Poster Abstract: SoftLoRa – A LoRa-Based Platform for Accurate and Secure Timing

Chaojie Gu
Nanyang Technological University

Rui Tan
Nanyang Technological University

Jun Huang
Peking University

ABSTRACT

LoRa is an emerging low-power wide-area network technology. Existing studies have focused on LoRa's communication performance. Differently, we study two physical properties of LoRa, i.e., its performance in timing the signal propagation and the transmitters' frequency traits. Signal timing is a basis for implementing clock synchronization, ranging, and advanced physical (PHY) layer techniques such as concurrent decoding. However, LoRa end devices do not provide PHY-layer timestamping that is needed for accurate timing. We propose a *SoftLoRa* design that integrates a low-power software-defined radio receiver with a LoRa transceiver to provide PHY-layer access. Experiments show that SoftLoRa achieves microseconds timing accuracy over one kilometer and in a multistory building with strong signal attenuation.

Signal propagation timing is in general susceptible to a *frame delay attack*. We implement this attack against LoRa by a combination of stealthy jamming and delayed replay. To address the attack, we investigate the inherent frequency biases of LoRa transmitters. With an efficient signal processing algorithm, our frequency bias estimation achieves a resolution of 0.14 parts-per-million (ppm) of the channel's central frequency. This resolution is sufficient to detect the attack that introduces an additional frequency bias of one or more ppm. In summary, this work provides an accurate and secure LoRa-based timing approach based on the SoftLoRa design.

CCS CONCEPTS

• **Computer systems organization → Sensor networks**; • **Networks → Time synchronization protocols**.

KEYWORDS

LoRa, LoRaWAN, timing, clock synchronization, jamming, replay

ACM Reference Format:
Chaojie Gu, Rui Tan, and Jun Huang. 2019. Poster Abstract: SoftLoRa – A LoRa-Based Platform for Accurate and Secure Timing. In *Proceedings of The International Conference on Information Processing in Sensor Networks (IPSN'19).* ACM, New York, NY, USA, 2 pages. https://doi.org/10.475/123_4

1 INTRODUCTION

Punctually timing the propagation of a wireless signal is an important basis for various system functions, e.g., clock synchronization and time-of-flight ranging and localization. Owing to LoRa's long-range communication capability, LoRa-based timing can facilitate the implementation of these system functions. For instance, the sub-millisecond clock synchronization among distributed microphones is critical to localizing gunshots [3–5], which is an ongoing threat to the public safety in certain countries. In a factory or a building, wireless industrial devices and structural health monitoring sensors generally need tight clock synchronization as well to make sense measurement data and coordinate nodes' actions. At a maritime port, coarse-grained localization of massive containers are useful to the port operator for logistics monitoring and optimization. If LoRa-based timing can achieve sub-millisecond or microsecond (μs) accuracy, the above systems can avoid relying on the power-consuming GPS receivers or multi-hop clock synchronization protocols (e.g., FTSP) that were designed for short-range radios and require dense deployment of nodes for connectivity. Tight clock synchronization can also enable innovations and performance improvement at the physical (PHY) layer of LoRa communications. For instance, in the design of a distributed Chirp Spread Spectrum (CSS) for concurrent uplink transmissions [1], a more accurate clock synchronization among end devices will allow more concurrent transmissions. Despite the above desirable use cases, the timing performance based on the narrowband LoRa signals has remained unclear in the following two aspects: *accuracy of timing* and *security of timing*.

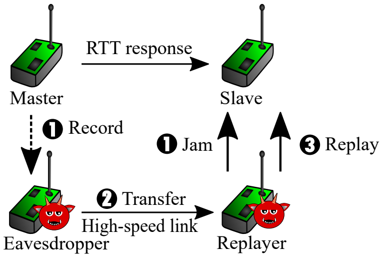

Figure 1: Frame delay attack by stealthy jamming and replay.

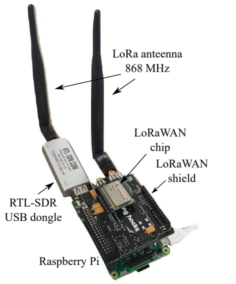

Figure 2: SoftLoRa hardware prototype.

To address the above issues, we propose a *SoftLoRa* design which integrates a low-power software-defined radio (SDR) receiver that enables μs-accurate PHY timestamping. For security, we consider a basic threat of *frame delay attack* described in the RFC 7384 [2] that delays the frame transmission in a timing process. As illustrated in Fig. 1, the attacker sets up two devices called *eavesdropper* and *replayer*. The attack consists of three steps. ❶ Once the replayer detects a frame transmission from the master to the slave of a timing process, it jams the slave's frame reception by transmitting a jamming frame. This jamming can be stealthy in that the LoRa chip

IPSN'19, April 2019, Montreal, Canada

ACM ISBN 123-4567-24-567/08/06…$15.00
https://doi.org/10.475/123_4

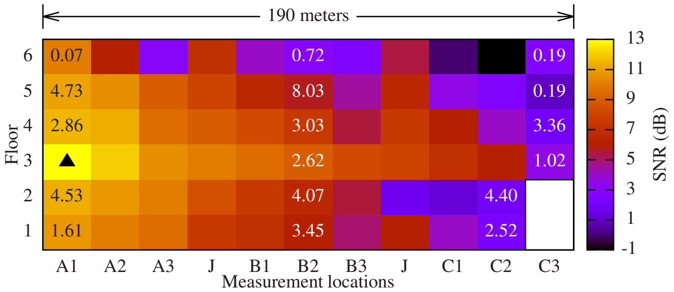

Figure 3: SNR survey in the building (lateral view) and timing accuracy. Triangle represents fixed node. Number in a cell is timing error in μs of the mobile node in the cell.

generates no alerts. Meanwhile, the eavesdropper records the radio waveform of the frame. ❷ The eavesdropper sends the recorded radio waveform data via a separate communication link to the replayer. ❸ After an intended malicious time delay, the replayer replays the recorded radio waveform received from the eavesdropper. This threat cannot be addressed by conventional measures such as cryptographic protection and frame counting. This attack can be easily implemented – two computer science undergraduate students have independently and separately implemented it. To address this threat, we track the LoRa transmitters' inherent frequency biases that can be extracted from the SDR receiver's samples to detect the replay step of the attack.

2 ACCURATE & SECURE TIMING BY LORA

SoftLoRa: This work is conducted based on a SoftLoRa hardware prototype that integrates a Raspberry Pi 3 Model B (as the host), a Cooking Hacks LoRaWAN shield (as the LoRa transceiver), and an RTL-SDR USB dongle (as the SDR receiver). Fig. 2 shows the prototype. The LoRaWAN shield consists of a Microchip RN2483 chipset that is based on Semtech SX1276, an 868 MHz antenna, and a GPIO interface. Mounted on the host via GPIO pins, the shield can be controlled using a C++ library from Cooking Hacks.

Accurate timing in a multistory building: We conduct experiments in a concrete building with six floors. Fig. 3 illustrates a lateral view of the building. We survey the SNR inside the building. We deploy a fixed SoftLoRa transmitter in A1-3, and then carry a mobile SoftLoRa receiver to different positions to measure the SNR. The heat map in Fig. 3 shows the SNR measurements. The SNR decays with the distance between the two nodes. The numbers shown in the cells of Fig. 3 are the measured timing errors in μs when the mobile node is at the corresponding locations. The timing is based on an advanced signal onset time detection algorithm called autoregressive Akaike Information Criterion (AR-AIC). With the SNR range in Fig. 3, AR-AIC performs well to yield sub-10μs timing accuracy. The timing error in this SNR range unnecessarily decreases with SNR.

Accurate timing over one km: We deploy a pair of SoftLoRa nodes in a campus, which are separated by an Euclidean distance of 1.07 km. The signal's one-way propagation time is 3.57 μs. The two nodes are deployed on the roof top of a building and in an open stair case of another building. We conducted four tests to evaluate the clock offset estimation error. It rained heavily during the tests. The measured errors during the four tests are 3.52 μs, 2.27 μs, 6.43 μs, 0.23 μs. Thus, SoftLoRa achieves microseconds clock synchronization accuracy over a distance of one km.

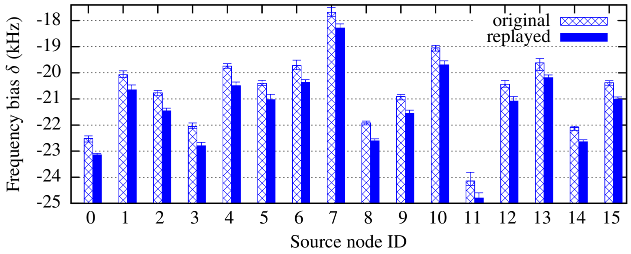

Figure 4: FBs estimated from the original LoRa signals from 16 nodes and those replayed by a USRP-based replayer. The error bar shows mean, minimum, and maximum of FBs in 20 frame transmissions.

Secure timing by tracking frequency bias: We use an SDR receiver to estimate the frequency biases (FBs) of 16 LoRa transmitters. The distance between the transmitter and the SDR receiver is about 5 m. The error bars labeled "original" in Fig. 4 show the results. We can see that the FBs for a certain node are stable and the nodes generally have different FBs. The absolute FBs are from 17 kHz to 25 kHz, which are about 20 ppm to 29 ppm of the nominal central frequency of 869.75 MHz. The precision of the estimation is about 0.14 ppm only. For the replayed frames used in the frame delay attack, additional FBs of about 0.54 kHz to 0.74 kHz (i.e., 0.62 ppm to 0.85 ppm) are introduced. Thus, by tracking the FB, the replay step of the frame delay attack can be detected. Note that this attack detection approach does not require distinct FBs among different LoRa transmitters.

3 CONCLUSION

This work investigates the timing performance and frequency biases of LoRa radios based on a *SoftLoRa* platform that integrates a low-power SDR receiver with a LoRa transceiver. The results show that, with LoRa signals, microseconds timing accuracy can be achieved in various realistic environments. We also show the insecurity of LoRa-based timing caused by a frame delay attack. To address the attack, this work develops efficient time-domain signal processing algorithms that estimate the frequency biases of transmitters. By tracking the frequency biases, the replay step of the frame delay attack can be detected. Our results also show the value of exposing certain PHY accesses to system developers for enhancing LoRa network performance and security.

REFERENCES

[1] Mehrdad Hessar, Ali Najafi, and Shyamnath Gollakota. 2019. NetScatter: Enabling Large-Scale Backscatter Networks. In *NSDI*.

[2] T. Mizrahi. 2014. Security Requirements of Time Protocols in Packet Switched Networks. https://tools.ietf.org/html/rfc7384

[3] Robert L. Showen, Robert B. Calhoun, and Jason W. Dunham. 2009. Acoustic location of gunshots using combined angle of arrival and time of arrival measurements. US Patent US7474589B2.

[4] Gyula Simon, Miklós Maróti, Ákos Lédeczi, György Balogh, Branislav Kusy, András Nádas, Gábor Pap, János Sallai, and Ken Frampton. 2004. Sensor network-based countersniper system. In *SenSys*.

[5] Peter Volgyesi, Gyorgy Balogh, Andras Nadas, Christopher B Nash, and Akos Ledeczi. 2007. Shooter localization and weapon classification with soldier-wearable networked sensors. In *MobiSys*.