Improving Security and Resilience of Cyber Physical Systems

Riccardo Orizio, Prof. Gregory Provan
University College Cork

General Problem

Cyber Physical Systems are systems made of three main parts: physical processes, computational resources and communication capabilities. These systems can represent many real systems, including complex and safety critical ones such as transportation networks, electrical and gas distribution, water treatment plants and SCADA systems. These critical systems need to operate reliably in all circumstances, therefore they need to be able to recover from faulty components behaviours as well as from external malicious attacks.
Our goal is to improve the resiliency of the system, starting from the current most used model based approach and expanding to new techniques.

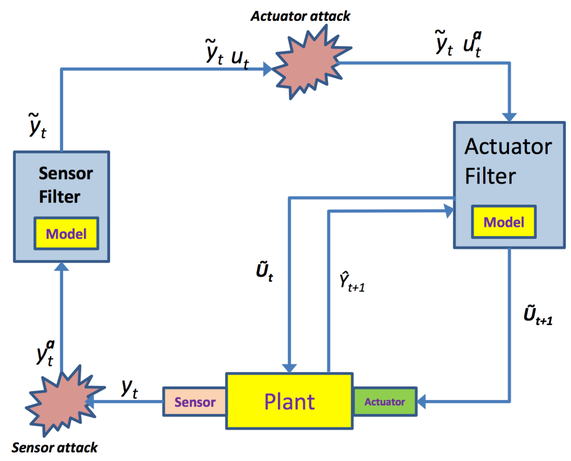
Distinguishing Faults from Attacks

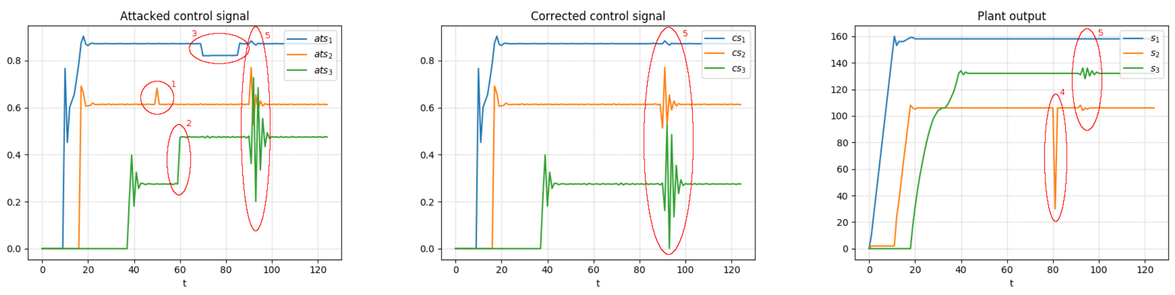
To improve the system security and resiliency we need to:

- **Detect** the unusual behaviour;
- **Identify** the component causing the anomaly;
- **Distinguish** the cause of the anomaly, either fault or attack.

In order to achieve our purpose, we introduced two components to the system:

Sensor filter: estimates the state of components knowing the sensors data.
Actuator filter: helps distinguishing the anomaly by delaying the current control signal of one step.





Model Based Approach

A system can operate in different modes (e.g. some drone operating modes can be taking-off, landing, wandering, surface-mapping, etc...). Each mode can be identified through a mathematical model, knowing its current internal state x_i:

$$\text{Modes}: \begin{cases} y_{m_1} = f_1(x_i) \\ y_{m_2} = f_2(x_i) \\ \quad \dots \\ y_{m_n} = f_n(x_i) \end{cases}$$

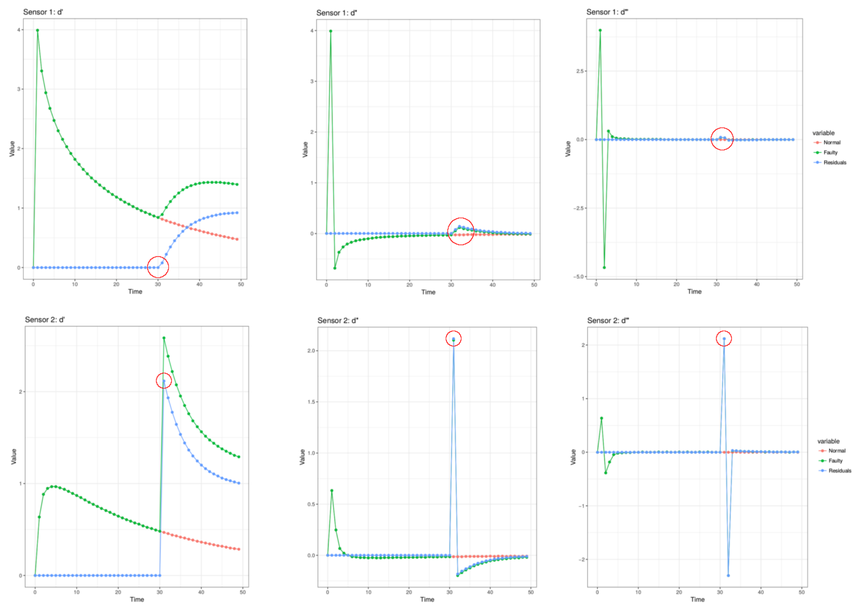
Forward inference: compute the mode behaviour $y_j = f_j(x_i)$

Inverse inference: find the internal state that led to the current behaviour $x_i = f_j^{-1}(y_j)$
The inverse inference is a difficult procedure to perform when f_j is linear, in most CPS these modes are non-linear.

Diagnosis: inverse inference including faulty modes in the set of modes.

Data Driven Algebraic approach

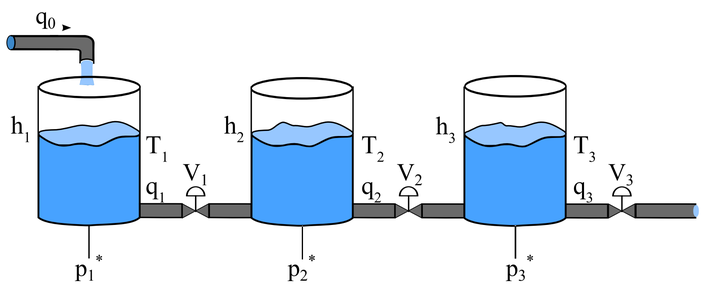
- System's sensors data and its derivatives analysis (derivatives studied up to third order);
- Looking for unusual *peaks* in the data behaviour and their neighborhood.



Model Based or Algebraic approach?

We compared the two approaches on the same set of experiments, finding:

- Algebraic approach seems better;
- Masked multi-anomalies and synergistic behaviours seem to be easier to detect with the algebraic approach than it is with the model based one.



Method	Faults	Detected	False Positive	Missed	FR
Model based	78	53	32	25	0.345
AvF	78	57	15	21	0.607
IAA	78	54	8	24	0.597

Papers contribution

- *Physics-Based Methods for Distinguishing Attacks from Faults*, CENICS 2017
- *Comparing Physics-Based Methods for Distinguishing Attacks from Faults*, DX'18
- *Physics-Based Methods for Responding to Attacks and Faults*, WIP

Future

- Integrate machine learning techniques to make the procedure self-aware to different behaviours and their classification;
- Signal Temporal Logic approach for diagnosis;
- Extension to other real-world applications (e.g. FCU).