Detection and Intrusion of Attacks in Cyber-physical Security for Additive Manufacturing

by

Enkai Bi

A dissertation submitted to the Graduate Faculty of
Auburn University
in partial fulfillment of the
requirements for the Degree of
Doctor of Philosophy

Auburn, Alabama
August 5, 2023

Keywords: Additive Manufacturing, Cyber-Physical System, Attack, Security, Dynamic Time Warping, Power Monitoring, Current Signal, 3D Printing.

Approved by

Dr. Gregory Purdy, Chair, Assistant Professor Industrial & Systems Engineering
Dr. Jia Liu, Member, Assistant Professor Industrial & Systems Engineering
Dr. Aleksandr Vinel, Member, Associate Professor Industrial & Systems Engineering
Dr. John Evans, Member, Professor Industrial & Systems Engineering

Abstract

Cyber-physical systems (CPS) have become increasingly prevalent in industrial production as they integrate sensing, computation, control, and networking into physical objects and infrastructure. One of the branches of CPS, additive manufacturing (AM) – also known as 3D printing – enables the fabrication of geometrically precise items layer by layer. This technology has revolutionized the manufacturing industry by allowing for more efficient and cost-effective production of complex and customized parts.

However, the widespread integration of physical facilities with the internet has amplified the risk of malicious activity, leaving entire systems vulnerable to cyber threats. As a result, concerns over security breaches in CPS within the Internet of Things (IoT) have escalated. While the security challenges in AM are multi-fold, this research specifically focuses on detecting cyber-physical threats and performing a side-channel attack to reconstruct the model, which may result in the theft of Intellectual Property (IP). By providing different contributions to solving these issues, the research aims to enhance the security of CPS and prevent unauthorized access, theft, or tampering of sensitive information.

With side-channel power monitoring, a novel intrusion detection method is proposed to counter threats in cyber-physical manufacturing systems. One of the potential malicious attacks in this context is the covert insertion of voids during printing, which can have severe consequences. To address this challenge, we propose a novel power-monitoring model based on Dynamic Time Warping (DTW) to detect malicious activity in a polymer AM process. Our results demonstrate that this approach not only facilitates rapid alteration detection compared to the other methods but also enables precise identification of void location down to a specific layer. Furthermore, we have

extended the application of the model to another machine, enabling us to verify the print's authentication remotely.

A physical-to-cyber domain attack is when information gathered from the physical domain is exploited to reveal sensitive information about the cyber domain. To illustrate the vulnerability of AM to such attacks, we propose a novel method for reconstructing the geometric form of a model using side-channel information obtained from the rotation of the motors. Our research highlights the need for preventive measures against Intellectual Property (IP) theft in AM and reveals that the model has been restored, closely matching the original CAD design.

This study contributes to the subject of the security domain in cyber-physical manufacturing systems, with an emphasis on intrusion detection as well as protection against possible vulnerabilities. Some limitations and future works are also provided here as proof of concept for further expansion into other security topics in CPS.

Acknowledgments

I would like to express my sincere gratitude and appreciation to the following individuals who have played significant roles in the completion of my doctoral dissertation:

First and foremost, I am deeply grateful to my advisor, Dr. Purdy, for his unwavering support, guidance, and invaluable insights throughout the entire research process. His expertise, patience, and commitment to my academic development have been instrumental in shaping the direction and quality of this dissertation.

I would like to extend my heartfelt thanks to the members of my dissertation committee, Dr. Vinel, Dr. Liu, and Dr. Evans, for their time, expertise, and constructive feedback. Their valuable contributions and scholarly insights have greatly enriched my research and refined the final outcome of this work.

I would like to acknowledge the support and assistance provided by my buddy Liangliang Xu. His intelligence and wisdom have been immensely valuable in shaping my ideas and broadening my understanding of the research domain.

I extend my gratitude to my family for their unwavering support, encouragement, and understanding throughout this demanding and fulfilling academic journey. Their unconditional love, patience, and belief in my abilities have been a constant source of motivation, and I am deeply grateful for their presence in my life.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

CPS	Cyber-physical Systems
AM	Additive Manufacturing
IoT	Internet of Things
IP	Intellectual Property
CMS	Cyber-Manufacturing Systems
DTW	Dynamic Time Warping
DSM	Fused Deposition Modeling
CAD	Computer-Aided Design
STL	STereoLithography
QC	Quality Control
CPMS	Cyber-physical Manufacturing System
DEMATEL	Decision-making Trial And Evaluation Laboratory
FFF	Fused Filament Fabrication
UCL	Upper Control Limit
LCL	Lower Control Limit
PWM	Pulse Width Modulation
GDP	Gross Domestic Product
SLA	Stereolithography
SLS	Selective Laser Sintering
SPI	Serial Peripheral Interface
TP	True Positive
TN	True Negative
CAGR	Compound Annual Growth Rate

1. Introduction

In the past four decades, additive manufacturing (AM) technologies have undergone rapid evolution since their initial introduction in the 1980s [1]. An impressive average annual growth rate of 27.4% for the AM industry has further solidified its position as a vital component of the manufacturing landscape [2]. According to *Wohler's Report 2021* [3], despite the challenges posed by COVID-19, the industry experienced significant growth of 7.5% in 2020, reaching a total value of $12.8 billion. This growth is a testament to the increasing adoption of AM in contemporary manufacturing systems.

Furthermore, the demand for Internet integration in both additive and subtractive manufacturing has given rise to the emergence of Cyber-Physical Systems (CPS) [4]. These systems involve the seamless integration of computing and communication systems with the physical realm, enabling more efficient and interconnected manufacturing processes [5]. This integration has led to improved control, monitoring, and optimization of AM processes, resulting in enhanced productivity and quality.

The increasing accessibility of the Internet has made connected systems vulnerable to cyber-related attacks, posing a higher risk of disruptive interventions against AM from various adversaries. According to the *2021 Global Threat Intelligence Report* [6], the manufacturing industry moved from being the eighth most targeted industry by cyber attackers to the second, behind only finance and insurance, with a reported 300% increase in attacks in a single year. Potential CPS challenges originating from both cyberspace and physical surroundings caused by attacks will impact quality, intellectual property (IP), and physical safety [7]. Consequently, critical infrastructure security for both cyber and physical aspects has become an active research area in recent years [8]. Therefore, the necessity for a deep exploration of security issues in AM

inspires this dissertation and motivates researchers' awareness of system defects in the design process [9]. To further expand the security topics in AM, three major contributions have been proposed to bring new ideas for researchers:

(1) Detection of Sabotage Attacks for Additive Manufacturing.

We present a novel power monitoring method to detect sabotage attacks on an AM system. The proposed method evaluates the current signals from motors when printing both the benign control group and the altered group caused by malicious activities. This layer-to-layer comparison enables the detection of any anomalies or deviations in the motor signals between the two groups.

(2) Side-channel Attack on Additive Manufacturing Systems.

To reveal the potential vulnerabilities in AM systems, we present a novel rotation side-channel attack technique that enables the accurate reconstruction of model dimensions without requiring direct access to the original design. By analyzing the rotational data from these motors, we can precisely track the movement and position of the printing head, allowing for a highly accurate reconstruction of the model's dimensions.

(3) Signal Variation Based on Complexity and Print Validation Across AM Platforms.

By analyzing the variances of the signals between the two machines, the relationship between prints' increased complexity and signal variation can be built. Furthermore, utilizing the previously developed anomaly detection method, we can compare the current

signals from each machine to effectively detect any abnormalities in the geometry. This research ensures the authenticity of prints from diverse sources.

The remainder of this dissertation is organized as follows. Chapter 2 discusses the related background information. Chapter 3 presents the literature review. Chapter 4 describes the proposed power-monitoring model based on Dynamic Time Warping (DTW). Chapter 5 presents a method of reverse engineering a CAD model of a part using the motor rotation side channel. Chapter 6 introduces a new experiment to investigate signal variances between the benchmark and the alternative machine. Chapter 7 summarizes the conclusions and provides ideas for future works.

2. Background

Additive manufacturing (AM) provides unique advantages over conventional manufacturing processes [10,11]. One such advantage is the ability to customize specialized parts to a high degree of precision, ensuring an exact fit for specific applications [12,13]. This customization capability reduces the need for excess material, minimizing material waste and lowering costs [14-17]. Another benefit of AM is the ability to rapidly produce dies with complex geometries that would be difficult or even impossible to realize with conventional manufacturing methods [18-22]. The intricate design possibilities of AM, enabled by the layer-by-layer printing process, allow for the creation of parts with complex internal structures and fine details, providing more functionality and reducing the need for assembly [23].

For example, NASA has already developed 3D-printed solar wings to lighten the load and reduce costs with a 3D-printed recycler [24]. The sustainability of long-duration space missions is accomplished through processing raw materials like polyethylene and converting plastic trash into reusable feedstock [25]. Moreover, 3D printing is widely used for air ducts [26], tooling prototypes [27], and even fuel injection nozzles for General Electric jet engines [28]. These examples demonstrate the transformative potential of AM in a variety of application areas.

By the International Organization for Standardization (ISO/ASTM 52900) [29], additive manufacturing technologies are categorized into seven types: (1) Vat photopolymerization, (2) Directed energy deposition, (3) Sheet lamination, (4) Powder bed fusion, (5) Binder jetting, (6) Material jetting, and (7) Fused deposition modeling (FDM). FDM is the most commonly used type, accounting for over 70% market share as of July 2018 [30]. According to *Wohler's Report,* an industry-leading annual survey, A.M. continues the expansion of 7.5% to nearly $12.8 billion in 2020, even though negatively impacted by Covid-19 [31].

Additive manufacturing (AM) is at a higher risk of economic loss due to security failures compared to traditional manufacturing methods because all the essential parameters of the process, from design models to printed parts, are centralized in a single file [32-35]. Significant profits from unlawfully acquired commercial secrets make AM an attractive target for attackers [36]. Security protection is crucial as IP-intensive AM industries is expected to expand at a compound annual growth rate (CAGR) of 20.8% from 2022 to 2030 [37-39]. Currently, most AM security issues occur through the cyber domain, but information leakage through the physical domain still exists [40]. Similarly, integration of the virtual and physical aspects of the AM process fundamentally transforms it into a CPS.

The modernization of critical infrastructure merging with CPS also raises concerns about cyber-physical threats [41-44]. The security matters for CPS in additive manufacturing are mainly composed of two categories, as depicted in Figure 1. These categories are the (1) Cyber scope and (2) Physical scope. For the cyber scope, the interconnectedness of various technologies installed in cyber systems can be a cause of concern, as it creates potential vulnerabilities that can be exploited by cyber attackers [45]. Industrial environments are exposed to a wide range of risks, including cyber threats that can impact people, data, and physical processes, and are among the most prevalent concerns in modern manufacturing [46-48]. For the physical scope, unauthorized exploitation of systems can lead to the theft of intellectual property, making it easy for models to be reconstructed through reverse engineering with the process information emitted as side-channels during operation. These types of attacks are often launched through physical channels [49,50].

However, the traditional IT-based security measures don’t entirely apply to CPS [51]. Cybersecurity systems and CPS are related in computation, communication, and networking [52].

The key difference between cyber-physical attacks and traditional cyber-attacks is that the former adds an extra layer of complexity with physical equipment in which the attack will influence the elements in both cyber and physical domains [53]. Consequently, common updates and IT security patches are incompatible with legacy CPS equipment [54,55]. According to Yampolskiy et al. [56], multiple attack vectors that compromise one or more AM workflow components can be roughly divided into five groups: (1) Actors or workflow roles, (2) Firmware and software, (3) Network communications, (4) Physical supply chain, and (5) Power supply.

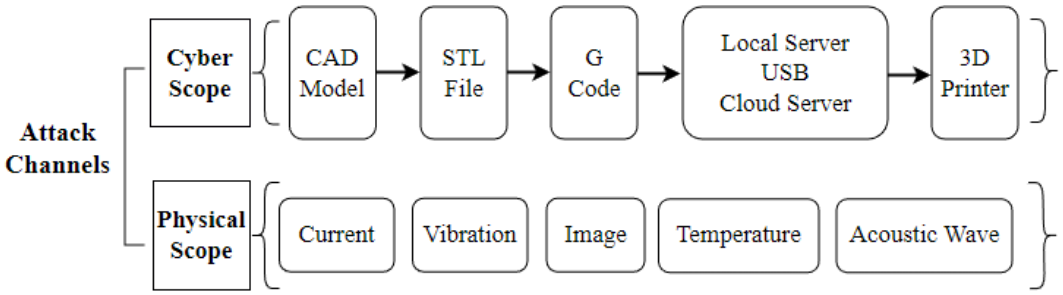


Figure 1. Different attack channels in the cyber and physical scopes for 3D printers.

The typical AM workflow from design to a finished part is also described in Figure 1. Each step may become part of vulnerable channels that could be exploited for attack [57]. After being designed with a Computer-Aided Design (CAD) tool such as SolidWorks, the file is converted to a STereoLithography (STL) file [58,59]. A slicing software, like Cura, converts the STL file into G code to be used by a 3D printer [60]. During printing, the firmware Marlin in the 3D printer translates the G-code into toolpath coordinates and other real-time activities of the machine until the part is eventually printed [61-63]. However, side-channels like acoustic emission [64], temperature [65], image [66], and vibration [67] carry useful information that describes the machine's activity. If these side-channel signals are illegally obtained by continuously monitoring manufacturing parameters, the leaked information can be used to speculate on the operations that

are not intended to be known by outsiders [68]. Consequently, intellectual property such as the geometric design can be reconstructed through reverse engineering [69]. Therefore, intrusion detection and attack methods through system monitoring are the focus of this dissertation.

3. Literature Review

Cyber-physical attacks typically start in digital format and infiltrate through a cyber network, potentially causing physical components such as machines, equipment, parts, assemblies, and products to experience over-wearing, breakage, scrap, or other changes that deviate from the original design [70]. As a result, it's necessary to have a thorough understanding of CPS security issues. This section reviews the literature on cyber-physical attacks, detection, and security incidents, involving cyber-physical manufacturing systems.

Research publications about cyber-physical security can be divided into four categories as shown in Figure 2: 1) Attack Detection, 2) Attack Methods, 3) Security Model Evaluation, and 4) Security Taxonomy.

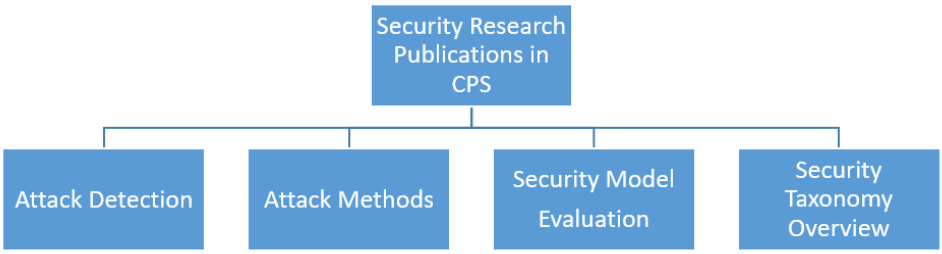


Figure 2. Identified categories for the cyber-physical security research publications in CPS.

The remainder of this section will describe each of these publication categories in detail.

3.1 Attack Detection

Inadequate security during the transfer of data can create vulnerabilities for the theft of technical data and execution of sabotage attacks. As a result, protecting the physical modalities is crucial in detecting any unlawful activities that aim to disrupt normal operations. Understanding system vulnerabilities and the various forms of attack methods is the primary focus of this section.

Yu creates a detection system that can accurately perceive the abnormal status by continuously comparing the collected side-channel data with the unmodified information [71]. Vincent builds a structural health monitoring system with piezoelectric materials to detect a possible malicious Trojan in the production of integrated circuits [72]. A real-time online process monitoring approach is also proposed by Vincent to defend against cyber-physical attacks by analyzing the data collected from sensory devices such as accelerometers, magnetometers, and video cameras [73]. Wu proposes a method to correlate cyber and physical alerts to detect cyber-physical attacks [74]. Chhetri builds up a method to model the behavior of the system through statistically estimating functions that map the relationship between analog emissions (audio) and corresponding cyber domain data (G-code) [75]. Brandman uses a physical hash to take a Q.R. code that contains a hash string of the nominal process parameters and toolpath to strengthen security [76].

J. Straub focuses on the detection of an object that is incorrectly positioned on the printer's build plate. He used an image-based solution by comparing the differences between the expected CAD file and produced object pictures to identify the discrepancies [77]. Straub also suggests a method in a 3D printing system to prevent material misuse [78] . Belikovetsky quantitatively introduces an object verification system to detect attacks with a digital side channel (audio signature) [79]. Gatlin suggests an approach based on the continuous monitoring of current supplied to individual stepper motors during a print and detects anomalies after comparing with a benign process [80]. Prakash introduces an image processing technique that analyzes the amplitude and phase variations in a series of sequential still images that represent frames of animation to filter if the intentionally introduced error sample has been detected [81].

3.2 Attack Methods

The extensive use of computerized systems in manufacturing processes and their broad application areas make CPS an attractive target for attacks. For example, in April 2021, hackers breached the Colonial Pipeline using a compromised password and forced the oil giant to pay $4.4 million as a ransom [82]. AM, being a highly information-integrated industry, is more vulnerable to these types of attacks. Therefore, a comprehensive understanding of attack methods is crucial for ensuring the security of AM systems [83].

Al Faruque is the first to successfully reconstruct a simple prototype by using the extracted audio data from the 3D printer at work, which draws attention to the vulnerability of additive manufacturing [84,85]. Backes has recovered 72 % of all the words printed by a dot-matrix printer with a microphone [86]. Burgess replicates the keyways with a 3D printer by taking a picture of the lock [87]. Mahan uses a simulation method based on G-code to accurately predict the physical output of a fused deposition modeling additive manufacturing machine in terms of both physical and digital artifacts [88]. Sturm introduces a technique focusing on attacking STL files and inserting voids in the tensile specimen, which affects the strength of the specimen [89]. Moore installs malicious firmware on the 3D printer replacing previous versions of the software to prove the vulnerabilities in the design of the data transferring process could cause an accident in industrial production. Quang Do proposes an attack method through protocols between clients and 3D printers. They impersonate a legitimate client using a Raspberry Pi connected to the network so that the printers can be remotely manipulated.

3.3 Security Taxonomy and Overview

In this section, we present a paper review on security taxonomies for multiple domains to specify the nature of attacks, with a focus on AM attacks and data theft. We also introduce security overviews and defense measures from various application areas.

Yampolskiy *et al.* thoroughly summarize all the publications on AM security in recent years [90]. Attack method and attack targets are both discussed in the way of taxonomy in two major security concerns: theft of technical data and sabotage of the AM process. Yampolskiy *et al.* outline the additive and subtractive manufacturing workflows [91]. He also proposes a framework for analyzing attacks on or using additive manufacturing systems and presents the major threat categories. The differences between the two workflows are identified to compare the two manufacturing paradigms from a security perspective, and the attack analysis framework is applied to demonstrate how the differences grow into threats. The analysis reveals that, while there is significant overlap concerning security, fundamental differences in the two manufacturing paradigms require a separate investigation of additive manufacturing security.

Elhabashy *et al.* propose an attack taxonomy that governs the relationships between quality control (QC) systems, manufacturing systems, and cyber-physical attacks in the context of malicious process changes [92]. The taxonomy was developed from a quality control perspective. The research is created from the attacker's perspective to aid manufacturers in understanding existing vulnerabilities and securing production systems against cyber-physical attacks.

Wu *et al.* propose a taxonomy for cross-domain attacks on cyber manufacturing systems (CMS) in four dimensions: attack vector, attack impact, attack target, and attack consequence [93]. This work provides a common language for cross-domain attacks in the manufacturing discipline

and helps researchers from both cyber security and manufacturing fields to better understand the nature of attacks in a CMS environment.

Lun *et al.* aim to identify, classify, and analyze existing research on CPS security with 118 primary studies as a result of the systematic mapping study [94]. This work presents a powerful comparison framework for existing and future research on this topic. It provides a reusable comparison framework for understanding, classifying, and comparing methods or techniques for CPS security. Besides, the proposed systematic review of current methods and techniques for CPS security is useful for both researchers and practitioners.

3.4 Security Models and Evaluation

Researchers have proposed various models to simulate or evaluate CPS vulnerabilities under various attacks, in order to identify optimal defense strategies [95]. System parameters such as reliability, availability, and stability are tested to improve CPS integrity [96].

Yu *et al.* utilize generalized stochastic Petri nets to model the system with three metrics: reliability, availability, and security to quantitatively measure the trustworthiness of the system [97]. A dynamic model that considers the spread of the malicious software is used to simulate the possible cyberattacks to analyze the system's behavior while under attack. As a result, the trustworthiness of the systems can be evaluated.

Zarreh *et al.* create a model using game theory to qualitatively analyze manufacturing systems rather than quantitative methods to address cyber-security threats. This method mainly focuses on finding the optimal defense strategy to defend against cyber threats. They use a zero-sum theory to model the trustworthiness of a system under cyber threats and analyze the different defense policies to encounter these attacks [98].

DeSmit *et al.* propose a systematic method for assessing cyber-physical vulnerability [99]. They represent manufacturing processes as intersection maps of different entity types. He uses decision tree analysis to evaluate the impact of vulnerabilities. The paper provides an approach for systematically identifying cyber-physical weaknesses and analyzing their potential impact on intelligent manufacturing systems in each intersection node.

Orojloo *et al.* suggest a new method that captures the dynamic behavior of CPS with and without attacks as well as models the impact propagation of attacks [100]. With the decision-making trial and evaluation laboratory (DEMATEL) method, the proposed method ranks the critical assets of CPS based on their sensitivity to disturbances and measures the direct and indirect consequences of attacks against them.

In general, protection, detection, and mitigation are the three fundamental approaches for countering attacks when developing treatment models [101]. However, none of the existing works offer a fast and accurate model for detecting anomalies in cyber-physical systems with signal power monitoring. Hence, we propose a novel power-monitoring model based on Dynamic Time Warping (DTW) to detect malicious activity in a polymer AM process. Building on this foundation, signals from other machines with the same make and model could be utilized to compare with the signal from the prototype machine, allowing for remote verification of the model's accuracy. Moreover, a reverse engineering approach other than the acoustic channel is proposed to expose the potential weakness in information integrity to prevent data leaking and IP theft. The primary objective of this dissertation is to develop a detection system and identify vulnerabilities in cyber-physical systems that could be unlawfully exploited, thereby contributing to enhancing CPS security.

4. Smart Voids Detection

The combination of digital and physical representation in 3D-printed objects increases their complexity and potential risks [102]. Once the system is compromised, the corrupted file may result in product failures, leading to injuries, litigation, or product recalls [103]. Malicious attacks in AM can cause potential quality issues, some of which are visible, while others like secretly-placed voids, may be intentionally concealed and remain unnoticed on the surface [104]. The voids can significantly affect the mechanical properties of the printed parts under load [105]. The invisibility of voids within the printed parts poses a significant challenge to quality assurance, as they may pass inspection and quality checks [106]. To mitigate these risks, an efficient and precise method is proposed for detecting anomalies during production.

4.1 Proposed Model Methodology

We propose a power monitoring model based on dynamic time warping (DTW) to monitor the current signals to detect voids in an AM part and determine the minimum detectable size of the voids. In this section, we outline the basic concept for the proposed power monitoring model and explain the detail of the current signal slicing and DTW.

4.1.1 Model Overview

The overall framework of the proposed model is illustrated in Figure 3. The moving direction of the Fused Filament Fabrication (FFF) nozzle is controlled by the combination of X-axis, Y-axis, and Z-axis motors. The current signal on each motor can be collected as a channel of current data to develop a data-driven model [107]. Each part geometry corresponds to specific current signals from those motors, so any geometric modification in one layer will alter the signal. Therefore, the deviation can be detected by comparing the corresponding data obtained by the printed part in each

channel with the signal in normal conditions. The detection of attacks is achieved by evaluating the signal discrepancy with thresholding.

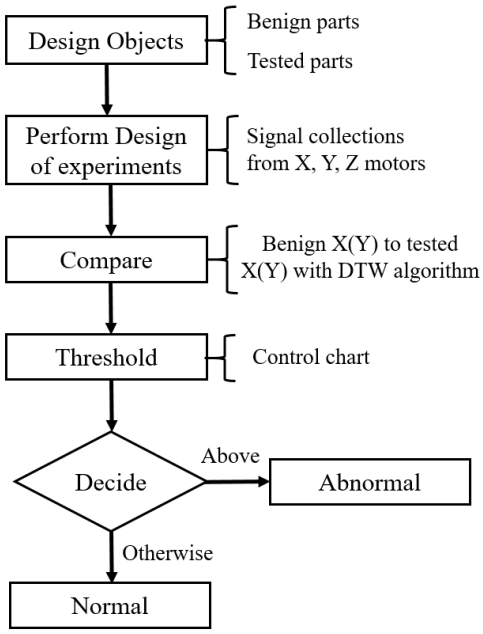


Figure 3. The framework of the proposed methodology.

4.1.2 Model Design

Any abnormal geometry of the printed part can be indicated by the current signals of the motors. Figure 4 shows the discrepancy between the current signals for an original part and the signals for an attacked part from all channels. (a) original signals from three sensor channels on the normal part; (b) signals on the attacked part. The discrepancy is indicated in the black box. All the signal data from the original part serve as a benign or control group for comparison. We propose a power monitoring model based on DTW to detect the deviation caused by possible sabotage attacks in the part geometry. DTW is an algorithm for measuring the similarity between two temporal sequences (e.g., current signals). DTW has the following advantages in modeling [108]: (1) it compares the similarity between two temporal data sequences with different lengths; (2) it has

high precision on the result; (3) it enables faster calculation by parallel computation. DTW has many applications, including speech, handwriting, and gesture recognition [109]. It is particularly useful in situations where two sequences have different lengths or are distorted in some way, as it can handle temporal variations and deformations.

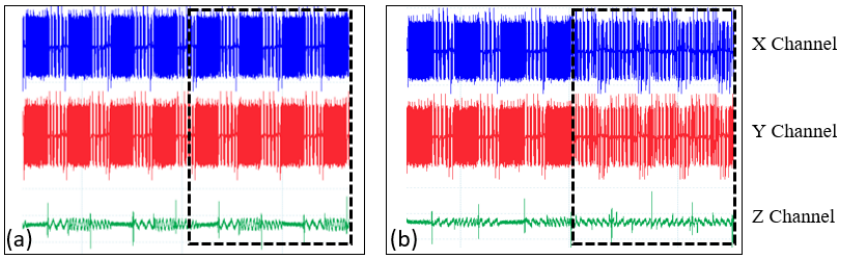


Figure 4. Original signal comparison between the normal and altered prints.

During the AM printing process, the motor moving along the Z-axis will lift the nozzle by one layer height and start printing the next layer when one layer is finished printing. That is the time when the peaks occur in the current signal on channel Z for the entire process, as shown in Figure 4. The small fluctuation between the peaks is caused by noise in the oscilloscope and probe system.

The duration between peaks in Z channels indicates the printing on a layer. It means motors on the X-axis and Y-axis are moving while the motor on the Z-axis is idle. Therefore, the time at these peaks is used to slice the signals the X and Y channels. Each sliced signal is for a specific layer, as shown in Figure 5. Each interval in the Z signal forms a black box. The first layer in the original group compares to the first layer in the altered group, continuing until the last layer.

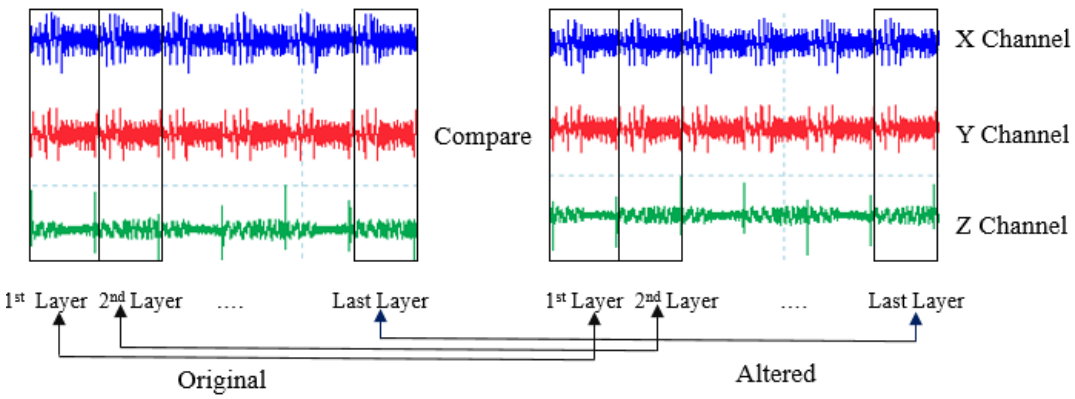


Figure 5. Comparison procedures.

After slicing, we compare the original signals (in the X channel and Y channel) of the normal part to the altered signals of the attacked part. The DTW algorithm is adopted to calculate the similarity for each sliced signal sequentially. Any abnormality will give rise to an increase in the comparison result from the DTW calculation. Given the layer-by-layer comparison mechanism, this DTW-based monitoring model not only detect the attack but also identify layers on which the anomaly exists.

4.1.3 Model Development and Algorithm Design

The proposed power-monitoring model based on DTW has two stages of signal processing. The first stage (Table 1) is to segment the current signals for the normal part and the attacked part and the second stage (Table 2) is to compare and calculate the similarity using DTW.

Taking current signals in channel X as an example, Table 1 implements signal segmentation, and its pseudo-code is shown below.

Algorithm 1 : SegmentByPeak

Input: Time-series data of signal X in Z axis $(XZ_1, \ldots, XZ_N)$ where N is the length of X, peak threshold σ, window size ω

Output: $List_{\text{Xseg}} = [x_1 x_2, \ldots, x_K]$ is the list of segments of X where $x_i = (s_i, e_i)$ is the start and end datapoint of i-th segment.

1: Initialize $List_{\text{pcaks}}$ as an empty list.
2: **for** $i = 1, \ldots, N$ **do**
3: **if** $|XZ_i| \geq \sigma$ **then**
4: Determine if $|XZ_i|$ is a peak by comparing to its neighbors in a range of ω. If yes, append i in $List_{\text{pcaks}}$
5: **end if**
6: **end for**
7: $List_{\text{pcaks}} = [p_1, \ldots, p_T]$ where T is its length.
8: Initialize $List_{\text{Xseg}}$ as an empty list, $s_1 = 1$.
9: **for** $t = 1, \ldots, T-1$ **do**
10: Determine e_t and $s_t + 1$ based on p_t and p_{t+1}
11: Append (s_t, e_t) to $List_{\text{Xseg}}$
12: **end for**
13: $e_T = N$, append (s_T, e_T) to $List_{\text{Xseg}}$

Table 1: Segment by peaks.

In Lines 2 to 6, the time stamps when the peaks on the signals in channel Z occur are marked on the timeline, and they are used to determine the changes in layers. The total number of peaks must equal the number of layers of the part. Two parameters from these timestamps are set to identify the position of the potential voids (caused by attacks): the peak threshold and the window size between two peaks in channel Z. Both parameters need to be properly set so that all the peaks of the current signals in channel Z can be correctly recognized. Otherwise, the unrecognized peak will lead to missing the counted number of layers. Line 7 to 12 depicts how the signals in channel X are segmented according to the same time indexes obtained from channel Z. Line 13 stores all the segmented signals in a list.

In Table 2, the segmented signals for the normal part and the attacked part in channel X denoted as $SegBenignX_t$ and $SegX_t$, are sequentially compared using DTW. DTW works by measuring the distance between corresponding elements of the two sequences at each time point and then finding the optimal path that connects these points with minimum cumulative distance. Even if the signals have different lengths and are not aligned in time, DTW aligns the two

sequences in a way that minimizes the distance between them. The distance metric between corresponding elements used here is Euclidean distance.

Algorithm 2 : SeriatimComparison

Input: Segment lists of signal $List_{\text{Xseg}}$ and $List_{\text{BenignXseg}}$ with length K.
Output: $List_{\text{DTW}} = [L_1, L_2, \ldots, L_K]$ is the list of segment-wise DTW distances of X and $BenignX$.

1: Initialize $List_{\text{DTW}}$ as an empty list
2: **for** $t = 1, \ldots, K$ **do**
3: Determine the segment of X based on $List_{\text{Xseg}}[t]$. // Do the same for BenignX. Denote the segments as $SegX_t$ and $SegBenignX_t$, with their length m and n
4: **for** $i = 1, \ldots, m$ **do**
5: **for** $j = 1, \ldots, n$ **do**
6: $c = |SegX_t[i] - SegBenignX_t[j]|$
7: $\text{dtw}[i, j] = c + \min\{\text{dtw}[i-1, j], \text{dtw}[i, j-1], \text{dtw}[i-1, j-1]\}$
8: **end for**
9: **end for**
10: $L_t = \text{dtw}[m, n]$. Append L_t to $List_{\text{DTW}}$
11: **end for**

Table 2: Seriatim comparison.

The formed m-by-n grid is calculated by the alignment of $X[i]$ and $BenignX[j]$. The warping path maps the elements in the grid to find the minimum distance. Line 2 to 7 is the optimal path computed by Equation 1, where d is the Euclidean distance [110]:

$$D_{min}(i_k, j_k) = \min_{i_{k-1}, j_{k-1}} D_{min}(i_{k-1}, j_{k-1}) + d(i_k, j_k | i_{k-1}, j_{k-1}) \quad (1)$$

Line 10 is the overall distance between the two signals by Equation 2 and adds them to a list $List_{PEAKS}$.

$$D = \sum_k d(i_k, j_k) \quad (2)$$

When the list length equals the total number of layers, all signals are correctly segmented. The generated minimum distance is the final similarity result to the specific layer. The last step is to normalize the comparison result. The calculated DTW result for each segment will be divided by its length to represent the dissimilarity in proportion.

4.2 Experiment And Analysis

In this section, we present our experimental setup and analyze the data collected from the current sensors. Additionally, the threshold that is used to determine the abnormality of a layer is identified. We also evaluate the detection capability of the proposed method by inserting different voids into AM parts.

4.2.1 Experimental Platform Setup

Figure 6 shows the experimental platform for the data acquisition system. Capturing current data is a non-invasive process. Three current probes (Picotech 60A (TA018)) are utilized, each of which converts the current flowing through a conductor into a voltage that can be observed and measured on the PicoScope 5000 series oscilloscope. The remainder of the experimental apparatus consists of a laptop and a FFF printer (LulzBot TAZ 6) with 2.85mm PolyLite PLA filament. For the software, we use Autodesk Fusion 360 to design the printed part. Marlin firmware in the Lulzbot printer translates the G-code created by the slicing tool Cura-Lulzbot into commands for the printer.

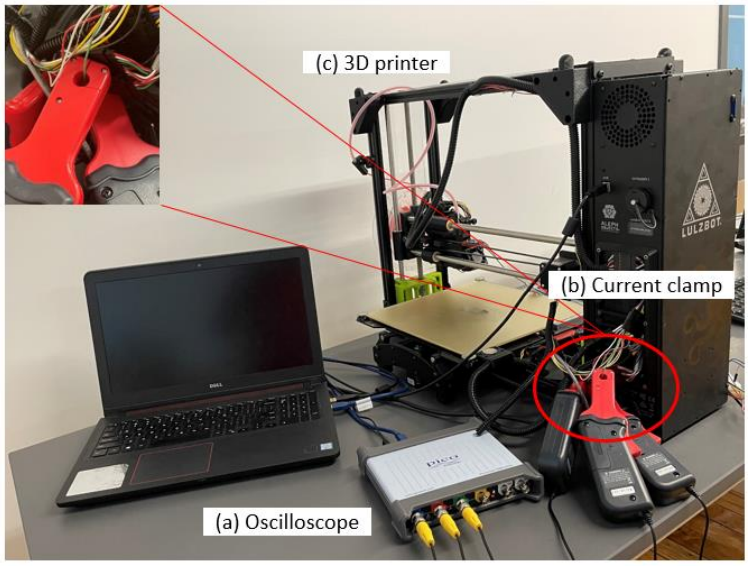


Figure 6. Experimental platform: (a) Oscilloscope, (b) Current Clamp, (c) 3D printer.

To save printing and data processing time, we set the "infill rate" of the printing process to 20% for all experiments. All other parameters of the printer are the default settings in the conducted experiments. According to Nyquist–Shannon theorem, the sampling rate of the oscilloscope is running at 100KS/s to be at least twice the highest non-noise frequency of the original signal [111].

4.2.2 Conducted Experiments

Among all the quality failures in FFF, a maliciously-placed hollow void inside a part can lead to destructive consequences in load-bearing applications [112]. The voids hidden inside the part geometry cannot be found easily since the exterior remains unchanged. The mechanical performance of the prints, like hardness, will be compromised. We will target such malicious attacks on FFF parts in the experiments.

The dimension for all the printed parts is designed to be 10mm×10mm×20mm. The internal geometry of the modified part contains two hollow voids at size 5mm×5mm×4mm. Figure 7 is the CAD model of the attacked part, and Figure 8 shows the actual printed part.

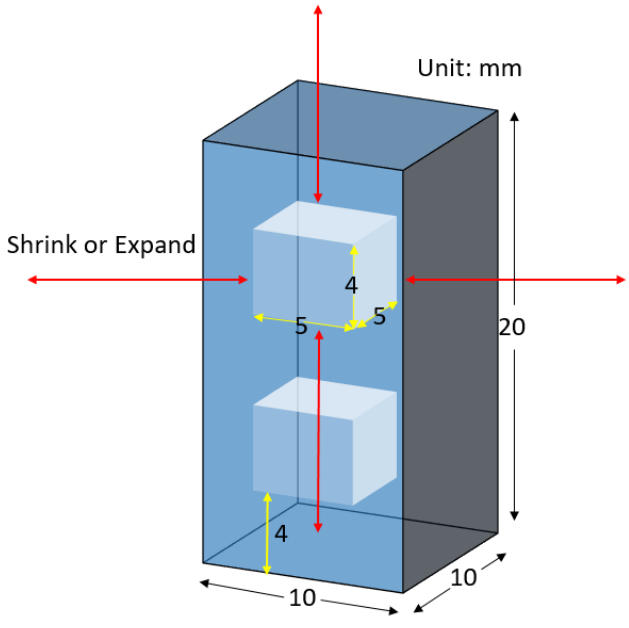


Figure 7. Perspective view for the altered part from the CAD model.

Figure 8. FFF Printed part with two voids inside.

Two types of CAD model is printed. One is the parts without a void, constituting the benign group under normal conditions. The other is the parts with two voids, constituting the altered group after the malicious attack. After getting the comparison result, we use a threshold value to determine the abnormal signals in channel X and channel Y, indicating the voids at certain printed layers. To find the smallest detectable size of the void, we gradually shrink its size in our experiments while keeping the exterior unchanged.

4.2.3 Detection Results

As the comparison result has been normalized, the y-axis represents proportions, i.e., the dissimilarity level. Figure 9 is the two detection results for *benign to benign* and *benign to altered groups* with void size 4mm×4mm×4mm. The abrupt increases in the discrepancy in channel X and channel Y indicate the locations of the two voids, i.e., the layers in the parts. The first detected void appears at layer 10 (highlighted by the red circle). According to the CAD model in Figure 7, the actual void should be 4mm away from the bottom of the part, i.e., layer 16, considering each

layer height is 0.25mm. There is a six-layer difference between the CAD model and the final detection result.

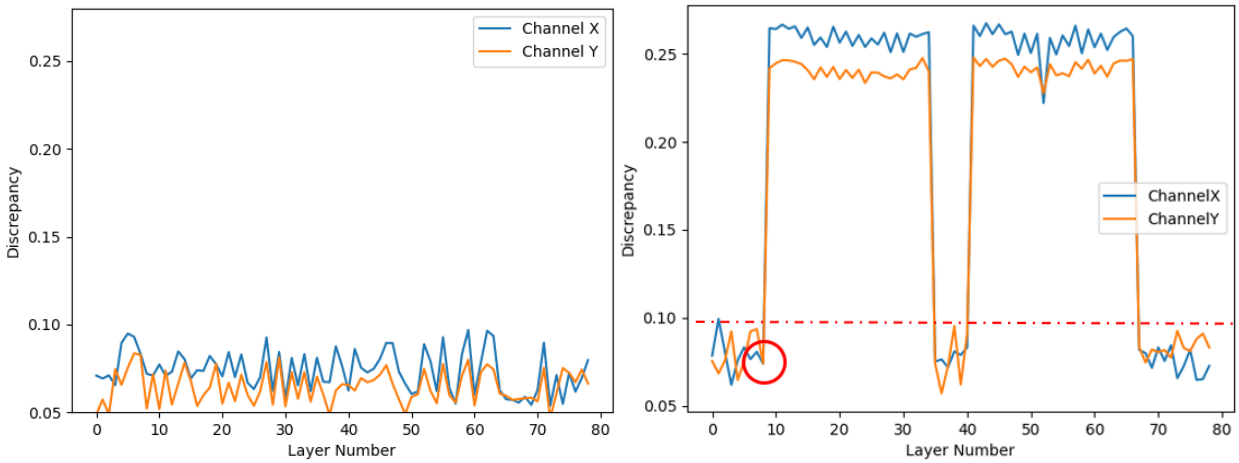


Figure 9. Detection results for "benign to benign groups" and "benign to altered groups".

Figure 10 is the actual infill rate layout when the default value is 20% for the benign part and the altered part. Due to the overhang [113] above the void, the infill rates for the layers around the voids are automatically increased to 100% to build a supporting plate so that later material can be deposited to create the voids.

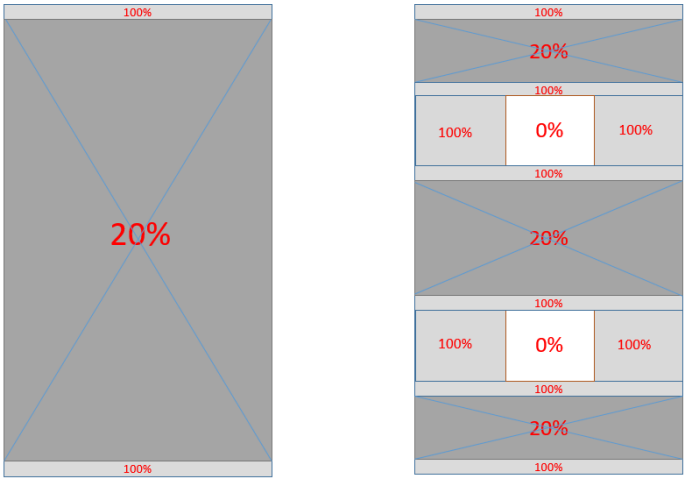


Figure 10. CAD models for the benign and altered parts with actual infill rate layout at 20%.

4.2.4 Criteria for Identifying Sabotage Activity

To identify the abnormal layer, we use a threshold from an $\bar{x}$ Chart (also known as an Individual Chart) [114]. The discrepancies between benign signals are calculated. We use 60% of the data as a training set to obtain the threshold, and the remaining 40% is used to evaluate the threshold. The following are the detailed steps:

First, we gather a pool of 240 benign data samples, and after removing data with significant noise, we retain 234 samples. When the motor is idle, the signal typically fluctuates within a range of -0.4 to +0.4 (A). However, any signals that exceed this range are considered outliers and are not included in our dataset. Then we use uniform distribution to randomly pick two of the samples without replacement and compare them to get an upper control limit (UCL) for both X and Y channels. For a single experiment, the discrepancy for two benign signals is calculated to obtain the UCL, as shown in Figure 11. The UCL in Individual Chart for X and Y Channel works as the threshold values.

Second, we calculate the average value for the 117 pairs of UCL results from 234 samples and get 0.098 for X and 0.097 for Y, with standard deviations of 0.013 and 0.015, respectively. Then we select the 0.098 UCL as the threshold, as shown in Table 3. The threshold here is the strictest criterion to claim whether it is an anomaly. Since the training data are all benign samples, we could adjust the threshold within three sigmas to incorporate all points below the threshold.

Third, we collect 60 altered data with voids and 60 benign as our test dataset. We use four different sizes of voids 1mm×1mm×1mm, 0.75mm×0.75mm×0.75mm, 0.5mm×0.5mm×0.5mm, 0.25mm× 0.25mm × 0.25mm. Each pair of voids are placed inside 15 different symmetrical positions. The reason we use a symmetrical structure is there might be a chance that an outlier appears in the void position, “pretending” to be detected. But the symmetrical structure can cancel

out this randomness as it's impossible that the detection are all caused by the outliers. Then we apply the threshold in the testing data to seek the detection rate in the next part.

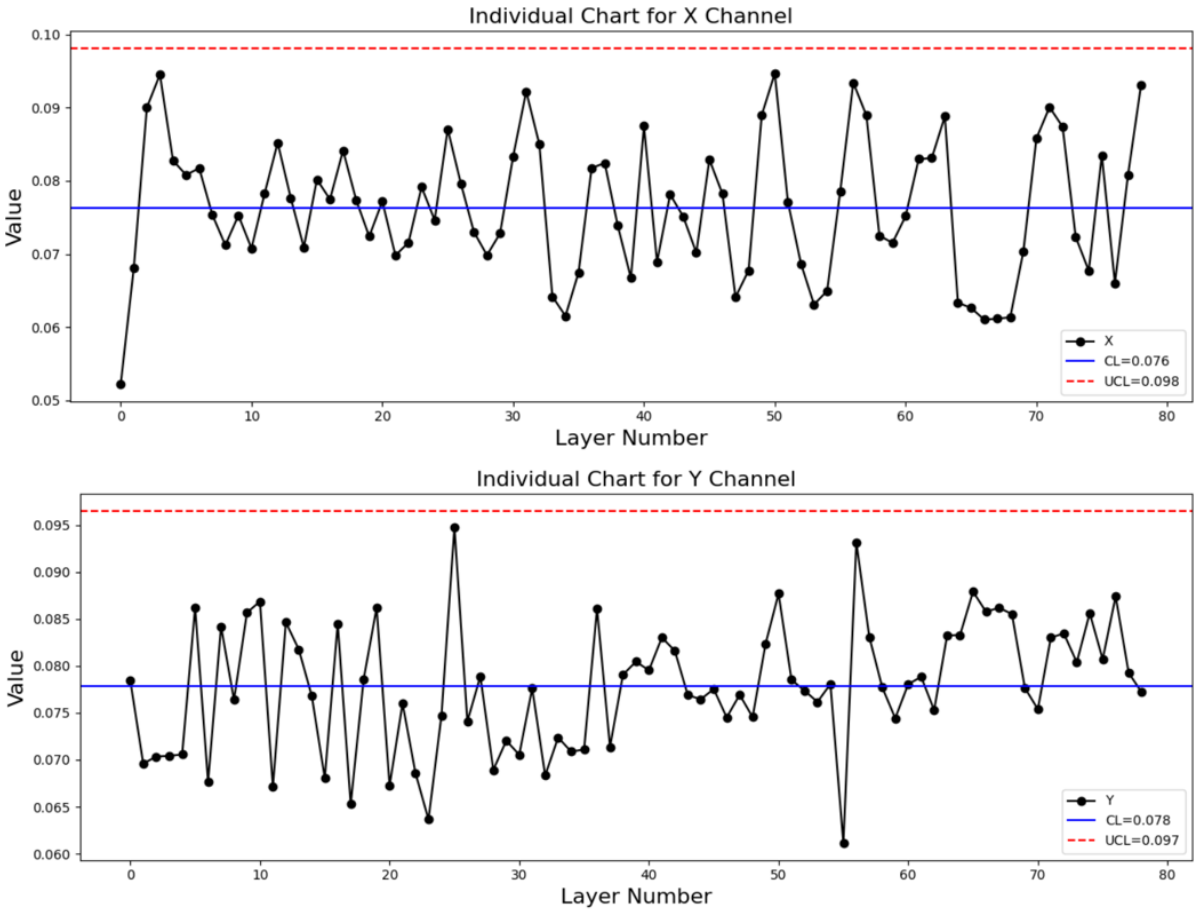


Figure 11. The threshold in UCL for X and Y Channels.

Channel	Training Data	Average Threshold	Testing Data
X	234	0.098	120
Y	234	0.097	120

Table 3: The dataset and threshold from X charts in channel X and channel Y.

4.2.5 Model Accuracy

In the testing data set, we provide 60 altered data for four void sizes at 15 positions. Then we randomly pick 15 benign data in sequence with uniform distribution from 60 benign datasets to match with each of the four void sizes groups. To find the detection rate of our method, we use 15 benign data to respectively compare with the 15 altered data for each of the four different void sizes and compare 15 benign data with another 15 benign data. The result is shown in Table 4.

Channel	Void sizes	No. of samples with voids (altered)	Correctly Detected	TP Rate	No. of samples without voids (benign)	Correctly Detected	TN Rate
X	0.25 mm	**15**	**14**	93.3%	15	15	100%
	0.50 mm	15	15	100%	15	15	100%
	0.75 mm	15	15	100%	15	15	100%
	1.00 mm	15	15	100%	15	15	100%
Y	0.25 mm	**15**	**14**	93.3%	15	15	100%
	0.50 mm	15	15	100%	15	15	100%
	0.75 mm	15	15	100%	15	15	100%
	1.00 mm	15	15	100%	15	15	100%

Table 4: Comparison results for different void sizes from X and Y channels.

For void sizes 0.50 mm, 0.75 mm, and 1.00 mm, the results are all correctly detected or classified in both X and Y channels, so the True Positive (TP) and True Negative (TN) rates are 100% [115]. But for 0.25mm size, there is one specimen that fails to be detected in the X channel, and one specimen that fails to be detected in the Y channel. Actually, “the failed-to-be-detected specimens” for 0.25mm is two different ones or at two different void positions. In other words, one altered specimen is detected with voids by X channel but fails to be detected by Y channel, while the other altered specimen is detected with voids by Y channel but fails to be detected by X channel. The 15 specimen results for the 0.25 mm void is shown in Table 5. To clarify, when we refer to "X and Y," it means the signal is detected by both the X and Y channels simultaneously. On the other hand, when we mention "X or Y," it means signal is detected by either the X channel or Y channel.

Consequently, the number of correctly detected specimens is 13 for "X and Y" and 15 for "X or Y." “Yes” means the void is successfully detected, while “No” means the void is not detected

Altered Specimens Number	1	2	3		15	No. of Correct Result
X	**Yes**	**No**	Yes	…	Yes	14/15
Y	**No**	**Yes**	Yes	…	Yes	14/15
X and Y	**No**	**No**	Yes	…	Yes	13/15
X or Y	**Yes**	**Yes**	Yes	…	Yes	15/15

Table 5: Detection results of 15 specimens for 0.25mm void.

To measure the detection rate, we utilize the accuracy of the confusion matrix as a representation. Table 6 is the confusion matrix for the altered data with 0.25 mm voids in channel X. Since the detection result is the same as that of channel X, the confusion matrix for the Y channel is also the same. The accuracy is 96.7%.

Truth	Prediction	
	Altered	Benign
Altered	14	0
Benign	1	15

Table 6: Confusion matrix for X/Y channel in 0.25mm void.

Table 7 is built using all the data from the X channel, and the same applies to the Y channel. The accuracy is 99.2%.

Truth	Prediction	
	Altered	Benign
Altered	59	0
Benign	1	60

Table 7: Confusion matrix for X/Y channel in all void sizes.

Table 8 combines the data from channel X and channel Y using the "X or Y" criterion to accurately detect and classify every altered or benign data instance. The accuracy is 100%.

Truth	Prediction	
	Altered	Benign
Altered	120	0
Benign	0	120

Table 8: Confusion matrix for all data ("X or Y").

If an attack truly happens, the signal X and Y will usually follow the same trend in both affected and unaffected sections. When employing the power-monitoring method, if the deviation in either channel X or channel Y exceeds the threshold, it indicates the presence of abnormal layers that may have been compromised by potential malicious activity.

0.25mm Detection Rate	Single Channel Detection Rate	Overall Detection Rate
96.7%	99.2%	100%
96.7%	99.2%	

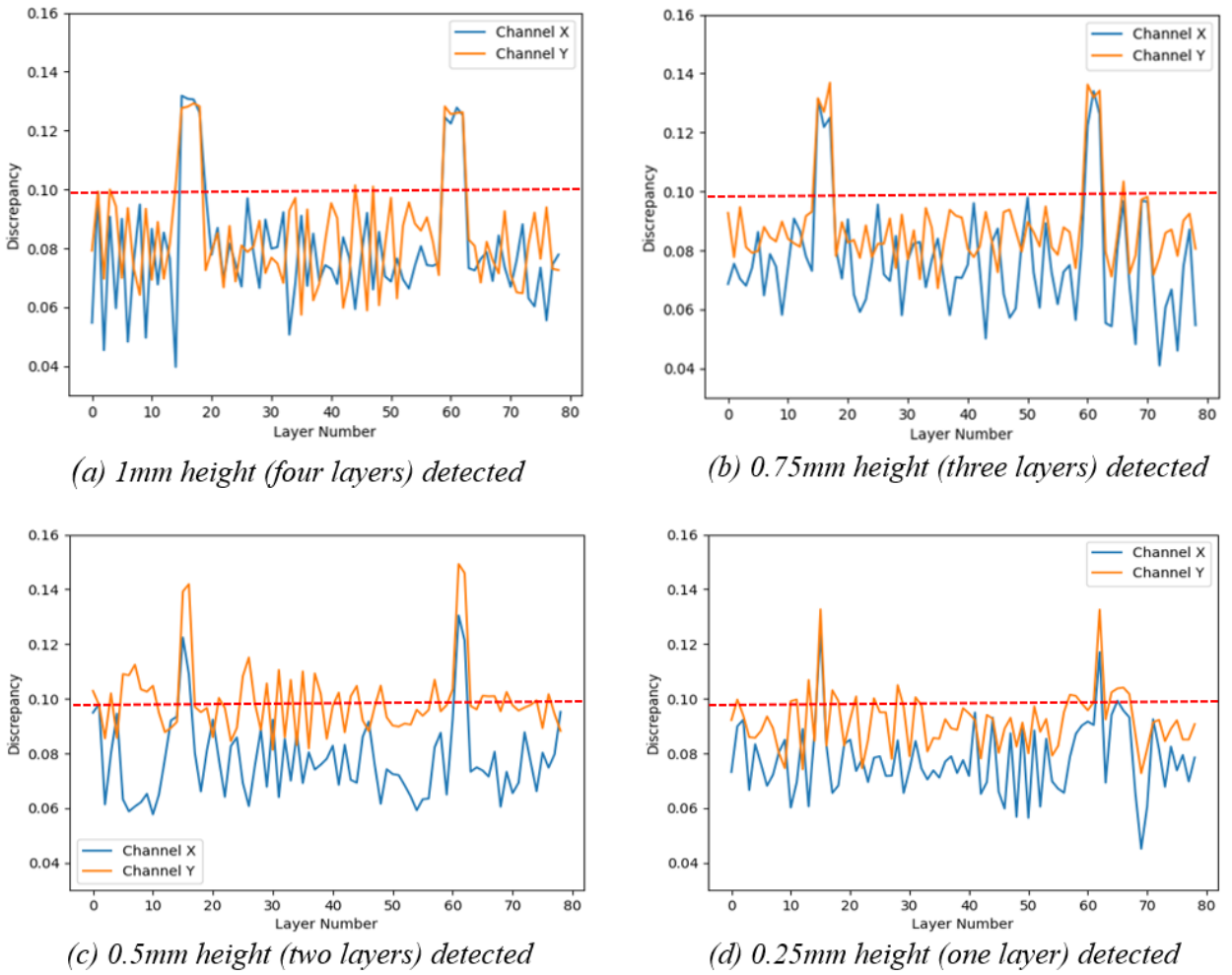
Table 9: Detection rate for different levels.

This criterion eliminates the possibility that one of the signals is accidentally lower than the threshold to be detected. Therefore, we decide to take "X or Y" as the final detection rate. As a result, the detection rate for each level, from low to high, is presented in Table 9.

4.2.6 Detection Capability

To find the detection limit of the proposed power-monitoring method, we gradually reduce the size of the inner voids. Detection outcomes for four different void sizes are presented in Figure 12. Their sizes are (a) 0.25mm×0.25mm×1mm, (b) 0.25mm×0.25mm×0.75mm, (c) 0.25mm×0.25mm×0.5mm, and (d) 0.25mm×0.25mm×0.25mm. It is noted in Figure 12 that the

number of data points above the threshold for each void is reduced by one as the void size decreases. For example, for voids with size 0.25mm×0.25mm×1mm, the height should contain four layers (layer height is 0.25mm), as shown in Figure 12 (a).



(a) 1mm height (four layers) detected

(b) 0.75mm height (three layers) detected

(c) 0.5mm height (two layers) detected

(d) 0.25mm height (one layer) detected

Figure 12. Detection outcomes for four different void sizes.

For the voids with a height smaller than 0.25mm, Figure 13 shows the proposed method cannot effectively detect them because this feature is too small, given the filament size of the additive process.

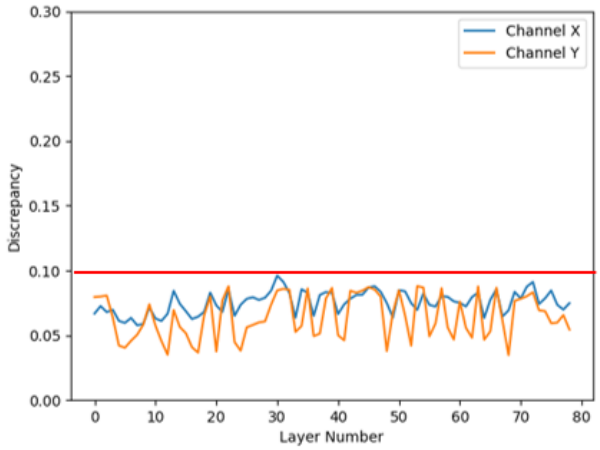


Figure 13. The detection outcome for a void smaller than 0.25mm.

Therefore, the minimum detectable height of the voids is equal to the filament size in this process. The minimum detectable width and length will also correspond to 0.25mm or equivalent to the filament size. The size of the largest printable and detectable void in the current FFF part is 9mm×9mm×18mm due to the dimensions of the nominal part.

4.3 Case Study Analysis

This section presents the case study in Figure 14 to demonstrate the method's effectiveness. In Case 1, we insert a minimum void inside of the original part and set the infill rate for the entire part to 20%. In addition, a new shape is designed with two random voids at a 100% infill rate to test the method's detectability under different circumstances. In Case 2, we set the infill rate to 100% to cancel out the surrounding auto-filling, allowing us to test whether the voids' position is aligned with the detection result.

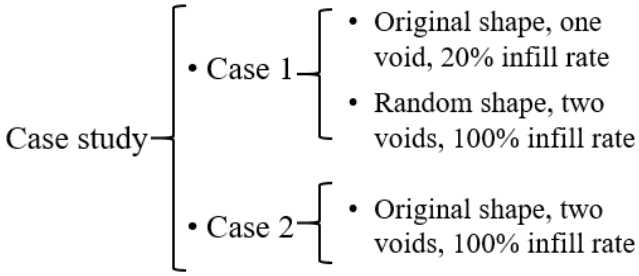


Figure 14. Outline for case study under different conditions.

For Case 1, we deliberately introduced a single void whose size is 0.25mm×0.25mm×0.25mm within the part, as depicted in Figure 15. This particular void size was selected to assess the limits of the proposed method. If the proposed method can effectively detect the minimum void size, it implies that any voids larger than the minimum size will also be detected accurately. The detection capability demonstrated with the smaller void establishes the method's sensitivity and reliability, providing the fact that it will successfully identify larger voids as well.

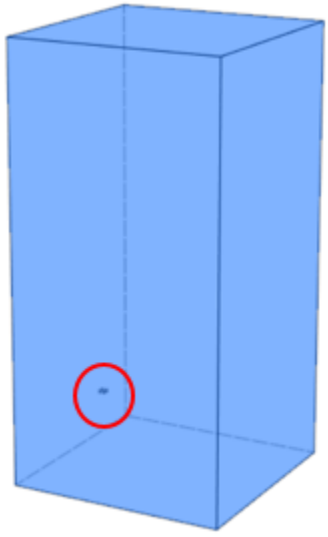


Figure 15. CAD view for the original shape with one void.

Figure 16 validates the model's detection capability by correctly identifying that only one data point should exceed the threshold.

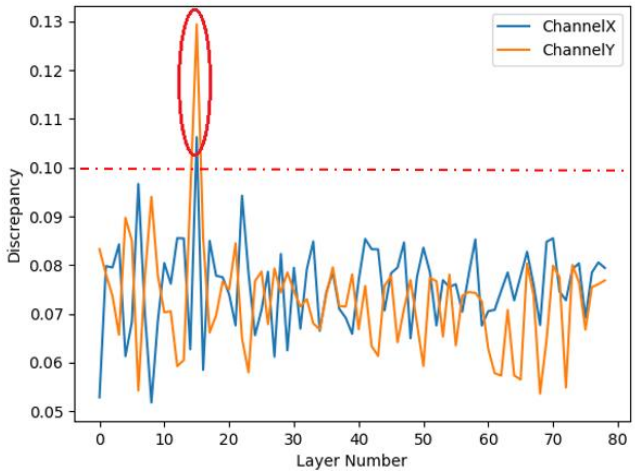


Figure 16. Detection result for original shape with one void.

Then we use a random shape (e.g., a cylinder) in Figure 17 with two voids (0.25mm×0.25mm×0.25mm) and increase the infill rate to 100%. It shows that the proposed power-monitoring model still performs well with the correct detection of the two voids in Figure 18.

Figure 17. CAD view for random shape with two voids.

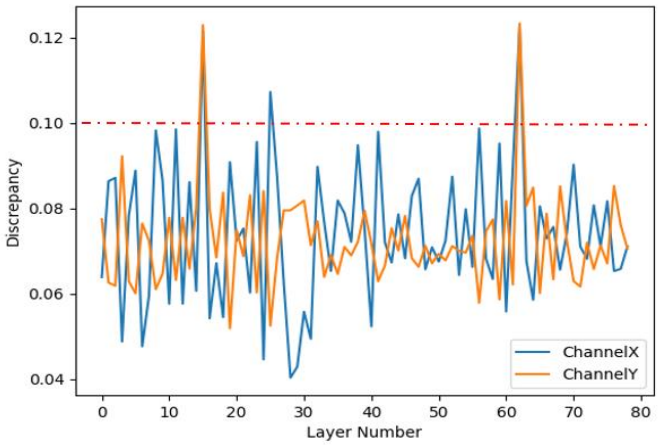


Figure 18. Detection result for random shape with two voids.

For Case 2, we design two voids (4mm×4mm×4mm) in the center position (4mm from the bottom and top) of the FFF part. We use the infill rate 100% to better mimic a real solid part, including the areas around the voids. Figure 19 shows the detected abnormal layers perfectly match the designs.

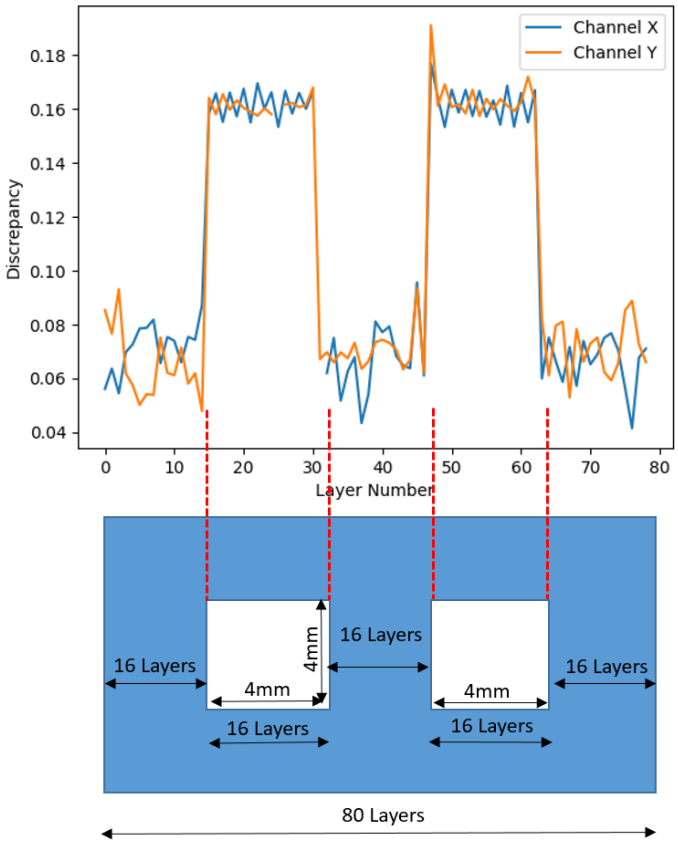


Figure 19. Signal alignment with 100% infill rate.

Compared with the width of the voids in Figure 9, the width in Figure 19 is narrower because the infill rate around the voids is the same as that in the benign part. Consequently, the proposed model will detect a narrow abnormal area due to the smaller width of the voids. For the other infill rate between 20% and 100%, the result will be the same as Figure 9, as their surrounding infill rates will all automatically increase to 100% regardless of the set value.

4.4 Contribution Summary

In this contribution, we propose a novel power monitoring method based on DTW to detect sabotage attacks on an AM system, specifically inserting unwanted voids inside FFF parts. To detect such voids, the current signals from the benign control group and altered group caused by malicious activity are evaluated through layer-to-layer comparison. If the discrepancy for any layer

exceeds the threshold, it is identified as the abnormal layer. The minimum void that can be detected is 0.25mm×0.25mm×0.25mm, with the height equal to the layer thickness. In the case study, the detection accuracy of the proposed method is at least 96.7%. Moreover, the model reveals the specific layers where the voids locate. With the layer-to-layer comparison mechanism, the method is particularly suitable for the FFF. This work will provide guidelines and significance of reference for sabotage attack detection in FFF and other AM processes.

In the future, multiple aspects of the current research can be expanded. For instance, the approach can be applied to temperature-related sabotage [116], which significantly impacts overall quality. One of the possible sabotage attacks is changing the temperature setting. For example, the default temperature for the nozzle is reduced, causing a material jam in the extruder nozzle. Future research will adopt another current clamp to monitor the extruder motor. Any block inside the nozzle will increase the workload on the extruder motor [117], affecting the current trace. Furthermore, the proposed method can be extended to other sabotage attacks on the extrusion of the nozzle listed in Table 10 by monitoring changes in the current signal or G-code.

Sabotage Tricks	Detectable
Travel Speed	Yes
Code Insertion	Yes
Code Deletion	Yes
Scaled Subject	Yes
Material Extrusion Malfunction	No
Tampered Temperature	No

Table 10: Detectability for other sabotage attacks.

Finally, the proposed power-monitoring method could be improved to be a real-time corrective system to correct the process once the anomaly is detected. Such a system is a pressing need for the industry to achieve high-quality products because of the potential savings in time and

resources in production. Likewise, with the demonstrated performance of anomaly detection, the approach has the potential to be adapted in metal AM systems where the majority of commercial parts are manufactured.

5. Rotary Side-Channel Attacks from Rotation on AM

In this chapter, we propose a novel side-channel approach for reconstructing the geometric form of a model. The direction of the nozzle is controlled by the X, Y, and Z motors, with each rotor movement dictated to the G-code instructions [118]. The printed dimensions of the model are determined by the combined rotation numbers of the rotors, resulting in a strong correlation between the nozzle and each rotor's movement. To capture this information, our method utilizes three sensors to collect the rotation data, which is then converted into corresponding coordinates. This allows us to determine the position of the nozzle at any given moment. In addition, our method is non-invasive, imposing no additional load on the nozzle, and requires no access to the internal hardware. Through this work, we have identified a vulnerability in AM that could potentially lead to intellectual property (IP) theft [119]. This work sheds light on the potential risks associated with AM and emphasizes the importance of safeguarding against unauthorized access to sensitive information [120-122].

5.1 Motivation

The increasing prevalence of additive manufacturing (AM) systems has exposed the information-intensive industry to a range of potential attacks from both cyber and physical domains. In the event that the printing process is compromised, the consequences can be severe, with the risk of intellectual property (IP) theft leading to significant economic losses [123]. It is therefore imperative to address and mitigate these risks in order to protect the integrity and security of the industry.

Traditionally, IP theft has been associated with cyber attacks [124]. However, recent studies have revealed that IP information can also be leaked from the physical domain [125]. Researchers have introduced a novel approach utilizing an acoustic side-channel to reconstruct G

code from a 3D printer [126]. This innovative attack demonstrates the potential for adversaries to exploit acoustic signals emitted during the printing process to extract sensitive information, posing a significant security concern [127]. This finding highlights the importance of developing countermeasures to protect against acoustic side-channel attacks and reinforcing the security of 3D printing systems. However, a new vulnerability that may lead to IP theft is discovered with the method proposed in this section. Using the approach, we reconstruct the dimensions of the design based on the rotor movement, which can be processed by reverse engineering to restore the geometric information.

5.2 Attack Model

A 3D printer usually possesses four stepper motors. One of these motors is responsible for extruding the filament during printing, while the remaining three motors control the movement of the nozzle. The specific coordinates in the G code for the extruder are achieved through the combined rotation of the X, Y, and Z motors along each respective axis. Since each motor operates independently during the printing process, it is possible to collect the rotation angles of the rotors within each motor. As the rotation angle is linear to the travel distance on the specific axle, the nozzle's travel information is correlated with the dimension of the CAD design. The design can be reconstructed if we know each rotor's rotation angle at every moment.

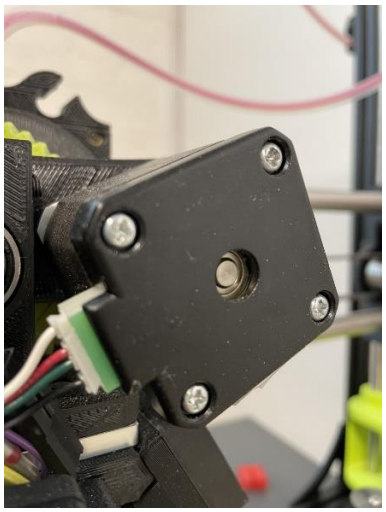


Figure 20. Stepper motor.

In Figure 20, the motor shaft is exposed through a small hole at the end cap. To determine the shaft rotation of X, Y, and Z, we attach a special radial magnet, as shown in Figure 21, to all the motor shafts to generate a magnetic field that follows the shaft's rotation.

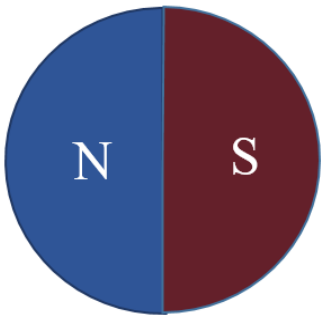


Figure 21. Radially magnetized magnet.

Consequently, the sensor, called a magnetic encoder, as shown in Figure 22 can detect the change in rotation angle. If the sensor on the extruder fails to detect any signal, it signifies that there is no active extrusion of material taking place.

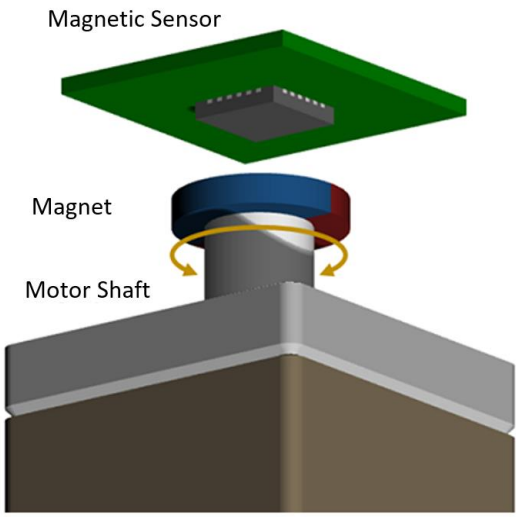


Figure 22. *Working diagram for magnetic encoder.*

To establish the relationship between the rotation angle and the travel distance of the nozzle along each axis, it is necessary to determine the specific distance traveled per degree of rotation. We conducted individual runs of the X, Y, and Z motors, with each motor running distances of 1mm, 5mm, 10mm, and 20mm, to determine the rotation degree per unit of measure. Then we divided the rotation degrees obtained for each motor by 1, 5, 10, and 20, respectively. Finally, we calculated the average unit rotation degree for each motor and compiled the results in Table 11.

Motor	1mm/1	5mm/5	10mm/10	20mm/20	Average Ratio (Unit: mm/°)
X	11.3mm	11.2mm	11.2mm	11.2mm	11.2
Y	9.1mm	9.3mm	9.2mm	9.2mm	9.2
Z	178.5mm	179.1mm	179.0mm	178.9mm	178.8

Table 11: Travel distance per degree for all the motors.

Algorithm 1 provides the pseudo code for plotting the trajectory of the printed part in Table 12. Line 2 to 6 determine if the moving direction is forward or backward. Line 7 calculates the travel distance on each axle by multiplying the ratio in Table 12. Lines 8 to 11 describe the behavior of

the signal from the extruder sensor. Given the sufficiently high sampling rate and the limitation that the rotation angle between two adjacent data points is never larger than 300°, we can employ this value as a threshold to determine the rotation direction. If the difference between consecutive data points is no greater than 300°, the magnet's rotation direction is considered clockwise; otherwise, it is counterclockwise.

Algorithm 1 : Dimension Plot

Input: Time-series data of rotating angles w.r.t. the X,Y,Z axis $[d_t^X, d_t^Y, d_t^Z]_{t=1}^T$,
Output: A plot showing the trajectory of the printed part in 3D space

Initialize $\text{List}^{\text{X}}, \text{List}^{\text{Y}}, \text{List}^{\text{Z}}$ as empty lists and append each list with a coordinate 0.
for $t = 1, \ldots, T$ **do**
  Extract data tuple $\mathbf{d}_t = (d_t^X, d_t^Y, d_t^Z)$ w.r.t. the X,Y,Z axis at time point t.
  for data point d_t^K in $\mathbf{d}_t$ where K = X,Y, or Z **do**
    $\text{diff} = d_t^K - d_{t-1}^K$
    if $|\text{diff}| < 1$ **then**
      $\text{diff} = 0$
    else if $\text{diff} > 300$ **then**
      $\text{diff} = \text{diff} - 360$
    else if $\text{diff} < -300$ **then**
      $\text{diff} = \text{diff} + 360$
    end if
    $\text{List}_t^{\text{K}} = \text{List}_{t-1}^{\text{K}} + \text{diff}/\text{ratio}^{\text{k}}$, where ratio^k is a distance-angle ratio w.r.t to axis K.
  end for
end for
Plot the trajectory in 3D space with $\text{List}^{\text{X}}, \text{List}^{\text{Y}}, \text{List}^{\text{Z}}$.

Table 12: Dimension plot.

If the signal changes, it signifies the creation of the dimensions. Conversely, if the signal remains constant, it indicates that the nozzle is in motion without any material being actively extruded. In such cases, the movement of the nozzle does not contribute to the actual printing process. This distinction between signal changes and constant signals allows us to differentiate between printing actions and simple nozzle movements during the printing.

5.3 Experimental Setup

Figure 23 depicts the testbed utilized for data collection purposes. The magnetic field information is collected using a rotary encoder (AS5048A), which detects position and speed by converting rotating mechanical displacements into electrical impulses [128]. The AS5048A is an absolute encoder with a 360° angle position sensor, offering a high-resolution output of 14 bits and a Serial Peripheral Interface (SPI) [129]. The encoder achieves a maximum rotation accuracy of 0.02° [130]. To ensure stable and precise data acquisition, we have designed a bridge setup as depicted in Figure 24. This setup allows the sensor to be securely attached to the bridge while maintaining a 5mm distance from the magnet. Four sensors are placed on the X, Y, Z, and extruder motors to capture the respective magnetic field information.

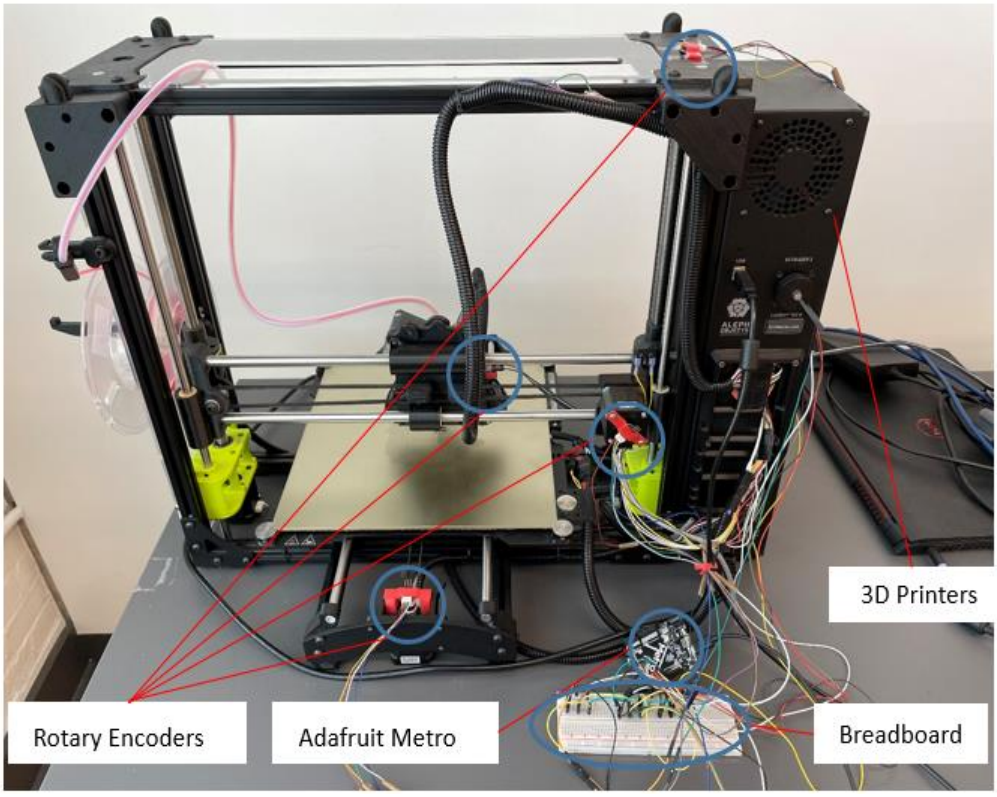


Figure 23. Testbed setup.

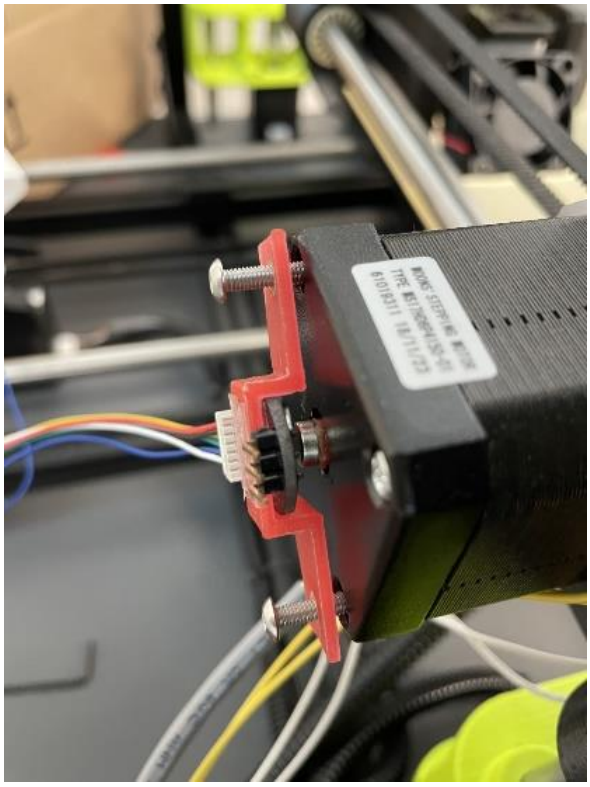


Figure 24. *Sensor bridge.*

The open-source electronics platform we use is Arduino Adafruit Metro [131] and a breadboard connecting wires and sensors. The time interval between data collection is set to 50 milliseconds to avoid missing any geometry-related detail. The 3D printer is LulzBot TAZ 6, an FDM type using Polymaker PLA as the filament [132]. Additionally, it is equipped with the open-source firmware Marlin, which runs on the 3D printer's main board. Marlin is responsible for managing all real-time activities of the printer according to the G code, including motor control and overall coordination of the printing process. The slicing software Cura installed on the Dell laptop controls the parameters of the print jobs and converts the model to G code.

5.4 Results

In this section, we present the reconstructed contour of the model using the rotation data. Due to the existing noise in the signal collection, the signal data may contain outliers that will interfere with the final result. Therefore, pre-processing is applied to eliminate the outliers and smooth the signal data. Then several different shapes are reconstructed to demonstrate the efficacy of the proposed method.

5.4.1 Pre-processing

Before finalizing the shape, preprocessing eliminates all outliers in the data collection [133]. The data obtained from the sensors indicate that the maximum distance between two adjacent points along any of the X, Y, and Z axes is no greater than 0.07 mm. However, for outliers, the distance can easily exceed 5.00 mm. To remove the outliers, we establish a threshold of 0.07 to identify and filter the outliers. If the difference between the second value and the first value exceeds 0.07, we consider the second value as an outlier and exclude it from the dataset. Figure 25 is the raw shape before pre-processing. Each data point is positioned in accordance with the algorithm's computed coordinates. The whole shape is formed by connecting all the coordinate points with blue lines. The significantly protruding lines are where the outliers exist.

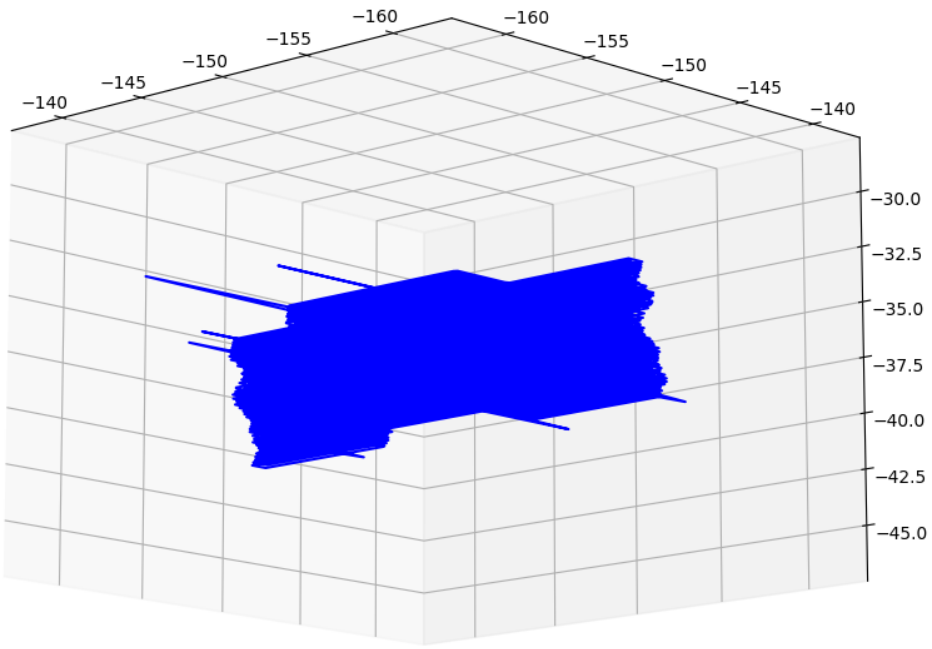


Figure 25. Reconstructed shape before pre-processing.

The signal from the extruder motor works as a flag to control if the point should be connected with blue lines. If the signal is in a state of change, that means the material is undergoing extrusion, resulting in connecting behavior. Then the flag is up, and the coordinate value is assigned to a queue for plotting, indicating this coordinate is connectable during the plot connecting. If the signal remains unchanged, we will set the flag as non-connectable, and the coordinate will no longer be added to the queue. Dimensions for different models are reconstructed, and the printed parts are also presented in Figure 26.

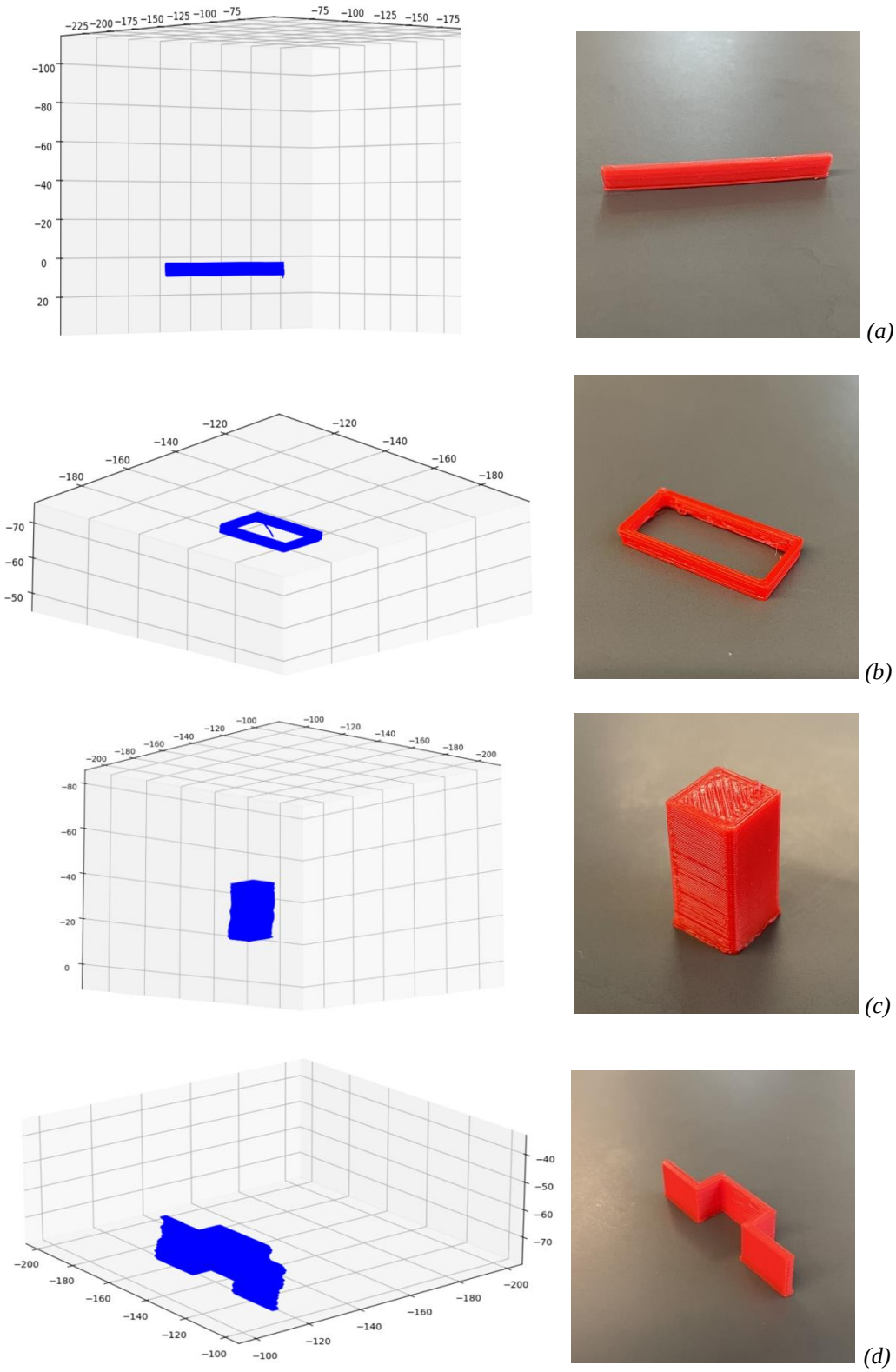


Figure 26. Reconstructed printing path of the object after pre-processing (unit: mm).

5.4.2 Deviation Extent

Though the images above could largely reveal the shapes, the rebuilt dimensions of the models do not perfectly match the actual prints. Since each coordinate is based on the previous location, each layer may not perfectly align with the preceding one, leading to slight discrepancies. As the discrepancies accumulate, the formed shape deviates slightly from the actual prints within a layer and between layers.

To quantify the degree of deviation from the nominal CAD design, the Euclidean distance serves as the primary index. Before effectively comparing the restored model with the CAD model, two assumptions need to be made.

First, we define the centroid of the first layer in the restored model as our reference coordinate, which is shared by the two models from two different systems. In other words, the centroid of the first layer from the rebuilt model is used as the centroid of the first layer from the CAD model for future comparison. In this case, two models are placed in the same coordinate system. For every subsequent centroid, its theoretical position is determined relative to the reference centroid. In Figure 27, the green dot indicates the position of the first layer's centroid in the restored model. Second, each layer in the model is assumed to have the same shape and be vertically well-aligned so that the centroid for each layer can be confirmed. Otherwise, that will be too complex or impossible to know the exact theoretical centroid position for each layer if we don’t know the shape details of the CAD model.

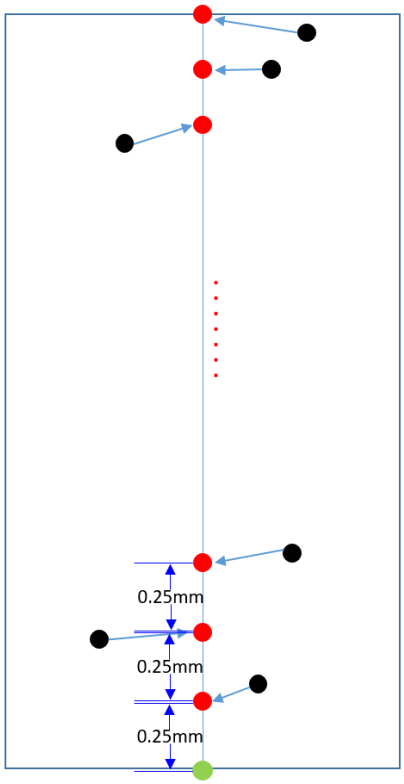


Figure 27. Deviation calculation between restored and CAD model.

Since the layer height is 0.25mm, we can determine the theoretical position of the centroids for each subsequent layer by adding 0.25mm to the current vertical coordinate, represented by the red dots. These red dots constitute all the reference coordinates for each layer. By utilizing data from the sensor, we know the actual position of the centroid for each layer, represented by the black dots. Consequently, we can calculate the average Euclidean distance as the final deviation index for the overall model by comparing the positions of the black dots with their corresponding reference coordinates layer by layer, as shown in Equation 3. From the equation, d_i is the Euclidean distance for the ith layer, n is the total number of layers, and D is the average deviation index.

$$D = \sum_{i=0}^{n} \frac{d_i}{n} \tag{3}$$

Table 13 displays the deviation extent of the aforementioned comparison. As the printing time for models (c) and (d) is much longer than models (a) and (b), we just run 35 for each. It is observed that the deviation extent increases with increasing complexity of the models.

No. of Experiments	45	40	35	35
Model	(a)	(b)	(c)	(d)
Standard Deviation	0.07	0.15	0.27	0.46
Average Deviation Extent (Unit: mm)	0.24	0.38	0.64	1.21

Table 13: Deviation extent for the different models.

To provide a clear understanding of the relationship between deviation and layer, we present the deviation values along the layers in Figure 28. To further visualize and compare the performance of different models, box plots are used in Figure 29. These box plots display the distribution of deviation values for each model, highlighting the range, median, and quartiles. As all the comparison result of the deviation range is very similar, one-time experiments for different models is also provided in the box plot. The deviation range becomes larger as the model complexity increases.

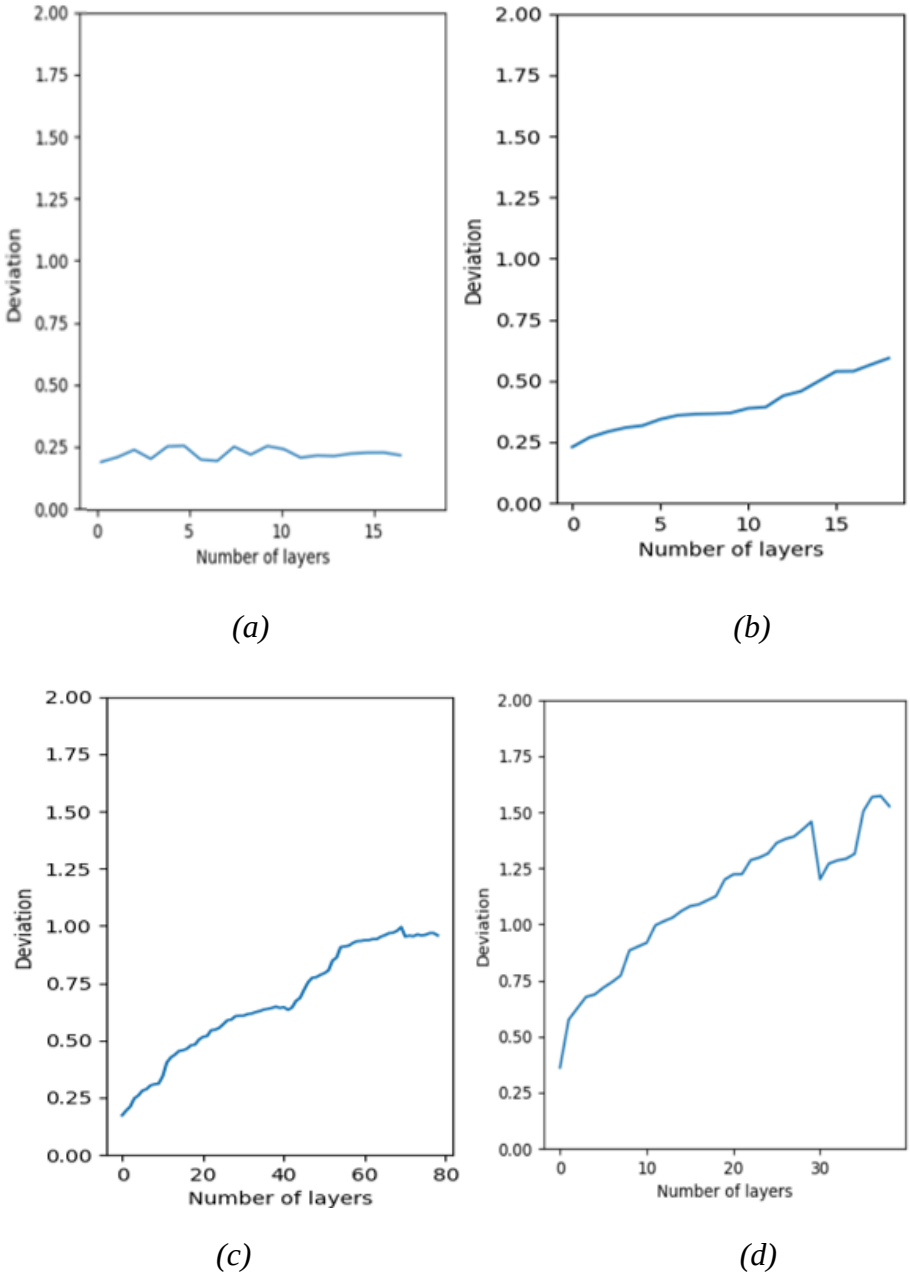


Figure 28. Deviation plots along layers for different models.

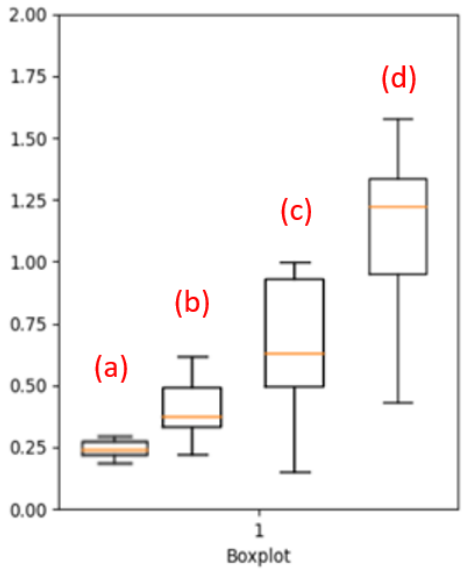


Figure 29. Boxplot comparison for different models.

The deviation values along the layers provide insights into how the deviation varies throughout the structure. As the height of the model increases, the restored peripheral dimension along the vertical direction becomes less accurate due to the accumulation of discrepancies. Therefore, the range in the boxplot becomes higher as the number of layers increases.

5.5 Limitations and Future Works

During the data collection stage, we observe that the signal fluctuates with a narrow range. The presence of noise can be attributed to two factors. First, there is inherent noise originating from the sensor itself [134]. Second, noise can also arise from the stability of the system structure.

The AS5048a sensor exhibits jitter ranging from 0.001° to 0.007° when the Pulse Width Modulation (PWM) signal is converted into an angle, particularly in relatively quiet testing environments [135]. The minor instability arising from the intrinsic properties of the sensor does not significantly impact the required accuracy. However, the majority of noise is generated by the vibrations originating from the 3D printer. Due to the supporting bridge where the sensor is

attached being tightly fixed on the motor, the vibration caused by the 3D printer will directly aggravate the signal instability with the internal noise that is generated by the sensors themselves. Consequently, the sensor signal slightly affected by these factors will experience subtle fluctuations. Furthermore, since the coordinates for each data point are derived based on the preceding values, the error accumulates over time and causes the global form to be skewed or jagged rather than a smooth contour.

In the future, we aim to develop a contactless structure where sensors are installed independently to eliminate the influence of vibrations. Leveraging this approach, our data collection system will be independent of the 3D printer system, leading to significantly enhanced stability and precision in the obtained data. Consequently, the reconstructed dimensions will closely align with the actual prints.

To ensure optimal experimental conditions, it is essential to maintain an isolated and silent environment, as even sound waves can induce minute vibrations that may affect the accuracy of the measurements.

The data collection positions for the X, Y, and Z channels are fixed. As the sensor on the extruder motor needs to move along with the printing head, it cannot be part of an independent system. To mitigate the impact of vibrations, we plan to introduce a buffer mechanism by placing soft materials between the bridge and the motor. This setup will help partially counteract the vibrations and minimize the effects.

5.6 Contribution Summary

The widespread adoption of AM in various industries is driven by its flexibility over conventional production methods. However, this increased adoption has also attracted the attention of hackers, leading to concerns regarding security risks such as IP theft. In order to identify potential

vulnerabilities in the system, we present a rotation side-channel attack aimed at accurately reconstructing the dimensions of a model without requiring access to the original design. This attack method poses a risk of IP theft for AM systems.

Our approach relies on utilizing rotation information from the X, Y, and Z motors to decipher the coordinates of the printing head at each moment and then connecting them using information from the extruder motor. We further apply preprocessing techniques to improve the shape reconstruction. Additionally, we propose several challenges and areas for future research to enhance the accuracy of these methods. However, achieving high accuracy in restoring the model's dimension with high complexity becomes challenging due to various factors, such as vibrations and sensor noises that are present during the data collection process.

This work highlights the existence of significant loopholes in AM systems that need to be addressed, serving as a warning to manufacturers to take measures to prevent the leakage of IP information. We believe that our work contributes to the development of novel ideas for IP protection in AM security research and encourages designers to consider side-channel leakage when securing their systems.

6. Signal Validation and Variances for Independent Additive Platforms

The rise in the complexity and frequency of attacks against cyber-physical systems (CPS) has driven the development of attack detection and protection approaches to address modern manufacturing vulnerabilities. With the proposed power monitoring method in Chapter 4, we could detect the geometry anomaly caused by malicious activity. However, the proposed detection system only utilizes the data collection from a specific machine, making it uncertain whether the method will be effective for other similar or identical platforms. In order to broaden the application in possible remote scenarios, we incorporate an additional identical additive manufacturing platform to assess the continued suitability of the proposed method. Moreover, the current signal from the two machines will be compared to highlight the variances when parts of varying complexity are printed. Based on the established method for Chapter 4, we collect the data for the same prints from both the new and original machines to perform the experiments. The result proves that the differences in signals between the machines become larger when the complexity of the part increases. Meanwhile, our detection method is demonstrated to be applicable to a similar model of a 3D printer when detecting anomalies, so it has the potential to provide a remote validation process.

6.1 Motivation

AM has demonstrated its advantages in providing flexibility in complex design and rapid prototyping. The increasing adoption of 3D printing in many safety-critical applications exposes both 3D printers and their processes to potential cyber-physical attacks. Breaches in the AM system could result in the theft of sensitive information and inflict damage upon the 3D printer, thereby diminishing production efficiency. More importantly, malicious activity can undermine a printing process by secretly altering key parameters, leading to a degradation in the mechanical

properties of the produced parts [136]. These defective or malfunctioning parts may appear to pass inspection but are prone to failure during actual operation, resulting in disastrous outcomes. For example, the yield load of a tensile test specimen can be decreased if an inconspicuous vacancy (less than 1 mm in size) is inserted into the 3D design [137].

Several proposed techniques focus on securing digital assets in order to counteract this rising security risk. However, the AM system consisting of interconnected hardware components will emit key side-channel information during the operation process such as current, acoustics, vibration, electromagnetic radiation, magnetic field, and power. If any malicious activity attempts to compromise the system, the corresponding side-channel signals will also change. Therefore, those signals can serve as indicators to reveal the printing status.

Instead of using a single machine such as in Chapter 4, we introduce another FDM machine to explore the differences between signals generated by the two machines. In this chapter, two major parts are proposed. First, signals from different sources are compared to find the relationship between the signal variation and model complexity. Second, we introduce another machine to collect the current data and compare it with the original machine for anomaly detection. Collectively, this approach is a first step towards the remote authentication of AM parts produced on a similar platform.

6.2 Proposed Methods

In Chapter 4, we proposed a power monitoring method to detect maliciously inserted voids and determined the minimum detectable size of these voids. In this section, our initial focus will be on examining the signal variances between the previously utilized machine and a new AM platform with nearly identical specifications and features. Furthermore, we will proceed by prioritizing the investigation of voids to assess the detectability of the method on the new machine.

6.2.1 Signal Variances in Different Machines

For the test machine, we use Lulzbot Workhorse and take Lulzbot Taz 6 as the benchmark machine. Both printers are designed for FFF 3D printing and are built on open-source Marlin firmware and software platforms. While the test and benchmark machines utilize the same model of motors, there are slight differences in their design. Workhorse desktop system builds upon the foundation of the previously released Taz 6 model but incorporates some feature upgrades that distinguish it from Taz 6. The Workhorse has a larger build volume compared to the TAZ 6, providing a larger space for printing objects. The Workhorse features an automatic bed leveling system, which helps ensure the print bed is properly leveled before each print. The TAZ 6, on the other hand, uses manual bed leveling, requiring the user to adjust the bed manually. The Workhorse incorporates an upgraded hot end, known as the LulzBot Modular Tool Head System, which offers enhanced performance and reliability. The TAZ 6 uses the previous generation's hot end.

To investigate whether these firmware and hardware discrepancies contribute to variations in output, signals are collected from each machine and analyzed to assess the differences.

In this section, two experiments are performed here. The first involves collecting data from each machine and comparing them using the Dynamic Time Warping (DTW) algorithm to quantify the extent of their similarities. The second involves exploring the signal variations across increasing part complexity when the prints have the same number of layers.

6.2.1.1 Comparison Strategy

As a high sampling rate is employed during current signal acquisition, the data volume becomes substantial, especially when the print time is long. If we use the Euclidean distance to calculate the differences between the two signals, the variance in the signal length renders the method ineffective due to desynchronization issues. Moreover, the presence of noise within the signal can

further impact the accuracy of the results. Hence, attempting to calculate the entire dataset with such a method would lead to inaccuracies. To solve the synchronization problem, we will employ DTW as our major metric to quantify the differences between the signals. DTW offers the advantage of accounting for temporal variations and aligning the signals, ensuring accurate comparisons. By considering the temporal aspect, DTW overcomes the synchronization problem and accurately assesses the differences between the signals. In this approach, we still take the "layer-to-layer" comparison strategy to calculate the differences by DTW individually. The next section is to compare different parts with the same height but varying complexities to explore the relationship between complexity and signal differences. By examining these variations, we aim to uncover any patterns or correlations that may exist between the complexity of the geometric features and the observed differences in the signals.

The following steps outline the procedures to measure the difference between the two data sets, incorporating some similar steps from Chapter 4:

Step One (Cutting): Since the data collection is synchronized in X, Y and Z channels, we use the Z channel signal to cut the X and Y channels. The time interval between the triggered signal in the Z-axis corresponds to the moment when the signal is generated for that specific layer in the X and Y channels. The signal content for the X and Y channels for each layer is accurately assigned to the corresponding layer number, based on the time interval between the triggered signal in the Z-axis.

Step Two (Comparing): Once we have cut the X and Y signal, the DTW value is applied to calculate the difference for each layer. Consequently, we will have the value for signal difference along the layer number for two channels X and Y.

Step Three (*Normalizing)*: In order to accurately represent the differences in terms of percentages, it is necessary to normalize the data. Normalization will ensure the signals are adjusted to a common scale, allowing for a fair and meaningful comparison of the observed differences. We will use Equation 4 to normalize the data. In the equation, $D(X,Y)$ is the DTW value for X and Y channels, and M is the maximum distance of $D(X,Y)$. Therefore, $S(X,Y)$ is the normalized dissimilarity measure for X and Y channels.

$$S(X,Y) = \frac{D(X,Y)}{M} \tag{4}$$

6.2.1.2 Result

For the first experiment, the dimension we print is 10mm×10mm×20mm. The result is shown in Figure 30. As the comparison result has been normalized, the y-axis represents proportions, *i.e.*, the maximum dissimilarity is no greater than 0.1 or 10%. During the operation of a 3D printer, the motor that controls the Z channel remains idle most of the time. Due to the substantial presence of noise in the data obtained from the Z channel, we chose not to include it in the comparison. Since the Z channel predominantly consists of noise rather than meaningful information, it would not provide valuable insights or contribute to the analysis. Hence, our analysis primarily focused on analyzing the X and Y channels, which contain the essential data for our comparisons.

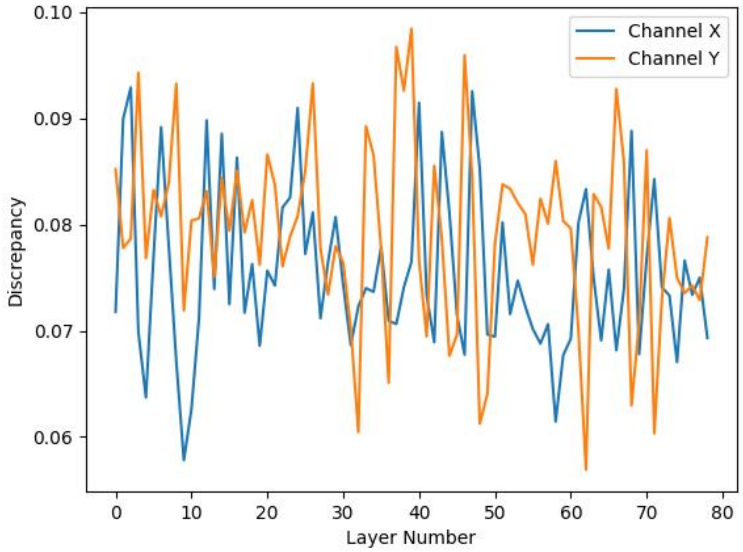


Figure 30. Comparison results about X and Y channels for new and benchmark machine.

For the second experiment, we will keep the height consistent for all the parts and focus on altering the base shape. In order to explore the relationship between discrepancy and complexity, we will design different base shapes, ranging from low to high complexity. The following base shapes will be utilized: rectangle, triangle, circle, random shape, and octopus. This experiment aims to analyze how the complexity of the base shape affects the signal discrepancy. To simplify the comparison result across complexity, we use average discrepancy from all layers DTW as the final metric. By using this averaged metric, we can effectively assess the impact of complexity on the overall signal differences. We run each model ten times to get the average value in Figure 31. It shows that as the complexity increases, the average discrepancy becomes higher, as a more complicated part tends to generate a more complicated signal.

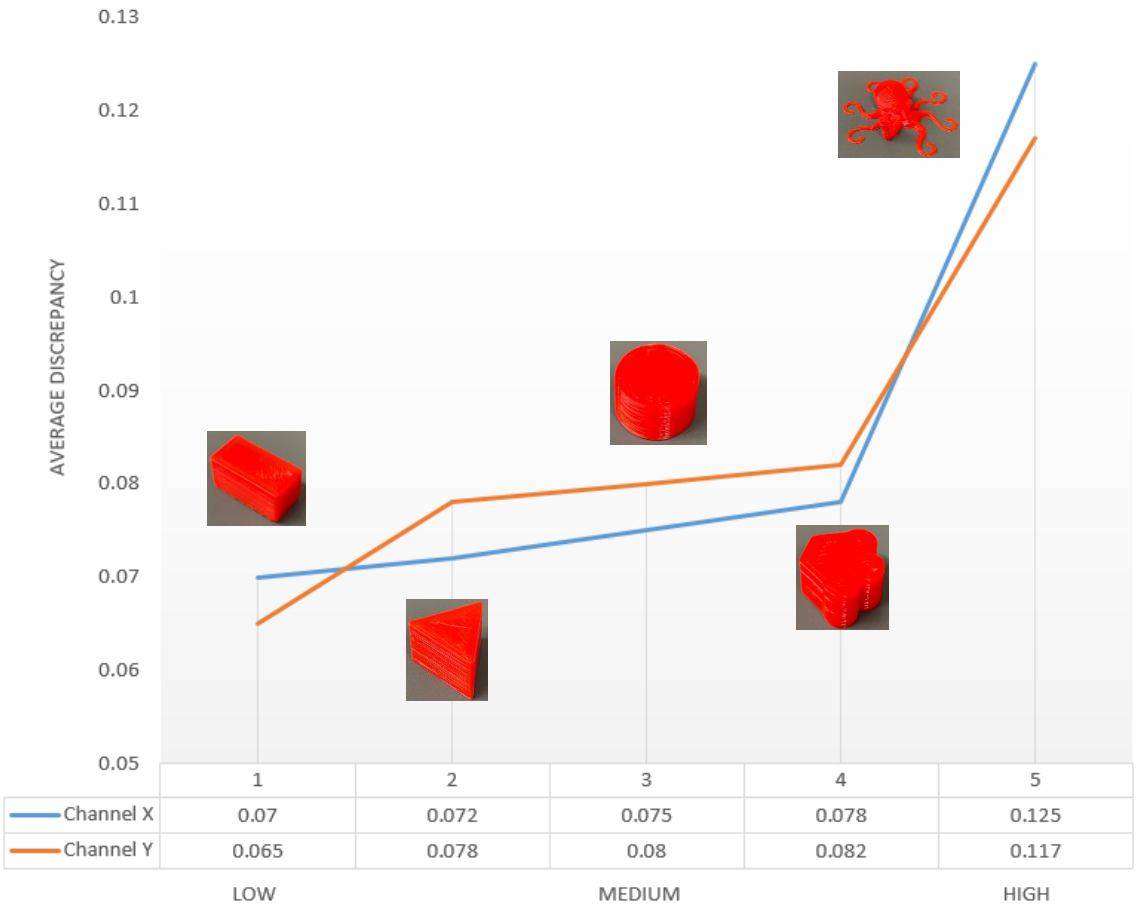


Figure 31. The average discrepancy for different base shapes with the same number of layers.

The complexity of a 3D printed model refers to its intricacy, level of detail, and structural complexity [138-140]. For example, the signal for printing a line is more stable than printing a part that needs to frequently change the printing direction. When printing complex models, the differences between two 3D printers can become more pronounced due to several factors. The first factor is precision and accuracy. Higher complexity models require greater precision and accuracy in the printing process [141-143]. If there are variations in the printers' capabilities or calibration, it can lead to differences in the printed output, resulting in higher signal differences [144].

The second factor is layer adhesion and support structures. Complex models often involve overhangs, intricate geometries, or support structures [145,146]. The printers' ability to properly

adhere the layers and generate the necessary supports can vary, leading to differences in the final print quality and resulting in higher signal differences. The third factor is filament flow and extrusion. The flow of filament and extrusion control can impact print quality, especially for complex models [147-149]. Differences in filament properties, extruder performance, or temperature control can cause variations in the printed layers. The fourth factor is print settings and parameters. Complex models may require specific print settings, such as layer height, print speed, or cooling, to ensure optimal results. Variations in these settings between the printers can affect the final output [150].

Overall, as the complexity of the 3D printed model increases, the printers' ability to accurately reproduce the intricate details becomes more critical. Any variations in printer capabilities, calibration, or print settings can result in higher signal differences between the printed models.

6.2.2 Anomaly Detection in Different Machines

The movement direction of the nozzle is determined by the combination of the X, Y, and Z motors. Consequently, the current signals from each motor can be individually collected to construct a data-driven model. Specific geometries correspond to distinct current signals from these motors, meaning that modifying the geometry in a particular layer will induce changes in the current signals. By comparing the acquired data from each channel with the original data, the deviation can be determined. If two sets of signals in a specific layer exhibit significant inconsistencies, it indicates the presence of abnormal geometry, which could potentially be attributed to sabotage activity.

6.2.2.1 Comparison Strategy

In Chapter 4, the data source was obtained from a single 3D printer. There are two sets of signals involved. One is generated as a benign set working as a control group, while the other works as an "altered" or "attacked" group. Our work has proved that the alteration in the G code or model design will be detected through our current-based method.

Based on the previous analysis, it can be concluded that when using the square shape as the specimen, the difference in signal between the X and Y channels is approximately 7%. This relatively small variation suggests that we can proceed with obtaining altered data generated by a new machine. This data can then be used to test whether the proposed method is still capable of detecting anomalies, as discussed in this chapter. The general method for the comparison mechanism is shown in Figure 32. This experiment allows us to determine if our method remains applicable in detecting anomalies across different machines.

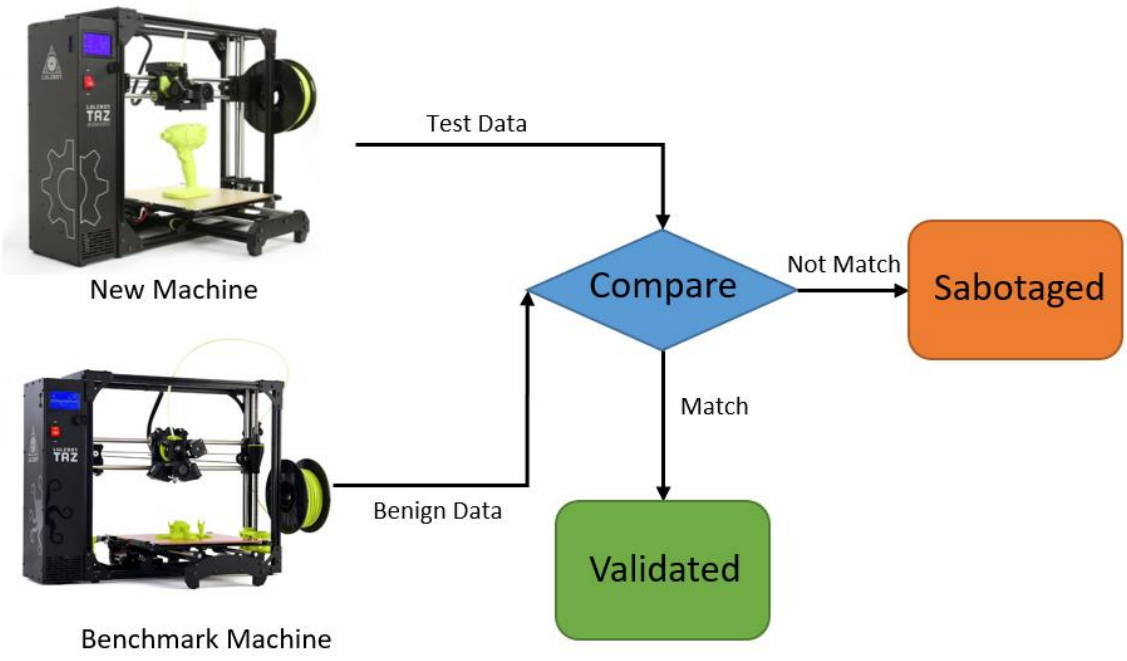


Figure 32. Comparison mechanism.

All the printed parts have a dimension of 10mm×10mm×20mm. To simulate malicious activity, we incorporate two voids within the altered part for comparison with the benign part. Additionally, we systematically reduce the size of the void while keeping the exterior dimensions unchanged in order to determine the smallest detectable void size. Additionally, a threshold is established beyond which we can claim a particular segment signal differs from the benign one.

6.2.2.2 Experimental Setup

The method to acquire the current signals from X, Y and Z motors is a non-invasive measurement without any hardware connection. The test machine (LulzBot TAZ Workhorse) and benchmark machine (LulzBot TAZ 6) share the same experimental setup shown in Figure 33. Three current probes (Picotech 60A (TA018)) are utilized for each printer. Each probe converts the current flowing through a conductor into a voltage that can be observed and measured on the PicoScope 5000 series oscilloscope. The remaining experimental apparatus includes a laptop and 2.85mm PolyLite PLA filament. Autodesk Fusion 360 software is utilized for designing the model. Marlin firmware in the Lulzbot printer translates the G code generated by the slicing tool Cura-Lulzbot into commands for the printer. To ensure accuracy, all the Cura parameters controlling the printing properties are set to be identical for both printers.

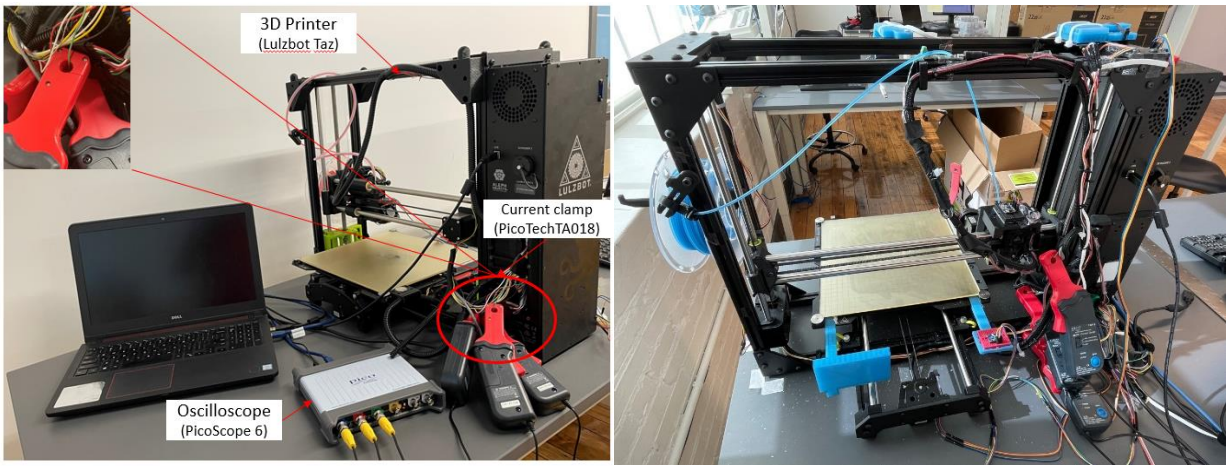


Figure 33. Experimental Setup for benchmark machine (left) and test machine (right).

6.2.2.3 Comparison Results

The experimental prints have a standardized size of 10mm×10mm×20mm, but the size of the inner double voids within the altered part may vary. The test machine is responsible for printing the altered part, while the benchmark machine is used to print the benign part. We first compare the altered one with a benign part, and then we gradually shrink the inner hollow part's volume to test the method's performance to find the detection limit. The comparison technique in *4.1.3 Model Development and Algorithm Design* in Chapter 4 will be employed in this section.

Figure 36 is the comparison result for double voids with 2mm×2mm×2mm under different infill rates. In fact, the G code converted from the STL file does not entirely reflect all the details of the CAD model.

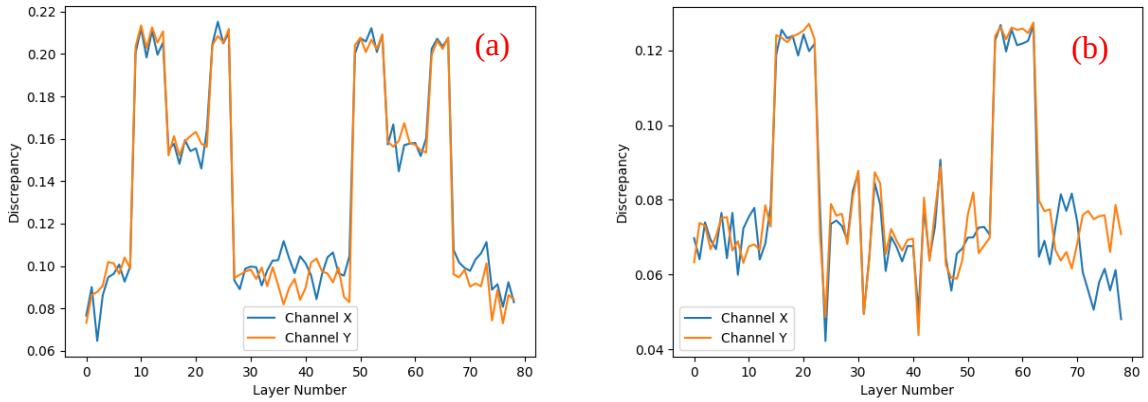


Figure 34. Comparison results for different infill rates. (a) 20% infill rate (b) 100% infill rate.

In the case of a 20% infill rate set in Cura, the actual infill rates for the surrounding areas of the hollow sections are automatically increased to 100% to create a supporting plate for subsequent material deposition. As a result, two bulges appear in the front and back of each void, as depicted in Figure 34 (a). When the infill rate for the entire part is set to 100%, the surrounding section will be the same as the benign part (also 100% infill rate), so the bulges disappear in Figure 34 (b).

To establish a threshold for identifying abnormal layers, we employ the statistics method X Chart (also known as Individual Chart). This chart displays the mean and variance of the process based on individual samples taken over a specific period. For determining the threshold, we utilize the X Chart with the comparison results of two benign signals under different infill rates. The upper control limit (UCL) is chosen as the threshold. The resulting threshold values are 0.104 for the 20% infill rate and 0.092 for the 100% infill rate.

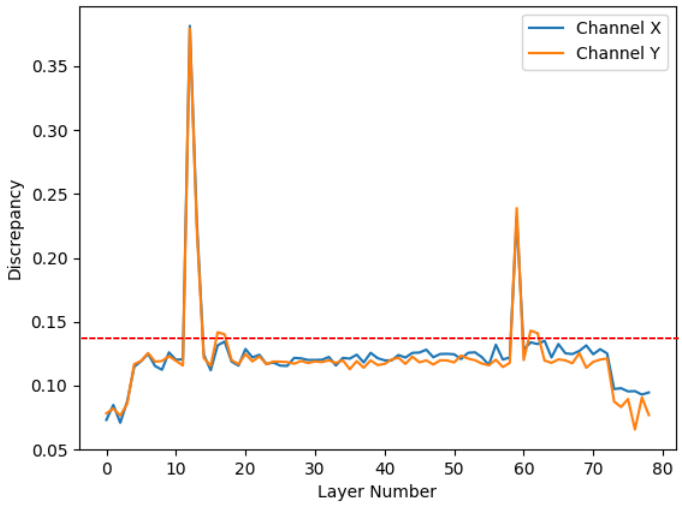


Figure 35. Comparison results for the minimum detectable void 0.25mm×0.25mm×0.5mm.

Regarding the minimum size for detectable voids, we gradually decrease the dimensions in height, width, and length until all calculation results fall below the threshold. We are going to Figure 35 shows the outcome for a void measuring 0.25mm×0.25mm×0.5mm. In this case, only one point exceeds the threshold, indicating that any smaller size would not be detected. In conclusion, we confirm that the detectability limit is 0.25mm×0.25mm×0.5mm.

6.3 Discussion

We have examined the variation among the signals generated by different machines and investigated the relationship between signal variances and model complexity. Additionally, our research validates the effectiveness of the proposed method in accurately detecting abnormal patterns caused by malicious activities on the new platform. The proposed method enables the possibility that remote model printing data can be monitored and validated by an on-site machine. This approach proves that comparing signals from different sources is a feasible way to detect anomalies, allowing for possible efficient and reliable remote validation processes.

This research represents an extension of the approach outlined in Chapter 4, where the comparison subject was collected from the same machine. In this contribution, we expand the scope by collecting data from different machines, enhancing the applicability and generalizability of our findings.

Considering the current signal is collected as a side-channel of the motors, signal amplitude has a tight relationship with the electronic hardware. However, the accuracy of the current signals is directly influenced by the Marlin firmware, which is responsible for controlling motor rotation. Both 3D printers adopt NEMA 17 stepper motors with a 1.8-degree step angle (200 steps/revolution). But the Z axis for Workhorse is 500 steps/mm, while the Lulzbot Taz 6 is 700 steps/mm. As the Workhorse is less accurate than the Taz 6, the Workhorse can't create as small of details as the Taz 6 in terms of the minimum detectable void size. The Lulzbot Taz 6 is capable of detecting the minimum void size as 0.25mm×0.25mm×0.25mm, while the Lulzbot Workhorse is only capable of 0.25mm×0.25mm×0.5mm. In addition to this hardware difference, the built-in configuration for the Marlin firmware and Cura software is also not exactly the same. Despite our efforts to maintain parameter consistency, there may be slight variations between the current signals. These differences contribute to the disparity between the comparison results and the conclusions drawn in our previous work. However, these variations do not undermine the effectiveness of the power monitoring method in detecting anomalies.

6.4 Future Work

Since we have concluded a threshold on the detectability of the method, any smaller voids cannot be detected. However, in cases where these smaller voids are dispersed within the part and do not accumulate in close proximity, the proposed method may not detect them, resulting in the potential passing of inspection. As a result, the mechanical properties of the part could be affected by these

clustered voids. In future research, we will perform a tensile test to explore the extent to which these voids may decrease the mechanical properties.

Currently, both machines employ the same model of motors. To broaden the scope of application, we will also incorporate some machines that have significantly different specifications of motors to compare with our benchmark machines to test if the proposed method is still applicable.

At present, our proposed method begins to process the data after the experiments are completed. Our future objective for this research is to develop a real-time model validation process that enables continuous remote monitoring. Once an anomaly is detected during the printing process, our goal is to ensure a rapid response and issue timely warnings. This will enable prompt intervention and mitigation measures to be taken, minimizing any potential adverse effects.

6.5 Contribution Summary

AM exposes various attack surfaces, making it challenging to identify attacks and prevent tampering with critical data. Our method has proved its effectiveness in detecting anomalies in the same machine. To validate the applicability of the proposed method on a different platform, we integrate another machine and apply the approach to assess its effectiveness. This allows us to gather insights into the method's performance across various platforms. Due to the variance in the motor specifications, the threshold is not the same as the scenario when data is collected and compared from the same machine. The result shows that the tiny alteration inside the part can still be detected, and the threshold for the smallest detectable size is as small as 0.25mm×0.25mm×0.5mm. Therefore, our method still has the potential to validate the system remotely. Overall, the method has the following advantages: (1) Capable of precisely tracking anomaly position; (2) Applicable to a different machine with similar motors; (3) Non-invasive

measurements; and (4) ease of use. In addition, we have shown the signal variations between the two machines and confirmed that a more complex part would produce increased variation between the signals. The demonstrated anomaly detection performance and the potential applicability to remote AM inspection systems make the proposed approach an important contribution to ensuring AM security in safety-critical systems.

7. Conclusion

The development of robust authentication mechanisms, encryption protocols, intrusion detection systems, and anomaly detection techniques tailored specifically for CPS brings a new angle to security issues. These advancements aim to protect CPS from unauthorized access, data breaches, tampering, and other malicious activities.

This dissertation introduced a novel current monitoring approach for anomaly detection and a new channel of reversing engineering a geometric design for an AM system. In this final chapter, a summary of the conclusions, contributions, and broad impact of this research is provided. Additionally, the limitations of the study and future research are presented.

However, the field of CPS security is still evolving, and new threats continue to emerge. As technologies advance and attackers become more sophisticated, it is essential to adopt a proactive and adaptive approach to CPS security. This includes continuous monitoring, timely updates and patches, threat intelligence sharing, and collaboration between researchers, industry experts, and policymakers.

Future research in CPS security should focus on addressing emerging threats such as Cloud-based threats, supply chain attacks, and Machine learning and AI-based attacks. Additionally, the development of standardized security frameworks and best practices specific to CPS will play a pivotal role in ensuring a consistent and high level of security across different systems.

To summarize, the security of CPS is an ongoing and ever-evolving challenge. By recognizing the unique characteristics of CPS and investing in research and development, we can build robust and resilient security measures to protect these systems. By ensuring the security of

CPS, we can harness their full potential and drive innovation while maintaining the trust and integrity of our critical infrastructure and social well-being.

7.1 Summary

In view of its wide application in manufacturing systems, the importance of the security protection of CPS becomes crucial to protect critical infrastructure, sensitive data, and public safety. Identifying deviations or abnormalities in the operation of CPS components, such as sensors, actuators, communication networks, and control systems, plays a crucial role in ensuring the integrity, reliability, and security of the overall CPS infrastructure. If abnormal activity is not detected in the AM manufacturing industry, poor-quality products will be made even though they may pass inspection. Moreover, undetected abnormal activity can impact the functionality and stability of systems, leading to malfunctions or complete failures. To protect AM systems from sabotage activity, anomaly detection is proposed to identify and respond to abnormal behavior or events that deviate from the normal patterns within the system. Additionally, our method could accurately track the affected position to layer level, making the remedial measures more targeted.

However, the measures of anomaly detection are not enough to provide complete protection for CPS and prevent the leakage of process information. Due to the fact that IP is highly centralized in a single file in AM, it’s crucial to safeguard a company's competitive differentiation and innovative creations, making it imperative to protect against infringement. To enhance the system's integrity, it is necessary to identify and address any loopholes that may release the key information. In this dissertation, we also proposed a novel side-channel approach for reconstructing the geometric form from motor rotation information. Our work serves as a reminder to system designers of the essential measures required to prevent information theft in AM.

To implement the possible remote model validation in the future, the differences between different FFF 3D printers need to be identified. The results of this dissertation show that signal variation increases when the print model complexity is higher, even on the same model of AM platform. Given that the observed variation is not significantly high, we utilize the DTW comparison method to analyze the data collected from both machines. This approach enables us to assess the applicability of anomaly detection and explore its potential for remotely verifying the authenticity of a part of the reference model.

7.2 Contributions

Researchers have consistently made significant contributions to AM security community. Most security studies concentrate on defense strategies, attack methods, mitigation techniques, detection mechanisms, and system monitoring. In terms of defensive strategies, countermeasures in intrusion scenarios aim to achieve protection, detection, and mitigation. When considering the purposes of attacks on CPS, the two primary effects are typically destruction and intellectual property (IP) theft. These two objectives are commonly associated with malicious actions targeting CPS. Therefore, three contributions are made in this dissertation to detect possible sabotage attacks on the AM and reveal the vulnerability in AM through side channels. Additionally, a new FDM 3D printer is introduced to test the applicability of the proposed method on a new platform. Contribution details are summarized in the following part.

(1) *Detection of Malicious Cyber-Physical Attacks for Additive Manufacturing with Dynamic Time Warping:* In this contribution, we present a novel power monitoring method utilizing the Dynamic Time Warping algorithm to detect sabotage attacks on an AM system. Specifically focusing on the insertion of unwanted voids within FFF parts. The proposed method evaluates the current signals from both the benign control group and the altered

group caused by malicious activities through layer-to-layer comparison. If the discrepancy for any layer surpasses the predefined threshold, it is identified as an abnormal layer indicating the presence of voids. The minimum detectable void size is 0.25mm × 0.25mm × 0.25mm, with the height equal to the layer thickness. Through a case study, the proposed method demonstrates a detection accuracy of over 96%. Furthermore, the model provides insight into the specific layers where the voids are located. Given the layer-to-layer comparison, the method is especially well-suited for FFF. This research serves as a valuable reference and offers practical guidelines for detecting sabotage attacks in FFF and other AM processes.

(2) *Magnetic Field Side-channel Attack on Additive Manufacturing Systems:* This study reveals the vulnerabilities in AM systems in which process information can be illicitly obtained. To disclose the potential risk, we introduce a rotation side-channel attack that aims to reconstruct the dimensions of a model with high accuracy without the need for direct access to the original design. This attack method poses the risk of IP theft. Our approach utilizes rotation information from the X, Y, and Z motors to determine the precise coordinates of the printing head at each moment. These coordinates are then connected using information from the extruder motor. To enhance the accuracy of shape reconstruction, we apply additional preprocessing techniques. The results of our experiments demonstrated that the restored model dimensions could achieve an accuracy of approximately 90% on average when compared with the CAD design. Relevant protection measures are also provided to prevent the unauthorized disclosure of IP information. This work reminds designers to consider side-channel leakage when securing

their systems, and we believe that our study contributes to the development of novel ideas for IP protection in AM security space.

(3) *Signal Variation Based on Complexity and Print Validation Across Multiple AM Platforms:* A new FFF 3D printer is introduced to work as a test platform to compare with the benchmark machine. By comparing the variances of the signals between the machines, we can conclude that a more complex part would produce increased variation between the different machine signals. Furthermore, we compare the current signal from each machine to detect any abnormalities in the geometry. The results have shown the DTW power monitoring method is still applicable to the new machine. Due to the hardware differences, the new machine is not able to provide as much detail as the benchmark machine. Therefore, the minimum detectable void size is 0.25mm × 0.25mm × 0.5mm. Our signal detection method can be used to remotely validate the authenticity of a print if the differences in the motor and hardware specification are not significant.

Throughout this study, we have examined the unique security challenges AM systems pose and explored the methodologies and techniques employed to safeguard the systems. However, some limitations in the experimental design restrict the method to be performed under specific conditions, and there is still room for improvement in the experiments. These limitations and future works will be discussed in further detail.

7.3 Limitations

In the data collection for different machines, the signals used in the comparison technique are all generated by the motors with identical models or specifications. If the machine is installed with a different type of motor, the signal will be significantly different, making it challenging to detect the minor change caused by the anomalies in the geometry.

So far, our method is only implemented on the FFF platform. There exist some non-FFF platforms like Stereolithography (SLA) or Selective Laser Sintering (SLS). These machines employ fundamentally different technology and different materials, which alters the method of signal collection and generation. As a result, the proposed method is not applicable to the new power supply mechanism in these platforms.

The proposed method based on DTW has a threshold for detecting the voids in the prints. The minimum detectable size is 0.25mm. Any smaller size of the voids below the threshold will not be detected as the dimension is too small to generate valid signals. Consequently, our current method would not be effective in detecting such attacks.

7.4 Future Work

Based on the contributions of this dissertation, we will also explore the possible application of the proposed method to detect other attack types beyond geometry alteration. In terms of key parameters affecting printing quality, if the temperature parameter for the nozzle is secretly altered, it can lead to material jams due to inadequate melting. This type of attack will help to determine the effectiveness and applicability of our approach in a broader range of scenarios.

For tiny “smart voids” under the derived threshold, we will continue improving the method for the case when they are small but discretely accumulating in mass. It’s unclear how much the formed porous structure will negatively impact the integral structural strength. As a result, we will take the tensile test as part of the experiments to test if those small smart voids will produce damage to the mechanical property.

The previous design for the experimental prints all shares the same shape in each layer, so we can use a single line to measure if the whole print is free from abnormal activity. But this measurement is not suitable for prints with different shapes in each layer. Because every shape of

layer has a unique threshold below which the layer can be claimed to be normal. In this scenario, utilizing partitioned lines or a curved structure may be more suitable for the part, as opposed to using a single line.

Due to their high precision nature, rotary encoders are susceptible to shock and vibration. The installation of sensors directly on the machine exposes them to significant interference from the vibrations generated by the machine, which greatly disrupts the normal signal collection process. In future research, we consider detaching the data collection system from the machine and building another collection system with sensors to avoid the vibration's direct impact. For sensors that cannot be separated from the machine, we will employ a buffer mechanism to mitigate the effects of vibration.

8. References

[1] T. Jacob, “Industrial Applications of 3D Printing: The Ultimate Guide,” AMFG, Jun. 13, 2021. https://amfg.ai/industrial-applications-of-3d-printing-the-ultimate-guide/

[2] J. Wan, A. Lopez, and M. Al Faruque, “Exploiting wireless channel randomness to generate keys for automotive cyber-physical system security,” ACM/IEEE Internation Conference on Cyber-Physical Systems (ICCPS’ 16), 2016.

[3] T. Wohlers, “Wohlers report 2014-3D printing and additive manufacturing-state of the industry,” Wohlers Associates, 2014.

[4] R. Mitchell and C. Ing-Ray. (2014) “A Survey of Intrusion Detection Techniques for Cyber Physical Systems.” In ACM Computer Survey Vol. 46. https://doi.org/10.1145/2542049.

[5] S. Salinas Monroy, M. Li, P. Li. (2018)“Energy-Based Detection of Defect Injection Attacks in IoT-Enabled Manufacturing.” In 2018 IEEE Global Communications Conference (GLOBECOM), 1–6. IEEE. https://doi.org/10.1109/GLOCOM.2018.8647631.

[6] P. Johnson, “Global Threat Intelligence Report,” 2020. https://globalthreatassociates.com/press83.html

[7] P. Sean, “Cybersecurity for Smart Factories in the Manufacturing Industry,” 2020. Deloitte United States https://www2.deloitte.com/us/en/pages/energy-and resources/articles/smart-factory-cybersecurity-manufacturing-industry.html

[8] M. Caroline. (2015) “Shellshock Attack on Linux Systems – Bash.” *International Research Journal of Engineering and Technology*, 1322–25.

[9] A. Paul et al., “A Real-Time Iterative Machine Learning Approach for Temperature Profile Prediction in Additive Manufacturing Processes,” in 2019 IEEE International Conference on

Data Science and Advanced Analytics (DSAA), Washington, DC, USA, Oct. 2019, pp. 541–550.

[10] M. Luís, A. Kangas, K. Kukko, B. Mølgaard, A. Säämänen, T. Kanerva, I. Flores Ituarte, (2017) "Characterization of Emissions from a Desktop 3D Printer." *Journal of Industrial Ecology* 21: S94–106. https://doi.org/10.1111/jiec.12569.

[11] Y. Li, W. Zhao, Q. Li, T. Wang, and G. Wang, "In-Situ Monitoring and Diagnosing for Fused Filament Fabrication Process Based on Vibration Sensors," *Sensors*, vol. 19, no. 11, p. 2589, Jun. 2019, doi: 10.3390/s19112589.

[12] O. Charlie, "Colonial Pipeline attack: Everything you need to know by ZDNet," 2021. https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/

[13] L. Hung-Jen, C. Lin, Y. Lin, and K. Tung. 2013. "Intrusion Detection System: A Comprehensive Review." *Journal of Network and Computer Applications* 36 (1): 16–24. https://doi.org/10.1016/j.jnca.2012.09.004.

[14] J. Lindsay. (2013) "*Stuxnet and the Limits of Cyber Warfare*." Security Studies 22 (3): 365–404. https://doi.org/10.1080/09636412.2013.816122.

[15] B. Burgess, E. Wustrow, and J. A. Halderman, "*Replication Prohibited: Attacking Restricted Keyways with 3D-Printing*. In 9th USENIX Workshop on Offensive Technologies (WOOT 15).," 2015.

[16] T. Mahan and J. Menold, "*Simulating Cyber-Physical Systems: Identifying Vulnerabilities for Design and Manufacturing Through Simulated Additive Manufacturing Environments*," Additive Manufacturing, vol. 35, p. 101232, Oct. 2020, doi: 10.1016/j.addma.2020.101232.

[17] L. D. Sturm, C. B. Williams, J. A. Camelio, J. White, and R. Parker, "Cyber-Physical Vulnerabilities in Additive Manufacturing Systems: A Case Study Attack on the .STL File with Human Subjects," *Journal of Manufacturing Systems*, vol. 44, pp. 154–164, Jul. 2017, doi: 10.1016/j.jmsy.2017.05.007.

[18] S. B. Moore, W. B. Glisson, and M. Yampolskiy, "Implications of Malicious 3D Printer Firmware.," *In Proceedings of the 50th Hawaii International Conference on System Sciences, 2017*.

[19] Q. Do, B. Martini, and K.-K. R. Choo, "A Data Exfiltration and Remote Exploitation Attack on Consumer 3D Printers," IEEE *Transactions on Information Forensics and Security*, vol. 11, no. 10, pp. 2174–2186, Oct. 2016, doi: 10.1109/TIFS.2016.2578285.

[20] Maggi, Federico, and S. Zanero. 2007. "On the Use of Different Statistical Tests for Alert Correlation – Short Paper." *In Recent Advances in Intrusion Detection*, 167–77. Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-74320-0_9.

[21] Manadhata, Pratyusa K., and J. M. Wing. 2010. "An Attack Surface Metric." IEEE *Transactions on Software Engineering* 3: 371–86.

[22] Y. Gao, B. Li, W. Wang, W. Xu, C. Zhou, and Z. Jin, "Watching and Safeguarding Your 3D Printer: Online Process Monitoring Against Cyber-Physical Attacks," *Association for Computing Machinery*. Interact. Mob. Wearable Ubiquitous Technol., vol. 2, pp. 1–27, Sep. 2018, doi: 10.1145/3264918.

[23] M. Wu and Y. Moon, "Alert Correlation for Cyber-Manufacturing Intrusion Detection," Procedia Manufacturing, vol. 34, pp. 820–831, 2019, doi: 10.1016/j.promfg.2019.06.197.

[24] T. Wohlers, "Wohlers report 2014-3D printing and additive manufacturing-state of the industry," *Wohlers Associates*, 2014.

[25] Economics and Statistics Administration, “Intellectual property and the u.s. economy: *Industries in focus*,” 2012.

[26] H. Stephanie, “3D Printed Air Duct Based on Fluid Dynamics: The Cool Parts Show #26,” 2021. https://www.additivemanufacturing.media/articles/3d-printed-air-duct-based-on-fluid-dynamics-the-cool-parts-show-26

[27] F.X. Standaert, T. G. Malkin, and M. Yung, “A unified framework for the analysis of side-channel key recovery attacks,” in *Advances in Cryptology-EUROCRYPT 2009*, pp. 443–461, Springer, 2009.

[28] U. Jerry, “GE Aviation Readies First 3-D Printed Jet Engine Nozzle at Alabama Plant,” Made in Alabama, Jun. 15, 2017. https://www.madeinalabama.com/2015/06/ge-aviation readies-first-3-d-printed-jet-engine-nozzle/

[29] C. Lucas, “The 7 Main Types of Additive Manufacturing, All3DP Pro,” 2019. https://all3dp.com/2/main-types-additive-manufacturing/

[30] S. K. Arul Prakash, T. Mahan, G. Williams, C. McComb, J. Menold, and C. S. Tucker, “Detection of System Compromise in Additive Manufacturing Using Video Motion Magnification,” *Journal of Mechanical Design*, vol. 142, no. 3, p. 031109, Mar. 2020, doi: 10.1115/1.4045547.

[31] T. Wohlers, “Wohlers report 2021-3D printing and additive manufacturing-state of the industry,” *Wohlers Associates*, 2021.

[32] S. Salvador and P. Chan, “Toward Accurate Dynamic Time Warping in Linear Time and Space,” *IDA*, vol. 11, no. 5, pp. 561–580, Oct. 2007, doi: 10.3233/IDA-2007-11508.

[33] A. Esmaeil, “An Illustrative Introduction to Dynamic Time Warping, Towards Data Science,” 2019. https://towardsdatascience.com/an-illustrative-introduction-to-dynamic-time-warping-36aa98513b98

[34] M. Backes et al., “Acoustic side-channel attacks on printers.,” in *USENIX Security Symposium*, pp. 307–322, 2010.

[35] B. Robin, “Key Design Considerations for 3D Printing,” Hubs, 2016. https://www.hubs.com/knowledge-base/key-design-considerations-3d-printing/

[36] M. Wu, Z. Song, and Y. B. Moon, “Detecting Cyber-Physical Attacks in CyberManufacturing Systems with Machine Learning Methods,” *Journal of Intelligent Manufacturing*, Feb. 2017, doi: 10.1007/s10845-017-1315-5.

[37] N. Ronald S, “How to Select the Right Oscilloscope Current Probe, Keysight,” 2018. https://www.keysight.com/us/en/assets/7018-05961/application-notes/5992-2656.pdf

[38] Elhabashy, Ahmed. 2018. “Quality Control Tools for Cyber-Physical Security of Production Systems.” Virginia Polytechnic Institute and State University.

[39] Kemmerer, R.A., and G. Vigna. 2002. “Intrusion Detection: A Brief History and Overview.” Computer 35 (4): supl27-supl30. https://doi.org/10.1109/MC.2002.1012428.

[40] Khamphakdee, Nattawat, N. Benjamas, and S. Saiyod. 2014. “Improving Intrusion Detection System Based on Snort Rules for Network Probe Attack Detection.” 2014 2nd *International Conference on Information and Communication Technology*, ICoICT 2014, no. May: 69–74. https://doi.org/10.1109/ICoICT.2014.6914042.

[41] Kim, A. Chan, W.H. Park, and D.H. Lee. 2013. “A Study on the Live Forensic Techniques for Anomaly Detection in User Terminals.” *International Journal of Security and Its Applications 7* (1).

[42] Kumar, M, S Siddique, and H. Noor. 2009. “Feature-Based Alert Correlation in Security Systems Using Self Organizing Maps.” Proceedings of SPIE - *The International Society for Optical Engineering* 7344 (Id). https://doi.org/10.1117/12.820000.

[43] Kumar, Mohit. 2018. “TSMC Chip Maker Blames WannaCry Malware for Production Halt.” The Hacker News. 2018. https://thehackernews.com/2018/08/tsmc-wannacry-ransomware-attack.html.

[44] Langner, Ralph. 2011. “Stuxnet: Dissecting a Cyberwarfare Weapon.” IEEE Security and Privacy 9 (3): 49–51. https://doi.org/10.1109/MSP.2011.67.

[45] Lee, Keunsoo, J. Kim, K.H. Kwon, Y. Han, and S. Kim. 2008. “DDoS Attack Detection Method Using Cluster Analysis.” *Expert Systems with Applications* 34 (3): 1659–65. https://doi.org/10.1016/j.eswa.2007.01.040.

[46] Kemmerer, R.A., and G. Vigna. 2002. “Intrusion Detection: A Brief History and Overview.” Computer 35 (4): supl27-supl30. https://doi.org/10.1109/MC.2002.1012428.

[47] Khamphakdee, Nattawat, N. Benjamas, and S. Saiyod. 2014. “Improving Intrusion Detection System Based on Snort Rules for Network Probe Attack Detection.” 2014 2nd *International Conference on Information and Communication Technology*, ICoICT 2014, no. May: 69–74. https://doi.org/10.1109/ICoICT.2014.6914042.

[48] Kim, A. Chan, W. H. Park, and D.H. Lee. 2013. “A Study on the Live Forensic Techniques for Anomaly Detection in User Terminals.” *International Journal of Security and Its Applications* 7 (1).

[49] Kumar, M, S Siddique, and H. Noor. 2009. “Feature-Based Alert Correlation in Security Systems Using Self Organizing Maps.” Proceedings of SPIE - *The International Society for Optical Engineering* 7344 (Id). https://doi.org/10.1117/12.820000.

[50] Kumar, Mohit. 2018. “TSMC Chip Maker Blames WannaCry Malware for Production Halt.” The Hacker News. 2018. https://thehackernews.com/2018/08/tsmc-wannacry-ransomware-attack.html.

[51] Langner, Ralph. 2011. “Stuxnet: Dissecting a Cyberwarfare Weapon.” *IEEE Security and Privacy* 9 (3): 49–51. https://doi.org/10.1109/MSP.2011.67.

[52] Lee, Keunsoo, J. Kim, K.H. Kwon, Y.Han, and S. Kim. 2008. “DDoS Attack Detection Method Using Cluster Analysis.” *Expert Systems with Applications* 34 (3): 1659–65. https://doi.org/10.1016/j.eswa.2007.01.040.

[53] Debar, Herve. 2017. “What Is Behavior Based Intrusion Detection?” SANS. 2017. https://www.sans.org/security-resources/idfaq/what-is-behavior-based-intrusion-detection/2/6.

[54] Delio, T., J. Tlusty, and S. Smith. 1992. “Use of Audio Signals for Chatter Detection and Control.” *Journal of Manufacturing Science and Engineering* 114 (2): 146. https://doi.org/10.1115/1.2899767.

[55] Duro, João A, J.A. Padget, C.R. Bowen, and H. A. Kim. 2016. “Multi-Sensor Data Fusion Framework for CNC Machining Monitoring.” *Mechanical Systems and Signal Processing* 67: 505–20.

[56] M. Yampolskiy, W. E. King, J. Gatlin, S. Belikovetsky, A. Brown, A. Skjellum, and Y. Elovici, “Security of additive manufacturing: Attack taxonomy and survey,” *Additive Manuf.*, vol. 21, pp. 431_457, May 2018.

[57] Elshoush, H. Tagelsir, and I.M. Osman. 2012. “An Improved Framework for Intrusion Alert.” *In Proceedings of the World Congress on Engineering*, I:4–9. http://www.iaeng.org/publication/WCE2012/WCE2012_pp518-523.pdf.

[58] H. Vincent et al., “Trojan detection and side-channel analyses for cyber-security in cyber-physical manufacturing systems,”

[59] J. Wan, A. Lopez, and M. Al Faruque, “Exploiting wireless channel randomness to generate keys for automotive cyber-physical system security,” ACM/IEEE Internation Conference on Cyber-Physical Systems (ICCPS’ 16), 2016.hit-by-wannacry-virus-fears-it-could-cripple-some-jet-production/.

[60] Giraldo, Jairo, E. Sarkar, A.A. Cardenas, M. Maniatakos, and M. Kantarcioglu. 2017. “Security and Privacy in Cyber-Physical Systems: A Survey of Surveys.” IEEE *Design and Test* 34 (4): 7–17. https://doi.org/10.1109/MDAT.2017.2709310.

[61] Giraldo, Jairo, D. Urbina, A. Cardenas, J. Valente, Mu. Faisal, J. Ruths, N.O. Tippenhauer, H. Sandberg, and R. Candell. 2018. “A Survey of Physics-Based Attack Detection in Cyber-Physical Systems.” *ACM Computing Surveys* 51 (4): 1–36. https://doi.org/10.1145/3203245.

[62] Hadžiosmanović, Dina, R. Sommer, E. Zambon, and P.H. Hartel. 2014. “Through the Eye of the PLC.” In Annual Computer Security Applications Conference, 126–35. https://doi.org/10.1145/2664243.2664277.

[63] Hansman, Simon, and R. Hunt. 2005. “A Taxonomy of Network and Computer Attacks.” Computers and Security 24 (1): 31–43. https://doi.org/10.1016/j.cose.2004.06.011.

[64] M. A. Al Faruque, S. R. Chhetri, A. Canedo, and J. Wan, “Acoustic Side-Channel Attacks on Additive Manufacturing Systems,” in 2016 ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS), Vienna, Austria, Apr. 2016, pp. 1–10. doi: 10.1109/ICCPS.2016.7479068.

[65] S. Chhetri and M. A. Al Faruque, “Side Channels of Cyber-Physical Systems: Case Study in Additive Manufacturing,” IEEE *Design & Test*, vol. 34, no. 4, pp. 18–25, Aug. 2017, doi: 10.1109/MDAT.2017.2682225.

[66] J. Wan, A. Lopez, and M. Al Faruque, “Exploiting wireless channel randomness to generate keys for automotive cyber-physical system security,” ACM/IEEE Internation Conference on Cyber-Physical Systems (ICCPS’ 16), 2016.

[67] S.-Y. Yu, A. V. Malawade, S. R. Chhetri, and M. A. Al Faruque, “Sabotage Attack Detection for Additive Manufacturing Systems,” IEEE Access, vol. 8, pp. 27218–27231, 2020, doi: 10.1109/ACCESS.2020.2971947.

[68] Kaspersky Lab. 2017. “The State of Industrial Cybersecurity 2017.” Business Advantage Group Limited.

[69] Waslo, René, T. Lewis, R. Hajj, and R. Carton. 2017. “Industry 4.0 and Cybersecurity: Managing Risk in an Age of Connected Production.” Deloitte University Press, 1–21.

[70] B. Leukers et al., “Hydroxyapatite scaffolds for bone tissue engineering made by 3D printing,” *Journal of Materials Science: Materials in Medicine*, vol. 16, no. 12, pp. 1121–1124, 2005.

[71] Z. Yu, L. Zhou, Z. Ma, and M. A. El-Meligy, “Trustworthiness Modeling and Analysis of Cyber-physical Manufacturing Systems,” IEEE Access, vol. 5, pp. 26076–26085, 2017, doi: 10.1109/ACCESS.2017.2777438.

[72] H. Vincent, L. Wells, P. Tarazaga, and J. Camelio, “Trojan Detection and Side-channel Analyses for Cyber-security in Cyber-physical Manufacturing Systems,” *Procedia Manufacturing*, vol. 1, pp. 77–85, 2015, doi: 10.1016/j.promfg.2015.09.065.

[73] Vincent, Hannah, L. Wells, P. Tarazaga, and J. Camelio. 2015. “Trojan Detection and Side-Channel Analyses for Cyber-Security in Cyber-Physical Manufacturing Systems.” *Procedia Manufacturing* 1: 77–85. https://doi.org/10.1016/j.promfg.2015.09.065.

[74] M. Wu, V. V. Phoha, Y. B. Moon, and A. K. Belman, “Detecting Malicious Defects in 3D Printing Process Using Machine Learning and Image Classification,” in Volume 14: Emerging Technologies; Materials: Genetics to Structures; Safety Engineering and Risk Analysis, Phoenix, Arizona, USA, Nov. 2016, p. V014T07A004. doi: 10.1115/IMECE2016-67641.

[75] S. R. Chhetri, A. Canedo, and M. A. A. Faruque, “KCAD: Kinetic Cyber-Attack Detection Method for Cyber-Physical Additive Manufacturing Systems,” in Proceedings of the 35th *International Conference on Computer-Aided Design* - ICCAD ’16, Austin, Texas, 2016, pp. 1–8. doi: 10.1145/2966986.2967050.

[76] J. Brandman, L. Sturm, J. White, and C. Williams, “A Physical Hash for Preventing and Detecting Cyber-Physical Attacks in Additive Manufacturing Systems,” *Journal of Manufacturing Systems*, vol. 56, pp. 202–212, Jul. 2020, doi: 10.1016/j.jmsy.2020.05.014.

[77] J. Straub, “Identifying Positioning-Based Attacks Against 3D Printed Objects and the 3D Printing Process,” Anaheim, California, U.S, 2017, p. 1020304. doi: 10.1117/12.2264671.

[78] J. Straub, “Physical Security and Cyber Security Issues and Human Error Prevention For 3D Printed Objects: Detecting the Use of An Incorrect Printing Material,” Anaheim, California, United States, Jun. 2017, p. 102200K. doi: 10.1117/12.2264578.

[79] S. Belikovetsky, Y. Solewicz, M. Yampolskiy, J. Toh, and Y. Elovici, “Detecting Cyber-Physical Attacks in Additive Manufacturing Using Digital Audio Signing,” arXiv:1705.06454, May 2017, [Online]. Available: http://arxiv.org/abs/1705.06454

[80] J. Gatlin, S. Belikovetsky, S. B. Moore, Y. Solewicz, Y. Elovici, and M. Yampolskiy, "Detecting Sabotage Attacks in Additive Manufacturing Using Actuator Power Signatures," IEEE Access, vol. 7, pp. 133421–133432, 2019, doi: 10.1109/ACCESS.2019.2928005.

[81] M. Brown and L. Rabiner, "Dynamic Time Warping for Isolated Word Recognition Based on Ordered Graph Searching Techniques," IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), 1982. https://ieeexplore.ieee.org/document/1171695. p. 1255-1258, doi: 10.1109/ICASSP. 117695

[82] F. Ahourai and M. A. Al Faruque, "Grid impact analysis of a residential microgrid under various penetration rates in grid lab," Center for Embedded Computer Systems, Irvine, CA, 2013.

[83] M. Faruque, L. Dalloro, S. Zhou, H. Ludwig, and G. Lo, "Managing residential-level charging using network-as-automation platform (nap) technology," in Electric Vehicle Conference (IEVC), 2012 IEEE International, pp. 1–6, IEEE, 2012.

[84] M. Al Faruque, S. Rokka Chhetri, A. Canedo, and J. Wan, "Acoustic side-channel attacks on additive manufacturing systems," ACM/IEEE Internation Conference on Cyber-Physical Systems (ICCPS' 16), 2016.

[85] M. A. Faruque, S. R. Chhetri, A. Canedo, and J. Wan, "Acoustic side-channel attacks on additive manufacturing systems," in Proc. ACM/IEEE Int. Conf. Cyber-Phys. Syst. (ICCPS), Apr. 2016, Art. no. 19. [Online]. Available: http://aicps.eng.uci.edu/papers/3-d-printer-securityalfaruque. Pdf

[86] M. Backes, M. Durmuth, S. Gerling, M. Pinkal, and C. Sporleder, "Acoustic Side-Channel Attacks on Printers.," 9th USENIX Workshop on Offensive Technologies (WOOT'15)., 2015.

[87] B. Burgess, E. Wustrow, and J. A. Halderman, “Replication Prohibited: Attacking Restricted Keyways with 3D-Printing. In9th USENIX Workshop on Offensive Technologies (WOOT 15).,” 2015.

[88] T. Mahan and J. Menold, “Simulating Cyber-Physical Systems: Identifying Vulnerabilities for Design and Manufacturing Through Simulated Additive Manufacturing Environments,” *Additive Manufacturing*, vol. 35, p. 101232, Oct. 2020, doi: 10.1016/j.addma.2020.101232.

[89] L. D. Sturm, C. B. Williams, J. A. Camelio, J. White, and R. Parker, “Cyber-Physical Vulnerabilities in Additive Manufacturing Systems: A Case Study Attack on the .STL File with Human Subjects,” *Journal of Manufacturing Systems*, vol. 44, pp. 154–164, Jul. 2017, doi: 10.1016/j.jmsy.2017.05.007.

[90] M. Yampolskiy, W. E. King, J. Gatlin, S. Belikovetsky, A. Brown, A. Skjellum, and Y. Elovici, “Security of additive manufacturing: Attack taxonomy and survey,” *Additive Manuf.*, vol. 21, pp. 431_457, May 2018.

[91] Yampolskiy, Mark, Anthony Skjellum, Michael Kretzschmar, Ruel A. Overfelt, Kenneth R. Sloan, and Alec Yasinsac. 2016. “Using 3D Printers as Weapons.” *International Journal of Critical Infrastructure Protection* 14: 58–71. https://doi.org/10.1016/j.ijcip.2015.12.004.

[92] Elhabashy, Ahmad E., Lee J. Wells, Jaime A. Camelio, and William H. Woodall. 2018. “A Cyber-Physical Attack Taxonomy for Production Systems: A Quality Control Perspective.” *Journal of Intelligent Manufacturing*. https://doi.org/10.1007/s10845-018-1408-9.

[93] M. Wu, V. V. Phoha, Y. B. Moon, and A. K. Belman, “Detecting Malicious Defects in 3D Printing Process Using Machine Learning and Image Classification,” in Volume 14:

Emerging Technologies; Materials: Genetics to Structures; Safety Engineering and Risk Analysis, Phoenix, Arizona, USA, Nov. 2016, p. V014T07A004. doi: 10.1115/IMECE2016-67641.

[94] Y. Z. Lun, A. D'Innocenzo, I. Malavolta, and M. D. Di Benedetto, "Cyber-Physical Systems Security: a Systematic Mapping Study," *Journal of Systems and Software*, vol. 149, pp. 174–216, Mar. 2019, doi: 10.1016/j.jss.2018.12.006.

[95] A. Canedo and M. A. Al-Faruque, "Towards parallel execution of iec 61131 industrial cyber-physical systems applications," in Design, Automation & Test in Europe Conference & Exhibition (DATE), 2012, pp. 554–557, IEEE, 2012.

[96] A. Canedo, H. Ludwig, and M. A. Al Faruque, "High communication throughput and low scan cycle time with multi/many-core programmable logic controllers," Embedded Systems Letters, IEEE, vol. 6, no. 2, pp. 21–24, 2014.

[97] S.-Y. Yu, A. V. Malawade, S. R. Chhetri, and M. A. Al Faruque, "Sabotage Attack Detection for Additive Manufacturing Systems," IEEE Access, vol. 8, pp. 27218–27231, 2020, doi: 10.1109/ACCESS.2020.2971947.

[98] A. Zarreh, C. Saygin, H. Wan, Y. Lee, and A. Bracho, "A game theory based cybersecurity assessment model for advanced manufacturing systems," *Procedia Manufacturing*, vol. 26, pp. 1255–1264, 2018, doi: 10.1016/j.promfg.2018.07.162.

[99] Z. DeSmit, A. E. Elhabashy, L. J. Wells, and J. A. Camelio, "An approach to cyber-physical vulnerability assessment for intelligent manufacturing systems," *Journal of Manufacturing Systems*, vol. 43, pp. 339–351, Apr. 2017, doi: 10.1016/j.jmsy.2017.03.004.

[100] H. Orojloo and M. A. Azgomi, “A method for evaluating the consequence propagation of security attacks in cyber–physical systems,” *Future Generation Computer Systems*, vol. 67, pp. 57–71, Feb. 2017, doi: 10.1016/j.future.2016.07.016.

[101] J. Garstka and G. Peters, “View-dependent 3d projection using depth-image-based head tracking,” in 8th IEEE International Workshop on ProjectorCamera Systems PROCAMS, pp. 52–57, 2011.

[102] C. Harris and M. Stephens, “A combined corner and edge detector.,” in Alvey vision conference, vol. 15, p. 50, Citeseer, 1988.

[103] B. D. Lucas, T. Kanade, et al., “An iterative image registration technique with an application to stereo vision.,” in *IJCAI*, vol. 81, pp. 674–679, 1981.

[104] M. S. Nixon and A. S. Aguado, Feature extraction & image processing for computer vision. Academic Press, 2012.

[105] A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, and S. Sastry, “Challenges for securing cyber physical systems,” in Workshop on future directions in cyber-physical systems security, 2009.

[106] Duro, João A, Julian A Padget, Chris R Bowen, and H Alicia Kim. 2016. “Multi-Sensor Data Fusion Framework for CNC Machining Monitoring.” *Mechanical Systems and Signal Processing* 67: 505–20.

[107] Elhabashy, Ahmad E., Lee J. Wells, Jaime A. Camelio, and William H. Woodall. 2018. “A Cyber-Physical Attack Taxonomy for Production Systems: A Quality Control Perspective.” *Journal of Intelligent Manufacturing*. https://doi.org/10.1007/s10845-018-1408-9.

[108] L. Robert, “Normalization for DTW,” 2007. http://luscinia.sourceforge.net/page26/page/14.html.

[109] Elshoush, H. Tagelsir, and I.M. Osman. 2012. “An Improved Framework for Intrusion Alert.” In Proceedings of the World Congress on Engineering, I:4–9. http://www.iaeng.org/publication/WCE2012/WCE2012_pp518-523.pdf.

[110] Goldenberg, Niv, and A. Wool. 2013. “Accurate Modeling of Modbus/TCP for Intrusion Detection in SCADA Systems.” *International Journal of Critical Infrastructure Protection* 6 (2): 63–75. https://doi.org/10.1016/j.ijcip.2013.05.001.

[111] Hadžiosmanović, Dina, R. Sommer, E. Zambon, and P.H. Hartel. 2014. “Through the Eye of the PLC.” In Annual Computer Security Applications Conference, 126–35. https://doi.org/10.1145/2664243.2664277.

[112] Kumar, Mohit. 2018. “TSMC Chip Maker Blames WannaCry Malware for Production Halt.” The Hacker News. 2018. https://thehackernews.com/2018/08/tsmc-wannacry-ransomware-attack.html.

[113] Langner, Ralph. 2011. “Stuxnet: Dissecting a Cyberwarfare Weapon.” IEEE *Security and Privacy* 9 (3): 49–51. https://doi.org/10.1109/MSP.2011.67.

[114] Quarta, Davide, M. Pogliani, M. Polino, F. Maggi, A.M. Zanchettin, and S. Zanero. 2017. “An Experimental Security Analysis of an Industrial Robot Controller.” 2017 IEEE *Symposium on Security and Privacy* (SP), 268–86. https://doi.org/10.1109/SP.2017.20.

[115] Roschke, Sebastian, F. Cheng, and C. Meinel. 2011. “A New Alert Correlation Algorithm Based on Attack Graph.” In Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 6694 LNCS:58–67. https://doi.org/10.1007/978-3-642-21323-6_8.

[116] Ahmadinejad, S.H., and S. Jalili. 2009. “Alert Correlation Using Correlation Probability Estimation and Time Windows.” 2009 International Conference on Computer Technology and Development, 170-175. Kota Kinabalu, Malaysia: Institute of Electrical and Electronics Engineers. doi: 10.1109/ICCTD.2009.22.

[117] Contag, Moritz, G. Li, A. Pawlowski, F. Domke, K. Levchenko, T. Holz, and S. Savage. 2017. “How They Did It: An Analysis of Emission Defeat Devices in Modern Automobiles.” Proceedings - IEEE Symposium on Security and Privacy, 231–50. https://doi.org/10.1109/SP.2017.66.

[118] Zhu, Bonnie, A. Joseph, S. Sastry. 2011. “A Taxonomy of Cyber Attacks on SCADA System.” Internet of Things (IThings/CPSCom), 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing.

[119] Duro, J.A, J.A. Padget, C.R. Bowen, and H.A. Kim. 2016. “Multi-Sensor Data Fusion Framework for CNC Machining Monitoring.” *Mechanical Systems and Signal Processing* 67: 505–20.

[120] Vincent, Hannah, L. Wells, P. Tarazaga, and J. Camelio. 2015. “Trojan Detection and Side-Channel Analyses for Cyber-Security in Cyber-Physical Manufacturing Systems.” *Procedia Manufacturing* 1: 77–85. https://doi.org/10.1016/j.promfg.2015.09.065.

[121] Giraldo, Jairo, D. Urbina, A. Cardenas, J. Valente, M. Faisal, J. Ruths, N.O. Tippenhauer, Henrik Sandberg, and Richard Candell. 2018. “A Survey of Physics-Based Attack Detection in Cyber-Physical Systems.” ACM Computing Surveys 51 (4): 1–36. https://doi.org/10.1145/3203245.

[122] Wuest, Thorsten, C. Irgens, and K.D. Thoben. 2014. “An Approach to Monitoring Quality in Manufacturing Using Supervised Machine Learning on Product State Data.”

Journal of Intelligent Manufacturing 25 (5): 1167–80. https://doi.org/10.1007/s10845-013-0761-y.

[123] Yampolskiy, Mark, A. Skjellum, M. Kretzschmar, R.A. Overfelt, K.R. Sloan, and A. Yasinsac. 2016. "Using 3D Printers as Weapons." *International Journal of Critical Infrastructure Protection* 14: 58–71. https://doi.org/10.1016/j.ijcip.2015.12.004.

[124] Roschke, Sebastian, F. Cheng, and C. Meinel. 2011. "A New Alert Correlation Algorithm Based on Attack Graph." In Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 6694 LNCS:58–67. https://doi.org/10.1007/978-3-642-21323-6_8.

[125] Hansman, Simon, and R. Hunt. 2005. "A Taxonomy of Network and Computer Attacks." Computers and Security 24 (1): 31–43. https://doi.org/10.1016/j.cose.2004.06.011.

[126] Jung, J. Hyuk, J.Y. Kim, H.C. Lee, and J.H. Yi. 2013. "Repackaging Attack on Android Banking Applications and Its Countermeasures." Wireless Personal Communications 73 (4): 1421–37. https://doi.org/10.1007/s11277-013-1258-x.

[127] Spring, Tom. 2018. Leaky Backup Spills 157 GB of Automaker Secrets. Threatpost. https://threatpost.com/leaky-backup-spills-157-gb-of-automaker-secrets/134293/.

[128] Kumar, Mohit. 2018. "TSMC Chip Maker Blames WannaCry Malware for Production Halt." The Hacker News. 2018. https://thehackernews.com/2018/08/tsmc-wannacry-ransomware-attack.html.

[129] Quarta, Davide, M. Pogliani, M. Polino, F. Maggi, Zanchettin, and S. Zanero. 2017. "An Experimental Security Analysis of an Industrial Robot Controller." 2017 IEEE Symposium on Security and Privacy (SP), 268–86. https://doi.org/10.1109/SP.2017.20.

[130] Lindsay, J. 2013. “Stuxnet and the Limits of Cyber Warfare.” Security Studies 22 (3): 365–404. https://doi.org/10.1080/09636412.2013.816122.

[131] Turner, Hamilton, J. White, J.A. Camelio, C. Williams, B. Amos, and R. Parker. 2015. “Bad Parts: Are Our Manufacturing Systems at Risk of Silent Cyberattacks?” IEEE Security and Privacy 13 (3): 40–47. https://doi.org/10.1109/MSP.2015.60.

[132] Moore, Samuel, M. Yampolskiy, J.T. McDonald, T.R. Andel, and J. Gatlin. 2016. “Buffer Overflow Attack’s Power Consumption Signatures,” 1–7. https://doi.org/10.1145/3015135.3015141.

[133] Orebaugh, Angela, and B. Pinkard. 2011. Nmap in the Enterprise: Your Guide to Network Scanning.

[134] Peterson, Leif. 2009. “K-Nearest Neighbor.” Scholarpedia. 2009. https://doi.org/10.4249/scholarpedia.1883.

[135] A. Slaughter, M. Yampolskiy, M. Matthews, W. E. King, G. Guss, and Y. Elovici, “How to ensure bad quality in metal additive manufacturing: In-Situ infrared thermography from the security perspective,” in Proc. 12th Int. Conf. Availability, Rel. Secur., 2017, Art. no. 78. P. Cano, E.

[136] Batlle, T. Kalker, and J. Haitsma, “A review of audio fingerprinting,” J. VLSI Signal Process. Syst. Signal, *Image Video Technol*., vol. 41, no. 3, pp. 271–284, 2005.

[137] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, and B. Sunar, “Trojan detection using IC fingerprinting,” in Proc. IEEE Symp. Security. Privacy (SP), May 2007, pp. 296–310.

[138] S. E. Zeltmann, N. Gupta, N. G. Tsoutsos, M. Maniatakos, J. Rajendran, and R. Karri, "Manufacturing and security challenges in 3D printing," *J. Minerals*, vol. 68, no. 7, pp. 1872–1881, 2016.

[139] M. Vaezi and C. K. Chua, "Effects of layer thickness and binder saturation level parameters on 3D printing process," *Int. J. Adv. Manuf. Technol.*, vol. 53, nos. 1–4, pp. 275–284, 2011.

[140] Y. Pan et al., "Taxonomies for Reasoning About Cyber-physical Attacks in IoT-based Manufacturing Systems," *Int. J. Interact. Multimed. Artif. Intell.*, vol. 4, no. 3, pp. 45–54, Mar. 2017.

[141] J. J. Johnson, "Print, lock, and load: 3-D printers, creation of guns, and the potential threat to fourth amendment rights," Univ. Illinois J. Law, Technol. Policy, p. 337, 2013.

[142] D. D. Hernandez, "Factors Affecting Dimensional Precision of Consumer 3D Printing," *Int. J. Aviat. Aeronaut. Aerosp.*, vol. 2, no. 4, pp. 1–43, Sep. 2015.

[143] S. Berumen, F. Bechmann, S. Lindner, J.-P. Kruth, and T. Craeghs, "Quality control of laser- and powder bed-based Additive Manufacturing (AM) technologies," Laser Assist. Net Shape Eng. 6 Proc. LANE 2010 Part 2, vol. 5, pp. 617–622, Jan. 2010.

[144] Rao PK, (Peter) Liu J, Roberson D, (James) Kong Z, Williams C. Online real-time quality monitoring in additive manufacturing processes using heterogeneous sensors. *J Manuf Sci Eng* 2015;137:61007–12. https://doi.org/10.1115/1.4029823.

[145] X. Z. Hang. (2013). Security Attack to 3D Printing. [Online]. Available: http://www.claudxiao.net/Attack3DPrinting-Claud-en.pdf.

[146] A. Ilie, H. Ali, and K. Mumtaz, ``In-built customized mechanical failure of 316L components fabricated using selective laser melting," Technologies, vol. 5, no. 1, p. 9, 2017.

[147] Elhabashy, Ahmad E., L.J. Wells, Jaime A. Camelio, and William H. Woodall. 2018. “A Cyber-Physical Attack Taxonomy for Production Systems: A Quality Control Perspective.” *Journal of Intelligent Manufacturing*. https://doi.org/10.1007/s10845-018-1408-9.

[148] Elhabashy, Ahmed. 2018. “Quality Control Tools for Cyber-Physical Security of Production Systems.” Virginia Polytechnic Institute and State University.

[149] A. Davis et al., “The visual microphone: Passive recovery of sound from video,” ACM Trans. Graph, vol. 33, no. 4, p. 79, 2014.

[150] J. Wan, A. Lopez, and M. Al Faruque, “Exploiting wireless channel randomness to generate keys for automotive cyber-physical system security,” ACM/IEEE Internation Conference on Cyber-Physical Systems (ICCPS’ 16), 2016.