Improving security and resilience of Cyber Physical Systems

Riccardo Orizio
Prof. Gregory Provan

Department of Computer Science
University College Cork

04 September 2018

Cyber Physical Systems

Cyber Physical Systems are made of three main parts:

- physical processes;
- computational resources;
- communication infrastructures.

Cyber Physical Systems

Cyber Physical Systems are made of three main parts:

- physical processes;
- computational resources;
- communication infrastructures.

Most real systems can be represented with this structure, i.e., transportation networks, electrical and gas distribution systems, water treatment plants, etc...

Cyber Physical Systems

Cyber Physical Systems are made of three main parts:

- physical processes;
- computational resources;
- communication infrastructures.

Most real systems can be represented with this structure, i.e., transportation networks, electrical and gas distribution systems, water treatment plants, etc...

These systems have to be reliable at all time and in all circumstances. Especially when anomalies occur, regardless of their nature, the system needs to react and overcome the issue.

Stuxnet: real life scenario threat

A malicious computer worm created in 2005 by American/Israeli governments to damage Iran's nuclear program;

Stuxnet: real life scenario threat

A malicious computer worm created in 2005 by American/Israeli governments to damage Iran's nuclear program;

Target SCADA infrastructure and PLC systems to physically compromise their centrifuges and reduce their overall productivity;

Stuxnet: real life scenario threat

A malicious computer worm created in 2005 by American/Israeli governments to damage Iran's nuclear program;

Target SCADA infrastructure and PLC systems to physically compromise their centrifuges and reduce their overall productivity;

Discovered only in 2010 because it spread itself too far.

Question

Can we create a tool that can help these systems in detecting, identifying and correcting an anomaly whenever one would occur?

Question

Can we create a tool that can help these systems in detecting, identifying and correcting an anomaly whenever one would occur?

Can it be used for real time systems?

Question

Can we create a tool that can help these systems in detecting, identifying and correcting an anomaly whenever one would occur?

Can it be used for real time systems?

And can it be an all purpose tool used on a wide variety of different systems?

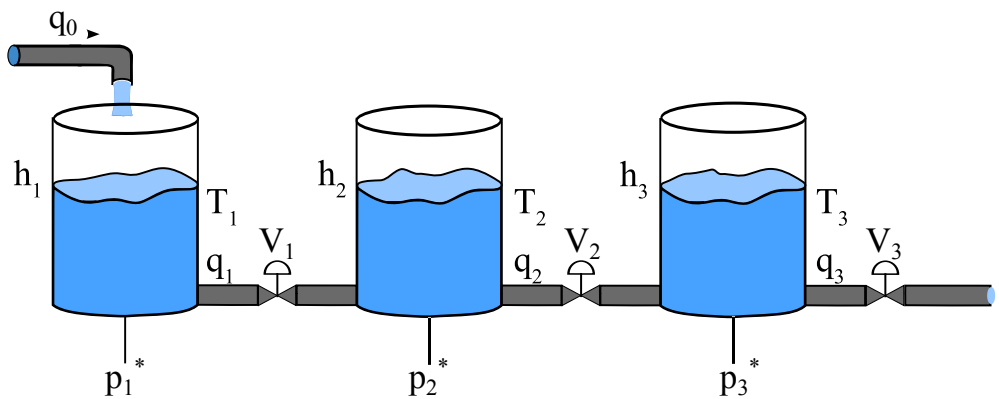
Research method

Experimental based approach;

Research method

Experimental based approach;

Currently experimenting on simulations of the three tanks model and its variations.



Model based approach

A CPS model can operate in different behaviours, called modes:

$$Modes : \begin{cases} y_{m_1} = g_1(x) \\ ... \\ y_{m_i} = g_i(x) \end{cases}$$

Model based approach

A CPS model can operate in different behaviours, called modes:

$$Modes: \begin{cases} y_{m_1} = g_1(x) \\ ... \\ y_{m_i} = g_i(x) \end{cases}$$

Diagnosis is an inverse inference on the modes set:

$$x = g_i^{-1}(y_i)$$

In most cases $g(\cdot)$ is non-linear.

Model based approach

A CPS model can operate in different behaviours, called modes:

$$Modes: \begin{cases} y_{m_1} = g_1(x) \\ ... \\ y_{m_i} = g_i(x) \end{cases}$$

Diagnosis is an inverse inference on the modes set:

$$x = g_i^{-1}(y_i)$$

In most cases $g(\cdot)$ is non-linear.

Multi modes simultaneously active will increase exponentially the inverse inference computation.

Residual study approach

Study the system only from the data provided from their sensors;

Residual study approach

Study the system only from the data provided from their sensors;

Residual: $r_i = y_{real_i} - y_{nominal_i} \ \forall i \in \{sensors\}$;

Residual study approach

Study the system only from the data provided from their sensors;

Residual: $r_i = y_{real_i} - y_{nominal_i} \ \forall i \in \{sensors\}$;

Anomaly identification activated iff $r > \delta$, studying the systems' sensors data and their first derivative;

Residual study approach

Study the system only from the data provided from their sensors;

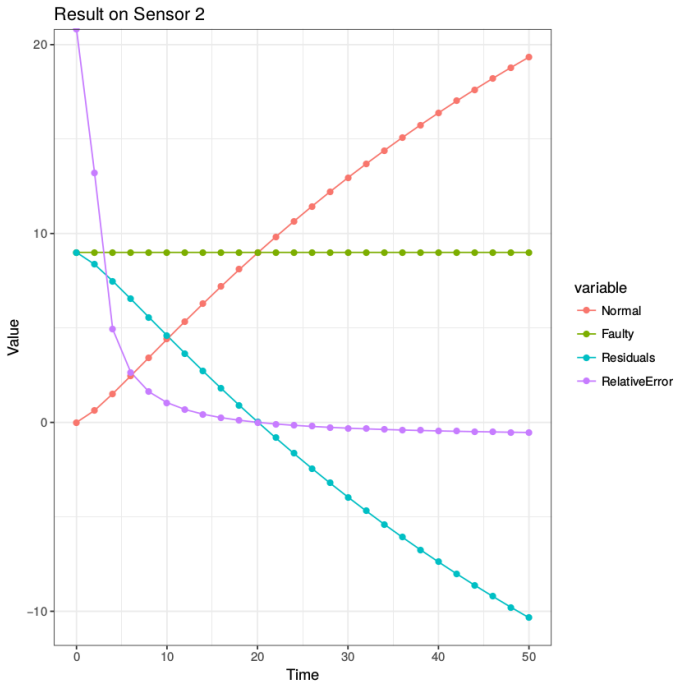
Residual: $r_i = y_{real_i} - y_{nominal_i} \ \forall i \in \{sensors\}$;

Anomaly identification activated iff $r > \delta$, studying the systems' sensors data and their first derivative;

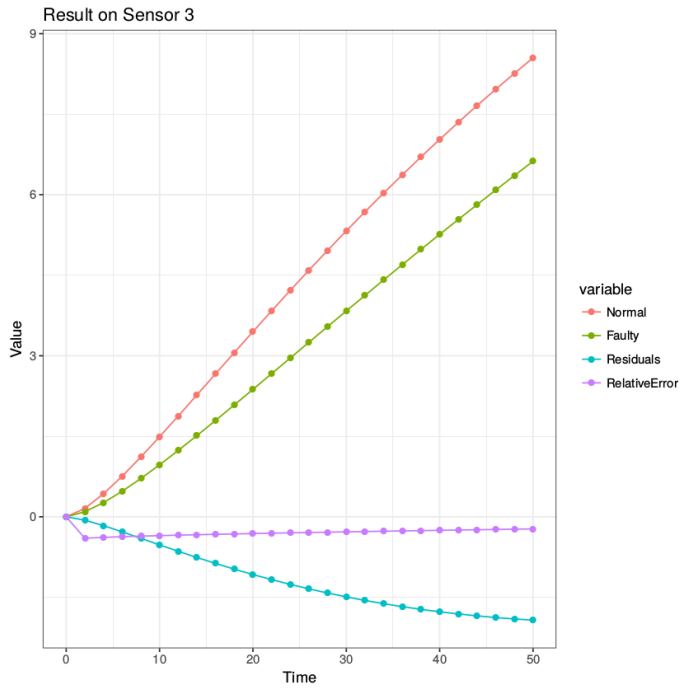
Results:

- Primitive and basic approach;
- Able to recognize some simple attacks;
- Plenty of false positives when the anomalies affects the internal components of the system.

Residual study results



A sensor of the system is attacked. Identifiable through: $\dot{y}_k = -\dot{r}_k$.



Synergies of the system make it harder to identify the anomaly.

Algebraic approach

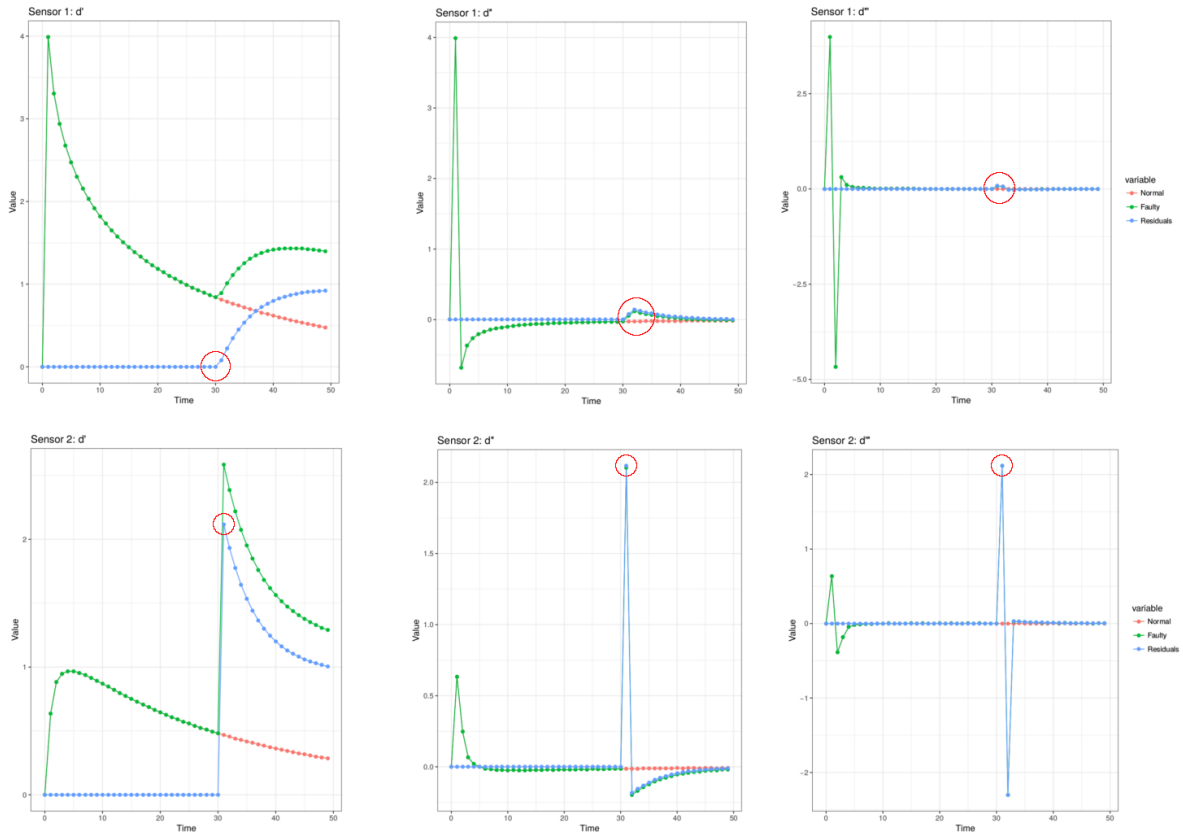
Basic: Extend the sensors data study to higher order derivatives looking for particular patterns that could identify the anomalies;

Algebraic approach

Basic: Extend the sensors data study to higher order derivatives looking for particular patterns that could identify the anomalies;

Improved: Use the patterns to find anomalies masked from other anomalies.

Example



Peculiar pattern of an actuator attack on the system and its side effects.

Data driven approach

Can we identify anomaly patterns automatically?

Data driven approach

Can we identify anomaly patterns automatically?

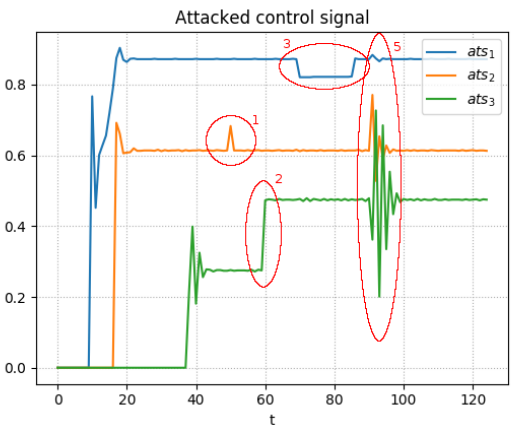
Classification of the anomalies' data behaviours through SVM, LSTM and HMM.

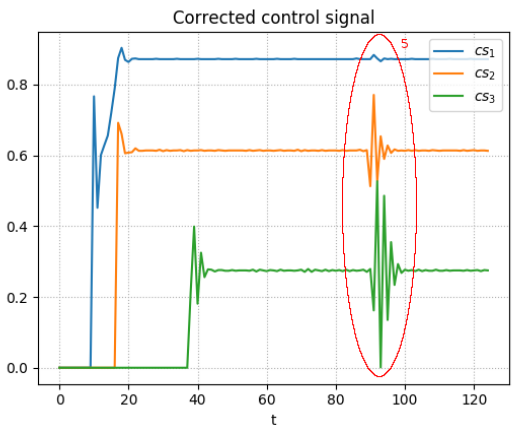
Results compared

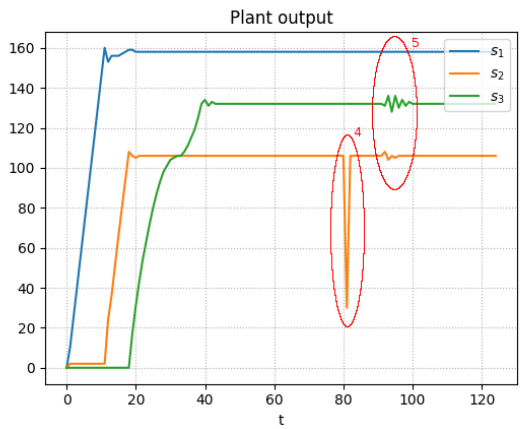
Method	Faults	Detected	False Positive	Missed	FR
Model based	78	53	32	25	0.345
AvF	78	57	15	21	0.607
IAA	78	54	8	24	0.597

Comparing the results of all the approaches studied to this point. The algebraic approach seems the best so far.

Attack or fault distinction: a novel method







Using the system to understand if the control signal has been tampered.

Future

Identify a small set of the best approaches for the diagnosis process, focusing mainly on data driven ones;

Increase the diagnosis efficacy combining different approaches;

Extend the tests to real systems;

Create a standalone diagnosis tool based on our method.


Thank
You