa` can send covert information over 250 m.

The second work investigates jamming of LoRa PHY and corresponding countermeasure. LoRaWAN forms a one-hop star topology where LoRa nodes send data via one-hop up-link transmission to a LoRa gateway. If the LoRa gateway can be jammed by attackers, the LoRa gateway may not be able to receive any data from any nodes in the network. Our empirical study shows that although LoRa physical layer (PHY) is robust and resilient by design, it is still vulnerable to synchronized jamming chirps. Potential protection solutions (*e.g.*, collision recovery, parallel decoding) may fail to extract LoRa packets if an attacker transmits synchronized jamming chirps at high power. To protect the LoRa PHY from such attacks, we propose a new protection method that can separate LoRa chirps from jamming chirps by leveraging their difference in the received signal strength in power domain. We note that the new protection solution is orthogonal to existing solutions which leverage the chirp misalignment in time domain or the frequency disparity in frequency domain. Besides, we discuss new types of attacking methods (*e.g.*, consecutive SFDs) and analyze their impacts on LoRa packet reception. We conduct experiments with COTS LoRa nodes and software-defined radios with varied experiment settings such as different spreading factors, bandwidths, and code rates. The results show that synchronized jamming chirps at high power can jam all previous solutions, while our protection solution can effectively protect LoRa gateways from the jamming attacks.

Publications arising from the thesis

1. **Ningning HOU**, Yuanqing Zheng, "CloakLoRa: A Covert Channel over LoRa PHY", IEEE 28th International Conference on Network Protocols (ICNP). IEEE, 2020.

2. **Ningning HOU**, Xianjin Xia and Yuanqing Zheng, "Jamming of LoRa PHY and countermeasure", IEEE 39th International Conference on Computer Communications (INFOCOM). IEEE, 2021.

3. Xianjin Xia, **Ningning HOU** and Yuanqing Zheng, "PCube: Scaling LoRa Concurrent Transmissions with Reception Diversities", The 27th Annual International Conference On Mobile Computing And Networking (MobiCom). ACM, 2021.

4. **Ningning HOU**, Xianjin Xia and Yuanqing Zheng, "Don't Miss Weak Packets: Boosting LoRa Reception with Antenna Diversities", under review, submitted to IEEE 40th International Conference on Computer Communications (INFOCOM). IEEE, 2022.

5. **Ningning HOU**, Yuanqing Zheng, "CloakLoRa: A Covert Channel over LoRa PHY", under review, submitted to IEEE/ACM Transactions on Networking (TON) in Octorber 2020.

6. **Ningning HOU**, Xianjin Xia and Yuanqing Zheng, "Jamming of LoRa PHY and countermeasure", under review, submitted to IEEE/ACM Transactions on Networking (TON) in February 2021.

Acknowledgements

Throughout the journey to becoming a Ph.D., I have received a great deal of support and assistance.

Firstly, I would like to express my sincere gratitude to my supervisor Prof. Zheng Yuanqing for his great support and guidance during my Ph.D. study. His great patience, continuous motivation, and immense knowledge helped me a lot in the past four years and will leave a lifelong impact on me. He said that research means "re- search" what you thought you have known and got something new. This view motivates me to stay hungry and stay foolish. His vision on impactful research inspired me when I was confronted with challenges and drives me to pursue a higher target. It is my great honor and luck to have a supervisor like him. I shall always remain indebted to my dear supervisor, and I hope that I can be a supervisor like him if I become a supervisor in the future. I am also grateful to my co-supervisor Prof. Xiao Bin. His insightful advice and critical judgment help me a lot in both research and life.

I sincerely appreciate my co-authors. I really appreciate the help and efforts from Dr. Xia Xianjin. I learned much through working closely with him and through his day-to-day insights about academia. And, while I have not had the opportunity to collaborate with Dr. Wang Yanwen(yet), he has served as an insightful bro at various points of my Ph.D. journey.

I would also like to thank Dr. Yang Lei, Dr. Lou Wei, Dr. Li Moand Dr. Gu Tao for their significant help and constructive and insightful suggestions during my Ph.D. study.

My sincere thanks also go to Ms. Cui Kaiyan, Mr. Yang Qiang, Mr. Shou Junhao, Mr. Liu Lihao for their kind help. I am indebted to them for their volunteering in hundreds of experiments and for providing me with feedback on numerous iterations

of my papers and talks. I learned so much from them. Meanwhile, I want to thank the supporting team in PolyU COMP department for their kind assistance with my experiments.

Besides, I would like to thank my dear friends and colleagues, Dr. Wang Shanshan, Dr. Lin Dongmei, Dr. Yang Wei, Ms. Ma Yeping, Mr. Li Shuai, Mr. Wang Fang, Ms. Cheng Haiming, Dr. Yang Yanni, Mr. An Zhenlin, Mr. Lu Zexin, Ms. Zhang Jie, Mr. Zhou Yu, Ms. Guo Wanwan, and Ms. He Mengxia for their companion, support, and tolerance. We used to have a lot of happy times and unforgettable trips. Thanks for brightening my journey!

Last but not least, I would like to thank my dear parents and all my family members for their firm support and selfless love. Thank you for believing in me when I lost belief in myself. I love you so much!

Table of contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Background

Recent years have seen the era of IoT (Internet of Things). Ericsson [24] forecasts that around 25 billion devices will connect to the Internet by 2025. Forbes [26] even triples the number of connected IoT devices to 75 billion by 2025, meaning that almost every object around us: streetlights, water pumps, cars, machines, meters, elevators, thermostats, wearables, *etc.* will be connected. The surging growth of IoT applications promises to bring immense value into our lives. For instance, in healthcare, smart infant monitors [68] can provide parents with real-time information about their baby's breathing, skin temperature, body position, and activity level on their smartphones. In smart city, sensors are installed at all parking spots and pass the occupancy status of each spot to the cloud. Applications catch the data and then guide drivers through the shortest route to an open spot. In smart industrial automaton, product flow monitoring, inventory management, quality control, packaging optimization, *etc.* are already being deployed intensively.

IoT envisions innovations by starting with ubiquitous communications. Since applications are widely diverse and multifaceted, there are several leading wireless technologies in support of different kinds of IoT usage scenarios. A common way to categorize IoT communication technologies is according to the desired commu-

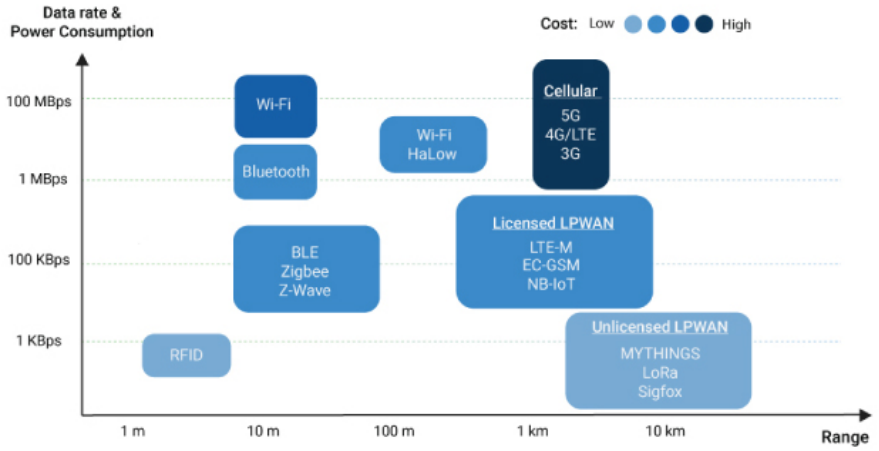


Figure 1.1: Comparison of existing IoT wireless communication technologies [10].

nication range. Specifically, RFID is commonly used to support short-range (*i.e.*, within 5 m) and low data rate requirement applications. Zigbee, Bluetooth, and Wi-Fi support a similar communication range (*i.e.*, 10-100 m) but Wi-Fi enables a higher data rate. However, these technologies are handicapped by their short-range signal coverage when applied to applications that require tens of kilometers such as in smart cities. Cellular technologies (*i.e.*, 3G/4G) thus have been used to cope with this problem. They are more suitable for longer range (*i.e.*, 1 km) as well as high data rate applications. However, cellular systems require high-capacity power supplies along with high-cost hardware and operational cost. Therefore, a low-cost, low-power, and long-range method is needed in IoT communications. To fill in this gap, Low power wide area network (LPWAN) emerged and it 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 (*i.e.*, 10 km) at extremely low power consumption.

LoRa-enabled applications are expected to grow in various fields, including the following example areas but not limited to [75]:

- **Smart Utilities**: This field is expected to witness the biggest growth rate. Traditional utility operations are labor-intensive because meters are often located in dense urban environments, indoors or even underground, which is hard to reach by many wireless technologies. By implementing LoRa-enabled sensors and LoRaWAN protocols, utility and metering companies can collect data remotely and use it for better management of resources.

- **Smart Agriculture**: LoRaWAN has been widely deployed to enable smart agriculture. For example, LoRa-enabled sensors have been used to measure environmental conditions(*i.e.*, temperature, humidity, *etc.*) that will influence crop production. It is reported that commercial farms [77] can save as much as 50% water consumption by implementing LoRa-based smart irrigation solution.

- **Smart Environment**: Benefiting from low power, low cost, and long communication range, LoRa is suitable for smart environment applications. Sensors and gateways embedded with LoRa technology can be deployed across a region to measure environmental indicators. The collected data can be analyzed to detect issues before they become crises. For instance, a LoRa-based autonomous flood sensor system [83] can be installed into complex, hard-to-reach regions along the water's edge in marshland, rough terrain, *etc.* to monitor water levels. These sensors are autonomous, weather-proof, and requiring no external power or wired network connection, which is suitable for the toughest environment.

- **COVID-9 Support**: COVID-19 pandemic brings the world unprecedented challenges. Recently, LoRa technologies have been used to provide public safety solutions [6] to fight against Coronavirus. For instance, medical gas valve equipped with LoRa technology can transmit digital pressure values remotely, allowing hospital staff to monitor and control the amount of oxygen remaining

in the cylinder miles away.

IoT brings vast opportunity while it also brings vast risks, among which security is a challenging one. Many previous works study security issues in traditional wireless communication methods such as RFID [35], Bluetooth [79], Wi-Fi [7], and cellular technologies [25]. Since LPWAN is relatively new, there are few works study security risks in LPWAN. Specifically, both NB-IoT and LTE-M are derived from LTE. The authentication and encryption security features by design make them more secure than LoRaWAN systems that operate at unlicensed spectrum. This thesis focuses on LoRa and explores potential security risks and corresponding countermeasures in LoRaWAN physical layer.

1.2 LoRa Primer

LoRa PHY. LoRa refers to the physical layer (PHY) of LoRaWAN, while LoRaWAN is the communication protocol and system architecture for the network. LoRa 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 at a constant rate over time. The chirp sweeps through and wraps around a predefined bandwidth. Fig. 1.2 shows the PHY samples of a LoRa packet collected with low-cost software defined radios (SDR).

LoRa uses different initial frequencies to modulate symbols. Fig. 1.3 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 $f_0 = -BW/2$

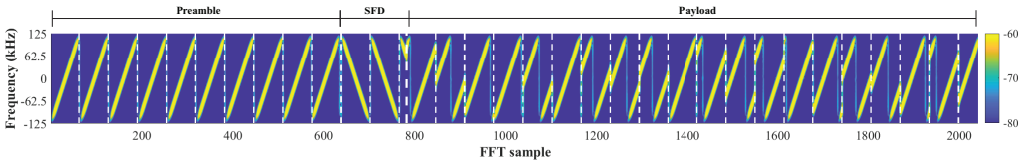


Figure 1.2: LoRa packet structure.

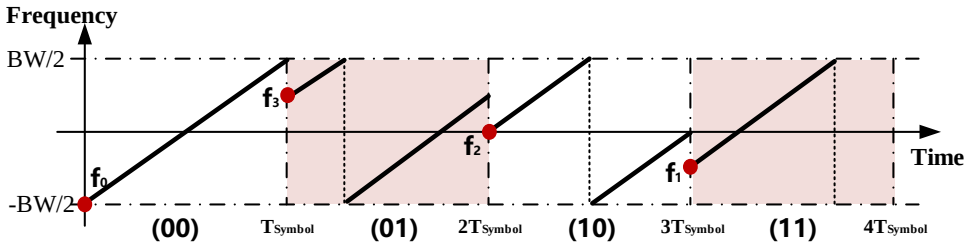


Figure 1.3: Example of CSS modulation.

is named base chirp, which modulates '00' as shown in Fig. 1.3.

In practice, depending on the spreading factor SF ($7 \leqslant SF \leqslant 12$), the number of possible symbols is 2^{SF}. Such a procedure can be represented as follows.

$$S(t, f_{sym}) = e^{j2\pi(\frac{k}{2}t+f_0)t} \cdot e^{j2\pi f_{sym}t} = C(t) \cdot e^{j2\pi f_{sym}t} \tag{1.1}$$

where f_{sym} denotes the initial frequency of an up-chirp (*i.e.*, encoded symbol). $C(t) = e^{j2\pi(\frac{k}{2}t+f_0)t}$ represents the base chirp; f_0 and k denote the initial frequency and increasing rate of base chirp, respectively.

LoRa Packet Structure. Fig. 1.2 shows PHY samples of a LoRa packet collected with software defined radios (SDR). A LoRa packet starts wtih several identical up-chirps as preamble and 2 sync word symbols followed by 2.25 start frame delimiter (SFD) as illustrated in the figure. In explicit header mode, physical header and payload follow the SFD in a LoRa packet. LoRa packets can have a varied number of preamble (*e.g.*, $>$ 4 up-chirps), but sync word and SFD are mandatory.

LoRa Packet Detection and Demodulation. LoRa packet reception process involves several key steps as illustrated in Fig. 1.4. First, a LoRa receiver detects arrivals of LoRa packets by detecting a preamble which consists of more than 4

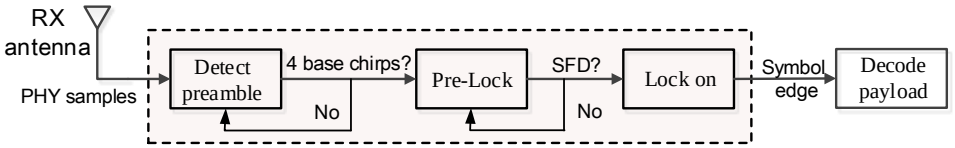


Figure 1.4: Locking process at LoRa receiver.

up-chirps. The preamble detection can be performed by correlating received PHY samples with an up-chirp generated locally at a LoRa receiver [63]. More than 4 consecutive peaks in correlation results indicates the arrival of one LoRa packet. One may also detect a preamble by tracking the continuity of frequency after multiplying incoming PHY samples with down-chirps [102]. After successful preamble detection, a LoRa receiver needs to accurately detect an SFD so as to determine chirp boundaries of PHY header and payload. To this end, a LoRa receiver multiplies incoming PHY samples with an up-chirp and monitors continuous frequency for 2.25 chirp duration to determine the chirp boundary of the first chirp in PHY header and payload. After successfully locking-on the chirp boundaries, a LoRa receiver can demodulate the chirps and decode incoming packets.

To demodulate a received chirp within a demodulation window, a LoRa receiver first multiplies the received signal with the *conjugate of the base chirp* denoted as $C^{-1}(t)$ and performs Fast Fourier Transform (FFT) on the multiplication results. After that, the LoRa receiver searches for the highest spike in FFT bins (which indicates the initial frequency) and thereby demodulate symbols. The demodulation process can be represented as follows

$$S(t, f_{sym}) \cdot C^{-1}(t) = e^{j2\pi f_{sym} t} \tag{1.2}$$

The FFT of $e^{j2\pi f_{sym} t}$ produces one highest spike in the FFT bins, indicating the initial frequency of f_{sym} [102].

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.

1.3 Motivation

LoRa is an emerging technology that enable long-range low-power wireless communication for battery-powered sensor nodes [51, 84, 30, 104]. A LoRa node is expected to transmit LoRa packets with a communication range of 10 km using AA batteries for ten years and enables innovative applications [75, 112, 101, 16] (*e.g.*, smart electricity metering, smart homes, supply chain, and health care). 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 systems are susceptible to security attacks because of the inherent features of LoRa communication. First, LoRa functions at an unlicensed frequency band. Current LoRaWAN secures application layer and network layer with simple 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 active attacks and information leakage. Second, compared to traditional wireless techniques (e.g., Bluetooth, Wi-Fi), LoRa packets usually have a long transmission window.

The long duration leaves sufficient time for attackers to launch spoofing and DoS attacks. Third, the large scale of LoRa deployments with low computation and power resources make it an ideal target for large-scale cyber attacks.

Covert channel attack is a typical attack in terms of information leakage. In specific, for example, in a smart home where LoRa-enabled IoT sensors are employed for door access [1], smart electricity, and water meter, a malicious attacker can compromise a sensor node and build a *covert channel* by modulating the neglected PHY parameters (*e.g.*, amplitude) to secretly collect the sensory data of a legitimate LoRa node without affecting the normal communication between it and a gateway. By synthesizing the sensory data of multiple IoT nodes (*e.g.*, building access records, electricity, and water metering, *etc.*), the attacker can learn the 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 [97, 19]. So in this thesis, we aim to reveal the vulnerability and demonstrate the feasibility of building a covert channel over LoRa PHY. We present the detailed implementation and evaluation in Chapter 3.

The above attack happens at the transmitter side. How about gateways at the receiver side? Is it secure for gateways to receive LoRa packets correctly without attack? Unfortunately, gateways are not safe either.

Jamming attack is a threat to LoRa gateway. LoRa adopts chirp spread spectrum (CSS) modulation in the physical layer (PHY), which is known to be resilient and robust to interference and noise. Therefore, it can transmit several kilometers away. Benefiting from the long communication range, LoRaWAN forms a one-hop star topology, where a large number of LoRa nodes can send packets via one-hop up-link transmissions to a LoRa gateway, which greatly simplifies the network pro-

tocol design and facilitates data collection. In such a star topology, however, if a LoRa gateway is jammed by malicious attackers, the LoRa gateway may not be able to receive LoRa packets from any nodes in the network, leading to a single point of failure. Neighbor gateways could help receive the packets in this case, but those gateways can also be under jamming attacks.

We note that wireless jamming attack has been extensively studied in literature [58] and LoRa jamming has also been attracting attention from both academia and industry recently. Some previous works [9, 69, 57] have demonstrated that it is indeed possible to jam LoRa nodes to some extent by emitting various jamming signals, while other measurement studies [51, 102, 23] show that LoRa nodes are inherently resilient and robust to interference and can even support parallel transmissions by resolving collisions. Therefore, deep analyses are needed to better understand LoRa demodulation under jamming attacks. We introduce our empirical study of jamming of LoRa PHY and countermeasure with COTS LoRa nodes and software defined radios in Chapter 4.

In summary, LoRa's inherent features make it vulnerable to attacks. It is indeed necessary to investigate the security threats of LoRa physical layer.

1.4 Contribution

This thesis mainly consists of two works I have done during my Ph.D. study. In this thesis, we study possible security issues at both the transmitter side and receiver side.

In the first work, we study the covert channel over LoRa PHY. Current LoRaWAN secures application layer and network layer with symmetric encryption. However, the PHY layer remains less protected. We observe that along the demodulation process, a LoRa receiver only examines the initial frequency of a LoRa chirp while over-

looks other physical layer parameters (*i.e.*, amplitude, phase, waveform, *etc.*). Based on this observation, we design and implement 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 can demodulate the original CSS information as the frequencies of LoRa chirps are unchanged. And the covert receiver 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 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. Besides, we also evaluate the impact of a 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 the 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.

In the second work, we study jamming attack at the receiver. Jamming attack is a common attack in wireless networks. What makes it special for LoRa is that LoRa signal itself is anti-interference by design. Previous works [9, 36, 94] have considered jamming attack as an attack component. However, these works lack comprehensive study and deep analysis of LoRa demodulation under jamming attacks. To fill this gap, we conduct experiments with COTS LoRa nodes and software defined radios. Our empirical study indicates that jamming attacks (*e.g.*, random interference and jamming chirps) may not necessarily affect packet receptions at LoRa gateways, meaning that LoRa by design is resilient to a certain type of jamming attacks and intentional interference.

By conducting deep analysis, however, we notice that if jamming chirps are well-aligned with LoRa chirps, LoRa gateways cannot extract the LoRa chirps from jamming chirps anymore. As such, a malicious attacker can send synchronized chirps at high power to jam LoRa chirps, which leads to dramatic performance degradation of LoRa communication. We note that existing time domain collision recovery solutions (*e.g.*, FTrack [102], mLoRa [93]) leverages misalignment edges of LoRa symbols. However, if LoRa chirps and jamming chirps are aligned, they cannot be separated

in the time domain. Frequency domain collision recovery solutions (*e.g.*, Choir [23]) cannot help either since attackers can send jamming chirps at the same frequency of LoRa chirps.

To further enhance LoRa PHY against synchronized jamming chirps, we propose a new protection method that separates LoRa chirps from jamming chirps by leveraging their difference in signal strength. We note that the new protection method is orthogonal to existing solutions which leverage timing information (*e.g.*, chirp boundary misalignment) or frequency information (*e.g.*, frequency disparity). As such, our protection method can be integrated with existing collision recovery solutions and complement each other.

We implement our jammer and protection method and conduct experiments with COTS LoRa nodes as well as software defined radios. Experiment results show that well-synchronized jamming chirps at high transmission power can jam all previous solutions with very high success rates, while our protection method can effectively protect LoRa gateways from all known LoRa jamming attacks including synchronized jamming chirps.

1.5 Thesis Structure

This thesis consists of six chapters:

- **Chapter 1** briefly introduces the research background and motivation, summarizes my main works, and highlights the research framework of my Ph.D. study;
- **Chapter 2** introduces the state-of-the-art works of LoRaWAN and reviews literature about security issues in existing wireless communication technologies. In specific, literature related to LoRaWAN security is highlighted;

- **Chapter 3** presents our experience in design, implementation, evaluation and application of `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 the current LoRaWAN security mechanism. We conduct comprehensive evaluations under various experiment settings. Our work is a pilot work that reveals the security vulnerability of LoRa PHY and LoRaWAN deployment;

- **Chapter 4** investigates the vulnerability of the current LoRaWAN physical layer under jamming attacks. We expose the risk of LoRa gateways under the attack of synchronized jamming chirps, which could lead to a single point of failure in LoRaWAN. We also propose a new collision recovery method as a countermeasure against the attack of synchronized jamming chirps by leveraging the difference in signal strength of jamming chirps and LoRa chirps. Comprehensive experiments are conducted with COTS LoRa nodes as well as software defined radios under various experiment settings. Experiment results demonstrate the effectiveness of our jamming and protection methods.

- **Chapter 5** presents my future work directions and some of our preliminary results.

- **Chapter 6** concludes the thesis.

Chapter 2

Literature Review

Recent successful deployments of low-power wide-area networks are attracting more attention from academia. A variety of LPWAN technologies such as SigFox [80], NB-IoT [70], LTE-M [47] and LoRa [5] have been deployed to support wide area network connection for IoT devices. In this thesis, we focus on LoRa and refer readers to [81, 92] for detailed comparison of existing LPWAN technologies. The goal of this chapter is to review works related to LoRa security. Before that, We will first introduce recent popular research topics of LoRa and introduce some state-of-the-art works. We also present security-related works in other wireless technologies to highlight the significance of LoRaWAN security.

2.1 LoRa Frontiers

2.1.1 LoRa Measurement Study

Recent years have seen the advent of LPWAN. Early researches on LoRa and LoRaWAN devote their efforts to measurement study and performance analysis [48, 60, 12, 30, 65, 64, 52]. Specifically, [12, 30] focus on energy consumption of LoRa. [12] introduces an energy consumption model based on LoRa and LoRaWAN. This model offers estimations of power consumption of different sensor node elements, which can be used in power management algorithms to maximize the sensor node

lifetime. EF-LoRa [30] aims to achieve energy consumption fairness among end devices in LoRa networks. It formulates the energy fairness problem as an optimization problem and studies the influence of different parameters (*i.e.*, frequency channels, spreading factors, *etc.*) on energy consumption. [65] focuses on the coverage of LoRa technology and conduct real-life measurements. This paper claims a maximum communication range of over 15 km on ground and nearly 30 km on water.This work also provides a channel attenuation model derived from the real-world measurement data. Except for power consumption and communication distance, LoRa's packet air time, the impacts of different parameters, and performances in different environments are evaluated in [66, 41, 62, 13, 91, 98, 60, 48]. Recent work [52] verifies the common claims about LoRa by comprehensive experiments and further provides an in-depth understanding of these claims, which is insightful and encouraging for future research.

Based on the above studies, some improvement schemes [49, 2, 53, 71, 27] are proposed for better performance. Some works aim to optimize parameter settings (*e.g.*, spreading factor [49, 2], frequency selection [27]) to achieve higher throughput and lower power consumption. [53] and [71] formulate optimization problems for maximizing the average packet detection rate and packet error rate fairness inside a LoRaWAN cell respectively. Litenap [104] improves the energy efficiency of LoRa by enabling LoRa nodes to operate in a downclock mode(*i.e.*, sub-Nyquist rates) for packet reception.

Besides measurement study and performance analysis, some early works aim to reverse engineer the proprietary LoRa PHY. The authors of [45] and [73] introduce detailed modulation and encoding elements that comprise the LoRa PHY and provide open source Software-defined radio platforms. These platforms empower wireless developers and security researchers to investigate LoRa and LoRaWAN protocol with great convenience.

2.1.2 Collision Recovery

LoRa is emerging as a compelling technology to achieve the long-standing vision of connecting billions of objects in ubiquitous community. Despite of low-power and long range communication, LoRa in practice faces challenges in ubiquitous connectivity, among which packet collision is one of the major problems to be addressed. Consider future smart cities where a few LoRa gateways collect sensor data from a large number of end-devices in the city. Radios will often collide as the deployment of end-devices becomes denser. Such collisions will drain battery life and waste spectrum resources in dense networks. The root cause of this problem is the limited capacity of both LoRa end-device and gateway. On one hand, LoRa end-devices are constrained by the limited power budget and computation resource, which cannot support sophisticated MAC layer and physical layer schemes to avoid collisions. On the other hand, although it is claimed that one gateway can simultaneously demodulate a maximum of eight concurrent transmissions, gateways still struggle to handle such a large number of collisions at city-scale.

To overcome the challenges of dense deployment despite the limited capability of LoRa nodes and gateways, many efforts have been made. [11] and [38] study characters of LoRa collision via simulation as well as commodity devices. While [69] considers multi-gateway and multi-provider to obtain insight into collisions within actual networks. In fact, existing solutions to collision problems in wireless networks can be divided into two categories, *i.e.*, collision avoidance and parallel decoding.

- **Collision Avoidance.** Current LoRaWAN uses ALOHA as MAC protocol. Some researchers [67, 72, 106] propose to improve the scalability of LoRaWANs through packet scheduling and try to adopt new MAC layer protocols (*e.g.*, CSMA). However, due to the lack of hardware support, full-fledged CSMA implementation is hard to achieve. DeepSense [43] takes advantages of artificial

neural networks to perform carrier sense. The high level idea of DeepSense is that neural networks can learn the coding mechanisms employed by LoRaWAN. Therefore, it can perform carrier sense to identify LoRa signals hidden in the noise. Recent work LMAC [29] leverages channel activity detection (CDA), which is available on all of the latest LoRa chips, to detect the occupancy of a targeted communication channel. To balance the communication loads, LMAC also designs and implements two advancing versions of CSMA. One advanced version balances communication loads among logic channels (*i.e.*, defined by different frequencies and spreading factors) by leveraging local information of end nodes. The higher version further combines global information at the gateway to achieve better performance. LMAC required no modifications to COTS LoRa node, which makes it readily deployed to current LoRaWAN networks. However, LMAC cannot handle hidden terminal problem, which is common in wireless networks.

- **Parallel Decoding.** Another kind of works [23, 93, 102, 103, 15, 54, 95, 37, 108, 96] aim at addressing collision problem with parallel decoding. Although LoRa encourages concurrent transmissions with different SFs at the same channel, it cannot disentangle collisions in the same channel with the same SF. To name a few, Choir [23] leverages frequency offsets introduced by hardware imperfection of LoRa devices to differentiate collisions. However, in practice, the frequency offset can drift due to various influencing factors (*e.g.*, phase jitters, time offset, temperature, *etc.*), which is not reliable to separate collisions. Besides, it is difficult to extract frequency offset under low SNR. FTrack [102] separates collisions by jointly exploiting the distinct frequency tracks and misaligned edges of LoRa symbols. This is motivated by two characteristics of LoRa frame. First, the symbol edges of symbols from the same frame is pe-

riodic, while symbols edges of different frames are usually misaligned in time. Second, the frequencies of LoRa chirps keep increasing in between the symbols edges, while frequencies change suddenly at the symbol edges. mLoRa [93] exploits Successive Interference Cancellation (SIC) to decode colliding packets. It iteratively decodes the partial clean symbols and then cancels them from the colliding signals. This method can only decode up to three collisions. CoLoRa [89] groups LoRa chirps to their corresponding LoRa nodes by examining the power level of the same frequency in different demodulation windows. The insight of CoLoRa is that the height of the peak of an incomplete chirp segment is proportional to the length of the segment. Two peaks of the same chirp at adjacent demodulation windows have the same frequency. They define peak ratio to represent the height of the latter peak to that of the former one. Thus, for chirps from the same frame, the peak ratio will also be the same. By calculating peak ratio, they can group symbols into different frames and then decode them. There are other works leveraging time offset between collided frames. For example, Pyramid [109] enables real-time LoRa collision decoding with peak tracking. NScale [88] amplifies the time offsets between colliding packets with non-stationary signal scaling.

At the heart of the above methods (except Choir), they leverage packet time offset to disentangle collided packets. However, these methods cannot work when collided packets are well-aligned in time. This leaves researchers to explore new dimension of methods to do parallel decoding. In contrast, in this thesis, we utilize this limitation of current parallel decoding methods to launch synchronized jamming attack. In our design, a jammer transmits jamming chirps intentionally to interfere the reception of legitimate chirps. To avoid being separated by the enhanced gateway with parallel decoding capability, we

further make jamming chirps align with legitimate chirps in both frequency and time domain.

Backscatter is another way to enable connectivity of billions of everyday objects. Compared with active radios, backscatter is extremely low power, smaller and cheaper for increasing access at scale. LoRa's high sensitivity and anti-interference properties make it a desirable choice for backscatter. LoRa backscatter [87] achieves wide-area backsctter communication with a range of hundreds of meters. However, it requires an extra device to generate the excitation signal. While PLoRa [63] takes ambient LoRa signal as excitation signal. PLoRa modulates data on the excitation signal and formulates it into a new LoRa chirp. By shifting this chirp to a new LoRa channel, the backscatter signal can be received by gateways without collision or interference with of original LoRa signal.

2.1.3 LoRa Sensing

Wireless sensing has attracted a lot of research attention with various wireless signals, including Wi-Fi RFID, mmWave, acoustic, and visible light. The basic idea behind wireless sensing is that the movements of target will cause signal variations in the reflected signal. We can get rich information about target by analyzing the signal variation. A variety of applications have been achieved by wireless sensing including indoor/outdoor localization, tracking/navigation, gesture/activity recognition and vital sign monitoring. However, due to the intrinsic nature of employing the weak reflected signal for sensing, the sensing range is limited. For example, the state-of-the-art Wi-Fi localization [82] can only achieve localization range of 100 meters, which is still not enough for long range sensing applications. Fortunately, LoRa offers exciting opportunities to significantly increase the sensing range to kilometers. LoRa adopts Chirp Spread Spectrum (CSS) to modulate data. This unique technology enables

LoRa to communicate even below the noise. Gain from the intrinsic nature of CSS modulation, LoRa is powerful and preferable for long-range sensing.

- **Localization.** Localization is one of the most popular sensing applications. [42] first studies the feasibility of using LoRa signal for indoor localization. They conduct experiments in both Line-of-Sight and None-Line-of-Sight scenarios and validate that LoRa is more stable than Wi-Fi and Bluetooth. However, this work uses RSSI measurement to localize target, which is still a coarse-grained estimation. Recent work uLocate [59] develops a multi-band backscatter prototype that works across 900 MHz, 2.4 and 5 GHZ. This work achieves 3D localization with ranges of up to 60 m away from the AP and accuracy of sub-meters. In contrast, WideSee [17] explores the passive sensing capability of LoRa signal. Combined with the mobility of a drone, WideSee achieves contactless wide-area sensing with a single LoRa transceiver pair. However, the localization error (*i.e.*, within 4.6 m) of this passive method is much higher than uLocate [59].

- **Activity Detection.** Efforts have also been made to human activity detection. [39], [4] and [40] study LoRa technology for human activity recognition. However, these works only leverage the long-range communication capability of LoRa to collect and transfer sensor data rather than utilize the LoRa signal itself for contact-free sensing. The latest works [112, 105, 17] move one step forward to explore the passive sensing capability of LoRa signal with off-the-shelf LoRa hardware without using dedicated sensors. [112] enables long-range through-wall sensing by exploring the long propagation distance and strong penetration capability of LoRa signal. It develops a signal propagation model and achieves fine-grained respiration sensing even when the target is 25 m away and tracks coarse-grained human walking 30 m away from the LoRa transceiver

pair. However, this work suffers severe interference. Sen-fence [105] addresses this issue in LoRa sensing by creating a virtual fence, which increases the movement-induced signal variation to its maximum possible value if the reflection signal is from the targeted area and keep the signal variation unchanged if the movement occurs outside of the virtual fence to constrain sensing within the area of interest. Sen-fence achieves fine-grained respiration monitoring with a sensing range of 50 m, twice the state-of-the-art sensing range of [112].

2.1.4 Cross Technology

Cross-technology Communication (CTC) technologies have gain increasing interest in recent years. Enable LoRa-based IoT devices to interact directly with other types of wireless radios such as Wi-Fi and Bluetooth in a heterogeneous environment is desirable. LoRaBee [78] enables cross-technology communication from LoRa to ZigBee, where information are conveyed from LoRa to ZigBee by embedding specific bytes in the payload of legitimate LoRa packets. ZigBee devices can extract the data by sampling the received signal strength (RSS) of the corresponding LoRa chirps. BLE2LoRa [50] presents a novel Bluetooth Low Energy (BLE) to LoRa CTC technology, which leverages the frequency shifting feature of BLE to construct ladder-shaped signals to emulate the spectrum of LoRa chirp. Specifically, it resembles a LoRa chirp by carefully manipulating the payload bits in a BLE frame to generate chirp-like signals. LoRaBee and BLE2LoRa only enables two kind of cross-technology communication. In contrast, XFi [55] enables mobile devices to use commodity WiFi radio to directly and simultaneously collect data from diverse heterogeneous IoT devices, including Wi-Fi, ZigBee and LoRa.

2.2 LoRa Security

Recent decades have seen wireless infrastructure and services proliferating to meet the rapidly increasing demands of IoT. Meanwhile, it is reported [85] that attacks are growing alongside the IoT, where billions of devices are abused for illicit criminal activities. As for LoRa, [8] analyzes the LoRaWAN stack, and investigates potential security vulnerabilities in different layers. Analysis demonstrates that due to the broadcast nature of wireless communication, LoRaWAN's physical layer is extremely vulnerable to attacks. Therefore, we mainly focus our study on security of physical layer. Before diving into security issues of LoRa PHY, we first study related works in other wireless technologies, for example, RFID, Bluetooth and WiFi,*etc.*, to gain some insights.

2.2.1 Common Attacks in PHY

Jamming attack is a common wireless attack. A malicious node in wireless networks can generate interference signals intentionally to disrupt the data communications between legitimate users. Wireless jamming has been extensively studied in literature [107, 115, 56]. To against jamming, spread spectrum techniques, such as DSSS (Direct Sequence Spread Spectrum) and FHSS (Frequency-Hopping Spread Spectrum) are commonly adopted. These techniques defend against jamming attacks by spreading the transmit signal over a wider spectral bandwidth than its original frequency band. Chirp Spread Spectrum (CSS) is also a kind of spread spectrum technique, that is why LoRa signal is robust to noise and resilient to interference.

Recent works study the impact of jammer to LoRaWAN and propose countermeasures. LoRaTS [36] studies the attack-aware data timestamping in LoRaWAN, which can protect LoRaWAN against frame delay attack. The key insight is that such an attack will introduce frequency biases. LoRaTS integrates a COTS LoRa node and

software defined radio to track the frequency biases caused by a legitimate node. To provide sufficient resolution for detecting the tiny frequency biases, LoRaTS develops a new time domain signal processing technology based on an analytic model of LoRa's CSS modulation. This method can achieve higher frequency resolution than Choir [23], which uses dechirping and traditional FFT pipeline to measure decimal part of frequency. LoRaTS also points out that using LoRa chirps to create collisions is more stealthy than brute-force jamming. SLoRa [94] leverages physical layer features to improve the security performance of LoRaWAN. The high-level idea of this work is to exploit the hardware imperfections of low-cost LoRa radios components. Specifically, it exploits CFO and link signature to do LoRa node authentication. To extract fine-grained CFO, SLoRa first proposes a CFO compensation algorithm and then uses an SVM model to mitigate the noise with linear fitting for received upchirps. In addition to CFO, it also combines spatial-temporal link signature, which presents large variation when transmitters are placed at different positions. Besides, Aras *et al.* [8] provide an analysis of the LoRaWAN network and identify a few security vulnerabilities of LoRaWAN including encryption key extraction, jamming attacks, and replay attacks. Aras *et al.* further explores jamming attacks in [9], where they use commodity LoRa nodes as jammers to selectively jam LoRa packets. This paper highlights that LoRa is vulnerable to a suite of attacks because of the slow modulation type.

Note that the aforementioned collision recovery and parallel decoding schemes in previous section can be used as countermeasures to against jamming attack if the jammer uses chirps as jamming signal. Basically, gateways can consider chirp jamming signals as collision packets and can use collision recovery method to extract legitimate packets from the received signal. In contrast, in this thesis, we study the impact of synchronized jamming chirps, which can mimic the legitimate chirps in both frequency domain and time domain. As a result, gateways equipped with

collision recovery schemes still fail to recover the legitimate chirp. Meanwhile, we propose countermeasure to protect against such new jamming attacks by leveraging information in a third domain (*i.e.*, power domain). Details can be found in Chapter IV.

In addition to jamming attacks, *covert channel attack* [90] has long been an area of interest for attackers. Covert channel was first introduced by Lampson [46]. It makes use of wireless medium to transmit information in a way that can bypass the security scheme of that system. Many works point out the potential covert channels in computer networks and different communication systems. [111] surveys the covert channels and countermeasures in computer network protocols. [14, 22] propose to use regularity tests to detect covert channels.

Covert channels in OFDM, WiMax, and LTE systems are introduced in [86, 32, 33]. Those works build covert channels by padding frames or packets. Other covert channels in OFDM and Wi-Fi systems are introduced in [18, 20, 34, 114]. Shadow Wi-Fi [74] embeds covert information by pre-filtering Wi-Fi frames prior to transmission. The covert receiver then extracts embedded information by analyzing CSI. And importantly, the modification on the transmitter side do not impact the reception of such frames by normal receiver. This is the first physical layer covert channel where both the transmitter and receiver are implemented on COTS Wi-Fi chip that is installed in smartphones. Another work hiding information in Wi-Fi is PN-ASK-WiFi. PN-ASK-WiFi [21] uses pseudo-noise asymmetric shift keying (PN-ASK) modulation to embed secret information into Wi-Fi signals. Specifically, it maps covert data by shifting the amplitude of primary symbols. Since a Wi-Fi receiver only cares about the phase of a symbol and regards the amplitude variation as the impact of noise or path loss degradation, it cannot detect the covert information. In this way, PN-ASK-WiFi successfully hides data to eavesdroppers who have no prior knowledge about this channel. There are also works build covert channel in acoustic signal. Dolphi-

nattack [113] is a typical one. Dolphinattack [113] launches hidden voice commands by modulating voice commands on ultrasonic carriers. Due to the non-linearity of microphone circuits, the modulated covert data (*i.e.*, low frequency commands) can be correctly demodulated and interpreted by the speech recognition systems. Recent work NICScatter [110] 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 [100] generates intended interference patterns in wireless communication to build an in-band covert channel without degrading the effective throughput of main channel.

LoRa is a quite new technology. There may exist vast opportunities to build covert channel over LoRa or LoRaWAN, which is a great concern for users. However, we have not found papers working on covert channel over LoRa PHY. To fill this gap, in this thesis, we prototype a covert channel over LoRa PHY, which reveals the vulnerability of current LoRaWAN physical layer.

2.2.2 Summary

Through literature review, we find that LoRa networks are susceptible to security attacks. The reason can be summarized in two folds. First, LoRa communication functions at unlicensed frequency band and uses very simple protocol to secure the communication, making it vulnerable to active attacks such as jamming attack. Second, compared with traditional wireless communications (*e.g.*, Wi-Fi), the time duration of LoRa packet is very long, which leaves sufficient time for attackers to launch DoS and spoofing attacks. In convention, we can enhance the security performance of LoRaWAN by adopting sophisticated cryptography mechanism in MAC layer [3]. However, this is infeasible due to the constrained resource of LoRaWAN

and limited low-cost hardware of LoRa node.

Chapter 3

A Covert Channel over LoRa PHY

3.1 Background and Motivation

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 [1], 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

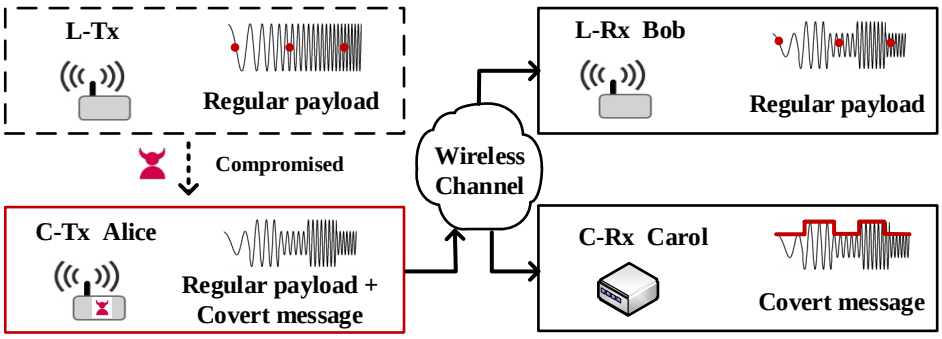


Figure 3.1: Covert communication scenario. Alice transmits regular LoRa packets to Bob and the malware on Alice embeds covert information by modulating the amplitude of transmitted LoRa signal. Bob does not check the amplitude of received signal. Only Carol will decode the covert AM information.

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 [97, 19].

In this work, 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 link 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 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 work 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.

3.2 Covert Channel over LoRa PHY

3.2.1 System Model and Assumptions

Fig. 3.1 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 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 pack-

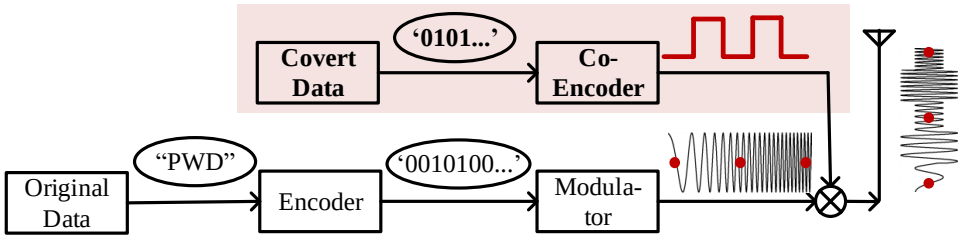


Figure 3.2: Workflow of covert channel transmitter.

ets. 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 also assume that an attacker does not necessarily need to access the sensor data from the device. An attacker can derive the covert bits from many different ways without accessing the sensor data. For example, an attacker may infer the data changing rate of a sensor by checking the charge and discharge rate of a specific capacitor. 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. e

3.2.2 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.

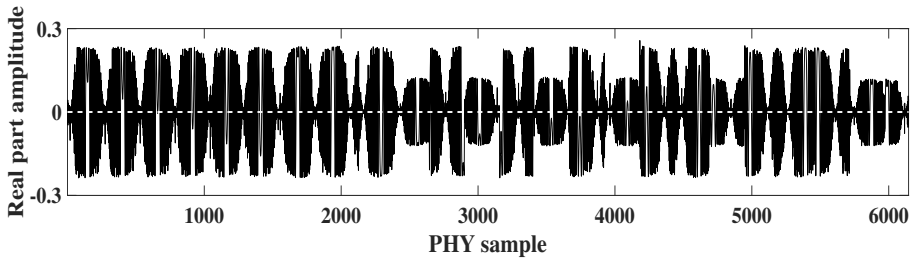
3.3 Covert Channel Design and Implementation

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.

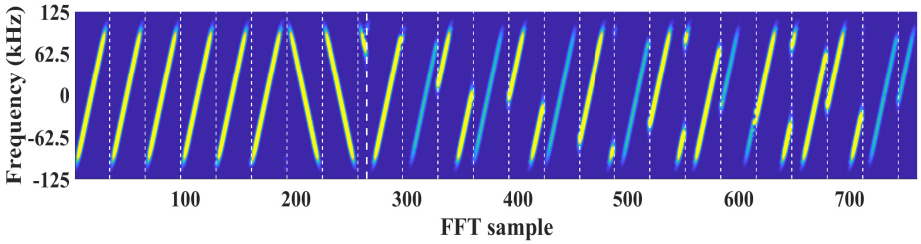
3.3.1 Proof-of-concept with Software Defined Radio

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 [44]. We add an amplitude-modulated (AM) component as shown in Fig. 3.2, 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



(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.

Figure 3.3: Covert channel signals captured by a software defined radio. The amplitude of LoRa chirps are modulated to carry covert information.

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. 3.3 shows the PHY samples collected by Carol. In both time domain (Fig. 3.3(a)) and frequency domain (Fig. 3.3(b)), we can observe alternating amplitudes of chirps in payload. The signal strength is color coded in Fig. 3.3(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.

3.3.2 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, 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 and Semtech sx1276 chip 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. 3.4, 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

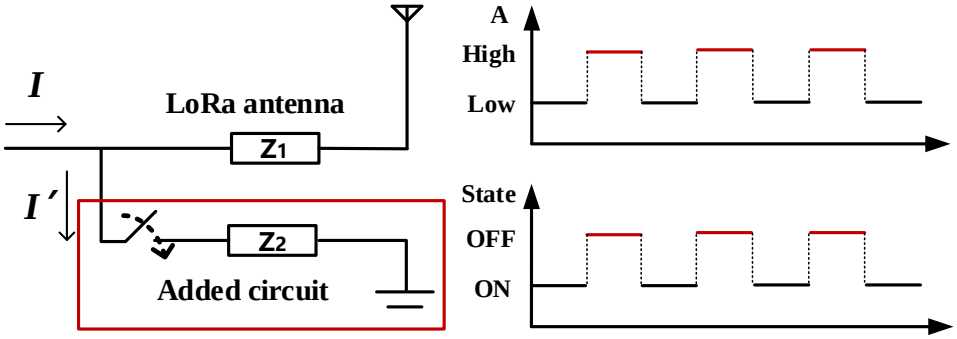


Figure 3.4: Circuit design. The ON/OFF state of the switch controls the amplitude of the outgoing signals. As a result, covert information can be conveyed to the receiver.

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. 3.5 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. 3.4. 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.

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 $BW = 250$ KHz). That means every 5 LoRa chirps are used to encode 1-bit covert information. Fig. 3.6 shows the received

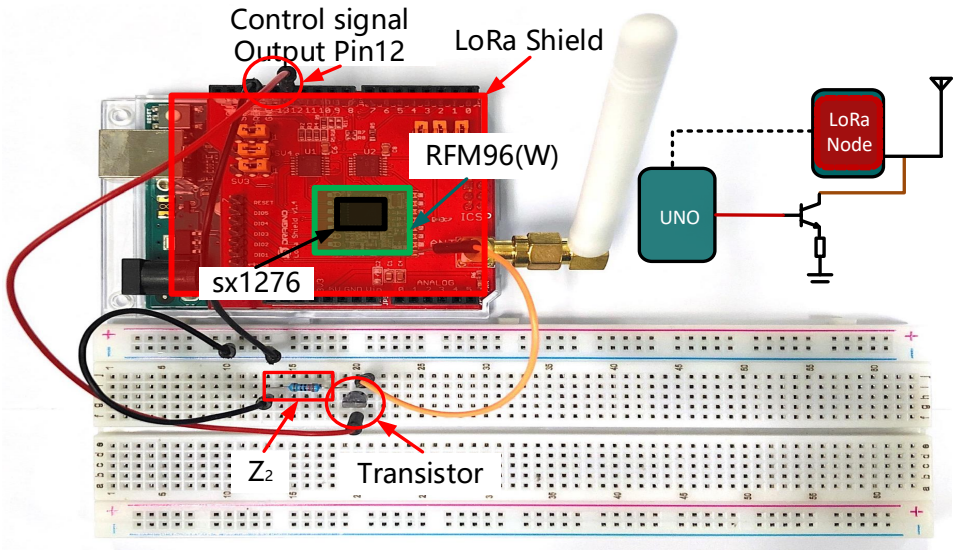


Figure 3.5: Hardware implementation of transmitter. The LoRa node is compromised to leak information. A low-cost transistor is used as a switch to directly modulate the amplitude of LoRa chirps.

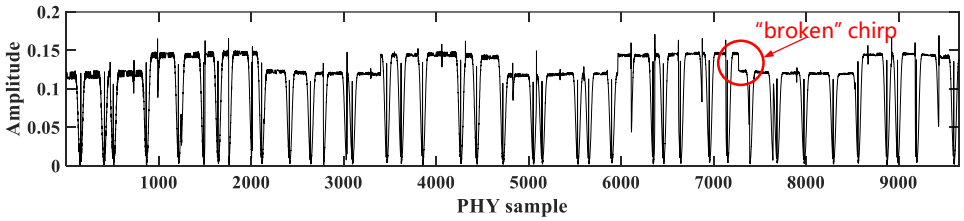
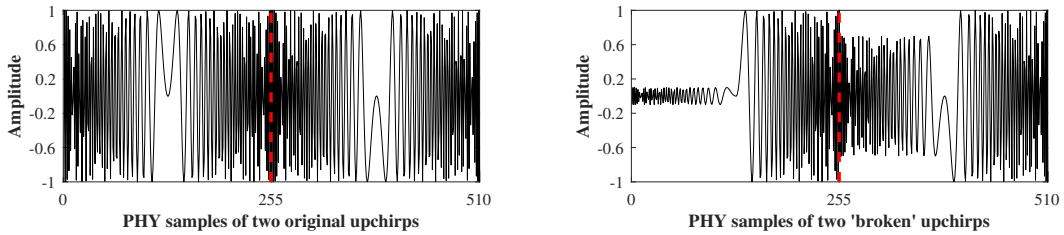


Figure 3.6: Physical samples of covert message with LoRa node.

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. 3.6, 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. 3.7, we



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

Figure 3.7: Original up-chirps and broken up-chirps.

first generate two complete up-chirps (Fig. 3.7(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. 3.7(b). In Fig. 3.7(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. 3.5) 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.

3.3.3 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. 3.8 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

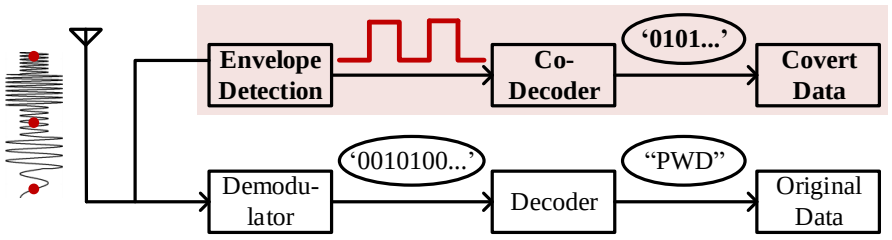


Figure 3.8: Workflow of covert channel receiver and regular LoRa receiver.

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 [44].

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.

3.3.4 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. 3.9 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. In particular, we use 8 alternating chips

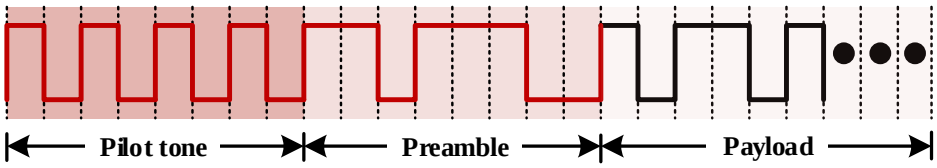


Figure 3.9: Covert packet structure.

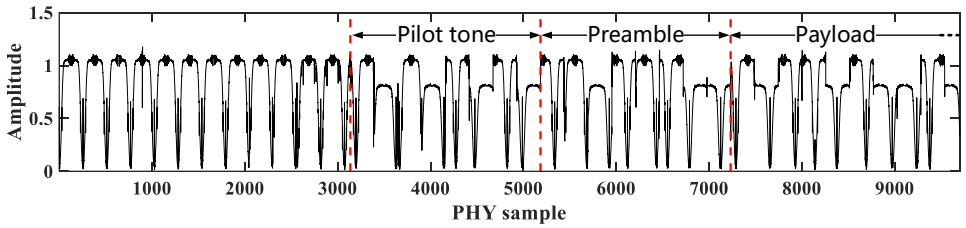


Figure 3.10: Physical samples of covert message.

(*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.

Packet reception. At the receiver side, the RTL-SDR records the received PHY samples. Fig. 3.10 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.

3.4 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 [31, 28]. 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:

$$I_c = K \times \frac{1}{2} \log_2 \left(1 + \frac{S}{N}\right) \tag{3.1}$$

where K is the amplitude changing rate of the transmitted signal. K is determined by the changing rate of switch in Fig. 3.5. $\frac{S}{N}$ 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:

$$S_r \propto \frac{(AD)^2}{r^2} = \frac{D^2}{r^2} P_{Tx} \tag{3.2}$$

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. 3.1 and Eq. 3.2, we can improve the covert channel efficiency by using a larger D (*e.g.*, 0.9) and a smaller r. Fig. 3.12 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. 3.11, 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

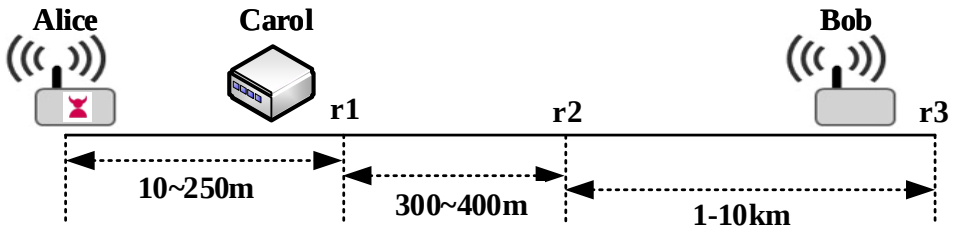
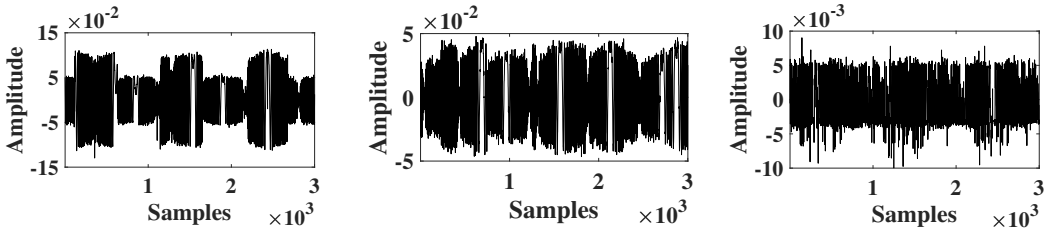


Figure 3.11: Efficiency versus distance.



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

Figure 3.12: Amplitude of signals recorded by SDR at different distances.

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.

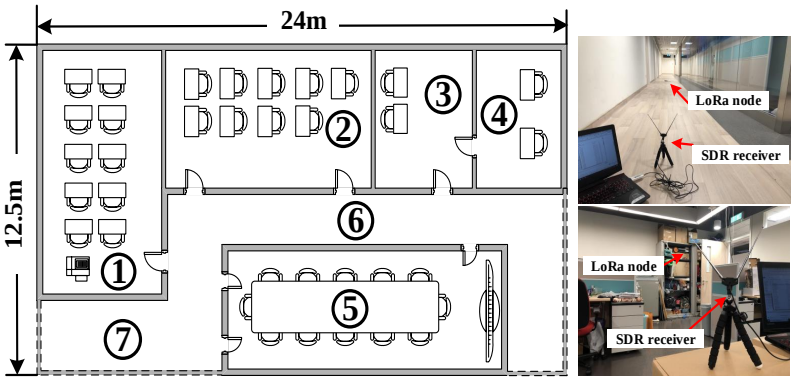
Besides D, channel condition also influences the regular LoRa communication. Since LoRa receiver has very high sensitivity, there is a large SNR margin to tolerate the reduction in chirp amplitude. AM modulated LoRa packets can be still received and decoded correctly when the amplitude change is within 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 3.5.4. 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. 3.11, in practice, Alice can adjust the transmission power and modulation depth so that Carol can receive within a range (*e.g.*, between 10 m to 250 m).

3.5 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) Outdoor experiment map.



(b) Indoor experiment map.

Figure 3.13: Experiment layout.

3.5.1 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 shown in Fig. 4.11. Outdoor field spans 279×205 m^2 (Fig. 4.11(b)) while a typical office building with the size of 12.5×24 m^2 (Fig. 4.11(a)).

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 3.1(a).

Default parameters: covert channel. We present the key parameters of covert channel transmitter and receiver in Table 3.1(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. We also measure the throughput of both covert channel and regular LoRa channel.

3.5.2 Effective Range of Covert Communication

We conduct this experiment in outdoor field (Fig. 4.11(b)). 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 3.1: **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. 3.14 shows the average and variance 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.

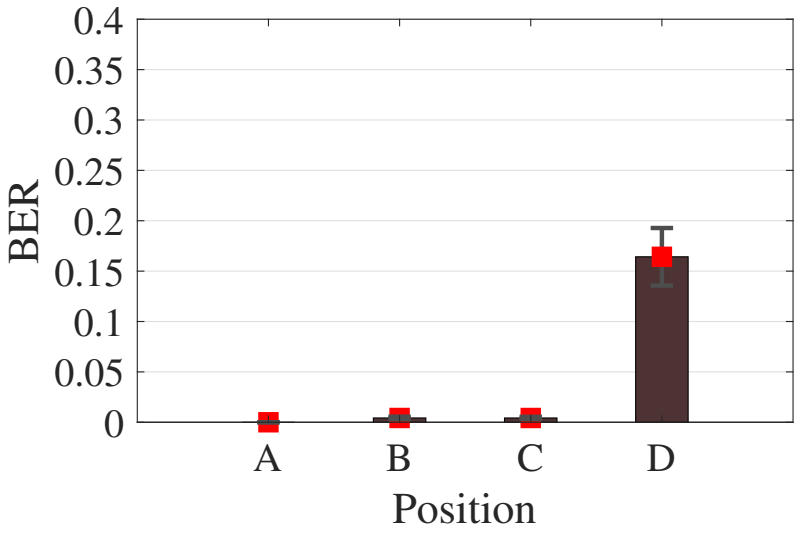


Figure 3.14: Outdoor performance at different positions.

3.5.3 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 3.1.

Fig. 3.15 shows the average BER and standard deviation of covert channel with different modulation depths of Tx ranging from 0.04 to 0.09. We only present the results with $0.04 \leqslant D \leqslant 0.09$. That is because the performance is most sensitive to D in such a range in this experiment setting. We notice that when $D = 0.04$,

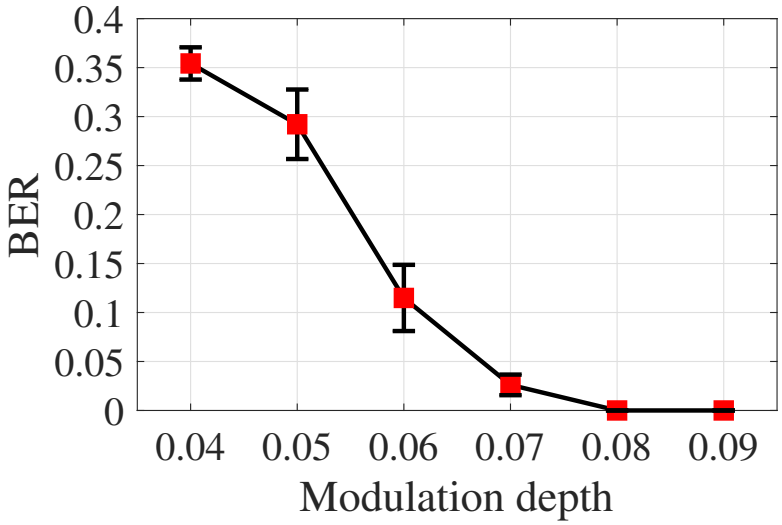


Figure 3.15: BER of covert channel using different modulation depths.

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.

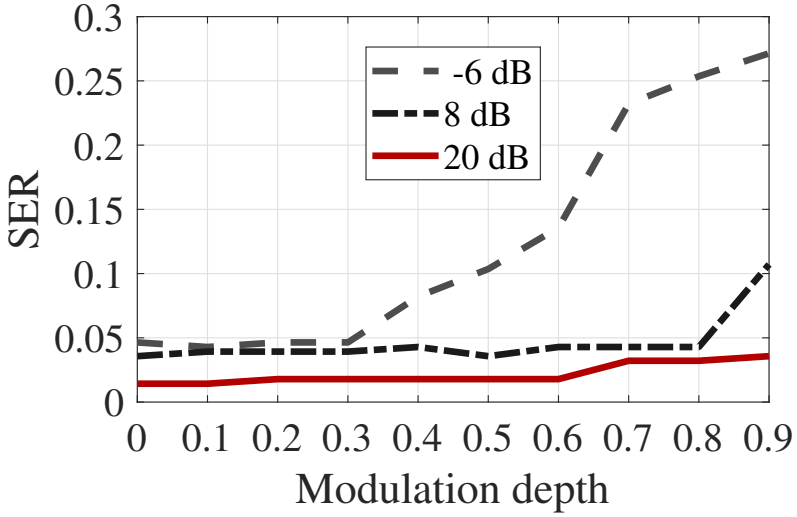


Figure 3.16: Symbol error rate of regular LoRa packets with different modulation depth.

3.5.4 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. 3.16 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

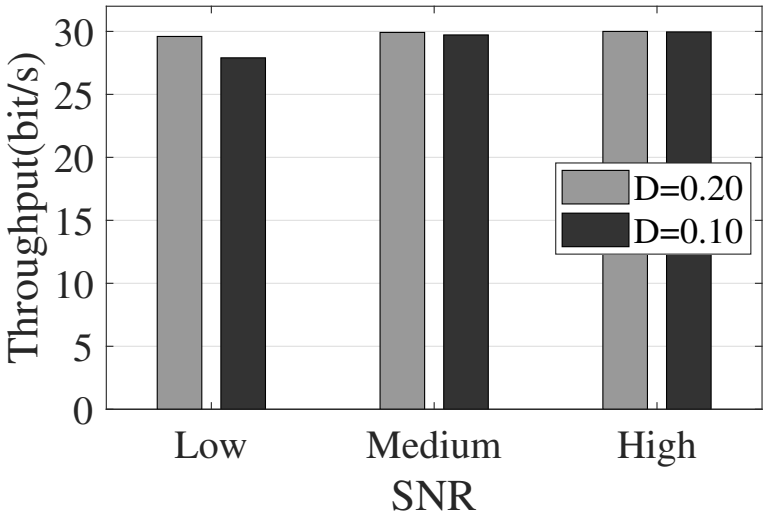


Figure 3.17: Throughput of covert channel.

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.

3.5.5 Throughput of Covert Channel and LoRa Regular Channel

In this subsection, we evaluate the throughput of covert channel and LoRa regular channel in different SNR scenarios. In this experiment, we configure the transmitter

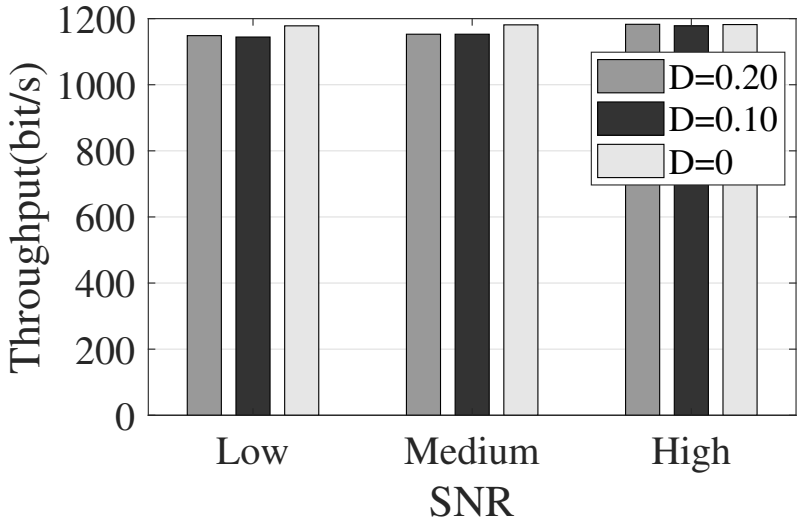


Figure 3.18: Throughput of regular node.

Alice (USRP) to transmit covert packets once per second. We put the RTL-SDR receiver at different locations and categorize the received signal into low, medium and high SNR conditions. The payload length of each covert packet and LoRa regular packet are 30 bits and 1200 bits, respectively. We evaluate the throughput with $D = 0.1$ and $D = 0.2$.

Fig. 3.17 shows the throughput of covert channel. We can observe that covert channel has almost ideal performance when SNR is high. In low SNR condition, the throughput with larger D (*i.e.*, $D = 0.2$) is better than that of smaller D (*i.e.*, $D = 0.1$). This is because a larger D means a larger variance in the amplitude of covert signal, which benefits the decoding process especially when the received signal strength is weak.

Fig. 3.18 shows the throughput of regular LoRa node with different D under different SNR conditions. In this experiment, we also evaluate the throughput of regular LoRa packets without varying its amplitude (*i.e.*, $D = 0$). We can observe from Fig. 3.18 that the regular LoRa node has larger throughput as SNR condition becomes better. We also noted that when $D \leqslant 0.2$, the covert channel has almost

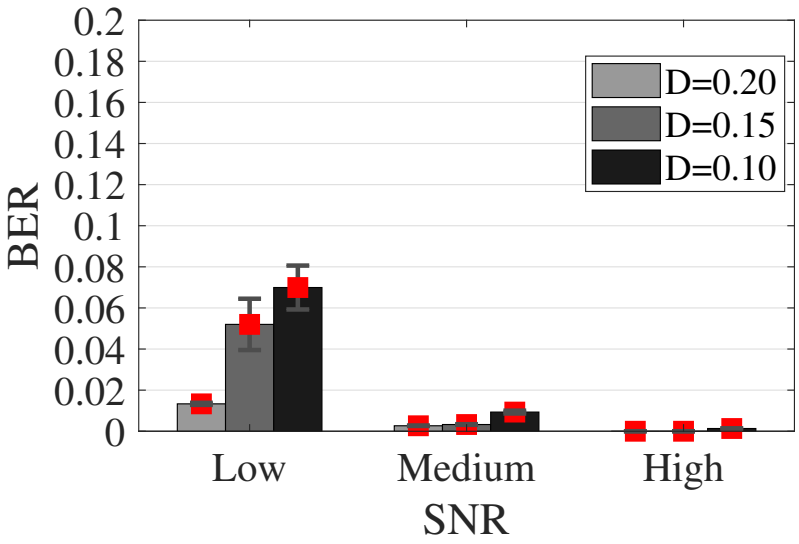


Figure 3.19: Performance of covert channel coexisting with other regular LoRa signals.

no influence on the throughput of regular LoRa channel.

3.5.6 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. 4.11(a). 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. 3.19, 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.

3.5.7 Impact of Different Sampling Rates

In order to successfully decode the covert messages sent by C-Tx, C-Rx should be able to receive the PHY samples that can capture the amplitude changes of LoRa chirps. We conduct this experiment in a meeting room ⑤ in Fig. 4.11(a). We set the transmission power of C-Tx to 5 dBm, which is the minimum transmission power. A LoRa shield can vary transmission power from 5 dBm to 23 dBm. C-Rx is positioned 5 m away from C-Tx. The gain of the covert channel receiver is set to 10 dB. We vary the receiving sampling rates with 250 Kbps, 300 Kbps, and 500s Kbp. 500 Kbps is the Nyquist Frequency of LoRa chirp signal. Other default parameters are set as in Table 3.1.

Fig. 3.20 plots the Cumulative Distribution Function (CDF) of BER using the above 3 different receiving sampling rates of C-Rx. We can observe from Fig. 3.20 that better performance can be achieved with higher receiving sampling rates. We note that these 3 sampling rates are much higher than the frequency of switch changes. By doing so, we can track a more complete and finer-grained envelope with a higher sampling rate, which leads to more accurate synchronization. Since we can achieve a better performance by increasing the sampling rates at the covert

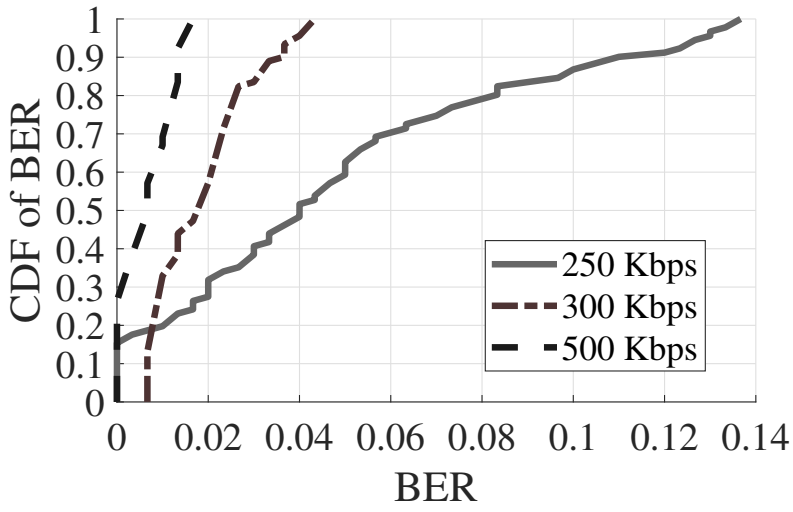


Figure 3.20: CDF of covert channel BER using different receiving sampling rate.

channel receiver side, we use $2 \times BW$ (500 Kbps) as the receiving sampling rate in the following experiments.

3.5.8 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. 4.11(a), corridor ⑥ and ⑦), (2) multipath-rich office (Fig. 4.11(a), room ①-⑤) and (3) dynamic environment with people walking nearby (Fig. 4.11(a), room ①). We use COTS LoRa device as Tx by adding a transistor and an impedance as shown in Fig. 3.5. The receiver is still the low-cost SDR. In each environment, we configure the covert channel transceiver by using default setting parameters in Table 3.1.

Fig. 3.21 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

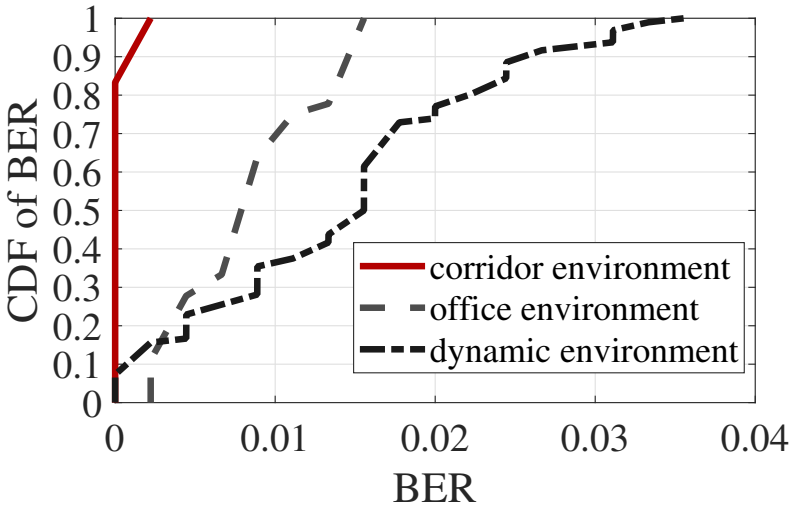


Figure 3.21: BER of covert channel under various environments.

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.

3.5.9 Through-wall Performance

This experiment aims to evaluate the performance of the covert channel in the through-wall scenarios, since C-Tx and C-Rx can be separated by walls in prac-

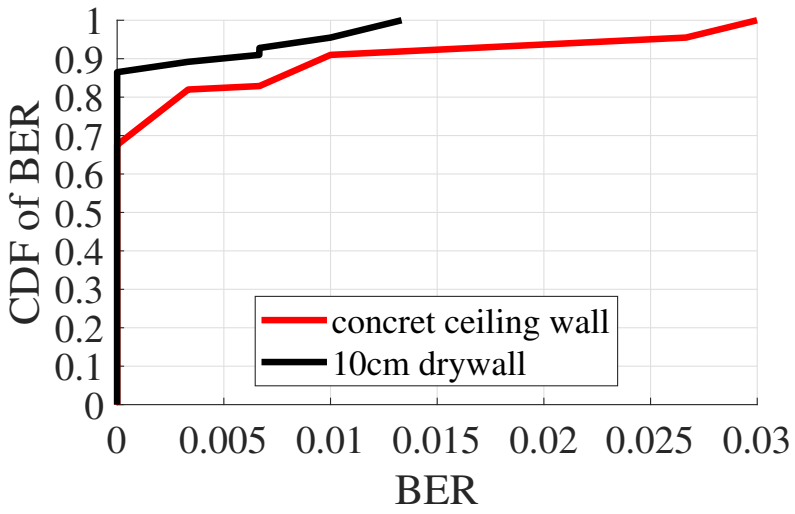


Figure 3.22: Through-wall performance.

tice. We conduct the experiment using USRP in a typical office building which is depicted in Figure 4.11(a). We test two scenarios: 1) a 10 cm drywall and 2) a concrete ceiling. The ceiling is made of reinforced concrete and metal studs. In the first scenario, C-Tx is placed inside the office room ① and C-Rx is placed in corridor ⑥. While in the second scenario, C-Tx is placed inside of office room ② and C-Rx is placed in an office room on the upper floor. The two office rooms have typical furniture including wooden tables, leather chairs, and large LED panel. We keep the doors of office rooms closed when conducting experiments. We configure the transmission power and receive gain to 10 dBm and 20 dB. We set the modulation depth to $D = 0.8$ to penetrate the walls. C-Tx and C-Rx are separated by a 10 cm drywall with a distance of around 2 m.

Fig. 3.22 plots the CDF of BER in the through-wall experiments. The experiment results show that covert data can be decoded with high accuracy in through-wall scenarios. Nearly 70% packets can be decoded without any errors even through the reinforced concrete ceiling wall and nearly 90% packets can be decoded without any errors through the 10 cm drywall. The maximum BER measured in the experiments

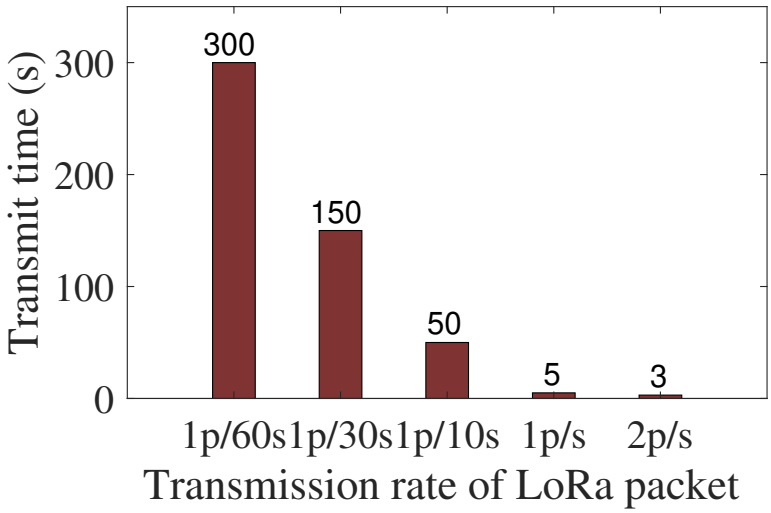


Figure 3.23: The time to leak 128-bit sensitive information (*e.g.*, NwkSKey).

is only 3%.

The results raise security concerns, since covert packets can be correctly decoded with a high accuracy even through walls. Note that in the experiment we set the lowest transmission power. Besides, a smaller modulation depth can further increase the decoding accuracy and the communication distance between C-Tx and C-Rx in the through-wall scenarios.

3.5.10 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. 3.23. 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.

3.6 Covert Channel for Security Enhancement

A covert channel can be used by attackers as well as defenders. Next, we show an example of using covert channel to enhance the security. Consider LoRaWAN-enabled fire (or earthquake) alarm and signaling systems [61]. These safety-critical cyber-physical systems are of great importance in early detection and further response to disruptive events. However, some malicious nodes may spoof the system by sending false data to trigger false alarms. In such systems, information provided by sensors is usually blindly believed to be trustworthy, which gives chances for malicious nodes to launch false alarm attacks.

To protect such fire alarm systems from false alarm attacks, we can build covert channels to secretly authenticate the alarming signals. Specifically, when a legitimate node transmits data with high security level (*i.e.*, alarming signal), it can add authentication information over the covert channel. Then the gateway can use the covert authentication information to check whether this alarming is from a legitimate node or a malicious node. The covert channel can hide the authentication information

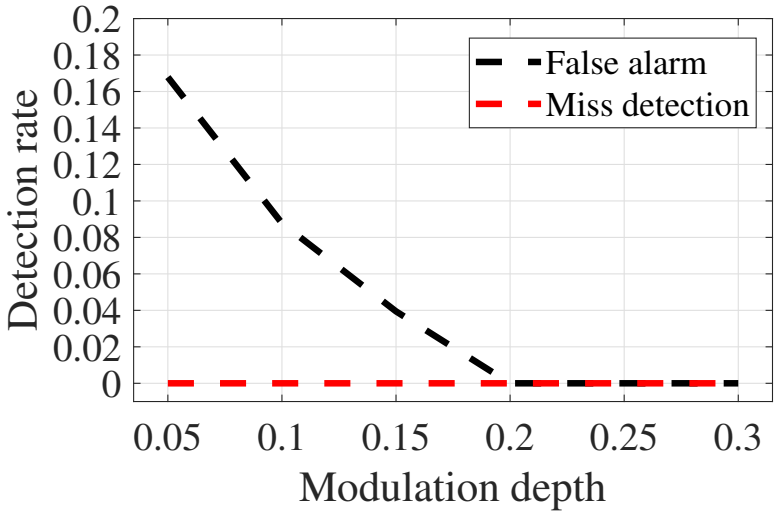


Figure 3.24: False alarm rate and miss detection rate of deceptive packets.

and is transparent to other LoRa devices. Since malicious nodes only transmit and receive LoRa signals, they cannot pass the authentication of the gateway. Therefore, the deceptive signals and malicious nodes could be filtered out by the gateway. We also envision many other scenarios that can benefit from covert channels for security enhancement including secret key sharing and one-time password delivering.

We further conduct a case study experiment using covert channel to filter out deceptive packets. LoRa packets without covert authenticate information are regarded as deceptive messages sent by malicious nodes. In this experiment, we use one USRP to transmit LoRa packets with covert authentication information (working as a legitimate node) and another USRP to transmit pure LoRa packets without covert authentication information (working as a malicious node). These two USRPs transmit LoRa packets alternatively. For the legitimate USRP, we evaluate with different modulation depth to encode covert data. With each modulation depth, we conduct over 200 measurements. We evaluate the miss detection rate and the false alarm rate of the malicious node. In our experiment, if a legitimate covert authentication packet has bit error rate larger than 0.4, the gateway will consider it as a deceptive packet.

This is a false alarm case of malicious nodes. Correspondingly, if a pure LoRa packet can be synchronized to our predefined covert message pilot tone and preamble and the BER is less than 0.4, we consider it as a miss detection of malicious node.

Fig. 3.24 shows the results. The black dash line shows the false alarm rate of deceptive packets and the red dash line shows the miss detection rate. In this experiment, the miss detection rate remains 0, meaning that all deceptive packets without covert authentication information cannot pass the authentication of the gateway. False alarm rate decreases as modulation depth increases and it reaches to 0 when $D = 0.2$. For real world applications, we can further decreases the false alarm rate by modifying D according to the node-gateway distance and channel quality.

3.7 Discussion

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 vulnerability 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 vulnerabil-

ity 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.

3.8 Conclusion

This work 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.

Chapter 4

Jamming of LoRa PHY and Countermeasure

4.1 Introduction and Motivation

Low-power wide-area networks such as LoRaWAN are emerging technologies that enable long-range low-power wireless communication for battery-powered sensor nodes [52, 84, 30, 104]. A LoRa node is expected to transmit LoRa packets with a communication range of 10 km using AA batteries for ten years and enables innovative applications [75, 112, 101, 17] (*e.g.*, smart electricity metering, smart homes, supply chain, and health care).

LoRa adopts chirp spread spectrum (CSS) modulation in physical layer (PHY), which is known to be resilient and robust to interference and noise. Benefiting from the long communication range, LoRaWAN forms a one-hop star topology, where a large number of LoRa nodes can send packets via one-hop up-link transmissions to a LoRa gateway, which greatly simplifies the network protocol design and facilitates data collection. In such a star topology, however, if a LoRa gateway is jammed by malicious attackers, the LoRa gateway may not be able to receive LoRa packets from any nodes in the network, leading to single point of failure. Neighbor gateways could help receive the packets in this case, but those gateways can also be under jamming

attacks.

We note that wireless jamming has been extensively studied in literature [58] and LoRa jamming has also been attracting attention from both academia and industry recently. Some previous works [9, 69, 57] have demonstrated that it is indeed possible to jam LoRa nodes to some extent by emitting various jamming signals, while other measurement studies [52, 102, 23] show that LoRa nodes are inherently resilient and robust to interference and can even support parallel transmissions by resolving collisions. To better understand LoRa demodulation under jamming attacks, we conduct experiments with COTS LoRa nodes and software defined radios. Our empirical study indicates that jamming attacks (*e.g.*, random interference and jamming chirps) may not necessarily affect packet receptions at LoRa gateways, meaning that LoRa by design is resilient to a certain type of jamming attacks and intentional interference.

By conducting deep analysis, however, we notice that if jamming chirps are well-aligned with LoRa chirps, LoRa gateways cannot extract the LoRa chirps from jamming chirps any more. As such, a malicious attacker can send synchronized chirps at high power to jam LoRa chirps, which leads to dramatic performance degradation of LoRa communication. We note that existing time domain collision recovery solutions (*e.g.*, FTrack [102], mLoRa [93]) leverages misalignment edges of LoRa symbols. However, if LoRa chirps and jamming chirps are aligned, they cannot be separated in the time domain. Frequency domain collision recovery solutions (*e.g.*, Choir [23]) cannot help either since attackers can send jamming chirps at the same frequency of LoRa chirps.

To further enhance LoRa PHY against synchronized jamming chirps, we propose a new protection method that separates LoRa chirps from jamming chirps by leveraging their difference in signal strength. We note that the new protection method is orthogonal to existing solutions which leverage timing information (*e.g.*, chirp bound-

ary misalignment) or frequency information (*e.g.*, frequency disparity). As such, our protection method can be integrated with existing collision recovery solutions and complement each other.

We implement our jammer and protection method and conduct experiments with COTS LoRa nodes as well as software defined radios. Experiment results show that well-synchronized jamming chirps at high transmission power can jam all previous solutions with very high success rates, while our protection method can effectively protect LoRa gateways from all known LoRa jamming attacks including synchronized jamming chirps.

Key contributions of this work can be summarized as follows.

- We investigate the vulnerability of current LoRaWAN physical layer under jamming attacks. We expose the risk of LoRa gateways under the attack of synchronized jamming chirps, which could lead to single point of failure in LoRaWAN.
- We propose a new collision recovery method as a countermeasure against the attack of synchronized jamming chirps by leveraging the difference in signal strength of jamming chirps and LoRa chirps.
- We conduct comprehensive experiments with COTS LoRa nodes as well as software defined radios under various experiment settings. Experiment results demonstrate the effectiveness of our jamming and protection methods.

4.2 System Model and Assumptions

Fig. 4.1 illustrates the jamming model, which consists of a LoRa node (which sends LoRa packets), a LoRa gateway (which receives LoRa packets), and a malicious jammer (which aims to jam LoRa communication).

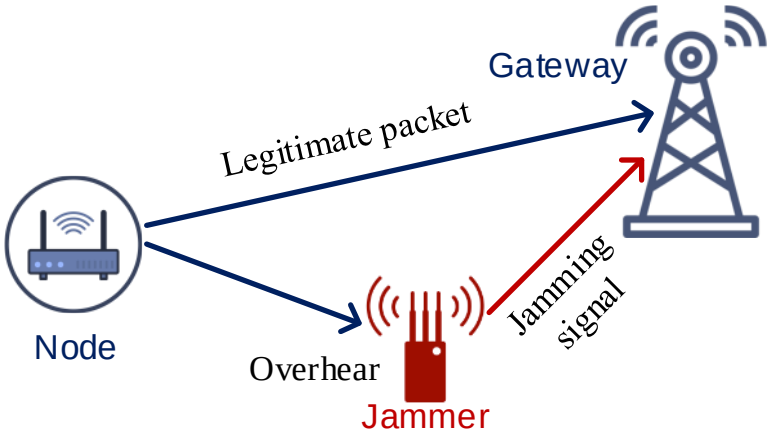
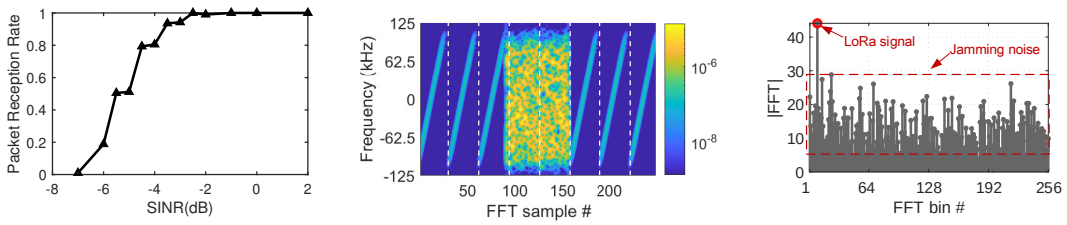


Figure 4.1: Attack model.



(a) (b) (c)

Figure 4.2: Jamming with Gaussian noise. (a) Packet Reception Rate of LoRa node under different SINR. (b) Spectrum of LoRa base chirps under Gaussian noise attack. (c) FFT after dechirp operation of chirp in red box in (b).

We assume that a LoRa gateway is equipped with software defined radios (SDR) to measure physical layer samples for collision recovery. We note that the LoRa gateway can use low-cost receive-only SDR (*e.g.*, RTL-SDR dongle) since it only needs to receive rather than transmit radio signals. For downlink from LoRa gateway to LoRa nodes, the gateway can use COTS LoRa modules for transmission.

We assume that a jammer is equipped with software defined radios (*e.g.*, USRP N210) for sniffing incoming LoRa packets and generating jamming radio signals accordingly. The jamming radio can be random Gaussian noise or LoRa signals. In LoRaWAN, LoRa nodes typically adopt low duty cycle mode (*e.g.*, 1% duty cycle).

As such, if a jammer constantly emits jamming signals at a high transmission power, the jammer can be easily detected and located. Therefore, we consider a jammer that adopts reactive jamming where the jammer stays quiet when the channel is idle, and starts emitting jamming signals when it detects on-going LoRa communication to selectively jam the LoRa communication. The objective of a jammer is to jam the communication between LoRa nodes and a LoRa gateway. We assume that the jammer aims to jam a specific gateway rather than all gateways in a network.

On the other hand, we want to design and implement a countermeasure to protect LoRa communication by enhancing a LoRa gateway against jammer. Ideally, the countermeasure should not require any modification to LoRa nodes to support a large number of already deployed COTS LoRa nodes.

4.3 Empirical Study of LoRa Jamming

LoRa jamming has been attracting wide attention due to the potential risk of single-point failure under jamming attacks. Previous works [9, 36, 69, 57] have demonstrated that it is indeed possible to jam LoRa nodes to some extent by emitting various jamming signals, while other measurement studies [52, 102, 23] show that LoRa nodes are inherently resilient and robust to interference and can even support parallel transmissions by resolving collisions. In the following, we conduct an empirical study to evaluate the impact of a variety of prior jamming attacks to LoRa communication.

4.3.1 Prior Jamming Attacks and Empirical Study

We investigate jamming LoRa with Gaussian noise and chirp signals.

Jamming LoRa with Gaussian Noise

Gaussian noise has been commonly used to jam wireless communication systems. In the following, we test if LoRa communication can be jammed using Gaussian noise and evaluate the impact of Gaussian noise to LoRa communication. To this end, we use a software defined radio as a jammer to emit Gaussian noise in the same frequency band as the LoRa communication. We vary the transmission power of a Gaussian noise jammer and measure the packet reception rate (PRR) under different Signal-to-Interference-plus-Noise Ratios (SINR) at a gateway. In this experiment, we keep the transmission power of a LoRa node transmitter unchanged. Both the LoRa node and the LoRa gateway remain static.

As shown in Fig. 4.2(a), we can observe that the gateway can achieve almost 100% PRR even when SINR is -2 dB and it can still achieve almost 80% PRR when SINR decreases to -4 dB. Intuitively, 0 dB means that the signal strength of a LoRa node is comparable with the interference and noise, while a negative SINR means that the received LoRa signal strength at a gateway is even weaker than the interference and noise.

The reason why LoRa can still receive packets even with negative SINR is that LoRa adopts CSS modulation, which is inherently robust to interference and noise. Fig. 4.2(b) plots the spectrum of LoRa chirps (preamble part) under Gaussian noise attack. In Fig. 4.2(b), we see that LoRa chirps are totally submerged by Gaussian noise. Fortunately, if we operate demodulation(*i.e.*, multiplying with down-chirp and FFT), we can still see a highest spike in the FFT bins corresponding to the correct initial frequency as shown in Fig. 4.2(c). That is because after de-chirp, the power of Gaussian noise will still be distributed to all FFT bins, while a LoRa chirp will concentrate into one FFT bin corresponding to the initial frequency of the chirp.

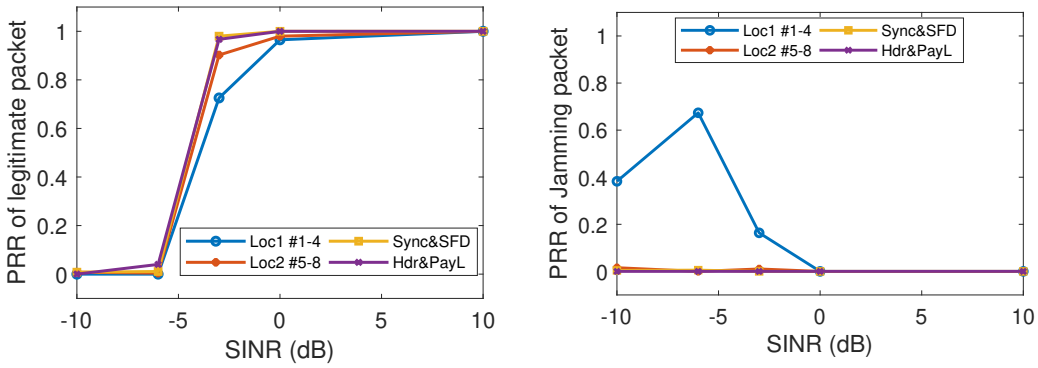
As a matter of fact, a LoRa node can adopt a more conservative parameter set-

ting (*e.g.*, spreading factor, bandwidth) to further enhance its robustness against interference and noise. A jammer can increase transmission power to improve jamming performance. However, this may make it easy to be detected because the high transmission power may exceed the maximum transmission power restricted by regulation. This experiment demonstrates that unlike other wireless technologies, LoRa PHY is inherently robust to Gaussian noise to some extent in practice.

Jamming LoRa with Chirps

Recent work [9, 36] proposes to jam LoRa nodes with LoRa packets and cause collisions to legitimate LoRa communication. [9] exploits maximum transmission power of jammer, while a legitimate LoRa node may transmit at a lower transmission power to reduce power consumption. [36] also mentions that using normal LORa frames to jam a LoRa gateway is better than brute-force jamming. We evaluate the impact of jamming chirps to LoRa chirps in collisions. A jamming LoRa packet is in the same packet structure as a legitimate LoRa packet as illustrated in Fig. 1.2. In this experiment, both legitimate transmitter and jammer are configured to use the same SF and bandwidth. We note that if they adopt different parameter settings, as LoRa gateways support parallel transmissions of LoRa packets with different parameter settings, legitimate packets can be received by gateways [52]. After setting the same parameters (*e.g.*, spreading factor, bandwidth, central frequency), we vary the transmission power of a jammer and evaluate the impact of jamming chirps under different SINR.

As we described in Chapter 4.1, LoRa demodulation process involves several key steps including preamble detection, frame alignment, and chirp demodulation in demodulation windows. As such, we consider the following four scenarios where jamming chirps collide with different parts of LoRa packets: 1) collision with the first four base chirps; 2) collision with the last four base chirps; 3) collision with sync



(a) (b)

Figure 4.3: Jamming packets collide with different parts of LoRa packets under different SINRs: (a) Packet Reception Rate of legitimate packets and (b) Packet Reception Rate of jamming packets.

word and SFD; and 4) collision with PHY header and payload. Fig. 4.3 shows the experiment results, from which we have the following key observations.

First, to jam LoRa signals with a COTS LoRa node, the power of jamming packets need to be orders of magnitude higher than that of a legitimate LoRa packet (*e.g.*, SINR $\leqslant -3\ dB$). If the received LoRa signal strength is comparable with that of jamming signal (*e.g.*, SINR $\geqslant 0\ dB$), legitimate packets can still be received correctly with high PRR (*e.g.*, $\geqslant 96.5\%$).

Second, a LoRa receiver is not likely to receive late coming jamming packets. This is because a LoRa receiver is more likely to detect and lock-on the preamble and SFD of the legitimate packet that arrive earlier than jamming packet. Yet, we do observe capture effect where a jamming packet colliding at the first four base chirps of legitimate packet with stronger signal strength is selected and demodulated (*e.g.*, SINR $\leqslant -3\ dB$).

Third, the impact of collisions at PHY header and payload seems weaker than that of collisions at preamble. Referring to Fig. 4.4, let us see how collisions at PHY header and payload part would influence the demodulation of legitimate chirps in

demodulation windows. Suppose a legitimate chirp (①) collides with a jamming chirp (② and ③) as illustrated in the figure. In demodulation process of PHY header and payload, a LoRa receiver multiplies PHY samples in a demodulation window with a down-chirp, and then performs FFT on the multiplication result. Due to collision in the demodulation window, the FFT operation will generate three spikes. Since jamming chirps are misaligned with legitimate chirps, the power of a jamming chirp will be divided into two adjacent demodulation windows and their corresponding spikes would be lower than that of a legitimate chirp. As such, we see that LoRa nodes can tolerate collisions with jamming chirps at PHY header and payload with comparable or even slightly stronger signal strength. However, if jamming chirps and legitimate chirps are well aligned (*e.g.*, $< 10\%$ misalignment), spikes of jamming chirps within demodulation windows could become higher than those of legitimate chirps. In this case, legitimate packets will be jammed because a LoRa receiver demodulates jamming chirps rather than legitimate chirps.

4.3.2 Anti-jamming Techniques in Other Wireless Networks

Previous countermeasures against jamming attacks in wireless networks have been studied in [58]. In general, frequency and channel hopping is the most commonly used countermeasure. However, as a LoRa packet has a quite long air-time, a jammer can easily track the transmitted LoRa packet during its long transmission time. Similarly, packet fragmentation also fails as LoRa chirps are long enough to be intercepted. Besides, frame masking [99], where a transmitter and a receiver agree on a secret pseudo-random sequence for the SFD in each packet, is proposed to protect packets from being detected by a jammer. However, as introduced in Section 4.2, a receiver needs to use SFD to lock-on a LoRa packet and extract symbol edges. As such, this method cannot be applied to LoRa in practice. Redundant encoding is another commonly used countermeasure to improve the resilience of packets against

jamming attacks. In fact, LoRa has already exploited certain levels of redundancy by configuring a *Code Rate (CR)* parameter. The code rates of LoRa control the ratio of actual data to forward-error-correcting capability that is added to the payload. Another anti-jamming technique is to use a directional antenna. However, this is not suitable for LoRa, since LoRa nodes typically communicate with gateways miles away. If we use directional antennas, any blockage along the direction will lead to packet loss.

4.3.3 Prior Collision Recovery Methods as Countermeasures

We can draw strength from recent advances in LoRa collision recovery and parallel transmissions to protect LoRa communication against jamming attacks. For example, recent works show that some LoRa collisions can be resolved by separating LoRa chirps of different LoRa nodes in time domain [23, 88, 89, 96, 102] and in frequency domain [23].

For example, LoRa collision recovery schemes (*e.g.*, FTrack [102], mLoRa [93]) can resolve collisions of multiple LoRa nodes as long as their chirp boundaries are misaligned in time domain. FTrack [102] detects the continuity of one chirp within a demodulation window to recover collisions. Referring to Fig. 4.4, we see the frequency of a legitimate chirp continuously increases while the frequency of jamming chirps are not continuous within a demodulation window due to chirp boundary misalignment. If jamming chirps and legitimate chirps are well-aligned in time domain, the heights of FFT spikes of jamming chirps and legitimate chirps will be very close to each other. In this case, if jamming chirps are slightly stronger than legitimate chirps, those collision recovery schemes will fail to resolve collisions.

Frequency domain collision recovery schemes (*e.g.*, Choir [23]) separate LoRa collisions by leveraging the frequency differences of colliding nodes due to their hardware imperfection. For example, Choir [23] notices that the fractional part of initial

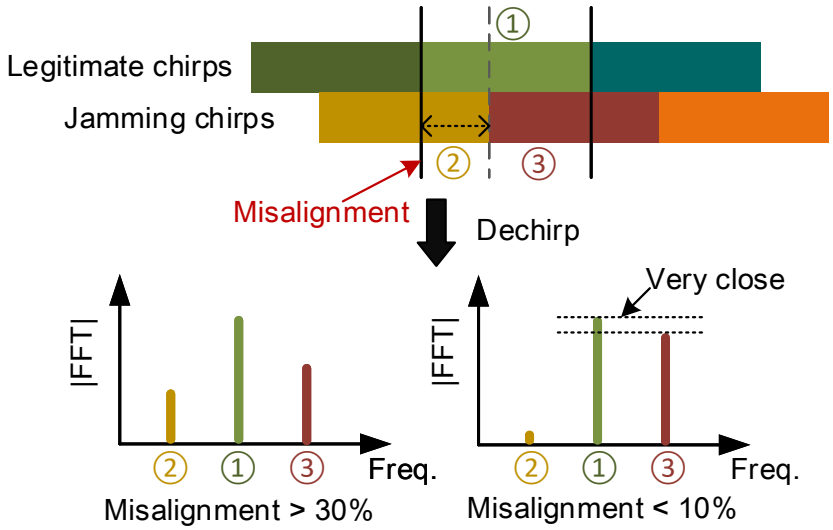


Figure 4.4: Demodulation example: Chirps misaligned with a demodulation window will have part of its power split out.

frequencies of different LoRa nodes are unique, which can be used as physical layer fingerprints. As such, Choir can group different chirps according to fractional parts and thereby separate colliding LoRa chirps. If the frequencies of jamming chirps are synchronized with those of legitimate chirps (*e.g.*, emitting jamming chirps with the same fractional part of initial frequencies), those collision recovery schemes cannot separate legitimate chirps from jamming chirps.

In summary, prior collision recovery methods cannot separate legitimate LoRa chirps from jamming chirps if the jamming chirps are aligned with the legitimate chirps in time domain and frequency domain. In this case, if the power of a jamming chirp is higher than that of a legitimate chirp, a LoRa receiver will demodulate jamming chirps within demodulation windows rather than legitimate chirps.

4.4 Defeating Prior Countermeasures with Synchronized Jamming Chirps

As we described in Section 4.3.3, in order to attack a legitimate LoRa node, an attacker needs to emit jamming chirps that satisfy the following three conditions. Otherwise, prior countermeasures can protect the legitimate LoRa node by separating legitimate chirps from jamming chirps.

4.4.1 Necessary Conditions of Jamming against Prior Countermeasures

C-1: Jamming chirps should be well-aligned with legitimate LoRa chirps in time domain. Prior collision recovery and parallel decoding methods (*e.g.*, FTrack [102], mLoRa [93]) separate LoRa collisions in time domain. As such, if jamming chirps are not aligned with legitimate chirps, the jamming chirps can be separated in time domain.

C-2: Jamming chirps should mimic legitimate LoRa chirps in frequency domain (e.g., central frequency). Frequency domain collision recovery schemes (*e.g.*, Choir [23]) separate LoRa collisions by leveraging the frequency differences of colliding nodes. To jam a LoRa node protected by frequency domain collision recovery schemes, a jammer needs to synchronize jamming chirps in frequency domain with legitimate LoRa node.

C-3: Jamming chirps should have a higher power than legitimate LoRa chirps at a LoRa receiver. If the power of a jamming chirp is weaker than that of a legitimate chirp, a LoRa receiver can correctly detect the initial frequency of the legitimate chirp.

We note *C2* (*i.e.*, frequency condition) and *C3* (*i.e.*, power condition) are relatively easy to satisfy. For example, a jammer can measure the frequency of a legitimate preamble and extract the fractional part of frequency. After that, the

jammer can emit jamming chirps with the same fractional part frequency, which can defeat frequency domain collision recovery scheme (*e.g.*, Choir [23]). To increase the power of jamming chirps at a receiver, a jammer can increase transmission power and get closer to the LoRa receiver.

However, *C1* (*i.e.*, timing condition) can be a bit challenging to satisfy because of signal processing delay caused by software defined radios, different communication distance between a LoRa node and a LoRa receiver, *etc.* As such, jamming chirps may not be well-aligned with legitimate chirps in time domain. In this case, the power of jamming chirps will be divided into two adjacent demodulation windows. Moreover, the aforementioned time domain collision recovery schemes can separate legitimate chirps from misaligned jamming chirps.

4.4.2 Jamming with Synchronized Chirps

We illustrate a basic jamming workflow in Fig. 4.5. A LoRa jammer hears LoRa packets over the air. Upon detecting a valid LoRa preamble, it will attempt to lock on the packet by extracting synchronization information. After that, it can identify and interpret the packet header like a normal receiver. If the packet is transmitted by a targeted node, the jammer will emit synchronized chirps to jam the legitimate packet. Specifically, to launch an effective jamming with well-synchronized chirps, a jammer needs to take all time/frequency offsets (*i.e.*, jamming conditions) into account and carefully compensate them before sending jamming chirps in real time. We present several key steps to generate synchronized chirp jamming in the following.

Accounting for propagation delay

Basically, jamming chirps are required to closely align with the chirps of a legitimate packet when received at a gateway. The communication distance between jammer and gateway and the corresponding propagation delay affects the arrival time of

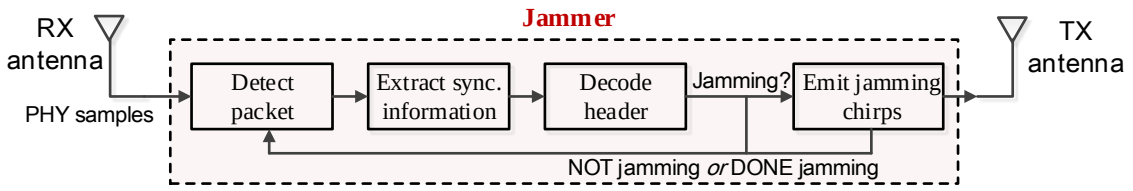


Figure 4.5: The general workflow of LoRa jammer.

jamming chirps at a gateway. We notice that as LoRa typically adopts narrow bandwidths (*i.e.*, $\leqslant 500\ kHz$), the sampling interval of a LoRa receiver is relatively large (*e.g.*, $> 2\ \mu$s). Signals arrived within 2 μs (which corresponds to a communication distance of 600 m) are aligned to the same PHY sample. In practice, a jammer can emit jamming chirps within 600 m away from a gateway to mitigate the influence of propagation delay.

Compensating carrier frequency offset (CFO)

When a jammer hears the preamble of a legitimate packet, it detects chirp boundaries from the preamble and aligns jamming chirps to legitimate chirps. Intuitively, a jammer can detect chirp edges by correlating the received preamble that is composed of successive base chirps with a locally generated base-chirp. However, the detected edges may not correspond to the correct chirp edges due to carrier frequency offset between the legitimate node and the jammer. As a result, the frequency offset translates into corresponding time offset for chirp signals [102, 88]. To be specific, let Δf_{cfo} denote the CFO. A received preamble chirp can be represented as

$$R_{pre}(t) = h \cdot e^{-j\Delta f_{cfo}t} \cdot C(t) \tag{4.1}$$

where $C(t)$ denotes a base up-chirp of preamble transmitted by a legitimate node, and h is the channel between the node and a jammer. If we directly correlate $R_{pre}(t)$ with a local base chirp $C(t)$, the detected chirp edge would be $\Delta t = \frac{2^{SF}}{BW^2}\Delta f_{cfo}$ away

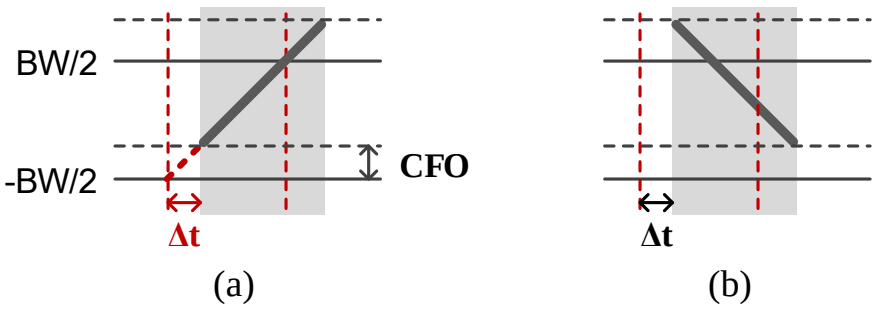


Figure 4.6: CFO affects edge detection: (a)Detected edge vs. real edge of base up-chirp in preamble. (b)Extracted SFD down-chirp with edge offset Δt.

from the real edge, as illustrated in Fig. 4.6 (a). According to our measurements, this edge offset Δt can be as large as ten samples in practice. As such, a jammer must compensate the timing offset caused by CFO and align jamming chirps to correct edges.

Firstly, a jammer needs to estimate CFO from the received signal. We exploit SFD that comes after preamble (see Fig. 1.2) for CFO estimation. In particular, a received SFD chirp can be represented as:

$$R_{sfd}(t) = h \cdot e^{-j\Delta f_{cfo}t} \cdot C^{-1}(t) \tag{4.2}$$

By multiplying Eq. (4.1) with Eq. (4.2), we obtain

$$R_{pre}(t) \cdot R_{sfd}(t) = h^2 \cdot e^{-j2\Delta f_{cfo}t} \tag{4.3}$$

We perform FFT (Fast Fourier Transform) on Eq. (4.3) and the resulting FFT peak indicates the value of Δf_{cfo}. We use Δf_{cfo} to compute the corresponding chirp edge offset $\Delta t = \frac{2^{SF}}{BW^2}\Delta f_{cfo}$, which is finally used to infer the correct chirp edge from detected edges.

As we may detect incorrect chirp boundaries from the received preamble due to CFO, one may wonder how to extract the correct preamble chirp and SFD chirp for CFO estimation. As a matter of fact, we can first perform correlation detection on

the received preamble to coarsely detect the boundary timing of chirps with a time offset, as illustrated by red dashed lines in Fig. 4.6. We use the coarsely detected timing to identify SFD chirps. We note that the extracted preamble base-chirp and SFD down-chirp have the same offset (*i.e.*, Δt) with their real edge timing, as illustrated in Fig. 4.6. As a result, the extracted chirps in Eq. (4.3) for CFO estimation are actually $R_{pre}(t - \Delta t)$ and $R_{sfd}(t - \Delta t)$, rather than the ideal $R_{pre}(t)$ and $R_{sfd}(t)$. As the edge time offset (Δt) translate into frequency offset Δf_{edge} for the up-chirp and an opposite frequency $-\Delta f_{edge}$ for the down-chirp, we have $R_{pre}(t - \Delta t) \cdot R_{sfd}(t - \Delta t) = R_{pre}(t) \cdot R_{sfd}(t)$. In summary, the above CFO estimation method (*i.e.*, Eq .(4.3)) still holds with the time offset in preamble and SFD detection.

Compensating hardware and software delay

A jammer also needs to process received signal and react in real time. It imposes a strict constraint on processing latency (termed *jamming delay*). We use a software defined radio (*i.e.*, USRP N210) as hardware and use an open-source GNU Radio (GR) as software to perform jamming on-line. In particular, we list the main contributors of jamming delay as follows.

- Data transfer: The delay of data transfers between different components, *e.g.*, from USRP Rx buffer to data processing blocks as well as from blocks to USRP Tx when emitting jamming chirps.
- Scheduling: The latency of OS (*i.e.*, operating system) and GR scheduling.
- Signal processing: The latency of signal processing including preamble detection, packet decoding, synchronization of jamming chirps, *etc.*

We note that as signal processing is generally performed on PCs with powerful CPUs, the processing latency is relatively short (*e.g.*, tens of μs on our Intel i5 PC).

In comparison, the air time of LoRa packet is of $2 \sim 3$ orders of magnitude longer. For instance, the transmission time of a typical LoRa chirp with $SF = 8, BW = 250$ kHz is about 1 ms (*i.e.*, 100× longer than signal processing). Theoretically, this would leave a sufficient amount of time for a jammer to finish signal processing and generate jamming chirps in real time.

On the other hand, we empirically observed that GR scheduling and data transfers exhibit time uncertainty in practice. The latency varies randomly from 100 μs to $10,000$ μs in our measurements. We configure the GR scheduler with a Single-Thread-Scheduler mode (*i.e.*, STS) to reduce the processing latency and time variation. We also configure the buffer size of inter-block data transfer to fit the size of LoRa chirps. As a result, the end-to-end jamming latency becomes rather stable (*e.g.*, 500 μs in our setting), which can be measured and compensated before sending jamming chirps.

In order to align a jamming chirp with a legitimate chirp, a jammer needs to infer which sample is currently transmitting in the air (*i.e.*, the front wave of a legitimate packet). To this end, the jammer continuously receives samples of a legitimate packet using USRP, which buffers the received samples and reports them when the buffer is full. In practice, the number of reported samples in every buffer and the corresponding timestamp can vary due to the uncertainly in GR scheduling. To address this problem, the jammer can estimate the current transmitting sample in the air with the latest received buffer size and its timestamp. By further counting in the processing latency, the jammer can determine the time compensation for precise alignment of jamming chirps with legitimate chirps.

4.4.3 Jamming with Identical Consecutive Chirps

The synchronized jamming approach satisfies all conditions listed in Section 4.4.1. A jammer can properly choose jamming chirps to mimic the payload of a legitimate

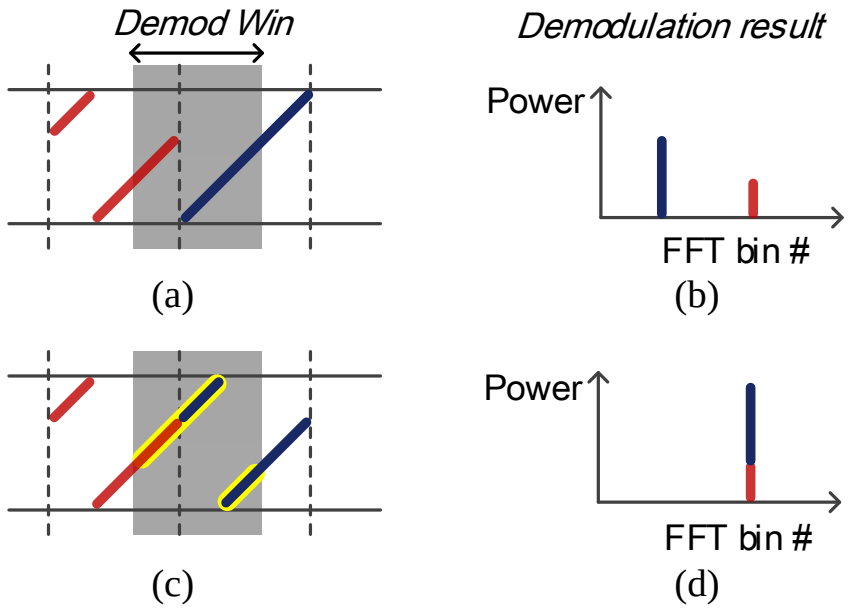


Figure 4.7: Jamming without synchronization: (a-b) Non-identical jamming chirps and demodulation result vs. (c-d) Identical jamming chirps and the demodulation result. When consecutive jamming chirps are identical, the samples from adjacent chirps form a complete chirp in the demodulation window which well-aligns with legitimate chirp.

packet, and employ synchronized jamming to defeat the existing collision recovery strategies. However, the synchronized jamming approach requires careful calibration and strict timing requirement to align jamming chirps with legitimate chirps. In the following, we demonstrate that it is possible to jam in a lightweight manner without strict synchronization (*e.g.*, delay compensation).

If we perform jamming without synchronization, jamming chirps are likely to misalign with chirps of a legitimate packet. Suppose a gateway uses a time domain collision recovery scheme to protect legitimate packets from jamming attacks. Let us consider a demodulation window that is aligned with a legitimate chirp but not jamming chirps. As illustrated in Fig. 4.7(a), since the demodulation window spans across two adjacent jamming chirps, jamming signals within this demodulation window would experience a sudden change in frequency at chirp boundary. As a result,

after demodulation, there will be two FFT spikes at different FFT bins (Fig. 4.7(b)).

However, if the two adjacent jamming chirps are the same, their frequency would experience no sudden change at the jamming chirp boundary (see Figure 4.7(c)). As a result, both the jamming chirp and the legitimate chirp exhibit frequency continuity within the demodulation window, meaning that the power of consecutive jamming chirps will concentrate in the demodulation window, as if one jamming chirp is well-aligned with the window, as illustrated in Fig. 4.7(c) and (d). As such, a jammer can emit the same consecutive chirps to defeat existing countermeasures without synchronizing to legitimate chirps.

However, COTS LoRa radio interleaves the payload data to avoid successive identical symbols in PHY layer. Although we can observe two consecutive chirps with the same initial frequency in practice, we seldom observe more than three identical symbols appearing successively in the payload of packets transmitted by COTS LoRa nodes. As such, a jammer can emit two consecutive chirps with the same initial frequency as jamming chirps.

We note that the consecutive chirp pattern still differs from the random chirp pattern of a legitimate packet payload. Existing time domain collision recovery schemes can be adapted to discern a consecutive jamming attack by detecting chirps' consecutive patterns. As a result, the consecutive jamming approach may not be as effective as the synchronized jamming approach against existing countermeasures.

4.4.4 Jamming with Consecutive Down-chirps

Another lightweight jamming method without strict synchronization is to jam with consecutive down-chirps. As introduced in Section 4.2, a LoRa receiver needs to first detect 4 consecutive preamble chirps to pre-lock a packet and continuously listen to an SFD (*i.e.*, 2.25 down-chirps) to further lock on the packet. A LoRa receiver relies on the SFD down-chirps to determine the frame timing of a packet. A jammer can

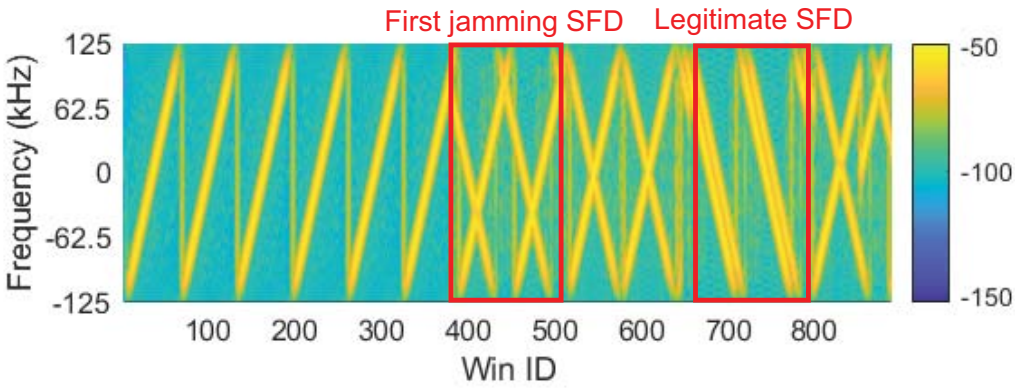
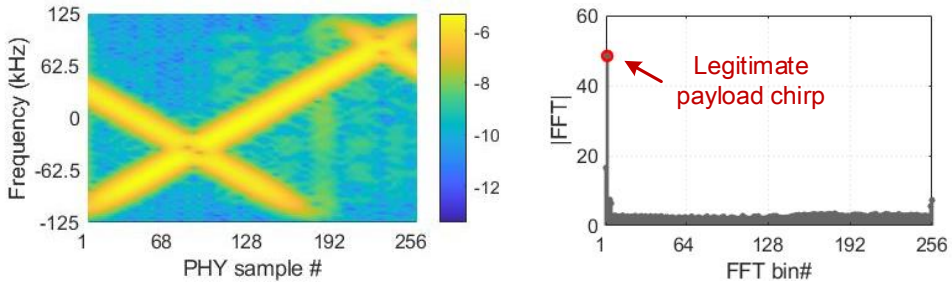


Figure 4.8: Jamming with consecutive down-chirps at preamble part. If a LoRa receiver falsely locks on jamming down-chirps or fails to lock on any SFD, it cannot correctly demodulate a legitimate packet.

mimic an SFD by sending consecutive down-chirps to block or interfere the lock-on process of a legitimate packet. If jamming down-chirps arrive in prior of the SFD of a legitimate packet, a normal receiver may lock on the false SFD or fail to lock on any SFD. As a result, a receiver cannot correctly detect the frame timing of a legitimate packet, leading to PHY-layer errors for the demodulation of legitimate packet.

We carry out an experiment to verify the effectiveness of the jamming method. In this experiment, a jammer transmits consecutive down-chirps immediately after detecting a LoRa packet (*e.g.*, 4 consecutive preamble chirps). Generally, a LoRa receiver pre-locks a packet upon detecting 4 consecutive preamble chirps. It completes locking on the packet by detecting an SFD (*i.e.*, 2.25 down-chirps). Fig. 4.8 displays the spectrum of a legitimate LoRa packet jammed by consecutive down-chirps. As we can see, the jamming down-chirps arrive earlier than the legitimate SFD. A receiver would mistakenly detect jamming down-chirps as the SFD of a legitimate packet. As a result, the frame timing of a legitimate packet is detected incorrectly, which can lead to failures of packet demodulation.

However, this jamming method has specific requirements and limitations. First, jamming down-chirps need to arrive before a legitimate SFD. This requires the



(a) (b)

Figure 4.9: Jamming with down-chirps does not influence the payload demodulation. (a) Spectrum of one payload chirp jammed by a down-chirp. (b) FFT magnitude after dechirping. The legitimate chirp still achieves the highest FFT magnitude.

preamble length of a legitimate packet to be long enough for a jammer to catch up. In our experiment, we set the preamble length of a legitimate packet to be 12. We empirically observe that a packet is difficult to be jammed by consecutive down-chirps if the length of preamble is less than 12. Second, jamming with consecutive down-chirps can only work at the preamble part of a packet. The jamming down-chirps do not interfere with the up-chirps in the payload of a legitimate packet. A receiver can successfully demodulate a payload up-chirp in presence of jamming down-chirps, due to orthogonality of the two types of signals. For example, Fig. 4.9 shows the spectrum and FFT results of a payload chirp jammed by a down-chirp. After being dechirped, the legitimate up-chirp still yields the highest FFT magnitude. Besides, similar to identical consecutive chirps, this jamming attack can be easily detected using down-chirp correlation and detection.

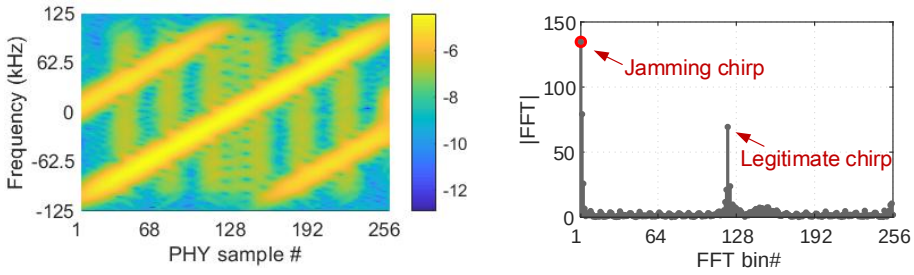
4.5 Countermeasure

In the previous section, we reveal that current LoRaWAN suffers the risk of synchronized jamming attack. In this section, we present a new countermeasure to protect LoRaWAN against synchronized jamming attack.

Recall jamming conditions in Section 4.4.1 (*i.e.*, *C-3*), in order to successfully jam a LoRa packet, it requires the power of a jamming chirp to be higher than that of a legitimate chirp in a demodulation window, as illustrated in Fig. 4.10(a). Essentially, we can expect a discrepancy of FFT magnitude between a jamming chirp and a legitimate chirp after demodulation, as shown in Fig. 4.10(b). This motivates us to differentiate a legitimate chirp from a jamming chirp by checking their received signal strength in *power domain*, which complements the conventional collision recovery schemes examining time and frequency domain.

The received signal strength (*i.e.*, RSS) of a LoRa packet can be affected by many factors (*e.g.*, transmit power, communication distance, receiver gain, *etc.*), but most of those factors are generally invariant during the transmission of one packet. For instance, the transmit power of a LoRa node can be adapted for each packet transmission, but will remain the same during one packet transmission. Besides, in our targeted scenarios, LoRa nodes generally remain stationary or move at a low speed. More importantly, since LoRa PHY (*i.e.*, CSS) does not modulate the amplitude of LoRa chirps, the power level of LoRa chirps from the same packet would remain pretty stable and share high similarity. In addition, as a selective jammer starts jamming after interpreting the header of a legitimate packet, it leaves the packet preamble intact. As such, a receiver (*i.e.*, gateway) can measure the RSS from the preamble of a legitimate packet and use the measured RSS to help extract legitimate chirps from jamming chirps.

Finally, we present an RSS-based LoRa decoder as a countermeasure to the synchronized jamming attack. The countermeasure decoding process generally works as follows. A receiver first detects the preamble of a LoRa packet. In addition to extracting symbol timing (*i.e.*, chirp edges) from preamble as in a standard LoRa decoder, we also measure the RSS of preamble chirps. We then employ the same method of a standard decoder to locate and demodulate symbol chirps in the pay-

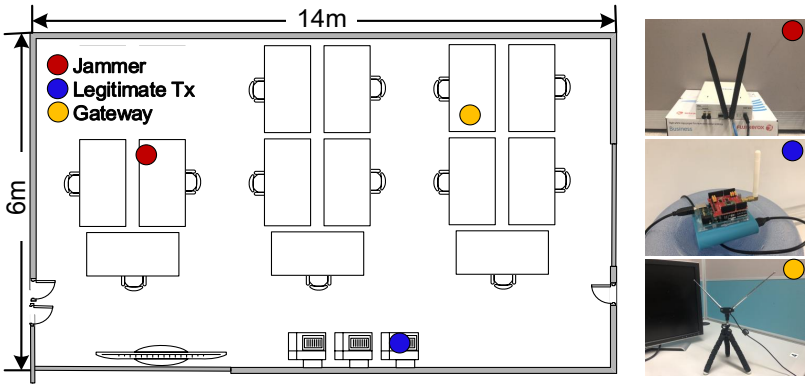


(a) (b)

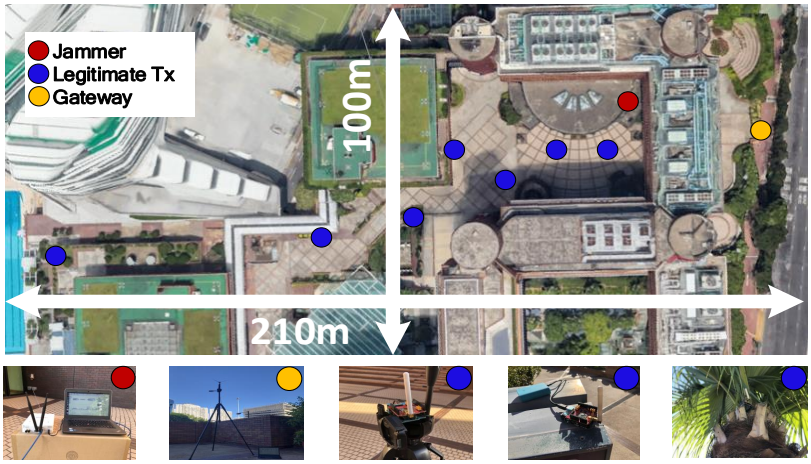
Figure 4.10: Jamming power is higher than legitimate power: (a)Received signal strength of a jamming chirp vs. a legitimate chirp. (b)FFT magnitude of a demodulated jamming chirp vs. legitimate chirp.

load. In each demodulation window, we can obtain the interleaved FFT results of demodulated legitimate and jamming chirps, as shown in Figure 4.10(b). Different from a standard decoder that selects the highest FFT peak as demodulation result, we pick the FFT peak with a magnitude that can best match the RSS measured from preamble as the demodulation result of legitimate chirp. We iteratively apply this method to demodulate all legitimate chirps and feed demodulated symbols into a standard decoder to produce the payload data of legitimate packets.

We note that if the RSS of jamming chirps and the RSS of legitimate chirps are very close, our RSS-based protection method alone cannot separate the legitimate chirps from the jamming chirps. In practice, it can be very challenging for a jammer to tune the transmission power of jamming chirps so that the RSS of jamming chirps received by a LoRa gateway can be of the similar RSS of legitimate chirps. Note that there is no feedback to the jammer from either the legitimate LoRa node or the LoRa gateway. Besides, in case of transmission failure because of jamming attack, a LoRa node would retransmit at different transmission power. Since our RSS-based protection method is orthogonal to the existing collision recovery methods which leverage time and frequency domain information, those existing methods can be used in parallel to enhance protection method.



(a) Indoor experiment map.



(b) Outdoor experiment map.

Figure 4.11: Experiment layout.

4.6 Implementation and Evaluation

4.6.1 Implementation and Setup

We implement synchronized jamming attack and corresponding countermeasure in real-world. We conduct experiments and evaluation in both indoor and outdoor environment. Specifically, as shown in Fig. 4.11, the indoor test bed spans 14×6 m^2 and it is a typical office room with rich multipaths. The outdoor test bed spans 210×100 m^2 and it is an urban outdoor environment with many skyscrapers. We use a COTS LoRa node (*i.e.*, LoRa shield, which consist of HopeRF's RFM96W transceiver module embedded with the Semtech SX1276 chip) as the legitimate transmitter and

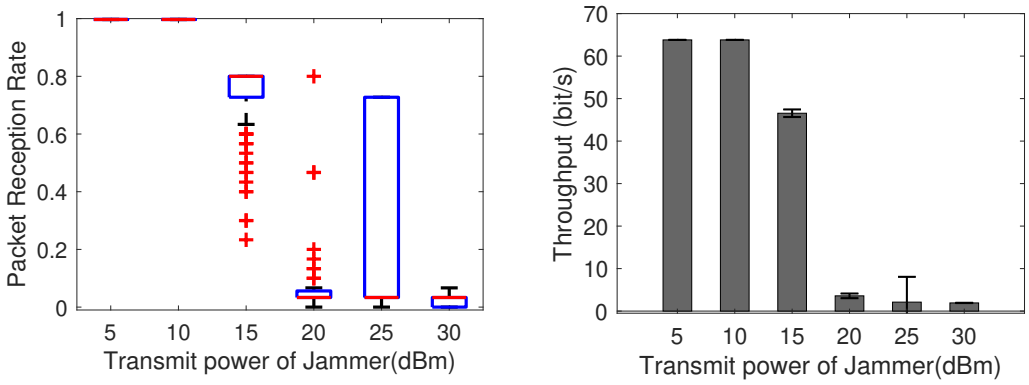
put it at different places (blue dots in Fig. 4.11(a) and Fig. 4.11(b)). A low-cost receive-only RTL-SDR dongle (*i.e.*, yellow dot) is used as the LoRa gateway to record the PHY samples. We implement the jamming process on a USRP N210 to work as a jammer (*i.e.*, red dot). And we integrate the calibration and compensation algorithms in the jammer with C++. For performance evaluation, we develop a standard LoRa demodulator and our own countermeasure in MATLAB to process PHY samples received by RTL-SDR dongle. All devices work at 915 MHz band. If not specified, we configure the spreading factor, code rate, and bandwidth of the LoRa chirp signal to 8, 4, and 250 KHz, respectively.

To evaluate the impact of jamming attack and the effectiveness of our countermeasure, we implement the following two schemes: **1) Victim**: Legitimate LoRa communication (uses standard LoRa demodulation) under jamming attack, which is used to evaluate the impact of jamming attack; and **2) Protege:** The victim protected by our countermeasure against jamming, which is used to demonstrate the effectiveness of our countermeasure.

We use the following metrics to evaluate the performance. **1) PRR:** Packet Reception Rate (PRR) is the ratio of correctly received packets over transmitted legitimate packets. **2) SER:** Symbol Error Rate (SER) is the ratio of incorrectly demodulated symbols over the total number of transmitted payload symbols; and **3) Throughput:** It quantifies the successfully received bits per unit time. We also compare our countermeasure with FTrack [102] and Choir [23] against jamming attack.

4.6.2 Basic Performance

We first evaluate the basic performance of our jamming method and countermeasure.



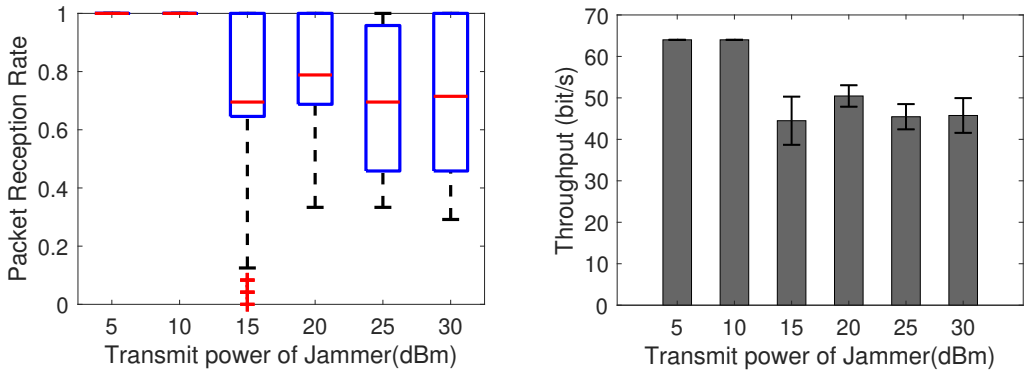
(a) (b)

Figure 4.12: Jamming with different transmission power. Victim's (a) PPR and (b) Throughput.

Impact of Jamming Attack

In this experiment, a legitimate transmitter sends LoRa packets every 2 seconds. The payload length of each packet is set to 30 with the lowest transmission power of (5 dBm) in indoor environment. We keep the three players (*i.e.*, in Fig. 4.11(a)) static and vary the transmission power of jammer from 5 dBm to 30 dBm. In each scenario, we conduct over 120 measurements.

Fig. 4.12 shows victim's PPR and throughput under jamming with different transmission power. We observe that when jamming power is relatively small (5 $\sim$ 10 dBm), the PRR of Victim is almost 100%, meaning that this jamming attack has no impact on LoRa communication due to its low jamming power. With further increase of jamming power (15 dBm), victim's PRR begins to decrease rapidly. When jamming power is above 20 dBm, the PRR decreases and almost all packets will be jammed by the attacker. Accordingly, the throughput of victim drops drastically when jamming power is 20 $\sim$ 30 dBm. This result reveals that LoRa communication is vulnerable to synchronized jamming attack with a relatively high transmission power and the performance of LoRa communication can be substantially affected.



(a) (b)

Figure 4.13: Countermeasure performance with different transmission power. Protege's (a) PRR and (b) Throughput.

Performance of Countermeasure

In this experiment, we evaluate the performance of countermeasure. We use the same settings as in subsection 4.6.2. Fig. 4.13 presents the results. The average PRR of protege is higher than 70% across all transmission power of jammer. In comparison with Fig. 4.12, the overall PRR and throughput of protege are much higher than those of victim, especially when jamming power is higher than 15 dBm. The throughput of protege is 20× higher than that of victim when jamming power is 25 dBm, and 23× when jamming power is 30 dBm. This is because when transmission power is higher than 15 dBm, the SINR at receiver is low ($-10 \sim -5$ dB). In this case, the power of legitimate chirps is weaker than that of jamming chirps, leading to incorrect demodulation results of victim. In contrast, our countermeasure can leverage the difference of received signal strength and separate legitimate chirps from jamming chirps. The experiment results indicate that our countermeasure can protect the LoRa gateway against such synchronized jamming attacks.

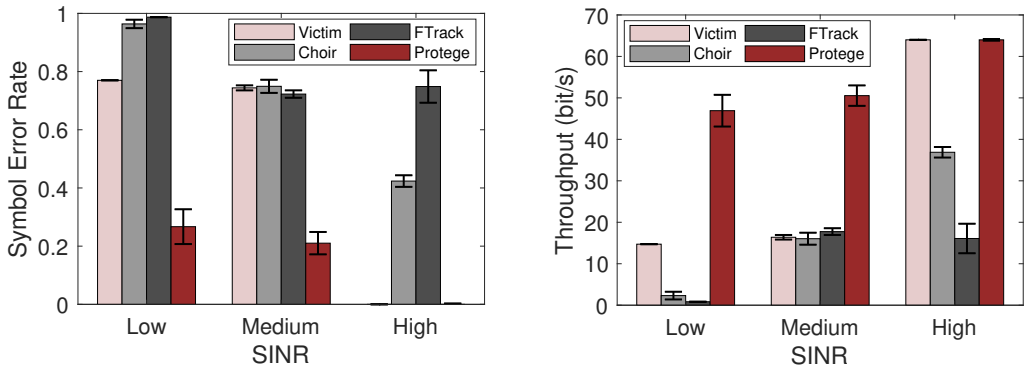
Comparison with Existing Countermeasures

In the following, we compare victim and protege with two typical collision recovery and parallel decoding methods, *i.e.*, FTrack and Choir. We compare these four methods in low ($-10 \sim -5\ dB$), medium ($-5 \sim\ 5\ dB$), and high ($5 \sim 10\ dB$) SINR scenarios. Each scenario includes over 120 measurements.

We plot the SER and throughput in Fig. 4.14. We observe that victim, Choir and protege have lower SERs as SINR becomes higher. However, FTrack has over 72% SER in all scenarios. This is because FTrack distinguishes colliding chirps by using frequency tracks caused by time misalignment of two chirps. However, jammer in this paper synchronizes jamming chirps with legitimate chirps, making it hard for collision recovery method which uses timing information to separate. Since Choir disentangles colliding chirps by leveraging the disparity in frequency domain, higher signal strength benefits its performance. We can also see that protege has best performance in terms of SER and throughput in all SINR scenarios. Specifically, in low SINR scenario, our countermeasure (*i.e.*, protege) only has 26% SER while FTrack and Choir have SER of 96.38% and 98.7% respectively, even higher than that of victim (77%) using standard LoRa demodulation. In high SINR scenario, Choir and FTrack still have very high SER and low throughput, while protege and victim have almost 0 SER and 100% throughput. This experiment demonstrates that our RSS-assisted countermeasure outperforms all existing countermeasures.

4.6.3 Impact of LoRa Configuration

The symbol error rate and throughput of LoRa nodes are sensitive to LoRa configuration parameters, including spreading factors, bandwidths, and code rates. In this subsection, we examine the impact of LoRa packet configuration on the performance of jamming attack and our countermeasure strategy. We adopt the same experiment

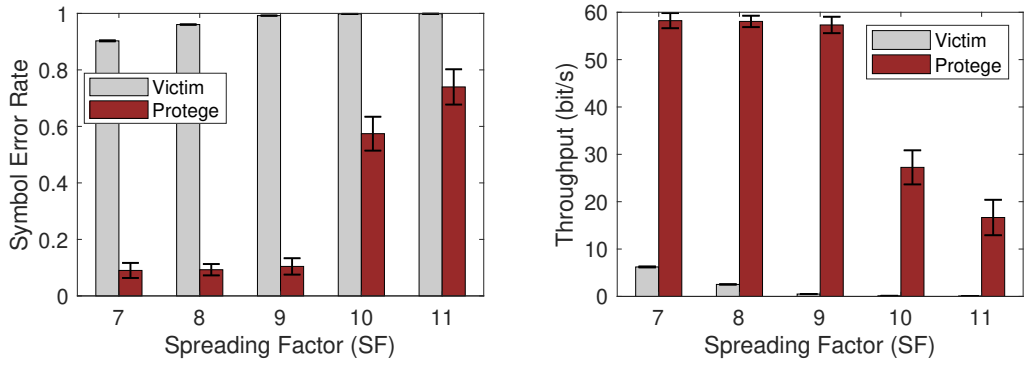


(a) (b)

Figure 4.14: Performance comparison of Victim, Choir, FTrack, and Protege under different SINRs: (a) Symbol Error Rate (SER) and (b) Throughput.

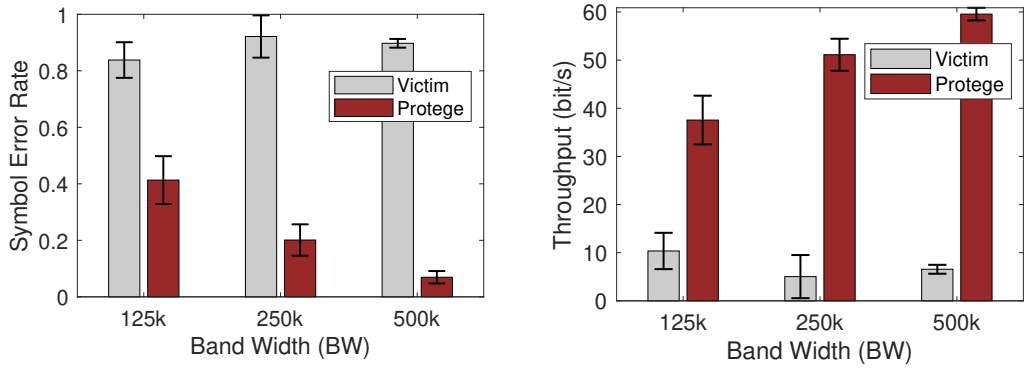
settings as in Section 4.6.2. Due to page limit, we only present the results of high jamming power ($\geqslant 20\ dBm$).

1) Impact of spreading factor (SF). In this experiment, we fix the bandwidth to 250 kHz and vary SF from 7 to 11. We compare PHY layer symbol error rates of standard demodulation method (*i.e.*, victim) and our countermeasure strategy (*i.e.*, protege) in Figure 4.15. As expected, the SER of victim stays at high level (*e.g.*, $> 90\%$) for all SFs due to the high jamming power. In contrast, the protege can decode legitimate packets with SER lower than 10% when $SF = 7 \sim 9$. We observe that the SER of protege increases dramatically to higher than 60% as SF increases to 10 and 11. This is because the frequency gap between LoRa symbols becomes narrower as SF increases, making it harder to demodulate symbols correctly. Figure 4.15(b) compares the throughput of victim and protege. The throughput of victim is very low and approaches to zero as SF increases to 10. In contrast, the average throughput of protege reaches more than 57 bit/s (90.0% of the ideal throughput) when SF is less than 10. However, when SF is greater than 9, the throughput of protege decreases to less than 30 bit/s. It demonstrates that packets with a larger SF are generally more vulnerable to jamming attacks. And protege achieves better



(a) (b)

Figure 4.15: Impact of SF on (a) Symbol Error Rate (SER) and (b) Throughput of Victim and Protege.



(a) (b)

Figure 4.16: Impact of BW on (a) Symbol Error Rate (SER) and (b) Throughput of Victim and Protege.

performance when SF is small.

2) Impact of bandwidth (BW). To explore the impact of bandwidth, we set $SF = 8$ and change BW from 125 kHz to 500 kHz in this experiment. In Figure 4.16(a), we observe that the average SER of standard LoRa decoder is higher than 81% across all bandwidth settings. However, compared with the high SERs of standard demodulation method (*i.e.*, victim), our countermeasure strategy can correctly demodulate legitimate chirps with $SER < 20\%$ when $BW \geqslant 250\ kHz$. As

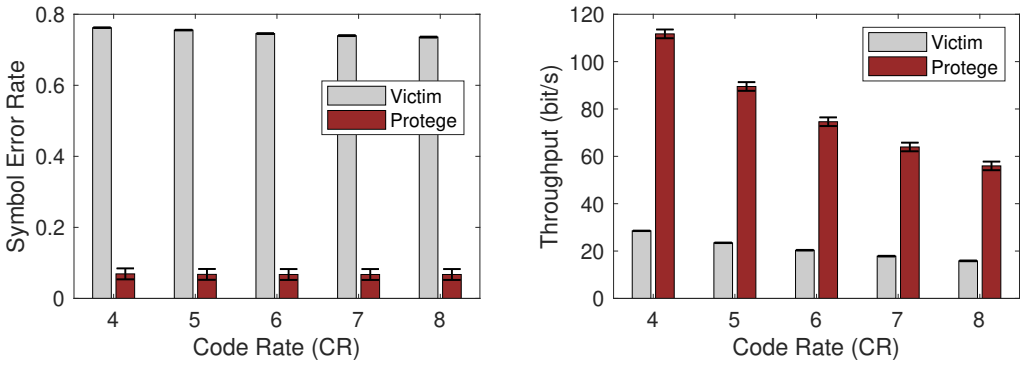
bandwidth increases, the SER of countermeasure decreases. This is because wider bandwidth can create larger frequency gap between LoRa symbols. As such, a wider bandwidth will generally make the demodulation more robust to jamming attack. Figure 4.16(b) illustrates the throughput of victim and protege across different BW configurations. As expected, victim yields low throughput (*i.e.*, less than 15 bit/s) with all bandwidth settings. Protege performs better as bandwidth increases. Specifically, protege obtains 59.6 bit/s when bandwidth is 500 kHz.

3) Impact of code rate (CR). To evaluate the impact of CR, we vary CR from 4 to 8, and fix SF to 8 and bandwidth to 250 kHz, respectively. In this experiment, we send packets once per second. Figure 4.17 shows the evaluation results. We can observe that the average SER of the standard LoRa decoder is high (*i.e.*, $> 73.6\%$) while the SER of our countermeasure is less than 6.9%. The SER of victim and protege remains stable across different code rates. However, as shown in Figure 4.17 (b) the throughput of both victim and protege decrease as the code rate increases. In specific, victim and protege achieve the highest throughput of 28.5 bit/s and 111.7 bit/s respectively when CR=4. This is reasonable because code rate represents the redundancy bits in encoding every 4-bit data. A larger CR indicates more redundancy bits in payload. Since the SER remains stable across different code rates, the overall valuable bits (*i.e.*, goodput) delivered decreases as code rate increases.

LoRa exploits redundancy to endure short interference. However, increasing CR fails to protect LoRa signals against synchronized jamming. Besides, a larger CR also increases the transmission time and thus decreases the goodput.

4.6.4 Impact of Jamming Distance

We perform testbed experiments in an outdoor environment as shown in Fig. 4.11(b). Unless otherwise specified, we adopt a default LoRa packet configuration of $SF = 8$, $BW = 250\,kHz$. In the first experiment, we place a jammer at a fixed distance ($15\,m$)



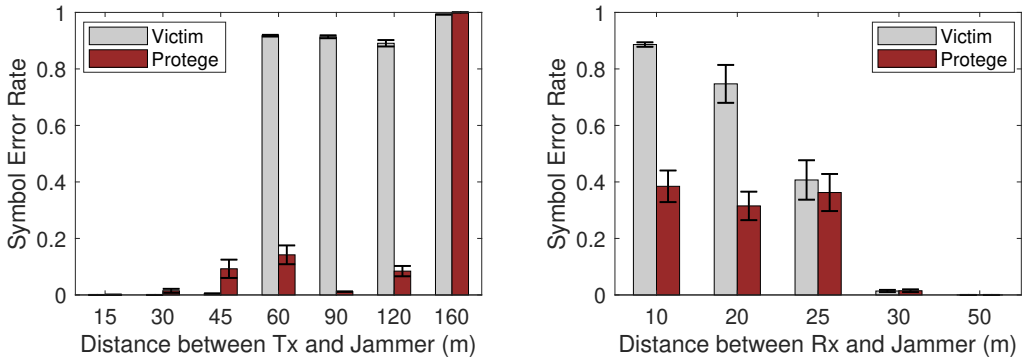
(a) (b)

Figure 4.17: Impact of CR on (a) Symbol Error Rate (SER) and (b)Throughput of Victim and Protege.

to a gateway and keep them static. We place a legitimate LoRa node at different locations to evaluate the effective jamming range. The transmission power of jammer is fixed to 20 dBm. We configure the legitimate node with the maximum transmission power (*i.e.*, 23 dBm) and change node locations with distances of 15 $\sim$ 160 m to the gateway.

We present the SER results of standard demodulation method (*i.e.*, victim) and our countermeasure strategy (*i.e.*, protege) in Figure 4.18(a). We observe that both victim and protege can correctly demodulate legitimate packets when the transmitter is within 45 m from the gateway because of the high SINR of packets (*i.e.*, higher signal power than jamming power). When the distance is 60 $\sim$ 120 m, the SER of victim increases dramatically($\geqslant$ 80%), because the signal power of legitimate packets falls below the jammer power. Protected by our countermeasure, protege can still demodulate packets correctly when the distance is 60 $\sim$ 120 m. When distance further increases to 160 m, the received signal strength of legitimate packets becomes too weak to be demodulated, leading to almost 100% SERs for both strategies.

In the second experiment, we keep a gateway and a legitimate node at fixed locations and move a jammer at different locations to evaluate the jamming perfor-



(a) (b)

Figure 4.18: Impact of (a) Distance between Tx and Jammer and (b) Distance between Rx and Jammer on SER of Victim and Protege.

mance. The legitimate node transmits with the maximum power (*i.e.*, 23 dBm). The distance between the legitimate node and the gateway is 20 m. We configure the jammer with the TX power gain of 80 dB. In Fig. 4.18(b), we find that the SER of standard demodulation method (*i.e.*, victim) decreases as jamming distance increases. Because the signal strength of jamming chirps becomes weaker as the distance increases. The SERs of protege are higher than 30% when jamming distance $\leqslant 25$ m because of the comparable signal power between jamming chirps and legitimate chirps. When the distance $\geqslant 30$ m, both victim and protege can correctly demodulate the symbols since the power of jamming chirps becomes too weak in this range.

In summary, when a jammer is very close to a gateway receiver, the receiver's performance will be dramatically affected by the jammer. With our countermeasure, protege can still demodulate some of the symbols correctly. Note that the LoRa PHY adopts error correction code to correct symbol errors in practice.

4.7 Conclusion

In this work, we reveal the vulnerability of LoRa PHY under the attack of synchronized jamming chirps. The insight of the jamming attack is that a well-synchronized jamming chirp cannot be separated from a legitimate LoRa chirp in the time domain. As a result, most existing protection methods cannot protect the LoRa PHY against such synchronized jamming chirps. To enhance the LoRa PHY, we propose a novel countermeasure, which leverages the difference between the received signal strength of legitimate chirps and jamming chirps in the power domain. The protection method can complement and enhance existing collision recovery schemes which leverage the chirp misalignment in time domain or the frequency disparity in frequency domain.

Chapter 5

Future work and Preliminary Results

5.1 LoRa Authentication

In the previous two chapters, we study covert channel and jamming attacks in LoRa networks. These two attacks are active attacks. Another common active attack is spoofing attack, where an attacker can impersonate a legitimate node to deliver deceptive packets to the gateway. These active attacks can greatly impede the development of LoRa networks. Then a natural question comes: can we enhance the security of LoRaWAN?

Adopting sophisticated cryptography mechanisms is commonly used to enhance security. However, it is not suitable for LoRa networks. This is because the design goals of LoRa nodes are low-power and low-cost. Implementing complex cryptography algorithms is too resource-consuming for existing LoRa nodes. Thus a lightweight security mechanism is needed.

In future work, we aim to improve the security performance of LoRa networks by node authentication. We try to extract unique physical-layer features of legitimate nodes as fingerprints to authenticate a LoRa node. To find unique features, we first turn to LoRa node hardware infrastructure. Fig. 5.1 shows the transmit chain of a

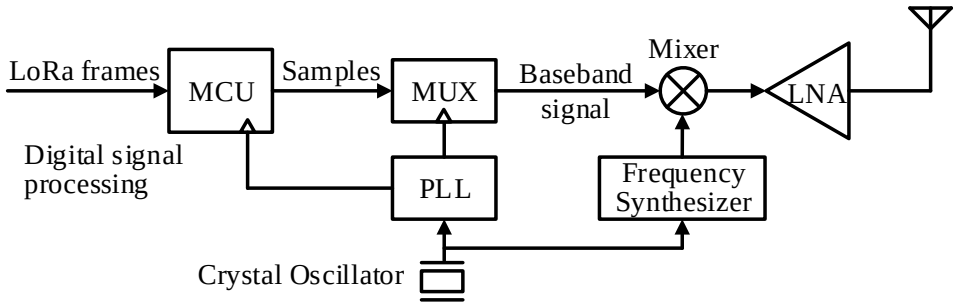
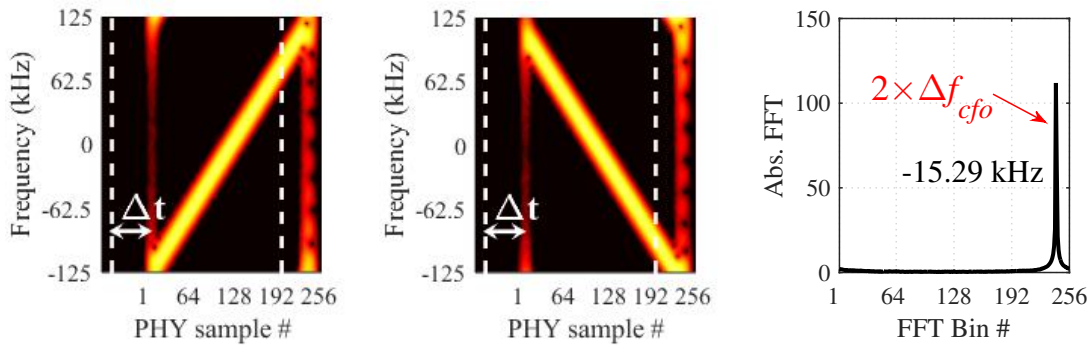


Figure 5.1: Simplified transmit chain of LoRa node.

LoRa radio [76]. The MCU first generates data samples according to the input LoRa frame data. The data samples are then passed to a multiplexer (MUX) to generate a baseband signal. Next, a mixer up-converts the baseband signal to the frontend. The transmit chain is typically driven by a 32 MHz crystal oscillator. Due to hardware imperfection, the oscillator frequency of a legitimate LoRa node can be different from that of a receiver, resulting in carrier frequency offset. CFO can lead to frequency deviation and phase rotations of received symbols, which provides us an opportunity to differentiate a legitimate node from a malicious node. Besides CFO, we find that signals transmitted by commodity LoRa radio suffer from frequency leakages, the distribution of which can also be used to help with authenticating legitimate LoRa nodes.

Besides, signatures relating to physical-layer radio propagation (*i.e.*, air-channel) can also be used to authenticate a LoRa node. The communication channel from a transmitter to a receiver involves not only RF chains of Tx and Rx radios but also wireless channel over the air (*i.e.*, *air-channel*). Suppose an attacker wants to launch a spoofing attack, it needs to mimic the legitimate link between a legitimate node and gateway. It can mimic the hardware imperfection of radios by compensating CFOs, however, it cannot extract features of air-channels between legitimate node and gateway. Air-channels are highly related the position of the node, which is im-



(a) Preamble chirp (b) SFD chirp (c) CFO estimation

Figure 5.2: Estimating CFO with a preamble up-chirp and an SFD down-chirp which are extracted with edge timing offset Δt. The white dashed lines indicate the real chirp edges.

possible to mimic unless it is at the same location as the legitimate node. Therefore, the signal propagation signature can also be employed to distinguish a legitimate node from a spoofing node.

5.1.1 Fine-grained CFO Extraction

The mismatched oscillator frequencies between transmitter and receiver result in CFO. We represent a received symbol with CFO as below.

$$y(t) = h^{air} \cdot e^{-j(2\pi\Delta f_{cfo}t+\varphi_{osc})} \cdot S(t, f_{sym}) + n(t), \tag{5.1}$$

where Δf_{cfo} and φ_{osc} are the oscillator frequency offset and phase offset between transmitter and receiver.

In the spoofing attack scenario, both legitimate LoRa nodes and spoofing LoRa nodes transmit packets to the same gateway. Thus, we can extract the oscillator frequency differences between legitimate transmitter and spoofing transmitter by comparing two CFOs.

We demonstrate that CFO can be reliably estimated with a preamble up-chirp and SFD down-chirp. The chirps in preamble and SFD share the same CFO and STO. We extract a preamble chirp and an SFD chirp based on the frame timing

detected from received raw signals. Both chirps deviate Δt from their real edges and thus correspond to $y_{pre}(t+\Delta t)$ and $y_{sfd}(t+\Delta t)$, respectively, as illustrated in Figure 5.2(a,b). Since the same time offset (*i.e.*, Δt) transforms into opposite frequency offsets for preamble up-chirp and SFD down-chirp [88], we can remove the effect of timing offset Δt by multiplying $y_{pre}(t+\Delta t)$ with $y_{sfd}(t+\Delta t)$, which produces the following (noise $n(t)$ is omitted for clarity and h^{air} means air-channel).

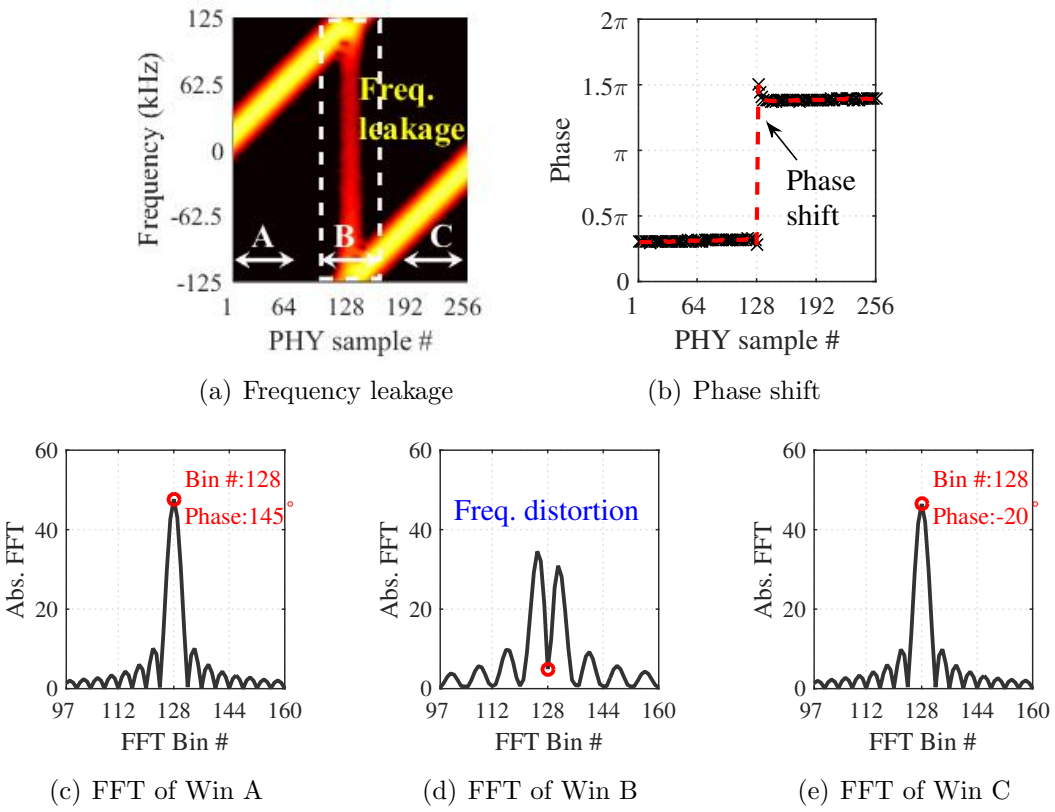
$$\begin{aligned} y_{pre}(t+\Delta t)\cdot y_{sfd}(t+\Delta t) &= y_{pre}(t)e^{j2\pi(\frac{BW^2}{2^{SF}}\Delta t)t}\cdot \\ & \quad y_{sfd}(t)e^{-j2\pi(\frac{BW^2}{2^{SF}}\Delta t)t} \\ &= (h^{air})^2\cdot e^{-j2\pi(2\Delta f_{cfo})t} \end{aligned} \tag{5.2}$$

We perform FFT on the resulting signal of Eq.(5.2), as shown in Figure 5.2(c). The FFT peak indicates the integer frequency of $2\Delta f_{cfo}$. Detailed methods for extracting CFO can be found in Chapter 4.

5.1.2 Frequency Leakage Extraction

We find that the signals transmitted by commodity LoRa radio suffer from frequency leakages. Figure 5.3(a) presents a chirp signal transmitted by Semtech SX1276 radio. We can observe weak power leaking from main frequencies (*i.e.*, *frequency leakage*) when the chirp signal transits from the maximum frequency to the minimum. Specifically, we compare the samples transmitted by SX1276 against an ideal chirp signal of the same symbol.

A phase shift is observed around positions of frequency leakage as shown in Figure 5.3(b). Figures 5.3(c,d,and e) further compare phase measurements of chirp signals from windows A, B, and C (*i.e.*, before and after the phase shift). The phase measurements differ by 165° because of the phase shift of transmitted samples. Figure (d) shows the frequency distortion at window B. The frequency distortion of a legitimate node may be different from that of a malicious node. We can calculate the distortion distribution to differentiate a legitimate node from a spoofing node. We



(a) Frequency leakage

(b) Phase shift

(c) FFT of Win A

(d) FFT of Win B

(e) FFT of Win C

Figure 5.3: Illustration of frequency leakage and impacts on phase measurements.

leave this problem for future work.

5.1.3 Propagation Signature Extraction

Propagation signatures indicate the location information of a transmitter, which can be used to identify a spoofing node. The communication channel from a transmitter to a receiver involves not only RF chains of Tx and Rx radios but also wireless channel over the air (*i.e.*, *air-channel*). We extract the air-channel features from phase measurements.

The raw phase measurements are affected by frequency offsets and phase noises, which challenges the extraction of air-channel. We extract air-channel from LoRa symbols by overcoming a number of practical challenges.

Distortions of radio hardware. The end-to-end communication channel h is composed of RF chains of transmitter and receiver radios (denoted by h^{rf}) and air-channel h^{air}, *i.e.*, $h = h^{air} \cdot h^{rf}$. The raw phase measurements from received symbols can be affected by various RF components of Tx and Rx radios (*i.e.*, h^{rf}). We summarize the primary sources of frequency and phase distortions introduced by radio hardware (*i.e.*, h^{rf}) as below.

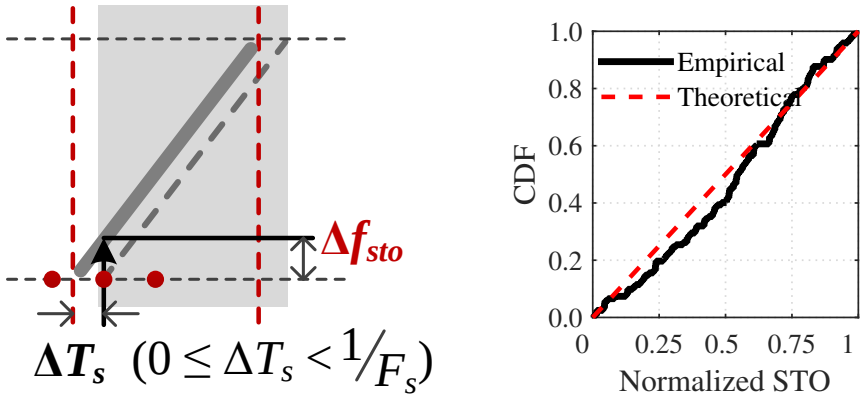
Central Frequency Offset (CFO). Due to hardware imperfection, the oscillator frequency of a LoRa node may be different from a gateway, resulting in central frequency offset. CFO can lead to frequency deviation of received symbols, as well as phase rotations across symbols of a packet.

Sampling Timing Offset (STO). Due to narrow bandwidth and low sampling rates of LoRa radio, the time offset between packet arrival and time of being sampled by a radio can be relatively long. It can cause non-negligible distortions to the frequency and phase of received symbols.

Radio frequency leakage. LoRa radio is subject to frequency leakage when the frequency of transmitted signals changes from one chirp to another (*e.g.*, at the boundary of two symbols) [104]. It adds unpredictable phase shifts to transmitted symbols, leading to inter-symbol phase variance.

The preamble of a LoRa packet is conventionally designed for frequency and frame timing synchronization. Our work explores to use preambles for channel phase calibration. In the previous section, we introduced how to extract fine-grained CFO and show the impact of radio frequency leakage. In the following, we mainly focus on how to mitigate the impact of STO and frequency leakage.

Compensating Sampling Timing Offset (STO). Incoming signal $y(t)$ will be sampled by an Analog-to-Digital Converter (ADC) into discrete samples $y[n]$. The time offset between signal arrival and sampling time of a receiver (*i.e.*, STO) introduces frequency and phase distortion to received chirps. As illustrated in Figure



(a) STO illustration

(b) Statistics of Δf_{sto}

Figure 5.4: Illustration of STO and empirical measurement results.

5.4(a), ΔT_s denotes the time offset of STO. The time offset would transform into a frequency offset Δf_{sto} and a phase offset φ_{sto} for a chirp signal. The received samples are represented below.

$$y[n] = e^{j(2\pi \Delta f_{sto} t + \varphi_{sto})} \cdot y(t), \quad t = \frac{n}{F_s} \tag{5.3}$$

where $\Delta f_{sto} = \frac{BW^2}{2^{SF}} \Delta T_s$, $\varphi_{sto} = 2\pi f_{sym} \Delta T_s$, $y(t)$ is given by Eq.(5.1) and f_{sym} is the initial frequency of chirp signal $y(t)$.

We note that STO is independent of CFO. STO does not influence CFO estimation because the received preamble chirp and SFD chirp share the same STO, which can be removed by Eq.(5.2). In particular, as STO is determined by both the arrival time of packet and sampling timing of receiver, STO changes across packets. It means that we cannot estimate STO in prior and use one estimation to calibrate for all packets. Instead, we should estimate and calibrate STO on a per-packet basis.

We estimate STO from the separated preambles of concurrent packets after CFO compensation. Since ΔT_s is basically less than a sample, Δf_{sto} is smaller than the frequency resolution of FFT ($\frac{BW}{2^{SF}}$), *i.e.*, Δf_{sto} is a fractional frequency.

In practice, we estimate the fractional frequency of a preamble chirp by pro-

gressively removing Δf from the received raw signal $y(t)$. The magnitude of FFT Bin #1 is maximized if Δf is removed completely. Let $Y(\Delta f)$ denote the FFT of $y(t)e^{-j2\pi\Delta ft} \cdot C^{-1}(t)$. The fractional frequency of preamble chirp in $y(t)$ is estimated as follows.

$$\Delta\tilde{f} = \arg \max_{-1<\Delta f<1} \|Y(\Delta f)@\text{Bin } \#1\| \tag{5.4}$$

As Δf is estimated based on the FFT magnitude of preamble chirp (*i.e.*, Bin #1), the method is resistant to noise and interference because the power of noise and interference do not accumulate in Bin #1. To accelerate the searching process, we first use grid search to find a coarse Δf within ± 1 FFT bin and next use binary search to find $\Delta\tilde{f}$ in a confined range.

Then we can use Eq.(5.4) to find Δf_{sto}. Figure 5.4(b) displays the CDF of Δf_{sto} measured from 500 LoRa packets. As expected, Δf_{sto} generally follows a uniform distribution in $[0, 1) \times \frac{BW}{2^{SF}}$.

Mitigating frequency leakage. After compensating received signals for CFO and STO, we expect to obtain consistent phase measurements from symbols of a packet. However, inter-symbol phase variance is still observed in payload. We take CFO, STO and inter-symbol phase variance into account and characterize the received signal of a LoRa symbol as below (noise $n(t)$ is omitted).

$$y(t) = h^{air} \cdot \underbrace{e^{-j(2\pi\Delta f_{cfo}t+\varphi_{osc})} e^{j(2\pi\Delta f_{sto}t+\varphi_{sto})} e^{j\varphi_{var}}}_{h^{rf}} \cdot S(t, f_{sym}), \tag{5.5}$$

where φ_{var} represents the phase variance introduced by frequency leakages of LoRa radio.

Note that the initial phase of symbol $S(t, f_{sym})$ is φ_{sym}, and the phase of air-channel h^{air} is denoted by φ^{air}. After we remove CFO and STO, the phase measurement from $y(t)$ becomes $\phi = \varphi^{air} - \varphi_{osc} + \varphi_{sto} + \varphi_{var} + \varphi_{sym}$. As the goal is to extract phase of air channel (*i.e.*, φ^{air}), we need to remove phase uncertainties of

radio hardware (*i.e.*, $\varphi_{osc}, \varphi_{sto}, \varphi_{var}, \varphi_{sym}$) from ϕ to derive φ^{air}.

We use two synchronized Rx antennas (named an *Rx-pair*) to calibrate hardware phase uncertainties. For clarity, we denote the two antennas of an Rx-pair by Rx1 and Rx2 respectively. As the signals received by Rx1 and Rx2 correspond to the same packet, they share the same inter-symbol phase variance (φ_{var}) and symbol initial phase (φ_{sym}), because φ_{var} and φ_{sym} are determined by Tx radio and thus are invariant at Rx1 and Rx2. Besides, as Rx1 and Rx2 share the same clock source, the phase of oscillator frequency and STO remain the same. We can remove phase uncertainties of both Tx and Rx radios by subtracting the phase measurements of Rx1 and Rx2, which gives $\phi_1 - \phi_2 = \varphi_1^{air} - \varphi_2^{air}$.

Phase Difference of Air-channels (PDoA). $\varphi_1^{air} - \varphi_2^{air}$ represents the phase difference between air-channels from transmitter to Rx1 and Rx2, termed *Phase Difference of Air-channels (PDoA)*. We plan to use PDoA as a phase feature of air-channel to identify spoofing nodes.

In practice, we use a pair of Rx antennas to extract PDoA for received symbols. We separately process the received signals of Rx1 and Rx2 (*e.g.*, CFO and STO compensation) to measure the phase for each symbol. We extract the PDoA of a symbol by subtracting the corresponding phase measurements of Rx1 and Rx2.

5.2 Preliminary Results

We first show the results of extracting air-channel phase. Figures 5.5(a) and (b) compare phase measurements before and after CFO and STO compensation. The phase measurements in preamble become invariant. Figure 5.5(c) presents the PDoA measurements from symbols of the packet in Figure 5.5(a,b). We can observe that the PDoA stays consistent across symbols in both preamble and payload of a packet.

To test the feasibility of using PDoA against spoofing attack, we place two com-

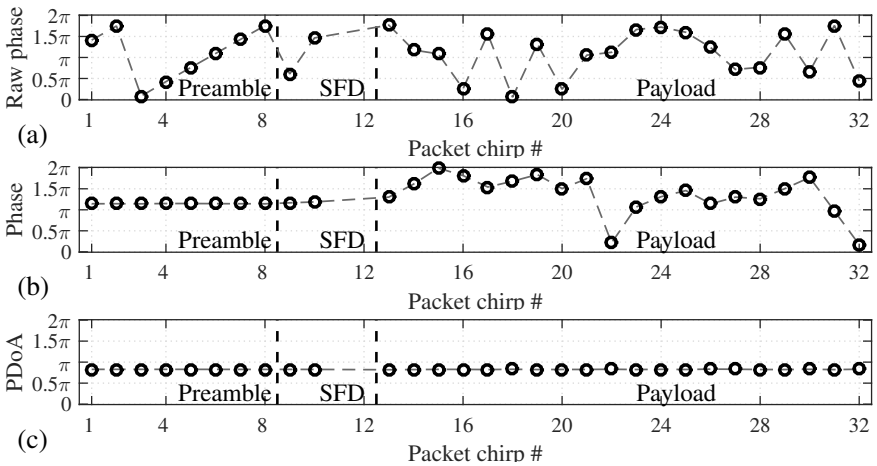


Figure 5.5: Phase measurements: (a) from received raw signals; (b) after compensating for CFO and STO; (c) after calibrating for both frequency and phase.

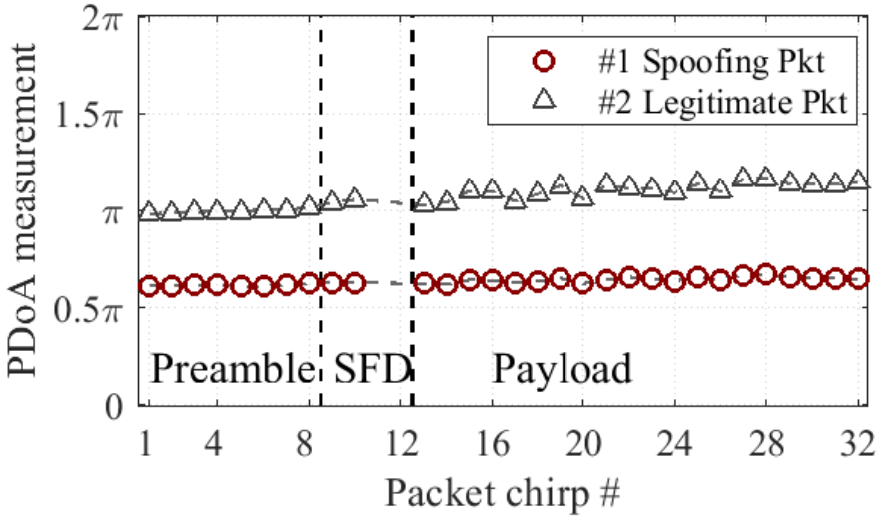


Figure 5.6: PDoA of two nodes located at different places.

modity LoRa nodes at two different locations and then extract the corresponding PDoA. Figure 5.6 shows the results. If we consider packet # 1 is from a spoofing node and packet # 2 is from a legitimate node, we can differentiate them by extracting PDoA. This experiment demonstrate that PDoA can be used as a propagation signature to assist LoRa node authentication.

Chapter 6

Conclusions

LoRa is a promising Low-Power Wide-Area Networking (LPWAN) technology that touted to provide long range ubiquitous connectivity for billions of everyday objects with an AA battery. It now has found wide applications in many areas such as smart agriculture, smart city, smart logistics and so on. Yet popular, the security of LoRa-enabled devices is one of the most important problems which may impede the further development of LoRaWAN. In this thesis, I focus on the security issues of LoRa physical layer. In specific, I study the possible security attack at both the transmitter side (covert channel) and receiver side (jamming attack) and propose corresponding countermeasures.

First, we reveal the vulnerability of current LoRaWAN physical layer where the legacy end-to-end security mechanisms fail to protect. We demonstrate this by designing and implementing a covert channel transceiver named `CloakLoRa` with COTS LoRa devices. We prototype `CloakLoRa` with simple passive components that can be secretly embedded into sensor nodes. We also design and implement a simple yet effective covert channel decoder using a low-cost software-defined radio. In this work, we conduct comprehensive experiments with COTS LoRa nodes as well as software defined radios under various experiment settings. Experiment results validate the feasibility of building a covert channel over LoRa. This work exposes 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.

Second, we study a possible attack at receiver. We investigate the vulnerability of LoRa gateway under jamming attacks. Though wireless jamming has been extensively studied in the literature, the case is different when it comes to LoRa for LoRa's unique chirp spread spectrum (CSS) modulation, which is inherently resilient and robust to interference. To better understand LoRa demodulation under jamming attacks, we conduct comprehensive experiments. By conducting experiments, we expose the risk of LoRa gateways under the attack of synchronized jamming chirps, which could lead to single point of failure in LoRaWAN. To against the attack of synchronized jamming chirps, we propose a new collision recovery method as a countermeasure by leveraging the difference in signal strength of jamming chirps and LoRa chirps. Experiment results demonstrate the effectiveness of our jamming and protection methods.

It is demonstrated that LoRa communication are prone to various security attacks, then we ask the question of whether we can enhance the security of LoRa by using some lightweight mechanism. We aim at a lightweight security mechanism because LoRa devices are designed with low-power and low-cost hardware. However, we can utilize the hardware imperfection of low-cost hardware to do physical layer authentication. Specifically, we use fine-grained carrier frequency offset (CFO) and distribution of frequency leakage as hardware signatures. Besides, we enhance the authentication scheme by combining unique propagation feature of legitimate packets. Specifically, we extract phase difference of air-channels (PDoA) as propagation signature to protect a gateway against spoofing attack.

In summary, the research in this thesis is a pilot work which reveals the security vulnerability of LoRa PHY.

Bibliography

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

[2] Khaled Abdelfadeel, Victor Cionca, and Dirk Pesch. Poster: A fair adaptive data rate algorithm for lorawan. In *Proceedings of the 2018 International Conference on Embedded Wireless Systems and Networks*, pages 169–170, 2018.

[3] Ferran Adelantado, Xavier Vilajosana, Pere Tuset-Peiro, Borja Martinez, Joan Melia-Segui, and Thomas Watteyne. Understanding the limits of lorawan. *IEEE Communications magazine*, 55(9):34–40, 2017.

[4] Md Atiqur Rahman Ahad. Activity recognition for health-care and related works. In *Proceedings of the 2018 ACM International Joint Conference and 2018 International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers*, pages 1765–1766, 2018.

[5] LoRa Alliance. Lorawan for developer. https://lora-alliance.org/lorawan-for-developers, 2020.

[6] LoRa Alliance. How lorawan can help fight covid-19. http://pages.services/pages.lora-alliance.org/covid-19-lorawan-solutions/, 2021.

[7] Wifi alliance. Wi-fi specification. https://www.wi-fi.org/discover-wi-fi/specifications, 2021.

[8] Emekcan Aras, Gowri Sankar Ramachandran, Piers Lawrence, and Danny Hughes. Exploring the security vulnerabilities of lora. In *2017 3rd IEEE International Conference on Cybernetics (CYBCONF)*, pages 1–6. IEEE, 2017.

[9] Emekcan Aras, Nicolas Small, Gowri Sankar Ramachandran, Stéphane Delbruel, Wouter Joosen, and Danny Hughes. Selective jamming of lorawan using commodity hardware. In *Proceedings of the 14th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, pages 363–372, 2017.

[10] BEHRTECH. 6 leading types of iot wireless tech and their best use cases. https://behrtech.com/blog/6-leading-types-of-iot-wireless-tech-and-their-best-use-cases/, 2020.

[11] Martin C Bor, Utz Roedig, Thiemo Voigt, and Juan M Alonso. Do lora low-power wide-area networks scale? In *Proceedings of the 19th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, pages 59–67, 2016.

[12] Taoufik Bouguera, Jean-François Diouris, Jean-Jacques Chaillout, Randa Jaouadi, and Guillaume Andrieux. Energy consumption model for sensor nodes based on lora and lorawan. *Sensors*, 18(7):2104, 2018.

[13] Marco Centenaro, Lorenzo Vangelista, Andrea Zanella, and Michele 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.

[14] RC Chakinala, Abishek Kumarasubramanian, R Manokaran, Guevara Noubir, C Pandu Rangan, and Ravi Sundaram. Steganographic communication in ordered channels. In *International Workshop on Information Hiding*, pages 42–57. Springer, 2006.

[15] Gonglong Chen, Wei Dong, and Jiamei Lv. Lofi: Enabling 2.4ghz lora and wifi coexistence by detecting extremely weak signals. In *IEEE INFOCOM'21*, 2021.

[16] Lili Chen, Jie Xiong, Xiaojiang Chen, Sunghoon Ivan Lee, Kai Chen, Dianhe Han, Dingyi Fang, Zhanyong Tang, and Zheng Wang. Widesee: Towards wide-area contactless wireless sensing. In *Proceedings of the 17th Conference on Embedded Networked Sensor Systems*, SenSys '19, page 258–270, 2019.

[17] Lili Chen, Jie Xiong, Xiaojiang Chen, Sunghoon Ivan Lee, Kai Chen, Dianhe Han, Dingyi Fang, Zhanyong Tang, and Zheng Wang. Widesee: Towards wide-area contactless wireless sensing. In *Proceedings of the 17th Conference on Embedded Networked Sensor Systems*, pages 258–270, 2019.

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

[19] Dragino. Decoding the chinese super micro super spy-chip super-scandal: What do we know – and who is telling the truth? https://bit.ly/2NlY9lS, 2019.

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

[21] Salvatore D'Oro, Francesco Restuccia, and Tommaso 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.

[22] Adel El-Atawy and Ehab Al-Shaer. Building covert channels over the packet reordering phenomenon. In *IEEE INFOCOM 2009*, pages 2186–2194. IEEE, 2009.

[23] Rashad Eletreby, Diana Zhang, Swarun Kumar, and Osman 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.

[24] Ericsson. Iot security. `https://www.ericsson.com/en/internet-of-things/iot-security`, 2021.

[25] ETSI. 4th generation (lte). `https://www.etsi.org/technologies/mobile/4G`, 2021.

[26] ETSI. Return on iot: Dealing with the iot skills gap. `https://www.forbes.com/sites/danielnewman/2019/07/30/return-on-iot-dealing-with-the-iot-skills-gap/#27017efb7091`, 2021.

[27] Akshay Gadre, Revathy Narayanan, Anh Luong, Anthony Rowe, Bob Iannucci, and Swarun Kumar. Frequency configuration for low-power wide-area networks in a heartbeat. In *17th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 20)*, pages 339–352, 2020.

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

[29] Amalinda Gamage, Jansen Christian Liando, Chaojie Gu, Rui Tan, and Mo Li. Lmac: Efficient carrier-sense multiple access for lora. In *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking*, pages 1–13, 2020.

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

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

[32] Iwona Grabska and Krzysztof 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.

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

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

[35] GS1. Epc uhf gen2 air interface protocol. `https://www.gs1.org/standards/epc-rfid/uhf-air-interface-protocol`, 2021.

[36] Chaojie Gu, Linshan Jiang, Rui Tan, Mo Li, and Jun Huang. Attack-aware data timestamping in low-power synchronization-free lorawan. In *IEEE ICDCS'20*, 2020.

[37] Xiuzhen Guo, Longfei Shangguan, Yuan He, Jia Zhang, Haotian Jiang, Awais Ahmad Siddiqi, and Yunhao Liu. Aloba: rethinking on-off keying modulation for ambient lora backscatter. In *Proceedings of the 18th Conference on Embedded Networked Sensor Systems*, pages 192–204, 2020.

[38] Jetmir Haxhibeqiri, Floris Van den Abeele, Ingrid Moerman, and Jeroen Hoebeke. Lora scalability: A simulation model based on interference measurements. *Sensors*, 17(6):1193, 2017.

[39] Tahera Hossain, Md Atiqur Rahman Ahad, Tahia Tazin, and Sozo Inoue. Activity recognition by using lorawan sensor. In *Proceedings of the 2018 ACM International Joint Conference and 2018 International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers*, pages 58–61, 2018.

[40] Tahera Hossain, Yusuke Doi, Tahia Tazin, Md Atiqur Rahman Ahad, and Sozo Inoue. Study of lorawan technology for activity recognition. In *Proceedings of the 2018 ACM International Joint Conference and 2018 International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers*, pages 1449–1453, 2018.

[41] Salaheddin Hosseinzadeh, Hadi Larijani, Krystyna Curtis, Andrew Wixted, and Amin 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.

[42] Bashima Islam, Md Tamzeed Islam, and Shahriar Nirjon. Feasibility of lora for indoor localization. *on-line, from semanticscholar. org*, pages 1–11, 2017.

[43] Justin, Anran Chan, and Shyamnath Gollakota Wang, Arvind Krishnamurthy. Deepsense: Enabling carrier sense in low-power wide area networks using deep learning.

[44] Matt Knight. Gr-lora. `https://github.com/BastilleResearch/gr-lora`.

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

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

[47] Mads Lauridsen, Istvan Z. Kovacs, Preben Mogensen, Mads Sorensen, and Steffen Holst. Coverage and capacity analysis of lte-m and nb-iot in a rural area. In *Proceedings of IEEE 84th Vehicular Technology Conference*, (VTC-Fall 2016), pages 1–5, Sep 2016.

[48] Alexandru Lavric and Valentin Popa. A lorawan: Long range wide area networks study. In *2017 International Conference on Electromechanical and Power Systems (SIELMEN)*, pages 417–420. IEEE, 2017.

[49] Yinghui Li, Jing Yang, and Jiliang Wang. Dylora: Towards energy efficient dynamic lora transmission control. In *IEEE INFOCOM 2020-IEEE Conference on Computer Communications*, pages 2312–2320. IEEE, 2020.

[50] Zhijun Li and Yongrui Chen. Ble2lora: Cross-technology communication from bluetooth to lora via chirp emulation. In *2020 17th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, pages 1–9. IEEE, 2020.

[51] Jansen C. Liando, Amalinda Gamage, Agustinus W. Tengourtius, and Mo Li. Known and unknown facts of lora: Experiences from a large-scale measurement study. *ACM Trans. Sen. Netw.*, 15(2), February 2019.

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

[53] Jin-Taek Lim and Youngnam Han. Spreading factor allocation for massive connectivity in lora systems. *IEEE Communications Letters*, 22(4):800–803, 2018.

[54] Li Liu, Yuguang Yao, Zhichao Cao, and Mi Zhang. Deeplora: Learning accurate path loss model for long distance links in lpwan. In *IEEE INFOCOM'21*, 2021.

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

[56] Yiliang Liu, Hsiao-Hwa Chen, and Liangmin Wang. Physical layer security for next generation wireless networks: Theories, technologies, and challenges. *IEEE Communications Surveys and Tutorials*, 19(1):347–376, 2017.

[57] Konstantin Mikhaylov, Radek Fujdiak, Ari Pouttu, Voznak Miroslav, Lukas Malina, and Petr Mlynek. Energy attack in lorawan: experimental validation. In *Proceedings of the 14th International Conference on Availability, Reliability and Security*, pages 1–6, 2019.

[58] Aristides Mpitziopoulos, Damianos Gavalas, Charalampos Konstantopoulos, and Grammati Pantziou. A survey on jamming attacks and countermeasures in wsns. *IEEE Communications Surveys & Tutorials*, 11(4):42–56, 2009.

[59] Rajalakshmi Nandakumar, Vikram Iyer, and Shyamnath Gollakota. 3d localization for sub-centimeter sized devices. In *Proceedings of the 16th ACM Conference on Embedded Networked Sensor Systems*, pages 108–119. ACM, 2018.

[60] Umber Noreen, Ahcène Bounceur, and Laurent Clavier. A study of lora low power and wide area network technology. In *2017 International Conference on Advanced Technologies for Signal and Image Processing (ATSIP)*, pages 1–6. IEEE, 2017.

[61] Lorenzo Parri, Stefano Parrino, Giacomo Peruzzi, and Alessandro Pozzebon. Low power wide area networks (lpwan) at sea: Performance analysis of offshore data transmission by means of lorawan connectivity for marine monitoring applications. *Sensors*, 19(14):3239, 2019.

[62] Gianni Pasolini, Chiara Buratti, Luca Feltrin, Flavio Zabini, Cristina De Castro, Roberto Verdone, and Oreste Andrisano. Smart city pilot projects using lora and ieee802. 15.4 technologies. *Sensors*, 18(4):1118, 2018.

[63] Yao Peng, Longfei Shangguan, Yue Hu, Yujie Qian, Xianshang Lin, Xiaojiang Chen, Dingyi Fang, and Kyle 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.

[64] Juha Petäjäjärvi, Konstantin Mikhaylov, Marko Pettissalo, Janne Janhunen, and Jari Iinatti. Performance of a low-power wide-area network based on lora technology: Doppler robustness, scalability, and coverage. *International Journal of Distributed Sensor Networks*, 13(3):1550147717699412, 2017.

[65] Juha Petajajarvi, Konstantin Mikhaylov, Antti Roivainen, Tuomo Hanninen, and Marko Pettissalo. On the coverage of lpwans: range evaluation and channel attenuation model for lora technology. In *2015 14th International Conference on ITS Telecommunications (ITST)*, pages 55–59. IEEE, 2015.

[66] Juha Petäjäjärvi, Konstantin Mikhaylov, Rumana Yasmin, Matti Hämäläinen, and Jari Iinatti. Evaluation of lora lpwan technology for indoor remote health and wellbeing monitoring. *International Journal of Wireless Information Networks*, 24(2):153–165, 2017.

[67] Congduc Pham. Investigating and experimenting csma channel access mechanisms for lora iot networks. In *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1–6. IEEE, 2018.

[68] Postscapes. Internet of things (iot) examples. `https://www.postscapes.com/internet-of-things-examples/`, 2021.

[69] Andri Rahmadhani and Fernando Kuipers. When lorawan frames collide. In *Proceedings of the 12th International Workshop on Wireless Network Testbeds, Experimental Evaluation & Characterization*, pages 89–97, 2018.

[70] Rapeepat Ratasuk, Benny Vejlgaard, Nitin Mangalvedhe, and Amitava Ghosh. Nb-iot system for m2m communication. In *Proceedings of IEEE Wireless Communications and Networking Conference*, (WCNC 2016), pages 1–5, Apr 2016.

[71] Brecht Reynders, Wannes Meert, and Sofie Pollin. Power and spreading factor control in low power wide area networks. In *2017 IEEE International Conference on Communications (ICC)*, pages 1–6. IEEE, 2017.

[72] Brecht Reynders, Qing Wang, Pere Tuset-Peiro, Xavier Vilajosana, and Sofie Pollin. Improving reliability and scalability of lorawans through lightweight scheduling. *IEEE Internet of Things Journal*, 5(3):1830–1842, 2018.

[73] Pieter Robyns, Peter Quax, Wim Lamotte, and William Thenaers. A multi-channel software decoder for the lora modulation scheme. 2018.

[74] Matthias Schulz, Jakob Link, Francesco Gringoli, and Matthias 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.

[75] Semtech. Lora applications. `https://www.semtech.com/lora/lora-applications`, 2021.

[76] Semtech. Lora transceivers sx1276. `https://www.semtech.com/products/wireless-rf/lora-transceivers/sx1276`, 2021.

[77] Semtech. Smart agriculture. https://www.semtech.com/uploads/technology/LoRa/app-briefs/AB-SEMTECH-LORA-SMART-AGR-VINDUINO.PDF, 2021.

[78] Junyang Shi, Di Mu, and Mo 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.

[79] SIG. Bluetooth specification. https://www.bluetooth.com/specifications/specs/, 2021.

[80] SigFox. Sigfox overview. https://www.sigfox.com/en/sigfox-iot-technology-overview, 2020.

[81] Rashmi Sharan Sinha, Yiqiao Wei, and Seung-Hoon Hwang. A survey on lpwa technology: Lora and nb-iot. *Ict Express*, 3(1):14–21, 2017.

[82] Elahe Soltanaghaei, Akarsh Prabhakara, Artur Balanuta, Matthew Anderson, Jan M Rabaey, Swarun Kumar, and Anthony Rowe. Millimetro: mmwave retro-reflective tags for accurate, long range localization. In *Proceedings of the 27th Annual International Conference on Mobile Computing and Networking*, pages 69–82, 2021.

[83] Green Stream. Track flood status. https://www.greenstream.com/, 2021.

[84] Jothi Prasanna Shanmuga Sundaram, Wan Du, and Zhiwei Zhao. A survey on lora networking: Research problems, current solutions and open issues. *IEEE Communications Surveys & Tutorials*, 22(1), 2019.

[85] synopsys. Attacks on iot devices have a domino effect. https://www.synopsys.com/blogs/software-security/cyber-physical-attacks/, 2019.

[86] Krzysztof Szczypiorski and Wojciech 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.

[87] Vamsi Talla, Mehrdad Hessar, Bryce Kellogg, Ali Najafi, Joshua R Smith, and Shyamnath Gollakota. Lora backscatter: Enabling the vision of ubiquitous connectivity. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 1(3):1–24, 2017.

[88] Shuai Tong, Jiliang Wang, and Yunhao Liu. Combating packet collisions using non-stationary signal scaling in lpwans. In *ACM MobiSys'20*, 2020.

[89] Shuai Tong, Zhenqiang Xu, and Jiliang Wang. Colora: Enable muti-packet reception in lora. In *IEEE INFOCOM'20*, 2020.

[90] Nilufer Tuptuk and Stephen Hailes. Covert channel attacks in pervasive computing. In *2015 IEEE international conference on pervasive computing and communications (PerCom)*, pages 236–242. IEEE, 2015.

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

[92] Benny Vejlgaard, Mads Lauridsen, Huan Nguyen, István Z Kovács, Preben Mogensen, and Mads Sorensen. Coverage and capacity analysis of sigfox, lora, gprs, and nb-iot. In *2017 IEEE 85th vehicular technology conference (VTC Spring)*, pages 1–5. IEEE, 2017.

[93] Xiong Wang, Linghe Kong, Liang He, and Guihai 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.

[94] Xiong Wang, Linghe Kong, Zucheng Wu, Long Cheng, Chenren Xu, and Guihai Chen. Slora: towards secure lora communications with fine-grained physical layer features. In *Proceedings of the 18th Conference on Embedded Networked Sensor Systems*, pages 258–270, 2020.

[95] Yuting Wang, Xiaolong Zheng, Liang Liu, and Huadong Ma. Polartracker: Attitude-aware channel access for floating low power wide area networks. In *IEEE INFOCOM'21*, 2021.

[96] Zhe Wang, Linghe Kong, Kangjie Xu, Liang He, Kaishun Wu, and Guihai Chen. Online concurrent transmissions at lora gateway. In *IEEE INFOCOM 2020-IEEE Conference on Computer Communications*, pages 2331–2340. IEEE, 2020.

[97] 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.

[98] Andrew J Wixted, Peter Kinnaird, Hadi Larijani, Alan Tait, Ali Ahmadinia, and Niall Strachan. Evaluation of lora and lorawan for wireless sensor networks. In *2016 IEEE SENSORS*, pages 1–3. IEEE, 2016.

[99] Anthony D Wood, John A Stankovic, and Gang Zhou. Deejam: Defeating energy-efficient jamming in ieee 802.15. 4-based wireless networks. In *2007 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, pages 60–69. IEEE, 2007.

[100] Kaishun Wu, Haoyu Tan, Yunhuai Liu, Jin Zhang, Qian Zhang, and Lionel M Ni. Side channel: Bits over interference. *IEEE Transactions on Mobile Computing*, 11(8):1317–1330, 2012.

[101] Xianjin Xia, Shining Li, Yu Zhang, Bingqi Li, Yuanqing Zheng, and Tao Gu. Enabling out-of-band coordination of wi-fi communications on smartphones. *IEEE/ACM Transactions on Networking*, 27(2):518–531, 2019.

[102] Xianjin Xia, Yuanqing Zheng, and Tao Gu. Ftrack: Parallel decoding for lora transmissions. In *Proceedings of the 17th Conference on Embedded Networked Sensor Systems*, pages 192–204, 2019.

[103] Xianjin Xia, Yuanqing Zheng, and Tao Gu. Ftrack: Parallel decoding for lora transmissions. *IEEE/ACM Transactions on Networking*, 28(6):2573–2586, 2020.

[104] Xianjin Xia, Yuanqing Zheng, and Tao Gu. Litenap: Downclocking lora reception. In *IEEE INFOCOM 2020-IEEE Conference on Computer Communications*, pages 2321–2330. IEEE, 2020.

[105] Binbin Xie and Jie Xiong. Combating interference for long range lora sensing. In *Proceedings of the 18th Conference on Embedded Networked Sensor Systems*, pages 69–81, 2020.

[106] Ting Xu and Ming Zhao. A lorawan-mac protocol based on wsn residual energy to adjust duty cycle. In *2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS)*, pages 1415–1420. IEEE, 2020.

[107] Wenyuan Xu, Wade Trappe, Yanyong Zhang, and Timothy Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*, pages 46–57, 2005.

[108] Zhenqiang Xu, Shuai Tong, Pengjin Xie, and Jiliang Wang. Fliplora: Resolving collisions with up-down quasi-orthogonality. In *2020 17th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, pages 1–9. IEEE, 2020.

[109] Zhenqiang Xu, Pengjin Xie, and Jiliang Wang. Pyramid: Real-time lora collision decoding with peak tracking. In *IEEE INFOCOM'21*, 2021.

[110] Zhice Yang, Qianyi Huang, and Qian 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.

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

[112] Fusang Zhang, Zhaoxin Chang, Kai Niu, Jie Xiong, Beihong Jin, Qin Lv, and Daqing Zhang. Exploring lora for long-range through-wall sensing. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 4(2):1–27, 2020.

[113] Guoming Zhang, Chen Yan, Xiaoyu Ji, Tianchen Zhang, Taimin Zhang, and Wenyuan Xu. Dolphinattack: Inaudible voice commands. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 103–117. ACM, 2017.

[114] Elzbieta Zielinska and Krzysztof 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.

[115] Yulong Zou, Jia Zhu, Xianbin Wang, and Lajos Hanzo. A survey on wireless security: Technical challenges, recent advances, and future trends. *Proceedings of the IEEE*, 104(9):1727–1765, 2016.