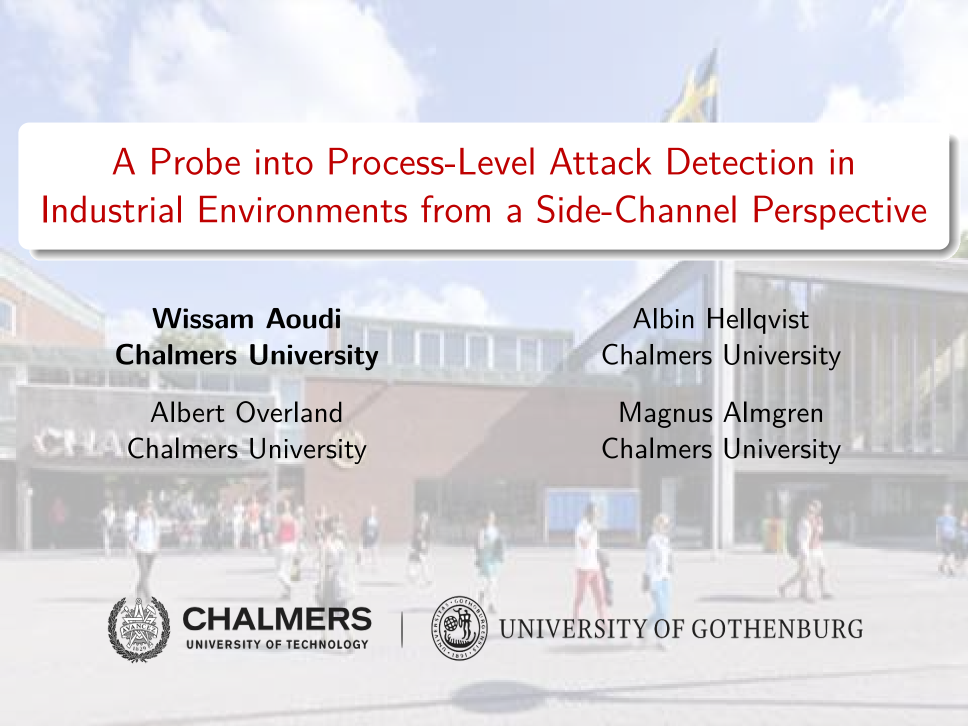


A Probe into Process-Level Attack Detection in Industrial Environments from a Side-Channel Perspective

Wissam Aoudi
Chalmers University

Albin Hellqvist
Chalmers University

Albert Overland
Chalmers University

Magnus Almgren
Chalmers University

CHALMERS UNIVERSITY OF TECHNOLOGY | UNIVERSITY OF GOTHENBURG

Industrial Control Systems

Industrial Control Systems (ICS)

- control industrial processes;
- typically operate on critical infrastructures.

Cyber-Attacks on ICS

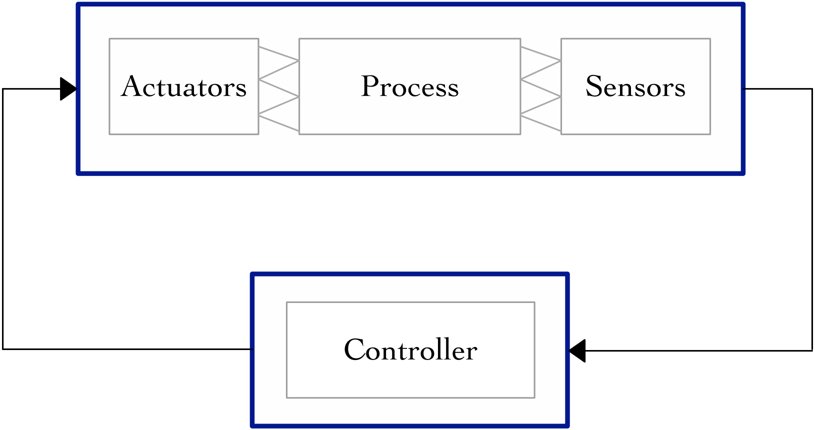
The Problem

- Attacks on ICS are increasing.
- Successful attacks on ICS
  - can be highly rewarding for attackers;
  - may have far-reaching consequences on society at large.
- Classical IT-based security is not sufficient.

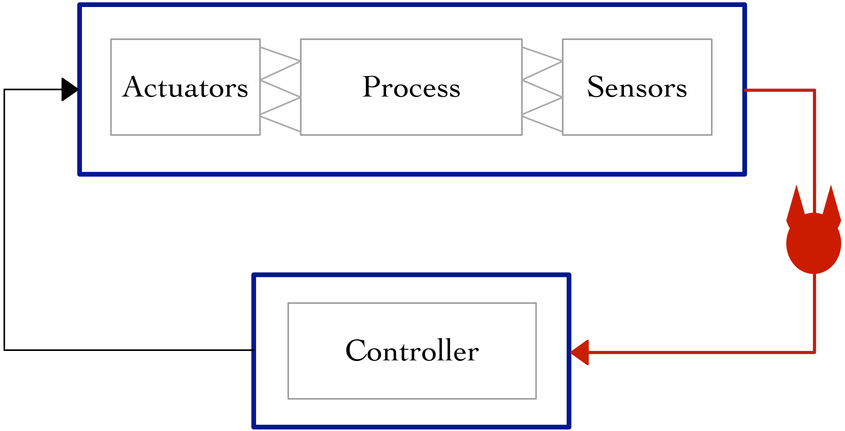
Process-Level Attack Detection

Why?	Because ICS combine both IT and OT technologies.
What?	Check if **physical process** deviates from **the norm**.
How?	By monitoring **process output** in real time.

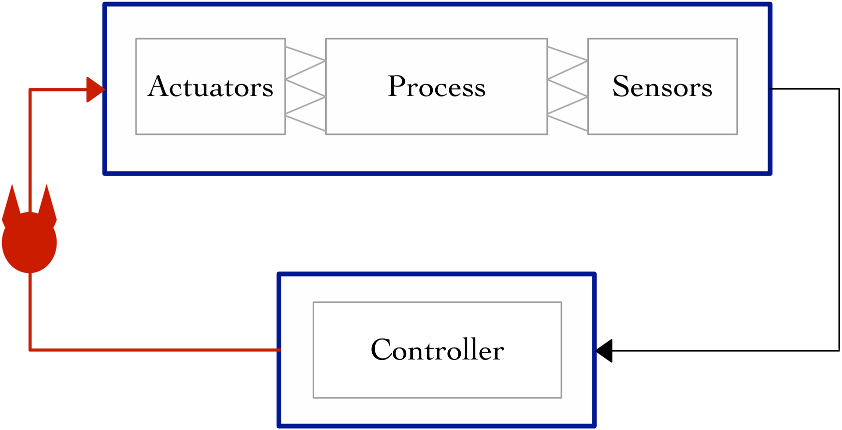
Control Loop and Attacker Model



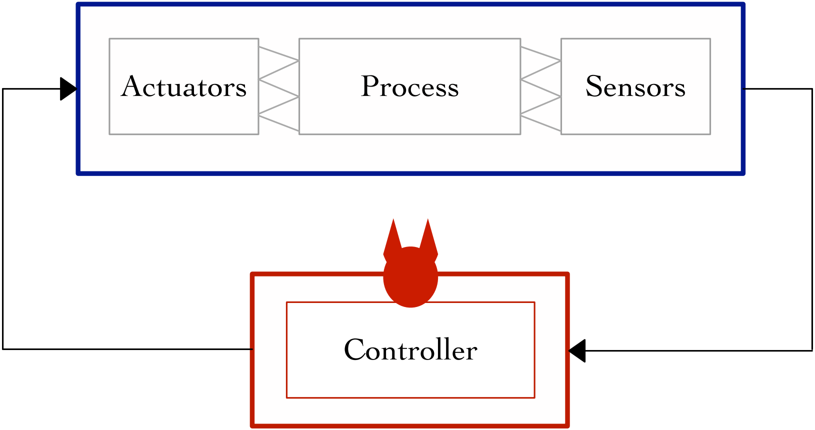
Control Loop and Attacker Model



Control Loop and Attacker Model



Control Loop and Attacker Model



ICS behavior is deterministic

ICS-Specific Features

- Controllers (e.g., PLCs) operate in a **cyclic** manner.
- Signals repeat ⇒ level of **determinism** is relatively high.
- Normal behavior can be **learned** or **modeled**.

ICS behavior is deterministic

ICS-Specific Features

- Controllers (e.g., PLCs) operate in a **cyclic** manner.

Regularity of ICS behavior enables data-driven approaches.

- Normal behavior can be **learned** or **modeled**.

Data-Driven Methods

Classical Approach

Build a model of the physical process

↓

Use the model to **predict** future system behavior

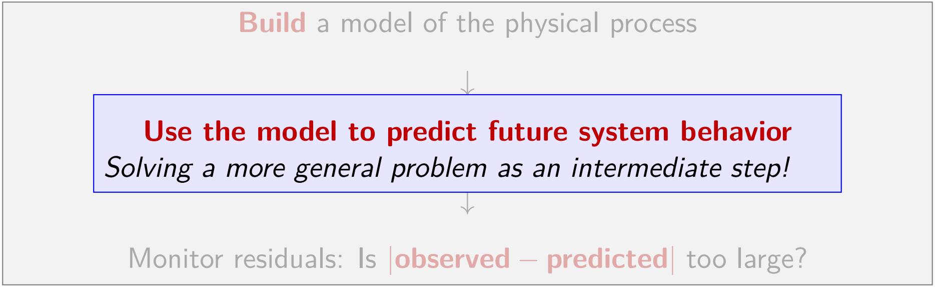
↓

Monitor residuals: Is |**observed** − **predicted**| too large?

Urbina, David I., et al. "Limiting the Impact of Stealthy Attacks on Industrial Control Systems." 2016 ACM Conference on Computer and Communications Security.

Data-Driven Methods

Classical Approach



Build a model of the physical process

↓

Use the model to predict future system behavior

Solving a more general problem as an intermediate step!

↓

Monitor residuals: Is $|\textbf{observed} - \textbf{predicted}|$ too large?

Urbina, David I., et al. "Limiting the Impact of Stealthy Attacks on Industrial Control Systems." 2016 ACM Conference on Computer and Communications Security.

PASAD: Process-Aware Stealthy-Attack Detection

PASAD

1. solves an easier problem;
2. requires limited knowledge of system dynamics;
3. is capable of detecting subtle changes in system behavior.

Wissam Aoudi, Mikel Iturbe, and Magnus Almgren. "Truth Will Out: Departure-Based Process-Level Detection of Stealthy Attacks on Control Systems." 2018 ACM SIGSAC Conference on Computer and Communications Security.

PASAD

1. solves an easier problem:

Learns normal behavior from historical data

↓

Measures to what extent **present** readings **conform** with the estimated dynamics.

Wissam Aoudi, Mikel Iturbe, and Magnus Almgren. "Truth Will Out: Departure-Based Process-Level Detection of Stealthy Attacks on Control Systems." 2018 ACM SIGSAC Conference on Computer and Communications Security.

PASAD

1. solves an easier problem:

Learns normal behavior from historical data

No need to predict the future!

Measures to what extent **present** readings **conform** with the estimated dynamics.

Wissam Aoudi, Mikel Iturbe, and Magnus Almgren. “Truth Will Out: Departure-Based Process-Level Detection of Stealthy Attacks on Control Systems.” 2018 ACM SIGSAC Conference on Computer and Communications Security.

PASAD

2. requires limited knowledge of system dynamics:

- It is entirely data-driven.
- Uses only **raw** sensor readings.
- It is model-free.

Wissam Aoudi, Mikel Iturbe, and Magnus Almgren. "Truth Will Out: Departure-Based Process-Level Detection of Stealthy Attacks on Control Systems." 2018 ACM SIGSAC Conference on Computer and Communications Security.

PASAD: Process-Aware Stealthy-Attack Detection

PASAD

2. requires limited knowledge of system dynamics:

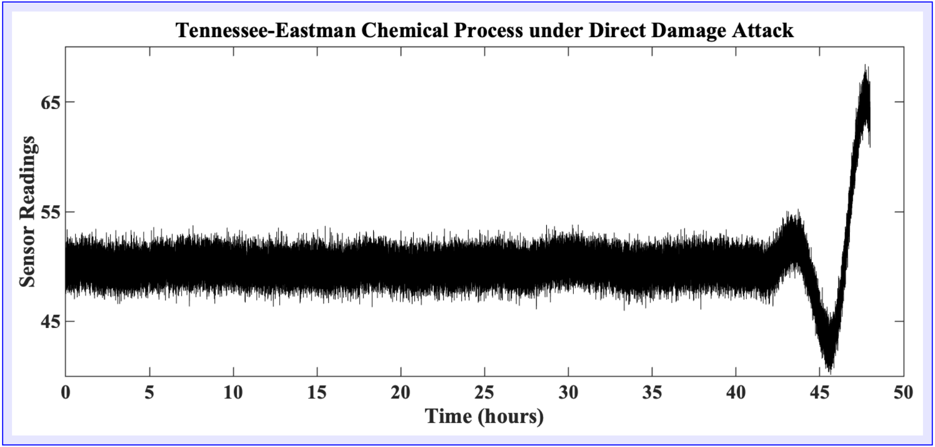
- It is entirely d
- Uses only **raw**
- It is model-free.

PASAD is specification-agnostic.
Applicable to various systems.

Wissam Aoudi, Mikel Iturbe, and Magnus Almgren. "Truth Will Out: Departure-Based Process-Level Detection of Stealthy Attacks on Control Systems." 2018 ACM SIGSAC Conference on Computer and Communications Security.

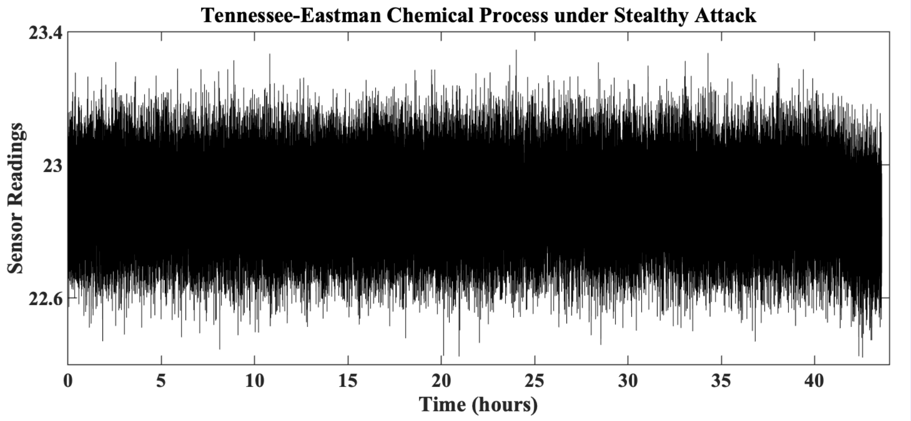
PASAD

3. is capable of detecting subtle changes in system behavior:



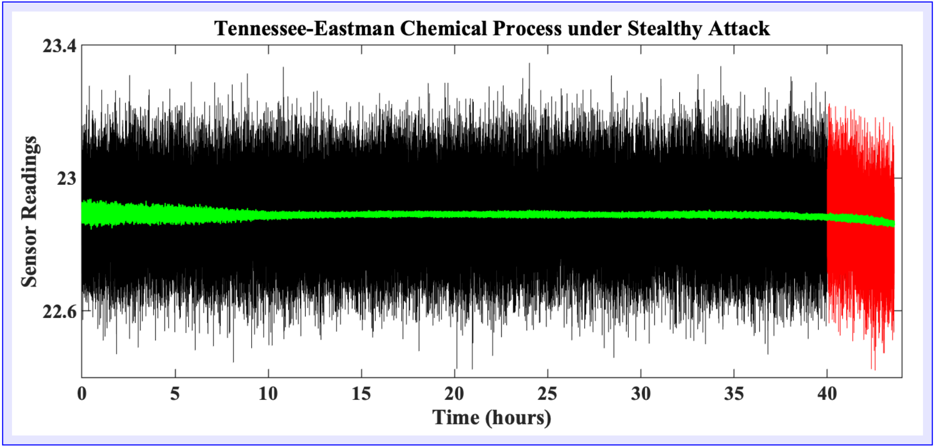
PASAD

3. is capable of detecting subtle changes in system behavior:



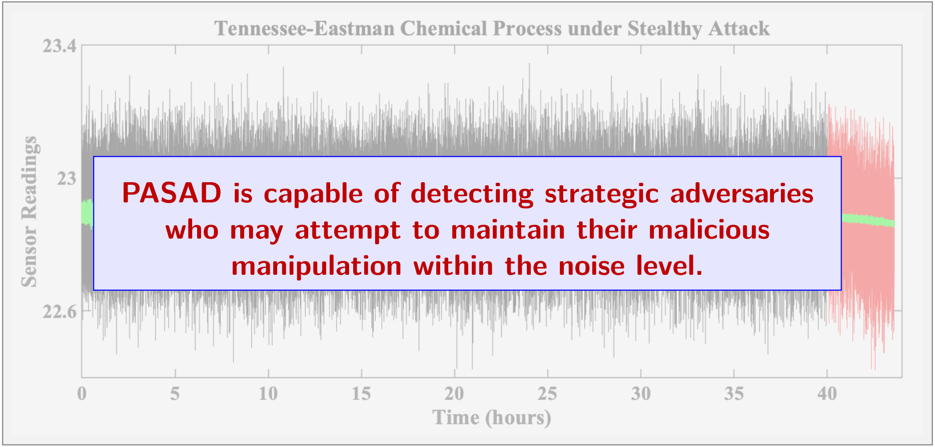
PASAD

3. is capable of detecting subtle changes in system behavior:



PASAD

3. is capable of detecting subtle changes in system behavior:



PASAD is capable of detecting strategic adversaries who may attempt to maintain their malicious manipulation within the noise level.

PASAD — Process-Aware Stealth-Attack Detection

Rationale: Detect attacks on ICS by monitoring sensor measurements for unusual behavior.

PASAD works in two phases: *Offline learning* and *online detection*.

PASAD — Process-Aware Stealth-Attack Detection

Rationale: Detect attacks on ICS by monitoring sensor measurements for unusual behavior.

PASAD works in two phases: *Offline learning* and *online detection*.
Learning Phase: Create a mathematical representation of the *norm*

- Extract noise-reduced signal information from noisy time series of sensor readings.
- Construct *Signal Subspace* and project training vectors.
- Compute centroid of the cluster formed by training vectors.

PASAD — Process-Aware Stealth-Attack Detection

Rationale: Detect attacks on ICS by monitoring sensor measurements for unusual behavior.

PASAD works in two phases: *Offline learning* and *online detection*.

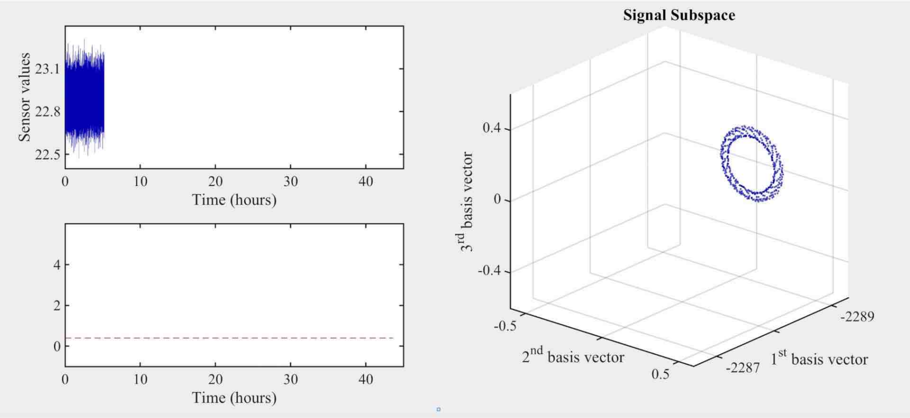
Learning Phase: Create a mathematical representation of the *norm*

- Extract noise-reduced signal information from noisy time series of sensor readings.
- Construct *Signal Subspace* and project training vectors.
- Compute centroid of the cluster formed by training vectors.

Detection Phase: Track distance from the centroid

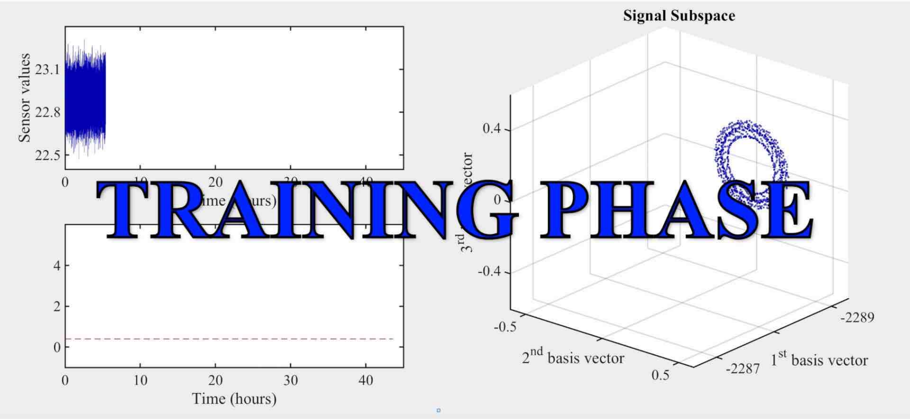
- Project most recent measurement vector onto the subspace.
- Compute a *departure score*: distance from the centroid.
- Raise an alarm if a certain threshold is crossed.

Validation — Visualizing the Departure



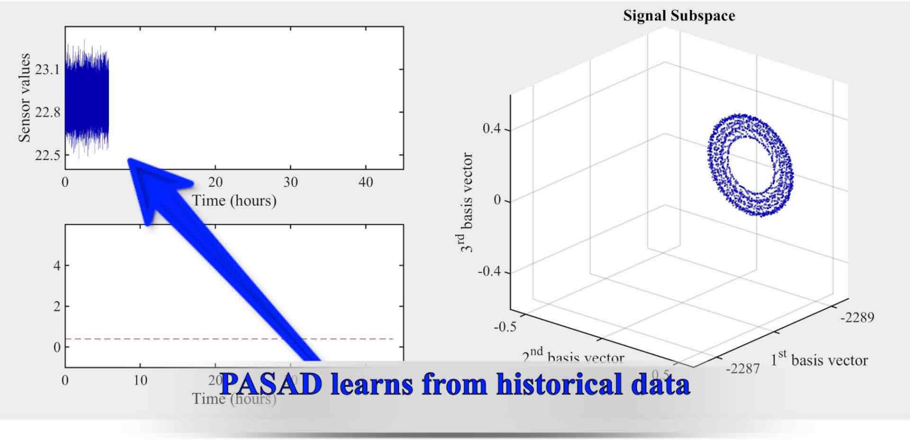
Watch the full video at https://youtu.be/SSs4IeM2MOs.

Validation — Visualizing the Departure



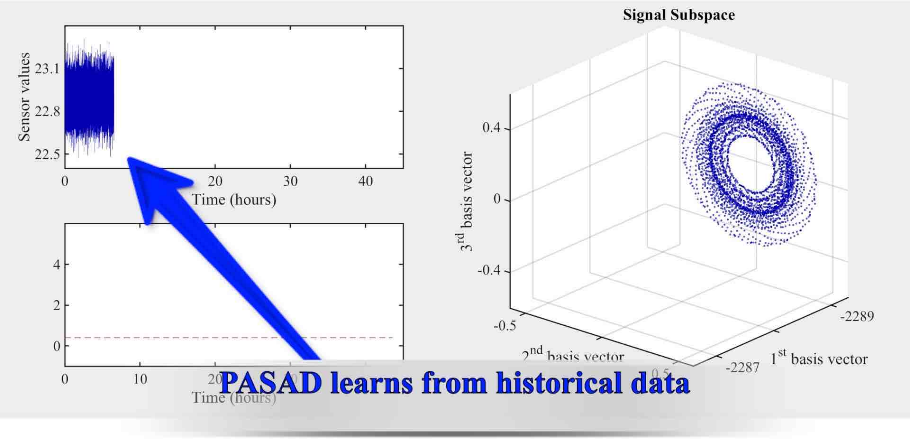
Watch the full video at https://youtu.be/SSs4IeM2MOs.

Validation — Visualizing the Departure



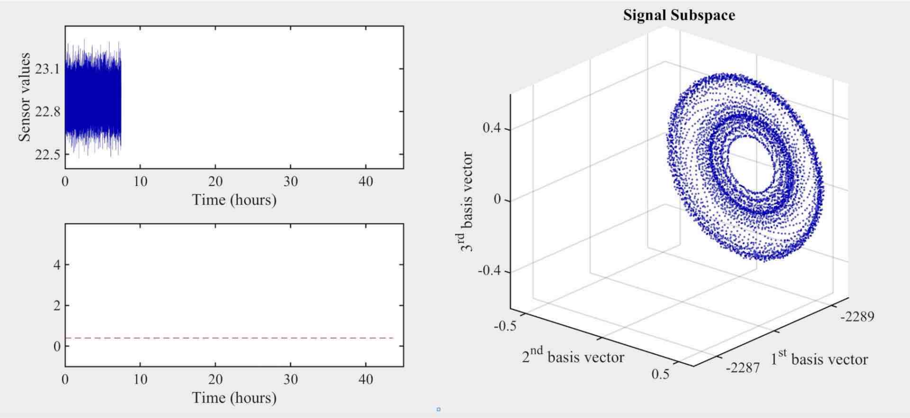
Watch the full video at https://youtu.be/SSs4IeM2MOs.

Validation — Visualizing the Departure



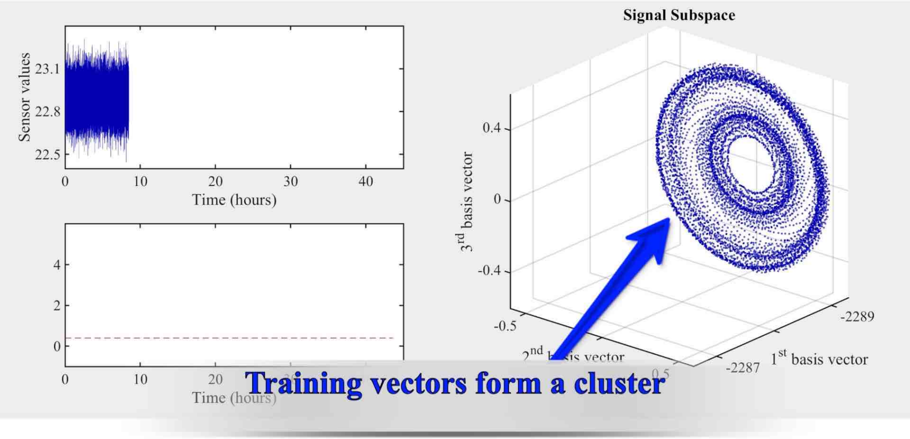
Watch the full video at https://youtu.be/SSs4IeM2MOs.

Validation — Visualizing the Departure



Watch the full video at https://youtu.be/SSs4IeM2MOs.

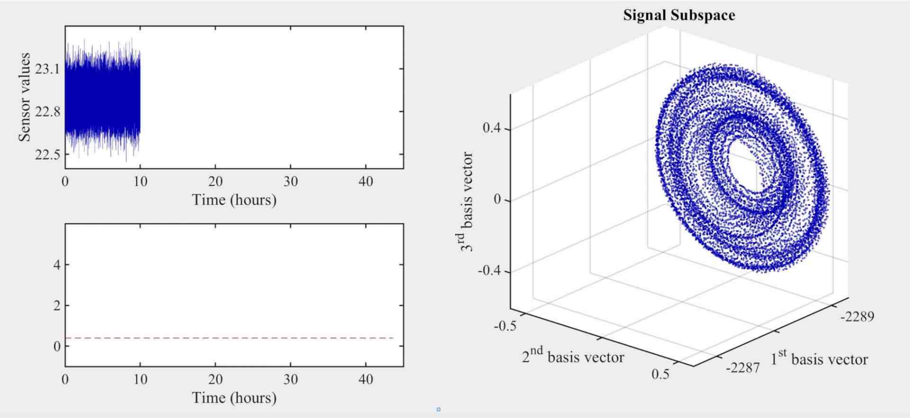
Validation — Visualizing the Departure



Training vectors form a cluster

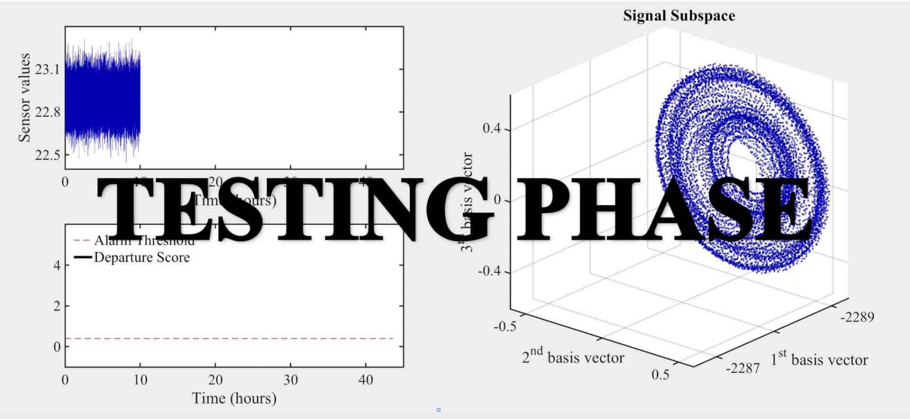
Watch the full video at https://youtu.be/SSs4IeM2MOs.

Validation — Visualizing the Departure



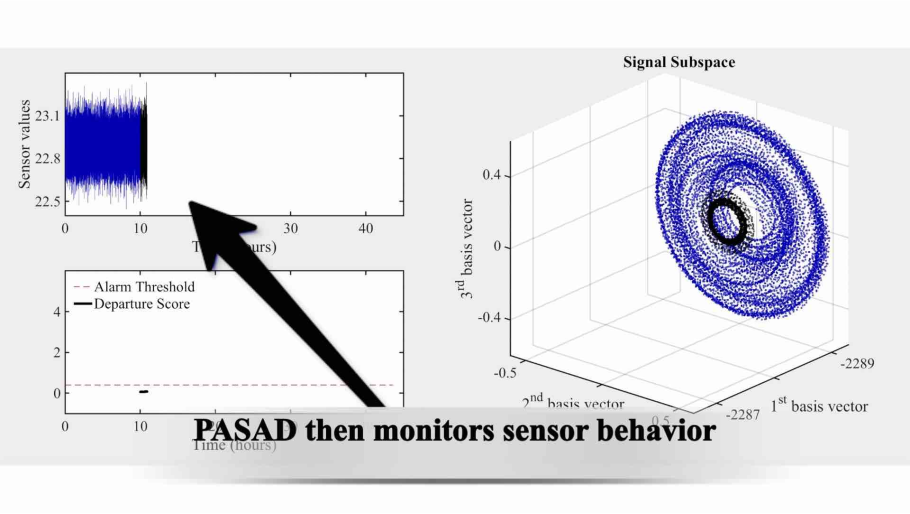
Watch the full video at https://youtu.be/SSs4IeM2MOs.

Validation — Visualizing the Departure



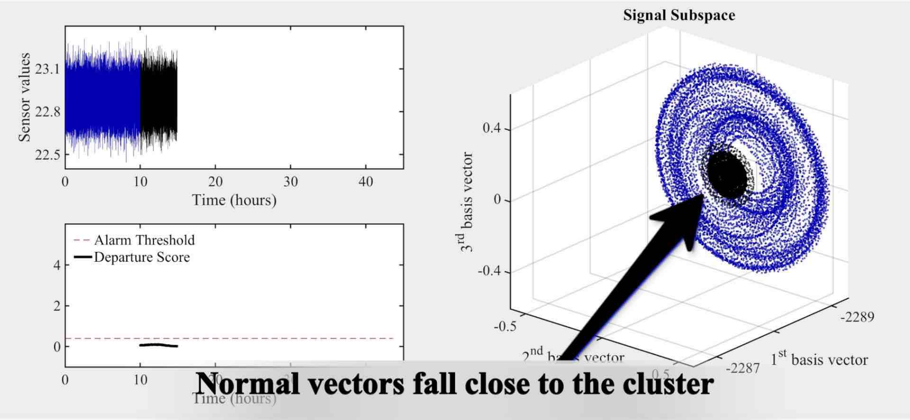
Watch the full video at https://youtu.be/SSs4IeM2MOs.

Validation — Visualizing the Departure



Watch the full video at https://youtu.be/SSs4IeM2MOs.

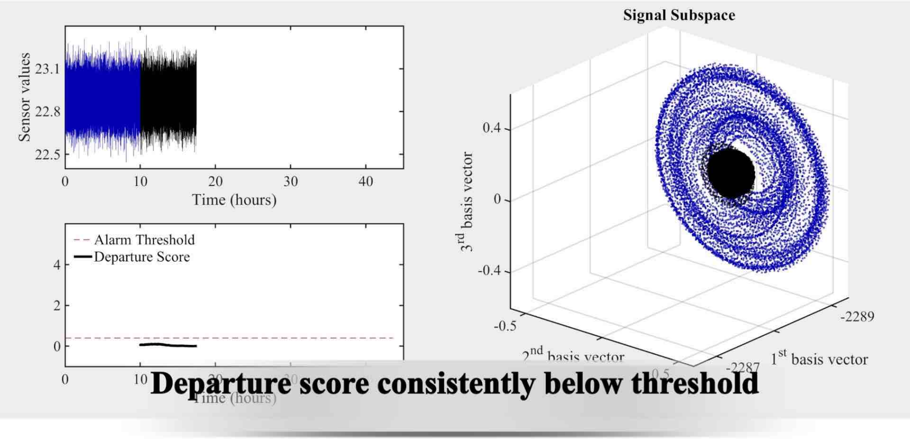
Validation — Visualizing the Departure



Normal vectors fall close to the cluster

Watch the full video at https://youtu.be/SSs4IeM2MOs.

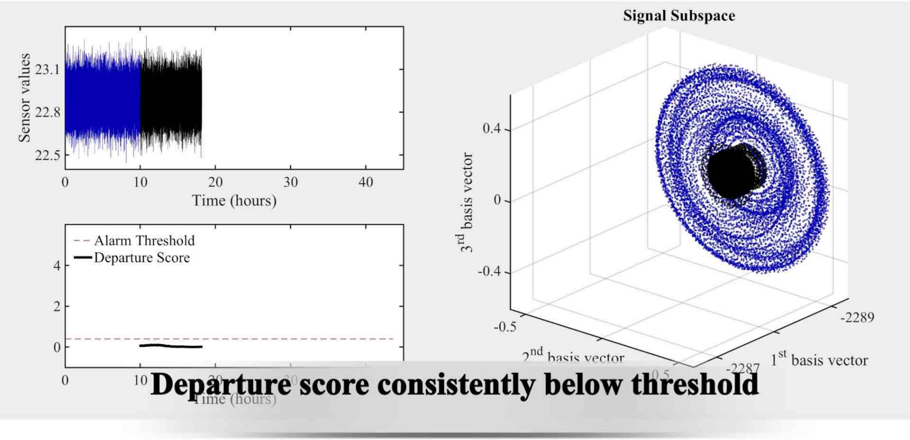
Validation — Visualizing the Departure



Departure score consistently below threshold

Watch the full video at https://youtu.be/SSs4IeM2MOs.

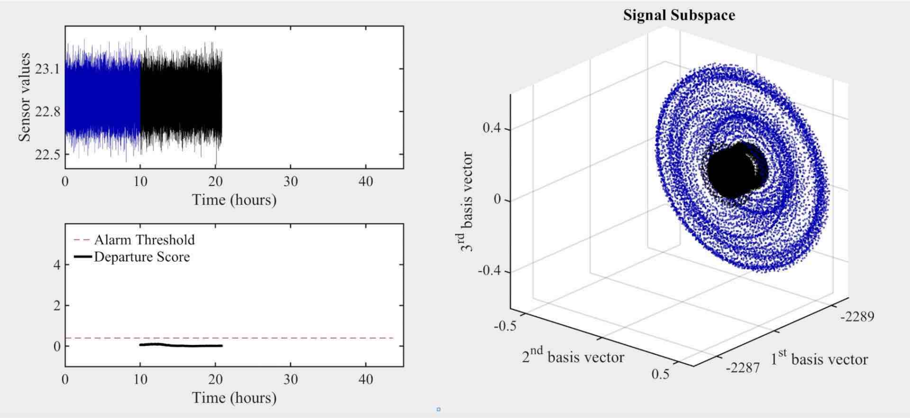
Validation — Visualizing the Departure



Departure score consistently below threshold

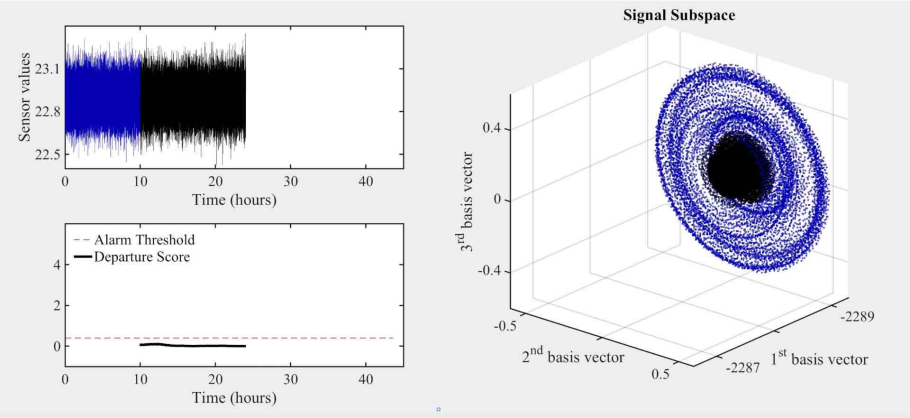
Watch the full video at https://youtu.be/SSs4IeM2MOs.

Validation — Visualizing the Departure



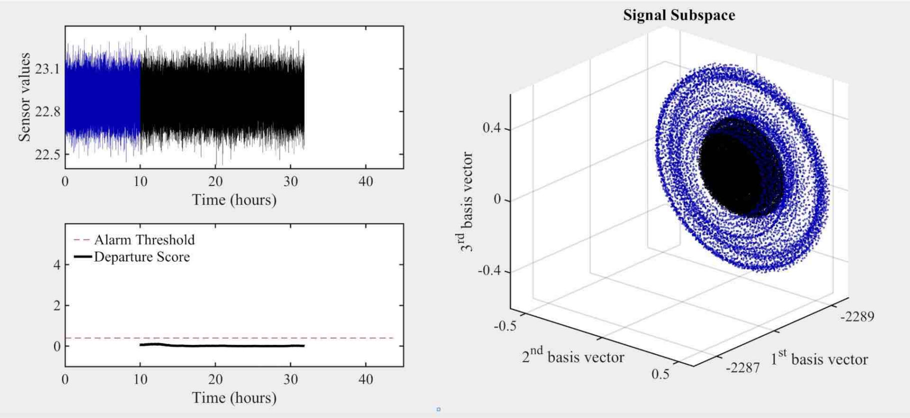
Watch the full video at https://youtu.be/SSs4IeM2MOs.

Validation — Visualizing the Departure



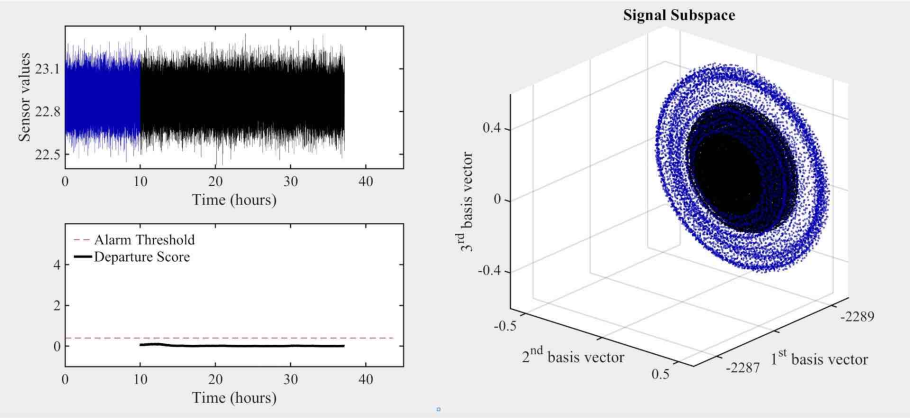
Watch the full video at https://youtu.be/SSs4IeM2MOs.

Validation — Visualizing the Departure



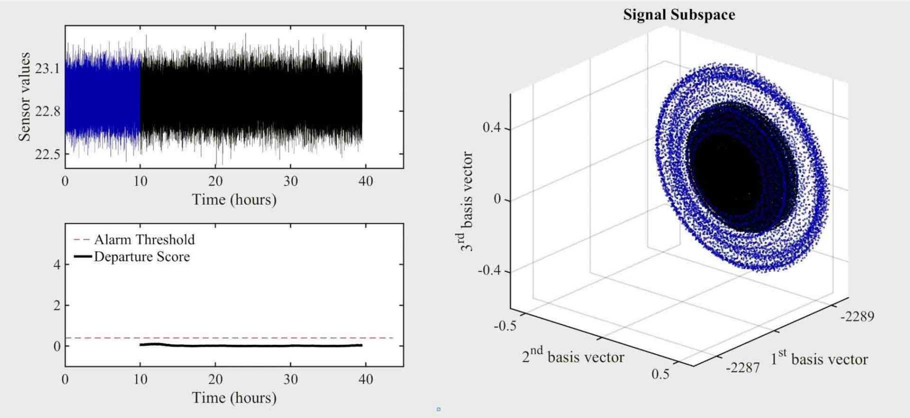
Watch the full video at https://youtu.be/SSs4IeM2MOs.

Validation — Visualizing the Departure



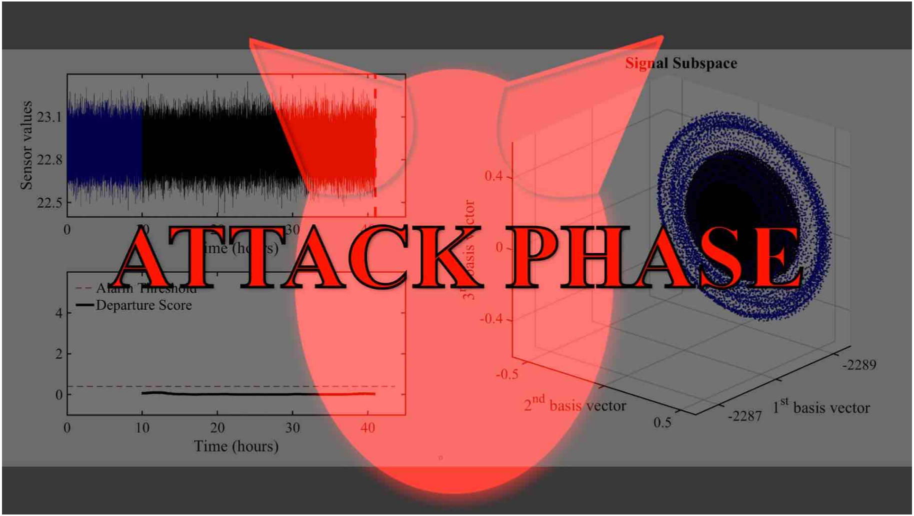
Watch the full video at https://youtu.be/SSs4IeM2MOs.

Validation — Visualizing the Departure



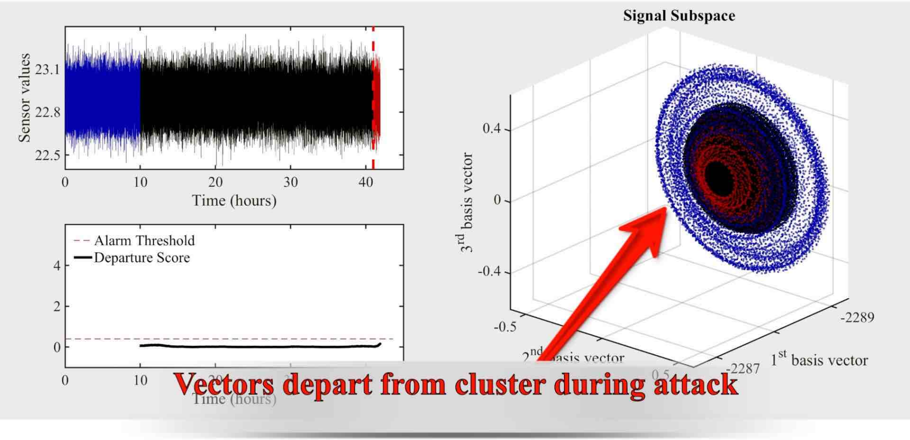
Watch the full video at https://youtu.be/SSs4IeM2MOs.

Validation — Visualizing the Departure



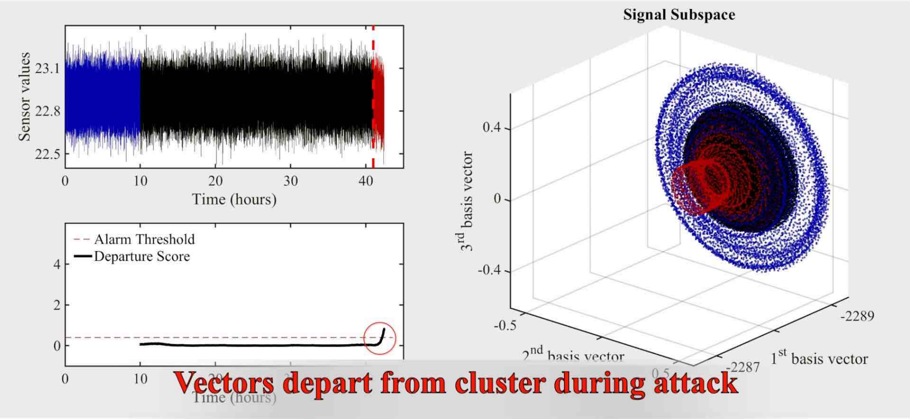
Watch the full video at https://youtu.be/SSs4IeM2MOs.

Validation — Visualizing the Departure



Watch the full video at https://youtu.be/SSs4IeM2MOs.

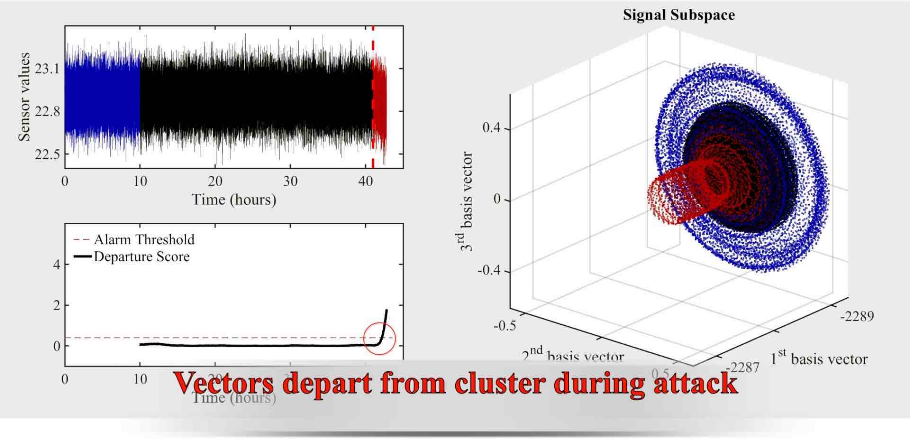
Validation — Visualizing the Departure



Vectors depart from cluster during attack

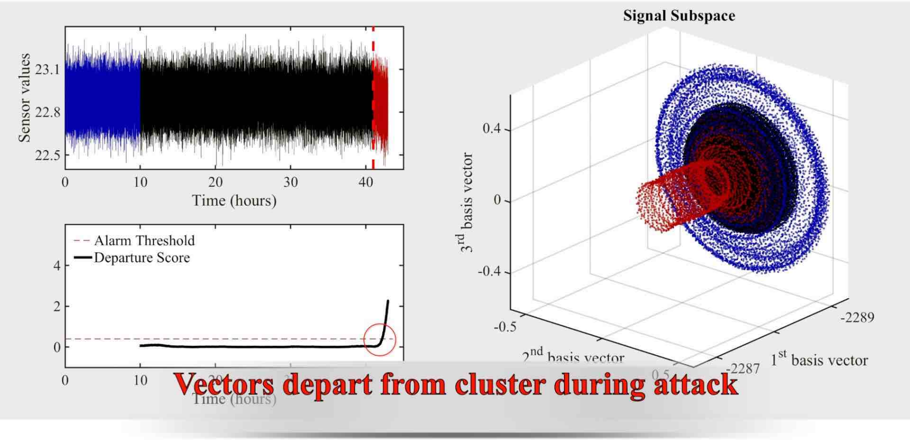
Watch the full video at https://youtu.be/SSs4IeM2MOs.

Validation — Visualizing the Departure



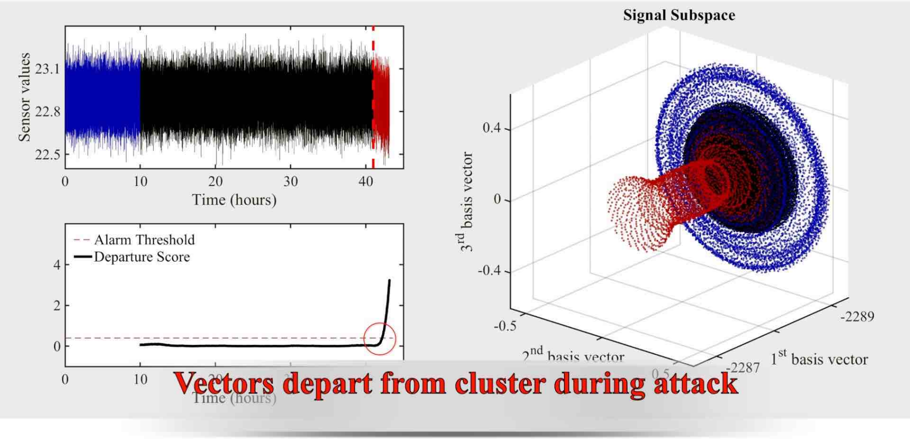
Watch the full video at https://youtu.be/SSs4IeM2MOs.

Validation — Visualizing the Departure



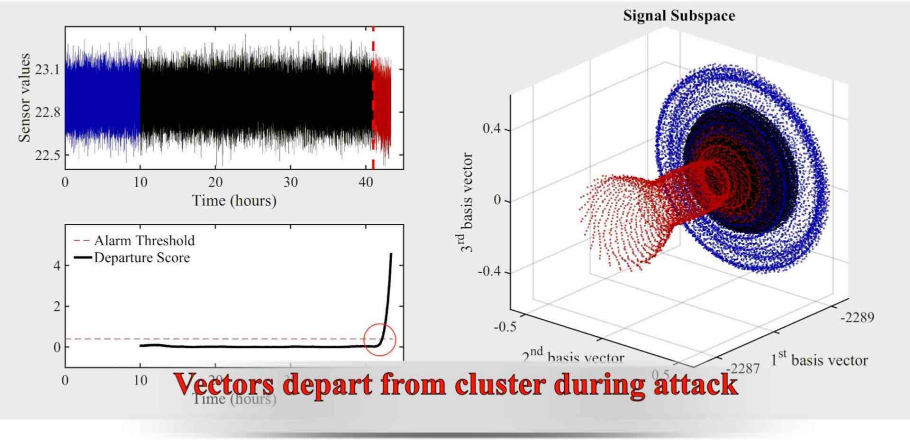
Watch the full video at https://youtu.be/SSs4IeM2MOs.

Validation — Visualizing the Departure



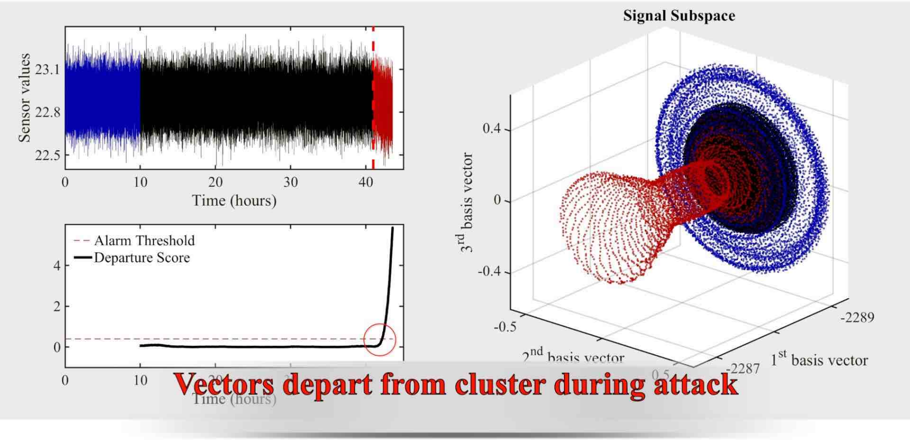
Watch the full video at https://youtu.be/SSs4IeM2MOs.

Validation — Visualizing the Departure



Watch the full video at https://youtu.be/SSs4IeM2MOs.

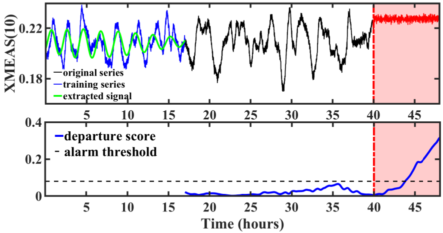
Validation — Visualizing the Departure

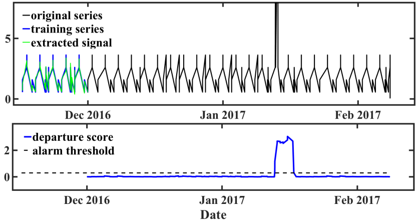


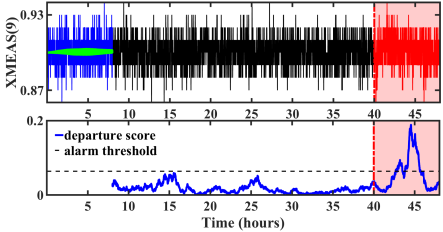
Vectors depart from cluster during attack

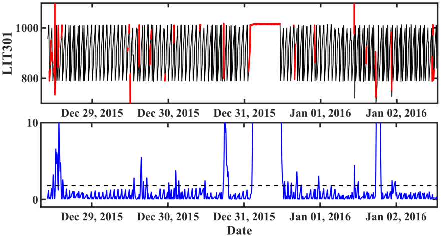
Watch the full video at https://youtu.be/SSs4IeM2MOs.

Validation — Evaluation on Various Systems









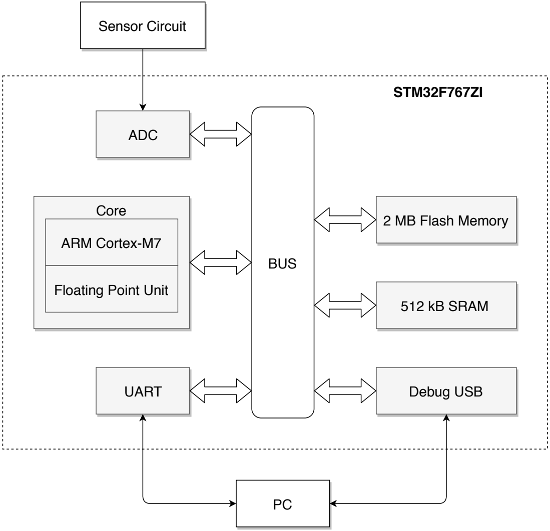
Rationale

- Under attack, industrial machines are poised to exhibit changes in physical properties.
- Mature sensor-level monitoring mechanisms are already available.
- Required hardware are cheap and widely available.

Motivation

- Cost-efficient and easy to deploy.
- A complementary measure that adds security to the physical process.
- Isolated and unreachable monitoring system.
- Generates its own data.

System Design



Design Choices

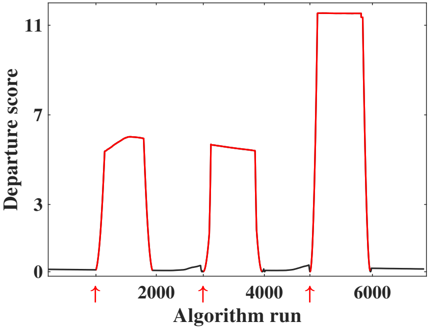
Off-the-shelf and widely available.

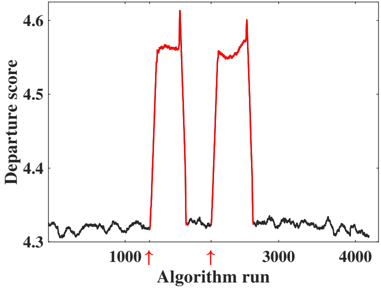
- Microphone sensor.
- Vibration sensor.
- Load sensor.

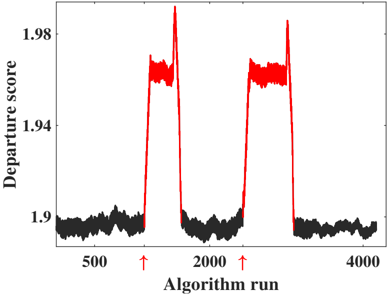
The metrics considered for the embedded system

- Computational performance.
- Amount of memory.
- The availability of analog-to-digital converter.
- Floating-point support.

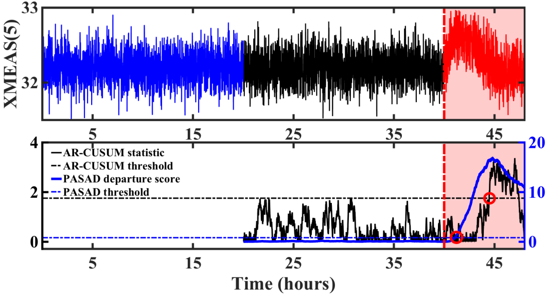
Experimental Results - Testbed Setting



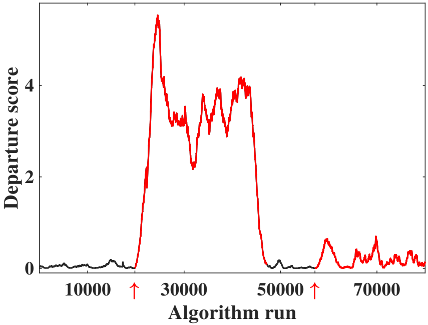


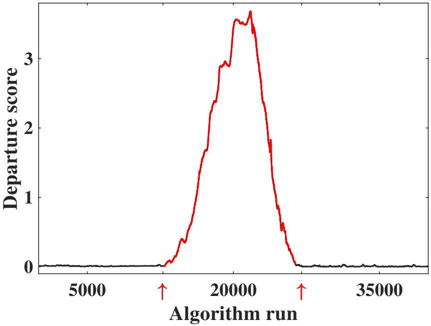


Experimental Results - Testbed Setting



Experimental Results - Real Setting





Technical Challenges

Tasks that required delicate engineering effort:

- Pre-processing analogue signals.
- Circuitry design and interfacing sensors.
- Implementing PASAD on the microcontroller.

More technical details in the paper.