# Defending Side Channel Attacks in Cyber-Physical Additive Layer Manufacturing Systems

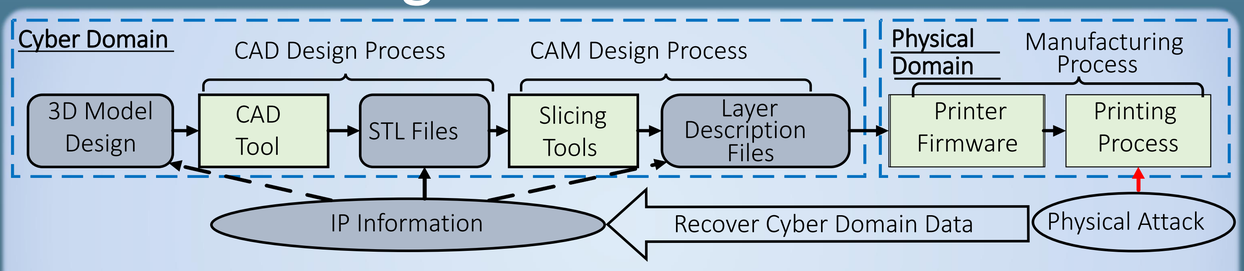
(EAGER: Cyber manufacturing, Project Number : CNS 1546993)

PI: Mohammad Abdullah Al Faruque
University of California, Irvine
alfaruqu@uci.edu

## Objective

- **Objective 1:**
  - To demonstrate novel side-channel attack models for additive layer manufacturing systems.
- **Objective 2:**
  - To present a machine-specific defense mechanism against the proposed attack models.
- **Objective 3:**
  - To present a new security-aware 3D printing algorithm for the machine-independent CAD tools.

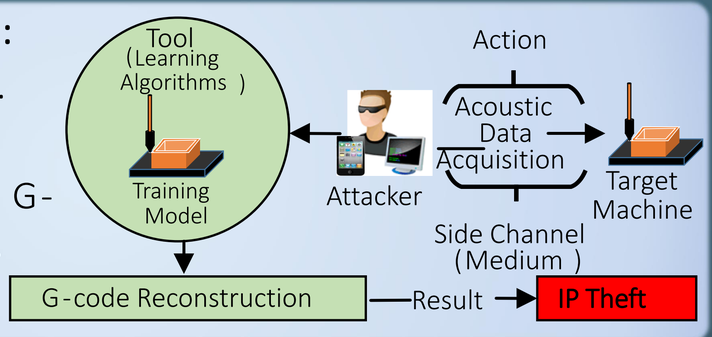
## Background and Motivation




- **Physical-To-Cyber Domain Attacks:**
  - Utilize physical domain data to conduct attack on Confidentiality (steal IP), Integrity, and Availability (CIA).

## Objective 1: Acoustic Attack Model

- **Acoustic Attack Model [1]:**
  - Train Learning Algorithms.
  - Record acoustics.
  - Extract Information about G-code (Used in 3D-Printes).
  - Reconstruct the Object.

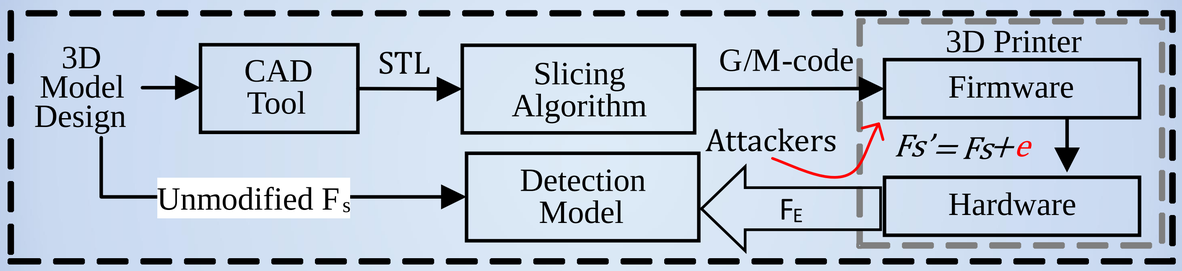



## Experimental Setup and Result



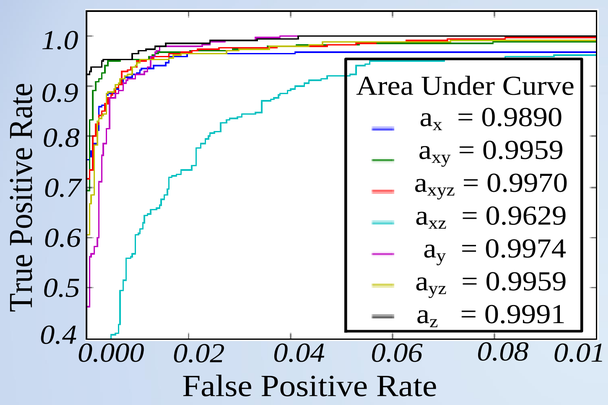

- **Test Parameters:**
  - Speed, Dimension, and Complexity (Movement in Multiple Axes).
- **Average Accuracy:**
  - Axis Prediction Accuracy Classification Models: **86.00%**.
  - Length Prediction Error of Regression Models: **11.11%.**
  - **Perimeter Accuracy of a Test Case (Key): 92.48%.**

## Attack Detection [2]

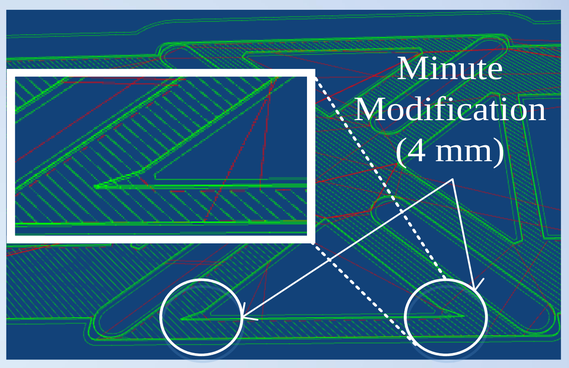



Firmware Modification Detection Model for Additive Manufacturing

## Results




(a) ROC Curve for Axis Modification Detection.




(b) G-code Trace after Kinetic Attack.

- **Average Accuracy:**
  - Average detection in range of variations: **77.45%**

## Future Work

- **Objective 1:**
  - Analyze multiple side-channels for complex attack models.
- **Objective 2:**
  - Design a framework for quantifying leakage for specific machine and provide a G-code generation algorithm.
- **Objective 3:**
  - Analyze slicing algorithm and tool-path generation algorithms for machine-independent CAM tools.

## Summary

- Side-channel leak information.
- Analog emission can be used for defense as well.
- Multiple side-channels can leak more information.
- It is imperative to incorporate side-channel leakage as a parameter in design methodology for secure additive manufacturing systems (future work).

## References

1. M. A. Al Faruque, S. Chhetri, A. Canedo, J. Wan, "*Acoustic Side-Channel Attacks on Additive Manufacturing Systems*", accepted to be published in the ACM/IEEE International Conference on Cyber-Physical Systems (**ICCPS'16**), Vienna, Austria, April, 2016
2. S. Chhetri, A. Canedo, M. A. Al Faruque, "*KCAD: Kinetic Cyber Attack Detection Method for Cyber-Physical Additive Manufacturing Systems*", accepted to be published in the ACM/IEEE International Conference on Computer-Aided Design (**ICCAD'16**), 2016