frontiers | Frontiers in Sensors

ORIGINAL RESEARCH
published: 04 May 2022
doi: 10.3389/fsens.2022.850056

Hardware Security in Sensor and its Networks

*Mohammad Mezanur Rahman Monjur[1], Joseph Heacock[1], Joshua Calzadillas[1], MD Shaad Mahmud[1], John Roth[2], Kunal Mankodiya[3], Edward Sazonov[4] and Qiaoyan Yu[1]**

[1]Department of Electrical and Computer Engineering, University of New Hampshire, Durham, NH, United States, [2]Department of Mechanical Engineering, John Olson Advanced Manufacturing Center, University of New Hampshire, Durham, NH, United States, [3]Department of Electrical, Computer, and Biomedical Engineering, University of Rhode Island, Kingston, RI, United States, [4]Department of Electrical and Computer Engineering, University of Alabama, Tuscaloosa, AL, United States

Sensor networks and IoT systems have been widely deployed in monitoring and controlling system. With its increasing utilization, the functionality and performance of sensor networks and their applications are not the only design aims; security issues in sensor networks attract more and more attentions. Security threats in sensor and its networks could be originated from various sectors: users in cyber space, security-weak protocols, obsolete network infrastructure, low-end physical devices, and global supply chain. In this work, we take one of the emerging applications, advanced manufacturing, as an example to analyze the security challenges in the sensor network. Presentable attacks—hardware Trojan attack, man-in-the-middle attack, jamming attack and replay attack—are examined in the context of sensing nodes deployed in a long-range wide-area network (LoRaWAN) for advanced manufacturing. Moreover, we analyze the challenges of detecting those attacks.

Keywords: sensor network, cybersecurity, LoRaWAN, hardware security, hardware Trojan, side-channel signal

OPEN ACCESS

Edited by:
Sungyong Jung,
University of Texas at Arlington, United States

Reviewed by:
Celestine Iwendi,
School of Creative Technologies University of Bolton, United Kingdom
Ivan Mezei,
University of Novi Sad Faculty of Technical Sciences, Serbia

****Correspondence:***
Qiaoyan Yu
qiaoyan.yu@unh.edu

Specialty section:
This article was submitted to Sensor Networks, a section of the journal Frontiers in Sensors

Received: *07 January 2022*
Accepted: *07 February 2022*
Published: *04 May 2022*

Citation:
Monjur MMR, Heacock J, Calzadillas J, Mahmud MDS, Roth J, Mankodiya K, Sazonov E and Yu Q (2022) Hardware Security in Sensor and its Networks. Front. Sens. 3:850056. doi: 10.3389/fsens.2022.850056

1 INTRODUCTION

With the advent of microelectronics and Internet-of-Things (IoT), sensor networks have received wide attention among scientific communities in developing smart sensor technology, and they are being used in various applications. For example, home and vehicle automation, logistics and transportation, environmental monitoring, healthcare, surveillance, education, and training Munir et al. (2007); Agnihotri et al. (2015). A sensor network is a collection of small sensor nodes with different sensing capabilities that record data at various environments and send it to a base station. Depending on the deployment location and application, sensor networks can be wired or wireless. In a wired sensor network, sensor nodes are connected by Ethernet cables; in contrast, a wireless sensor network uses Bluetooth, WiFi, cellular, Near-Field-Communication (NFC), Narrowband Internet of Things (NB-IoT), and Long-Range (LoRa) technologies. Due to the distributed nature of the sensor deployment, wireless sensor networks have gained much more attention than wired sensor networks.

Depending on the application, sensor networks can cover a large area of interest for a variety of objectives. They can be deployed in terrestrial, underground Muduli et al. (2018); Minhas et al. (2018) or underwaterMohamed et al. (2011) environments. As a result, sensor networks have an ever-expanding set of uses that includes but not limited to environmental monitoring Xu et al. (2014); Ullo and Sinha (2020), health monitoring Ayyildiz et al. (2019); Abdulkarem et al. (2020),

TABLE 1 | Sehrawat and Gill (2019) Different types of sensors used in IoT Networks.

Sensors	Type and short description	Applications
Proximity	Electromagnetic wave. By nature, can be inductive, capacitive, photoelectric, magnetics etc. Detects nearby object	Industries
Occupancy	Consists of either/in combination of pressure, humidity, light and air sensors, used for remote sensing	As per requirement
Motion	Hybrid in nature, can sense any physical movement in range. Versatile, recordings can be captured in form of photos/videos if programmed	Home security
Velocity	Linear/Angular velocity detection, enable real time velocity remote monitoring	Smart city vehicle monitoring
Temperature	Can detect heat changes allows monitoring real time temperature changes	Wearables devices, agriculture
Pressure	Senses pressure changes	Environment, agriculture, home-pressure monitor
Chemical	Detects changes in chemical compositions in different mediums i.e. air, water	Air/water quality observation
Humidity	Works as temperature, moisture and signal sensor	Food quality observation, agriculture, environment
Water quality	Basically monitors ion, pH, conductivity changes in the water	Water quality monitor
Gyroscope	Measure angular movement/velocity	3D mouse, robotic devices, aircrafts

precision agriculture Thakur et al. (2019); Kiani and Seyyedabbasi (2018), military applications Azzabi et al. (2017); Ahmad et al. (2016), transportation Alawad and Kaewunruen (2018); Gaber et al. (2018), smart cities Alías and Alsina-Pagès (2019); Hanif et al. (2018).

Sensors are mainly classified based on their purpose, i.e., the types of physical conditions monitored by the specific sensors. The general conditions monitored by the sensors are sound, distance, heat, light, or any measurable changes. Sensor outputs are connected to an IoT network through devices, thus building a management network where security is crucial to prohibit data breaches and unwanted exposure. As far as security is concerned, the most common sensors used in modern residential and commercial purposes include infrared sensors Singh et al. (2016), photoelectric beam based sensors, microwave sensors security and safety have always been critical to the welfare of individuals (2020), tomographic motion detection sensors Forstater (2014), audio sensors, and motion sensors. **Table 1** shows a list of the existing sensors commonly used in IoT networks with their applications.

As sensor networks have been commonly applied in medical, automobiles, agriculture, military, and mining applications, attackers from various sectors are motivated to intrude the sensor network to manipulate the sensor data, leak information, blind monitoring systems, or cause malfunctions in control infrastructure. With the increasing utilization of remote working mode, the integrity and trustworthiness of sensor networks have become more critical than ever. To ensure the sensor data flow securely in the network, a group of researchers Papadogiannaki and Ioannidis (2021) have investigated IoT network traffic processing systems. Agencies such as the European Union Agency for Cybersecurity ENISA (2019) support the efforts that improve the regulation and implementation guidelines for IoT networks. Unfortunately, sensor networks could be attacked by users not only from cyber space, but also from local users and the globalized supplied chain. Moreover, not all existing wireless communication protocols are equipped with sufficient security features. The use of obsolete network infrastructure and low-end sensors/edge devices make sensor networks vulnerable to various attacks, such as Denial of Service (DoS), sinkhole, blackhole, greyhole, wormhole, selective forwarding, Sybil, replay, and hello flood attack. The work Ng et al. (2015) reports that a sensor can be leveraged as a backdoor to trigger hardware Trojans. External ambient variables such as temperature were introduced to trigger the Trojan and leak the AES secret key. The work Schellenberg et al. (2018) shows an integrated sensor that can be used to exploit the power distribution network (PDN) to extract the secret key. If the compromised sensor is implemented in PDN, the malicious sensor could sense the voltage fluctuation of other modules and facilitate the side-channel analysis attack. Since the setup of a sensor network varies with its specific application, the security challenges for the sensor network are unique when it is deployed in advanced manufacturing and industries.

The existing literature lacks the quantitative analysis on security threats in practical applications. The attacks from the physical devices have not been examined extensively and holistically. In this work, we make the following main contributions:

- We take one of the emerging applications, advanced manufacturing, as an example to analyze the security challenges in the sensor network. Instead of using theoretical proof and simulation-based analysis, we perform our quantitative analysis based on both laboratory and on-site measurements.
- Four types of attacks—hardware Trojan attack, man-in-the-middle attack, jamming attack and replay attack—are examined in the context of sensing nodes deployed in a long-range wide-area network (LoRaWAN) for advanced manufacturing. Both time-domain and frequency-domain studies are conducted to reveal the stealthiness of representable attacks.
- A security tracking framework is proposed in this work to facilitate the research on sensor network security. Moreover, we analyze the challenges in detecting the highlighted attacks in sensor networks.

The rest of this work is organized as follows. In **Section 2**, we introduce the preliminary knowledge of sensors and its

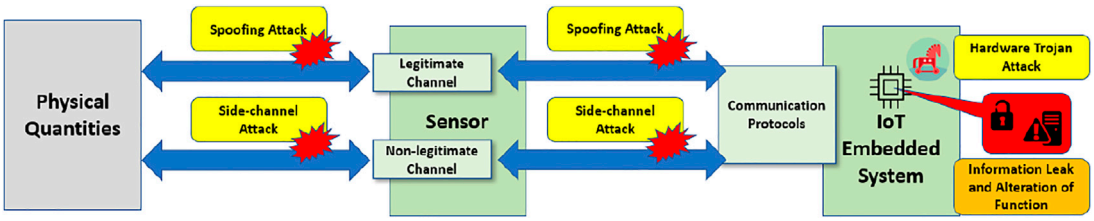

FIGURE 1 | Attack vectors of sensor network system.

application in LoRaWAN. In **Section 3**, we propose a framework that facilitates the analysis on the security threats in sensor networks. In addition, our laboratory and on-site experimental setup are summarized. In **Section 4**, we examine the typical attacks observed in sensor networks. Quantitative and comprehensive analysis is performed, as well. Challenges on attack detection are reasoned in **Section 5**. This work is concluded in **Section 6**.

2 PRELIMINARIES FOR LORAWAN AND SECURITY THREATS

2.1 Introduction of LoRaWAN

Long-Range (LoRa) technology is commonly used in Internet-of Things. LoRa networks connect sensors to the cloud and enable real-time communication of data and analytics to enhance efficiency and productivity. Due to its low power and long-range capability, LoRa technology has been widely used in automated manufacturing industries. As a critical part of advanced manufacturing, LoRa nodes are mainly implemented with sensors to monitor the ambient environment, track the machine motion, and provide the primary control system with real-time data feedback via Long-Range Wide-Area Network (LoRaWAN). LoRaWAN incorporates three main parts end devices (LoRa Nodes), a network server (Gateway), and an applications server (Cloud). The overview of LoRaWAN connection topology is shown in **Supplementary Figure S1**.

LoRa nodes are end devices, which are mainly configured as slave devices to sense surrounding environmental data and transmit data packets to the cloud. Depending on the power of transmission and computation, LoRa devices are classified into three categories: Class A, B, and C. Class A LoRa features the most energy-efficient node and is mostly used for remote sensor data transmission. Class B LoRa has a beacon-like feature and sends data packets with a certain interval. Class C LoRa offers high power consumption compared to all other classes as it continuously transmits the data to the LoRa gateway Polonelli et al. (2019). A LoRa gateway is a radio transceiver, the heart of the LoRaWAN topology. LoRa gateways receive modulated RF packets from the end device (LoRa node) and forward them to the network server through an IP backhaul connection. LoRa gateways have higher process power and the ability to handle more tasks than LoRa end devices Zhou et al. (2019). The network server is the core of LoRaWAN management and enables the communication between end nodes to end-users. The network server manages the connection authentication and monitors the nodes, gateways, and end-user application traffic. The network server implements the LoRaWAN protocol and validates the authenticity and integrity of the LoRa devices Zhou et al. (2019). The application server handles the LoRaWAN application layer for decryption and encryption of the data. The application server can easily link data management systems or launch template integration with the leading IoT platform of Amazon Web Services (AWS), Azure, and Google cloud Industries (2021).

2.2 Security Challenges From Sensors

Although LoRaWAN includes some security features such as data origin authentication and integrity Han and Wang (2018) shown in **Supplementary Figure S2**, the LoRaWAN security cannot be fully assured. The LoRaWAN consists of a low-powered embedded device (LoRa nodes) integrated with sensors and a gateway to connect the cloud. Most LoRa end devices are low-powered and lack adequate security due to power constrain. As sensors do not have any encryption engine Noura et al. (2020), the raw data collected by a sensor could be altered before reaching the storage or processing unit connected with that sensor. **Figure 1** depicts three types of attack—spoofing attacks, side-channel attacks, and hardware Trojan insertion attacks—that could be performed in a sensor network system. An adversary could take advantage of the sensor network's vulnerability and carry out malicious activity. For example, an adversary can reverse engineer communication protocols such as (I^2C), SPI, and uses asynchronous serial communication (UART) Monjur et al. (2020). Therefore, adversaries can alter the sensor data conversion and the sensor mechanism to launch spoofing and fault injection attacks He et al. (2017). Sensors transmit the data to the embedded system through the network and malicious node can trigger a hardware Trojan (HT) and leak critical information. The HT can be inserted during the chip fabrication process and stay dormant until its activation condition is satisfied. Once triggered, HT can cause severe data breaches or alteration of instruction to the system.

Many side-channel attack studies have pointed out the security vulnerability of LoRaWAN protocols. The LoRa node is subject to side-channel attacks. For example, the authors demonstrated that they can retrieve the AES key used for transmitted packets using correlation power

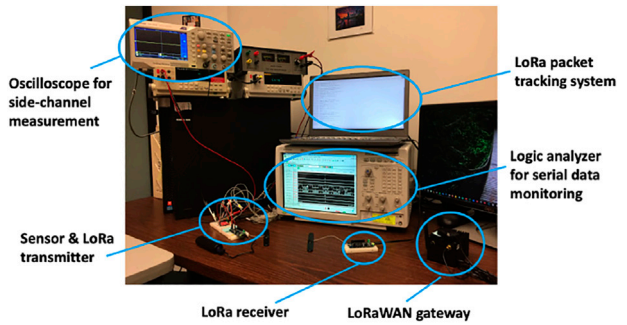

FIGURE 2 | Experimental setup for LoRa node-to-node communication in a research laboratory.

analysis Fukushima et al. (2020). The other side-channel attacks, such as electromagnetic-leakage traces, can recover 12 bytes of the key for the payload encryption process and the message authentication code generation process Fukushima et al. (2019).

3 PROPOSED ANALYSIS FRAMEWORK FOR THE SECURITY STUDY OF SENSOR AND ITS NETWORK

3.1 Experimental Setup

The quantitative analysis performed in the rest of this work is based on the measurement results from two sets of experimental setup, one from a research laboratory and one from an advanced manufacturing center.

For simplicity, we first performed node-to-node communication in a research laboratory. The overview of the setup is shown in **Figure 2**. The LoRa gateway was built based on RAK7244. The sensors deployed in our system were integrated on a single board, SparkFun ICM-20948 9DoF IMU, which includes an accelerometer, a gyro meter, and a temperature sensor. The LoRa node was programmed on Arduino MKR WAN 1300. Two Arduino boards were configured into the LoRa packet transmitter and receiver. The packets transferred via LoRaWAN were monitored by the Arduino IDE's serial monitor.

Next, we deployed a LoRaWAN in the UNH John Olson Advanced Manufacturing Center Olson (2021), which hosts the manufacturing machines for automate machine tending, metrology, deburring, and metal sheet forming. As a case study, we collected the real-time LoRa packets from the double-sided incremental sheet forming machine. The corresponding onsite setup is shown in **Figure 3**.

3.2 Framework for Information Tracking and Security Analysis

Figure 4 provides an overview of the proposed framework to enable the security threats analysis in sensors, LoRa end nodes, gateways, and servers. An attacker can tamper with sensing devices to alter the original sensed value, harming the data integrity. An adversary can also sniff and capture the transmitted packet between nodes and gateways, or capture data packets via some open-source hardware (e.g., Software-Defined Radio (SDR) device). Even if not knowing the encryption key applied in the data packet, an attacker can still impersonate a sensing node and replay the captured packets to the network.

As highlighted in the framework, we use a signal logic analyzer to examine the integrity of real-time sensor data and detect the abnormal behavior of sensing nodes. A signal spectrum analyzer will be utilized to monitor the wireless signals between LoRa nodes and LoRa gateways. The spectrum analyzer measures the gain, power, distortion, harmonics, the bandwidth of a LoRa transmitted signal in the operating frequency range of the LoRa node. Although the LoRa payload is encrypted, analyzing the metadata can still provide us some insights. The information we can extract from a gateway log file includes records of gateway status, uplink, and downlink messages. The records of LoRa packets contain a timestamp, message ID, frequency, bandwidth, and data rate. Analyzing this information under normal conditions and under

FIGURE 3 | Our onsite experimental setup on the sheet forming machine in the John Olson Advanced Manufacturing Center.

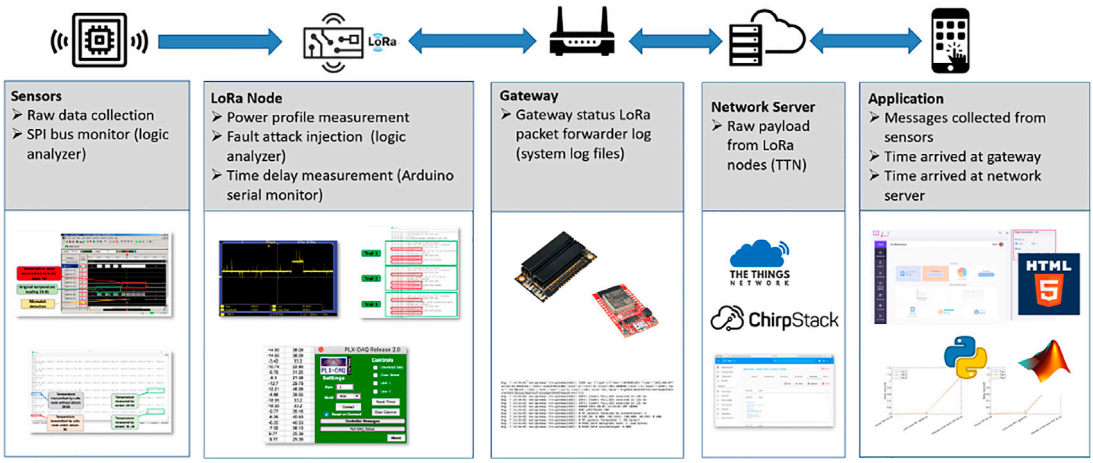

FIGURE 4 | Overview of proposed security tracking and analysis system.

attack makes it possible to detect some abnormal behavior such as replay attacks. Additionally, feeding a large number of records extracted from the gateway logs to Machine Learning algorithms can help us more effectively and accurately achieve this goal. **Supplementary Figure S3** highlights the attacks on sensors, edge node and LoRaWAN gateway devices, as well as and their connection network. As many existing works have extensively investigated secure boot, anomaly detection, data encryption, and secure communications of LoRaWAN, the proposed attack analysis framework concentrates on the attacks performed on the physical devices.

Sensors have become a critical part of revolutionizing the automation of industry 4.0. Sensors are used in a passive or active mode to measure the physical properties of the surrounding environment. Many IoT devices have been integrated into sensor networks. As most of the end devices are low-powered and lack adequate security, an adversary can take advantage of the weakly-protected sensing nodes to cause system failures or carry out malicious activity. There are many prevention and detection mechanisms for software and network vulnerability, but end devices blindly trust sensing inputs and lack robust defense mechanisms against the attacks from compromised sensors. The attacks on sensing nodes can be classified into three major attacks: spoofing attacks, side-channel attacks, and hardware Trojan attacks. Reserves engineering on the sensor mechanism can launch spoofing attacks. Sensors transmit data to an embedded system through the network. If the sensor is compromised, it can trigger a hardware Trojan and leak critical information. **Supplementary Figure S4** shows an example of Trojans in a sensing node could lead to the failure in key management. Hardware Trojans can be inserted during the chip fabrication process and stay dormant until activation conditions are satisfied. Once triggered, they can cause severe data breaches or alteration of instruction to the system.

One challenge in assuring sensor security is the fact that the sensing mechanisms rely on diverse electrical, mechanical, and chemical properties. Attacks on these sensors are various and complicate, and thus the attack mitigation varies accordingly. The existing literature Polonelli et al. (2019); Reynders et al. (2016); Han and Wang (2018); Yang et al. (2018); Aras et al. (2017) mainly focuses on the security threats from the channel between network servers and application users and they investigate the key management strategies for sensor networks. There is limited work available to study the security vulnerabilities of the hardware devices for sensing. This work fills this gap.

4 QUANTITATIVE SECURITY THREAT ANALYSIS

4.1 Attack Scenarios

In this section, we perform quantitative and comprehensive security threat analysis on a sensor network communicated via LoRa technology. Most literature focuses on the cyber attacks in the server and application layers Reynders et al. (2016); Yang et al. (2018); Aras et al. (2017). The work Rocha and Correia (2011) outlines how confidential data such as passwords and cryptographic keys may be extracted from cloud server storage by a malicious insider of the cloud service provider. Unauthorized access remains a challenge as LoRaWAN differs from one implementation to another Oniga et al. (2017). The unauthorized access or mapping of the network can compromise the backend network communications between the gateway and the LoRaWAN server de Moraes and da Conceição (2021).

To harm the security of LoRaWAN, attackers could manipulate the network through the physical access, as well. 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. Typically, those attacks happen in LoRa nodes and gateways, as shown in

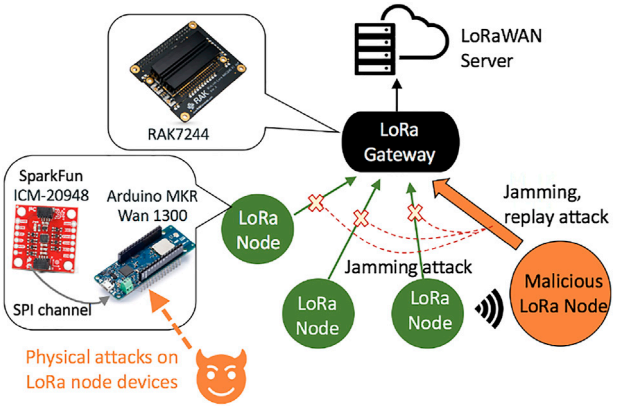

FIGURE 5 | Attack scenario interested in this work.

Figure 5. The particular LoRa devices shown in the zoom-in view are the ones adopted in our case studies.

LoRa nodes are typically formed by configuring low-end programmable devices, such as Arduino, STMicroelectronics and Raspberry Pi Choi et al. (2018). Since those devices are generic, the integrity and reliability of diverse commercial-off-the-shelf LoRa nodes cannot be guaranteed. Some LoRa devices (labeled as malicious LoRa node in **Figure 5**) 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, such as SPI, 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 behaviors and performance of the LoRaWAN.

Alternatively, on-site physical attack could be conducted by an adversary close to the site where the sensor network is deployed, for instance, an advanced manufacturing factory. As LoRaWAN can support wireless transmission in a radius of 10 km Petajajarvi et al. (2015), 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.

4.2 Demonstration of Practical Attacks

4.2.1 Hardware Trojan Attack: Manipulate Sensor Data

Hardware Trojan is a malicious modification on physical devices. The hardware Trojan in a LoRa node aims for tampering with the data transferred from the sensor to the LoRa gateway. This type of attack is executed before the device authentication and data encryption algorithm in the gateway, network server and application layers. Being inserted through an untrusted design house, a hardware Trojan can be activated by a specific sensor measurement value and its payload could harm the memory and

TABLE 2 | Unique hardware Trojans in sensor networks.

Trojan	Location	Example of triggering/payload mechanisms
Trigger	1. Sensor 2. I/O Interface 3. Memory for firmware	1. Temperature range 2. Motion acceleration speed 3. Transmission rate 4. Illumination level
Payload	1. Cache memory 2. Arithmetic module 3. RF transmitter	1. Spreading factor configuration 2. Channel bandwidth configuration 3. Frequency configuration

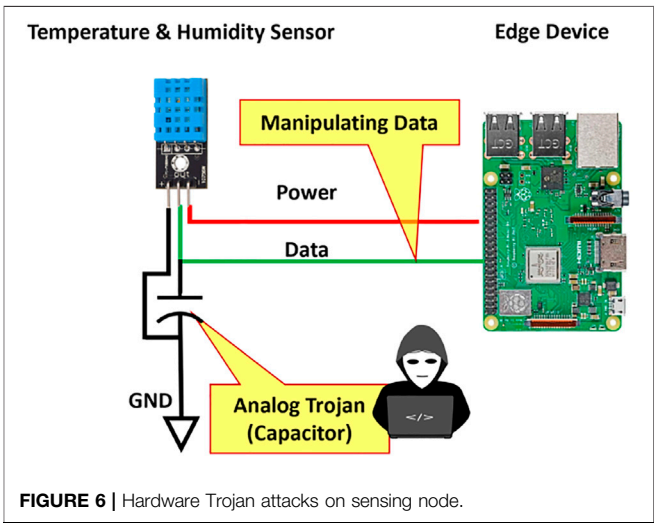

FIGURE 6 | Hardware Trojan attacks on sensing node.

radio frequency (RF) signal transmitter. More unique hardware Trojan triggering and payload designs are summarized in **Table 2**. **Figure 6** depicts how a Trojan attack can sabotage sensing node: either manipulate sensing data or tamper with some electronic components.

In our case study, we programmed one Arduino board to form a malicious LoRa node. The compromised LoRa node will activate the Trojan with a specific trigger condition and alter the sensor data. We monitor the consequence of the Trojan attack through an Ardunio IDE serial monitor. As shown in **Figure 7**, the temperature sensed and transmitted by the sensor node is different with what is accepted by the LoRa node. The highlighted temperature changes indicate that the malicious LoRa node alters the temperature of 31.14°C–96.00°C. We also compare the LoRa packets with/without the Trojan attack via a logic analyzer. **Supplementary Figure S5A** shows the waveform for the temperature reading by the sensor and the temperature transmitted by the LoRa node. Our simple comparison logic implemented in a testing program can detect whether the attack is triggered (bus 7 is high as shown in **Supplementary Figure S5B**).

Both IDE monitoring and logic analyzer based detection are not a ascalable Trojano detection approach, as they typically require precise control on the timing and the prior knowledge of the expected abnormal behaviors. Unfortunately, it is not

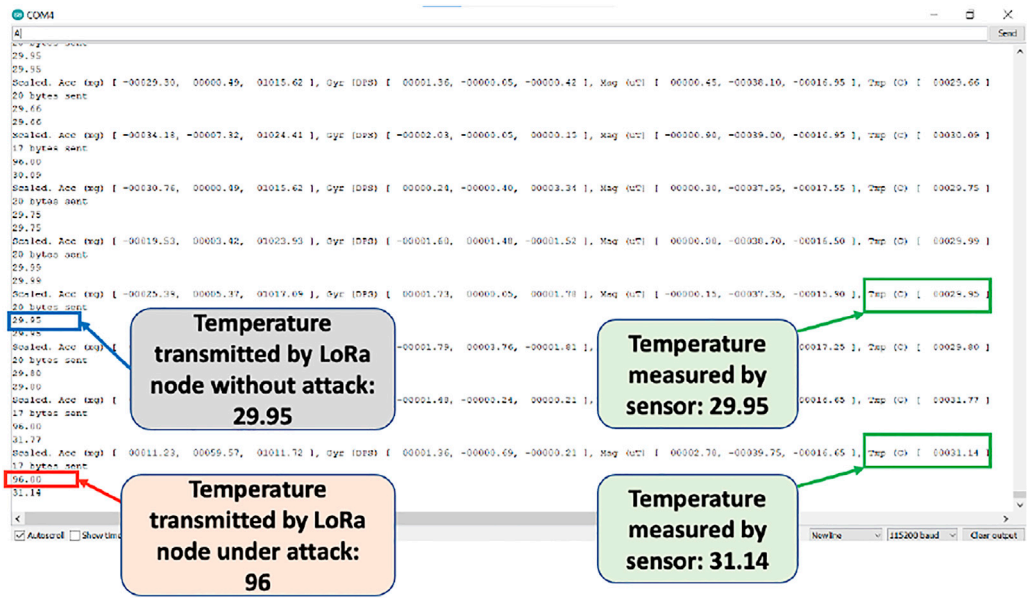

FIGURE 7 | Sensor temperature transmitted by a LoRa node before and after attack.

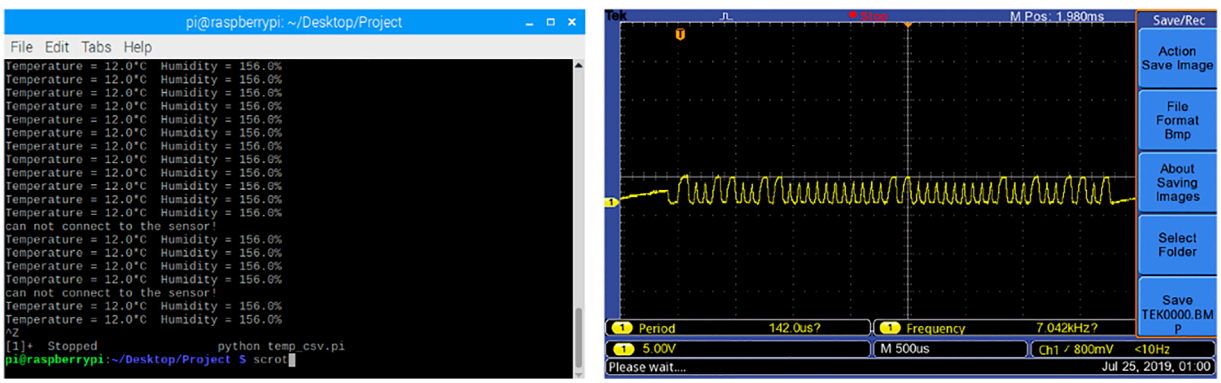

FIGURE 8 | Results of the analog Trojan attack on a sensing node showing data interruption.

practical to execute such Trojan detection procedure in real applications. Therefore, hardware Trojan detection for sensor networks needs more investigation from the sensor community.

In another case study, we implemented an analog Trojan attack on the single wire data line of the sensor. As shown in **Figure 6**, a capacitor was added between the temperature and humidity sensor and the ground data line. The sensor receives the request signal from the Raspberry Pi and completes the successful handshaking between the sensor and the Raspberry Pi. When the sensor starts to transfer data, and the capacitor (analog Trojan) completes the path to the ground will begin to alter the sensor transmitting data end device, as shown in **Figure 8**.

4.2.2 MITM Attack: Leak Sensor Information

Man-In-The-Middle (MITM) attack is a physical attack that can be performed on a LoRa node (sensing node) shown in **Figure 9**. As sensors transmit data to end devices and are usually vulnerable, no encryption is not implemented on the sensor side. An adversary can target the communication protocol between the sensor and the node device and activate some malicious logic at the end node. The adversary can implement a Trojan circuit during the third-party fabrication process. Malicious logic such as restarting the LoRa node will cause the node to re-advertise the network session key. A SDR device can capture the radio packets containing the key. As all LoRa nodes in the same network transmit data to all existing LoRa gateway, it is challenging to differentiate the LoRa packets injected by the MITM attack from those transmitted by the legitimate LoRa nodes. Any monitoring mechanisms at the LoRa node will enable to shorten the process of MITM attack detection. However, such a detection mechanism comes with the disadvantage of more power consumption at end devices.

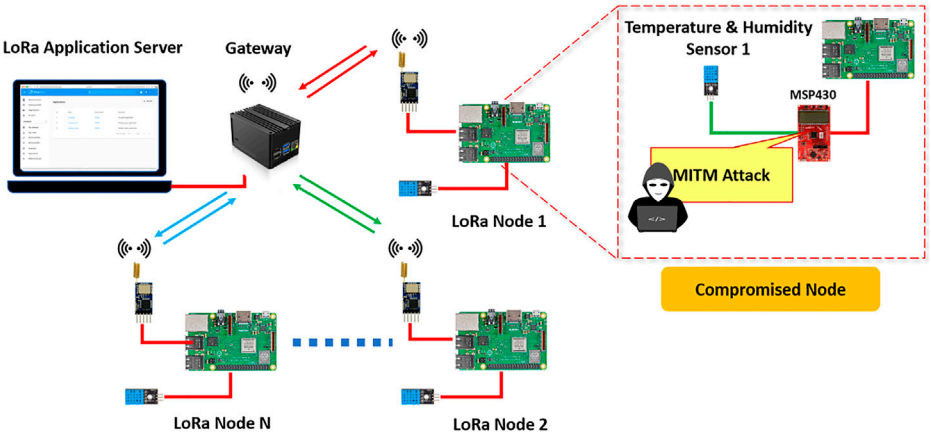

FIGURE 9 | An example of MITM attack on a LoRa node (sensing node).

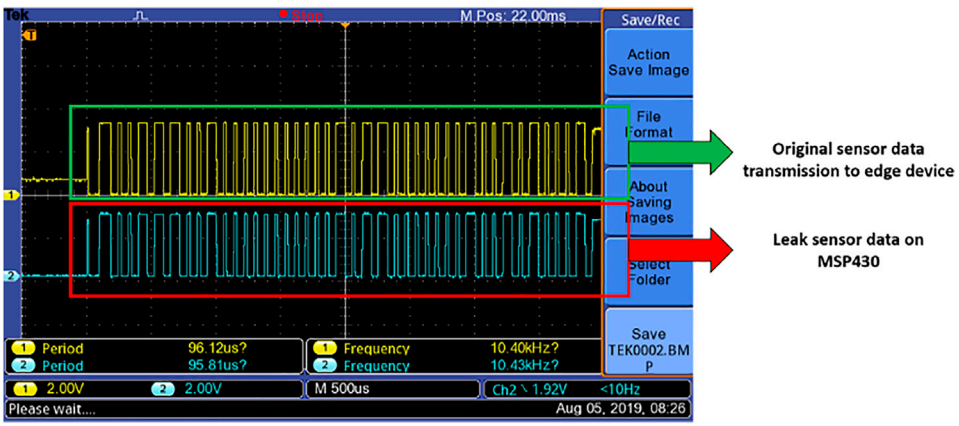

FIGURE 10 | Results of the MITM attack on a sensing node showing information leaking.

In our MITM case study, a microcontroller (MSP430FR6989) was adopted to implement the MITM attack between a digital temperature and humidity sensor (DHT11) and a signal processing node formed by a single-board computer (Raspberry Pi 3B+). The microcontroller receives the request signal from the Raspberry Pi and relays the request to the sensor. After the successful handshaking between the sensor and the Raspberry Pi, the sensor starts to transfer data through the middle hop, the MSP340 microcontroller, to the processing node. As the microcontroller has the power to manipulate the data (e.g., bitwise operation, bounding, or addition or subtraction) during the transmission, the MITM attack is able to leak the measurement value or alter it before reaching the application server. We used an oscilloscope to monitor the signal through the microcontroller. As shown in **Figure 10**, the data sent by the sensor is successfully captured and leaked by the microcontroller.

4.2.3 Jamming and Replay Attacks: Deplete Sensor Network Bandwidth

Attacks in sensing nodes could further impact the network performance. Jamming and replay attacks are the ones leading the depletion of network bandwidth. In this section, we zoom in how a compromised sensing node could facilitate jamming or replay attacks.

The jamming attack is the process of interrupting communications by broadcasting data over the same network. In our case study, we conducted a constant jamming attack, which sends out data continuously at the frequency of 915 MHz, not hopping around to other frequencies due to the constraint of the carrier frequency allocated to LoRa in US. We used a low-end LoRaWAN compatible IoT device, Arduino MKR WAN 1300 Arduino (2021) to implement four LoRa nodes, three for legitimate communication and one for jamming attack. We monitored the physical transmission of LoRa packets through GQRX software Alexandru Csete (2021). **Figure 11A** shows the packets for the normal LoRa packet transmission without jamming attack. As shown, the packets are being dispersed over a constant transmission rate. After we initiated the jamming attack, a large volume of LoRa packets were intensively injected to the LoRa network and they were centered around the frequency of 915 MHz, as shown in **Figure 11B**.

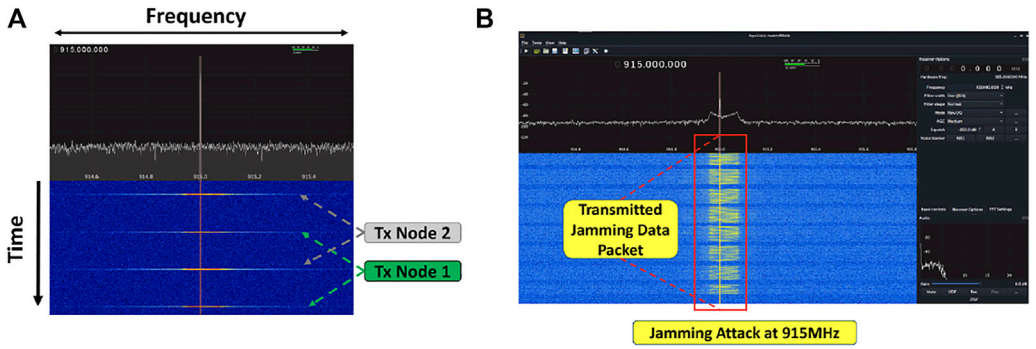

FIGURE 11 | LoRa packet transmission history for the case **(A)** without attack and **(B)** with a successful jamming attack.

The attack example shown in **Figure 11B** is one kind of jamming attacks—constant jamming attack. There are many other types, including random, reactive, and selective jamming attacks Raymond and Midkiff (2008); Sufyan and Saqib (2013). Those attacks are more stealthy than the constant jamming attack, as their triggering moments do not follow a predictable pattern and the induced malicious packets are time intensive.

The replay attack is a process of intercepting data from a particular communication medium and then sending either the same data or an altered version to the communication stream. We continue to use a Arduino MKR WAN 1300 to conduct a replay attack, which interfered the communication between the legitimate LoRa nodes and gateways in the LoRaWAN. The replay attack allows an adversary to gain unauthorized access to LoRa packets and further alter that data for malicious reasons. As shown in **Supplementary Figure S6A**, our attack successfully replied the LoRa message that is highlighted by the red rectangle boxes. Note that our replay attack further altered the original message. The observation of frequency spectrum shown in **Supplementary Figure S6B** indicates how the replay attack occupies the channel bandwidth and its time density. Compared with the jamming attack shown in **Figure 11B**, the replay attack causes less bandwidth depletion.

5 CHALLENGES ON DETECTING AND MITIGATING PHYSICAL ATTACKS IN SENSOR NETWORKS

We analyze the observation from our case studies and summarize the challenges on detecting and mitigating the physical attacks on the sensor network applied in the John Olson Advanced Manufacturing Center.

5.1 Challenge 1: Weak Side-Channel Signals

Side-channel signals have been widely used in hardware Trojan detection Narasimhan et al. (2013); Jin and Makris (2008). We extracted two types of typical side-channel signals from our case studies to assess if we can exploit those signals to detect the active compromised LoRa nodes in the LoRaWAN.

The first side-channel signal is the power consumption of a LoRa node device. Each LoRa node in our case study was powered by a 5V-supply. We inserted a small resistor between the external voltage source and the voltage input pin of the LoRa device to measure the voltage drop on the resistor and thus calculate the power consumption of the LoRa node. In a compromised LoRa node, we emulated a hardware Trojan in the hardware module for the SPI communication interface. The Trojan will be triggered by an external event (e.g., a special temperature range) and its payload will tamper with the data provided by the temperature sensor or accelerometer sensor before forming LoRa packets (thus the data encryption does not help to protect the data from this Trojan attack). As shown in **Supplementary Figures S7A,B**, once the Trojan is triggered, there will be a stable voltage glitch, whose magnitude is only 3.6 and 1.6% of the supply voltage, respectively. Although the duration and magnitude of the voltage glitch slightly vary with the content that the LoRa node is transmitting, a simple but powerful hardware Trojan only leads to negligible change on the side-channel signal, voltage fluctuation (and then power).

The second side-channel signal is transmission latency of LoRa packets. In this case study, we compare the latency for Trojan free, a Trojan with simple logic function (simple mathematical calculation), and an advanced Trojan with complicated logic (complex mathematical iteration). The timestamps of each LoRa packet (PKT) were collected from the log files of Arduino IDE, gateway, and the data extraction from the upstream JSON object in the LoRa application. By analyzing the timestamps, we obtained the latency of LoRa packet transmission. As shown in **Figure 12**, the latency overhead induced by a hardware Trojan in the LoRa node is not significant: the latency for the sensor-to-node transmission is increased by 0.033 s and the latency increase from the node to gateway is only 3.29% over the Trojan-free case. Based on our case study, we believe that the delay-based Trojan detection may lead to a high false positive/negative detection rate.

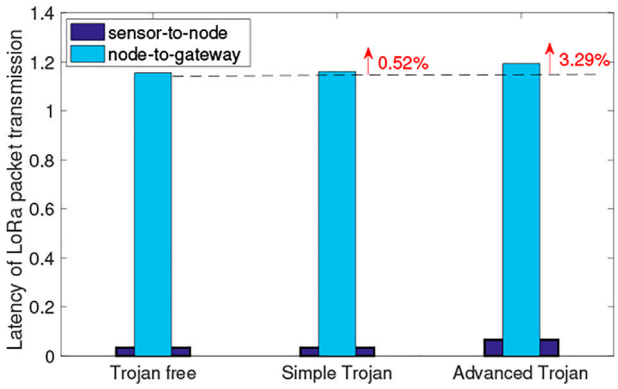

FIGURE 12 | Impact of hardware Trojan in a LoRa node device on the transmission latency of LoRa packets.

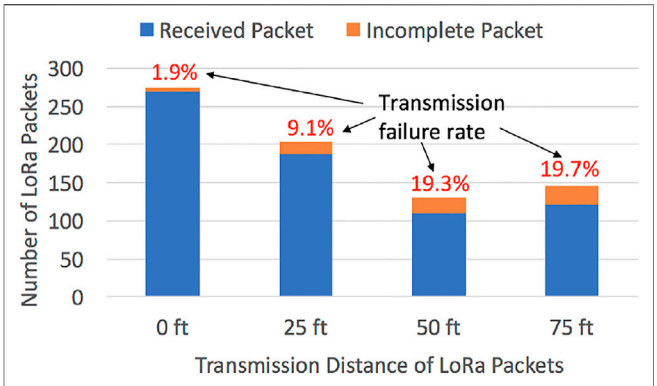

FIGURE 13 | Impact of the distance between LoRa transmitter and receiver on LoRa packet transmission.

5.2 Challenge 2: Single Carrier Frequency and Narrow Channel Bandwidth

In LoRaWAN, the primary frequency for LoRa packet transmission is 915 MHz and the channel bandwidth is 125–500 kHz for US spectrum bands. Although LoRa nodes are implemented with low-power devices, they provide for long-range communications: up to 10 miles (15 km) or more in rural areas. The fact that all LoRa packets are transmitted through a narrow spectrum bandwidth and a LoRaWAN covers a wide area significantly increases the difficulty of differentiating a legitimate LoRa packet from the malicious ones induced by a jamming or replay attack.

In the specification of LoRaWAN, the spreading factor (SF) is designated to control the time interval that each LoRa packet transmission will take. **Supplementary Figure S8** shows the spectrum of transmitted packets at SF = 0, SF = 6, and SF = 12, respectively. If an attack is performed by a malicious LoRa node configured with a lower SF, the attack effect could be immersed in the spectrum of the normal packets and the LoRaWAN communication channels will not be depleted dramatically in a short period of time. Thus, a simple frequency-domain monitoring will not be sufficient to detect such attacks.

The channel bandwidth is another critical parameter for LoRa node configuration. **Supplementary Figure S9** shows the spectrum of LoRa packets that are transmitted with a channel bandwidth of 125, 150, and 250 KHz. If the channel bandwidth is set to small for the purpose of power saving, the LoRa packet receiver may not be able to obtain the complete LoRa packets. Consequently, there will be natural LoRa packet dropping. This leaves an exploration space for attackers to insert malicious packets via one kind of jamming attacks or replay attacks without bringing in significant changes on the signal density in the frequency spectrum.

5.3 Challenge 3: Natural Packet Drop

With the setup shown in **Figure 2**, we monitored the real-time LoRa packets that carry the accelerometer measurement for the manufacturing tips' movement on X, Y, and Z directions at the transmission distance of 0, 25, 50, and 75 feet (ft). As shown in **Figure 13**, more incomplete LoRa packets are received and the LoRa transmission failure rate increases as the distance between transmitter and receiver increases. We consider the incomplete packets either missing a fraction of sensor data or carrying an invalid data as a natural packet drop. Theoretically, LoRaWAN supports long-range communication. However, as the LoRa node is typically formed by a low-power device, the success rate of LoRa packet transmission naturally decreases with the increasing communication distance of LoRa packets. It is challenging to differentiate the loss of packet integrity caused by the LoRa itself or by a compromised LoRa device. Moreover, our practical experiments reveal that the number of packet transmission failures will vary if the environment has more obstacles and other interference source for LoRa transmission. Thus, it is difficult to establish a golden reference for attack detection. If we detect the malicious LoRa nodes by simply examining the success packet transmission rate, we could have a high false-positive detection rate. Based on the LoRa log files and external measurement results, we will extract the features of LoRa transmission in both timing and frequency domains and then apply them to the presentable machine learning algorithms (e.g., supervised learning Caruana and Niculescu-Mizil (2006) and reinforcement learning Sutton and Barto (2018)) to differentiate the natural packet drop and the attack induced packet loss.

6 CONCLUSION

Sensors and sensor networks collect and process information from remote places and have significantly benefit applications like home and vehicle automation, intelligent transportation, environmental monitoring, remote healthcare, and surveillance. However, due to the limited budget on power consumption in sensors and local processing nodes, sensor nodes do not include security features such as advanced data encryption and device authentication. As a

result, sensor networks are vulnerable to attacks from cyber space to local users. It is challenging to assure the integrity and trustworthiness of sensor networks. In this work, we analyze the security threats in the sensor network deployed in LoRaWAN. This work demonstrate practical physical attacks on LoRa node devices and analyzes the challenges of detecting and mitigating those attacks. Based on our laboratory experiments and on-site measurement in an advanced manufacturing center, we conclude that it is not practical to use the side-channel signals (power and delay) to detect the compromised LoRa nodes in the LoRaWAN. This is due to the unique low-power nature of LoRa node devices and the constraints of the LoRa transmission frequency and spectrum bands. In future work, we will investigate effect attack mitigation methods for sensor networks.

DATA AVAILABILITY STATEMENT

The original contributions presented in the study are included in the article/**Supplementary Materials**, further inquiries can be directed to the corresponding author.

AUTHOR CONTRIBUTIONS

MR conducted most of the experiments. JH programed LoRa nodes. JC performed jamming and replay attacks. MM contributed to the survey on sensors. JR provided the experiment facility in Olson Center. KM and ES provided the discussion of sensor network background information and applications QY led this project.

FUNDING

This work is partially supported by National Science Foundation Grant CNS-1652474 and UNH Collaborative Research Excellence (CoRE) IWG Project.

SUPPLEMENTARY MATERIAL

The Supplementary Material for this article can be found online at: https://www.frontiersin.org/articles/10.3389/fsens.2022.850056/full#supplementary-material

Supplementary Figure 1 | Overview of basic LoRa network architecture.

Supplementary Figure 2 | Overview of LoRa network security protocols.

Supplementary Figure 3 | Sensor data transmission venerability and attack implementation from low level to high level of LoRa sensor network.

Supplementary Figure 4 | LoRa network security challenges due to key management system and low powered end devices.

Supplementary Figure 5 | Logic analyzer readings **(A)** before and **(B)** after attack.

Supplementary Figure 6 | Successful replay attack confirmed by **(A)** the transmission log saved by Arduino IDE and **(B)** real-time frequency-domain observation.

Supplementary Figure 7 | Hardware Trojan induced variation on the side-channel signal—voltage drop on the resistor assisting in measuring power consumption of a LoRa node transmitting **(A)** temperature sensor and **(B)** accelerometer sensor values.

Supplementary Figure 8 | Impact of spread factor on the malicious node transmission.

Supplementary Figure 9 | Bandwidth effects on the malicious node transmission.

REFERENCES

Abdulkarem, M., Samsudin, K., Rokhani, F. Z., and A Rasid, M. F. (2020). Wireless Sensor Network for Structural Health Monitoring: A Contemporary Review of Technologies, Challenges, and Future Direction. *Struct. Health Monit.* 19, 693–735. doi:10.1177/1475921719854528

Agnihotri, R. B., Singh, A. V., and Verma, S. (2015). "Challenges in Wireless Sensor Networks with Different Performance Metrics in Routing Protocols," in 2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), 1–5. doi:10.1109/ICRITO.2015.7359295

Ahmad, I., Shah, K., and Ullah, S. (2016). Military Applications Using Wireless Sensor Networks: A Survey. *Int. J. Eng. Sci. Comput.* 6.

Alawad, H., and Kaewunruen, S. (2018). Wireless Sensor Networks: Toward Smarter Railway Stations. *Infrastructures* 3, 24. doi:10.3390/infrastructures3030024

[Dataset] Alexandru Csete, C. S. (2021). Welcome to Gqrx. Available at: https://gqrx.dk/.

Alías, F., and Alsina-Pagès, R. M. (2019). Review of Wireless Acoustic Sensor Networks for Environmental Noise Monitoring in Smart Cities. *J. Sensors* 2019, 1–13. doi:10.1155/2019/7634860

Aras, E., Ramachandran, G. S., Lawrence, P., and Hughes, D. (2017). "Exploring the Security Vulnerabilities of Lora," in 2017 3rd IEEE International Conference on Cybernetics (CYBCONF), 1–6. doi:10.1109/CYBConf.2017.7985777

[Dataset] Arduino (2021). MKR WAN 1300 | Arduino Documentation | Arduino Documentation. Available at: https://docs.arduino.cc/hardware/mkr-wan-1300.

Ayyildiz, C., Erdem, H. E., Dirikgil, T., Dugenci, O., Kocak, T., Altun, F., et al. (2019). Structure Health Monitoring Using Wireless Sensor Networks on Structural Elements. *Ad Hoc Networks* 82, 68–76. doi:10.1016/j.adhoc.2018.06.011

Azzabi, T., Farhat, H., and Sahli, N. (2017). "A Survey on Wireless Sensor Networks Security Issues and Military Specificities," in 2017 International Conference on Advanced Systems and Electric Technologies (IC_ASET), 66–72. doi:10.1109/aset.2017.7983668

Caruana, R., and Niculescu-Mizil, A. (2006). "An Empirical Comparison of Supervised Learning Algorithms," in ICML '06: Proceedings of the 23rd International Conference on Machine Learning (New York, NY, USA: Association for Computing Machinery), 161–168. doi:10.1145/1143844.1143865

Choi, C.-S., Jeong, J.-D., Lee, I.-W., and Park, W.-K. (2018). "LoRa Based Renewable Energy Monitoring System with Open IoT Platform," in 2018 Intl. Conf. on Electronics, Info., and Communication, 1–2. doi:10.23919/ELINFOCOM.2018.8330550

de Moraes, P., and da Conceição, A. F. (2021). A Systematic Review of Security in the Lorawan Network Protocol. *CoRR abs/2105.00384*.

[Dataset] ENISA (2019). Industry 4.0 - Cybersecurity Challenges and Recommendations. Available at: Online https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations (Accessed May 20, 2019).

[Dataset] Forstater, J. D. (2014). *Tomographic Motion Detection*.

Fukushima, K., Marion, D., Nakano, Y., Facon, A., Kiyomoto, S., and Guilley, S. (2020). "Evaluation of Side-Channel Key-Recovery Attacks on Lorawan End-Device," in *Information Systems Security and Privacy*. Editors P. Mori, S. Furnell, and O. Camp (Cham: Springer International Publishing), 74–92. doi:10.1007/978-3-030-49443-8_4

Fukushima, K., Marion, D., Nakano, Y., Facon, A., Kiyomoto, S., and Guilley, S. (2019). "Experiment on Side-Channel Key-Recovery Using a Real Lpwa End-

Device," in Proceedings of the 5th International Conference on Information Systems Security and Privacy - ICISSP,. INSTICC (Setúbal, Portugal: SciTePress), 67–74. doi:10.5220/0007259500670074

Gaber, T., Abdelwahab, S., Elhoseny, M., and Hassanien, A. E. (2018). Trust-based Secure Clustering in WSN-Based Intelligent Transportation Systems. *Computer Networks* 146, 151–158. doi:10.1016/j.comnet.2018.09.015

Han, J., and Wang, J. (2018). An Enhanced Key Management Scheme for Lorawan. *Cryptography* 2, 34. doi:10.3390/cryptography2040034

Hanif, S., Khedr, A., Al Aghbari, Z., and Agrawal, D. (2018). Opportunistically Exploiting Internet of Things for Wireless Sensor Network Routing in Smart Cities. *Jsan* 7, 46. doi:10.3390/jsan7040046

He, W., Breier, J., Bhasin, S., Miura, N., and Nagata, M. (2017). "An Fpga-Compatible Pll-Based Sensor against Fault Injection Attack," in 2017 22nd Asia and South Pacific Design Automation Conference (ASP-DAC), 39–40. doi:10.1109/ASPDAC.2017.7858291

[Dataset] Industries, T. T. (2021). What Is a Lorawan Network Server? Available at: https://www.thethingsindustries.com/docs/reference/components/application-server/.

Kiani, F., and Seyyedabbasi, A. (2018). Wireless Sensor Network and Internet of Things in Precision Agriculture. *ijacsa* 9. doi:10.14569/IJACSA.2018.090614

Minhas, U. I., Naqvi, I. H., Qaisar, S., Ali, K., Shahid, S., and Aslam, M. A. (2018). A WSN for Monitoring and Event Reporting in Underground Mine environmentsConference Name. *IEEE Syst. JournalIEEE Syst. J.* 12, 485–496. doi:10.1109/JSYST.2016.2644109

Mohamed, N., Jawhar, I., Al-Jaroodi, J., and Zhang, L. (2011). Sensor Network Architectures for Monitoring Underwater Pipelines. *Sensors* 11, 10738–10764. doi:10.3390/s111110738

Monjur, M. R., Sunkavilli, S., and Yu, Q. (2020). "Adobf: Obfuscated Detection Method against Analog Trojans on I2c Master-Slave Interface," in 2020 IEEE 63rd International Midwest Symposium on Circuits and Systems (MWSCAS), 1064–1067. doi:10.1109/MWSCAS48704.2020.9184680

Muduli, L., Mishra, D. P., and Jana, P. K. (2018). Application of Wireless Sensor Network for Environmental Monitoring in Underground Coal Mines: A Systematic Review. *J. Netw. Comput. Appl.* 106, 48–67. doi:10.1016/j.jnca.2017.12.022

Munir, S. A., Bin, Y. W., Biao, R., and Jian, M. (2007). "Fuzzy Logic Based Congestion Estimation for Qos in Wireless Sensor Network," in 2007 IEEE Wireless Communications and Networking Conference, 4336–4341. doi:10.1109/WCNC.2007.791

Narasimhan, S., Du, D., Chakraborty, R. S., Paul, S., Wolff, F. G., Papachristou, C. A., et al. (2013). Hardware Trojan Detection by Multiple-Parameter Side-Channel Analysis. *IEEE Trans. Comput.* 62, 2183–2195. doi:10.1109/tc.2012.200

Ng, X. T., Naj, Z., Bhasin, S., Roy, D. B., Danger, J.-L., and Guilley, S. (2015). "Integrated Sensor: A Backdoor for Hardware Trojan Insertions?," in 2015 Euromicro Conference on Digital System Design, 415–422. doi:10.1109/DSD.2015.119

Noura, H., Hatoum, T., Salman, O., Yaacoub, J.-P., and Chehab, A. (2020). Lorawan Security Survey: Issues, Threats and Possible Mitigation Techniques. *Internet of Things* 12, 100303. doi:10.1016/j.iot.2020.100303

[Dataset] Olson, J. (2021). John Olson Advanced Manufacturing center. Available at: https://ceps.unh.edu/Olson-Center.

Oniga, B., Dadarlat, V., De Poorter, E., and Munteanu, A. (2017). "Analysis, Design and Implementation of Secure LoRaWAN Sensor Networks," in 2017 13th IEEE International Conference on Intelligent Computer Communication and Processing (ICCP), 421–428. doi:10.1109/ICCP.2017.8117042

Papadogiannaki, E., and Ioannidis, S. (2021). A Survey on Encrypted Network Traffic Analysis Applications, Techniques, and Countermeasures. *ACM Comput. Surv.* 54, 1–35. doi:10.1145/3457904

Petajajarvi, J., Mikhaylov, K., Roivainen, A., Hanninen, T., and Pettissalo, M. (2015). "On the Coverage of Lpwans: Range Evaluation and Channel Attenuation Model for Lora Technology," in 2015 14th International Conference on ITS Telecommunications (ITST), 55–59. doi:10.1109/ITST.2015.7377400

Polonelli, T., Brunelli, D., Marzocchi, A., and Benini, L. (2019). Slotted Aloha on Lorawan-Design, Analysis, and Deployment. *Sensors* 19, 838. doi:10.3390/s19040838

Raymond, D. R., and Midkiff, S. F. (2008). Denial-of-service in Wireless Sensor Networks: Attacks and Defenses. *IEEE Pervasive Comput.* 7, 74–81. doi:10.1109/MPRV.2008.6

Reynders, B., Meert, W., and Pollin, S. (2016). "Range and Coexistence Analysis of Long Range Unlicensed Communication," in 2016 23rd International Conference on Telecommunications (ICT), 1–6. doi:10.1109/ICT.2016.7500415

Rocha, F., and Correia, M. (2011). "Lucy in the Sky without Diamonds: Stealing Confidential Data in the Cloud," in 2011 IEEE/IFIP 41st Intl. Conf. on Dependable Systems and Networks Workshops, 129–134. doi:10.1109/DSNW.2011.5958798

Schellenberg, F., Gnad, D. R. E., Moradi, A., and Tahoori, M. B. (2018). "An inside Job: Remote Power Analysis Attacks on Fpgas," in 2018 Design, Automation Test in Europe Conference Exhibition (DATE), 1111–1116. doi:10.23919/DATE.2018.8342177

Sehrawat, D., and Gill, N. S. (2019). "Smart Sensors: Analysis of Different Types of Iot Sensors," in 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI) (Tirunelveli, India: IEEE), 523–528. doi:10.1109/icoei.2019.8862778

Singh, A., Aggarwal, P., and Arora, R. (2016). "Iot Based Waste Collection System Using Infrared Sensors," in 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO) (Noida, India: IEEE), 505–509. doi:10.1109/icrito.2016.7785008

Sufyan, N., Saqib, M., and Zia, N. A. (2013). Detection of Jamming Attacks in 802.11b Wireless Networks. *EURASIP J. Wireless Commun. Networking* 208. doi:10.1186/1687-1499-2013-208

Sutton, R. S., and Barto, A. G. (2018). *Reinforcement Learning: An Introduction*. Cambridge, MA, USA: MIT press.

Thakur, D., Kumar, Y., Kumar, A., and Singh, P. K. (2019). Applicability of Wireless Sensor Networks in Precision Agriculture: A Review. *Wireless Pers Commun.* 107, 471–512. doi:10.1007/s11277-019-06285-2

Ullo, S. L., and Sinha, G. R. (2020). Advances in Smart Environment Monitoring Systems Using IoT and Sensors. *Sensors* 20, 3113. doi:10.3390/s20113113

Xu, G., Shen, W., and Wang, X. (2014). Applications of Wireless Sensor Networks in marine Environment Monitoring: A Survey. *Sensors* 14, 16932–16954. doi:10.3390/s140916932

Yang, X., Karampatzakis, E., Doerr, C., and Kuipers, F. (2018). "Security Vulnerabilities in LoRaWAN," in 2018 IEEE/ACM 3rd Intl. Conf. on Internet-of-Things Design and Implementation, 129–140. doi:10.1109/IoTDI.2018.00022

Yier Jin, Y., and Makris, Y. (2008). "Hardware Trojan Detection Using Path Delay Fingerprint," in 2008 IEEE International Workshop on Hardware-Oriented Security and Trust, 51–57. doi:10.1109/HST.2008.4559049

Zhou, Q., Zheng, K., Hou, L., Xing, J., and Xu, R. (2019). Design and Implementation of Open Lora for Iot. *IEEE Access* 7, 100649–100657. doi:10.1109/ACCESS.2019.2930243

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors, and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.