Trustworthy Cyber-Physical Additive Manufacturing with Untrusted Controllers (Award #1739259)

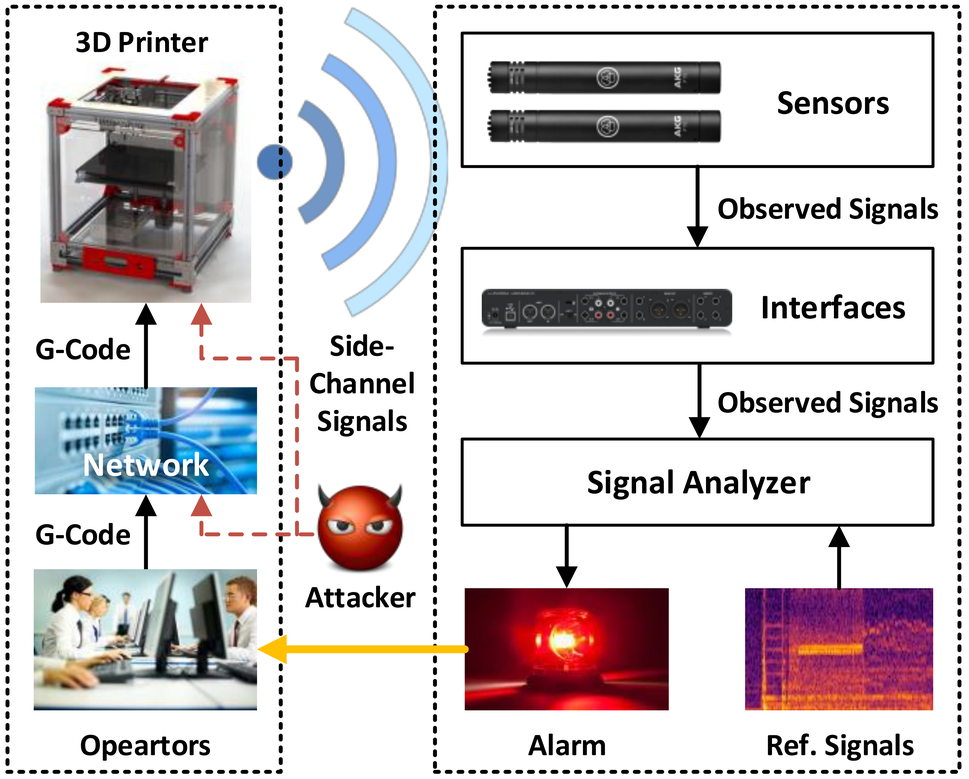
Saman Zonouz, Mehdi Javanmard, Athina Petropulu (Rutgers University), Raheem Beyah (GaTech)

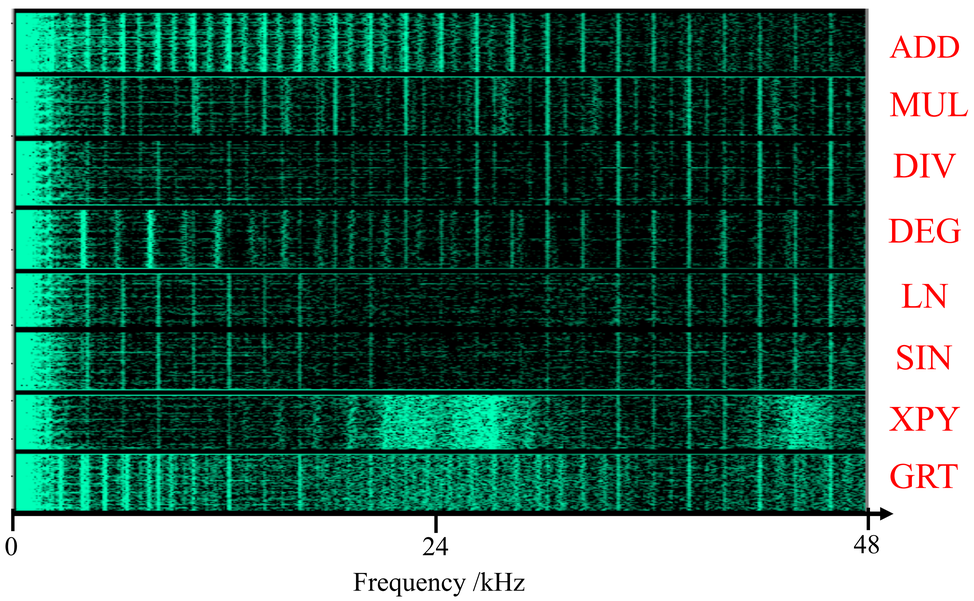
Challenge:

- Use noisy side-channels in manufacturing for intrusion detection with high accuracy
- Prevent malicious confidential 3D printer design disclosures using side channels
- Prevent malicious corruption of 3D printer designs preprint

Solution:

- Dynamic window matching (ICDCS'21) algorithm to for noisy side channel signal alignments
- Trusted integrity verifier (DSN'21) to verify 3D printer design files using AI and finite element analysis





Scientific Impact:

- our signal alignment and intrusion detection algorithms can work on any CPS side-channels
- Our trusted integrity verifier follows the same idea as our trusted safety verifier (NDSS'14) paper for PLC control logics

Broader Impact:

- Additive manufacturing facilities ensure structural integrity of the printed objects against attacks
- Those facilities ensure design confidentiality against intrusions
- Worked with undergraduates; regularly with a female high school student (admitted to Cornell)