Poster: A Realizable Framework for Intrusion Detection in Additive Manufacturing Systems Using Analog Side-Channels

Sizhuang Liang
Georgia Institute of Technology
liangsizhuang@gatech.edu

Raheem Beyah
Georgia Institute of Technology
rbeyah@ece.gatech.edu

***Abstract*—Additive Manufacturing (AM) relies heavily on computers to work. As a result, they are susceptible to cyberattacks. For example, the firmware of a printer can be compromised such that the printer behaves maliciously and reports normal status to operators. This can result in printed objects being defective. Once deployed, a defective object can cause the system with the object to fail, resulting in damage or even loss of lives. To defend against this type of attacks, several intrusion detection systems leveraging analog side-channels, such as acoustic emissions, power consumption, vibration, and electromagnetic fields, have been proposed in the literature. These systems monitor analog side-channel signals in a printing process, called measurement, and compare the measurement to ground truth to detect anomalies. Existing systems work fine for simple lab-based experiments, but not are practical because they do not address deployment-related issues, such as the segmentation problem, synchronization problem, and window size problem.**

To solve the aforementioned problems, we propose a realizable framework for intrusion detection in AM using analog side-channels. In this framework, both ground truth and measurement can exist in three domains, namely, the layer information domain, control signal domain, and side-channel domain. Inter domain conversion transforms information in one domain to another domain. Intra domain conversion changes the representation in the same domain. We can avoid the segmentation problem and window size problem by avoiding conversion from the side-channel domain to the control code domain. We address the synchronization problem by using the master track method and the dynamic time warping method. To evaluate the framework, we setup an intrusion detection system with a microphone, a power sensor, and an inertial measurement unit to collect data on a SeeMeCNC Rostock Max V3 printer. Experimental results shows that the system can avoid the aforementioned problems.

I. Introduction

Additive Manufacturing (AM), also known as 3D printing, refers to a collection of manufacturing processes where material is joined together layer by layer to make objects directly from Computer-Aided Design (CAD) models. AM is gaining popularity in critical manufacturing industries, but also facing more cyberattacks. Moore et al. demonstrated that by compromising the firmware of a printer, one can take over the control flow of a printer and initiate a malicious print, or secretly modify important parameters that control the printing process, rendering printed objects defective [1]. Belikovetsky et al. showed that, by compromising an AM system that manufacturers propellers for drones, an attacker can maliciously insert voids into a printed propeller, causing the propeller to break in a flight, resulting in the drone with the propeller to fall from the sky [2].

II. Existing Solutions and Problems

To protect AM systems from the aforementioned attacks, there are research efforts to build intrusion detection systems using analog side-channels [3], [4], [5], [6]. The general structure of these systems is shown in Fig. 1.

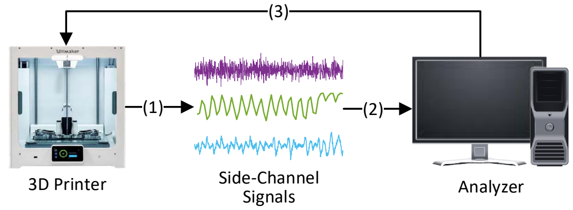


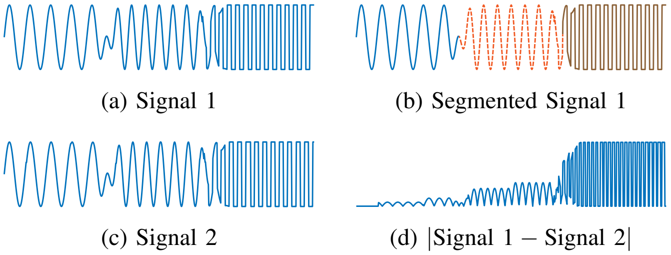
Fig. 1: General structure of intrusion detection systems using analog side-channels. (1) A group of sensors capture analog side-channel signals, and they are the measurement. (2) The signals are analyzed and compared to the ground truth to determine if an anomaly happens. (3) If an anomaly is detected, the analyzer alerts AM operators and stops the printer.

These IDS systems are air-gapped from the AM systems to be protected, and there is no overhead on the AM systems to deploy the IDS systems. However, the existing solutions lack practicality or suffer from performance issues due to problems shown in Table I.

Segmentation Problem. Analog side-channel signals are continuous time-series data. Segmentation refers to a process to segment the signals into pieces with each piece corresponding to its control code, as shown in Fig. 2 (b). This is a required and important process in Chhetri's system. However, Chhetri's system implicitly assumes that this process has been done.

Synchronization Problem. Moore and Belikovetsky's systems detect anomaly by comparing two analog side-channel signals pointwisely. Even if the two signals are aligned perfectly at the beginning, a slight change in one signal can easily make them out of synchronization, and renders the comparison invalid. Signals in Figs. 2 (a) and (c) differ slightly but their absolute difference increases wildly, as shown in Fig. 2 (d).

Window Size Problem. The acoustic layer in Bayen's system uses very large constant size windows for analysis.



(a) Signal 1

(b) Segmented Signal 1

(c) Signal 2

(d) |Signal 1 − Signal 2|

Fig. 2: Example signals to illustrate the problems in existing intrusion detection systems using analog side-channel signals.

TABLE I: Problems of existing systems.

Method	Segmentation	Synchronization	Window Size	Distance Metric	Invasive Sensor
Chhetri [3]	✓				
Bayens [4]			✓	✓	✓
Moore [5]		✓			
Belikovetsky [6]		✓			

This makes the acoustic layer in Bayen's system resistant to the synchronization problem, but insensitive to changes that last a short period of time.

Distance Metric Problem. The acoustic layer in Bayens' system yields a vector of scores for each new print. However, the scores only count matches and do not penalize mismatches. As a result, it is possible for a different print to have a higher score than the ground truth print.

Invasive Sensor Problem. The linear potentiometer in the spatial layer in Bayens's system may collide with the object being printed and thus affects the normal operation of a printer.

III. Our Framework

In order to address the aforementioned problems, we propose a realizable framework for intrusion detection in AM using analog side-channels. The details are as follows.

- Both measurement and ground truth can exist in three domains, as shown in Fig. 3.
- Unlike existing solutions, the framework does not stipulate the exact ground truth or measurement. Instead, the framework discusses all possible choices and combinations of ground truth and measurement, to find the best combination for each AM system.
- In this framework, measurement must come in the side-channel domain, whereas ground truth can come in any domain. Ground truth in each domain has its advantages and disadvantages.
- There are intra domain and inter domain conversions. Whereas inter domain conversion changes information from one domain to another domain, intra domain conversion changes representation in the same domain.
- Ground truth and measurement must be in the same domain and representation before comparison.

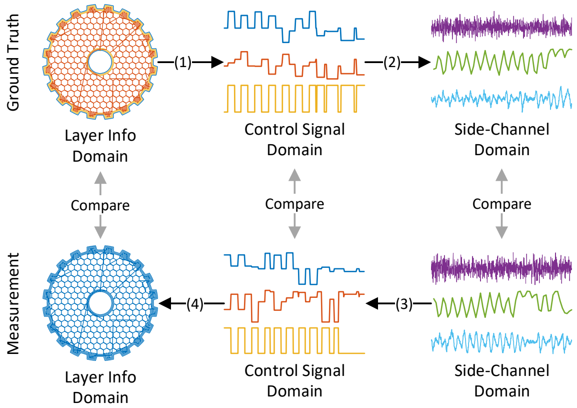


Fig. 3: Layer information domain, control signal domain, and side-channel domain for ground truth and measurement.

We address the synchronization problem using two methods. The first method uses the ground truth as the master track, and we sweep the master track and find its corresponding match in the measurement. The second method is called the dynamic time warping, which is a method used in automatic speech recognition for signals that are not in synchronization.

Segmentation is hard and requires advanced analysis. However, segmentation is not required if there is no conversion from side-channel domain to control signal domain. Segmentation can also be avoided by using a constant window size.

The window size problem only affects performance and does not make an IDS impractical. This problem can be avoided if there is no conversion from side-channel domain to control signal domain.

The distance metric problem can be solved by using a proper distance metric, and we do not use invasive sensors such as linear potentiometers.

References

[1] S. B. Moore, W. B. Glisson, and M. Yampolskiy, "Implications of malicious 3d printer firmware," in *Proceedings of the 50th Hawaii International Conference on System Sciences*, (Honolulu, HI), pp. 6089 – 6098, 2017.

[2] S. Belikovetsky, M. Yampolskiy, J. Toh, J. Gatlin, and Y. Elovici, "dr0wned – cyber-physical attack with additive manufacturing," in *11th USENIX Workshop on Offensive Technologies (WOOT 17)*, (Vancouver, BC), USENIX Association, 2017.

[3] S. R. Chhetri, A. Canedo, and M. A. A. Faruque, "Kcad: Kinetic cyber-attack detection method for cyber-physical additive manufacturing systems," in *2016 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, pp. 1–8, Nov 2016.

[4] 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 *26th USENIX Security Symposium (USENIX Security 17)*, (Vancouver, BC), pp. 1181–1198, USENIX Association, 2017.

[5] 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," *CoRR*, vol. abs/1709.01822, 2017.

[6] S. Belikovetsky, Y. Solewicz, M. Yampolskiy, J. Toh, and Y. Elovici, "Digital audio signature for 3d printing integrity," *IEEE Transactions on Information Forensics and Security*, pp. 1–1, 2018.

A Realizable Framework for Intrusion Detection in Additive Manufacturing Systems Using Analog Side-Channels

Sizhuang Liang and Raheem Beyah
Georgia Institute of Technology
liangsizhuang@gatech.edu, rbeyah@ece.gatech.edu

Introduction

Additive Manufacturing (AM) is gaining popularity and widely used in critical industry sections, such as aerospace, military, and medicine.

- SpaceX used 3D metal printing techniques to manufacture parts in SuperDraco, a hypergolic propellant liquid rocket engine.
- Naval Air Systems Command (NAVAIR) installed a titanium 3D printed link assembly for the engine nacelle in MV-22B Osprey.
- Oak Ridge National Laboratory created the military's first 3D printed submarine hull out of carbon fiber composite material.

AM systems are susceptible to cyber-attacks. Research efforts in the literature has shown that

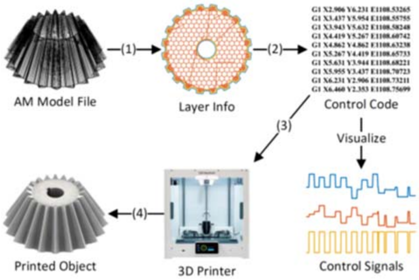
- The firmware of a 3D printer can be compromised to perform malicious activities despite being sent benign control code.
- An attacker can insert malicious features such as voids into printed objects without being detected by AM operators.
- Malicious features can result in degradation of structural integrity and printed objects can break in operation, causing damage [1].

Existing research efforts on intrusion detection systems using analog side-channel signals in AM are not practical, because there are the

- **Synchronization Problem**. Many systems are based on comparing ground truth and measurement, both of which are time-series data, point by point. These methods require the ground truth and measurement be synchronized perfectly, which is impractical.
- **Segmentation Problem**. Some systems require the measured signals be segmented according to their corresponding control code. This is actually hard to do, and these systems do not have a solution.
- Other problems, such as the window size problem, distance metric problem, invasive sensor problem.

To address the problems, we propose a framework for generating practical intrusion detection systems using analog side-channel signals.

General Printing Process



```
G1 X2.906 Y6.231 E1108.53265
G1 X3.437 Y5.954 E1108.55755
G1 X3.943 Y5.632 E1108.58248
G1 X4.419 Y5.267 E1108.60742
G1 X4.862 Y4.862 E1108.63238
G1 X5.267 Y4.419 E1108.65733
G1 X5.631 Y3.944 E1108.68221
G1 X5.955 Y3.437 E1108.70723
G1 X6.231 Y2.906 E1108.73211
G1 X6.460 Y2.353 E1108.75699
```

Figure 1. *A general AM printing process.*

(1) An AM model file is sliced into layers with each layer containing layer information.
(2) Along with manufacturing parameters, the layer information is converted into control code.
(3) The control code is sent to a printer. The firmware of the printer interprets the control code and instructs various actuators in the printer to work.
(4) An object is printed as a result.

Hardware Structure of the Framework

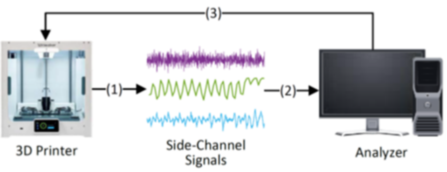


Figure 2. *Hardware structure of intrusion detection systems using side-channel signals.*

(1) A series of sensors measure analog side-channels signals such as acoustic emission, acceleration, vibration, electromagnetic fields, etc.
(2) The measured data are sent to an analyzer for analysis.
(3) The analyzer alerts AM operators or stops the printer when abnormally is detected.

Software Structure of the Framework

The core idea of the framework is to detect anomalies by comparing ground truth with measurement. Both ground truth and measurement can exist in three domains, as shown in Fig. 3.

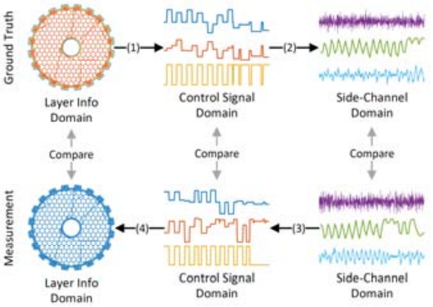


Figure 3. *Layer information domain, control signal domain, and side-channel domain for ground truth and measurement in AM systems.*

Ground Truth Selection: Ground truth can come from any domain. The side-channel domain has most information but requires recording a whole benign printing process. Measurement always comes in the side-channel domain.

Domain Conversion: Ground truth and measurement should be in the same domain before comparison. Otherwise, they should be converted into the same domain.

Comparison Engines: Point by point comparison is impractical due to the synchronization problem. Instead, methods that can tolerate time mismatches should be used.

Preliminary Experimental Results

We setup a measurement system and tested on a Rostock Max V3 printer. Fig. 4 shows an example of step (2) in Fig. 3 for acoustic emission. Fig. 5 shows an example of step (3) in Fig. 3 for velocity along the X direction.

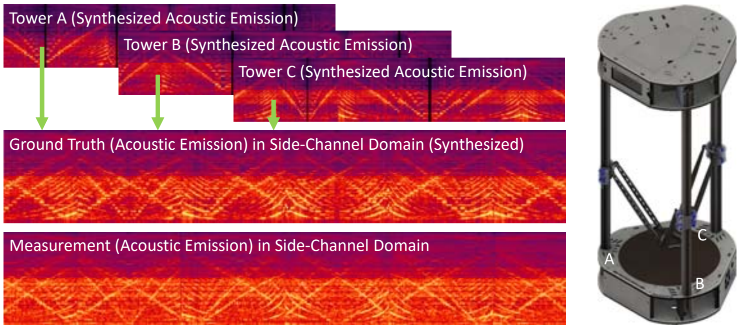


Figure 4. *An example of step (2) in Fig. 3. The printer is shown on the right.*

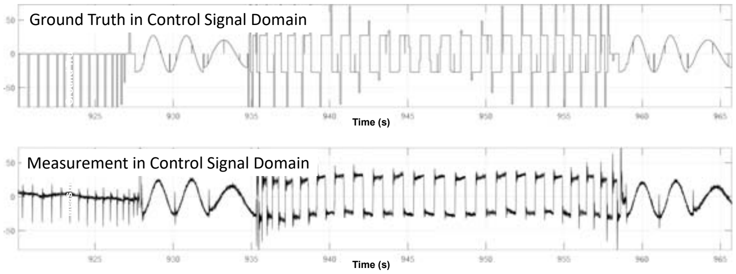


Figure 5. *An example of step (3) in Fig. 3. Shown are velocities along X direction.*

Acknowledgments

This project is supported by NSF under grant number 1739259.

References

[1] S. Belikovetsky, M. Yampolskiy, J. Toh, J. Gatlin, and Y. Elovici, "dr0wned – cyber-physical attack with additive manufacturing," in 11th USENIX Workshop on Offensive Technologies (WOOT 17), (Vancouver, BC), USENIX Association, 2017.

[2] 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 26th USENIX Security Symposium (USENIX Security 17), (Vancouver, BC), pp. 1181–1198, USENIX Association, 2017.