Attack-Aware Synchronization-Free Data Timestamping in LoRaWAN

CHAOJIE GU, LINSHAN JIANG, RUI TAN, and MO LI, Nanyang Technological University, Singapore
JUN HUANG, Massachusetts Institute of Technology, United States

Low-power wide-area network technologies such as LoRaWAN are promising for collecting low-rate monitoring data from geographically distributed sensors, in which timestamping the sensor data is a critical system function. This paper considers a synchronization-free approach to timestamping LoRaWAN uplink data based on signal arrival time at the gateway, which well matches LoRaWAN's one-hop star topology and releases bandwidth from transmitting timestamps and synchronizing end devices' clocks at all times. However, we show that this approach is susceptible to a *frame delay attack* consisting of malicious frame collision and delayed replay. Real experiments show that the attack can affect the end devices in large areas up to about $50,000\,m^2$. In a broader sense, the attack threatens any system functions requiring timely deliveries of LoRaWAN frames. To address this threat, we propose a LoRaTS gateway design that integrates a commodity LoRaWAN gateway and a low-power software-defined radio receiver to track the inherent frequency biases of the end devices. Based on an analytic model of LoRa's chirp spread spectrum modulation, we develop signal processing algorithms to estimate the frequency biases with high accuracy beyond that achieved by LoRa's default demodulation. The accurate frequency bias tracking capability enables the detection of the attack that introduces additional frequency biases. We also investigate and implement a more crafty attack that uses advanced radio apparatuses to eliminate the frequency biases. To address this crafty attack, we propose a pseudorandom interval hopping scheme to enhance our frequency bias tracking approach. Extensive experiments show the effectiveness of our approach in deployments with real affecting factors such as temperature variations.

CCS Concepts: • **Networks** → *Sensor networks*; • **Security and privacy** → *Distributed systems security*.

Additional Key Words and Phrases: Low-power wide-area networks, LoRaWAN, data timestamping, wireless security.

ACM Reference Format:
Chaojie Gu, Linshan Jiang, Rui Tan, Mo Li, and Jun Huang. 2019. Attack-Aware Synchronization-Free Data Timestamping in LoRaWAN. *ACM Trans. Sensor Netw.* 1, 1, Article 1 (January 2019), 32 pages. https://doi.org/0

1 INTRODUCTION

Low-power wide-area networks (LPWANs) enable direct wireless interconnections among end devices and gateways in geographic areas of square kilometers. It increases network connectivity

A preliminary version of this work appears in The 40th IEEE International Conference on Distributed Computing Systems (ICDCS 2020). This research was supported in part by two MOE AcRF Tier 1 grants (2019-T1-001-044 and 2018-T1-002-081).
Authors' addresses: Chaojie Gu, gucj@ntu.edu.sg; Linshan Jiang, LINSHAN001@e.ntu.edu.sg; Rui Tan, tanrui@ntu.edu.sg; Mo Li, limo@ntu.edu.sg, Nanyang Technological University, School of Computer Science and Engineering, N4-B02A-01, 50 Nanyang Avenue, Singapore, 639798; Jun Huang, Massachusetts Institute of Technology, Sloan School of Management, 100 Main St, Cambridge, United States, MA 02142, junhuang@mit.edu.

1550-4859/2019/1-ART1 $15.00
https://doi.org/0