Hardware Security in Advanced Manufacturing

Mohammad Monjur, Joshua Calzadillas, Mashrafi Alam Kajol, and Qiaoyan Yu
University of New Hampshire
Durham, NH, USA

ABSTRACT

More and more digitized techniques and network connectivity are deployed to advanced manufacturing to enable remote system monitoring and automated production; however, this trend also leads to the traditional assumption of security in manufacturing not holding true any longer. For instance, the option of remote access makes advanced manufacturing infrastructures vulnerable to various security attacks from physical devices to cyberspace. Existing literature that addresses the attacks in advanced manufacturing is mainly at the network level. In this work[1], we study the role of hardware security in the process of advanced manufacturing. More specifically, our analysis focuses on the security vulnerability of sensors, local data processing nodes, and the interface implementation for standardized communication protocols. Unique attack examples such as hardware Trojan, interface sniffing, and fraudulent data injection attacks are provided in this work to highlight the unique challenges of attack detection and mitigation in advanced manufacturing.

CCS CONCEPTS

• **Computer systems organization** → **Embedded systems, Redundancy**; • **Security** → *Hardware Security*; • **Advanced Manufacturing** → *Robotics*; • **Networks** → Network reliability.

KEYWORDS

Hardware security, advanced manufacturing, sensor network, hardware Trojan, jamming attack, replay attack, LoRaWAN.

ACM Reference Format:
Mohammad Monjur, Joshua Calzadillas, Mashrafi Alam Kajol, and Qiaoyan Yu. 2022. Hardware Security in Advanced Manufacturing. In *Proceedings of the Great Lakes Symposium on VLSI 2022 (GLSVLSI '22), June 6–8, 2022, Irvine, CA, USA.* ACM, Irvine, CA, USA, 6 pages. https://doi.org/10.1145/3526241.3530829

1 INTRODUCTION

Advanced manufacturing techniques enable the rapid transfer of science and technology into manufacturing products and process [12]. The utilization of innovative information, automation, computation, software, sensing, and network techniques in advanced manufacturing factories empowers the production system to efficiently generate a small or large volume of products and accommodate the demand of customized manufacturing [2]. The representable manufacturing process technologies described in the definition of advanced manufacturing include rapid prototyping [15], information technologies [13], advanced robotics and intelligent production systems [4], automation, the ability to support custom manufacture, and the flexibility of adjusting production scalability [11].

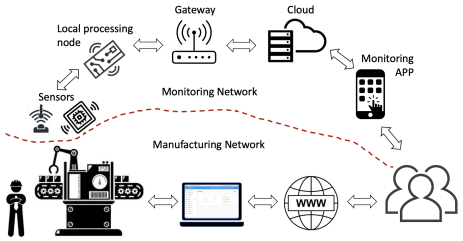


Figure 1: Communication pathways in advanced manufacturing networks.

Based on the recent attack reports, the National Institute of Standards and Technology (NIST) advocates more attention to cybersecurity attacks on manufacturers, especially industrial control systems (ICS). For instance, Tesla's factory cameras were breached in 2021 [7]. The primary target of that hack was a company that has products of video cameras, which have cloud based access for users to monitor their environment. Hackers gained access to that company's servers and retrieved the archived customers data [9]. Compromised edge devices could be exploited as a gateway to conduct a large-scale distributed denial-of-service (DDoS) attack (e.g., the Mirai botnet [10] attack against the company *SONY*). Existing literature mainly concentrates on the attack from the cyber space. There are limited studies available to examine the security threats from the hardware components deployed in advanced manufacturing. This work addresses in this need.

The rest of this paper is organized as follows. In Section 2, we briefly introduce advanced manufacturing. In Section 3, the importance of hardware security in advanced manufacturing is analyzed. In Section 4, we propose the key challenges of addressing those threats in our work. Section 5 includes conclusion and future work.

2 INTRODUCTION OF ADVANCED MANUFACTURING

Despite the production flow of advanced manufacturing varies with different applications, we simplify its communication pathways as shown in Fig. 1. The physical and internet network for tangible product manufacturing involves machines, workers, computer-aided design systems, internet, and customers. We assume that network can be protected with techniques such as conventional firewall and air-gapped network. In automated manufacturing factories, there will be another network that monitors the operation

[1]This work is partially supported by National Science Foundation Award #1652474.

GLSVLSI '22, June 6–8, 2022, Irvine, CA, USA

ACM ISBN 978-1-4503-9322-5/22/06…$15.00
https://doi.org/10.1145/3526241.3530829

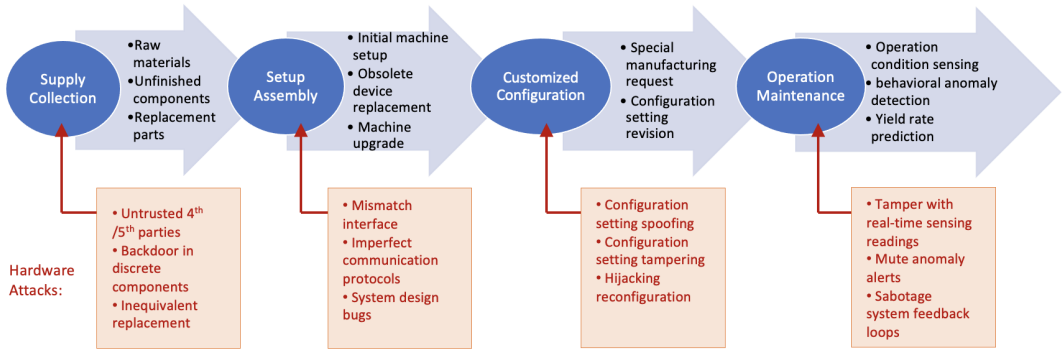


Figure 2: Hardware attacks sectors in advanced manufacturing production line.

status of machines and workers. Sensors are either mounted on the manufacturing machines or located nearby. The sensed data is first processed by local node and then transmitted to a server or cloud via gateways. Customers can check the manufacturing status through user monitoring Apps. In the monitoring network, multiple communication protocols are deployed to fulfill the mission of data transfer. SPI, UART and I^2C are commonly used in the communication between sensors and local processing nodes. Wireless communication techniques, such as Zigbee, Bluetooth, and Long-Range (LoRa), facilitate the data transmission between local nodes and gateways.

Although advanced manufacturing techniques bring in better flexibility and accommodate faster technology transfer than traditional manufacturing, the complicated network of physical devices, weakly-protected interfaces, and immature communication protocols impeded a secure design flow. Operation maintenance is vulnerable to attacks from different sectors as shown in Fig. 2. In the supply chain of raw materials, unfinished components, and machine assembly devices, we can choose the goods needs from security-certified 3^{rd} parties but we cannot control the trustworthiness of the 3^{rd} parties' own supply chain i.e. 4^{th} and 5^{th} parties. It is particularly true for large brand companies, which are easy to become a target. The security vulnerabilities of the physical interfaces for various communication protocols or obsolete operating systems could be exploited by attackers to breach the integrity of manufacturing machines. To accommodate the flexibility featured in advanced manufacturing, we need to support customized machine configurations in a time-efficient manner. The configuration setting channels maybe suffer from spoofing and hijacking attacks. Compared to the previous phases, more attack surfaces could occur in the stage of operation maintenance since more sensing data storage and transmission via wired or wireless media are involved.

3 WHY HARDWARE SECURITY MATTERS IN ADVANCED MANUFACTURING?

In industry 4.0 [3], sensors, edge devices, and various network techniques are extensively deployed to manufacturing factories. Driven by commercial profits, attackers could leverage the following facts to implement attacks at different levels as shown in Fig. 3:

- Default, weak, guessable passwords utilized in networked devices/equipment

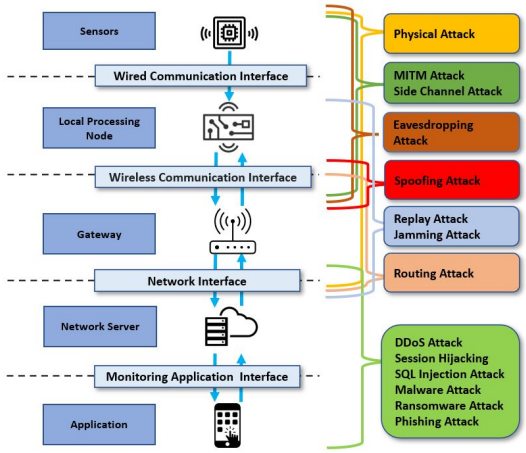


Figure 3: Potential attacks in advanced manufacturing.

- Out-of-date firmware in IoT and embedded systems
- Insecure communication/network protocols
- Obsoleted operation systems
- Weakly-protected storage media
- Hardware components from untrusted supply chain

3.1 Roles of Hardware Security

Among all attacks in manufacturing, there are substantial attacks that could originate from compromised hardware components deployed in manufacturing systems. In this section, we analyze the roles of hardware security in advanced manufacturing, with special emphasis on sensing devices, local elements and interface.

3.1.1 Sensing Devices. The common sensors used in manufacturing plants include infrared sensors, photoelectric beam based sensors, motion detection sensors, audio sensors, and motion sensors[8], which monitor sound, distance, heat, light, or other measurable changes. If sensors are connected to a wired/wireless network, the integrity of sensors becomes crucial to prohibit denial-of-service, data breaches, and unexpected loss of intellectual property. A counterfeit sensor could yield inaccurate sensing data or emit unspecified signals to facilitate information leaking via a covert channel. Malfunctioning sensors may form a rare trigger condition for Trojans embedded in manufacturing systems.

3.1.2 Local Storage and Processing Elements. The trustworthy local storage and processing elements deployed in real-time monitoring systems are also critical in assuring the security of advanced manufacturing. If the memory for firmware storage is compromised, the confidentiality of edge devices' configuration and authentication would be breached. The main memory for log file storage could be tampered by invasive attacks from the semiconductor supply chain. The integrity loss of sensing logs would impede the timely notification of the real-time malfunction in manufacturing plants. Malicious operations defined by hardware Trojans in processing elements could directly alter the function of a monitoring system.

3.1.3 Interface Implementation. A sensor network in advanced manufacturing may involve several protocols for wired and wireless communication networks. Data format conversion, handshaking, integrity check, and data authentication are mainly executed by low-power distributed devices. As hardware manufacturing industries partially outsource the design and verification to third parties, adversaries can take advantage of the globalized supply chain to insert hardware Trojan through untrusted third-party IP vendors, SoC developers, and semiconductor foundries [14]. We zoom in on the attacks performed on the interfaces for wired and wireless communication.

At wired communication interfaces, physical attacks are easy to implement since the low-end commercial-off-the-shelf devices such as Arduino, STMicroelectronics, and Raspberry Pi [5] are loosely protected. The communication protocols (e.g., SPI) between sensors and local processing nodes could be realized by untrusted source code. If a malicious code segment is inserted in the system configuration program, the data passing through the interface could be tampered with stealthily. At wireless communication interfaces, more sophisticated attacks can take place. Wireless sensor networks in advanced manufacturing (e.g., LoRaWAN) could be sabotaged by a hardware Trojan, which turns the edge device into a malicious node to cause abnormal activities via replay and jamming attacks. An attack that targets at the critical sensor data for monitors and automation could lead to a halt in the production line and supply chain, resulting in a loss of millions dollars [6].

The current attention in industries is the attack from the network level. There is limited study available to investigate the security challenges of physical devices in advanced manufacturing. Thus, this work provides practical attack examples and highlights the pressing need to address hardware security issues in advanced manufacturing.

3.2 Attack Examples

In this section, we use sensor network as the background of our case studies to demonstrate the attacks that harm the operations in advanced manufacturing. The sensor network monitors and assures the proper data collection for industrial automation storage, analysis, and production line control. The common protocols applied in sensor networks include NB-IoT, Sigfox, Zigbee, WLAN, and LoRa. As LoRaWAN covers a wide range and has the feature of low power consumption, we examine the security weaknesses of LoRaWAN applied in the sensor network for advanced manufacturing. Figure 4 shows the threat model interested in this section. When the hardware components and their connection become the attack targets

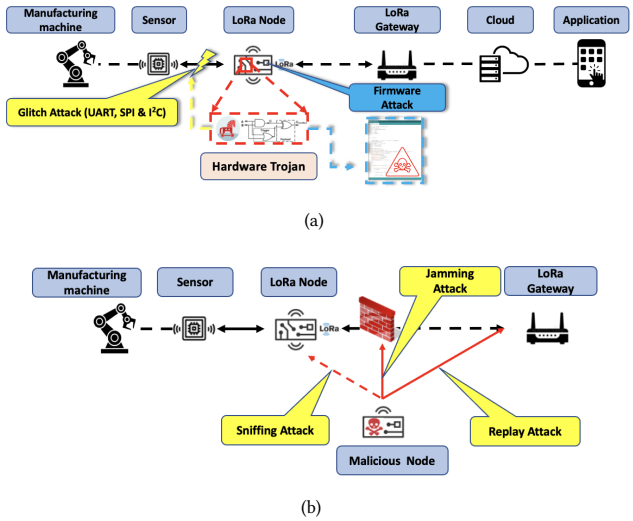


Figure 4: Attacks in (a) wired connection and (b) wireless communication in advanced manufacturing flow.

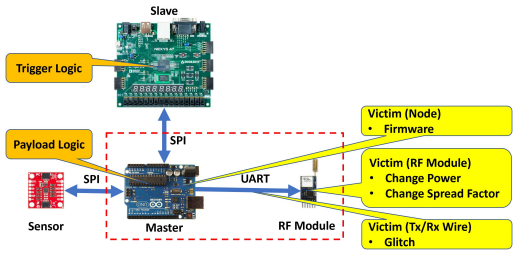


Figure 5: Hardware Trojan attack in a local sensing node.

(shown in Fig. 4(a)), hardware Trojan attack, voltage glitch attack, man-in-the-middle attack, and firmware updating attack could lead to hardware malfunctions or performance deviation in sensing nodes. Consequently, the raw sensing data will not reflect the true operating conditions in the manufacturing sites. As far as the security of wireless communication networks is concerned, spoofing, jamming, and replay attacks are the common attack scenarios to be considered.

3.2.1 Hardware Trojan Attack. In Industry 4.0, more and more modern manufacturing processes are digitized and implemented with a set of microcontrollers, FPGAs, systems-on-chip, and general-purpose embedded systems. Due to the well-known hardware security threats from the supply chain, malicious modification of hardware design (a.k.a hardware Trojan) is a typical threat that challenges the integrity of sensing and local processing elements. We used the setup shown in Fig. 5 to perform a hardware Trojan attack on a LoRa-based sensing node (implemented on an Arduino board). The Trojan trigger logic examines the arrival of special conditions. The Trojan payload either manipulates the incoming sensor data (alters its value), re-sends the previous value, or injects dummy data to jam the transmission link. As most sensing networks are composed of low-end edge devices, authentication and integrity

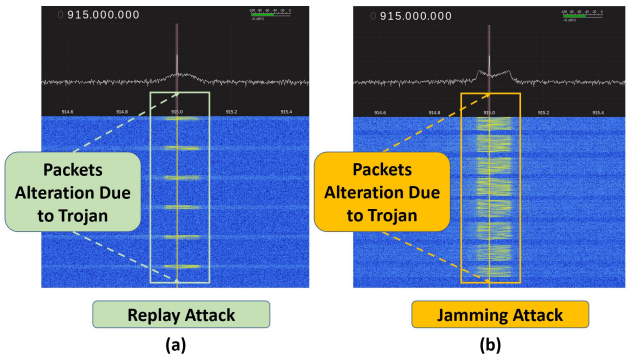


Figure 6: Spectrum view of LoRa packet transmission via a LoRa-based sensing node that is compromised by a hardware Trojan in a malicious LoRa node. (a) Replay attack, and (b) jamming attack.

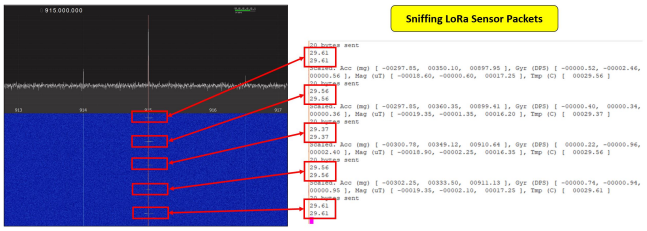


Figure 7: Sniffing attack performed by a SDR device on LoRa communication in advanced manufacturing.

check in sensor networks are loosely deployed. Figures 6(a) and (b) demonstrate that the hardware Trojan attack in the LoRa node successfully replays the previous message several times and depletes the bandwidth by injecting dummy LoRa packets, respectively.

3.2.2 Sniffing Attack. A sniffing attack can capture transmitted data in the sensor network. Several off-shelf RF devices can receive and retransmit data packets available in a broad range of frequencies. Following the conceptual setup shown in Fig. 4(b), we performed a sniffing attack on the wireless communication link of our LoRaWAN-based sensor network. A software-defined radio (SDR) system carried out the operation of data capturing with the support of software and external RF hardware. To remove the noise interference, we used a narrow-band filter to precisely capture the LoRa packets. Figure 7 shows the temperature sensor data sniffed by the SDR device at the frequency of 915MHz. Even though the data are encrypted with a key, an adversary can decrypt the captured data once the root session key stored in the cloud server is leaked. The success of a sniffing attack will enable the follow-up reverse engineering attack on the sensor network and understand the sensor's role in ICS. Consequently, sniffing attacks at the physical level will challenge the trustworthiness of the entire monitoring system for advanced manufacturing.

3.2.3 Fraudulent Data Injection Attack. Fraudulent data injection attacks could be performed at the physical device level and all the way up to the network level. Counterfeit sensors could produce

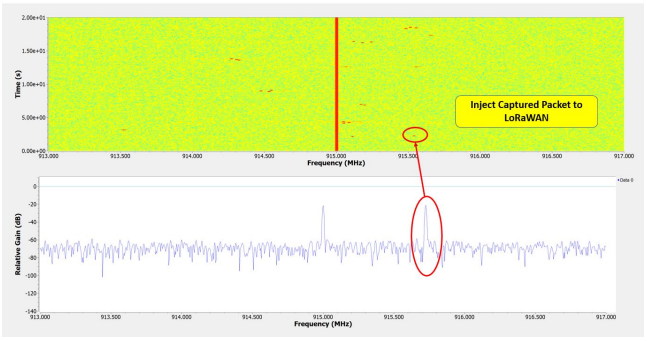


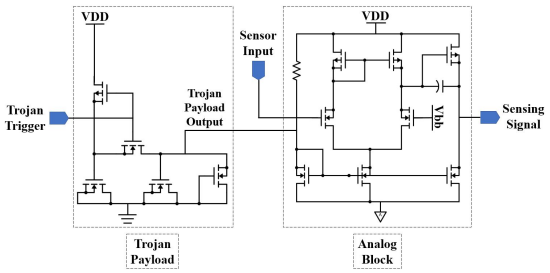
Figure 8: Injecting fraudulent data in the sensor network.

biased sensing data. A compromised interface between sensors and local processing elements could sabotage the integrity of the original data packets. Local data processing nodes tampered by hardware Trojans could inject fraudulent data packets as adversaries desire. Fraudulent data injection attacks will result in network bandwidth depletion, mute the indication of anomaly, and mislead the overall judgment on the overall manufacturing environment. We resumed the case study on LoRaWAN to demonstrate the success of fault data injection attacks. The second peak circled in Fig. 8 indicates a none real-time data of the sensor. In this case, the fraudulent data packet will transmit close to the transmitted packet's original frequency with a similar gain to the original transmitted packets. As a result, the LoRa receiver node would receive fraudulent data.

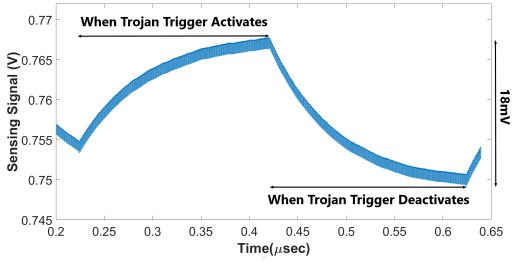
4 CHALLENGES OF ADDRESSING SECURITY ISSUES IN ADVANCED MANUFACTURING

4.1 New Attack Detection against Interference from Analog Variation

Diverse sensors in advanced manufacturing industries enable us to learn the real-time manufacturing condition and then minimize the loss caused by abnormal manufacturing behaviors. However, sensing nodes face challenges in assuring its security due to the analog nature, noise margin, coupling effect, and process, voltage, and temperature variation. To demonstrate the impact of a hardware Trojan on an analog sensor, we implemented a simplified sensing circuit as shown in Fig. 9(a). The Trojan trigger signal is activated by an arbitrary event and the Trojan payload injects an adjustable voltage to the analog block for voltage sensing to manipulate the sensing output. Since the current flowing through the differential pair determines the sensing node's critical parameters (e.g., gain, bandwidth, and power consumption), the hardware Trojan placed in the sensing node will result in a significant malicious behavior. However, the presence of such a hardware Trojan only brings in a negligible change in the signal, gain, -3dB bandwidth and power consumption. As shown in Fig. 9(b), the voltage fluctuation measured on the sensor output is only 18mV for the circuit powered by a supply voltage of 1.8V. We further compared the gain, unity gain-bandwidth, -3dB Bandwidth and power consumption of the sensing node with and without the Trojan in Table 1. The difference in the critical parameters of the Trojan free and Trojan deactivated cases is too small to be useful for Trojan detection. Thus, functional



(a)



(b)

Figure 9: Challenge on Trojan detection in analog circuit. (a) Circuit diagram for Trojan in sensing node, and (b) voltage variation due to analog Trojan.

Table 1: Comparison of Sensing Node's Critical Parameters

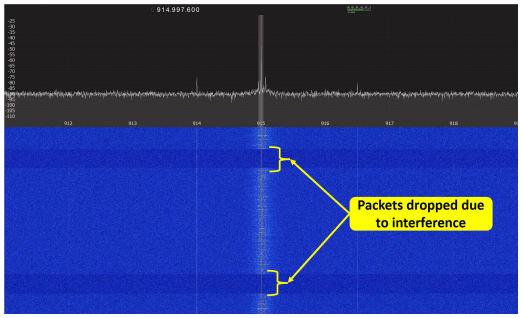
Parameters	Trojan Free	Trojan Deactivated	Trojan Activated
Gain	19 dB	19.32 dB	17.91 dB
-3dB Bandwidth	91.09 KHz	91.09 KHz	7.51 KHz
Unity Gain-Bandwidth	2.57 MHz	2.54 MHz	2.89 MHz
Power Consumption	19.61 μW	19.98 μW	23.5 μW

testing and side-channel signal based Trojan detection methods for digital circuits are not effective for the analog circuit used in the sensing network.

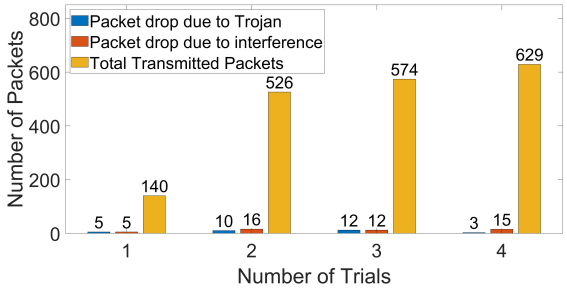
4.2 New Attack Detection Against Interference from Environmental Noise

In the environment of advanced manufacturing, there exists concurrently running machines, some of which are radio devices and emit electromagnetic fluxes. The mobile devices carried by the onsite manufacturing workers will also bring electromagnetic-related interference to the wireless communication network. The manufacturing environment creates unique noise such as electromagnetic crosstalk, temperature and humidity influence, and human interaction. Such as noise could lead the monitoring system to experience some natural faults. Due to those faults having high similarity with the effect of security attacks, it is challenging to differentiate the anomaly induced by attacks from natural faults.

We implemented a LoRa node (Arduino UNO) as master and a NEXYS A7 FPGA board as a slave in our experimental setup shown in Fig. 5. The LoRa node connects the DHT11 temperature, humidity sensor and the REYAX RYL896 RF module. The receiver



(a)



(b)

Figure 10: Packet drop in LoRaWAN packet transmission. (a) Packet drop due to natural electromagnetic flux interference in advanced manufacturing site, and (b) comparison of packet drop caused by Trojan and environmental noise.

LoRa node is collects the sensor data. We used HackRF One to analyze the spectrum to monitor the transmitted signal. The entire setup was placed in the John Olson Advanced Manufacturing Center to measure the packet drop rate due to the environmental noise and the attacks in the sensor network. The trigger circuit was implemented in the slave device (NEXYS A7). When the trigger is active, the slave device will activate the payload on the master (Arduino UNO) and change the spreading factor of the RF module. The triggered hardware Trojan in the LoRa node will lead to LoRa packet drop. However, in our onsite experiments, we also observed the packet drop from the spectrum domain even if the Trojan was not triggered. As shown in Fig. 10(a), there are two periods of time missing LoRa packets. Four trials with different time intervals were used to examine the packet drop induced by Trojan and natural noise interference in the manufacturing environment. As can be seen from Fig. 10(b), the number of packet drops caused by the triggered Trojan and environmental interference are comparable. The Trojan in the LoRa node results in the packet drop rates of 3.57%, 1.9%, 2.09% and 2.86% for trails 1, 2, 3, and 4, respectively. The environmental noise in the manufacturing center leads that 3.57%, 3.04%, 2.09% and 2.38% of LoRa packets are lost for the four trails, respectively. This case study indicates that the packet loss caused by a hardware Trojan in the sensing node is not worse than the effect originating from the environmental noise.

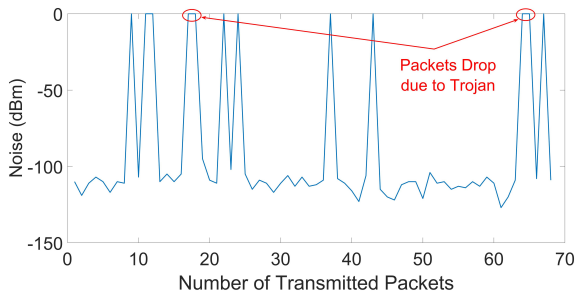


Figure 11: Total noise for LoRa packets transmission with respect to 125 feet transmission distance in the Olson Center.

In our case study, two primary sources of noise interfere with the transmission of LoRa packets. One source is the RF module in the LoRa transmitter and the other source is electromagnetic devices near the antenna of the LoRa receiver. Noise from both sources contributes to the total noise that interferes with the standard sensing data transmission over the air. In our experiment, we placed the transmitter (Tx) and the receiver (Rx) 125 feet apart. The noise range is typically between 0 dB to -120 dB in wireless communication. We correlated the loss of LoRa packets with the noise measured based on Eq.(1).

$$Noise_{dB} = RSSI_{dB} - SNR_{dB} \tag{1}$$

The received signal strength indicator (RSSI) and signal-to-noise (SNR) values were collected from the Rx node. The noise value is zero, which indicates no active transmission due to the packet drops. As shown in Fig. 11, four packets (the 17th, 18th, 64th, and 65th packets) were dropped during the process of LoRaWAN transmission due to the activated hardware Trojan and the rest of eight packet drops were caused by the combination of environmental noise. This case study confirms that the background noise in advanced manufacturing could provide a masking effect to the malicious activity originating from the compromised devices. Given 68 packet transmission, the Trojan attack only induces 5.9% packet drop and the environmental noise leads to 11.76% packet loss. This observation proves confirms that the packet drop rate is not a reliable metric to detect the presence of compromised sensing hardware deployed in advanced manufacturing.

5 CONCLUSION

Modern manufacturing industries apply advanced sensing, monitoring, control, automation, and maintenance techniques. As more network connectivity is enabled in advanced manufacturing, the assumption of security in the manufacturing environment needs to be revisited. In this work, we analyze the role of hardware security in advanced manufacturing and examine the specific security threats that could harm the sensor network deployed in manufacturing plants. Case studies are provided to demonstrate the practical attacks.We further highlight the unique challenges of attack detection and mitigation in advanced manufacturing.

NIST's National Cybersecurity Center of Excellence (NCCoE) has demonstrated various approaches and examples for detecting anomalous behaviors observed in industrial control systems [1]. From a hardware perspective, we envision that device scanning, real-time data integrity check, and network visibility enhancement are critical for ensuring security in manufacturing. Device scanning will facilitate to examine the device connectivity, configuration, and integration check. Default settings for devices' initial configuration are typically open to the public or accessible from the non-volatile memory. The leak or the integrity loss of the deployed devices' configuration parameters should be inspected at hardware level. The operation monitoring network for advanced manufacturing generates extremely large volume of data. It will be challenging to scrutinize all sensing data. If a real-time response is required, the integrity check of those data will be further ambitious. To support forensic, secure storage of the high-volume sensing data will be imperative. As many internet-enabled devices are employed in advanced manufacturing, the network ecosystem becomes more complicated than ever. To thwart cyber attacks, network visibility needs to be improved from the defender's point of view. The deviation of physical devices' behavior should be reflected in the monitoring network.

REFERENCES

[1] Wissam Aoudi, Mikel Iturbe, and Magnus Almgren. 2018. Truth Will Out: Departure-Based Process-Level Detection of Stealthy Attacks on Control Systems. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (Toronto, Canada) *(CCS '18)*. Association for Computing Machinery, New York, NY, USA, 817–831.

[2] Christian Cavallo. 2022. *What is Advanced Manufacturing?* Retrieved Feb.2022 from https://www.thomasnet.com/articles/services/what-is-advanced-manufacturing

[3] Baotong Chen, Jiafu Wan, Lei Shu, Peng Li, Mithun Mukherjee, and Boxing Yin. 2018. Smart Factory of Industry 4.0: Key Technologies, Application Case, and Challenges. *IEEE Access* 6 (2018), 6505–6519.

[4] Yonghua Chen and Fenghua Dong. 2013. Robot machining: recent development and future research issues. In *The International Journal of Advanced Manufacturing Technology*, Vol. 66. 1489–1497.

[5] Chang-Sic Choi, Jin-Doo Jeong, Il-Woo Lee, and Wan-Ki Park. 2018. LoRa based renewable energy monitoring system with open IoT platform. In *2018 Intl. Conf. on Electronics, Info., and Communication.* 1–2.

[6] Andrew Ginter. 2018. *THE TOP 20 CYBERATTACKS on Industrial Control Systems.* Waterfall Security Solutions LTD.

[7] Kyle Hyatt. March 9 2021. Tesla factory cameras breached by hackers, report says. https://www.cnet.com/roadshow/news/tesla-factory-cameras-hacked/.

[8] Dirk Lehmhus, Claus Aumund-Kopp, Frank Petzoldt, Dirk Godlinski, Arne Haberkorn, Volker Zöllmer, and Matthias Busse. 2016. Customized Smartness: A Survey on Links between Additive Manufacturing and Sensor Integration. *Procedia Technology* 26 (2016), 284–301. 3rd International Conference on System-Integrated Intelligence: New Challenges for Product and Production Engineering.

[9] Entrepreneur en Español New Haven Register. March 11 2021. Operation Panopticon: 150,000 security cameras hacked into Tesla, banks, prisons and hospitals. https://www.nhregister.com/business/article/Operation-Panopticon-150-000-security-cameras-16016013.php.

[10] Department of Justice. December 9, 2020. Individual Pleads Guilty to Participating in Internet-of-Things Cyberattack in 2016. https://www.justice.gov/opa/pr/individual-pleads-guilty-participating-internet-things-cyberattack-2016.

[11] G. Putnik, A. Sluga, H. ElMaraghy, R. Teti, Y. Koren, T. Tolio, and B. Hon. 2013. Scalability in manufacturing systems design and operation: State-of-the-art and future developments roadmap. *CIRP Annals* 62, 2 (2013), 751–774.

[12] Deborah Stine. 2010. *PCAST Launches Policy Forum on the Future of U.S. Advanced Manufacturing.* Retrieved Feb. 2022 from https://obamawhitehouse.archives.gov/blog/2010/04/07/policy-forum-future-advanced-manufacturing-united-states

[13] Fei Tao, Jiangfeng Cheng, Qinglin Qi, Meng Zhang, He Zhang, and Fangyuan Sui. 2018. Digital twin-driven product design, manufacturing and service with big data. In *The International Journal of Advanced Manufacturing Technology*, Vol. 94. 3563–3576.

[14] K. Xiao, D. Forte, Y. Jin, R. Karri, S. Bhunia, and M. Tehranipoor. 2016. Hardware Trojans: Lessons Learned after One Decade of Research. *ACM Trans. Des. Autom. Electron. Syst.* 22, 1 (2016).

[15] Sheng Yang and Yaoyao Fiona Zhao. 2015. Additive manufacturing-enabled design theory and methodology: a critical review. In *The International Journal of Advanced Manufacturing Technology*, Vol. 80. 327–342.