Detection and Defense of cyber-physical attacks

GT SSLR 2021 presentation

HOUSSEIN MERANEH Awaleh, Marc-Oliver Pahl and Hélène Le Bouder

IMT Atlantique

10/2020 - 10/2023

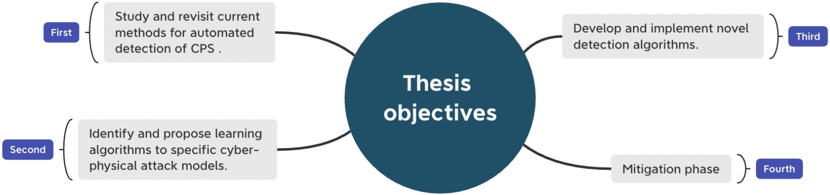
Plan

1. Thesis context: objectives and research questions.
2. State-of-the-art:
   - Review Anomaly Detection methods of CPS.
   - Side-channels based intrusion detection.
3. Current work.
4. Conclusion and references.

Thesis context

Research Questions and Thesis objectives

1. How to detect cyber-physical attacks using the side-channels based intrusion detection?
   - What are the most relevant attacks against the CPS (cyber-physical systems)?
   - What it is the side-channels based intrusion detection for CPS?


Thesis objectives
First
Study and revisit current methods for automated detection of CPS .
Second
Identify and propose learning algorithms to specific cyber-physical attack models.
Third
Develop and implement novel detection algorithms.
Fourth
Mitigation phase

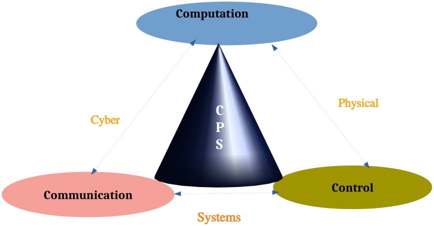
Definition and application of CPS

CPS definition [Lee06]

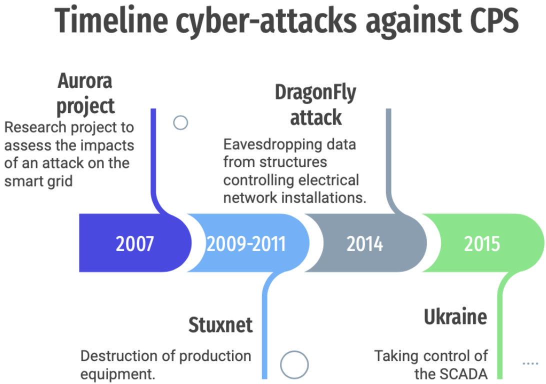
The CPS is defined as the combination of digital and physical components that interact via a communication network.

The CPS application are:

- IoT and communication
- Robotics
- Health care
- Military
- Transportation
- Industrial



Cyber-attacks against CPS



Timeline cyber-attacks against CPS

Aurora project
Research project to assess the impacts of an attack on the smart grid

2007

Stuxnet
Destruction of production equipment.

2009-2011

DragonFly attack
Eavesdropping data from structures controlling electrical network installations.

2014

Ukraine
Taking control of the SCADA

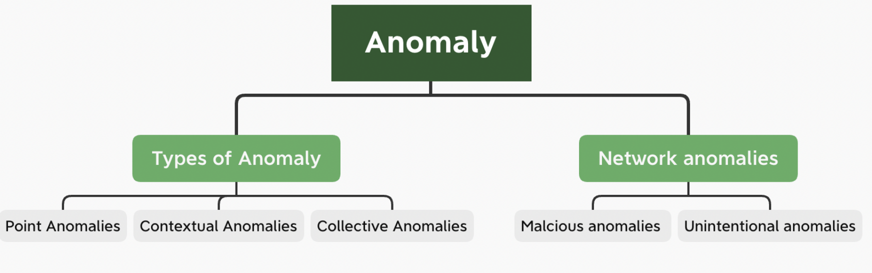
2015

....

↪ Ensuring the security of the CPS is important and essential.

State-of-the-art

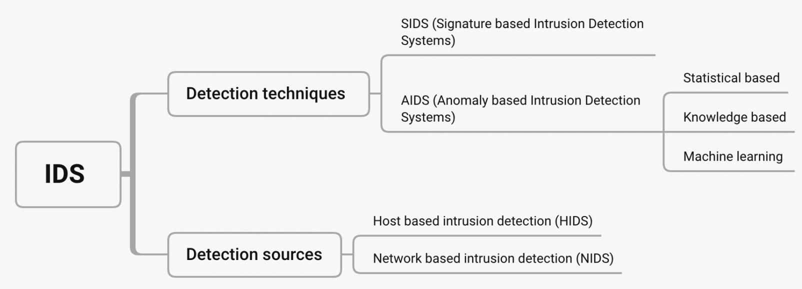
Background of anomalies detection [CBK09]



The application domains of Anomaly Detection are:

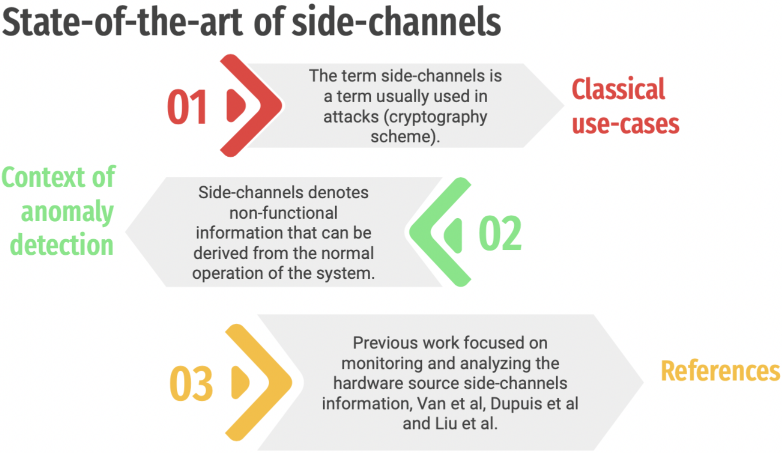
- Intrusion Detection
- Fraud Detection
- Fault/Dammage Detection
- ...etc

Overview of Intrusion Detection Systems (IDS) of CPS [MC14]


IDS
Detection techniques
SIDS (Signature based Intrusion Detection Systems)
AIDS (Anomaly based Intrusion Detection Systems)
Statistical based
Knowledge based
Machine learning
Detection sources
Host based intrusion detection (HIDS)
Network based intrusion detection (NIDS)

↪ Combine several detection techniques to finally have a solid protection method against cyber-physical attacks.

Side-channels based intrusion detection methods [BGH]



State-of-the-art of side-channels

01 The term side-channels is a term usually used in attacks (cryptography scheme).

Classical use-cases

02 Side-channels denotes non-functional information that can be derived from the normal operation of the system.

Context of anomaly detection

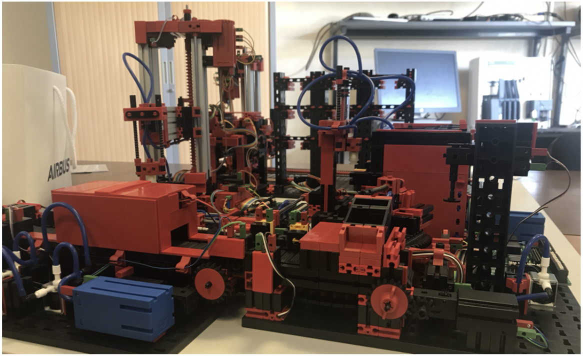
03 Previous work focused on monitoring and analyzing the hardware source side-channels information, Van et al, Dupuis et al and Liu et al.

References

Current work

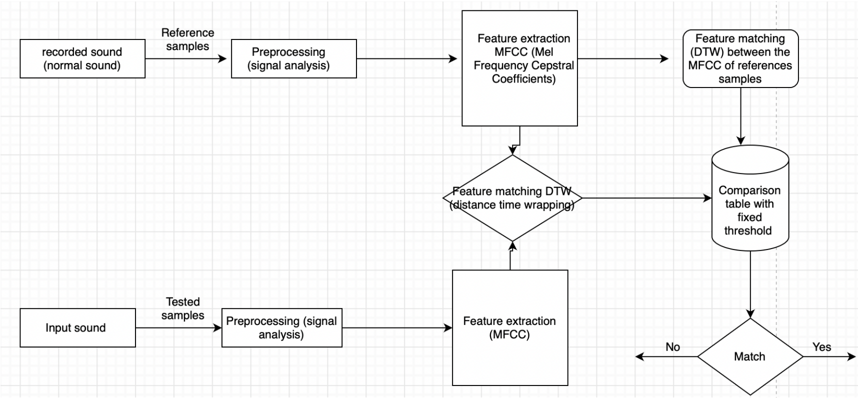
Prototype description

Fishertechnic models



- Pneumatic processing center.
- Conveyor Belt.
- Indexed line.
- Robot Arm.

Sound Detection Approach



recorded sound (normal sound)

Reference samples

Preprocessing (signal analysis)

Feature extraction MFCC (Mel Frequency Cepstral Coefficients)

Feature matching (DTW) between the MFCC of references samples

Feature matching DTW (distance time wrapping)

Comparison table with fixed threshold

Input sound

Tested samples

Preprocessing (signal analysis)

Feature extraction (MFCC)

Conclusion

- Review Anomaly Detection methods of CPS (survey).
- Study the side-channels intrusion detection techniques in ICS.
- Experiment the sound detection approach.

References

Roland Bolboacă, Béla Genge, and Piroska Haller.
Using side-channels to detect abnormal behavior in industrial control systems.

Varun Chandola, Arindam Banerjee, and Vipin Kumar.
Anomaly detection: A survey.
ACM computing surveys (CSUR), 41(3):1–58, 2009.

Edward A Lee.
Cyber-physical systems-are computing foundations adequate.
In *Position paper for NSF workshop on cyber-physical systems: research motivation, techniques and roadmap*, volume 2, pages 1–9. Citeseer, 2006.

Robert Mitchell and Ing-Ray Chen.
A survey of intrusion detection techniques for cyber-physical systems.
ACM Computing Surveys (CSUR), 46(4):1–29, 2014.