SLoRa: Towards Secure LoRa Communications with Fine-grained Physical Layer Features

[1]Xiong Wang, [1]Linghe Kong, [1]Zucheng Wu, [2]Long Cheng, [3]Chenren Xu, [1]Guihai Chen
[1]Shanghai Jiao Tong University, [2]Clemson University, USA,
[3]Peking University, China

ABSTRACT

LoRa, which is considered as an appealing wireless technique for Low-Power Wide-Area Networks (LPWANs), has found wide applications in fields such as smart cities, intelligent agriculture. Despite its popularity, there exists a growing concern about secure communications mainly due to the free frequency band and minimalist design specified in LoRa communications. For example, an attacker can forge messages to launch spoofing attack. To mitigate the threat, an authentication mechanism is needed. In this paper, we propose a lightweight node authentication scheme named SLoRa for LoRa networks by leveraging two physical layer features–Carrier Frequency Offset (CFO) and spatial-temporal link signature. In particular, we propose a novel CFO compensation algorithm, and identify slight CFO variations by adopting linear fitting for received upchirps to mitigate the noise's randomness on fine-grained CFO estimation. Besides, we can obtain fine-grained link signatures without the conventional de-convolution operation based on the theoretical analysis. Then, we show how these two physical-layer features complement each other to conquer the drift challenge brought by weather and environment variations. Combining these two features, SLoRa can distinguish whether the received signal is conveyed from a legitimate LoRa node or not. Experiments covering indoor and outdoor scenarios are conducted to demonstrate a high accuracy for node authentication in SLoRa, which is around 97% indoors and 90% outdoors.

CCS CONCEPTS

• **Networks → Network protocol design**.

KEYWORDS

LoRa Communications, CFO, Multipath Effect, Cryptographic Mechanisms, Node Authentication

ACM Reference Format:
[1]Xiong Wang, [1]Linghe Kong, [1]Zucheng Wu, [2]Long Cheng, [3]Chenren Xu, [1]Guihai Chen. 2020. SLoRa: Towards Secure LoRa Communications with Fine-grained Physical Layer Features. In *The 18th ACM Conference on Embedded Networked Sensor Systems (SenSys '20), November 16–19, 2020, Virtual Event, Japan.* ACM, New York, NY, USA, 13 pages.

SenSys '20, November 16–19, 2020, Virtual Event, Japan

ACM ISBN 978-1-4503-7590-0/20/11…$15.00

1 INTRODUCTION

As an important wireless technique designed for LPWANs, Long Range (LoRa) communications have gained considerable attentions from both academia and industry due to its low-power and low-cost [11, 13, 25]. Yet, the other side of the coin is that LoRa nodes bear the risk of attacks, which is of great concern to the reliability of LoRa networks.

In convention, LoRa networks are susceptible to security attacks, and the reason is two-fold. First, LoRa communications use the unlicensed frequency band and simple protocol specifications, rendering itself vulnerable to active attacks such as spoofing attacks and Denial-of-Service (DoS) attacks. Secondly, compared to traditional wireless techniques (e.g., WiFi, ZigBee), LoRa packets usually have a long duration. The wide transmission window provides sufficient time for attackers to launch spoofing and DoS attacks [3, 33].

The security performance of LoRa networks can be enhanced by adopting the symmetric-key cryptography mechanism in MAC layer [1]. Meanwhile, low-power and low-cost, which are the design goals of LoRa networks, make the implementation of complicated encryption algorithms infeasible. Then, an attacker may counterfeit legitimate nodes by compromising the encryption protocol. It is non-trivial to defend against active attacks by only leveraging existing hardware and infrastructure.

To comply with the design goal of LoRa protocol, this paper aims to improve LoRa's security by integrating the physical-layer authentication into LoRa communications, which extracts fine-grained CFO and spatial-temporal link signatures as the unique signature of legitimate LoRa nodes. Specifically, we exploit fine-grained CFOs which are based on hardware imperfections to distinguish LoRa nodes, and use proposed link signatures that highly rely on endpoints' positions of wireless links to distinguish locations of these LoRa nodes, and thus provide two-dimensional authentication. Launching active attacks such as spoofing attack or DoS attack, which should simultaneously eliminate the two types of differences between the attacker and legitimate nodes through manipulation, becomes extremely difficult.

We identify several practical challenges to capture CFO and temporal link signatures in LoRa networks. First, LoRa specifies its operation at a much narrower bandwidth such as 250 KHz within a wider coverage compared with traditional wireless techniques (e.g., WiFi). Fine-grained CFO extraction becomes much more challenging in the presence of noise and other interference. Secondly, the temporal link signature, which represents the physical layer characteristic of the radio channel between a transmitter and a receiver, is hard to extract in complex environments. Finally, CFO drift occurs due to temperature change and hardware aging, and

the link signature undergoes temporal variations induced by environmental dynamics. Stable CFO and link signature extraction is a particularly involved challenge.

To address above challenges, we provide node authentication and improve the security performance of LoRa communications. At the heart of our approach is a strategy that exploits hardware imperfections of low-cost components in LoRa radios, where signals sent by such hardware produce offset in time, frequency, and phase at the receiver (e.g., gateway). The hardware offset can be manifested as distinct aggregate frequency shift Δf, and the received upchirp signal can be represented as $e^{j2\pi\Delta f t}C$ after downconverting, rather than the standard upchirp C. Then, we can observe an FFT peak at Δf. In conventional LoRa demodulation process, the CFO Δf is coarsely estimated as an integral multiple of a Fourier transform bin. Compared to the coarse-grained CFO estimation, the peak location actually includes an arbitrary fraction of a Fourier bin since CFO is a physical phenomenon and then not need to be an integral multiple of a Fourier bin. We employ fine-grained CFOs composed of both fractional and integral parts as the node signature to distinguish nodes in LoRa networks. Specially, we propose a novel CFO compensation algorithm to measure Δf. However, there exist subtle fluctuations in estimated CFOs due to the noise effect in actual implementations. We then investigate the relationship between estimated CFOs and noises by employing linear fitting for received upchirps, and transform this relationship into a new relationship between CFOs and pairs of slope gradient and truncation rate of linear lines. According to pairs of slope gradient and truncation rate, we apply the Support Vector Machine (SVM) model to identify CFOs even with slight fluctuations, thus achieving fine-grained CFO estimation.

Besides the CFO estimation, we define the spatial-temporal link signature at a high level, which highly depends on endpoints' positions of wireless links. Similarly, we propose a lightweight link signature measurement methodology for the spatial-temporal link signature, and it can act as a sensitive feature for distinguishing LoRa nodes at different positions. To extract fine-grained link signatures, we first investigate the relationship between CFOs and link signatures, and find that fine-grained CFO estimation is conducive to the sensitive link signature extraction. Existing research work on the link signature estimation relies on the computation-intensive and complicated de-convolution which introduces inaccurate estimation simultaneously [24, 29]. To break the routine, we propose a theoretical model leveraging the unique demodulation mechanism of LoRa communications to achieve the fine-grained link signature estimation without de-convolution and verify that the link signature is highly related to the channel impulse response. Then, it can be used to indicate the physical layer characteristic of the radio channel.

Finally, we combine extracted CFOs and link signatures to achieve a robust node authentication and adapt to the drift of these two features induced by temperature variations and environment dynamics.

Research work on device authentication and security enhancement in wireless networks requires extra RFID tag [20, 35], or receiver and antenna deployment [12]. These schemes are costly and operating-inefficient for large-scale LoRa networks. Consequently, we propose SLoRa, a lightweight system based on passive radio analysis. We implement SLoRa on a testbed of conventional LoRa radios operating at 868 MHz. We employ an USRP N210 to emulate the LoRa gateway and utilize a commercial LoRa node as the transmitter, while using another ten LoRa nodes at different locations to launch attacks. The commodity client transmits data to the gateway in an office building and outdoor environments. We compare SLoRa's performance with individual CFO and link signature based schemes since existing research work using CFOs or link signatures have focused on node authentication in WiFi networks. Experiments conducted in both indoor and outdoor scenarios reveal that the authentication accuracy for legitimate nodes is about 97% indoors and 90% outdoors, while maintaining a low false alarm rate and small delay of around 100 ms.

The contributions can be summarized as follows.

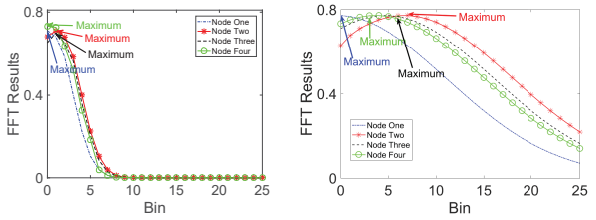
- This paper presents a novel physical layer authentication method named SLoRa which exploits two physical layer features in wireless communications–CFOs and link signatures, to improve the security performance in LoRa networks.
- To extract fine-grained CFOs, we present a CFO compensation algorithm and then employ the SVM model to identify the subtly fluctuated CFOs in the presence of noise by leveraging linear fitting for received upchirps. Meanwhile, we define the spatial-temporal link signature and propose a lightweight measurement method. Specifically, we combine the demodulation mechanism with a proposed theoretical model to extract fine-grained link signatures without deconvolution.
- Besides the fine-grained CFO and link signature extraction, we show how to combine these two features to adapt to the drift challenge induced by dynamic temperature and environments.
- We have implemented a prototype of SLoRa, in which LoRa nodes act as the transmitter and an USRP N210 act as the LoRa gateway.

2 MOTIVATION

Coupled with the recent world-wide deployment [10, 32, 40], the security of LoRa networks has gradually become a major hurdle. However, it is non-trivial to secure large-scale LoRa networks due to the resource-constraints in LoRa (e.g., low power and low-cost hardware). Although the symmetric-key cryptography mechanism can be used to guarantee security, the wide transmission window, free operated frequency band, and public standard make LoRa networks susceptible to malicious attacks [6]. The attacker can impersonate a legitimate node to convey deceptive packets to the gateway. Thus, it deserves attentions to further strengthen the security in LoRa networks. Accordingly, a lightweight security mechanism is desirable.

From another perspective, low-cost crystal oscillators embedded in LoRa nodes have an inherent mismatch with their nominal frequency value. Therefore, the down-conversion is performed with a different frequency than the up-conversion, which results in a CFO of the baseband signals. We have collected the received signals from four LoRa nodes which exhibit similar CFO patterns. As

shown in Fig. 1(a), we cannot utilize the coarse-grained CFOs based on the conventional LoRa demodulation to distinguish node one from node four, as well as for nodes two and three when setting SF as 8, since they are located at the same bin. In LoRa, one bin covers the frequency bandwidth equaling to $\frac{BW}{2^{SF}}$ and BW denotes the whole bandwidth. Then, if we perform a Fourier transform over a wider window when setting SF as the highest one−12, we can observe that CFOs of these four nodes differ from each other, respectively corresponding to 0, 4, 6, and 7 FFT bins. Consequently, these fine-grained CFOs can be exploited to distinguish large-scale LoRa nodes, yet lacking wide applicability for all SFs.



(a) SF=8 (b) SF=12

Figure 1: The CFO estimation based on the conventional LoRa demodulator when setting the spreading factor as 8 and 12, respectively.

Meanwhile, the LoRa modulation technique is relatively impervious to the initial frequency offset between the transmitter and receiver, which indicates that a high frequency offset tolerance up to dozens or even hundreds of KHz can be withstood while maintaining the link reliability [27]. If a fine-grained CFO between one LoRa node and gateway can be extracted, we can utilize this unique CFO as the signature for distinguishing large-scale LoRa nodes. The reason is that although crystal oscillators are constructed using the same manufacturing and packaging processes, no two are identical.

In addition to CFOs, we seek to improve the node distinguishability using the spatial-temporal link signature, which highly depends on the transmitter's location. Research work of [24, 34] has verified that the link signature in WiFi networks demonstrates a high diversity when endpoints locate at different positions. In adversary settings, an attacker cannot measure the legitimate link between legitimate nodes and the gateway, unless it is located at exactly the same location as the gateway. Even if an attacker can measure a link signature, it can hardly present the same link signature at the gateway unless it is at the same location as the legitimate node. Hence, the unique link signature can be employed as another sensitive signature for distinguishing LoRa nodes with a large-scale deployment. The coarse link signature can be extracted highly relying on WiFi's modulation mode (i.e., OFDM) and incurring certain computation overhead simultaneously [24]. However, it is hard to achieve this due to the unique modulation mode (i.e., CSS) in physical layer of LoRa communications. A more accurate and lightweight scheme for the link signature extraction is required to build a lightweight system for node authentication in LoRa networks.

3 RELATED WORK

To improve the security of wireless networks, cryptographic mechanisms have been proposed for WiFi [2], Zigbee [9], and RFID [15, 20, 26].

Research work in [8] uses the received signal strength (RSS) as the signature for node authentication in 802.11e networks. However, RSS may undergo variations and becomes unreliable. Furthermore, much research work employs link signatures as the signature of end devices to defend against active attacks [18, 19, 41]. Wang et al. [36] propose to extract the peculiar propagation characteristics of creeping waves to discern on-body devices for authentication. The authors of [28] perform a man-in-the-middle attack and inject control commands into WiFi links leveraging the security vulnerabilities. To improve the security of WiFi networks, xiong et al. [37] propose a signal processing algorithm named SecureArray by leveraging multi-antenna access point, in order to construct the direction profiles at which a client's signals arrive. It highly depends on the AoA information to construct highly sensitive signatures. However, these schemes are not suitable for LoRa communications. First, LoRa communications can only provide little channel information in the physical layer compared to WiFi. Hence, it is impossible to obtain the AoA information in LoRa communications. Secondly, the link signature estimation requires complicated processing (e.g., IFFT operations), which challenges the lightweight node authentication design.

Meanwhile, design enhancements are proposed to improve the security performance of Zigbee [22, 23]. The authors of [5] introduce a robust and fast chaotic encryption algorithm since chaotic functions can be used to construct high speed and strong stream ciphers.

In addition, the security of RFID communications has received widespread attentions due to the simplified design [17, 31]. The authors of [35] propose a physical layer authentication protocol which is resilient to attacks like tag counterfeiting. It mainly leverages the features of inductive coupling of two tags and signal randomization to secure the RFID communications.

There exists a weak security mechanism with free band and public standard in LoRa communications [4, 30]. The authors of [3] explore the potential security vulnerabilities, and they analyze the LoRa network stack and present several kinds of attacks leveraging commercial-off-the-shelf hardware. Analysis demonstrates that LoRa communications are prone to multiple security attacks.

To defend against these attacks, the authors of [38] propose a key establishment protocol, which employs a number of signal processing techniques to significantly improve the key generation rate. Recently, Choir proposed in [11] aims to resolve the collision problem based on relative CFOs corresponding to different LoRa nodes. However, it becomes more challenging for SLoRa since it should extract the absolute CFOs to serve as the signature of LoRa nodes.

The research work most related to SLoRa is an CFO based security scheme in [14]. Both of them leverage CFOs to serve for node authentication, yet differing in the CFO estimation algorithms. The authors of [14] extract fine-grained CFOs by applying the linear regression and least squares methods to fit the time-domain LoRa signals. Differently, a novel frequency-domain CFO estimation is

proposed in SLoRa leveraging the demodulation mechanism. Meanwhile, compared to [14] based on CFO, SLoRa combines both CFO and link signature to improve the security performance of LoRa communications.

4 SLORA IN A NUTSHELL

In this section, we introduce the threat model in LoRa networks, followed by the system architecture of SLoRa.

4.1 Threat Model

In LoRa networks, the most common scenario is the data uploading from nodes to the gateway. In a typical attack case, the legitimate node transmits the sensed information to the gateway. Immediately, at the node side, two time windows are set to receive an acknowledgement from the gateway. During this process, a powerful attacker who has a prior knowledge of the LoRa protocol and the legitimate node (e.g., the coding strategy, carrier frequency and transmission power) can leverage an omnidirectional antenna to detect the interaction [7, 39]. Then, it utilizes a directional antenna to inject fake data (e.g., the DoS command or spoofing data). If the gateway accepts the spoofed command, it results in an rejection or unauthorized access to legitimate nodes.

In this work, we assume the adversary is able to launch various active attacks against the integrity (e.g., false data injection or replay attacks) and availability (e.g., DoS attacks) of LoRa networks. Although LoRa employs symmetric-key cryptographic mechanisms, such attacks are still possible if the encryption key is leaked.

4.2 System Overview

With SLoRa, we can detect above active attacks, and Fig. 2 describes its framework, which mainly consists of the offline feature extraction phase and online detection phase. The offline phase in SLoRa is responsible for collecting LoRa signals from legitimate nodes. Then, it extracts fine-grained CFOs and link signatures respectively according to two designed feature extraction algorithms, and they are fed into the SVM model for training. When a new LoRa node joins the LoRa network, we collect LoRa signals transmitted from this node and extract the physical layer features.

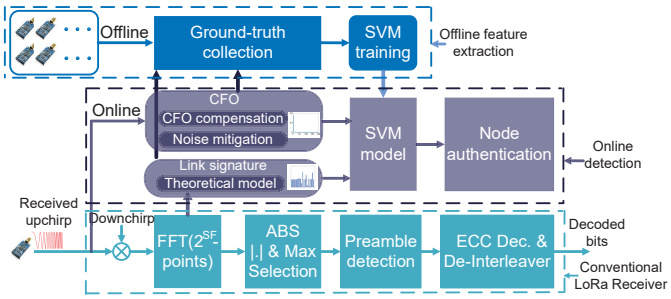


Figure 2: The framework of SLoRa.

The online detection phase of SLoRa first extracts CFO and link signature sent from an anonymous LoRa node. These unique features are fed into the SVM model, and then it compares the online collected features with the features learnt from the offline phase. According to the similarity comparison, the SVM model determines whether the derived node is within the set of legitimate nodes. SLoRa identifies that the received signal is conveyed from a legitimate node. Otherwise, it comes from an attacker and an alarm is generated. For benign cases, the newly obtained features are fed into the ground-truth collection module in the offline phase, while the oldest feature pair is discarded for constant memory usage and feature update.

5 SLORA DESIGN

This section presents technical details about the lightweight node authentication system through passive radio analysis, including the fine-grained CFO extraction, spatial-temporal link signature measurement, and combination of CFO and link signatures.

5.1 CFO Extraction

The first signature for node authentication is CFO presented when downconverting is executed at the receiver, since crystal oscillators in different LoRa nodes produce different carrier frequencies. However, it is challenging to extract fine-grained CFOs in actual environments. Naturally, there exist three factors affecting the carrier frequency of crystal oscillators, including the initial error, the noise effects, the temperature drift, and the aging drift. In this subsection, we leverage CFOs caused by the initial error as the node signature. Subsequently, we show how to accommodate for the drifts induced by the temperature and ageing.

5.1.1 ***CFO Compensation Algorithm.*** In the CFO compensation algorithm, we exploit the preamble part of LoRa packets to achieve CFO estimation. This is because we can directly read-off the locations of peaks as CFOs when performing FFT on the multiplication result of received upchirps of the preamble part with the standard downchirp. Specifically, in the ideal case, the bin index of the FFT peak is zero. However, it actually shifts to one nearby bin index due to CFO Δf. For example, assuming one low-cost LoRa node conveys signals at the actual frequency f_c, which is offset by Δf from the nominal one f_0. After down-converting to the baseband, the time-domain signal can be represented as $h \star e^{j2\pi\Delta f t}C$, where h and C represent the wireless channel response and standard upchirp in the preamble part, respectively. After de-chirping by multiplying with the standard downchirp C^{-1} and FFT execution, we can observe an FFT peak at the frequency offset Δf.

However, this coarse-grained CFO estimation which only consists of the integral FFT bin index restricts the distinguishing accuracy of SLoRa, especially for large-scale deployed LoRa nodes. It should be noted that CFO is a physical phenomenon such that data bits are loaded on integer bins in the Fourier transform, while CFOs need not. Actually, it need not be an integer multiple of an FFT bin, which implies that the above coarse-grained CFO estimation loses some information pertaining to the frequency offset which is a fraction of the FFT bin. Consequently, the distinguishing accuracy can be dramatically improved if we can obtain the fractional part of CFOs.

To achieve fine-grained CFO estimation including both the integral and fractional parts, we design a novel CFO compensation algorithm. Detailed steps are illustrated as below.

In wireless communications, the received signal $y(t)$ is the convolution result of the channel response $h(t)$ and conveyed signal $s(t)$, which is described as

$$y(t) = h(t) \otimes s(t), \tag{1}$$

where $\otimes$ represents the convolution operation. In LoRa communications, we can use the standard upchirp C in the preamble part to represent $s(t)$, which can be defined by

$$y(t) = h(t) \otimes e^{j2\pi f_c t} C, \tag{2}$$

where f_c denotes the actual carrier frequency. In the demodulation process, the LoRa receiver first down-converts the received signals to baseband coupled with CFO, and then de-chirped by multiplying the received upchirp with the standard downchirp C^{-1}. The de-chirped signal can be represented as

$$y(t)C^{-1} = h(t) \otimes e^{j2\pi\Delta f t}. \tag{3}$$

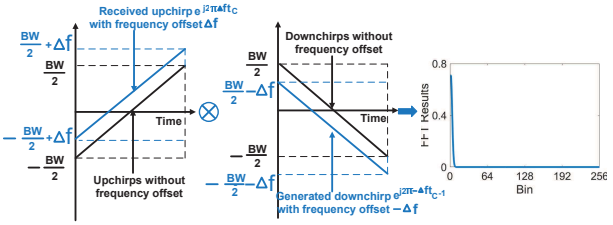


Figure 3: The process of extracting fine-grained CFOs in LoRa communications.

As demonstrated in Equation 3, the frequency domain representation of the de-chirped signal (obtained via FFT), denoted as $F(yC^{-1})$, results in one FFT peak corresponding to the CFO Δf. As mentioned above, the observed CFO is at the integer boundaries of one FFT bin, which is denoted as $\overline{\Delta} f$. Actually, the more fine-grained CFO Δf differs from the observed one, yet close to the observed one.

We first introduce a key observation behind the CFO compensation algorithm. As shown in Fig. 3, assuming we produce a standard downchirp C^{-1} with the frequency offset of $-\Delta f$ to multiply with the received upchirp $e^{j2\pi\Delta f t}C$, we can obtain the de-chirped signal $e^{j2\pi \mathbf{0} t}$, and observe an FFT peak at bin index 0.

According to this observation, let us revisit the de-chirping procedure, which employs a standard downchirp C^{-1} without frequency offsets to multiply with the received upchirps. Like these upchirps coupled with frequency offsets, we can artificially generate a series of downchirps with different frequency offsets at the LoRa receiver, which are denoted as $C^{-1}e^{j2\pi(-\overline{\Delta}f-nF)t}$, $C^{-1}e^{j2\pi(-\overline{\Delta}f-(n-1)F)t}$,..., $C^{-1}e^{j2\pi-\overline{\Delta}ft}$,..., $C^{-1}e^{j2\pi(-\overline{\Delta}f+nF)t}$. Here, F indicates the frequency resolution in CFO estimation and n denotes the CFO estimation range. Obviously, these frequency offsets are set close to the observed CFO $\overline{\Delta} f$ in order to achieve computation-efficient search since $\overline{\Delta} f$ can be regarded as the integral part of the actual CFO. Then, we only need to estimate the fractional part, which considerably reduces the search space.

Then, we multiply the received upchirp with generated downchirps with different frequency offsets one by one. During this process, the bin index corresponding to the FFT peak should be or close to zero when the downchirp with frequency offset $-\Delta f$ appropriately compensates for the frequency offset Δf in the received upchirp. Put differently, when one artificially generated downchirp with the frequency offset of $-\Delta f$ can eliminate the CFO influence in the received upchirp, the bin index at the FFT peak should be at or close to zero. Therefore, the problem with respect to fine-grained CFO estimation can be expressed as

$$\Delta f = -\arg \min_{(f \in (\overline{\Delta}f - nF, -\overline{\Delta}f + nF))} Index(F(yC^{-1}e^{j2\pi f t})), \tag{4}$$

where $Index$ represents the function which returns the bin index corresponding to the FFT peak, and $F()$ denotes the FFT operation. Naturally, we can perform FFT with a higher frequency resolution, in order to obtain more fine-grained CFO estimation in function $Index$. In the FFT operation, the frequency resolution is equal to $\frac{f_s}{N}$, where f_s and N respectively denote the sampling rate and FFT size. Therefore, we perform a Fourier transform over a wider window (10× larger) by zero-padding the signal to enlarge N.

5.1.2 ***Noise Effect Mitigation.*** Unfortunately, the inevitable noise has a more severe effect on CFO estimation with a higher frequency resolution. In actual implementations, we observe that the estimated CFO fluctuates slightly according to the intuitive CFO compensation strategy. The reason is that the uncertain nature of noise randomly shifts upchirps up or down within a small frequency offset range. Consequently, it is infeasible to extract stable and fine-grained CFOs simultaneously. The unstable CFO estimation will incur erroneous node authentication and then restrict the distinguishing accuracy of SLoRa. To deal with this challenge, we attempt to investigate the noise effect on the CFO estimation, and then build the relationship between the noise effect and fluctuated CFOs. According to this relationship, SLoRa can identify the fine-grained CFO in the presence of noise.

Notice that upchirps in frequency domain are formed according to the CSS modulation, implying that the frequency increment between two adjacent samples remains constant. Therefore, we can employ linear lines with constant slopes to describe the relationship between these discrete samples within upchirps. As shown in Fig. 4, we set the sample sequence as the X axis and corresponding phase values as the Y axis. However, the received upchirps are distorted after propagating over the wireless channels, yet their basic shapes are maintained. To deal with the inevitable distortion, we adopt the linear fitting method to derive the line expression for the received upchirps of the preamble part. We can observe that these linear lines fit well with upchirps if without noise influence. Both the slope gradient and truncation rate of linear lines determine the intersection with Y axis, which represents the initial frequency of standard upchirps. Consequently, the slope gradient and truncation rate can be leveraged to reflect the frequency offset, since the initial frequency of standard upchirps is ideally zero, but actually shifted by the CFO and noise.

Due to the noise, both the slope gradient and truncation rate of linear lines undergo variations, as demonstrated in Fig. 5. On the other hand, during the linear fitting process, the noise effect can be averaged, which then restrains the uncertainty of noise and amplifies the effect of CFO. Consequently, we exploit the variations related to the slope gradient and truncation rate to indicate the noise influence on CFO estimation.

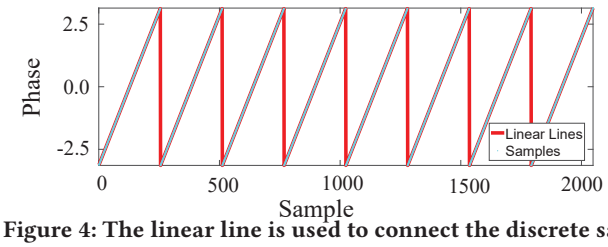


Figure 4: The linear line is used to connect the discrete samples within a standard upchirp.

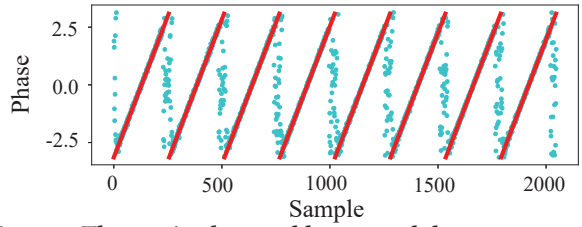


Figure 5: The received preamble part and the same preamble part based on the linear fitting.

Experimental results with regard to the slope gradient and truncation rate are shown in Fig. 6 when setting the distance between the transmitter and receiver as 20 meters and frequency resolution F as 0.1 times of FFT transform bin. We can observe that the fractional part of Δf slightly fluctuates from -0.1 to 0.3 bins, and meanwhile the pair of slope gradient and truncation rate demonstrates a distinguishable pattern corresponding to different CFOs. More specifically, the pair of slope gradient and truncation rate gradually shifts to right coupled with the CFO increase. Therefore, we can identify the slight CFO variation induced by noise through capturing the relationship between CFOs and pairs of slope gradient and truncation rate. For example, we can obtain the proper fractional part of Δf corresponding to different pairs of slope gradient and truncation rate under different noise conditions (e.g., border lines 1, 2, and 3 in Fig. 6).

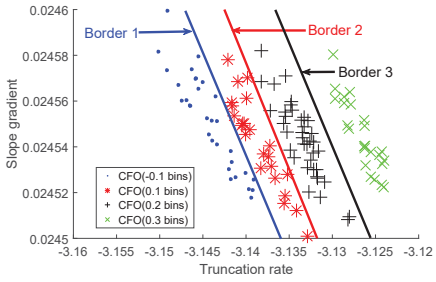


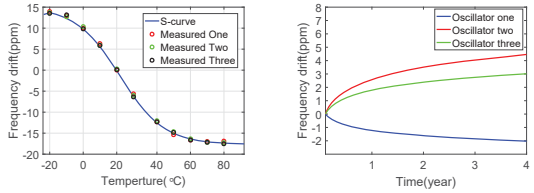
Figure 6: The experimental results with respect to the slope gradient and truncation rate.

To achieve this aim, we employ the Support Vector Machine (SVM) to achieve the classification. First, the training process is performed for the SVM module. It mainly involves calculation of a special matrix ω_A based on the collected LoRa signals from legitimate node A. If the CFO derived by the SVM module (i.e., using $\omega_A * S - b$) which is fed by the pair of a received frame's slope gradient and truncation rate equals to the directly measured CFO, then SLoRa regards the received signal is conveyed from the legitimate node A. Otherwise, it is transmitted from an attacker. In general, the SVM model consists of multiple groups of matrices like ω_A since LoRa networks conventionally include multiple nodes. In order to reduce the computation overhead, we first coarsely estimate the CFO of the received frame, and only choose legitimate nodes whose CFOs are closed to the estimated one to compare with. Consequently, based on the designed scheme, SLoRa can achieve fine-grained CFO estimation even in the presence of noise. Then, SLoRa can provide node authentication for large-scale LoRa networks. When the frequency resolution is set as 0.1 times of FFT transform bin (e.g., about 100 Hz frequency resolution when SF is 8 and BW is 250 KHz), SLoRa can distinguish more than 400 LoRa nodes when the frequency offset tolerance is just 20 KHz, which is a huge step forward for node authentication compared to traditional wireless networks (e.g., the largest number of identified nodes is 138 reported in 802.11 networks [6]). Combined with the link signature, SLoRa can provide a satisfactory performance for node authentication in large-scale LoRa networks.

5.1.3 ***Drift elimination.*** However, any crystal oscillator, even centered at the right frequency at ambient temperature, will exhibit a temperature dependency, also called 'drift'. This drift may affect the CFO estimation accuracy since fine-grained CFO estimation is required in SLoRa. Then, we attempt to quantify the frequency drift caused by temperature. As shown in Fig. 7(a), most crystal oscillators in LoRa nodes follow an S-shape curve in terms of the temperature and frequency drift [16]. The unit *ppm* in the y-axis is utilized to quantify the frequency drift ϵ, which can be defined by

$$\epsilon[ppm] = \frac{ActualFrequency - TheoreticalFrequency}{TheoreticalFrequency} \times 10^6. \quad (5)$$

The inflexion point of this curve stands relatively close to the ambient temperature, which is equal to $25°$. Upper and lower turnover points represent a distance where the frequency response over temperature is almost linear. Consequently, we can compensate for the frequency drift by establishing the linear relationship between the frequency drift and temperature. In convention, the temperature in a specific city has a narrow range, which could allow for more precise compensation under specific temperature. However, there may exist different linear relationships between the frequency drift and temperature due to the manufacturing difference. According to the experimental results of [14] and empirical study in this paper, we find that the linear relationship only undergoes slight variations for different LoRa nodes. The little frequency drift difference caused by relationship variations has a negligible impact on SLoRa's performance since it can endure CFO estimation with small variations, which will be illustrated later.



(a) Temperature drift (b) Aging drift

Figure 7: The carrier frequency drift caused by temperature and aging.

In addition to the temperature factor, there also exists the carrier frequency drift induced by aging. This is because crystals embedded in LoRa nodes are electromechanical devices, and as such they are subject to aging. Unfortunately, there is no simple rule to predict the aging of a crystal, or even that of a batch of crystals. Figure 7(b) demonstrates the frequency drifts of three crystal oscillators embedded within three different LoRa nodes caused by aging, which implies that this behavior over time is not monotonous. Therefore, it is almost impossible to compensate for the aging drift theoretically.

Meanwhile, we can also observe that the frequency drift induced by aging experiences a slow variation. Thanks to the low aging rate, we can adopt an update strategy to accommodate for the slow frequency drift. Details about the update scheme will be illustrated combined with the temporal link signature in Subsection 5.3.

5.2 Link Signature Estimation

This subsection presents the definition of the spatial-temporal link signature and how to extract fine-grained link signatures at the gateway side. The spatial-temporal link signature relies on the fact that the link variation within a period when the transmitter locates at the same position is large than the link difference when the transmitter locates at different positions.

Figure 8 depicts a communication scenario in indoor environments, where the gateway is located at position P1 and a legitimate LoRa node is at position P2. The link between the gateway and node is composed of multiple individual paths, including $L1$, $L2$, and $L3$. Assuming an adversary at position $P3$ can detect the key of the wireless link established between the gateway and legitimate node, it then impersonates the legitimate node and launch DoS or spoofing attacks to the gateway.

To defend against the attack, we observe that multiple paths between the gateway and adversary is composed of links $L4$, $L5$, and $L6$, which completely vary from the link between the gateway and legitimate node. Consequently, we can leverage this distinction to detect the attack.

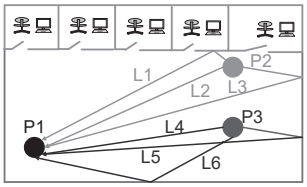


Figure 8: An example of LoRa communication scenario in indoor environments.

To defend against attacks, we rely on the observation that multiple paths between the gateway and adversary completely vary from the link between the gateway and legitimate node. Consequently, we can use this distinction to detect attacks.

In multipath scenarios, the lengths of multiple paths differ from each other, which result in different transmission times. Meanwhile, different copies of source signal undergo different attenuations and interactions with the surrounding environments. Hence, these copies of signal arrive at the gateway with different time delays, phases, and amplitudes. In other words, the received signal can be regarded as the linear combination of these signal copies. We define the relationship of this linear combination as the temporal link signature, which can also be regarded as a linear filter, i.e., the channel impulse response. The relationship between the link signature and linear filter will be verified later. Compared to the conventional multipath effects highly relying on the transmitted signal strength, the temporal link signature only focuses on the relative relationship between the arrival time and attenuation of these signal copies, and then has a more stable performance. The temporal link signature between node i and gateway can be defined by

$$h_i(\tau) = \sum_{l=1}^{L} a_l e^{j\phi_l} \delta(\tau - \tau_l), \tag{6}$$

where a_l and ϕ_l are the amplitude and phase of the lth link, and τ_l represents its time delay. L denotes the total number of multiple paths, and $\delta(\tau)$ is the Dirac delta function.

In convention, receivers measure the received signal $y(t)$ and perform a de-convolution combined with $s(t)$ to deduce $h_i(t)$. However, the complicated de-convolution produces orders of magnitude of computation and complexity, and introduces measurement inaccuracy simultaneously. In order to simplify this process, we show how to achieve accurate link signature measurement without de-convolution. Substituting Equation 6 into Equation 3, we then rewrite Equation 3 as

$$y(t)C^{-1} = (\sum_{l=1}^{L} a_l e^{j\phi_l} \delta(t - \tau_l)) \star (e^{j2\pi\Delta f t}). \tag{7}$$

According to the convolution theory, Equation 7 can be further transformed into

$$y(t)C^{-1} = (\sum_{l=1}^{L} a_l e^{j\phi_l} \times e^{j2\pi(\Delta f + \frac{\tau_l}{2^{SF}} \times f_s)t}). \tag{8}$$

Obviously, there exist multiple peaks at different bins (e.g., $\Delta f + \frac{\tau_l}{2^{SF}} \times f_s$) with different amplitudes $a_l e^{j\phi_l}$ in one upchirp, when performing FFT on the dechirped signals $F(y(t)C^{-1})$. Meanwhile, fine-grained CFO estimation in Subsection 5.1 (i.e., Δf) contributes to sensitive link signatures, since different nodes bring different CFOs at the receiver side. It should be emphasized that there may not exist multiple distinguishable FFT peaks as expected. The reason is that these FFT peaks may interfere with each other (e.g., stronger peaks overwhelm weaker peaks) due to the close arrival times of different signal copies, which then constructs the unique link signature. Consequently, the link signature formed by these FFT peaks varies corresponding to different nodes which locate at different places.

Next, we demonstrate the relationship between the channel impulse response $h(t)$ and proposed link signature. We multiply the standard downchirp C^{-1} on both sides of Equation 1 and then perform FFT, which can be expressed as

$$F(y(t)C^{-1}) = F(C^{-1}s(t) \star h(t)), \tag{9}$$

where $s(t)$ can be represented by the standard upchirp C in the preamble part. Therefore, Equation 9 can be rewritten as

$$F(y(t)C^{-1}) = F(h(t)). \tag{10}$$

Combining Equations 8 and 10, it can be concluded that the obtained link signature is actually the Fourier transform of the channel impulse response $h(t)$, which is the representation of the linear filter between the node and gateway. Therefore, we can obtain the link signature (i.e., the channel impulse response in frequency domain) simply by leveraging the available demodulation module, which lays a good foundation for a lightweight system aiming at node authentication and security improvement. The only difference compared to the conventional LoRa demodulation is that we perform FFT with a larger size of $2*2^{SF}$, in order to achieve more detailed observation of link signatures and maintain the decoding accuracy simultaneously.

According to the above theoretical model, we have collected certain link signatures extracted from the received signals when one LoRa node respectively locates at three different positions. Since link signatures induced by multiple signal copies with different delays and attenuations manifest themselves consistently across multiple frames from the same transmitter, yet distortions to link signatures caused by noise own a more random nature, which follows the Gaussian distribution $W \sim N(0, \delta^2)$. Consequently, we adopt a sliding window to average these link signatures, which thus can amplify the features of link signatures while lowering down the ambient noise effect.

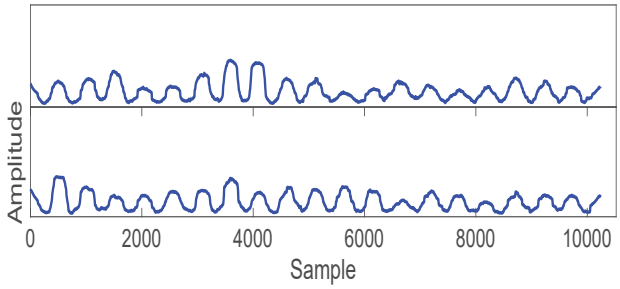


Figure 9: The link signature measured at position D.

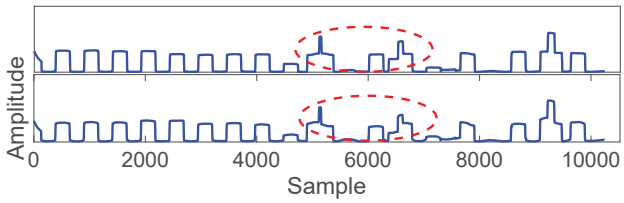


Figure 10: The link signature measured at position C.

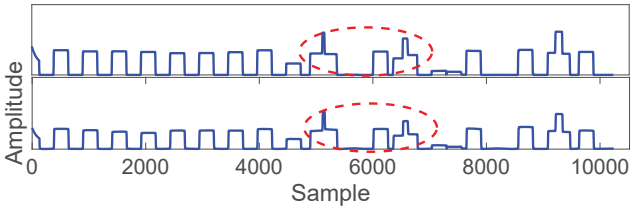


Figure 11: The link signature measured at position B.

We place the LoRa node at three different positions, for example, position B, C, and D, respectively. Figure 9 describes the link signatures when the LoRa node is at position D, relatively far away from the gateway. Figure 10 shows the obtained link signatures at position C, which is closer to the gateway compared to position D. From these two figures, we can observe that link signatures vary dramatically at different locations. Yet, they have a high similarity at the same position, despite of small variations in amplitude.

We have also investigated the link signatures when the node locates at position B, which is a little closer to the gateway compared to position C as shown in Fig. 11. The link signatures from these two close positions have a relatively high degree of similarity. However, if we take a detailed observation, we find that link signatures experience more variations at position C compared to position B in terms of the envelope of link signatures, which is shown as the red dotted line in Fig. 11 and Fig. 10. In order to investigate the environmental variations on the link signature, we have intentionally set two or three person walked around in the measurement environment. We can find that small environmental changes have little impact on the link signature.

Before introducing the specific algorithm to distinguish the link signatures at different locations, SLoRa should fetch representative features from the link signatures. As mentioned above, multiple copies of source signals arrive at the gateway with different amplitudes, phases, and delays, which either constructively or destructively interfere with each other in the form of amplitude. Then, FFT peaks corresponding to different delays can construct the unique signature. Therefore, we select the features with respect to the amplitude envelop to represent the link signatures.

Intuitively, SLoRa can directly extract the received samples for comparison, which is distorted by the ambient noise especially for long-range communications. Hence, only the envelope remains insufficient for constructing the reliable link signature. In SLoRa, we also extract three additional features, including maximum, minimum, and variance of FFT results to enrich the link signatures. More specifically, SLoRa extracts these features by computing the envelope, variance, maximum, and minimum within every standard upchirp since one single upchirp is utilized as an unit upon which FFT is performed. Similar with the CFO estimation, we can also employ the SVM model to achieve the link signature based authentication in the presence of noise. In the experimental part, we collect 100 link signature items to train the SVM model when LoRa nodes locate at a fixed position. Finally, it should be noticed that SLoRa only employs the preamble part which consists of certain standard upchirps for the link signature estimation, regardless of the payload length.

5.3 Combination of CFO and Link Signature

Two dimensional features can provide strict authentication for unauthenticated nodes and then prevent active attacks, yet simultaneously restricting the detection accuracy for legitimate nodes. To balance these two metrics, we select n LoRa nodes (e.g., 2, 3, or other numbers depending on the specific conditions) according to the comparison similarity in SLoRa, rather than only one LoRa node obtained from the SVM model. For example, SLoRa selects 3 LoRa nodes according to the CFO extraction scheme, such as N1, N2, and N3 in a decreasing similarity order. Meanwhile, it also outputs 3 another LoRa nodes (e.g., N2, N3, and N4) based on the temporal link signature. Combing these two node series according

to two different detection schemes, SLoRa considers that the signal is conveyed from LoRa node N2. If N2 is within the set of legitimate LoRa nodes, then the received signal comes from a legitimate node. Otherwise, SLoRa regards the signal is delivered from an attacker, which will be discarded.

However, as mentioned above, both CFOs and link signatures experience variations caused by small drifts over time. To overcome this challenge, we propose an update strategy to accommodate for these changes. Similar with the slow frequency drift induced by the low ageing rate, the link signature remains almost the same even small variations occur in surrounding environments during the relatively short period. To adjust for large variations within a long period, we set a history of link signatures denoted as L_i between the gateway and one node N_i used for detection, which includes N measured link signatures. Like the collected history with regard to the link signature, SLoRa also stores a collected history C_i for CFO, which consists of N recently measured CFOs. To illustrate, the initial measured CFO based on the signal conveyed from node N_i is F_i, and SLoRa obtains two node sets according to the comparison similarity, respectively as C_i, C_{i+1}, C_{i-1} and L_i, L_m, L_n. However, coupled with ageing, the carrier frequency in the crystal oscillator undergoes certain changes. Assuming the estimated CFO at the gateway side will shift to the next frequency value F_{i+1}, corresponding to LoRa node N_{i+1}. In this case, the node set becomes C_{i+1}, C_i, C_{i-1} according to the CFO estimation and the other node set remains the same, which is equal to L_i, L_m, L_n. Combining these two node set, SLoRa can still consider that the signal is transmitted from node N_i. For constant memory usage, the oldest measurement in the N CFOs is then discarded and the newest measured CFO is added. Similar with the CFO update, we also perform the similar operation for the update of link signatures.

6 NODE AUTHENTICATION

We integrate SLoRa with the MAC layer security protocol since it is an security design enhancement in physical layer over existing LoRa communications. Then, we show how SLoRa enables node authentication in physical layer and defend against active attacks. Compared to conventional encryption algorithms, SLoRa only differs in that it leverages two physical-layer features (e.g., CFO and link signature) to safeguard LoRa communications. In what follows, we discuss cases where SLoRa achieves node authentication and prevents deauthentication deadlock attack, jamming and replay attack, and man-in-the-middle attack.

SLoRa leverages two fine-grained physical layer features (e.g., CFO and multipath profiles) to safeguard LoRa communications. It can also act as a secondary security perimeter for the already-implemented cryptographic mechanism in MAC layer. Compared to individual CFO or multipath profiles based schemes, SLoRa can provide two-dimension security for LoRa networks. For example, SLoRa can detect the attacker even it demonstrates the same CFO feature with one of legitimate LoRa nodes, since the attacker does not locate at the same position with the legitimate node. On the other hand, even the attacker locates at the same location with legitimate nodes without being discovered, it can easily be detected by SLoRa due to the different CFO feature. Next we will show how to enable device authentication and defend against two conventional attacks in LoRa networks–node forgery and malicious congestion.

Deauthentication Deadlock Attack. There exist kinds of active attacks. A typical DoS attack takes the vulnerability before a secure LoRa link has been established. We consider a specific scenario that an authentication handshake is executed. During the process, an attacker can inject an unauthorized deauthentication notification after receiving an acknowledgement (ACK) from the gateway. Accordingly, the protocol deadlock occurs. To detect the deauthentication attack, SLoRa adds two additional feature extraction process (i.e., CFO and link signatures) at the gateway side, with slight protocol change. Upon receiving the deauthentication message, SLoRa extracts the CFO and link signatures as illustrated in Sections 5 and compare with legitimate nodes. If the SVM model identifies the deauthentication command is conveyed from an attacker, the gateway then discards this frame in upper layer.

Jamming and Replay Attack. An attacker equipped with multiple antennas can launch a jamming and replay attack. The attacker can jam the association packets reception with one directional antenna and records the packet with another antenna. The received signal during jamming are the signal superposition of the legitimate user and attacker, resulting in different CFOs and link signatures. It can be easily detected by SLoRa at the gateway. The attacker then replays the recorded packets to the legitimate device. Although the recorded message is same with the legitimate node, the message conveyed by the attacker will demonstrate variations in terms of CFO and link signatures compared to the legitimate node due to the hardware imperfections and location differences. Therefore, the gateway can detect that the replay message is from the attacker and drops these frames in upper layers. Similarly, SLoRa can prevent other active attacks such as authentication deadlock attack in the same way.

Man-in-the-middle Attack. An attacker can also receive the signal from a legitimate LoRa node. Then, it calculates the CFO of the legitimate node with respect to itself. Consequently, the attacker can impersonate the signal of the legitimate node by compensating the CFO, which then is received by the gateway. In convention, this attack is called the man-in-the-middle attack. However, SLoRa can detect this kind of attack since SLoRa combines both CFOs and link signatures to achieve node authentication. This is because that although the attacker can mimic the CFO of the legitimate node by adjusting the carrier frequency, it is non-trivial to impersonate the unique link signature between the legitimate node and gateway.

7 EVALUATION

We first introduce the implementation of our prototype, followed by the detailed performance evaluation of SLoRa.

7.1 Implementation

We implement SLoRa on a testbed of software radio base stations and clients built using commodity components, i.e., the commercial LoRa node. The base station mainly consists of USRP N210 software radios and the WBX daughterboards which operate at the 868 MHz bands. We leverage the UHD+GnuRadio library and then propose our node authentication scheme, the algorithms of which are written in C++ to deal with the received signals and

intermediate results. There is only one antenna embedded in the base station and the clients are the microchip RN2483 node, both of which specify their bandwidths as 250 KHz.

We carry out experiments in our campus, including indoor and outdoor environments, in order to demonstrate the widespread application of SLoRa. We employ three extra off-the-shelf LoRa nodes at 10 different locations to act as the attacker. In indoor scenarios, we investigate its performance covering both line-of-sight (LoS) and non-line-of-sight (NLoS) cases.

Baseline: We compare SLoRa with two baselines: **LoRa+CFO:** One is the scheme only using fine-grained CFOs, since CFO has been utilized as the signature for node authentication in 802.11 networks [6]. **LoRa+Link signature:** the other one is the scheme only leveraging the link signature since link signatures have been widely used as another signature for security improvement in wireless networks [18, 19, 41].

Metrics: Similar with [20], we also utilize two metrics to evaluate the overall performance of SLoRa. **True Positive Ratio:** True positive ratio, referred to as **TPR** in this paper, is defined as the ratio of the received signals from legitimate nodes to be correctly detected by SLoRa in all received signals. **False Positive Ratio:** False positive ratio named **FPR** denotes the ratio of the number of received signals from attackers to be wrongly detected as the legitimate node by SLoRa in all received signals.

7.2 Experiments

We carry out experiments in both indoor and outdoor environments since LoRa can be employed in indoor environments such as smart home, besides outdoor scenarios like smart agriculture.

As demonstrated in Fig. 13, we fix the LoRa receiver at position L1, and increase the distance between the receiver and transmitter by moving the transmitter to position L2, L3, L4, L5, and L6, respectively. The attacker is located at L7, L8,..., L16, respectively.

As shown in Fig. 12, experiments are conducted in the corridor of an office building with different distances set between the transmitter and receiver.

(a) Receiver (b) Transmitter

Figure 12: The experimental setup.

LOS communications scenarios indoors. As a critical factor in SLoRa, we first investigate how much fine-grained frequency resolution can be achieved to demonstrate an accurate CFO estimation? Experimental results are shown in Fig. 14 in the case of *SF* equaling to 8. Figure 14(a) describes the TPR and FPR performance when setting the transmitting power as 15 dbm and the distance between the transmitter and receiver as 5 meters. In this figure, 0.5 indicates that the frequency resolution is set as 0.5 times of FFT transform bin, and smaller number implies more fine-grained

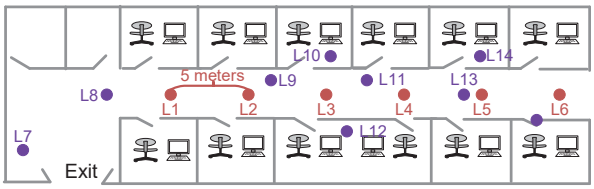


Figure 13: The experimental scenario where the LoRa transmitter locates at L1, and receiver locates at L2, L3, L4, L5, and L6, respectively.

frequency resolution. We can observe that TPR decreases with the increase of frequency resolution, while FPR increases. The reason is that more fine-grained frequency resolution amplifies the noise effect on CFO estimation although contributing to more granular estimated CFOs.

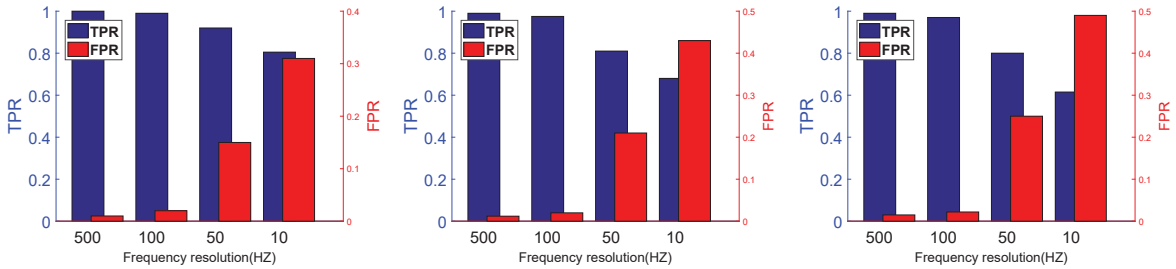
Experimental results at around 0°C are shown in Fig. 14(b) when setting the distance between transmitter and receiver as 10 meters. We can observe the similar variation trend of TPR and FPR with the case of distance equaling to 5 meters. Meanwhile, TPR in this case is lower than the case of 5 meters due to the distance increase. This is because that longer propagation distance results in higher attenuation and lower received signal strength.

We have then explored SLoRa's performance using different transmission powers. Figure 14(c) describes the experimental results when setting the transmission power as 3 dbm and distance as 5 meters. Compared to the power of 15 dbm, SLoRa demonstrates a worse performance for both TPR and FPR due to the lower transmission power.

According to above experimental results, we can observe that TPR dramatically declines to below 95% and FPR increases when the frequency resolution is higher than 0.1 times of FFT bin. From another perspective, if we set a coarse-grained frequency resolution– 0.5, SLoRa can achieve the highest TPR and lowest FPR, yet the number of LoRa nodes distinguished by SLoRa will considerably decline. Consequently, we set the frequency resolution as 0.1 times of FFT transform bin, and then TPR can exceed 98% and FPR is lower than 2%.

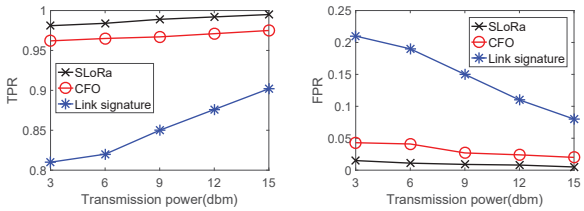
Next, we investigate both TPR and FPR performances combined with the link signature under different transmission powers and distances. First, we set the distance as 10 meters using different transmission powers, respectively as 3, 6, 9, 12, and 15 dbm. Experimental results are shown in Fig. 15(a), from which we find that TPR increases with the transmission power. Even when the transmission power is set as 3 dbm, TPR in SLoRa can still maintain a high level up to 98%. Meanwhile, Fig. 15(b) describes the FPR performance, which stays at a low level. Compared to schemes based on individual CFO and link signature, SLoRa demonstrates a superior performance in terms of both TPR and FPR. Furthermore, SLoRa and individual CFO based scheme can achieve a higher TPR than the link signature. This is because the link signature is more susceptible to noise and other interferences, especially in dynamic environments.

SLoRa is also evaluated with different distances between transmitter and receiver, ranging from 5 to 25 meters with a step of 5 meters. As shown in Fig. 16(a), TPR based on these three different schemes slightly declines with the distance increase. The reason is that longer transmission distance introduces more noise influence



(a) Power=15dbm, distance=5m (b) Power=15dbm, distance=10m (c) Power=15dbm, distance=10m

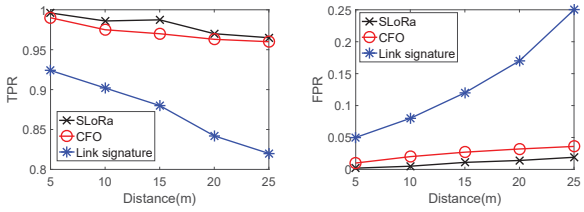
Figure 14: The experimental results in terms of TPR and FPR with different frequency resolutions when setting different transmitting power, and different distances between the transmitter and receiver.



(a) TPR with distance=10m (b) FPR with distance=10m

Figure 15: The experimental results in terms of both TPR and FPR with different transmission powers.

and reduces the received signal strength, which then reduces the detection accuracy. However, SLoRa still achieves a high detection accuracy up to 97% with various distances, and FPR lower than 2% can be achieved, as demonstrated in Fig. 16(b). With respect to both TPR and FPR, SLoRa performs better than individual CFO and link signature under different distances. Finally, we find that the most common scenario incurring FPR is that the CFO of the attacker is close to one legitimate node, and locates nearby this legitimate node. However, this scenario rarely occurs, and even if presented, the attacker can be easily detected.



(a) TPR with power=9dbm (b) FPR with power=9dbm

Figure 16: The experimental results in terms of both TPR and FPR with different distances.

NLOS communications scenarios indoors. Besides LOS communication scenarios, we have also investigated SLoRa's performance in NLOS scenarios. Figures 17(a) and (b) illustrate the experimental results with different transmission powers in NLOS scenarios. Obviously, we can observe that TPR increases with transmission power, while FPR decreases. Figures 17(c) and (d) describe the FPR performance when the distance increases from 3 to 15 meters, which are similar with the case of LOS scenarios. Compared to LOS, TPR based on these three schemes becomes slightly lower in NLOS scenes. The reason is that the obstacle shields the LOS path and lowers down the received signal strength. More specifically, TPR based on individual link signature in this case is higher than the LOS case. This is because the NLOS scenarios can construct more distinguishable link signatures, which can be utilized as the unique feature of nodes.

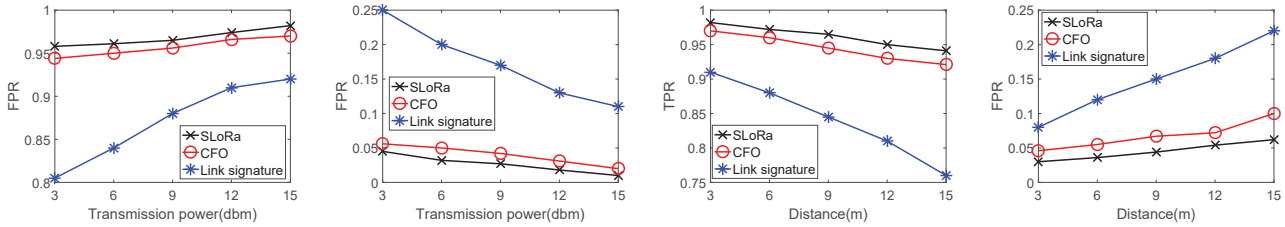
LOS communications scenarios outdoors. We have also conducted experiments in outdoor scenarios. The LoRa gateway locates nearby an open window at the third floor of an office building and node is placed on the outside ground.

Similarly, we have first explored the frequency resolution in outdoor scenarios. It should be noted that one LoRa node can reach a transmission distance up to 400 meters at a relatively high quality when setting *SF* as 8, due to the tall buildings, trees, and hardware limitations of the USRP's receive chain [21]. Consequently, we explore the appropriate frequency resolution in the worst case–the distance is set as 400 meters. Figure 18(a) verifies that we can set the frequency resolution as 0.3. The reason is that this frequency resolution can provide a relatively fine-grained CFO estimation while maintaining a high TPR higher than 91%.

Next, we investigate the TPR and FPR performances with the distance increasing from 100 to 400 meters. Experimental results are demonstrated in Fig. 18(b), from which we can observe that TPR gradually decreases with the distance.

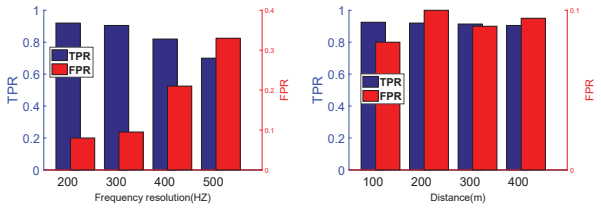
We compare the TPR results based on above three schemes in outdoor scenarios, as shown in Fig. 19(a). It can be seen that SLoRa demonstrates a superior performance of more than 91% for TPR compared to individual CFO and link signature based schemes. However, unlike the indoor scenarios, link signature based scheme outperforms the CFO based scheme in outdoor scenarios. The reason is that long range communications result in weak received LoRa signals, which then challenges the fine-grained CFO estimation while constructing distinguishable link signatures. Compared to the indoor case, SLoRa demonstrates a performance degradation due to more severe attenuation in outdoor scenarios.

Above experiments are conducted when setting *SF* as 8. Next, we have investigated the TPR performance of SLoRa when setting *SF* as 10. From Fig. 19(b), we can observe that TPR when setting *SF* as 10 is higher than the case of *SF* equaling to 8. The reason is that LoRa can expand its extended channel through adjusting SF, which in turn contributes to both processing gain and anti-jamming ability improvement. With SF becoming larger, the processing gain and anti-jamming ability for LoRa signals increase.



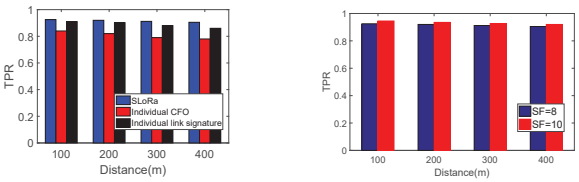
(a) Distance=9m (b) Distance=9m (c) Power=9dbm (d) Power=9dbm

Figure 17: The experimental results with different distances and transmission powers in NLOS scenarios.



(a) Distance=400m (b) Power=15bdm

Figure 18: The detection accuracy with different frequency resolutions when setting the distance between the transmitter and receiver as 400 meters, and the detection accuracy when setting different distances between the transmitter and receiver.



(a) (b)

Figure 19: The detection accuracy when setting different distances, and the detection accuracy when setting different SFs with different distances.

Time consumption. Finally, we simply compare the delay induced by SLoRa with different *SFs*. The delay time is defined as the time consumption from the instant of detecting the preamble to the moment of node identification decision. We find that the detection when setting *SF* as 8 consumes less time (e.g., around 50ms) than the case of *SF* equaling to 10, the delay time of which is around 180ms. Consequently, we can conclude that SLoRa is a lightweight system for node authentication and security enhancement.

8 DISCUSSION AND LIMITATIONS

In this paper, we have proposed a lightweight system to achieve physical-layer node authentication and improve the security. Unlike the attacker can crack encryption keys, these two features are non-trivial to obtain and even if they can be gained, attackers can hardly manipulate themselves as the same (e.g., satisfying the CFO and link signature features simultaneously) with the legitimate LoRa node. Therefore, we believe SLoRa is a robust node authentication system.

As demonstrated in the experimental results, the accuracy based on SLoRa (i.e., the combination of CFO and link signature) is around 2% improvement than the scheme only based on CFO, which implies that the link signature adds a little value in the performance of SLoRa. However, in the scenario that the attacker mimics the victim's CFO, the link signature can play an important role in defending against this kind of attack since the CFO difference between the attacker and victim node has been eliminated by manipulation. In this case, SLoRa can still prevent the attack because it is non-trivial for the attacker to eliminate the link signature difference between itself and victim node in wide coverage areas. Therefore, we believe SLoRa is a robust node authentication system.

However, when setting long distances between the transmitter and receiver, heavy attenuation occurs and thus the noise and other interference have a serious impact on fine-grained CFO estimation. SLoRa does not demonstrate a satisfactory performance in outdoor scenarios. Another limitation of SLoRa is that both LoRa gateways and nodes should be at relatively fixed positions in order to construct reliable link signatures, which restricts SLoRa from being applied to mobile scenarios. Therefore, SLoRa can not support LoRa node authentication in mobile state. Finally, SLoRa can only defend against active attacks and makes no exploration of protecting against passive attacks such as eavesdropping attacks and information leakage. The challenge of dealing with passive attacks remains an open problem.

9 CONCLUSION

This paper presents SLoRa to achieve node authentication and improve security of LoRa communications leveraging CFOs and link signatures. We design two novel algorithms by making full use of LoRa's demodulation mechanism to extract fine-grained CFOs and link signatures, which can act as unique signatures for individual LoRa node. Extensive experiments conducted in both indoor and outdoor environments to demonstrate that SLoRa is a reliable system for node authentication.

10 ACKNOWLEDGEMENTS

We thank the anonymous shepherd and reviewers for their helpful feedback in improving the paper. This work was supported in part by the National Natural Science Foundation of China 61972253, U190820096, 7191101302, 61672349, 61802007.

REFERENCES

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

[2] Marco Domenico Aime, Giorgio Calandriello, and Antonio Lioy. 2007. Dependability in wireless networks: Can we rely on WiFi? *IEEE Security & Privacy* 5, 1 (2007), 23–29.

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

[4] Aloÿs Augustin, Jiazi Yi, Thomas Clausen, and William Townsley. 2016. A study of LoRa: Long range & low power networks for the internet of things. *Sensors* 16, 9 (2016), 1466.

[5] Bassem Bakhache, Joseph M Ghazal, and Safwan El Assad. 2013. Improvement of the security of Zigbee by a new chaotic algorithm. *IEEE Systems Journal* 8, 4 (2013), 1024–1033.

[6] Vladimir Brik, Suman Banerjee, Marco Gruteser, and Sangho Oh. 2008. Wireless device identification with radiometric signatures. In *Proceedings of the 14th ACM international conference on Mobile computing and networking*. ACM, 116–127.

[7] Ismail Butun, Nuno Pereira, and Mikael Gidlund. 2018. Analysis of LoRaWAN v1. 1 security. In *Proceedings of the 4th ACM MobiHoc Workshop on Experiences with the Design and Implementation of Smart Objects*. ACM, 5.

[8] Gayathri Chandrasekaran, John Austen Francisco, Vinod Ganapathy, Marco Gruteser, and Wade Trappe. 2009. Detecting Identity Spoofs in IEEE 802.11e Wireless Networks. In *Global Telecommunications Conference*.

[9] Gianluca Dini and Marco Tiloca. 2010. Considerations on security in Zigbee networks. In *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*. IEEE, 58–65.

[10] Adwait Dongare, Craig Hesling, Khushboo Bhatia, Artur Balanuta, Ricardo Lopes Pereira, Bob Iannucci, and Anthony Rowe. 2017. OpenChirp: A low-power wide-area networking architecture. In *2017 IEEE International Conference on Pervasive Computing and Communications Workshops*. IEEE, 569–574.

[11] Rashad Eletreby, Diana Zhang, Swarun Kumar, and Osman Yağan. 2017. Empowering low-power wide area networks in urban settings. In *Proceedings of the Conference of the ACM Special Interest Group on Data Communication*. ACM, 309–321.

[12] Song Fang, Yao Liu, Wenbo Shen, and Haojin Zhu. 2014. Where are you from?: confusing location distinction using virtual multipath camouflage. In *Proceedings of the 20th annual international conference on Mobile computing and networking*. ACM, 225–236.

[13] Branden Ghena, Joshua Adkins, Longfei Shangguan, Kyle Jamieson, Philip Levis, and Prabal Dutta. 2019. Challenge: Unlicensed LPWANs Are Not Yet the Path to Ubiquitous Connectivity. In *The 25th Annual International Conference on Mobile Computing and Networking*. ACM, 43–55.

[14] Chaojie Gu, Jiang Linshan, Tan Rui, Li Mo, and Huang Jun. [n. d.]. Attack-Aware Data Timestamping in Low-Power Synchronization-Free LoRaWAN. *arXiv preprint arXiv*.

[15] Ari Juels et al. 2006. RFID security and privacy: A research survey. *IEEE journal on selected areas in communications* 24, 2 (2006), 381–394.

[16] Min Qiang Li, Xian He Huang, Feng Tan, Yan Hong Fan, and Xun Liang. [n. d.]. A novel microcomputer temperature-compensating method for an overtone crystal oscillator. *IEEE Transactions on Ultrasonics Ferroelectrics & Frequency Control* 52, 11 ([n. d.]), 1919–1922.

[17] Ticyan Li and Guilin Wang. 2007. Security analysis of two ultra-lightweight RFID authentication protocols. In *IFIP international information security conference*. Springer, 109–120.

[18] Yao Liu and Peng Ning. 2012. Enhanced wireless channel authentication using time-synched link signature. In *INFOCOM*. IEEE.

[19] Yao Liu, Peng Ning, and Huaiyu Dai. 2010. Authenticating Primary Users' Signals in Cognitive Radio Networks via Integrated Cryptographic and Wireless Link Signatures. In *Symposium on Security and Privacy*. IEEE.

[20] Zhiqing Luo, Wei Wang, Jun Qu, Tao Jiang, and Qian Zhang. 2018. ShieldScatter: Improving IoT Security with Backscatter Assistance. In *Proceedings of the 16th ACM Conference on Embedded Networked Sensor Systems*. ACM, 185–198.

[21] Marwa Mamoun. 2014. Software Defined Radio. (2014).

[22] Anthony Patrick Melaragno, Damindra Bandara, Duminda Wijesekera, and James Bret Michael. 2012. Securing the ZigBee protocol in the smart grid. *Computer* 45, 4 (2012), 92–94.

[23] Son Thanh Nguyen and Chunming Rong. 2007. Zigbee security using identity-based cryptography. In *International Conference on Autonomic and Trusted Computing*. Springer, 3–12.

[24] Neal Patwari and Sneha K Kasera. 2007. Robust location distinction using temporal link signatures. In *Proceedings of the 13th annual ACM international conference on Mobile computing and networking*. ACM, 111–122.

[25] Yao Peng, Longfei Shangguan, Yue Hu, Yujie Qian, Xianshang Lin, Xiaojiang Chen, Dingyi Fang, and Kyle Jamieson. 2018. PLoRa: A passive long-range data network from ambient LoRa transmissions. In *Proceedings of the Conference of the ACM Special Interest Group on Data Communication*. ACM, 147–160.

[26] Melanie R Rieback, Bruno Crispo, and Andrew S Tanenbaum. 2006. The evolution of RFID security. *IEEE Pervasive Computing* 1 (2006), 62–69.

[27] Pieter Robyns, Eduard Marin, Wim Lamotte, Peter Quax, Dave Singelée, and Bart Preneel. 2017. Physical-layer fingerprinting of LoRa devices using supervised and zero-shot learning. In *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. ACM, 58–63.

[28] Nils Miro Rodday, Ricardo de O Schmidt, and Aiko Pras. 2016. Exploring security vulnerabilities of unmanned aerial vehicles. In *IEEE/IFIP Network Operations and Management Symposium*. IEEE, 993–994.

[29] Rupul Safaya. 1997. A multipath channel estimation algorithm using a kalman filter. *Diss. University of Kansas* (1997).

[30] Vamsi Talla, Mehrdad Hessar, Bryce Kellogg, Ali Najafi, Joshua R Smith, and Shyamnath Gollakota. 2017. LoRa backscatter: Enabling the vision of ubiquitous connectivity. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 1, 3 (2017), 105.

[31] Chiu C Tan, Bo Sheng, and Qun Li. 2008. Secure and serverless RFID authentication and search protocols. *IEEE Transactions on Wireless Communications* 7, 4 (2008), 1400–1407.

[32] JP Tomás. 2018. Operators in Korea, Netherlands deploy LoRa networks for IoT 2016.

[33] Stefano Tomasin, Simone Zulian, and Lorenzo Vangelista. 2017. Security analysis of LoRaWAN join procedure for Internet of Things networks. In *Wireless Communications and Networking Conference Workshops*. IEEE, 1–6.

[34] Beibei Wang, Yongle Wu, Feng Han, Yu-Han Yang, and KJ Ray Liu. 2011. Green wireless communications: A time-reversal paradigm. *IEEE Journal on Selected Areas in Communications* 29, 8 (2011), 1698–1710.

[35] Ge Wang, Haofan Cai, Chen Qian, Jinsong Han, Xin Li, Han Ding, and Jizhong Zhao. 2018. Towards replay-resilient RFID authentication. In *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking*. ACM, 385–399.

[36] Wei Wang, Lin Yang, Qian Zhang, and Tao Jiang. 2018. Securing On-Body IoT Devices By Exploiting Creeping Wave Propagation. *IEEE Journal on Selected Areas in Communications* (2018), 696–703.

[37] Jie Xiong and Kyle Jamieson. 2013. SecureArray: Improving WiFi security with fine-grained physical-layer information. In *Proceedings of the 19th annual international conference on Mobile computing & networking*. ACM, 441–452.

[38] Weitao Xu, Sanjay Jha, and Wen Hu. 2018. LoRa-key: Secure key generation system for LoRa-based network. *IEEE Internet of Things Journal* (2018).

[39] Xueying Yang, Evgenios Karampatzakis, Christian Doerr, and Fernando Kuipers. 2018. Security Vulnerabilities in LoRaWAN. In *IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation*. IEEE, 129–140.

[40] Asif M Yousuf, Edward M Rochester, Behnam Ousat, and Majid Ghaderi. 2018. Throughput, Coverage and Scalability of LoRa LPWAN for Internet of Things. In *IEEE/ACM 26th International Symposium on Quality of Service*. IEEE, 1–10.

[41] Junxing Zhang, Mohammad Hamed Firooz, Neal Patwari, and Sneha Kumar Kasera. 2008. Advancing wireless link signatures for location distinction. In *ACM International Conference on Mobile Computing & Networking*. ACM.