UNIVERSITY OF CALIFORNIA,
IRVINE

Data-Driven Modeling for Minimizing the Side-Channel Information Leakage in Additive Manufacturing

DISSERTATION

submitted in partial satisfaction of the requirements
for the degree of

MASTER OF SCIENCE

in Computer Engineering

by

Sina Faezi

Dissertation Committee:
Associate Professor Mohammad Al Faruque , Chair
Professor Nader Bagherzadeh
Assistant Professor Aparna Chandramowlishwaran

2017

DEDICATION

To my parents for giving me all the love and support in the world that I needed.
To Sami, my awesome little brother.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGMENTS

I would like to express my sincere gratitude to my advisor and committee chair, Professor Mohammad Al Faruque, for his consistent support and valuable insights through out this project. Without his guidance, I would not have been able to complete this thesis today.

I would also like to thank my committee members, Professor Nader Bagherzadeh and Professor Aparna Chandramowlishwaran, for assigning their valuable time to review my work, and for all the lessons that I learned in their courses which directly and indirectly helped me in my research.

I like to thank my colleagues in Advanced Integrated Cyber-Physical Systems (AICPS) laboratory, in particular Sujit Rokka Chhetri, senior PhD student, for all the research related discussions that we had. It was truly the greatest environment that I could have imagined for research.

I thank IEEE for giving me the permission to use the content of our original paper [6] published in *2017 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. The text of this thesis is a reprint of the material as it appears in *DATE'17*. The co-authors listed in this publication directed and supervised the research which forms the basis for this thesis.

Finally, I would like to thank UCI's Department of Electrical Engineering and Computer Science, for giving me the initial fellowship funding which enabled me to thrive in this wonderful path. I would also like to thank NSF for partially funding my work under CPS grant CNS-1546993.

ABSTRACT OF THE DISSERTATION

Data-Driven Modeling for Minimizing the Side-Channel Information Leakage in Additive Manufacturing

By

Sina Faezi

Master of Science in Computer Engineering

University of California, Irvine, 2017

Associate Professor Mohammad Al Faruque , Chair

Cyber-physical additive manufacturing systems consists of tight integration of cyber and physical domains. This results in new cross-domain vulnerabilities that poses unique security challenges. One of the challenges is preventing confidentiality breach due to physical-to-cyber domain attacks, where attackers can use physical analog emissions to steal the cyber-domain information. This information theft is based on the idea that an attacker can accurately estimate the relation between the analog emissions (acoustics, power, electromagnetic emissions, etc.,) and the cyber-domain data (such as G-code). To obstruct this estimation process, it is crucial to generate computer aided manufacturing tools, such as slicing and tool-path generation algorithms, that are aware of these information leakage. In this thesis, we present a novel methodology that uses mutual information as a metric to quantize the information leakage from the side-channels, and demonstrates how various design variables (such as object orientation, nozzle velocity, etc.,) can be used in an optimization algorithm to minimize the information leakage. Our methodology integrates this leakage aware algorithms to the state-of-the-art slicing tools and achieves 24.76% average drop in the information leakage through acoustic side-channel. To the best of our knowledge, this is the first work that demonstrates the idea of generating information leakage aware computer aided manufacturing tools for protecting the confidentiality of the manufacturing system.

Chapter 1

Introduction

The fundamental enabler of the fourth industrial revolution (Industry 4.0) are the Cyber-Physical Systems (CPS) [20]. These systems will lay the foundation for the creation of the Industrial Internet of Things, which is predicted to have value of $15 trillion global GDP by 2030 [8], and have improvement in production by as much as 30% [8]. However, with the incorporation of CPS in manufacturing, its inherent security issues will also pose severe challenges to the industrial revolution. In fact, attackers have already leveraged various vulnerabilities [26] of the CPS to target the manufacturing industry, making it the second most-attacked industry in 2015 [2]. Hence, these cyber-physical manufacturing systems will have to meet the security requirements such as *confidentiality*, *integrity*, and *availability* amid the new threats.

In manufacturing, *confidentiality* breach can cause loss of Intellectual Property (IP) worth large amount to a company. To highlight this issue, in this thesis, cyber-physical Additive Manufacturing (AM) systems are analyzed for understanding cross-domain attacks that result in the confidentiality breach. AM has been considered as one of the proponents of Industry 4.0 [19]. Various companies, and agencies are using it to produce *complex*, *light-*

weight, and *free-form* 3D objects on demand [13]. The major contribution of AM towards the next industrial revolution will be customized and decentralized production, which will drastically reduce the transport distance, stock in hand, and raw materials used. However, this promising technology has caveats associated with it when it comes to the *confidentiality* of the system. It has been estimated that with the proliferation of AM in manufacturing industries, IP worth $100 billion will be lost globally by the year 2018 [15].

1.1 Related Works

In order to tackle inevitable security issue of *confidentiality* breach in cyber-physical AM, researchers have focused on various security solutions.[27] have provided a new outsourcing model, described the requirements for secured outsourcing, and also proposed various future works for achieving these requirements. Some of the solutions involved are encryption and decryption of the cyber-data being sent to the manufacturer, *watermarking* of the 3D object and the manufacturing process, etc. *Watermarking* has been extensively studied for 3D printing, whereby unique keys are covertly embedded in the 3D objects. [14] have presented a method of encoding a unique key in the geometrical structure of the 3D object by altering the vertices. In [21], researchers have used the geometry of the object to encode the unique key into an object. Even companies have developed technologies to authenticate the 3D object, either by using infinitesimal natural surface faults of the 3D object, or by depositing nano particles on the object's surface [12].

In summary, most of the research work is focused on protecting the IP of the product after it has been built. However, there is presence of persistent threat to the *confidentiality* of the system during the manufacturing process as well [15]. Maintaining *confidentiality* during the manufacturing process might be more crucial due to the fact that these AM systems are extensively used for rapid-prototyping, and information leaked during this stage can cause the company to permanently lose its IP [5]. In addition, researchers have recently shown that emissions from a AM system such as 3D printers reveal the various design parameters of the 3D objects [4, 23, 11, 7].Therefore, it is imperative to analyze various analog emissions from different side-channels (such as acoustics, power, electromagnetic, etc.), and protect the system from physical-to-cyber-domain attacks during the manufacturing process.

1.2 Motivation for Leakage Aware Security Solution

It has been well established that in CPS, various physical components divulge the information due to the observability of their physical actions [3]. Moreover, these physical actions have the tendency to unintentionally leak information about the cyber-domain from the side-channels. Side-channels have been previously used in cryptanalysis to determine the secret key by utilizing the analog emissions leaked from the physical implementation of a cryptosystem rather than using the brute force or theoretical weakness of the algorithms [25]. The digital process chain of additive manufacturing consists of Computer Aided Design (CAD) tools for modeling 3D objects, and Computer Aided Manufacturing (CAM) tools for converting 3D models to slices of 2D polygons [16], and then generating tool-path (G/M-codes) based on those 2D polygons [17]. These G/M-codes (cyber-data) are eventually converted to control signals that actuate the physical components. During actuation, mechanical and electrical energies flows through the system, and may leak the information about the G/M-codes(cyber-data). In order to avoid these leakages, one may simply employ physical-domain security solutions such as putting the 3D printer inside a secured box. Although those solutions may look effective, they are only practical if the other physical properties of the 3D printer is not changed and the additional cost is moderate. However, if we can provide a feedback to the cyber-domain about the presence of leakages, we can incorporate optimization algorithms in the CAM software to minimize such leakages in advance.

1.3 Problem and Research Challenges

Designing a methodology to minimize information leakage in the physical domain through incorporation of security aware solutions in the cyber-domain of the cyber-physical additive manufacturing system poses the following key challenges:

1. Understanding physical (*mechanical* and *electrical*) models of the system to understand and quantify the information leakage.
2. Determining design variables in cyber-domain that can be optimized to minimize the information leakage.
3. Formulating an optimization problem that can be placed in the digital process chain, which can be generalized for all side-channels, and can balance the trade-off between the design variables and the associated costs (*leakage amount*, *printing time*, *power consumption*, etc.).

1.4 Our Novel Contributions

To address the above mentioned challenges, we propose a novel methodology capable of generating information leakage aware secured cyber-physical additive manufacturing tools that employs:

1. **Leakage Modeling of the Additive Manufacturing System**, which incorporates physics-based leakage model (**Section 2.1**) to understand the mechanical and electrical source of information leakage, estimates data-driven leakage model (**Section 2.2**) to ease the leakage modeling, and performs information quantification using *mutual information.*

2. **Formulation of an Optimization Problem**, (**Section 3**) that describes various design variables (orientation θ and travel feed-rate v) to optimize, and provides it as an input to the slicing algorithm and the tool-path generation algorithm in the digital process chain.

Chapter 2

System Modeling

The methodology proposed for security aware computer aided manufacturing tool is general, however, the solution provided by the optimization problem depends on the leakage model, and is machine specific. This is due to the fact that the side-channel leakage rely on physical implementation of the system, and there are various types of cyber-physical manufacturing machines [13]. In our methodology, we first start with the physics-based leakage modeling of the system, to understand the relation between the G/M-code and the analog emissions introduced in the side-channel. This understanding will allow us in determining the design variables to optimize for the specific side-channel. The leakage model is then used to quantify the information leakage, and provide it as a feedback to the optimization algorithm. However, physics-based models become complicated for complex manufacturing systems. Hence, we also perform data-driven leakage modeling to efficiently estimate the leakage model. In this paper, we use our methodology in Fused-Deposition Modeling (FDM) based additive manufacturing systems also known as 3D printers, consider acoustic side-channel to determine the design variables for the optimization problem, and demonstrate the efficiency of optimization algorithm in reducing the mutual information, and hence the information leakage from the acoustic side-channel.

2.1 Physics-based Leakage Model

A 3D printer may be considered as a cartesian robot [18]. The physical modeling of the kinematics of the cartesian robot have been extensively explored in [18]. Based on these modeling, the dynamic response of the 3D printer may be calculated. Besides, apart from the vibration from the dynamic response of the 3D printer, the stepper motors present in the 3D printer itself vibrate based on the current supplied to its winding. Hence, we will also present the electro-mechanical leakage model of the 3D printer.

2.1.1 Dynamic Model of the 3D Printer

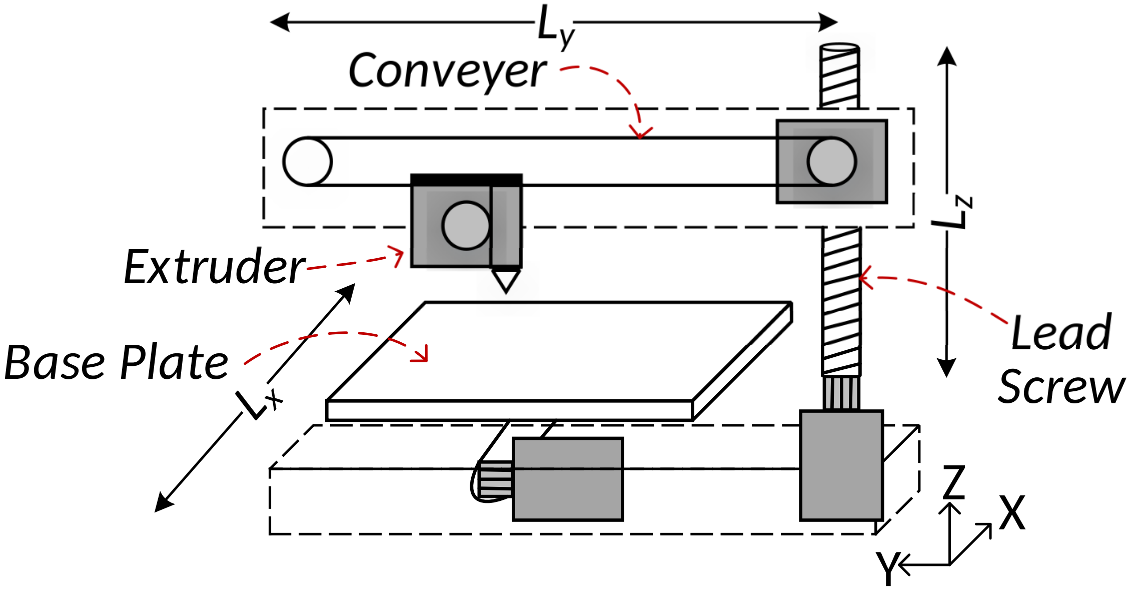


Figure 2.1: Simplified Mechanical Structure of a 3D Printer.

Simplified diagram of the state-of-the-art desktop 3D printer is shown in Figure 2.1. It has three Degrees Of Freedom (DOF) for the extruder. There are three stepper motors that move the nozzle in the corresponding axis. The extruder consists of a stepper motor that pushes the thermo-plastic through the heating filament present in the nozzle. 3D printers realize the three DoF in various ways. Considering the nozzle as the *end-effector*, and the *base plate* as a point of reference, the 3D printer consists of three kinematic chains, each consisting of a prismatic actuator (stepper motors). We can define the generalized position of the *end-effector* as $q = [q_x, q_y, q_z]$, where $q \in \mathbb{R}^{n\times 1}$, and q_x, q_y, and q_z are the *joint position* of each of the joints (x, y and z axis). Since the *joint* is prismatic, $q_{i\in(x,y,z)} = d_i$, where d_i corresponds to displacement of the *joint* in each axis. The *end-effector* cartesian coordinate (x, y, z) is function of the generalized position q. Now, we can define the Lagragian $L(q, \dot{q})$ as the difference between the kinetic and the potential energy of the system. Thus,

$$L(q, \dot{q}) = T(q, \dot{q}) - V(q) \tag{2.1}$$

where T is the kinetic energy and V is the potential energy of the system. Then the dynamic equation of the 3D printer can be given as follows:

$$\frac{d}{dt}\left[\frac{\partial L(q, \dot{q})}{\partial \dot{q}}\right] - \frac{\partial L(q, \dot{q})}{\partial q} = \Upsilon \tag{2.2}$$

where Υ is the external force given as follows:

$$\Upsilon = \tau - f(\tau, \dot{q}) \tag{2.3}$$

where $\tau \in \mathbb{R}^{n\times 1}$ is the torque produced by each of the stepper motors in the joints, and $f(\tau, \dot{q}) \in \mathbb{R}^{n\times 1}$ is the friction vector. The general dynamics equation of the 3D printer can also be written as follows [24]:

$$M(q)\ddot{q} + C(q, \dot{q})\dot{q} + g(q) + f(\tau, \dot{q}) = \tau \tag{2.4}$$

where, $M(q) \in \mathbb{R}^{n\times 1}$ is an inertial matrix, $C(q, \dot{q}) \in \mathbb{R}^{n\times n}$ is the torque matrix, and $g(q) \in \mathbb{R}^{n\times 1}$ is the vector gravity torque. To produce these torques, the current is supplied in the coils of the stepper motors. Considering two phase hybrid stepper motors, the total torque produced by the motor due to the current i_A and i_B passing in the two phases can be calculated as follows:

$$\tau = -p\Psi_m i_A sin(p\theta) - p\Psi_m i_B sin(p(\theta - \lambda)) \tag{2.5}$$

where Ψ_m is the maximum stator flux linkage, p is the number of rotor pole pairs, λ is the angle between the two stator windings, and θ is the mechanical rotational angle. By accurately measuring the all the coefficients in Equation 2.4, we may be able to measure the frequency response and the corresponding vibration of the 3D printer system. However, this is non-trivial and also lacks consideration of mechanical degradation due to aging effect.

2.1.2 Electro-mechanical Model of the 3D Printer

In the dynamic model of the 3D printer, the frequency response of the 3D printer due to the applied torque and the corresponding frequency present in each joint is explained. However, apart from this, the stator of the stepper motor in each of the axis also vibrates due to the fluctuating radial electromagnetic force on the stator. From Maxwell stress tensor, we can calculate the magnitude of the radial force per unit area at any point of the air gap as follows:

$$\sigma = \frac{b_n^2 - b_t^2}{2\mu_o} \tag{2.6}$$

where b_t is the tangential air-gap flux density, b_n is radial air-gap flux density, and μ_o is the permeability of the free space. The magnetic flux density is the function of current flowing through the stator, number of windings turns in each stator core, magnetic flux path length, etc. This radial forces per unit area can be abstracted and expressed as follows:

$$p_r(\alpha, t) = P_r cos(r\alpha - \omega_r t) \tag{2.7}$$

where r is the order of the force wave, ω_r is the angular frequency of the force of the r_{th} order, α is the angular distance from the given axis, and P_r is the amplitude of the radial force pressure in N/m^2. Each of the stepper motors used in the 3D printer is a source of vibration with its own stator natural frequency expressed as follows [10]:

$$f_r \approx \frac{1}{2\pi}\sqrt{\frac{K_r + K_r^f + K_r^w}{M + M_f + M_w}} \tag{2.8}$$

where K_r, K_r^w, and K_r^f is the lumped stiffness of the stator, tooth-slot zone including winding, and frame where stepper motor is connected, respectively. M, M_w, and M_f are the mass of the stator core, winding, and frame, respectively. Next assuming, the transfer path for various components of the 3D printer to be linear, we can use the transfer path analysis method to determine the sound pressure spectrum at point i due to a force acting upon point j, in direction k as follows:

$$p_{ijk}(\omega) = H_{ijk}.F_{jk}(\omega) \tag{2.9}$$

where H_{ijk} is the frequency response function between point i and j, F_{jk} is the force spectrum at point j. Then the sound pressure, only considering the prismatic DOF, at point i is obtained as follows [22]:

$$p_i(\omega) = \sum_{j=1}^{N}\sum_{k=1}^{3} H_{ijk}.F_{jk}(\omega) \tag{2.10}$$

Equation 2.10 becomes complex when we consider revolute DOFs. Moreover, calculation of the frequency response function and the fluctuating force itself is non-trivial. This fact points out that, it is less strenuous to use data-driven model to estimate the sound production.

2.2 Data-driven Leakage and Adversary Model

In the adversary model, we assume that there are M side-channels from which an attacker can acquire the leakage information. The G-code is the *sensitive variable*, that an attacker seeks to extract from the 3D printer. Let G represent the *sensitive* discrete random variable, with probability distribution function $p(g)$, where $g_1, g_2, \ldots, g_k$ represents the possible G-code instructions. Then the leakage from each channel can be written as follows:

$$L_i = \delta_i(G) + N_i \quad i = 1, 2, \ldots, M \tag{2.11}$$

where N_i denotes an independent noise (independent from the variable G) in the i^{th} channel, $\delta(.)$ represents the deterministic function, and L_i is the leakage in the i^{th} channel. Moreover, for each G-code instruction g_k, the corresponding leakage may be given as follows:

$$l_{(i,k)} = \delta_i(g_k) + n_{(i,k)} \quad k = 1, 2, \ldots, K \tag{2.12}$$

where $n_{(i,k)}$ represents the leakage noise value in the i^{th} channel for the k^{th} leakage measurement, and K is the total number of G-code instructions. To breach the confidentiality of the system, an attacker measures leakages $l_{(i,k)}$ from m side-channels for all the G-code instructions used to print a 3D object. An attacker will apply a *leakage model function* $f(l_{(i,k)})$ to estimate the G-code instruction $\hat{g}_k = f(l_{(1,k)}, l_{(2,k)}, \ldots, l_{(M,k)})$. There are two phases for an attacker. The first one is the training phase, where the attacker acquires the leakage signal from M channels using various sensors and test objects. Then the *leakage model function* is estimated $\hat{f}(., \alpha)$, where α is the tuning parameter for the function. Then in the second phase, leakage for real objects are gathered and the original G-code is extracted using the estimated functions. Various statistical tools can be used to model the *leakage model function*

$\hat{f}_i(., \alpha)$, such that

$$i = \underset{1 \leq i \leq N}{\arg\min} \sum_{k=1}^{K} |g_k - \hat{f}_i(., \alpha)| \tag{2.13}$$

where N is the total *leakage model function* the attacker can estimate. The accuracy of the estimated function depends on the amount of information leaked about G in the side-channels. We use *mutual information* as a *metric* to quantify the information leakage from each of the channels. Given that we have the *joint probability distribution function* $p(g, l_i)$, and marginal probability distribution $p(g)$ and $p(l_i)$ for the discrete random variables G and L_i, we can calculate the mutual information between the G-code instruction and the leakage as follows:

$$I(G; L_i) = \sum_{l_i \in L_i} \sum_{g \in G} p(g, l_i) log_2 \left(\frac{p(g, l_i)}{p(g)p(l_i)} \right) \tag{2.14}$$

since we have used base 2 for the logarithm, the unit of the mutual information is *bits.* Using Equation 2.14, we can quantify the leakage of information in each side-channel separately.

Chapter 3

Leakage Aware Optimization

The data-driven leakage modeling for quantifying the information leakage (as shown in Figure 3.1) may be done in two stages:

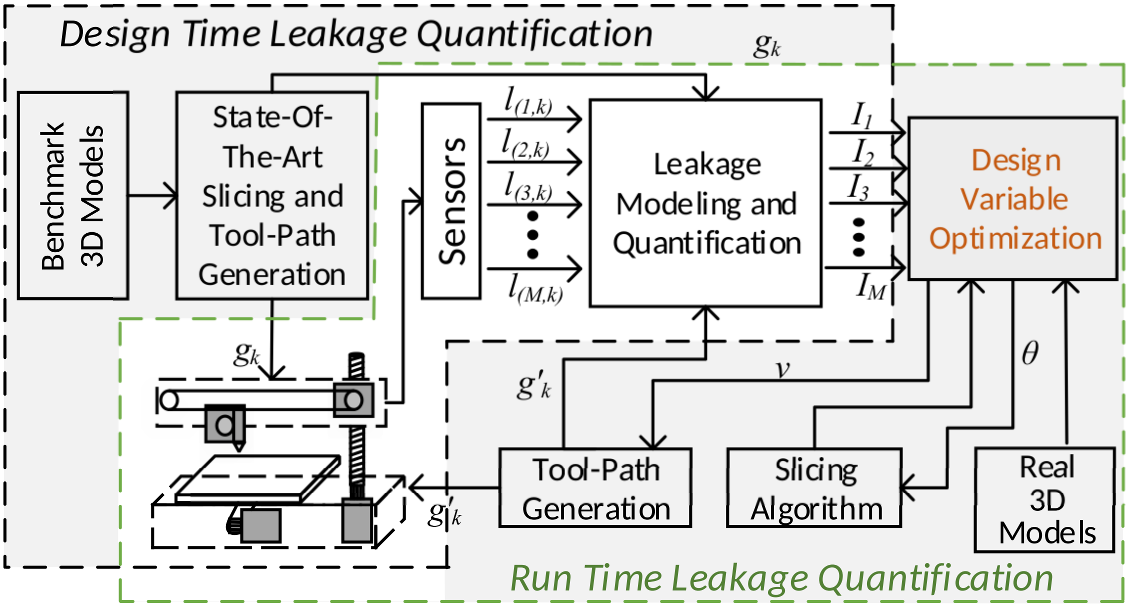

Design Time Leakage Quantification
g_k
Benchmark 3D Models
State-Of-The-Art Slicing and Tool-Path Generation
Sensors
$l_{(1,k)}$
$l_{(2,k)}$
$l_{(3,k)}$
$l_{(M,k)}$
Leakage Modeling and Quantification
I_1
I_2
I_3
I_M
Design Variable Optimization
g_k
g'_k
v
θ
Tool-Path Generation
Slicing Algorithm
Real 3D Models
g'_k
Run Time Leakage Quantification

Figure 3.1: Leakage Modeling and Security Aware Optimization Algorithm.

3.1 Design-Time Leakage Quantification

During the design phase, manufacturer can use the data-driven leakage model to measure the mutual information between the various signals leaked from the side-channels and the G-code acquired from the benchmark 3D models used for testing the quality of the printer. This mutual information can then be used to optimize the design variables. This type of quantification is only done once, and 3D printer users need not perform the leakage quantification.

3.2 Run-Time Leakage Quantification

The components in the physical domain continuously go through the process of degradation. These degradation can have both positive or negative impacts on the mutual information. In scenarios where these degradation increase the mutual information, the design variables have to be optimized again for minimizing the leakage. Hence, run-time leakage quantification is necessary to make sure that the environmental condition and aging of the physical system do not aid in the leakage of the information.

Based on the physics-based leakage model of the 3D printer, we propose two design variables that can be used to minimize the amount of leakage from the acoustic side-channel.

Preposition 1: *Given the nozzle movement in xy-plane during printing a single layer in additive manufacturing in a straight line, let the nozzle have velocity* $\boldsymbol{v}$ *with angle* θ *with the x-axis, and* $f(\theta) = \sum_{i=1}^{M} I_i$*, be a function that gives the sum of mutual information between the analog emissions and the G-code for the given angle* θ*. Then* $\exists \beta \in \mathbb{R} : \beta = \arg\min_{\theta} f(\theta)$*. Where,* $0 \leq \beta \leq 2\pi$*.*

Proof. The angle β states if the movement of the nozzle occurs in single or multiple axis. If $\beta = 0°$, then the nozzle moves parallel to x-axis. The dynamics of the system changes when there are different axis movements. Due to discretization of signals, environmental noise, and similarity of load/frame structure, different axis movements will have varying leakage in the side-channel. Mutual information will be low if these complex axis movements leakages cannot be distinguished. Hence, there exists a certain angle for which we can obtain minimum $I(G; L_i)$ value. □

Remark 1: In 3D printing, there are large number of straight line segments, optimizing the θ for each segment to minimize leakage can affect the convergence of the optimizing algorithm. Rather, we use Principal Component Analysis (PCA) to to find the common orientation angle of all the line segments. In digital process chain, the 3D model is converted to a file with tessellated triangles that describe the geometry. From this file, using the cross product, a vector, $\vec{u}$, normal to the plane of the triangular surface is calculated. Next, PCA is performed on the collection of vectors $\vec{u}$ calculated for all the triangular surfaces. We then use the first principal component which has the highest eigenvalue. This value represent the most common normal vector of all the line segments. We define θ as the angle of the vector $\vec{u'}$ which is perpendicular to the first principal component of the vector $\vec{u}$.

Preposition 2: *Given the nozzle movement to print a line segment of length l in xy-plane, let v_x and v_y be its velocity in x and y-axis respectively. Where travel feed rate is $v = \sqrt{v_x^2 + v_y^2}$. Then $\exists v' \in \mathbb{R} : v' = \arg\min_v f(v)$. Where $f(v) = \sum_{i=1}^{M} I_i$, gives the mutual information for various speed.*

Proof. v' values that will achieve the minimum mutual information in the side-channel lie in the higher travel feed ranges. Considering the acoustic side-channels, first the higher frequency excitation due to faster travel feed-rates will cause reduction in the amplitude of the vibration as most of the time this excitation force act in opposing direction of the vibration, and second, the leakage signal will be corrupted quickly by new analog emission from the next G-code. Due to this, the sample of data collected for the G-codes with large travel feed-rate, will be less in number, and may be contaminated by other G-code leakage signal. Hence, due to mixture of the leakage signals for different G-code, the mutual information extracted will be low. □

State-of-the-art CAM Tools: Current slicing algorithms for fused deposition modeling based desktop 3D printers do not consider the information leakage through the side-channels and have tool-path generation that are optimized for machining efficiency (time, material deposition, etc.) and precision of the printing process only.

Optimization Problem Statement: For minimizing the information leakage from acoustic side-channel, based on preposition 1 and 2, we propose a new leakage aware algorithm. We define our design variables as, $0 \leq \theta \leq 2\pi$, and $v = \sqrt{v_x^2 + v_y^2}$. Where $v_x \in \mathbb{R}$, and $v_y \in \mathbb{R}$. For the speed in x and y axis, we have two variable bounds such as $v_{xmin} \leq v_x \leq v_{xmax}$ and $v_{ymin} \leq v_y \leq v_{ymax}$. Where v_{xmin} and v_{ymin} are the minimum machine specific travel feed-rate in x and y axis respectively, and v_{xmax} and v_{ymax} the maximum machine specific travel feed-rate in x and y axis respectively. We have a simple constraint such that $T \leq kT_{orginal}$. Where $T_{original}$ is the printing time of the state-of-the-art slicing and tool-path generation algorithm, and $k \geq 1$ is the user defined constant. The leakage functions in fact, estimate the joint probability distribution $p(g, l_i)$ present in the equation 2.14, and for simplicity we define an estimation function that give the relation between the design variables and the analog emissions, $\hat{f}_\theta(., \alpha_\theta)$ and $\hat{f}_v(., \alpha_v)$. Based on these functions we can calculate the mutual information between the G-code and the leakage signal $I_{\theta_i}(G; L_i)$ and $I_{v_i}(G; L_i)$. Using a non-linear polynomial functions $f_{\theta_i}(I_{\theta_i}, \theta_i)$ and $f_{v_i}(I_{v_i}, v_i)$, we can estimate the relation between the mutual information and the design variables in different side-channels. Then our multi-objective optimization function can be given as follows:

$$(\theta, v) = \arg\min_{(\theta,v)}(f_{\theta_1}, f_{\theta_2}, \dots, f_{\theta_M}, f_{v_1}, f_{v_2}, \dots, f_{v_M}) \tag{3.1}$$

Based on the value given by the optimized design variable, slicing and tool-path generation will generate new G-code with minimum information leakage.

Algorithm 1: Leakage Aware G-code Generation.

```
   Input: Estimated Functions $\hat{f}_\theta(.,\alpha_\theta)$, $\hat{f}_v(.,\alpha_v)$, STL File
   Output: G-code $g'$
1  Define step size $\triangle_\theta$, $\triangle_v$ and range $min_\theta, min_v$ and $max_\theta, max_v$
2  for $i = 1 : M$ do
3      for each $j \in (\theta, v)$ do
4          for $k = min_j$ :$\triangle_j$: $max_j$ do
5              $I_{(j_i,k)} = I_k(G; L_i)$                    // Based on $\hat{f}_j(.,\alpha_j)$
6      Estimate Nonlinear function $f_{j_i}$
7  Optimize $\arg\min_{(\theta,v)}(f_{\theta_1}, f_{\theta_2}, \dots, f_{\theta_M}, f_{v_1}, f_{v_2}, \dots, f_{v_M})$
8  $g'$ =SliceandToolPathGeneration($\theta, v$, STL File)
9  return $g'$
```

In algorithm 1, functions estimated by collecting the leakage and the G-code data while printing the benchmark 3D models are passed to the algorithm. Then in line 1, first the step size for estimating the cost function based on the design variables θ, v are defined, along with their range. Then from line 2 to 6, using the functions $\hat{f}_\theta(.,\alpha_\theta)$, $\hat{f}_v(.,\alpha_v)$, various mutual information values are calculated for the varying design variables. In line 6, polynomial function is used to estimate the relation between the design variables and the mutual information calculated in line 5. Then based on the description of the problems statement, mixed multi-objective non linear integer programming is used to optimize the design variables. In line 8, the modified design variables are passed to the slicing and tool-path generation function to generate a G-code with minimum leakage, which is finally returned in line 9.

Chapter 4

Experimental Results

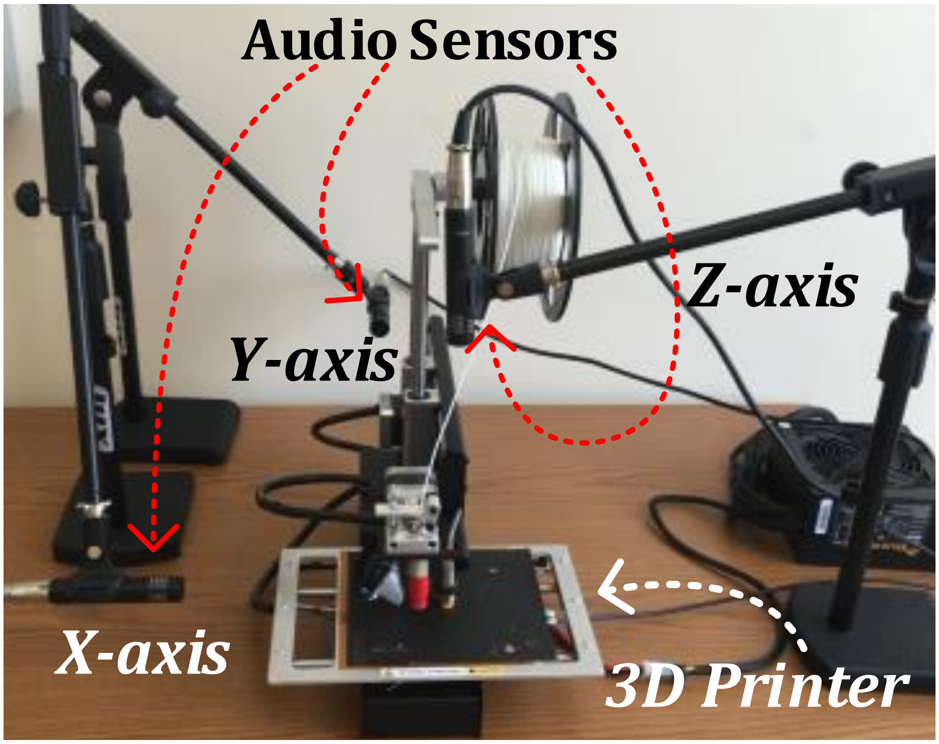


Figure 4.1: Experimental Setup.

The experimental (as shown in Figure 4.1) setup consists of a fused deposition modeling based desktop 3D printer [9]. We put three AT2021 cardioid condenser audio sensors [1] parallel to x, y and z-axis, respectively and treat them as individual channels. Hence, we have $M = 3$. In order to calculate the mutual information, the raw leakage signal with higher sampling rate may not result in good description of the signal. Hence, we have calculated the power spectral density of the audio signal and used the three principal components to represent the mutual information.

4.1 Mutual Information

4.1.1 Design Variable - θ

We varied θ from 0° to 90° with the step size $\triangle_\theta = 10^\circ$. Based on the data collected joint probability function $p(\theta, l_i)$ is estimated and used in calculating the mutual information using Equation 2.14.

In Figure 4.2, three principal components and the curve representing the estimation of the mutual information variation corresponding the θ is presented. We can see that for audio signals placed in z-axis and y-axis the mutual information is lower when the nozzle movement is not parallel to x or y-axis. However, for x-axis, the mutual information is the least when the angle is 90°. This may be due to the fact that when the angle is parallel to y-axis, the audio signal captured by the audio sensor does not have much variation.

4.1.2 Design Variable - v

We varied the travel feedrate from 700 mm/min to 3300 mm/min with the step size $\triangle_v =$ 200 mm/min. In Figure 4.3, we present the mutual information between the three principal components of the power spectral density and the varying travel feedrate. As expected, we can observe that for all the audio signals collected, the mutual information is higher during slower travel feed-rate and lower for the faster travel feedrate.

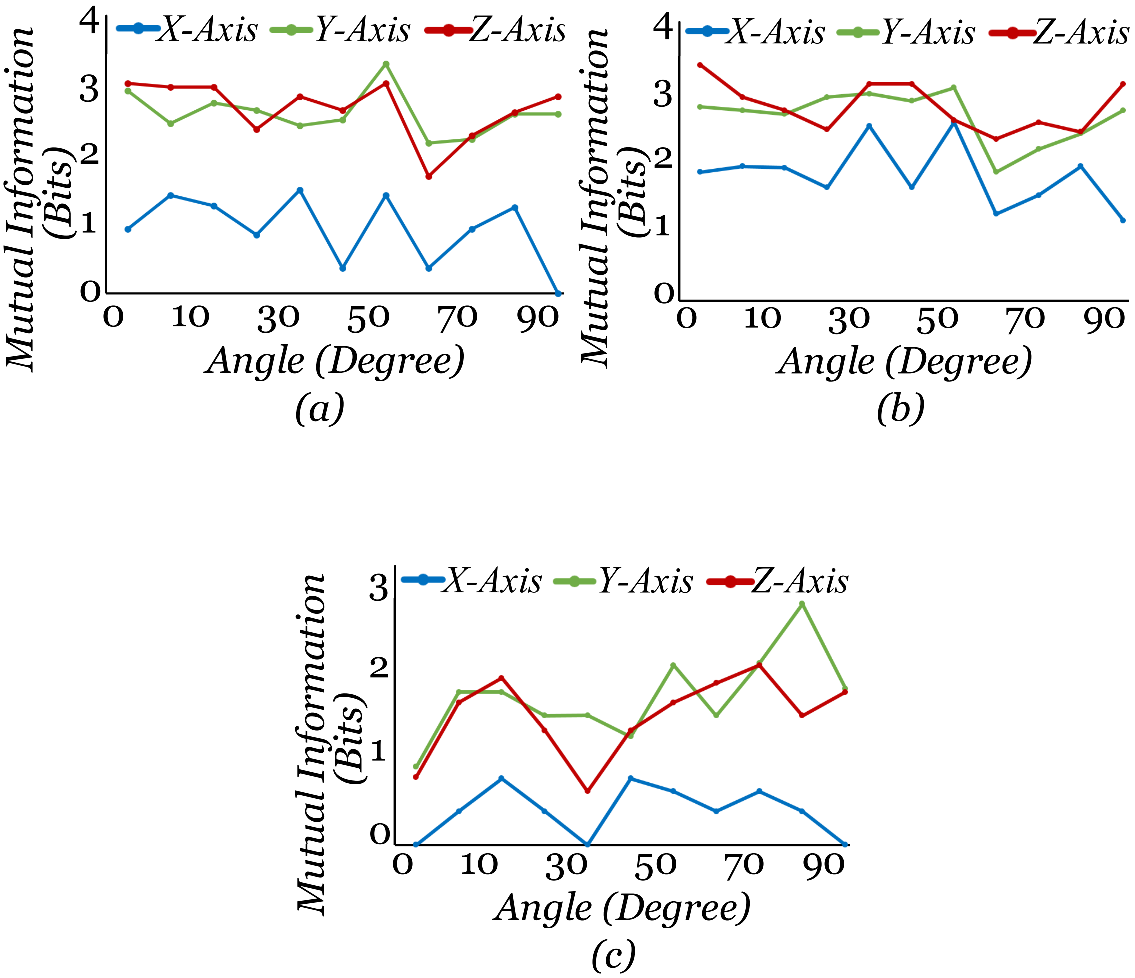
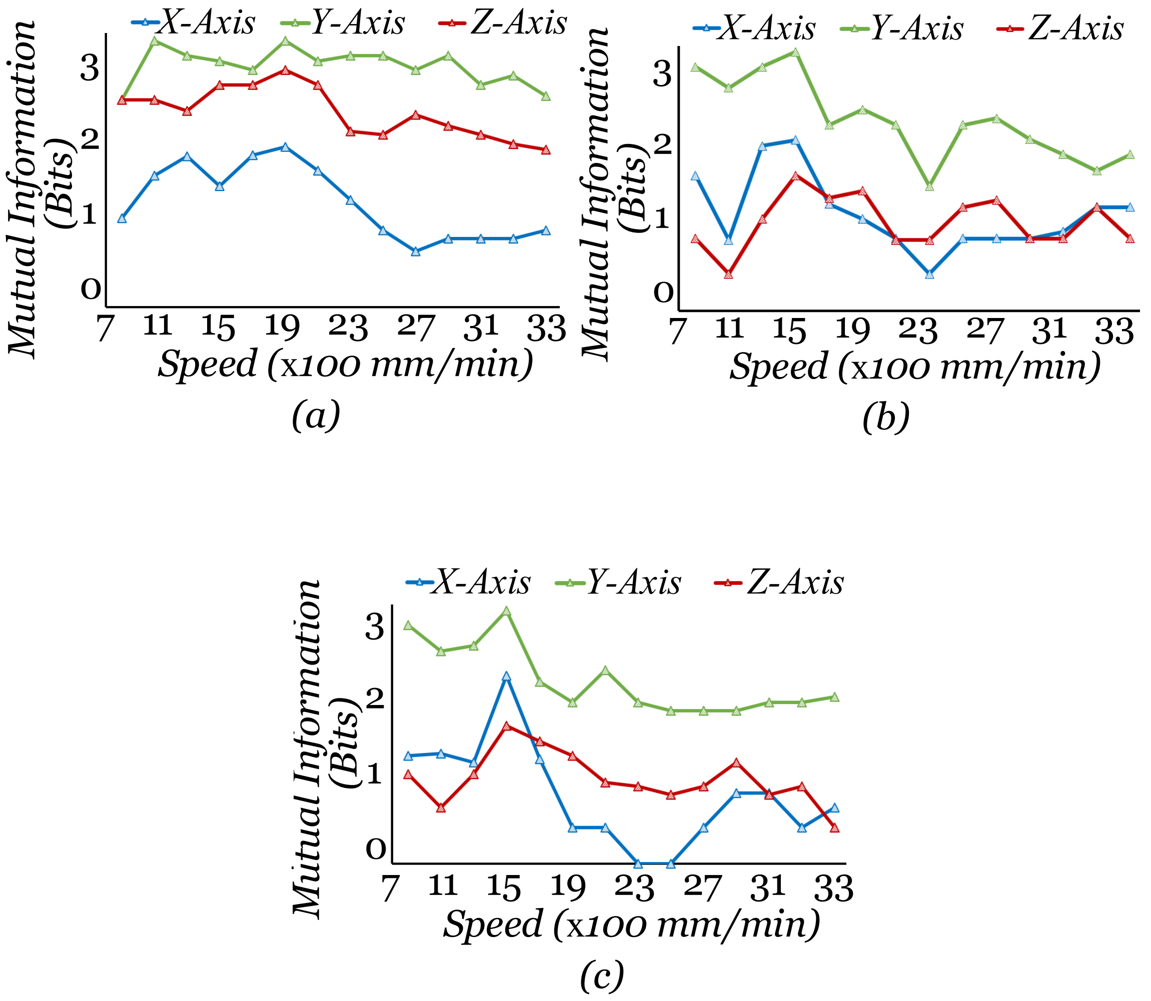


Figure 4.2: Mutual Information between Angle and Leakage, with total Angle Entropy of 3.4594 bits. (a) Principal Component 1, (b) Principal Component 2, (c) Principal Component 3.



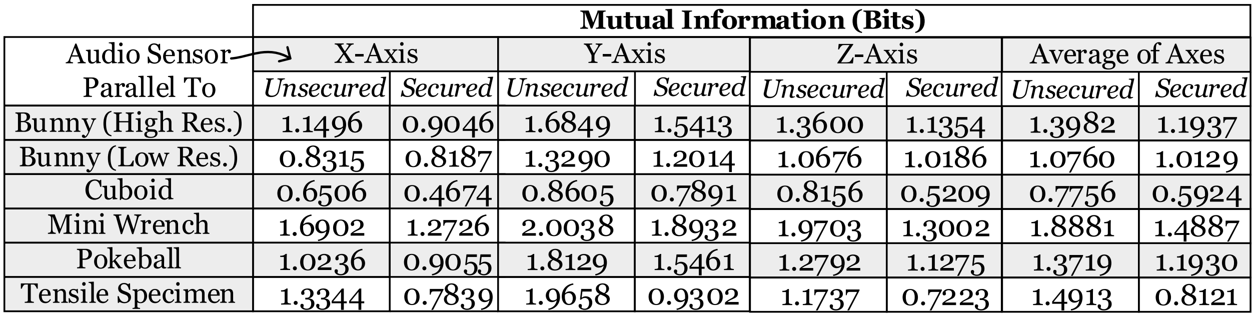
(a)

(b)

(c)

Figure 4.3: Mutual Information between Speed and Leakage, with total Speed Entropy of 3.8074 bits. (a) Principal Component 1, (b) Principal Component 2, (c) Principal Component 3.

Table 4.1: Mutual Information Between G-code of and Acoustic Signal.



	Mutual Information (Bits)							
Audio Sensor→	X-Axis		Y-Axis		Z-Axis		Average of Axes	
Parallel To	*Unsecured*	*Secured*	*Unsecured*	*Secured*	*Unsecured*	*Secured*	*Unsecured*	*Secured*
Bunny (High Res.)	1.1496	0.9046	1.6849	1.5413	1.3600	1.1354	1.3982	1.1937
Bunny (Low Res.)	0.8315	0.8187	1.3290	1.2014	1.0676	1.0186	1.0760	1.0129
Cuboid	0.6506	0.4674	0.8605	0.7891	0.8156	0.5209	0.7756	0.5924
Mini Wrench	1.6902	1.2726	2.0038	1.8932	1.9703	1.3002	1.8881	1.4887
Pokeball	1.0236	0.9055	1.8129	1.5461	1.2792	1.1275	1.3719	1.1930
Tensile Specimen	1.3344	0.7839	1.9658	0.9302	1.1737	0.7223	1.4913	0.8121

4.2 Test with Benchmark 3D Models

We have selected benchmark models that are easily available and used for testing the 3D printer's performance. These models include *Stanford bunny* in high and low resolution, a simple *cuboid*, mini *wrench*, *pokeball*, and a *tensile test specimen* in the shape of a dogbone. We can see (in Table 4.1) that with the optimized design variable, the mutual information between the G-code and the acoustic leakage have dropped for all the signals collected by thee microphones placed parallel to each of the axis. Moreover, we present the average mutual information across all the audio signals in Figure 4.4.

The models that have smaller line segments (*cuboid*) and more curves (*bunny* with high resolution) have lower mutual information in acoustic side-channel compared to the others. Moreover, the *tensile test specimen* which has longer line segments had highest mutual information reduction of **45.54%** when the speed and angle was optimized for it. It can be seen that compared to the unsecured G-code generated from the slicing and tool-path generation, our secured approach reduces the mutual information for all the 3D models. From Figure 4.4, we can see that the average drop in mutual information for the benchmark models is **24.76%**. Furthermore, our secured G-code only increased the average printing time for all the models by **0.58%**.

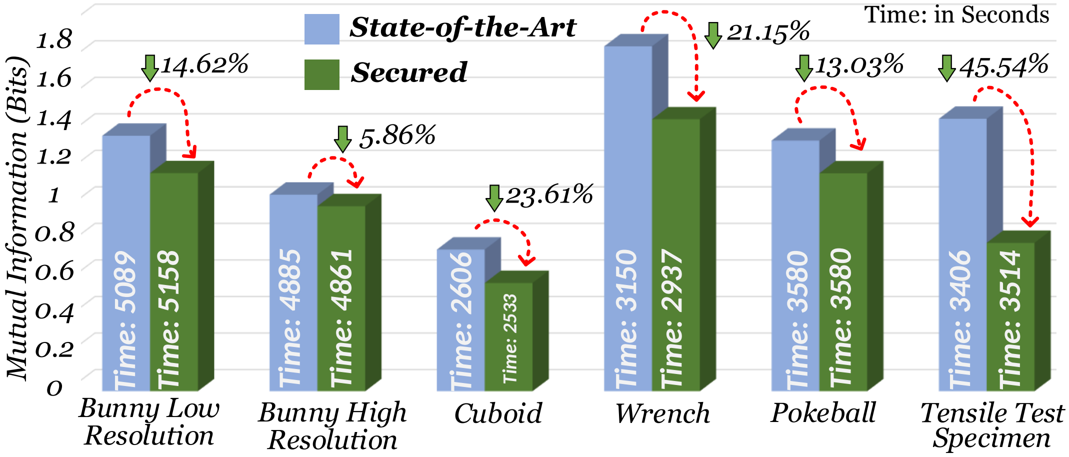


Figure 4.4: Mutual Information for Benchmark 3D Models.

Chapter 5

Conclusion

In this thesis we present a novel methodology that provides security solution to maintain the *confidentiality* of the system during the cyber-physical manufacturing process. This solution is incorporated within the computer aided manufacturing tools such as *slicing algorithm* and the *tool-path generation* which are in the cyber-domain. This effectively mitigates the cross domain physical-to-cyber domain attacks which can breach the confidentiality of the manufacturing system to leak valuable intellectual properties. In our methodology, we provide the physics and data-driven leakage models for acoustic side-channel, define various design variables (*orientation* and *speed*), provide an optimization algorithm, and incorporate it in the digital process chain. For various benchmark 3D models, our solution obtains an average mutual information reduction of **24.76%**. With this work, we highlight the capability of leakage aware secured computer aided manufacturing tools to maintain one of the fundamental security requirement, *confidentiality*, of the cyber-physical manufacturing systems.

Bibliography

[1] AT2021 Cardioid Condenser Microphone. Audio-Technica, 2016.

[2] IBM Cyber Security Intelligence Index. IBM., 2016.

[3] R. Akella, H. Tang, et al. Analysis of information flow security in cyber–physical systems. *International Journal of Critical Infrastructure Protection*, 3(3):157–173, 2010.

[4] M. A. Al Faruque, S. Rokka Chhetri, et al. Acoustic side-channel attacks on additive manufacturing systems. In *International Conference on Cyber-Physical Systems (ICCPS)*. IEEE, 2016.

[5] W. Ashford. 21 percent of manufacturers hit by intellectual property theft. August 2014.

[6] S. R. Chhetri, S. Faezi, and M. A. Al Faruque. Fix the leak! an information leakage aware secured cyber-physical manufacturing system. In *2017 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pages 1408–1413. IEEE, 2017.

[7] S. R. Chhetri, S. Faezi, A. Canedo, and M. A. Al Faruque. Thermal side-channel forensics in additive manufacturing systems. In *Proceedings of the 7th International Conference on Cyber-Physical Systems*, page 22. IEEE Press, 2016.

[8] P. Daugherty, P. Banerjee, et al. Driving unconventional growth through the industrial internet of things. *New York: Accenture*, 2014.

[9] B. Drumm. Printrbot: Your first 3d printer. *Retrieved November*, 26:2013, 2011.

[10] A. Ellison and S. Yang. Natural frequencies of stators of small electric machines. *Electrical Engineers, Proceedings of the Institution of*, 118(1):185–190, 1971.

[11] M. A. Faruque, S. Chhetri, S. Faezi, and A. Canedo. Forensics of thermal side-channel in additive manufacturing systems-semantic scholar. *Irvine, CA*, 2016.

[12] F. Ghilassene. 3D printing and IP rights: some issues, any solutions? ParisTech review., 2014.

[13] I. Gibson, D. W. Rosen, et al. *Additive manufacturing technologies*, volume 238. Springer, 2010.

[14] T. Harte and A. G. Bors. Watermarking 3D models. In *International Conference on Image Processing*. IEEE, 2002.

[15] M. Hvistendahl. 3d printers vulnerable to spying. *Science*, 352(6282):132–133, 2016.

[16] R. Jamieson and H. Hacker. Direct slicing of cad models for rapid prototyping. *Rapid Prototyping Journal*, 1(2):4–12, 1995.

[17] G. Jin, W. Li, et al. Adaptive tool-path generation of rapid prototyping for complex product models. *Journal of manufacturing systems*, 30(3):154–164, 2011.

[18] H. S. Kim and L.-W. Tsai. Design optimization of a cartesian parallel manipulator. *Journal of Mechanical Design*, 2003.

[19] H. Lasi, P. Fettke, et al. Industry 4.0. *Business & Information Systems Engineering*, 6(4):239, 2014.

[20] J. Lee et al. A cyber-physical systems architecture for industry 4.0-based manufacturing systems. *Manufacturing Letters*, 2015.

[21] R. Ohbuchi et al. Watermarking three-dimensional polygonal models through geometric and topological modifications. *IEEE Journal on selected areas in communications*, 1998.

[22] J. Plunt. Finding and fixing vehicle nvh problems with transfer path analysis. *Sound and vibration*, 39(11):12–17, 2005.

[23] S. Rokka Chhetri, A. Canedo, and M. A. Al Faruque. Kcad: kinetic cyber-attack detection method for cyber-physical additive manufacturing systems. In *Proceedings of the 35th International Conference on Computer-Aided Design*. ACM, 2016.

[24] P. Sánchez-Sánchez and F. Reyes-Cortés. *Cartesian Control for Robot Manipulators*. INTECH Open Access Publisher, 2010.

[25] F.-X. Standaert et al. A unified framework for the analysis of side-channel key recovery attacks. In *Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2009.

[26] J. Wan et al. Security-aware functional modeling of cyber-physical systems. In *20th Conference on Emerging Technologies & Factory Automation (ETFA)*. IEEE, 2015.

[27] M. Yampolskiy et al. Intellectual property protection in additive layer manufacturing: Requirements for secure outsourcing. ACM, 2014.