CPS: Medium: Collaborative Research: Trustworthy Cyber-Physical Additive Manufacturing with Untrusted Controllers

PIs: Raheem Beyah (GaTech) and Saman Zonouz (Rutgers University)
Students: Sizhuang Liang, Sriharsha Etigowni, Tuan Le, Mingbo Zhang

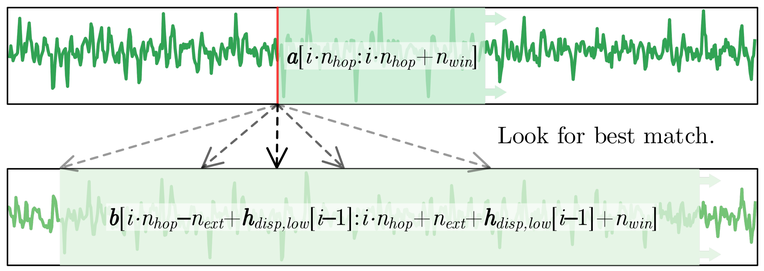
The goal is to protect additive manufacturing systems from cyberattacks by analyzing the side-channel signals in a printing process. For this purpose, we propose NSYNC, the first practical framework to effectively compare side-channel signals for intrusion detection. The core of NSYNC is an algorithm called Dynamic Window Matching (DWM), which replaces Dynamic Time Warping (DTW).

Scientific Challenges

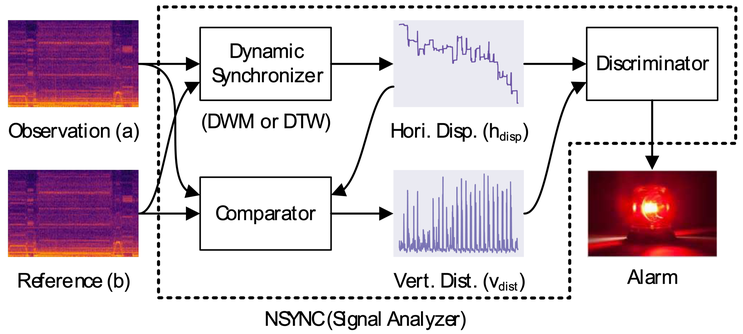
- Compare long signals that are out-of-alignment and possess different paces.
- Determine the thresholds for intrusion detection.
- Study different side channels to ascertain which side channels are effective for intrusion detection.

Scientific Impact

- The proposed Dynamic Window Matching (DWM) algorithm can be used to analyze general signals, as an effectively replacement for Dynamic Time Warping (DTW).
- The proposed method can be used to monitor a broader range of cyber-physical systems, not just AM systems.



Dynamic Window Matching (DWM). The core idea of DWM is to establish a pair of linked sliding windows on the signals to be compared. The relative displacement between the windows is kept track of. As the windows slide, we perform Time Delay Estimation (TDE) to update the relative displacement.



Overview of NSYNC. The most important component of NSYNC is the dynamic synchronizer, typically implemented by DWM. The discriminator uses One-Class Classification (OCC) to determine the best thresholds for intrusion detection. This system can reach an accuracy of 0.99, outperforming existing IDSs, whose accuracy ranges from 0.50 to 0.88.

Broader Impact

- Researchers and engineers who deal with signals might be interested in the newly proposed DWM algorithm. DWM is an effective alternative to the well-known DTW algorithm, which finds wide applications in speech processing, gene analysis, etc.
- NSYNC can be combined with computer vision to automatically analyze process monitoring videos. We are design a project for students to practice their research skills by using NSYNC with deep networks to perform automatic process monitoring.

2021 NSF Cyber-Physical Systems Principal Investigators' Meeting
June 2-4, 2021

Award ID#: 1739259