Sabotage Attack Detection for Additive Manufacturing Systems

SHIH-YUAN YU, (Student Member, IEEE), ARNAV VAIBHAV MALAWADE, (Student Member, IEEE), SUJIT ROKKA CHHETRI, AND MOHAMMAD ABDULLAH AL FARUQUE, (Senior Member, IEEE)
Department of Electrical Engineering and Computer Science, University of California-Irvine, Irvine, CA 92697, USA
Corresponding author: Shih-Yuan Yu (shihyuay@uci.edu)

ABSTRACT This paper presents a novel multi-modal sabotage attack detection system for Additive Manufacturing (AM) machines. By utilizing multiple side-channels, we improve system state estimation significantly in comparison to uni-modal techniques. Besides, we analyze the value of each side-channel for performing attack detection in terms of mutual information shared with the machine control parameters. We evaluate our system on real-world test cases and achieve an attack detection accuracy of 98.15%. AM, or 3D Printing, is seeing practical use for the rapid prototyping and production of industrial parts. The digitization of such systems not only makes AM a crucial technology in Industry 4.0 but also presents a broad attack surface that is vulnerable to kinetic cyberattacks. In the field of AM security, sabotage attacks are cyberattacks that introduce inconspicuous defects to a manufactured component at any specific process of the AM digital process chain, resulting in the compromise of the component’s structural integrity and load-bearing capabilities. Defense mechanisms that detect such attacks using side-channel analysis have been studied. However, most current works focus on modeling the state of AM systems using a single side-channel, thus limiting their effectiveness at attack detection. In this paper, we demonstrate the value of a multi-modal sabotage attack detection system in comparison to uni-modal techniques.

INDEX TERMS Additive-manufacturing, cyber-physical systems security, side-channel analysis, 3D-printer security, sabotage attack.

I. INTRODUCTION Additive Manufacturing (AM), or 3D Printing, is a manufacturing process that constructs a 3D physical object layer-by-layer according to its digital representation. Fused Deposition Modeling (FDM) is one of the standard AM methods that forms an object by depositing melted thermoplastic material at the proper temperature. FDM-based AM technologies have been vastly applied in the manufacturing of functional end-products across fields [1], [2]. For example, the Airbus 350 aircraft has been flying with more than 1000 3D-printed functional parts [3], while General Electric (GE) has also additively produced over 30,000 fuel nozzle tips for Leading Edge Aviation Propulsion (LEAP) jet engines [4], [5]. In the medical field, AM has also proved useful in manufacturing patient-specific parts for implants or prosthetics [6], [7]. The growth of AM plays a vital role in Industry 4.0 as it brings manufacturing to the next level where data can be gathered and analyzed across machines enabling faster, more flexible, and more efficient processes to produce higher-quality goods at a reduced cost [8]. In 2018, GE reported that the expected economic value brought by AM would be US$32.78 billion by 2023 [9]. The state of printing report from Sculpteo in 2019 also indicated that AM had been actively used in production applications by 51% of the enterprises [10]. The computerization of the production process propels these technological advancements; however, this also introduces new vulnerabilities to AM systems; hence great effort is spent studying cyberattacks on these systems [11]–[16]. Since AM systems are intrinsically Cyber-Physical Systems (CPS), cyberattacks on AM systems can have impacts that extend beyond the cyber domain into the physical one.

A. MOTIVATION Kinetic cyberattacks originate from the cyber domain and can lead to physical damage, injury, or even death [17]. In AM,
Sabotage attacks are one kind of kinetic cyberattack that target manufactured functional parts by decreasing their mechanical strength or reducing a part’s resistance to fatigue [12], [18]. By introducing inconspicuous yet damaging alterations in any specific process of the AM digital process chain, the structural integrity of a manufactured component can be compromised in a manner that is invisible to a human observer. If the manufactured objects are critical for their system, the attacks can even compromise the whole system’s structural integrity and pose a severe safety risk to its users. For example, an inconspicuous void (less than 1 mm in dimension) placed in the 3D design of a tensile test specimen can reduce its yield load by 14% [11]. Several works have focused on resolving AM security issues. However, existing AM security studies primarily focus on securing digital assets [19], [20], overlooking the fact that AM systems are cyber-physical systems. The AM system, or the printer, is comprised of a set of connected hardware components, and thus can unintentionally produce analog emissions during the operation of printing through different physical side-channels such as acoustics, electromagnetic radiation, vibration, and power. Sabotaging the structural integrity of 3D objects requires the attacker to make subtle variations to one or more of the sub-processes in the AM process chain, resulting in a change in the printer’s control parameters and a corresponding change to its analog emissions. To detect such modifications, we propose an attack detection system that continuously monitors and analyzes the side-channel information leaked during the operation of AM systems, allowing us to identify unusual analog emissions resulting from potential sabotage attacks.

**B. RESEARCH CHALLENGES**

AM sabotage attacks compromise the functionality or structural integrity of 3D objects by introducing flaws in the design. In AM systems, the information flow in the cyber domain has at least one corresponding signal flow in the physical domain. These signal flows actuate the physical processes accordingly, leading to the conversion of energy from one form to another, resulting in side-channel emissions that have a high degree of mutual information with the cyber domain control signals. This fact, in turn, allows us to correlate information between the two domains and validate that physical domain signals match their cyber domain counterparts. Since cyber-physical systems present a complex multi-domain attack surface, the vulnerabilities of AM systems are challenging to analyze and mitigate at design time. In this case, monitoring the operation of the targeted AM systems can be the most direct defense mechanism. The research challenges of designing such a defense system include:

1) Accurately modeling and estimating the state of the AM machine using side-channel information to distinguish intrusions/attacks from the normal operational errors with tolerances.

2) Developing an accurate detection system within the limitations of low-cost sensors and capable of detecting intrusions/attacks that can occur at various points in the AM digital process chain.

3) Making the system non-intrusive so that it can be applied to existing AM systems.

**C. NOVEL CONTRIBUTIONS**

Our previous work has tackled the research challenges mentioned above using acoustic side-channel information from a single sensor for sabotage attack detection [21]. Another previous work has investigated the use of various analog emissions (vibration, acoustic, magnetic, and power) to breach the confidentiality of 3D printed objects and how machine parameters are leaked to these different side-channels [22]. AM systems leak information about machine parameters in the form of analog emissions to different side-channels because of the physical characteristics of their actuation and movement. In this manner, a system that monitors and fuses all the available side-channel information can better model the state of an AM system and be a more accurate sabotage attack detection system. To this end, our novel research contributions are as follows:

1) **Modeling of an Adversary** to understand the various attack points in the digital process chain for effective implementation of the attack detection method.

2) **Statistical Estimation** to model the behavior of the AM systems by analyzing the relationship between the analog emissions in various side-channels and the control signals.

3) **Analysis of Various Analog Emissions** to determine the amount of control signal information leaked by the AM system to each side-channel, which can be used for sabotage attack detection.

4) **Multi-Modal Sabotage Attack Detection System** which uses multiple low-cost sensors to capture information from various side-channels and demonstrates better performance at sabotage attack detection compared to uni-modal techniques.

**D. PAPER ORGANIZATION**

The rest of this paper is organized as follows: Section II presents the related work on the current security issues in CPS and AM and how those security threats are defended; Section III introduces the background information about the AM process chain from both cyber (Section III-A) and physical (Section III-B) perspectives; Section IV illustrates the adversary model (Section IV-A) and the overall architecture of our proposed sabotage attack detection system (Section IV-B); the experimental setup and the results we have achieved are presented in Section V; the discussion regarding the limitations and feasibility of our system follows in Section V-F; finally, the paper will be concluded in Section VI.

**II. RELATED WORK**

The impacts of real-world kinetic cyberattacks have driven a significant research thrust into manufacturing...
CPS security [23]–[25]. One famous kinetic cyberattack was Stuxnet: a malicious computer worm that attacked Iran’s nuclear program, causing the catastrophic failure of uranium centrifuges [23]. Another cyber attack caused a sewage system failure leading to the release of more than 1 million liters of untreated sewage in Maroochy Shire [24]. In 2014, a steel mill in Germany fell victim to a cyberattack that prevented a blast furnace from shutting down, resulting in the first known massive damage to an industrial factory [25].

Inadequate security measures at any point in the process chain can enable two kinds of attacks: the theft of technical data and sabotage attacks [12]. On the one hand, sabotage attacks are a class of kinetic cyberattacks that alter 3D printed objects by introducing inconspicuous yet damaging alterations in any intermediate stage of production [12]. Researchers from Rutgers University-New Brunswick and Georgia Institute of Technology have proven that by hacking into the firmware, an alteration to the inside of a 3D-printed object can be invisible to a human observer, but can lead to the breach of the structural integrity of manufactured components [26]. Furthermore, even a change of machine parameters (the orientation of printed objects on a printer’s build plate) can impact the tensile strength of the resultant 3D objects [14]. On the other hand, the leakage of sensitive information (machine parameters) from acoustic or thermal side-channels can result in the theft of technical data or Intellectual Property (IP) [27], [28]. Later the power-consumption based side-channel was also proven effective at attacking AM systems [29]. Moreover, the confidentiality of sensitive data in AM can be compromised using low-cost sensors installed in smartphones [30]. Similarly, in bio-engineering applications such as protein and DNA synthesis, analyzing the acoustic side-channel of a DNA synthesizer can lead to breaches of sensitive IP (synthetic oligonucleotide sequences) and can potentially cause biotechnology companies to lose millions of dollars’ worth of IP [31].

Defensive measures against AM security threats include improved software checks, hashing/secure signing, and improved process monitoring of the different steps in the AM digital process chain [11], [19], [20], [32]. In the cyber domain, blockchain approaches leverage digital asset management techniques to secure 3D printing transactions, but require the printers and the automation supplier to be fully-trusted [19], [20]. In AM printers (CPSSs), various hardware components divulge information due to the observability of their actions through physical side-channels [33]. This side-channel information can be utilized to protect AM systems. Regarding improved software checks, optimizing the manufacturing process or design product parameters in computer-aided manufacturing tools can reduce the success rate of the cyber-domain confidentiality breaches as it can decrease the information leakage in physical side-channels [34]. As for secure signing and hashing, tracking, and tracing AM products using Radio-Frequency Identification (RFID) tags or by adding chemicals has been shown effective in reducing the likelihood of sabotaging AM products [35]. Furthermore, digitally signing the whole printing process using acoustic side-channel emanations can be useful in detecting the deviation of audio signatures that are triggered by malicious modifications [36]. Another collection of methods target process monitoring using physical side-channel information against AM security threats. In 2017, Bayens et al. used the acoustic emissions to detect malicious attacks to the infill pattern of a 3D print [26]. Besides, the power side channel of the stepper motors in a 3D printer also has proven useful in detecting sabotage attacks [29]. Other detection techniques have been explored as well; for example, Wu et al. showed that malicious attacks on 3D printer infills could be detected from images of the 3D print [37]. Our previous work showed that, by using a microphone, the acoustic side channel of a 3D printer could be exploited to correlate the acoustics of printer movements with G/M codes to detect malicious G/M code modifications made by compromised 3D printer firmware [21]. While it is possible to have process monitoring systems that utilize physical side-channel information against AM security threats, existing methods have only focused on the use of a single side-channel. Since various analog emissions can have different capabilities in revealing machine parameters [22], using a single modality can limit the effectiveness of a detection system. Therefore, in this paper, we propose a multi-modal attack detection system that incorporates multiple physical side-channels to defend against sabotage attacks.

III. BACKGROUND

This section introduces the fundamentals of the AM process chain from both cyber (Section III-A) and physical (Section III-B) perspectives. The manufacturing of 3D objects in AM requires a chain of cyber-physical processes that leverage a variety of software applications, data transportation methods, and transportation methods of physical items [12]. We primarily depict the chain in Figure 1 according to the Fused Deposition Model (FDM) based AM.

A. THE AM DIGITAL PROCESS CHAIN

In the cyber domain, the process chain begins with an idea of a 3D object. The first item on the workflow is to substantiate the design specifications using Computer-Aided Design (CAD) tools. Next, the generated CAD model gets converted into the STereoLithography (STL) format that uses a series of triangles to model the surface geometry. In the Computer-Aided Manufacturing (CAM) process, the slicing algorithms convert the STL files into a layer-by-layer description file to instruct the physical printer how to create the 3D object. The description file uses a Numerical Control Programming Language called G/M-code. The G-codes describe the motion and flow settings of the printer; they are responsible for determining the speed of the nozzle along each axis and the amount of material to deposit for each printing step. As an example, G1 F2100 X5 Y6 Z1.2 E2.1 represents a single line of G-code for controlling the movement of the nozzle, where G1 means...
coordinated linear motion, F defines travel feed rate (speed) which is measured in mm/min, and distance and extrusion are measured in mm. On the other hand, the M-codes control the machine settings such as temperature, coolant. Lastly, the printer’s firmware interprets each received G/M-code instruction into the corresponding control signals y that actuate the hardware components attached to the printer. In this study, we primarily focus on FDM based AM and represent its control signals as \( y = [v, a, t, d] \). Among these control signals, \( v = [v_x, v_y, v_z, v_e] \) represents the speed of the nozzle in different axes, along with the speed of extrusion, where \( v_e \in \mathbb{R} \geq 0. a = [a_x, a_y, a_z, a_{xy}, a_{xz}, a_{yz}] \) represents the axis movement such that \( a_{xy} = \{0, 1\} \), where \( a_i = 1 \) represents the presence of movement in the given axis and \( a_i = 0 \) represents the absence of movement. \( t \in \mathbb{R} \geq 0 \) represents the temperature of the nozzle. \( d = [d_x, d_y, d_z, d_e] \) represents the distance of the nozzle in different axes, along with the amount of extrusion where \( d_t \in \mathbb{R} \). These control signals (Y) are essentially cyber-domain data regarding how to construct a 3D object, and in turn, precisely instruct the nozzle movement. These control signals are then sent to the physical domain of the process chain in turn, and it is repeated for each G/M-code that the printer has been given to process.

B. THE AM SYSTEM SIDE-CHANNELS

In the physical domain, an FDM based printer manufactures the 3D physical objects using thermoplastic filament materials such as PolyLactic Acid (PLA) or Acrylonitrile Butadiene Styrene (ABS). The printer uses motors and belts to control the properly heated nozzle to melt and extrude the materials, depositing them onto the surface of the build platform at a precisely controlled rate. An array of stepper motors enables the fine-grained degree of control, each controlling movement along a single axis. However, the printer hardware also acts as a significant source of information leakage because of its analog emissions during the operation. The side-channels are the streams of information outside of the primary data path, which contains the information that is correlated with the data passing through the primary data path. In this case, the primary data path includes the control signals sent to the stepper motors inside the printer.

Treating an FDM based printer as a Cartesian robot, it can leak information from the Vibration side-channel while moving the internal hardware components during the printing. Regarding the system vibration, the natural frequency of the 3D printer can be determined from its general dynamics [38]. Besides, the stepper motors act as a major source of vibration due to the fluctuating radial force acting on the stator core of the stepper motor. Therefore, the vibration in each stepper motor is a direct result of the various machine parameters sent to the 3D printer. On the other hand, most of the acoustic signals observed from the Acoustic side-channel of a 3D printer are also a result of vibration produced during the movement of the stepper motors inside the printer. The acoustic emissions come from the power radiated from a hybrid stepper motor’s stator core and torque ripples. They can be calculated assuming that the stator core of the stepper motor is cylindrical [39]. For the Magnetic side-channel, the Ampere-Maxwell law relates magnetic fields to electric currents, meaning that the magnetic field can be calculated for any device in which there is a varying electric field. Lastly, the Power side-channel reveals the primary consumers of power in a 3D printer, such as the heating elements, stepper motors, fans, bed heater, and the internal control circuitry. Of these components, the stepper motors’ power consumption varies with their movement speeds. Techniques such as Simple Power Analysis (SPA) and Differential Power Analysis (DPA) have been demonstrated as effective non-intrusive methods of extracting information such as digital-domain encryption keys from power consumption measurements [40]. Most 3D printers have a constant DC power supply. Hence, a DC clamp can be placed to monitor the varying current flow and capture the power consumption in the 3D printer for each G/M-code. In short, due to the physical nature of the stepper motors and internal hardware components, the information about the control signals can be unintentionally leaked through the mentioned side-channels, thus being able to be inferred by analyzing the signal streams acquired from those side-channels.

IV. MULTI-MODAL SABOTAGE ATTACK DETECTION

Section III-B mentioned that the printer hardware can unintentionally leak cyber information about the control signals from various physical side-channels. Leveraging this, we propose a system that can statistically model the AM system behavior by utilizing these side-channel information streams. By continuously monitoring the side-channels, the system utilizes various machine learning models to estimate the cyber-domain information. It compares them...
As described in Figure 1, the sensitive information of a detection potential sabotage attacks.

we describe the system architecture of the sabotage attack protects the data flow in the AM digital process with the unmodified information to detect potential sabotage attacks.

A. ADVERSARY MODEL

As described in Figure 1, the sensitive information of a 3D object flows through the AM digital process chain and is converted into various intermediate forms. Each conversion step requires the assistance of different tools such as CAD software, CAM software, and even the printer firmware, presenting multiple attack surfaces for adversaries to exploit in cyberattacks. By altering the integrity of the tools or the computer used in operation, the attackers can infiltrate at any stage of the process chain to modify the intermediate forms of the 3D object. For example, the Stuxnet worm entered the Iranian nuclear plant network via a malicious USB stick inserted into a PC by a double agent [23]. In another example, the attackers in the German steel mill hack used spear-phishing emails to enter the internal facility network and trigger a shutdown of the blast furnace, causing significant damage [25]. In [13], phishing was used to gain access to a computer and maliciously modify a 3D printed object’s STL file before printing, resulting in a sabotage attack and catastrophic part failure. AM systems are vulnerable to these forms of attacks, as many of them have network connectivity and are often connected to internal networks for monitoring and control. Other potential sources of entry for a well-funded attacker include hardware Trojans: malicious modifications to the core hardware of a system done in the device’s supply chain. Many have shown that hardware Trojans can be feasibly introduced by adversaries in the supply chain and are very difficult to detect using conventional cybersecurity methods [41]. Two famous examples of hardware vulnerabilities: Meltdown and Spectre, are hardware-level exploits that allowed attackers to breach the confidentiality of user programs on PCs [42], [43]. If a hardware Trojan is inserted into an additive manufacturing system in the supply chain, it could allow attackers to perform sabotage attacks without being detected or prevented by security measures in higher layers.

Given the attack surface presented by the AM digital process chain, several common attack vectors are shown in Figure 2. Typically, the primary information stream \( u_1 \), \( u_2 \), \( u_3 \) flows from one process to another on the AM digital process chain and gets converted to corresponding control signals \( y \) to be sent to the AM machine. In each step of this process chain, the attackers \( A_1, A_2, A_3, A_4 \) can make alterations to intermediate forms of the information by adding the corresponding exogenous inputs \( e, e_1, e_2, e_3 \). We present this modified information as \( u'_1, u'_2, u'_3 \). At the end of the process chain, the modified information gets converted to the corresponding modified control signals \( y' \). The relationship between \( y \) and \( y' \) is described in Equation 1.

\[
\begin{bmatrix}
  v \\
  d
\end{bmatrix} =
\begin{bmatrix}
  a & e_v \\
  d & e_t
\end{bmatrix}
\begin{bmatrix}
  a' \\
  d'
\end{bmatrix}
\]

where the exogenous inputs can be both discrete and continuous values, \( \{ e_v, e_t \} \in \mathbb{R} \geq 0 \), and \( e_a \in \{0, 1\} \), changing the original information \( y \) to the modified one \( y' \).

Intuitively, attacks on the digital process chain will eventually result in the modification of the control signals. In FDM-based AM, a sabotage attack results in the modification of the control signals from \( y \) to \( y' \), leading to the compromise of the initial 3D object design. Cyber-security techniques can help mitigate risks further upstream in the digital process chain, such as at the CAD design and slicing steps. However, the security of cyber-physical systems themselves is often overlooked. To this end, we focus our attack detection system on detecting adversarial attacks on the printer firmware that modify the control parameters \( y \) directly, resulting in a sabotaged 3D object. As mentioned previously, AM systems often have network connectivity or physical access ports, enabling an adversary to exploit firmware vulnerabilities and compromise the system.

With this attack model in mind, we assume that the G-codes sent to the AM system have not been previously tampered with and are representative of the correct 3D object model. In this case, the movement of the AM machine’s internal components during a sabotage attack will not match the movements described by the instructions given in the G-code file, and thus, will result in different side-channel emissions. In Section III-B, we mentioned that the various analog emissions emitted during printing are highly correlated to the control signals sent to the printer hardware by the firmware. By comparing these side-channel emissions with the G-codes sent to the printer, we can infer the values of the control signals and determine if the printer firmware has been hacked.

B. SYSTEM ARCHITECTURE

Given the adversary model presented in Section IV-A, we propose a system that detects the potential sabotage attacks by continuously observing AM system side-channels \( O \) and by cross-comparing the inferred control signals \( \hat{Y} = [\hat{V}, \hat{A}, \hat{T}, \hat{D}] \) with the uncompromised ones \( Y = [V, A, T, D] \). The fundamental working principle behind our approach is that \( O \) must have high Mutual Information (MI) with \( Y \), where \( Y \) and \( O \) are random variables denoting the
control information signals and observed analog side-channel emissions. The MI of two random variables $A, B$, is defined as $I(A; B)$ that measures the quantified amount of information regarding the mutual dependence. Upon observing the analog emissions $O$, the mutual information is then defined as $I(V; O), I(A; O), I(T; O), I(D; O)) > 0$, where the random variables $O, V, T, D$ are continuous whereas $A$ is discrete.

The overall system architecture is described in Figure 3. The information that our proposed detection system acquires is assumed to be secure and free from any modification. In the training phase, our proposed system finds the estimation functions $\hat{f}_i(o(t))$ using various supervised machine learning approaches for each control signal $i$. The dataset for the training consists of the analog emission $o(t)$ from the benchmark printer along with the secure information flow in the form of control signals $y(t)$ which are parsed from the G-codes $g(t) = [g_1, g_2, \ldots, g_t]$ by the interpreter. Once the training is finished, the best estimation function $\hat{f}_i(o(t))$ will be selected to estimate control signal $i$. In the testing phase, the function $\hat{f}_i(o(t))$ infers the respective control signal $\hat{y}_i(t)$ by continuously observing the analog emissions $o(t)$ from the monitoring printer. The sabotage attack detecting algorithm takes the unmodified control signals $y$ and the estimated ones $\hat{y}$ as inputs to determine if a sabotage attack has occurred. The benefit of having the proposed system is that it can run in parallel to the AM process chain non-intrusively and can be applied to legacy AM systems at a low cost.

In the system, the choice of sensors can be any combination of current, electromagnetic, vibration, and acoustic sensors. Given the fact that sabotage attacks introduce variations $e_v, e_d, e_l, e_t$ for each control parameter, the sampling frequency and the bandwidth for sensors should be selected such that those alterations are detectable in the observed analog emissions $o(t)$. Although there are factors such as the distance and the angle of sensor placement that can affect the Signal to Noise Ratio (SNR), the calculated MI can be used to evaluate the relation between analog emissions and control signals. Based on the MI, the corresponding side-channel emissions can either be incorporated or discarded from the group of features to be used for efficiently estimating the behavior of the AM system. The observed signals from various sensors can be too large for learning the estimation functions. Therefore, it is necessary to perform feature selection on observed analog emissions to extract only the informative values from the original signals such that the processing time can be further improved. The type of features extracted is specific to the category of the observed analog emission. Principle Component Analysis (PCA) is used to reduce the dimension of the extracted features. As for the control signals, each line of G-code sent to the machine contains control signal information. Control signals $A$ and $V$ are highly correlated with printer movement at each unit of time. However, control signals $D$ and $T$ do not vary with the analog emissions of the printer at each unit of time, making it difficult to correlate side-channel information with these parameters. As a result, only kinetic cyberattacks affecting the control parameters $V$ and $A$ are considered as part of our detection system. We leverage the interpreter used in our previous work to convert these instructions into canonical machine commands. The acquired control signals are then sent to System Estimation Model for the training.

The control signals $i$ used as labels for each movement are the movement axis labels: $A = [A_x, A_y, A_z]$ (diagonal), which indicate the axis of motion, and the velocity labels: $V = [V_x, V_y]$, which indicate the speed of movement in each axis in mm/s. Each line printed by the 3D printer results in a set of observed analog emissions with a corresponding set of label values. During the training phase, the system estimation model utilizes supervised machine learning approaches to learn the estimation function $\hat{f}_i$ with $i = [A_x, A_y, A_z, V_x, V_y]$ using the secure training data-set of observed analog emissions. For each control parameter $i$, different predictive models are used to train the estimation function and to get the model parameters. For control signals, $V$ which are continuous values, regression models such as Gradient Boosting Regression, Ridge Regression, Stochastic Gradient Descent Regression (SGD), AdaBoost Regression, Bayesian Ridge Regression (BayesianRidges), Linear Support Vector Regression (LinearSVR), Decision Tree Regression (DecisionTree), Lasso Linear Regression (Lasso), Lars Lasso Linear Regression (LarsLasso), and K-Nearest Neighbor Regression (KNN) are evaluated. For control signals $A$ that have discrete values, binary or multi-class classifiers such as Linear Support Vector Machine Classification (LinearSVC), Logistic Regression, Stochastic Gradient Descent Classification, Decision Tree Classification, AdaBoost Classification, Random Forest Classification, PassiveAggressive Classification, K-Nearest Neighbors Classification, Gradient Boost Classification, and a Sequential Neural Network are then used. The training of estimation functions can be done either online or offline, as the printer could have varying analog emissions over a long period due to the tear of the mechanical structures in physical hardware. In our system, we consider offline training only in order to show a proof-of-concept example.

In the testing phase, the sabotage attack detection algorithm compares the real control signals given by the interpreter and the values calculated by the estimated functions $\hat{f}_i$. If there is a mismatch between the expected control parameters and the estimated values that exceed the defined error

![FIGURE 3. Sabotage attack detection system architecture.](image-url)
thresholds, the system flags this as a sabotage attack. The
detailed steps are described in Algorithm 1. The error var-
ation thresholds are defined in Line 1. This value is based on
the accuracy of the estimated functions $\hat{f}_i$ during the training
phase of the detection model. Lines 3 to 7 determines if the
estimated control parameters and the real control parameters
vary more than the error threshold. Lines 8-10 set the attack
detection flag to high if any of the control parameters change
more than the error variation threshold. Finally, in line 11,
the attack flag is returned.

### Algorithm 1 The Sabotage Attack Detection Algorithm

**Result:** Actual and Estimated Control Parameters $[v, a, d, t], [\hat{v}, \hat{a}, \hat{d}, \hat{t}]$

1. Define Error Thresholds $e^v_T, e^a_T, e^d_T, e^t_T$;
2. Initialize $f_v = 0, f_a = 0, f_d = 0, f_t = 0$;
3. for each $i \in \{v, a, d, t\}$ do
   4.   if $|i - \hat{i}| > e^i_T$ then
       5.     $f_i = 1$
   6. end
7. end
8. if $\sum_{i \in \{v, a, d, t\}} f_i \geq 1$ then
9.   $F_A = 1$
10. end
11. return $F_A$

## V. EXPERIMENTAL RESULTS

In this section, we present our experimental results and
detection system performance. First, we describe our experi-
mental setup (Section V-A), evaluate the mutual informa-
tion shared between the control parameters and each modal-
ity (Section V-B), and present results for axis classification
and velocity regression (Section V-C). Then, we discuss
our detection system’s performance on synthesized sabo-
tage attacks (Section V-D) as well as real-world test cases
(Section V-E). Lastly, Section V-F discusses the experimental
result, feasibility, and limitations of our proposed approach.

### A. EXPERIMENTAL SETUP

The testbed for verifying our detection system consists of
an Ultimaker 3 3D-printer, four microphones, three vibra-
tion sensors (accelerometers), three magnetic sensors (mag-
netometers), one current sensor, a Data Acquisition (DAQ)
device, two Arduino microcontroller boards coupled with
MCP4725 boards for digital-to-analog conversion (DAC),
and a personal computer for managing communication and
data acquisition. The snapshot of the system is shown in
Figure 4.

To synchronize the sensor readings with the G-codes from
the printer, we configured the printer to export the current
G-code along with the timestamp information to the computer
for each instruction it executes. Next, we match the features
extracted for the sensor values with the corresponding
G-codes using timestamps, giving us a labeled dataset.

### B. AM SYSTEM SIDE-CHANNEL LEAKAGE ANALYSIS

In contrast to the attack detection systems presented in [21],
[26], [29], our implementation leverages multiple multiple

![FIGURE 4. Experimental setup.](image-url)
to obtain a better model of the AM system. The modalities used include the acoustic, magnetic, vibration, and power side channels. To evaluate the value of each modality for prediction, we calculated the mutual information between features of each modality and label. For each modality, we selected the feature with the highest mutual information score in bits. The results are shown in Table 1.

The vibration side-channel appears to have the highest mutual information with the control parameters of the 3D printer. Additionally, the magnetic and acoustic side channels seem to have a high correlation with these parameters as well. The higher overall mutual information with $V_x$ and $V_y$ labels is likely because $V_x$ and $V_y$ are continuous labels. At the same time, $A_x$, $A_y$, and $A_{xy}$ are binary labels, meaning that a higher quantity of information can be shared between the velocity parameters and the side channel emissions.

For all labels, the current appears to have relatively low mutual information. This can potentially be attributed to the precision of the current sensor; with a more sensitive current sensor, we could differentiate between control signals with greater accuracy and increase the mutual information in this side channel. Additionally, the current sensor was placed on the common power source for all three motors; if we set one current sensor on each stepper motor’s power line separately, we would likely improve this channel’s mutual information significantly. However, implementing this non-intrusively may not be possible on most printers.

Overall, our results show that the 3D printer leaks side-channel information to all of these modalities. Therefore, intuitively, we can improve performance significantly over uni-modal techniques by leveraging a multi-modal approach. To empirically prove this claim, we evaluate the axis classification performance of each modality in comparison to a multi-modal approach.

### C. AM SYSTEM STATE ESTIMATION

Since our axis tracking is implemented as an array of binary labels (one for each axis: $A_x$, $A_y$, $A_{xy}$), we train binary classifiers for each label to correlate the side channel feature information with the label value.

The performance of our classifiers at varying decision boundaries in terms of TPR and FPR is shown in Figure 5. The figure indicates that all classifiers achieve a very high TPR and very low FPR for $A_{xy}$. This is likely because of the movement of two stepper motors instead of one results in more acoustic, magnetic, vibration, and current emissions than single-axis movements. For $A_x$ and $A_y$, it can be seen that GradientBoost consistently outperforms the other classifiers. However, all classifiers seem to show relatively good performance. The performance of the top classifiers for each label is shown in Table 2 in terms of Accuracy, TPR, FPR, and F1 Score.

![Figure 5](image-url) Receiver operating characteristics for axis classification.

![Table 1](table-url) Mutual information between control parameters and modalities.

| Parameter | Acoustic | Magnetic | Vibration | Power |
|-----------|----------|----------|-----------|-------|
| $A_x$     | 0.2179   | 0.1064   | 0.2250    | 0.1062|
| $A_y$     | 0.2615   | 0.1234   | 0.3027    | 0.1252|
| $A_{xy}$  | 0.1461   | 0.0808   | 0.1757    | 0.0658|
| $V_x$     | 0.3458   | 0.4370   | 0.5674    | 0.1237|
| $V_y$     | 0.3665   | 0.3420   | 0.4400    | 0.1514|

![Table 2](table-url) Classification performance.

| Axis    | Classifier  | Accuracy | TPR   | FPR   | F1   |
|---------|-------------|----------|-------|-------|------|
| $A_x$   | GradientBoost | 96.75%   | 0.9149| 0.0164| 0.9295|
| $A_y$   | RandomForest | 94.98%   | 0.8425| 0.0174| 0.8871|
| $A_{xy}$| NeuralNetwork| 94.20%   | 0.9374| 0.0565| 0.8832|
| $A_x$   | GradientBoost | 96.86%   | 0.9282| 0.0194| 0.9314|
| $A_y$   | RandomForest | 95.05%   | 0.8842| 0.0298| 0.8914|
| $A_{xy}$| NeuralNetwork| 93.81%   | 0.9517| 0.0660| 0.8761|
| $A_x$   | GradientBoost | 98.43%   | 0.9952| 0.0280| 0.9854|
| $A_y$   | RandomForest | 98.51%   | 0.9976| 0.0292| 0.9861|
| $A_{xy}$| NeuralNetwork| 98.26%   | 0.9938| 0.0300| 0.9838|
we achieve an overall classification accuracy of 97.66%. Although Gradient Boost, Random Forest, and the Neural Network all use different approaches to build models for classification, all three models display excellent performance in all classification tasks. Gradient Boost and Random Forest outperform the Neural Network in terms of accuracy, given a decision threshold of 0.5.

To evaluate our multi-modal approach in comparison to uni-modal methods, we assessed the axis prediction performance of our classifiers on subsets of features specific to each modality. We separated the features based on the type of sensor (microphone, accelerometer, magnetometer, current sensor) and performed training and testing of all of our classifiers. The results of the highest accuracy classifiers in each modality in comparison to our multi-modal approach and the approach presented in [21] are shown in Figure 6. Besides, we show the difference in accuracy between our multi-modal method and these other techniques. Since [21] used a single microphone to record data, we compare against this method by selecting only the features from a single microphone for performing training and testing. As shown in Figure 6, our multi-modal technique outperforms the uni-modal methods as well as the technique from [21]. Notably, the acoustic and vibration modalities show the highest uni-modal accuracy and reach within 5% of the accuracy of the multi-modal technique. This aligns with the results shown in Table 1, where the acoustic and vibration modalities had the highest mutual information shared with the control parameters. Since [21] only uses a single sensor as input, it does not perform as well as a multi-sensor acoustic or vibration modality approach. Overall, these results demonstrate that our multi-modal technique results in performance improvement over uni-modal methods.

Intuitively, as motor speed changes, so do the leaked acoustic, magnetic, vibration, and power side-channel information. Leveraging this correlation, we use regression algorithms to estimate the axis movement speeds in the X and Y axis using extracted side-channel features. We collected velocity values from normal 3D printing operations, resulting in a wide range of velocity values for each axis, as shown in Figure 7. Figure 7 shows that the velocity values for $V_x$ and $V_y$ ranged from $\pm 250$ mm/s, with the majority of values between $\pm 25$ mm/s. Although this method of data collection leads to an uneven distribution of velocity values, it preserves the distribution of velocity values in real printing tasks, making our system more effective in real-world scenarios. We used scikit-learn’s StandardScaler to normalize the velocity values before scoring regression. Tables 3 and 4 show the overall performance of our regressors in terms of MSE, MAE, and MedianAE.

### Table 3. Regression performance for X-axis velocity.

| Regressor   | MSE   | MAE   | MedianAE |
|-------------|-------|-------|----------|
| GradientBoost | 0.6877 | 0.3829 | 0.0828   |
| LarsLasso   | 0.8517 | 0.4995 | 0.1803   |
| BayesianRidges | 0.9043 | 0.5286 | 0.2643   |
| Lasso       | 0.9087 | 0.4615 | 0.0107   |
| DecisionTree | 1.4879 | 0.4617 | 0.0106   |
| LinearSVR   | 2.3166 | 0.5459 | 0.2805   |

Despite the range of velocity values ($\pm 250$ mm/s), in both $V_x$ and $V_y$, we can predict axis velocity with relatively low MAE and MSE. The regression model with the smallest
TABLE 4. Regression performance for Y-axis velocity.

| Regressor     | MSE   | MAE   | MedianAE |
|--------------|-------|-------|----------|
| GradientBoost| 0.6137| 0.3793| 0.0652   |
| Lasso        | 0.8285| 0.5497| 0.2824   |
| Lasso        | 0.9672| 0.5135| 0.0151   |
| Ridge        | 1.0704| 0.5867| 0.3714   |
| DecisionTree | 1.2185| 0.5435| 0.0055   |
| LinearSVR    | 1.3466| 0.5439| 0.2813   |

TABLE 5. Axis attack detection performance.

| Parameter | Accuracy | TPR | FPR | F1 | AUC |
|-----------|----------|-----|-----|----|-----|
| A_x       | 99.43%   | 0.9945| 0.0064| 0.9962| 0.9941|
| A_y       | 99.38%   | 0.9925| 0.0049| 0.9937| 0.9938|
| A_xy      | 98.69%   | 0.9827| 0.0089| 0.9868| 0.9869|

TABLE 6. Velocity attack detection performance with a detection threshold of ±25 mm/s.

| Parameter | ∆V (mm/s) | Accuracy | TPR | FPR | F1 | AUC |
|-----------|-----------|----------|-----|-----|----|-----|
| V_x       | 25        | 39.03%   | 0.2174| 0.0544| 0.3522| 0.5815|
| V_y       | 31.25     | 89.86%   | 0.8839| 0.0544| 0.9300| 0.9147|
| V_z       | 37.5      | 98.24%   | 0.9938| 0.0544| 0.9885| 0.9697|
| V_x       | 25        | 86.68%   | 0.6471| 0.0506| 0.7262| 0.7982|
| V_y       | 31.25     | 94.36%   | 0.9283| 0.0506| 0.8999| 0.9388|
| V_z       | 37.5      | 95.03%   | 0.9527| 0.0506| 0.9127| 0.9510|

overall error is the Gradient Boosting Regressor. Therefore, it was selected as the primary model for velocity estimation.

D. MULTI-MODAL SABOTAGE ATTACK DETECTION

To evaluate our attack detection system, we generate synthetic attacks by procedurally adding adversarial modifications to G-code files. Then, we pass the unmodified sensor data and the modified G-code files as inputs to our attack detection system to evaluate its ability to detect mismatches between the sensor data and the modified G-codes.

For axis labels, these modifications took the form of changing the binary label value from 0 to 1 or 1 to 0. For velocity labels, different degrees of modifications were implemented and tested, ranging from ±37.5mm/s from the original velocity value. Since the range of velocity values is ±250mm/s, ±37.5mm/s was selected as the primary model for velocity estimation.

We tested our detection algorithm for each control parameter separately at various error threshold levels to determine the optimal error threshold values. We selected an error threshold of 25mm/s, as this provided the best trade-off of detection accuracy and precision. This threshold represents a deviation of 10% from the original velocity value. We then evaluated our algorithms attack detection performance at various modification degrees (\(\Delta V\)) on a row-by-row basis. The results are shown in Tables 5 and 6.

Our overall row-level accuracy is 99.17% for axis labels. For velocity labels with modifications of more than 37.5mm/s and a detection threshold of 25mm/s, our average accuracy is 96.64%. Based on these results, our overall attack detection accuracy for all control parameters is 98.15%. Although these attacks are synthetic, they provide empirical benchmarks to demonstrate the attack detection system’s capabilities. To validate these results in a real scenario, we tested two real-world test cases of sabotage attacks.

E. REAL-WORLD EXAMPLES

We tested our detection system on two different types of load-bearing test objects: a gear and a wrench. Since gears and wrenches are generally placed in high-stress scenarios, it is plausible that a kinetic cyberattack could compromise their structural integrity and significantly increase the chance of equipment failure. Moreover, these parts serve as analogs to other load-bearing 3D printed parts to demonstrate that our detection system can identify kinetic cyberattacks on these types of components.

As described in Section IV-A, an adversary can inject malicious defects into the print by hacking the 3D printer firmware directly and manipulating the control signals sent to the printer hardware. In this attack model, legitimate G-codes will be sent to the printer; however, the control signals sent to the printer hardware will be manipulated by the adversary, resulting in alterations to the printed object. To replicate this attack model, we give our detection system the G-codes corresponding to the correct, legitimate print and the side channel data for the maliciously modified print. Then, the detection system predicts the axis and velocity labels based on the side channel data, compares it with the G-codes it is given, and determines if an attacker has modified the printed part.

To implement the adversarial attack, we added several small fractures, 4mm in length, to the 3D design of both parts using the computer-aided design tool SketchUp. These fractures were added by inserting segments and removing material in the wrench at the ends of the shaft, where stress is likely to be concentrated during regular use. In the gear, the fractures were added to two of the gear teeth at the area where the teeth attach to the center of the gear. Under normal loads, these fractures serve as points of weakness, significantly reducing the effective strength of the part and leading to permanent part failure.

The original and attacked wrenches are shown in Figure 8 and the adversarial modifications to the gear are shown in Figure 9. Although these specific modifications are visible to the human eye in the final print, this was done primarily for demonstrative purposes. These modifications can easily be concealed in internal layers of the print without modifying the outward appearance of the object, enabling it to pass visual quality inspections done by both machines and employees. This form of attack was demonstrated in [13]. Furthermore, these minute modifications can be done in ways that enable the printed part to pass stress tests while still reducing its yield strength. Load-bearing parts are generally manufactured with enough strength to withstand loads higher than the maximum expected load of their application, and...
stress testing is often performed with forces at or below this load. As a result, an attacked part could potentially pass these stress tests while still reducing the total yield strength of the part, leading to reduced part lifetime or random failures at maximum expected load.

As shown in Figure 10, the adversarial modifications introduced do not just alter existing segments but add additional segments to the print. In addition to compromising the structural integrity of the printed object, this can result in increased print time and material usage. Since we use timestamps to match G-codes with the corresponding sensor data and adversarially modified prints increase print time, even small adversarial modifications will propagate over time and cause mismatches between sensor readings and G-codes. This allows us to detect even minute adversarial modifications.

We evaluated our detection system on the real-world test cases by identifying how many segments were changed compared to the original print and how many segment mismatches were detected. The results are shown in Table 7.

For both test cases, the detection system was able to detect the attack. In both attack scenarios, the number of mismatches is higher than the number of modified segments because of the propagation of mismatched segments over time, as mentioned previously. These tests demonstrate that our methodology can be applied to real-world, practical AM tasks.

F. DISCUSSION

Overall, the results show that our methodology performs well in multiple scenarios and outperforms uni-modal approaches using the same dataset. Additionally, we found that the vibration modality has the most mutual information with the control parameters in this dataset. From our tests, we found that GradientBoost classification and regression had the highest overall accuracy. Finally, we demonstrated our attack detection system on two real-world test cases of sabotage attacks successfully.

1) LIMITATIONS

Our detection system is an improvement over previous uni-modal detection strategies. However, further work is needed in certain areas, such as detecting attacks on non-linear print movements. Components that are printed with a large number of curved surfaces are challenging to model with our system because curves are implemented as a series of very short segments. Since we correlate sensor data with each segment, it is difficult to align sensor readings with these small segments perfectly. Additional work will be needed to identify ways to address this limitation.

Furthermore, since we perform detection for each control parameter separately, our methodology is potentially susceptible to tiny adversarial modifications on multiple parameters. By implementing a detection strategy that incorporates various parameters for each detection, we can potentially improve our algorithm’s performance. We also leave this task for future work.

Another limitation of our work was the fact that we only tested our detection system on one model of 3D printer. Although printer specifications differ, and the use of different
motors and configurations can lead to different side-channel emissions, the physical properties of the motors remain the same. Multiple related works have demonstrated the ability to correlate side-channel emissions with digital domain information on various AM systems [21], [26], [28], [29], [36], [45], [46]. Since our system only requires sensor data and G-codes to model the system, it can generalize to any AM system that similarly uses stepper motors.

2) FEASIBILITY
One important consideration is the practicality of implementing this attack detection framework as a real-world production system. Since our hardware consists entirely of low-cost sensors and microcontrollers commonly found in IoT devices, it is feasible for a company producing safety-critical components to implement this detection system in their AM pipeline. One aspect which we have not explored in this work is the implementation of the detection system as a real-time or near the real-time system. However, in the same way that production lines randomly select from batches to ensure product quality, a company could use our system to randomly select and inspect one print in each production batch to determine if their AM security has been breached; if an attack is detected, the batch can be discarded. This reduces the overall computational power required to perform detection and compensates for data processing latency.

3) COMPARISONS TO EXISTING WORK
Our work is not the first to propose a sabotage attack detection system for AM systems; several uni-modal strategies have been proposed. However, to the best of our knowledge, our work is the first to suggest a multi-modal sabotage attack detection system. Here, we compare our technique and results with existing works. For example, [21] used a single microphone capturing the acoustic side-channel only; we replicated this technique by using a single microphone channel from our dataset and achieved an accuracy of 91.07% for axis prediction. In comparison, our multi-modal technique achieved an accuracy of 99.17% at axis prediction. The multi-step detection method described in [26] and the image-based attack detection method described in [37] both demonstrate high accuracy at malicious infill modification detection. These approaches could be used in conjunction with our approach in future work for improved overall performance. Moore et al. showed considerably high accuracy using power side-channel analysis [29]. In their work, probes were placed near each stepper motor in the printer, allowing for accurate differentiation between motors and motor speeds. If we implement a similar current sensing capability to our system, we will likely see a significant increase in mutual information with the power side channel.

VI. CONCLUSION
AM systems are core to the future of manufacturing and Industry 4.0. Since these systems are advancing in terms of complexity and connectivity as well as producing parts for increasingly critical and taxing applications, the security of these systems is a major concern. Since AM systems are cyber-physical systems, they present a broad and diverse attack surface, making attack detection and prevention a daunting task. Our proposed sabotage attack detection system has demonstrated the ability to detect various attacks by correlating multiple forms of physical-domain emissions of the AM system with cyber-domain information. We have achieved an overall detection accuracy of 98.15% on synthetic benchmarks and demonstrated that our system could detect two real-world scenarios of sabotage attacks. Although our solution addresses a significant security risk in AM systems, more work is needed to address the broad scope of potential AM vulnerabilities.

REFERENCES
[1] S. Mueller, S. Im, S. Gurievich, A. Teibrich, L. Pfisterer, F. Guimbretière, and P. Baudisch, "WirePrint: 3D printed previews for fast prototyping," in Proc. 27th Annu. ACM Symp. User Interface Softw. Technol., 2014, pp. 273–280.
[2] R. Smith. (Jun. 2015). 7 ways 3D Printing is Already Disrupting Global Manufacturing. Forbes Magazine. Accessed: Dec. 5, 2019. [Online]. Available: https://www.forbes.com/sites/ricksmith/2015/06/29/7-ways-3d-printing-is-already-disrupting-global-manufacturing
[3] B. Krassenstein. (May 2015). New Airbus A350 XWB Aircraft Contains 1,800 3D Printed Parts. 3DPrint.com. Accessed: Dec. 5, 2019. [Online]. Available: https://3dprint.com/63169/airbus-a350-xwb-3d-print
[4] (Nov. 2017). How 3D Printing Will Change Manufacturing. GE Reports. Accessed: Dec. 5, 2019. [Online]. Available: https://www.ge.com/reports/epiphany-disruption-ge-additive-chief-explo-n3d-printing-will-upend-manufacturing
[5] (Oct. 2019). New Manufacturing Milestone: 30, 000 Additive Fuel Nozzles. GE Additive. Accessed: Dec. 5, 2019. [Online]. Available: https://www.ge.com/additive/blog/new-manufacturing-milestone-30000-additive-fuel-nozzles
[6] (Sep. 2019). Medical Applications of 3D Printing. U.S. Food and Drug Administration. Accessed: Dec. 5, 2019. [Online]. Available: https://www.fda.gov/medical-devices/3d-printing-medical-devices/medical-applications-3d-printing
[7] F. Marga, K. Jakab, C. Khatiwala, B. Shepherd, S. Dorfman, B. Hubbard, S. Colbert, and F. Gabor, "Toward engineering functional organ modules by additive manufacturing," Biofabrication, vol. 4, no. 2, Jun. 2012. Art. no. 022001.
[8] M. Rüßmann, M. Lorenz, P. Gerbert, M. Waldner, J. Justus, P. Engel, and M. Harnisch, "Industry 4.0: The future of productivity and growth in manufacturing industries," Boston Consulting Group, vol. 9, no. 1, pp. 54–89, 2015.
[9] (Mar. 2018). Printing the Future: What Additive Manufacturing Means for Innovation. GE Reports. Accessed: Dec. 5, 2019. [Online]. Available: https://www.ge.com/reports/printingthefuture/
[10] L. Columbus. (May 2019). The State of 3D Printing, 2019. Forbes Magazine. Accessed: Dec. 5, 2019. [Online]. Available: https://www.forbes.com/sites/louiscolumbus/2019/05/27/the-state-of-3d-printing-2019
[11] L. Sturm, C. Williams, J. Camelo, J. White, and R. Parker, “Cyber-physical vulnerabilities in additive manufacturing systems,” Context, vol. 7, no. 7, p. 8, 2014.
[12] 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.
[13] S. Belikovetsky, M. Yampolskiy, J. Toh, J. Gatlin, and Y. Elovici, “drf0wned—Cyber-physical attack with additive manufacturing,” in Proc. 11th USENIX Workshop Offensive Technol., 2017, p. 1.
[14] S. E. Zeltmann, N. Gupta, N. G. Tsotsos, M. Maniatakos, J. Rajendran, and R. Karri, “Manufacturing and security challenges in 3D printing,” JOM, vol. 68, no. 7, pp. 1872–1881, Jul. 2016.
[15] S. R. Chhetri, N. Rashid, S. Faizi, and M. A. A. Faruque, “Security trends and advances in manufacturing systems in the era of industry 4.0,” in Proc. IEEE/ACM Int. Conf. Comput.-Aided Design (ICCAD), Nov. 2017, pp. 1039–1046.

[16] M. Wu and Y. B. Moon, “Taxonomy for secure cybermanufacturing systems,” in Proc. ASME Int. Mech. Eng. Congr. Expo., 2018, Art. no. V002T02A067.

[17] S. D. Applegate, “The dawn of kinetic cyber,” in Proc. 5th Int. Conf. Cyber Conflict, Jun. 2013, pp. 1–15.

[18] H. Turner, J. White, J. A. Camelio, C. Williams, B. Amos, and R. Parker, “Bad Parts: Are Our Manufacturing Systems at Risk of Silent Cyberattacks?” IEEE Secur. Privac., vol. 13, no. 3, pp. 40–47, May 2015.

[19] M. Holland, J. Stjepanidic, and C. Nigischer, “Intellectual property protection of 3D print supply chain with blockchain technology,” in Proc. IEEE Int. Conf. Eng., Technol. Innov. (ICE/ITMC), Jun. 2018, pp. 1–8.

[20] M. Holland, C. Nigischer, J. Stjepanidic, and C. Chen, “Copyright protection in additive manufacturing with blockchain approach,” Transdisciplinary Eng., A Paradigm Shift, vol. 5, pp. 914–921, Jul. 2017.

[21] S. R. Chhetri, A. Canedo, and M. A. A. Faruque, “KCAD: Kinetic cyber-attack detection method for cyber-physical additive manufacturing systems,” in Proc. IEEE/ACM 35th Int. Conf. Comput.-Aided Design (ICCAD), Nov. 2016, p. 74.

[22] S. Rogika Chhetri and M. A. Al Faruque, “Side channels of cyber-physical systems: Case study in additive manufacturing,” IEEE Des. Test., vol. 34, no. 4, pp. 18–25, Aug. 2017.

[23] N. Falliere, L. O. Murchu, and E. Chien, “W32 stuxnet dossier,” White Paper, Symantec Corp., Secur. Response, vol. 5, no. 6, p. 29, 2011.

[24] J. Slay and M. Miller, “Lessons learned from the maroochy water breach,” in Proc. 12th Int. Conf. Crit. Infrastruct. Protection, Spring Arbor, MI, USA, Jun. 2013, pp. 73–82.

[25] R. M. Lee, M. J. Assante, and T. Conway, “German steel null cyber attack,” Ind. Control Syst., vol. 30, p. 62, Dec. 2014.

[26] C. Bayens, T. Le, L. Garcia, R. Beyah, M. Javanmard, and S. Zonouz, “See no evil, hear no evil, feel no evil, print no evil? Malicious fill patterns detection in additive manufacturing,” in Proc. 26th USENIX Secur. Symp., 2017, pp. 1181–1198.

[27] M. A. Al Faruque, S. R. Chhetri, A. Canedo, and J. Wan, “Acoustic side-channel attacks on additive manufacturing systems,” in Proc. ACM/IEEE 7th Int. Conf. Cyber-Phys. Syst. (ICCPS), Apr. 2016, p. 19.

[28] M. A. Al Faruque, S. R. Chhetri, A. Canedo, and J. Wan, “Forensics of thermal side-channel in additive manufacturing systems,” Ph.D. dissertation, Univ. California, Irvine, CA, USA, 2016.

[29] S. B. Moore, J. Gatlin, S. Belikovetsky, M. Yampolskiy, W. E. King, and Y. Elovici, “Power consumption-based detection of sabotage attacks in additive manufacturing,” 2017, arXiv:1709.01822. [Online]. Available: https://arxiv.org/abs/1709.01822

[30] C. Song, F. Lin, Z. Ba, K. Ren, C. Zhou, and W. Xu, “My smartphone knows what you print: Exploring smartphone-based side-channel attacks against 3D printers,” in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., 2016, pp. 895–907.

[31] S. Faizi, S. R. Chhetri, A. V. Malawade, J. C. Chaput, W. H. Grover, P. Brisk, and M. A. Al Faruque, “Oligo-Snoop: A non-invasive side channel attack against DNA synthesis machines,” in Proc. NDSS, 2019, pp. 1–15.

[32] M. Wu and Y. B. Moon, “Intrusion detection system for cyber-manufacturing system,” J. Manuf. Sci. Eng., vol. 141, no. 3, 2019, Art. no. 031007.

[33] R. Akella, H. Tang, and B. M. McMillin, “Analysis of information flow security in cyber-physical systems,” Int. J. Crit. Infrastructure Protection, vol. 3, nos. 3–4, pp. 157–173, 2010.

[34] S. R. Chhetri, S. Faizi, and M. A. Al Faruque, “Information leakage-aware computer-aided cyber-physical manufacturing,” IEEE Trans. Inf. Forensics Security, vol. 13, no. 9, pp. 2333–2348, Sep. 2018.

[35] S. Flank, G. E. Ritchie, and R. Maksimovic, “Anticounterfeiting options for three-dimensional printing,” 3D Printing Additive Manuf., vol. 2, no. 4, pp. 180–189, Dec. 2015.

[36] S. Belikovetsky, Y. Solewicz, M. Yampolskiy, J. Toh, and Y. Elovici, “Detecting cyber-physical attacks in additive manufacturing using digital audio signing,” 2017, arXiv:1705.06454. [Online]. Available: https://arxiv.org/abs/1705.06454

[37] 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 Proc. ASME Int. Mech. Eng. Congr. Expo., 2016, Art. no. V014T07A004.
MOHAMMAD ABDULLAH AL FARUQUE
(Senior Member, IEEE) received the B.Sc. degree in computer science and engineering (CSE) from the Bangladesh University of Engineering and Technology (BUET), in 2002, the M.Sc. degree in computer science from Aachen Technical University, in 2004, and the Ph.D. degree in computer science and the Karlsruhe Institute of Technology, Germany, in 2009.

He is currently with the University of California Irvine (UCI), where he is also an Associate Professor (with tenure) and directing the Cyber-Physical Systems Laboratory. Besides more than 100 IEEE/ACM publications in the premier journals and conferences, he holds eight U.S. patents. His current research is focused on the system-level design of the Internet-of-Things (IoT), embedded systems, and Cyber-Physical-Systems (CPS) with special interests on design automation methodologies, data-driven modeling techniques, including machine learning for design and CPS security. His work involves novel hardware and software design for various CPS application areas, including Industry 4.0 (manufacturing), smart-grid, and autonomous vehicles.

He was a recipient of the School of Engineering Mid-Career Faculty Award for Research 2019, the IEEE Technical Committee on Cyber-Physical Systems Early-Career Award 2018, and the IEEE CEDA Ernest S. Kuh Early Career Award 2016. He was also a recipient of the UCI Academic Senate Distinguished Early-Career Faculty Award for Research 2017 and the School of Engineering Early-Career Faculty Award for Research 2017. He has served as the Emulex Career Development Chair, from October 2012 to July 2015. Before, he was with Siemens Corporate Research and Technology, Princeton, NJ, USA. He also received the Thomas A. Edison Patent Award 2016 from the Edison foundation, the 2016 DATE Best Paper Award, the 2015 DAC Best Paper Award, the 2009 IEEE/ACM William J. McCalla ICCAD Best Paper Award, the 2016 NDSS Distinguished Poster Award, the 2008 HiPEAC Paper Award, the 2015 Hellman Fellow Award, the 2015 Kane Kim Fellowship Award, the 2017 DAC Best Paper Award Nomination, the 2012 DATE Best IP Award Nomination, the 2005 DAC Best Paper Award Nomination, the EECS Professor of the year 2015–16 Award, and the 2015 UCI Chancellor’s Award for Excellence in Fostering Undergraduate Research.

* * *

VOLUME 8, 2020