Cyber-physical attacks detection mechanisms: Case Study Autonomous Systems

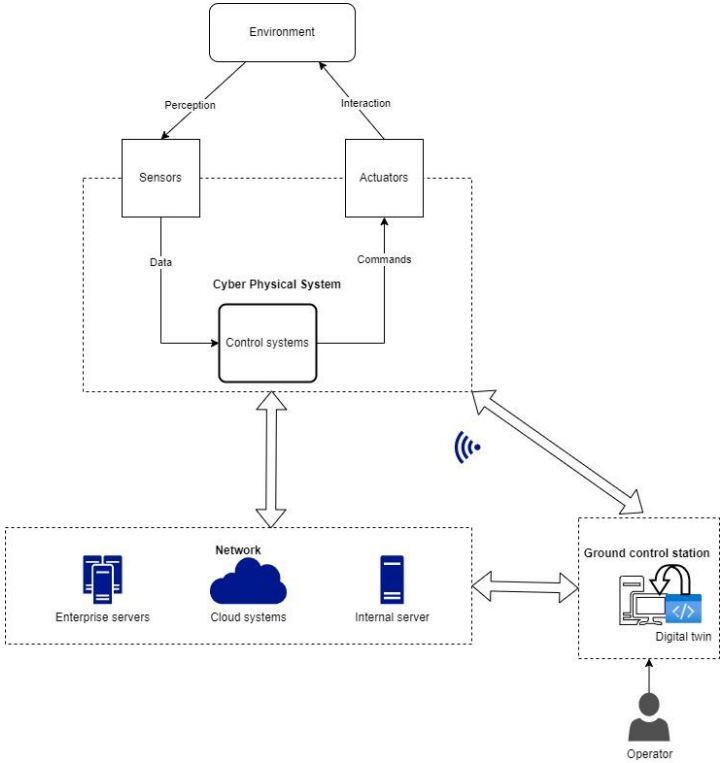
Asmae Bni

Norwegian University of Science and Technology

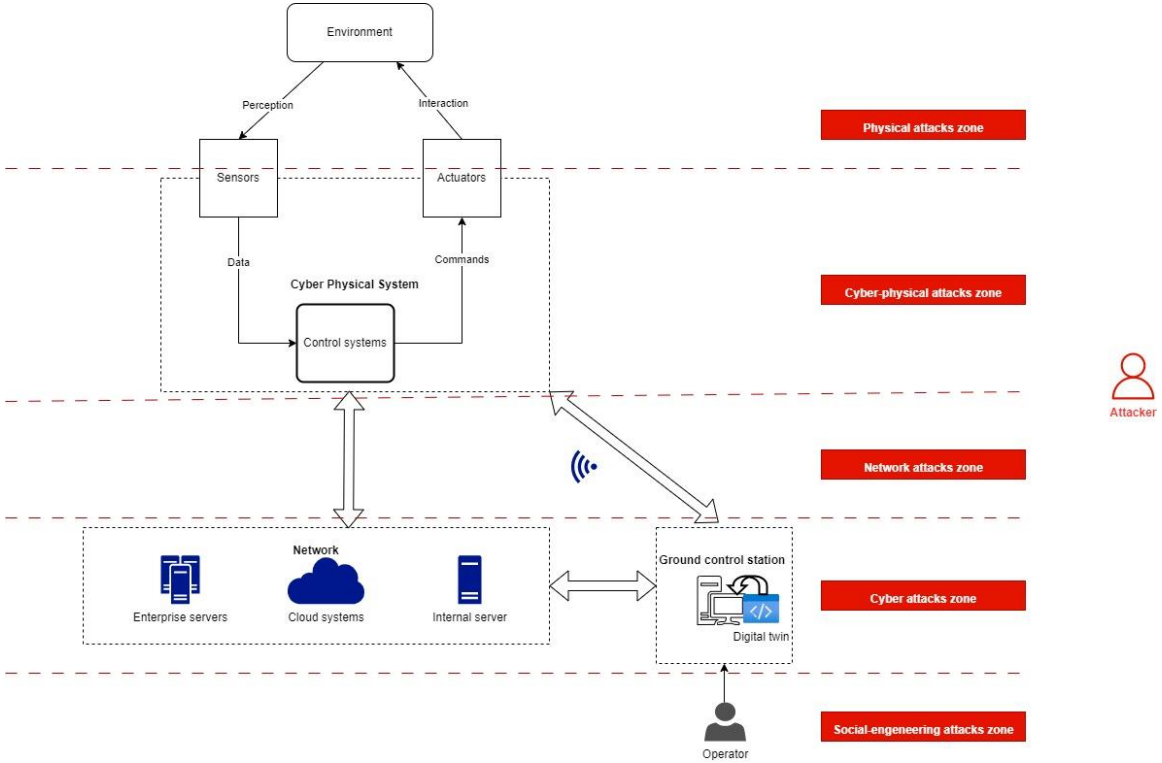
Agenda

- Autonomous system model
- Cyber-physical threats analysis
- Intrusion detection strategies
- Limitations and research gap

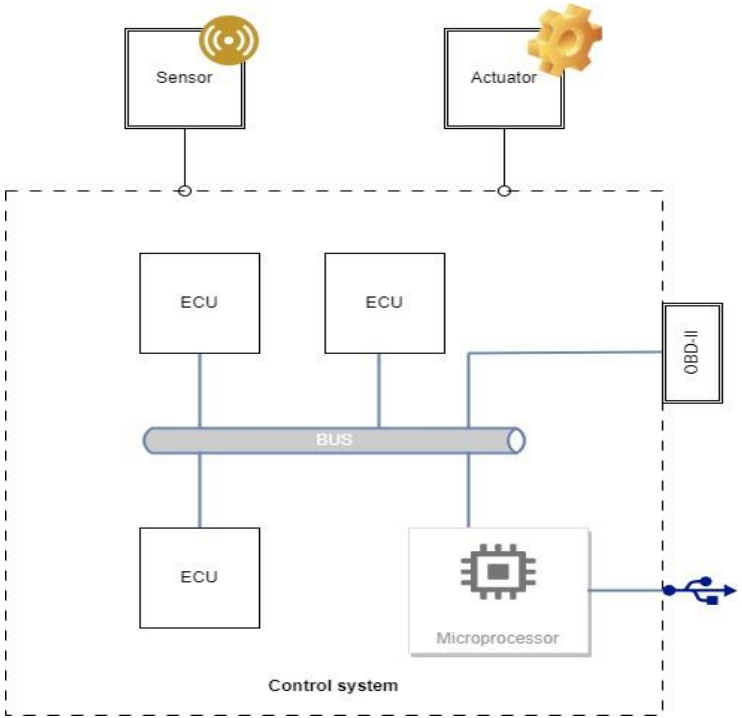
Autonomous system model



Autonomous system model



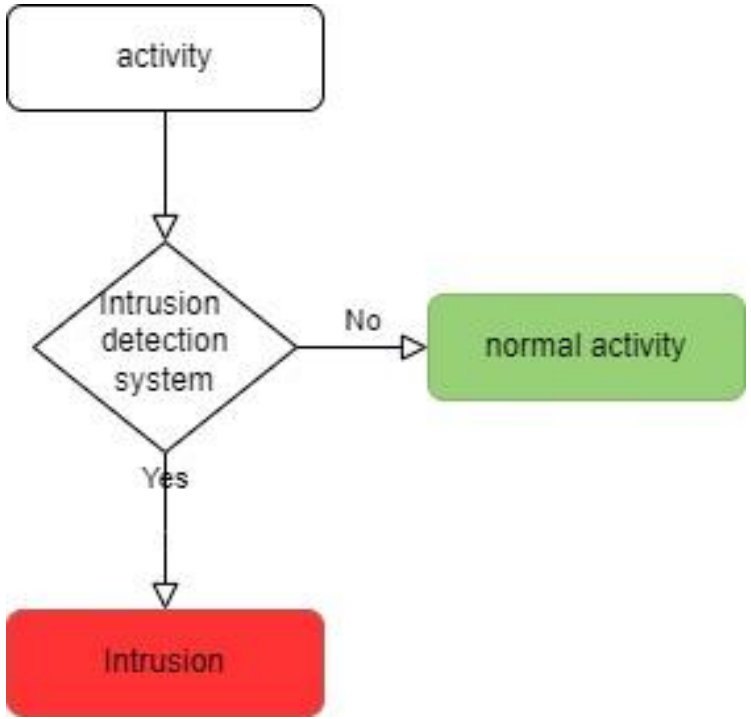
Cyber-physical threats



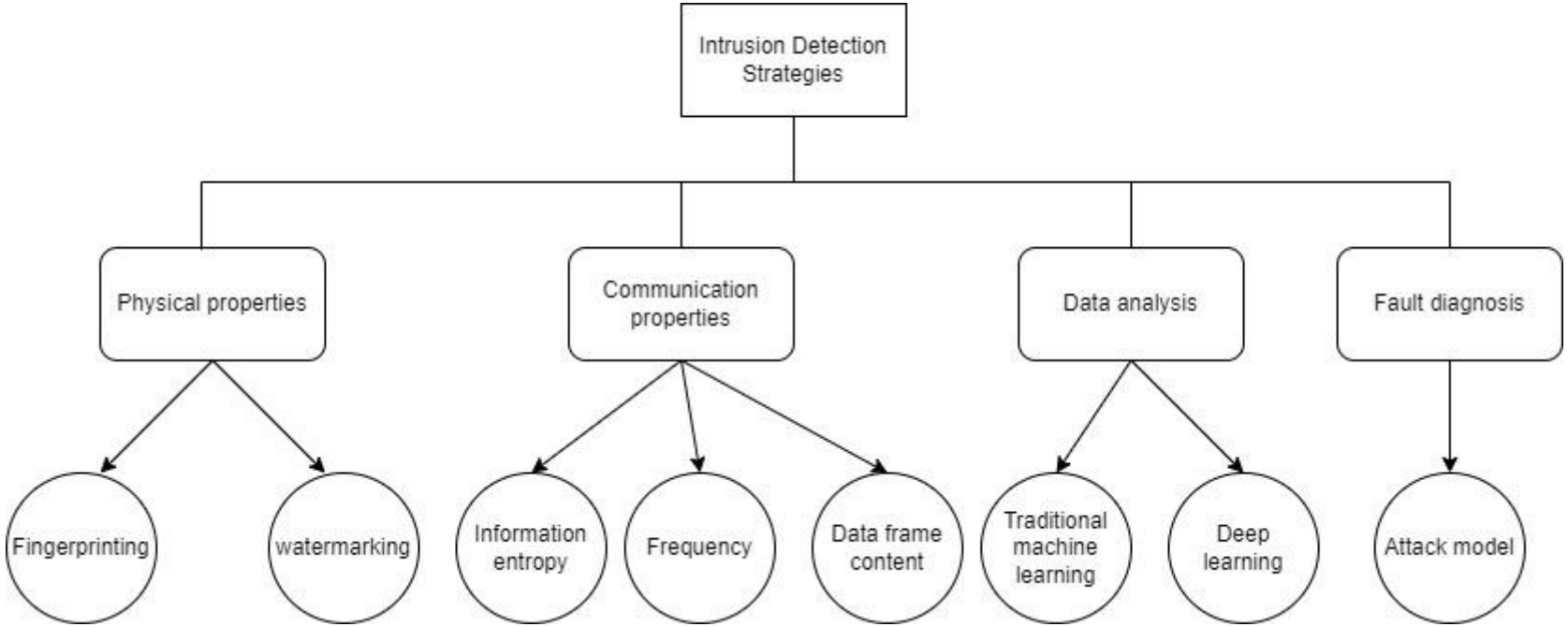
cyber physical attacks zone	
Spoofing	• Sybil attacks • Replay attacks • Impersonation attacks • Remote sensor attacks
Tampering	• Data injection attacks • Sensor confusion attacks • Masquerade attacks • Actuator control acquisition
Denial of service	• Jamming attacks • Bus-off attacks
Information disclosure	• side-channel attacks

Intrusion Detection Systems

Hardware or software systems that are designed to identify unusual, malicious or suspicious activity.



Intrusion Detection Systems



Intrusion detection strategies

based on physical properties

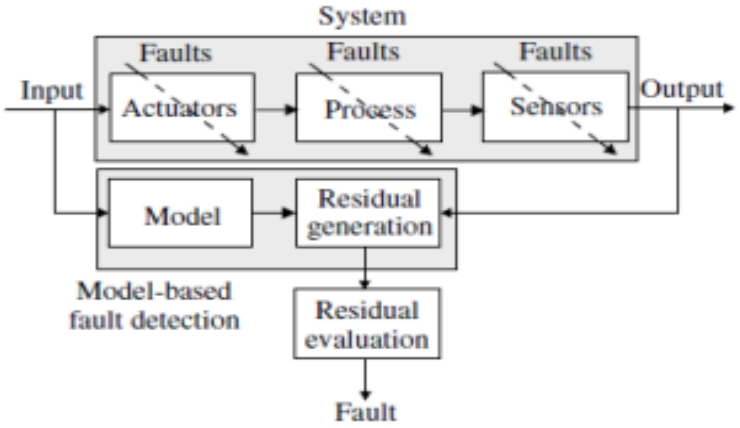
- **Fingerprinting** is computing a hardware characteristic to create a fingerprint to identify the source device of the transferred message on the bus.
- **Physical watermarking** is a technique to detect spoofing attacks by injecting a secret noisy signal that trace the origin of the received observation or measurement and helps to determine its authenticity.

Intrusion detection strategies
based on communication properties

- Training stage to collect and analyze data related to the parameters:
  - **Information entropy**
  - **Frequency**
  - **Data frame content**
- The baseline is computed and referred to as the normal value or expected behavior.
- Anomalies that differs from the baseline are identified as potential attacks.

Intrusion detection strategies
based on fault diagnosis

- The fault detection algorithm generates residual values using the formal system model and the external observer model.
- The observer model is generated based on the attack model that should be detected by the fault diagnosis scheme.
- The computed residuals values are compared to a detection threshold or filter.



Maryam Naghdi,Mohamad Ali Sadrnia, Javad Askari
Fault Detection and Isolation for Nonlinear System via ESO.
January 2014International Journal of Computer Applications 88(16)
DOI:10.5120/15434-3663

Intrusion detection strategies

based on data analysis

- Machine learning techniques uses training datasets to classify anomalies or predict malicious activities.
- Machine learning based IDS have been applied to:
  - Network data

    Ex. Raw network packets
  - Sensor generated data

    Ex. Camera imaging, LiDAR point clouds

Limitations and research gap

- Trade-off between security and computational constraints of autonomous cyber physical systems.
  - ➢ Design lightweight IDS solutions.
- Lack of datasets to study unknown threats or emergent behaviors of the autonomous systems.
  - ➢ Develop advanced fuzz testing approaches.
- Physical based IDS do not identify effeciently compromised or corrupted sensors.
  - ➢ Improve and fuse physical based IDS with other IDS methods.

Thank you!