Challenges of Securing Low-Power LoRaWAN Devices Deployed in Advanced Manufacturing

Mohammad Monjur, Joseph Heacock, Joshua Calzadillas, Rui Sun, and Qiaoyan Yu
University of New Hampshire, Durham, NH 03824, USA

2022 23rd International Symposium on Quality Electronic Design (ISQED) | 978-1-6654-9466-3/22/$31.00 ©2022 IEEE | DOI: 10.1109/ISQED54688.2022.9806290

***Abstract*—Compared to traditional manufacturing, advanced manufacturing is expected to support more innovative, reliable, and affordable manufacturing. Cutting-edge technologies, such as Long-Range Wide-Area Network (LoRaWAN), have been adopted in advanced manufacturing to enable the increasing demand for cost-effective automation, remote monitoring and control, and long-duration maintenance. However, the utilization of LoRaWAN will bring in new and unexplored security threats to the manufacturing pipeline. This work demonstrates three physical attacks (hardware Trojan, jamming, and replay attacks) executed in the LoRa nodes and analyzes the challenges of detecting and mitigating those attacks.**

I. Introduction

Advanced manufacturing technologies have attracted increasing attention from manufacturing industries for automotive, steel and industrial machinery, medical devices, computer and other high-tech devices. The utilization of sensor networks, smart devices, and wireless communication technologies such as Long-Range Wide-Area Network (LoRaWAN) in advanced manufacturing makes the manufacturers confront new security challenges. The existing research effort mainly focuses on cyber attacks, rather than the security threats from the untrusted supply chain or on-site physical attacks. Moreover, a recent survey [1] indicates that most analysis of the LoRaWAN security challenges relies on theoretical analysis and simulation-based evaluation rather than practical experiments. There is limited work available to study the security vulnerabilities of the LoRa hardware devices, and this work fills this gap. We examine the impact of compromised LoRa hardware devices on the LoRaWAN in advanced manufacturing and observe that the physical attacks in LoRaWAN complement the cyber attacks reported in other studies. Our case studies indicate that the low-power nature of LoRa node devices brings unique challenges for attack detection.

II. Attack Scenarios and Our Case Study

In this work, We focus on the attacks that manipulate the network through physical access to harm the security of LoRaWAN. The so-called 'physical access' can be before or after device deployment. The former one is originated from an outsourced untrusted supply chain. The later one is conducted by attackers having access to the physical LoRa network in the manufacturing factory, such as the one shown in Fig. 1. Typically, those attacks happen in LoRa nodes and gateways, for example, the LoRa devices shown in Fig. 2. LoRa nodes are typically formed by configuring low-end programmable devices. Since those devices are generic, the integrity and reliability of diverse commercial-off-the-shelf LoRa nodes cannot be guaranteed. Some LoRa devices could be counterfeited or carry hardware Trojans. More specifically, the hardware Trojan in a LoRa node could tamper with the hardware implementation of communication protocols to cause the loss of the integrity of sensing data. The hardware Trojan could also alter the original functionality of a LoRa node to store the LoRa packets stealthily and then replay those packets occasionally. The physical attacks induced by hardware Trojans will eventually sabotage the normal behavior and performance of the LoRaWAN.

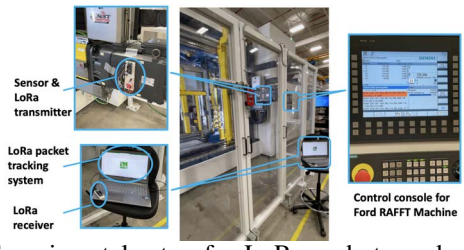

Fig. 1: Experimental setup for LoRa node-to-node communication in the Olson Center [2].

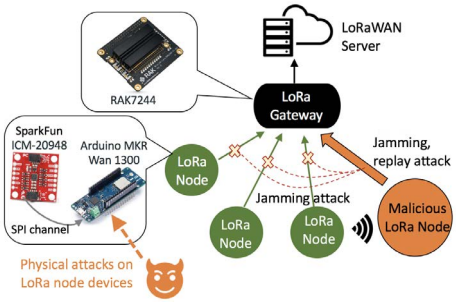

Fig. 2: Attack scenario interested in this work.

Alternatively, an on-site physical attack could be performed by an adversary close to the advanced manufacturing factory. As LoRaWAN can support wireless transmission in a radius of 10 kilometers, it is practical to have a malicious LoRa node outside the factory to induce a jamming attack in the LoRaWAN area and manipulate the manufacturing operations. Different than the compromised LoRa devices from the untrusted supply chain, the malicious LoRa node in the on-site attack could be any devices that implement the LoRaWAN.

References

[1] J. P. Shanmuga Sundaram, W. Du, and Z. Zhao, "A Survey on LoRa Networking: Research Problems, Current Solutions, and Open Issues," *IEEE Comm. Surveys Tutorials*, vol. 22, no. 1, pp. 371–388, 2020.

[2] "John olson advanced manufacturing center, = https://ceps.unh.edu/Olson-Center,."