An Attack Analysis Framework for LoRaWAN Applied Advanced Manufacturing

Mohammad Mezanur Rahman Monjur, Joseph Heacock, Rui Sun, and Qiaoyan Yu
Department of Electrical and Computer Engineering
University of New Hampshire
Durham, NH 03824
Email:qiaoyan.yu@unh.edu

***Abstract*—Advanced manufacturing is transitioning into automated production, which enables the remote system monitoring, increases the online system configuration, and thus reduces the overall cost on workforce. However, the remote access to production plants makes advanced manufacturing vulnerable to various security attacks from physical devices to cyber space. The traditional assumptions on the security of manufacturing plants do not hold true any longer. It is imperative to perform holistic assessment on the emerging security vulnerabilities in advanced manufacturing network. In this work, we propose an attack analysis framework to enable the comprehensive assessment on the potential attacks that challenge the advanced manufacturing factories. As the long-range wide-area network (LoRaWAN) is commonly applied in advanced manufacturing sites, we examine the security weaknesses in commercial LoRa nodes, gateways, and LoRaWAN connection in this work. Jamming attack, replay attack, and man-in-the-middle attack from physical and cyber access are analyzed in this work. The security vulnerabilities disclosed from the proposed framework have great potential to facilitate the development of effective defense methods for advanced manufacturing industries in future[1].**

***Index Terms*—Cybersecurity, LoRa, LoRaWAN, sensor network, advanced manufacturing, jamming attack, replay attack, man-in-the-middle attack.**

I. Introduction

The current industry is transitioning into an automated production system through smart technologies. Due to the connection to the cyber space, advanced manufacturing is unavoidably challenged by cybersecurity issues. The cyber threats from nation-states and international organizations are continuously growing over the years. For instance, an adversary can gain unauthorized access to an individual's or organization's network to disrupt or steal intellectual property and sensitive data. Data leakage or malicious modification caused by cyber attacks will result in severe effects on the production line in manufacturing industries. According to the Cybersecurity Ventures, the damage cases related to cyber threat was projected to hit 6 trillion annually by 2021 [1]. Consequently, there is a pressing need to examine the potential attack surfaces that cyber attackers could use to harm the advanced manufacturing industries.

Long-Range (LoRa) ratio technology has been widely used in automated manufacturing industries due to its low power and long-range capability. As a critical part of advanced manufacturing, LoRa nodes are mainly used for sensor-based applications to monitor the industrial system and provide the primary control system with real-time data feedback via Long-Range Wide-Area Network (LoRaWAN). LoRaWAN is a low-power wireless modulation technique based on Chirp Spread Spectrum. The spread spectrum modulated is robust against disturbances, and long-distance data transmission can be achieved. In general, LoRaWAN is considered secure since it includes some security features such as data origin authentication and integrity [2]. Advanced Encryption Standard (AES) is commonly adopted in LoRaWAN to protect the end-to-end security. Cipher-based Message Authentication Code (CMAC) algorithm is also used to assure the message integrity and authenticity [2]. However, the assurance on security varies with the deployed network connection method. LoRaWAN uses a chirp-spread-spectrum modulation at the physical layer and supports two different network connection methods: Over-The-Air Activation (OTAA) and Activation by Personalization (ABP). A LoRa node for OTAA does not embed the application key in the LoRa node device for joining the network and the one using ABP has the key embedded in the device itself. In ABP activation, the LoRa node has a fixed 32-bit device address and the session keys for network connection [3]. The hardcoded key in ABP device makes the LoRa node more vulnerable to A distributed denial-of-service (DDoS) attack than an OTAA device.

Despite the many benefits offered by LoRaWAN, the security vulnerabilities in LoRaWAN has not been widely investigated. In this work, we analyze the existing commercial LoRa node devices and project the potential attack surfaces. A proposed framework will be discussed to identify critical vulnerability and possible solutions. The rest of this work is organized as follows. Section II provides an overview of the attack scenarios that could happen in advanced manufacturing sites or networks. Section III briefly introduces the main characteristics of LoRa node devices, gateways, network servers, and communication protocols in LoRaWAN. In Section IV, we propose a holistic attack analysis framework for the LoRaWAN applied in advanced manufacturing. We present three case studies in Section V. This work is concluded in Section VI.

[1]This work is partially supported by NSF award CNS-1652474.

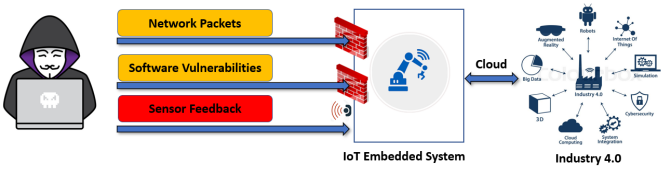


Fig. 1. Attack scenarios in advanced manufacturing network.

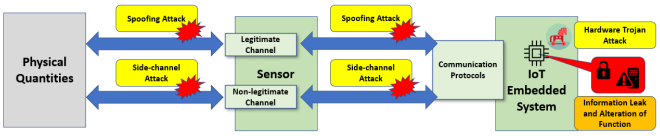


Fig. 2. Attack surfaces in the physical network of advanced manufacturing industry.

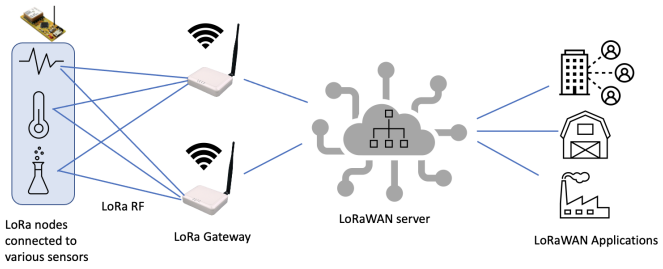


Fig. 3. Overview of a simplified LoRaWAN.

II. Overview for Attach Scenarios in Advanced Manufacturing Network

A. Attacks from Cyber Space

Cyber-attack leads to a catastrophic effect on advanced manufacturing. A cyber-attack is usually carried out by a malicious program to leak information from a targeted attack to disrupt the normal operation flow. Automated manufacturing systems heavily rely on IoT networks to gather the real-time status of the equipment and then control them accordingly. An IoT network is often integrated with an embedded software platform and wireless communication technologies. Some of the manufacturing plants still run on old version operating system such as Windows XP or Windows 7. They are subject to worm attacks as they do not have a host Firewall [4]. Once the office network is compromised, the connected server will be compromised as well. Consequently, the tampered operating system will yield a catastrophic effect on the manufacturing network. Any fault in the production line will cause a stall supply chain and result in revenue loss.

Recently, a meat processing plant, JBS, paid an $11 million ransom after the plant was halted due to significant ransomware attacks [5]. Any type of insecure wireless network is the subject of a cyber-attack manufacturing network. In 2013, the malfunction in Austrian and German power grid was induced by a self-inflicted DDoS attack and flooded the central command center with traffic [6]. The DDoS attack can temporarily block the LoRaWAN units with the central operation. As a result, the manufacturing plant operation will lose the monitoring capability of sensitive sensor data.

There are many prevention and detection mechanisms for software and network vulnerability [7], [8]. For instance, as shown in Fig. 1, malicious network traffics, and software vulnerabilities can be prevented by using a firewall. Depending on the requirements firewall can have different operations and consider first defense against malware and virus. The firewall blocks most of the distributed denial-of-service (DDoS) attacks, port scanning attacks, and computer worms [9]–[12]. However, IoT networks sometimes blindly trust network traffics (sensor data), and thus making it challenging to prevent attacks [13].

B. Physical Attacks on Sensing and Data Processing Nodes

As a critical part of revolutionizing the automation of industry 4.0, sensors are used as passive and active modes to measure the physical properties of the surrounding environment. An adversary can take advantage of the sensor network vulnerability and carry out malicious activity. Figure 2 depicts three types of attacks: spoofing attacks, side-channel attacks, and hardware Trojan attacks.

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 [14]; as a result, the raw data collected by a sensor could be altered before reaching the storage or processing unit connected with that sensor. For example, an adversary can reverse engineer communication protocols such as (I^2C), SPI, and UART [15]. Therefore adversary can alter the sensor data conversion and the sensor mechanism to launch spoofing and fault injection attacks [16].

Many side-channel attack studies have pointed out vulnerability for LoRaWAN protocols. The LoRa node is subject to side-channel attack as the authors demonstrated recover AES-128 keys used for transmitted packets using correlation power analysis [17]. 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 [18].

Sensors transmit the data to the embedded system through the network and 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, they can cause severe data breaches or alteration of instruction to the system.

III. Introduction of 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 Fig. 3. LoRa nodes are end devices, which are mainly configured as slave devices to sense surrounding environmental data and transmit data packets to the cloud.

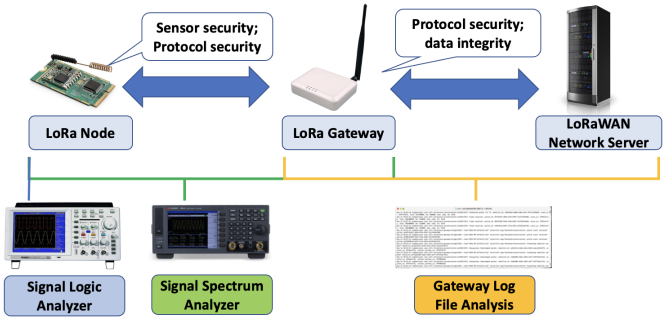


Fig. 4. Proposed holistic attack analysis framework for LoRaWAN security.

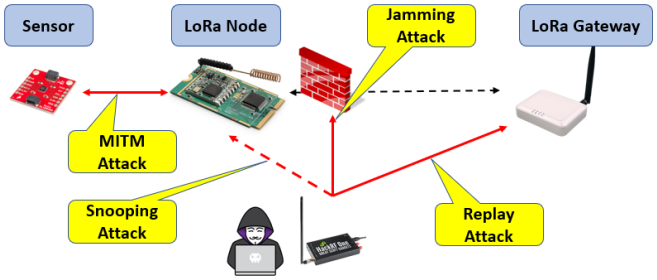


Fig. 5. Attack scenarios in LoRaWAN.

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 [19].

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 [20].

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 [20].

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 [21].

IV. Proposed Attack Analysis Framework

A. Overview of Proposed Framework

We propose a framework to facilitate the investigation of various attacks on a LoRaWAN. Figure 4 provides an overview of the proposed framework to enable the security threats in LoRa end nodes, gateways, and servers. Various attacks can be performed in a LoRaWAN. An attacker can tamper with the sensing device to alter the original sensed value, harming the data integrity. An adversary can sniff and capture the transmitted packet between nodes and gateways. An adversary can also capture the LoRa packets via some open-source hardware (e.g., Software-Defined Radio (SDR) device). Even if not knowing the encryption key applied in the LoRa packet, an attacker can still impersonate a LoRa node and replay the captured packets to the LoRa 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, data rate, etc. Analyzing this information under normal conditions and under 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.

Figure 4 highlights the attacks on edge node and LoRaWAN gateway devices and their connection network. In the following sections, we demonstrate three attack scenarios, a Man-in-the-Middle attack (MITM) on the node side, a jamming attack and a replay attack during the LoRa packet transmission. 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, including sensing nodes, LoRa node devices, LoRa gateways, and LoRa servers.

B. Attack Assessment

1) Jamming Attack: Jamming attack is a common attack carried out by an adversary to disrupt the normal network operation by increasing the transmission loss of valid LoRa packets. A jamming attack scenario is shown in Fig. 5. In this case, the adversary will access a SDR device to generate some unwanted signals in the target frequency range and inject them to the LoRa network. Any unwanted interference with the valid signals transmitted by LoRa nodes will degrade the signal and result in the packet loss at the gateway. The packet loss can be detected by analyzing the gateway log files to see

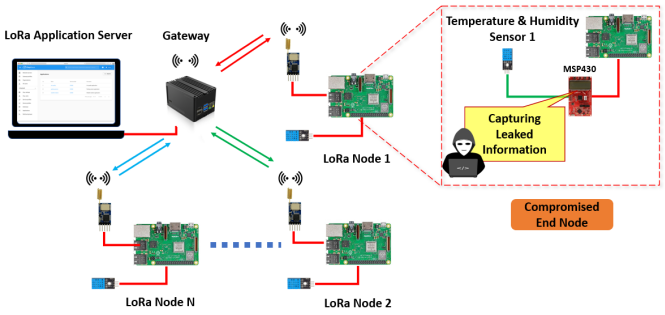


Fig. 6. An example of MITM attack on a LoRa node.

if the gateway device shows a sudden drop on the number of received LoRa packets.

2) Replay Attack: Replay attack is another typical attack that an adversary carries out to disrupt the network. The replay attack scenario is also depicted in Fig. 5. The adversary also has access to a SDR device to capture the LoRa packets. The LoRa node is connected to the LoRa gateway and transmit data. A malicious node will try to communicate with the gateway multiple times. During the replay attack, the malicious node will occupy one of the gateway channels. We can set up a monitoring system at the gateway to observe the abnormal behaviors of a gateway and examine the frame counter of the transmitted packets from the gateway to the application server. Analyzing the gateway log file will provide valuable information to determine the appearance of replay attacks.

3) MITM Attack: MITM attack is a physical attack that can be performed on a LoRa node, as shown in Fig. 6. 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.

C. Tools for Attack Analysis

1) Hardware Tools: A Packet Monitor32 sniffer can be used to capture the transmitted packets. The captured packets can be analyzed with Wireshark to decode all the critical information. For example, we can check for the join request message without a decryption process. This step will not raise any alarm in the LoRa network. We can use HackRF One for the hardware implementation to sniff and capture the wireless packets. In our case studies, LoRaWAN operates at the frequency of 915 MHz. Targeting a specific LoRa devices, the HackRF One can send joining request messages to complete the handshaking process. In addition, the HackRF One can replay the previously captured packet messages to the LoRa gateway.

2) Software Tools: Software-Defined Radio (SDR) is a software module running on a generic hardware platform consisting of digital signal processing and hardware to implement radio functions. A SDR consists of two main features hardware and software. The hardware part, we discussed in the hardware tool section, such as HackRf One. To analyze the frequency spectrum, different types of open-source tools such as GNU Radio, GQRX, SDR, HDSDR, and SDR++ can be integrated with the HackRF One [22]. The GNU Radio Companion (GRC) has a block flow diagram and python function to create digital signal processing. There are also add-ons such as Gr-lora and LoRaTap available to assist in processing the raw signals detected by the radio. The open-source software, Wireshark, is commonly used to analyze encrypted or unencrypted LoRa packets. Based on those tools, we can study the security vulnerabilities in LoRaWAN and analyze various attacks performed at different levels.

V. Case Studies

In this section, all the experiments were performed based on a LoRaWAN composed of Arduino MKR WAN 1300 as LoRa nodes, temperature sensors, and Raspberry Pi 4 based RAK7244 as LoRa gateway. The LoRa gateway consists of a router, a packet forwarder running on a Raspberry Pi, and an RF module. In general, gateway log files can be generated by Semtech UDP Packet Forwarder, ChirpStack Concentratord, and Basic Station Packet Forwarder. In our case study, we used ChirpStack Concentratord to record log files.

A. Case Study #1: Analyzing Jamming Attack on LoRa Nodes

1) Implementation of Jamming Attack: In this case study, we used the GNU Ratio Companion software to design a jamming attack circuit and then implemented the circuit in a HackRF One device. The frequency range of LoRaWAN used in North America is from 902 MHz to 928 MHz. The attacker who performs the jamming attack first needs to identify the exact frequency utilized in the target LoRaWAN. The software GQRX was used in our case study to detect the specific frequency for LoRa packet transmission. As shown in Fig. 7, the intensive red horizontal lines in the zoomed in the picture are around the frequency of 915 MHz. This indicates that the GRQX can successfully capture the carrier frequency of LoRa packets. The attacker can use the GNU to further examine the signal-noise-ratio over a wide frequency spectrum. As confirmed in Fig. 8, the peak relative gain (-37 dB) of the LoRa packet transmission indeed appears at 915 MHz.

2) Attack Detection and Analysis: We analyze the jamming attack in multiple ways. First, we can use the GNU Radio IDE (GRC) to monitor the frequency spectrum occupied by the LoRa packet transmission over time. The waterfall graph

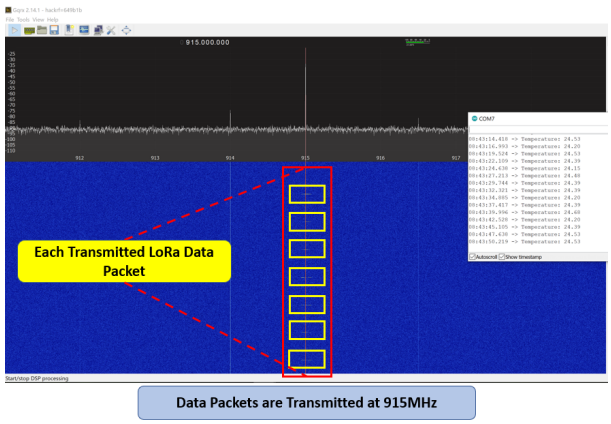


Fig. 7. GQRX waterfall graph for LoRa packet transmission.

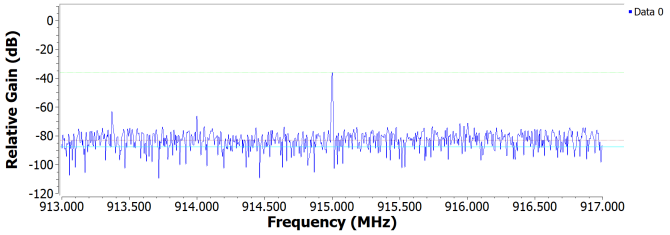


Fig. 8. Relative gain observed from the GNU Radio IDE showing the frequencies used by LoRa packet transmission.

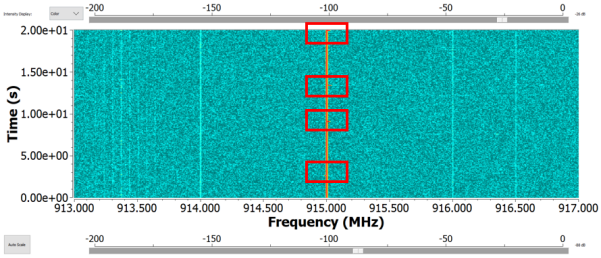


Fig. 9. Waterfall graph obtained from GNU Radio IDE showing the frequency used by LoRa packet transmission.

shown in Fig. 9 provides a global view of which frequency is used in LoRa packet transmission and how often that frequency is used. By analyzing the waterfall graph obtained from GRC, we are able to detect the jamming attack.

Once the jamming device HackRF One is deployed at the physical layer of the LoRaWAN, the malicious device starts to transmit jamming packages and disrupt the network. Figure 10 illustrates that the jamming attack occupies the frequency spectrum between 912 MHz to 916 MHz, and the signal-to-inference-plus-noise ratio for the jamming messages is close to that for a normal LoRa packet. This means, the jamming messages will degrade the effective signal-to-inference-plus-noise ratio of the valid LoRa packets and the LoRa gateway will not be able to receive all the LoRa packets successfully. Thus, the jamming attack interferes with the normal LoRa transmission.

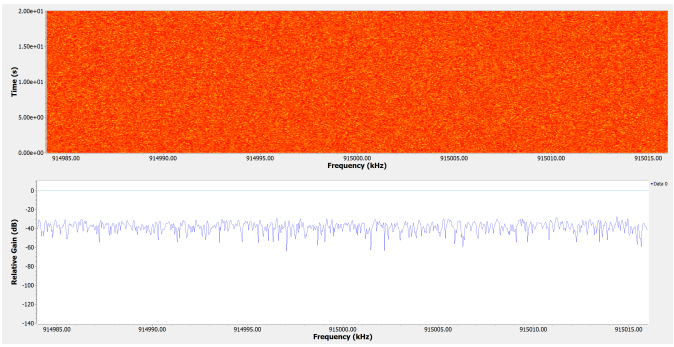


Fig. 10. Relative gain for the signals induced by jamming attack.

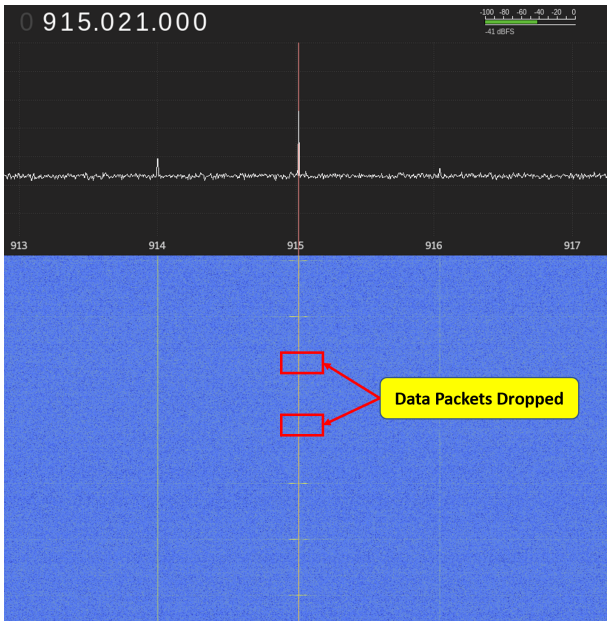


Fig. 11. Normal LoRa packet dropping at 915MHz due to the jamming attack.

As the frequency range of 912 MHz to 916 MHz is taken by the jamming messages transmitted by the malicious device, HackRF One, the number of normal LoRa packets will be reduced. Figure 11 shows that the target LoRa node failed to transmit the LoRa packets. The effectiveness of jamming attacks depends on the noise power and the occupied frequency range. Based on our log file analysis, we calculate the number of LoRa frames received in the LoRa gateway. As shown in Fig. 12, the jamming attack reduces the number of frames by 86.7% for the 2-minute jamming attack.

B. Case Study #2: Replay Attack on LoRa Gateway

1) Implementation of Reply Attack: Section V-A demonstrates the jamming attack that obstructs the LoRa packet transmission from a LoRa node to a LoRa gateway. Packet jamming could also happen in the channel between a LoRa gateway and a LoRaWAN server. A replay attack is a low-cost attack that causes packet jamming. In our experiment, the HackRF One device captured the signal transmitted by the LoRa node with a duration of 45 seconds. This captured signal

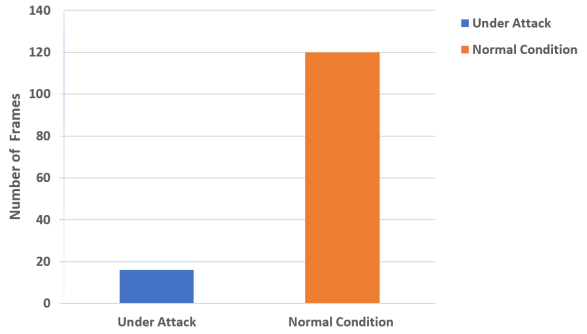


Fig. 12. The number of frames received by a gateway during a 2-minutes time period under normal condition and under attack.

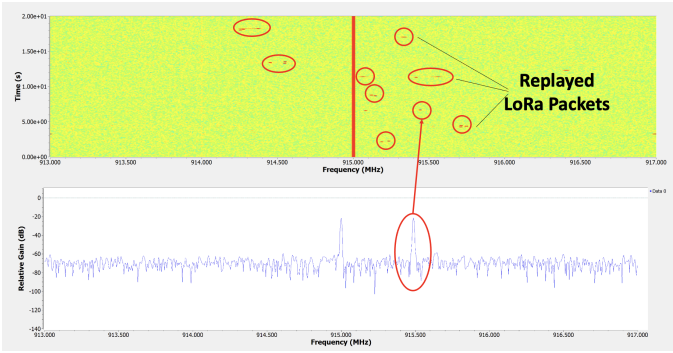


Fig. 13. Real-time waterfall graph and frequency response for the captured LoRa packet transmission observed from GRC.

is then transmitted over HackRF One for the replay attack on the gateway. Even though HackRf One(malicious node) is not registered with the application server, the gateway will still forward the captured signal and waste one of the channels of the gateway.

2) Attack Detection and Analysis: Attackers could use the GNU ratio IDE to capture one LoRa packet and then use that packet as a source to perform a replay attack. Our attack analysis framework is capable of detecting the replayed LoRa data packets, as shown in the bottom half of the Fig. 13. If we zoom in on the relation gain over the frequency spectrum, we can observe the replayed packet in a particular frequency. As illustrated in the bottom half of Fig. 13, there is a signal having the relative gain of -20dB at a particular moment. That indicates that one replayed LoRa packet appears to be detected.

Other than the frequency domain response, another detection checkpoint for replay attacks is the frame counter of the LoRa nodes. The frame counter can be read in the application server. By analyzing the frame counter, we can tell how much granted data has been transmitted from a LoRa node to the application server through the gateway. In this case study, we used the Chirpstack application server to monitor the frame counter in the messages forward by the gateway. While the legitimate LoRa node keeps transmitting packets and thus increasing the frame counter value, the HackRF One replays the recorded signal and repeats the frame counter values. As shown in the right side picture of Fig. 14, the frame counter for the legitimate LoRa packets reaches 208. In contrast, even though we accessed the frame counter at the same time, the frame counter for the packet induced by the replay attack is only 91. The comparison of the two frame counters confirms that the replay attack can be detected by our attack analysis framework.

C. Case Study #3: Analyzing Physical Attacks on a Sensing Node

1) Implementation of MITM Attack: In this case study, we implement a MITM attack at a sensing node. The overview of the attack scenario is shown in Fig. 6. 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 3 B+). 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.

2) Attack Detection and Analysis: We used an oscilloscope to monitor the signal through the MSP430FR6989 microcontroller. As shown in Fig. 15(a), the data sent by the sensor is successfully captured and leaked by the microcontroller. We can further observe the tampered temperature and humidity values from the Raspberry Pi terminal (i.e., LoRa node). Figure 15(b) shows that a voltage glitch induced by the MITM attack changes the temperature and humidity sensed by the sensor to some abnormal values.

VI. Conclusion

This work proposes a framework to analyze the security attacks on the LoRaWAN applied advanced manufacturing. We present the jamming attack, replay attack, and man-in-the-middle attack scenarios in a LoRaWAN. Three case studies are provided to demonstrate those attacks implemented at a LoRa node, a LoRa gateway, and a sensing device, respectively, and show how the proposed framework can enable the attack detection.

References

[1] CyberObserve, "29 must-know cybersecurity statistics for 2020," https://www.cyber-observer.com/cyber-news-29-statistics-for-2020-cyber-observer/, 2020.
[2] "Lorawan® security," https://lora-alliance.org/wp-content/uploads/2020/11/la_faq_security_0220_v1.2_0.pdf.
[3] "Abp vs otaa," https://www.thethingsindustries.com/docs/devices/abp-vs-otaa/.
[4] V. Stoffer, "Outdated computers and operating systems," https://commons.lbl.gov/display/cpp/Outdated+Computers+and+Operating+Systems, 2013.
[5] L. Giliver, "Meat giant jbs pays out $11 million ransom after 'cyber-attack' shut down operations," https://plantbasednews.org/news/economics/meat-giant-jbs-pays-ransom-after-cyber-attack/, 2021.

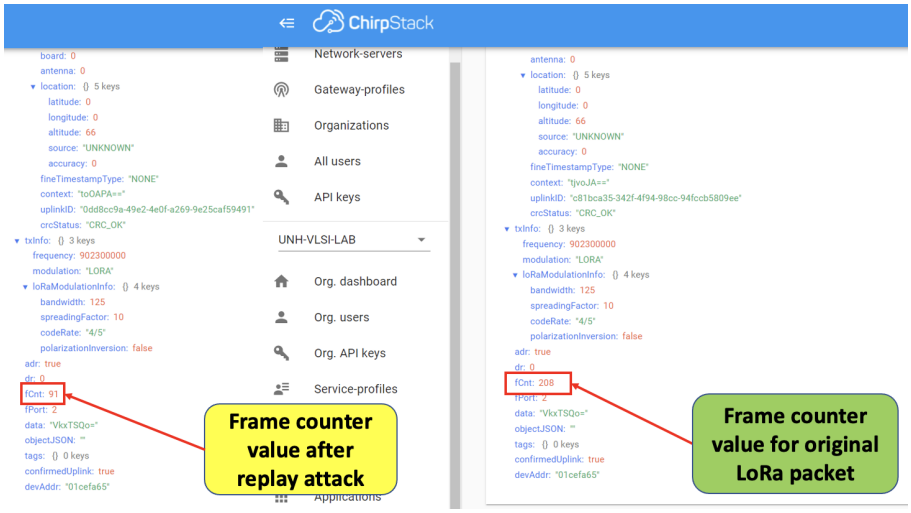
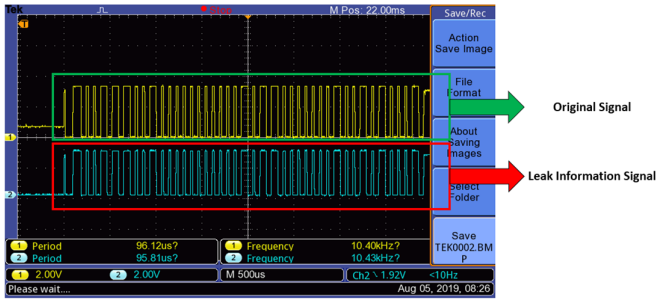
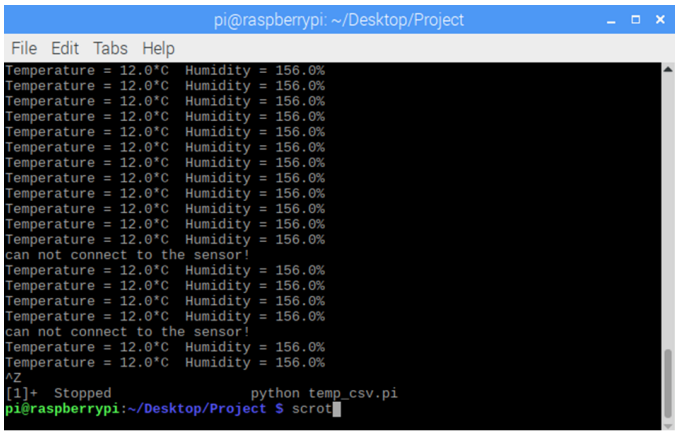


Fig. 14. Comparison of the frame counters for the packets transmitted by a legitimate LoRa node (left) and a replay attack (right).



(a)



(b)

Fig. 15. Results of the MITM attack on a sensing node. (a) Information leaking, and (b) data altering.

[6] C. Wueest, "Targeted attacks against the energy sector," https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/targeted_attacks_against_the_energy_sector.pdf, 2014.

[7] X. Yang, E. Karampatzakis, C. Doerr, and F. Kuipers, "Security vulnerabilities in lorawan," in *2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI)*, 2018, pp. 129–140.

[8] N. E. L. M. N. A. E. F. A. Silva FSD, Silva E, "Taxonomy of ddos attack mitigation approaches featured by sdn technologies in iot scenarios," *Sensors (Basel)*, 2020.

[9] A. G. Johansen, "What is a firewall? firewalls explained and why you need one," https://us.norton.com/internetsecurity-emerging-threats-what-is-firewall.html, 2021.

[10] M. Lessing, "How to prevent computer worms," https://www.sdxcentral.com/security/definitions/how-to-prevent-computer-worms/, 2020.

[11] C. J. F. P. Ullrich, J., "The role and security of firewalls in cyber-physical cloud computing," *EURASIP Journal on Information Security*, 2016.

[12] J. PETTERS, "What is a port scanner and how does it work?" https://www.varonis.com/blog/port-scanning-techniques/, 2020.

[13] R. Ivanov, M. Pajic, and I. Lee, "Attack-resilient sensor fusion for safety-critical cyber-physical systems," *ACM Trans. Embed. Comput. Syst.*, vol. 15, no. 1, Feb. 2016. [Online]. Available: https://doi.org/10.1145/2847418

[14] H. Noura, T. Hatoum, O. Salman, J.-P. Yaacoub, and A. Chehab, "Lorawan security survey: Issues, threats and possible mitigation techniques," *Internet of Things*, vol. 12, p. 100303, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2542660520301359

[15] M. R. Monjur, S. Sunkavilli, and Q. Yu, "Adobf: Obfuscated detection method against analog trojans on i2c master-slave interface," in *2020 IEEE 63rd International Midwest Symposium on Circuits and Systems (MWSCAS)*, 2020, pp. 1064–1067.

[16] W. He, J. Breier, S. Bhasin, N. Miura, and M. Nagata, "An fpga-compatible pll-based sensor against fault injection attack," in *2017 22nd Asia and South Pacific Design Automation Conference (ASP-DAC)*, 2017, pp. 39–40.

[17] K. Fukushima, D. Marion, Y. Nakano, A. Facon, S. Kiyomoto, and S. Guilley, "Evaluation of side-channel key-recovery attacks on lorawan end-device," in *Information Systems Security and Privacy*, P. Mori, S. Furnell, and O. Camp, Eds. Cham: Springer International Publishing, 2020, pp. 74–92.

[18] K. Fukushima., D. Marion., Y. Nakano., A. Facon., S. Kiyomoto., and S. Guilley., "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. SciTePress, 2019, pp. 67–74.

[19] J. Tan, "A gentle introduction to lorawan gateways nodes," https://www.seeedstudio.com/blog/2021/04/27/a-gentle-introduction-to-lorawan-gateways-nodes/, 2021.

[20] Q. Zhou, K. Zheng, L. Hou, J. Xing, and R. Xu, "Design and implementation of open lora for iot," *IEEE Access*, vol. 7, pp. 100 649–100 657, 2019.

[21] T. T. Industries, "What is a lorawan network server?" https://www.thethingsindustries.com/docs/reference/components/application-server/.

[22] "The big list of rtl-sdr supported software," https://www.rtl-sdr.com/big-list-rtl-sdr-supported-software/, 2014.