CHALMERS
UNIVERSITY OF TECHNOLOGY

INTRUSION DETECTION FOR INDUSTRIAL CONTROL SYSTEMS

WISSAM AOUDI

DAT 300 – 2019/2020

Industrial Control Systems (ICS)

Functionality, whereabouts, and current state

Industrial Control Systems

Monitor and control industrial processes and often operate on critical infrastructure

Nuclear plants

Electricity grids

www.kiplinger.com

Transportation

Water systems

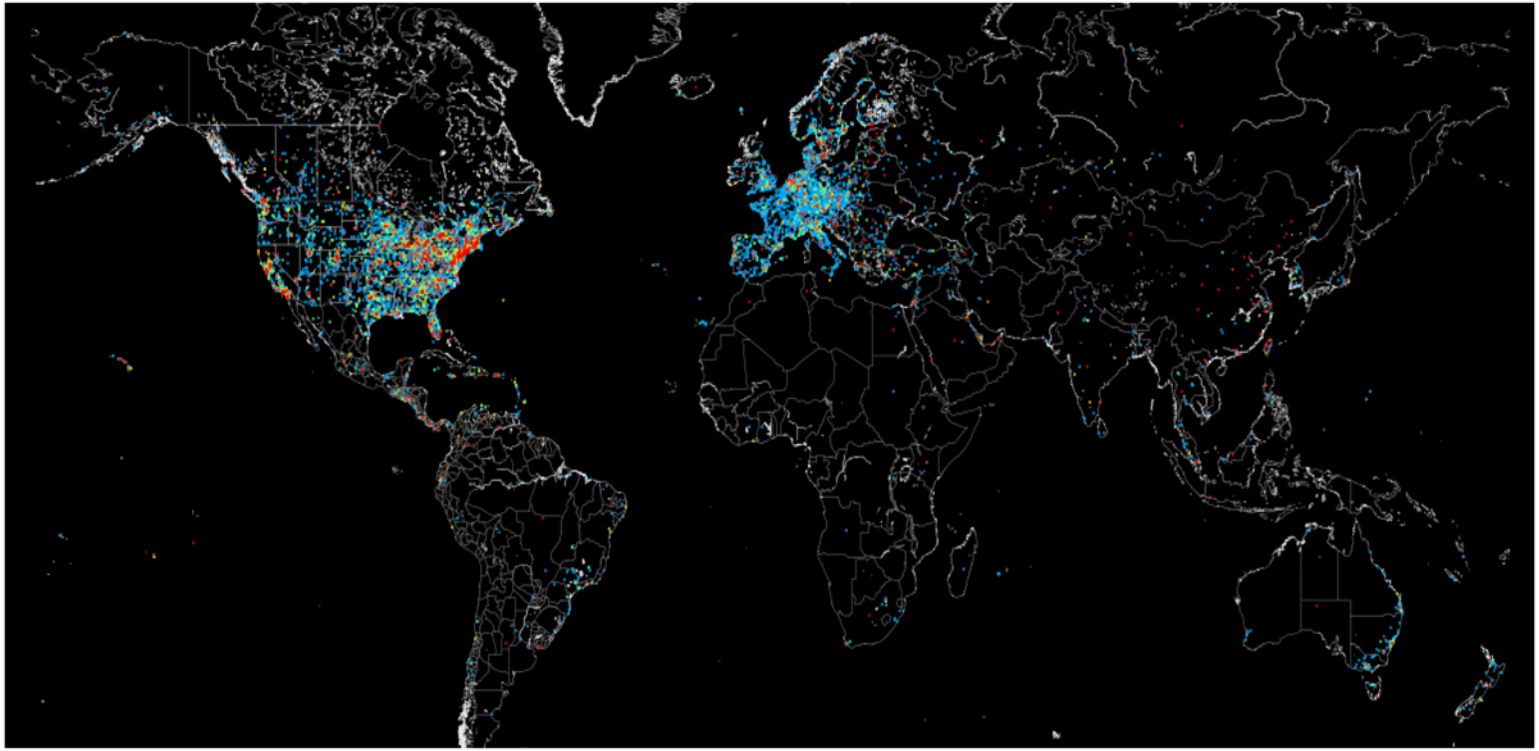
www.kiplinger.com

Gas pipelines

Communication

www.kiplinger.com

Map of Industrial Control Systems on the Internet



www.shodan.io

CNN BUSINESS Markets Tech Media Success Perspectives Video

The Internet's most dangerous sites

Some things just shouldn't be connected to the Internet. With Shodan, a search engine that finds connected devices, it's easy to locate dangerous things that anyone can access without so much as a username or password.

Traffic light controls

When something that literally anyone in the world can access says "DEATH MAY OCCUR !!!" it's generally a good idea to build some kind of security around it.

Oops - no. For some reason, someone thought it would be a good idea to put traffic light controls on the Internet. Making matters way, way worse is that these controls require no login credentials whatsoever. Just type in the address, and you've got access.

PHOTO: DAN TENTLER/ THINKSTOCK

This is why Caps Lock was invented.

www.money.cnn.com

CNN BUSINESS Markets Tech Media Success Perspectives Video

The Internet's most dangerous sites

Some things just shouldn't be connected to the Internet. With Shodan, a search engine that finds connected devices, it's easy to locate dangerous things that anyone can access without so much as a username or password.

A swimming pool acid pump

Swimming pools have acid pumps to adjust the pH balance of the water. They're usually not connected to the Internet.

At least one of them is, though. So, exactly how powerful and toxic is this acid pump?

"Can we turn people into soup?" wondered Tentler.

Tentler said there was no distinguishing text in this app to tip him off to where the pool was located or whom it is owned by, so the owners haven't been contacted. Enter at your own risk!

www.money.cnn.com

CNN BUSINESS Markets Tech Media Success Perspectives Video

The Internet's most dangerous sites

Some things just shouldn't be connected to the Internet. With Shodan, a search engine that finds connected devices, it's easy to locate dangerous things that anyone can access without so much as a username or password.

A hydroelectric plant

French electric companies apparently like to put their hydroelectric plants online. Tentler found three of them using Shodan.

This one has a big fat button that lets you shut off a turbine. But what's 58,700 Watts between friends, right?

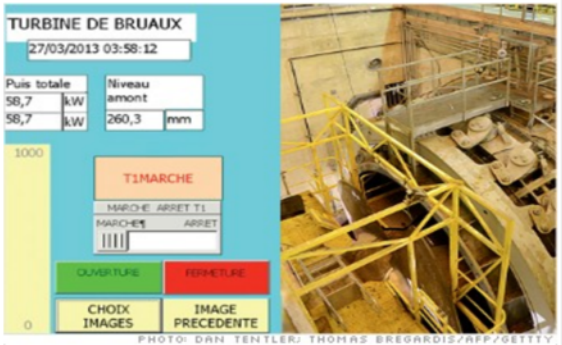


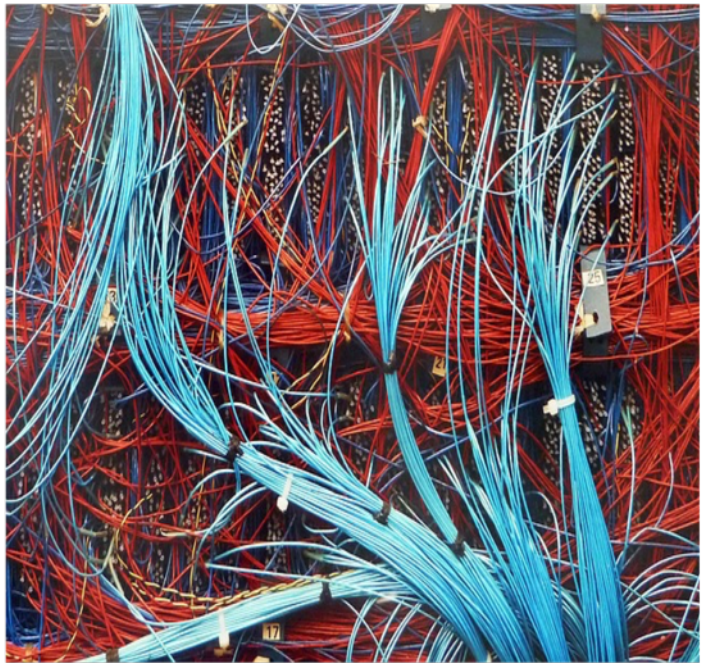
PHOTO: DAN TENTLER; THOMAS BREGARDIS/AFP/GETTTY

Wait, does that say kilowatts?

It's not just France that has a problem. The U.S. Department of Homeland Security commissioned researchers last year to see if they could find **industrial control systems for nuclear power plants** using Shodan. They found several.

www.money.cnn.com

Connectivity of ICS: A Curse or a Blessing?



+ Improved operational efficiency
+ Efficient use of resources
+ Customized services
+ Enhanced interfacing
+ Better diagnostics

– Exposing critical systems to cyberattacks

www.aspistrategist.org.au

Attacks on ICS

Attacks on ICS

Attacks on ICS

Cyber Warfare in the Horizon

MilitaryTimes

Military plans to counter Iran include possible 120,000 troop deployment, cyber attack 'Nitro Zeus'

The updated military plans do not call for an Iraq War-style land invasion but instead focus on air strikes and a potential cyber-attack, which in previous plans had been called "Nitro Zeus" and would have attempted to disable major Iranian cities, military facilities and the power grid. That plan dates to at least 2010 or earlier, experts have said.

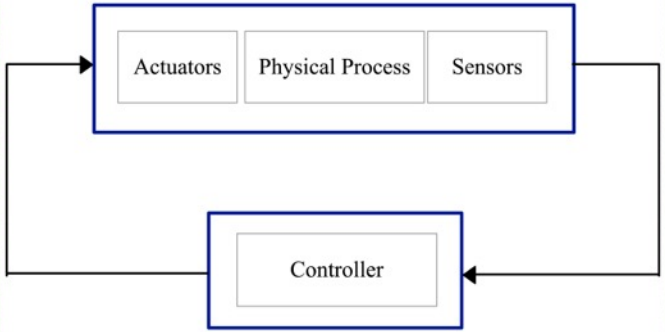
The Pentagon recently presented a military plan to the president's top national security aides that calls for up to 120,000 troops deploying to the Middle East and a potential crippling cyber-attack on Iran's infrastructure should Iran speed up its nuclear program or attack U.S. forces.

www.militarytimes.com

Securing Industrial Control Systems

Challenges and opportunities

Abstract representation of ICS



Importance of securing ICS

- ICS interact with the physical world
- Far-reaching attack consequences
- Too much at stake

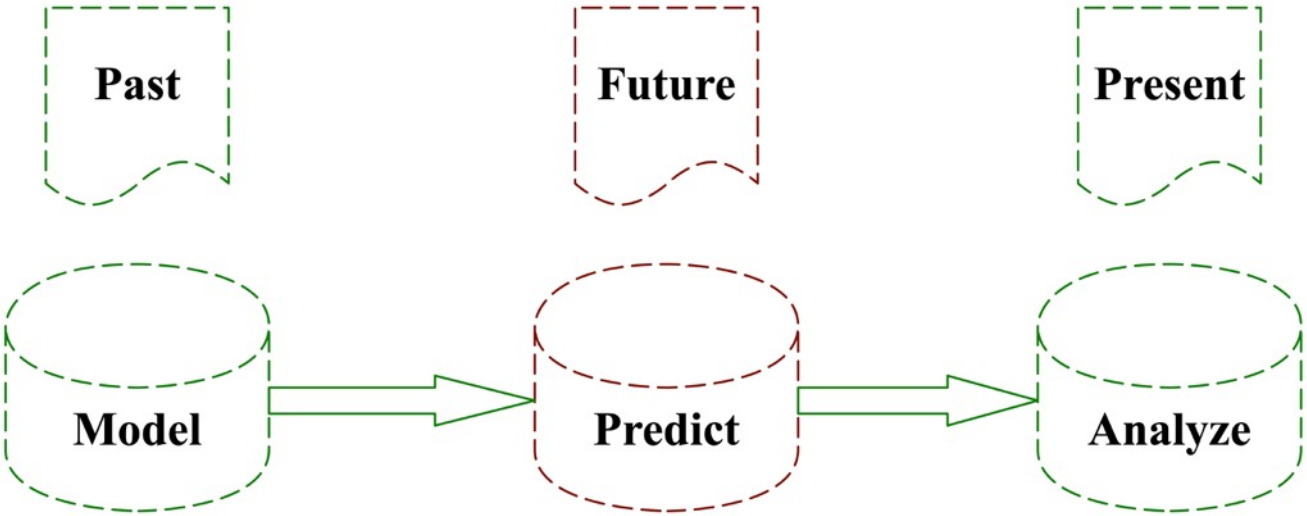
Challenges

- Closed-source, legacy, proprietary, and widely different
- Real-time requirements
- Data is sensitive and hard to access

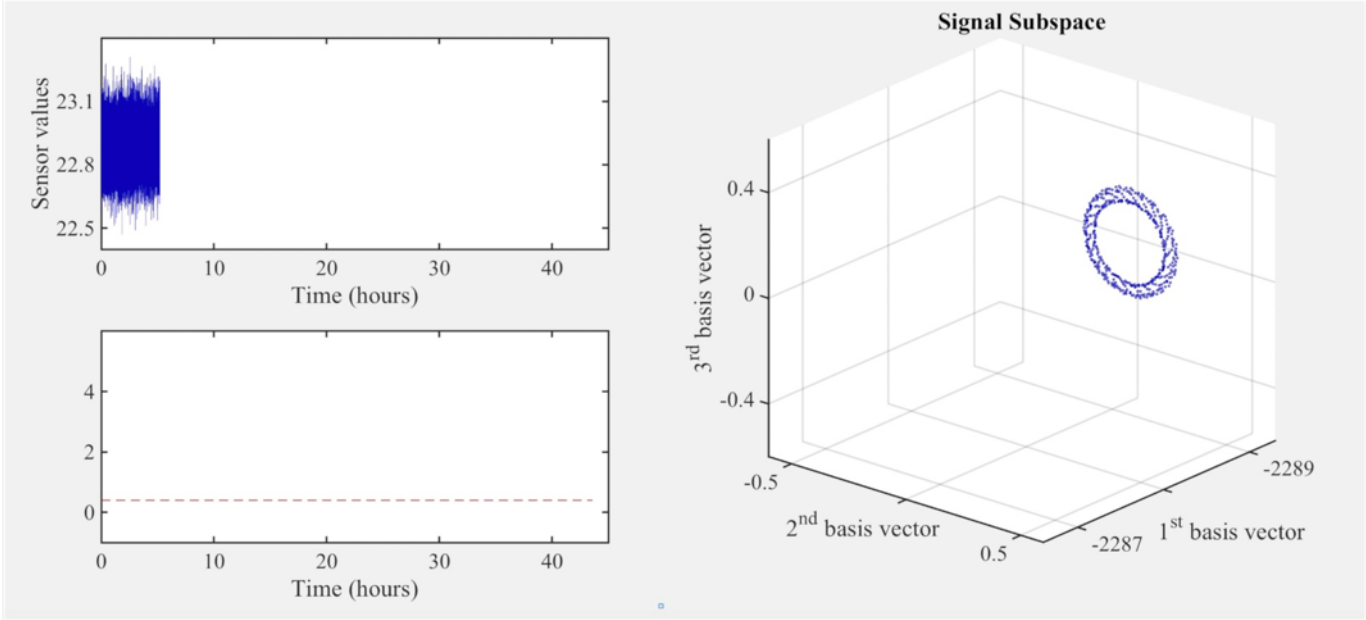
Opportunities

- Process behavior is deterministic
- Static topologies
- Machine-to-machine traffic is highly regular
- Normal system behavior can be learned or modeled

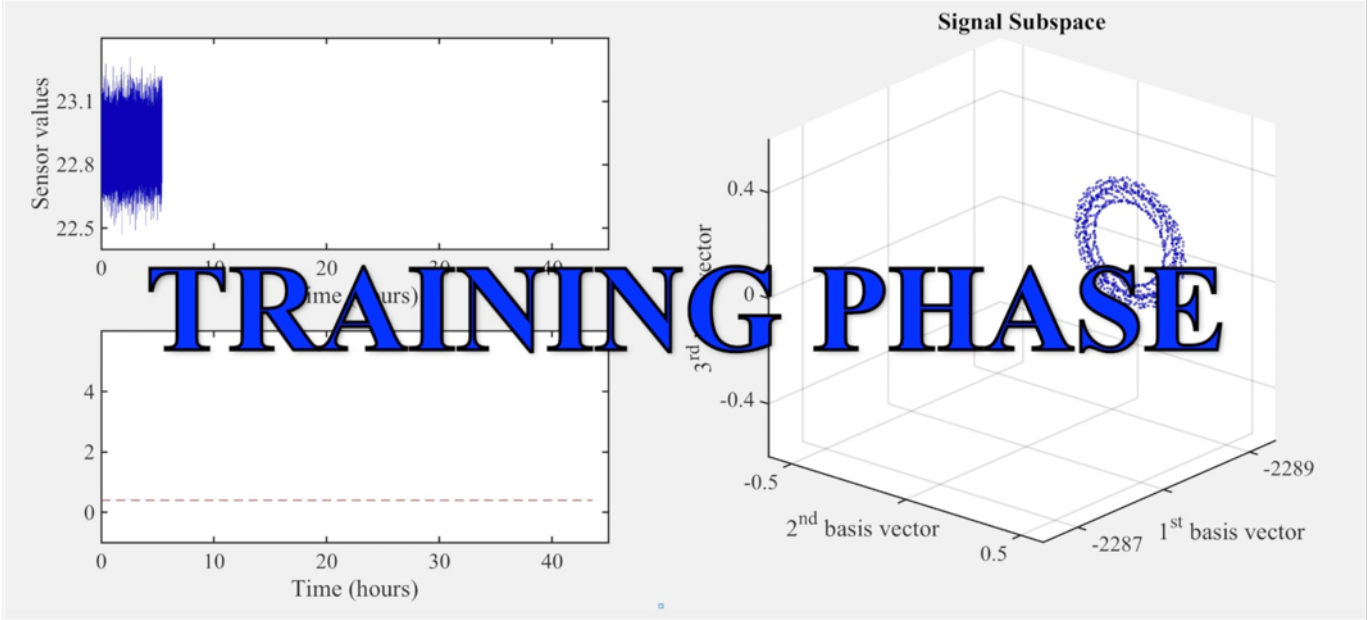
State-of-the-Art Methodology



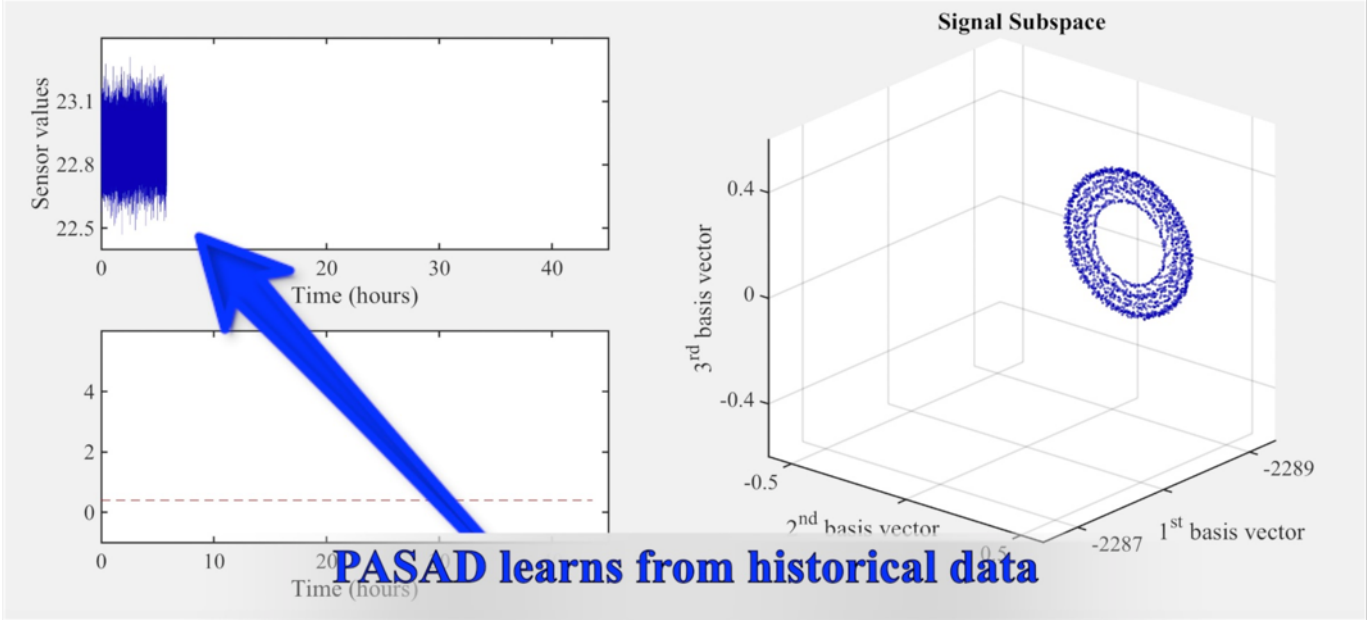
Visualization



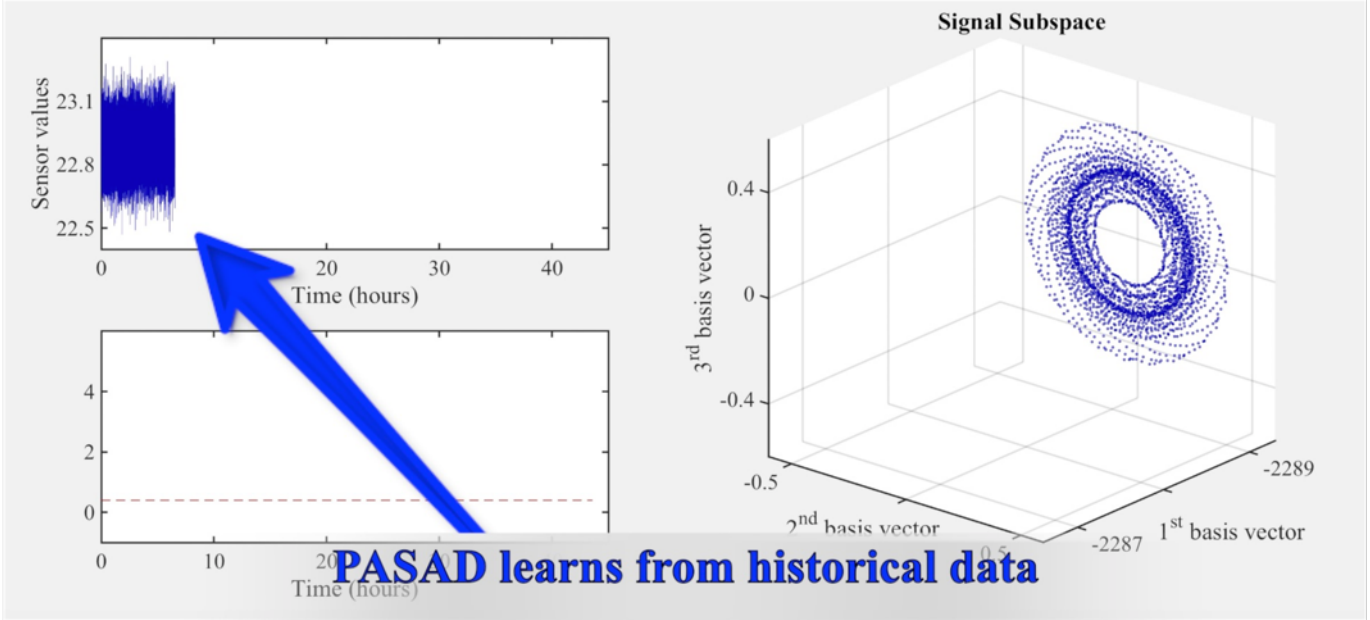
Visualization



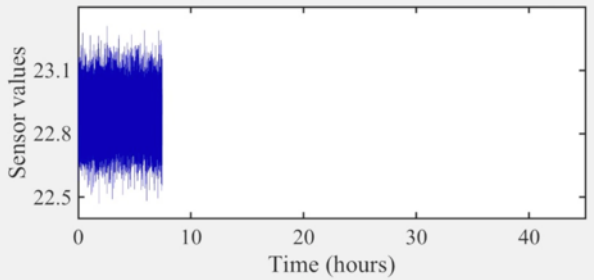
Visualization

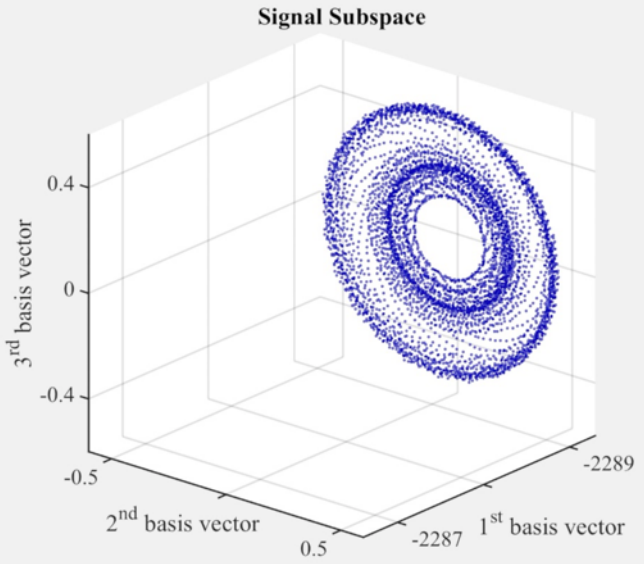


Visualization

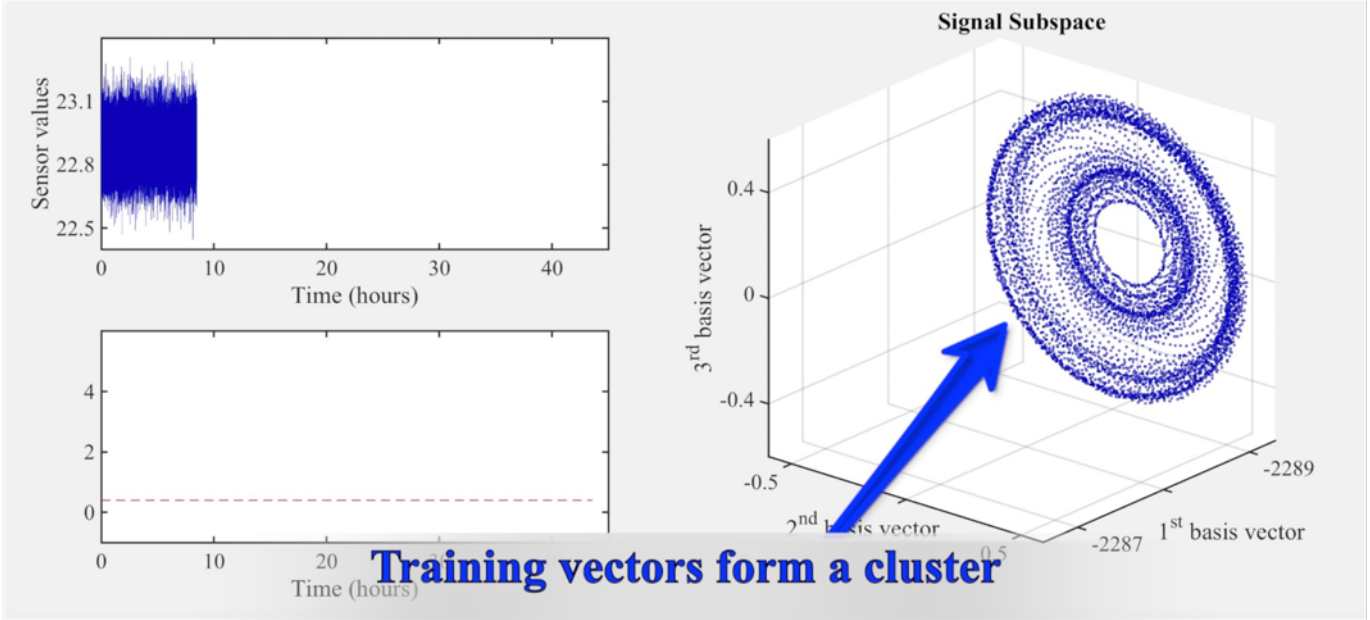


Visualization

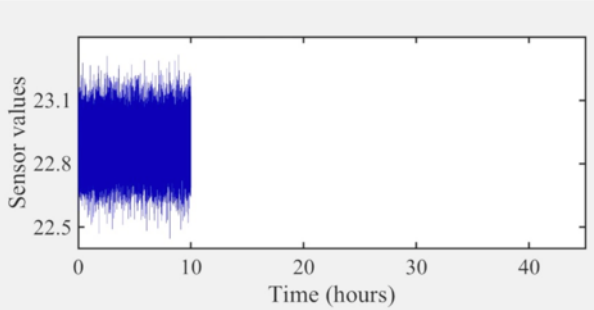


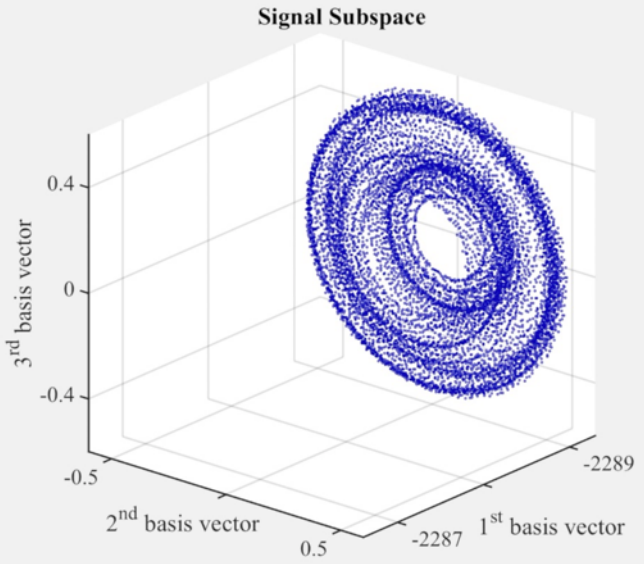


Visualization

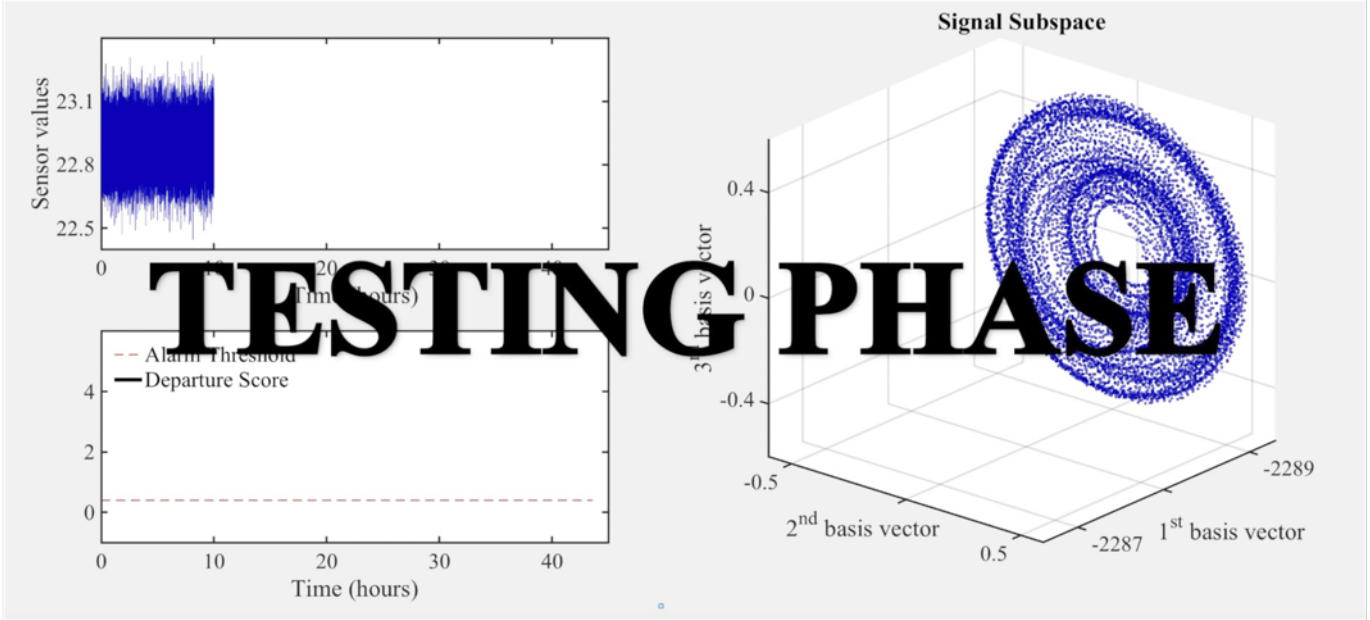


Visualization



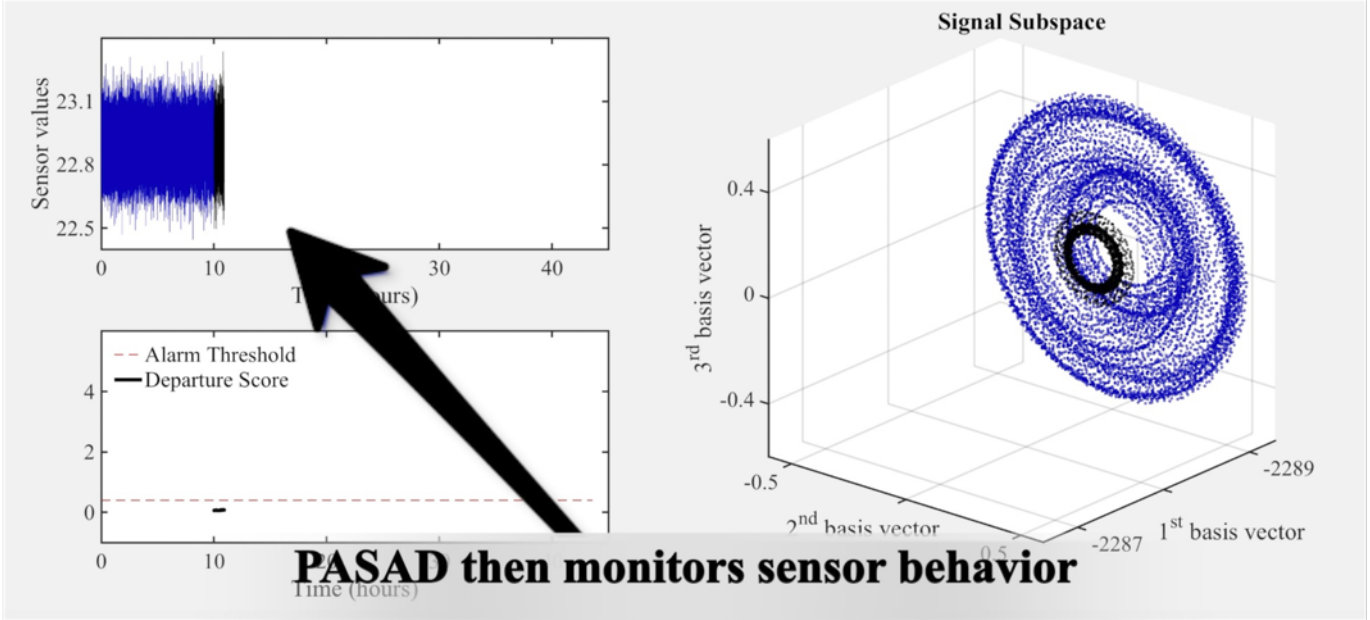


Visualization

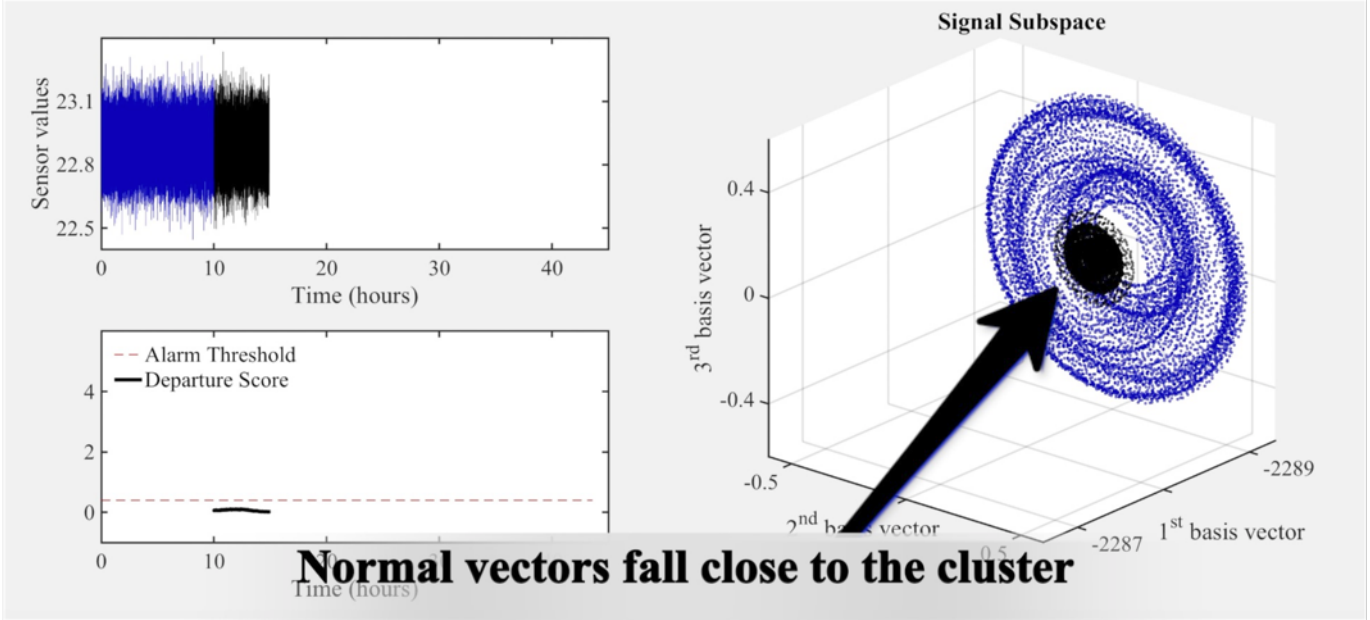


TESTING PHASE

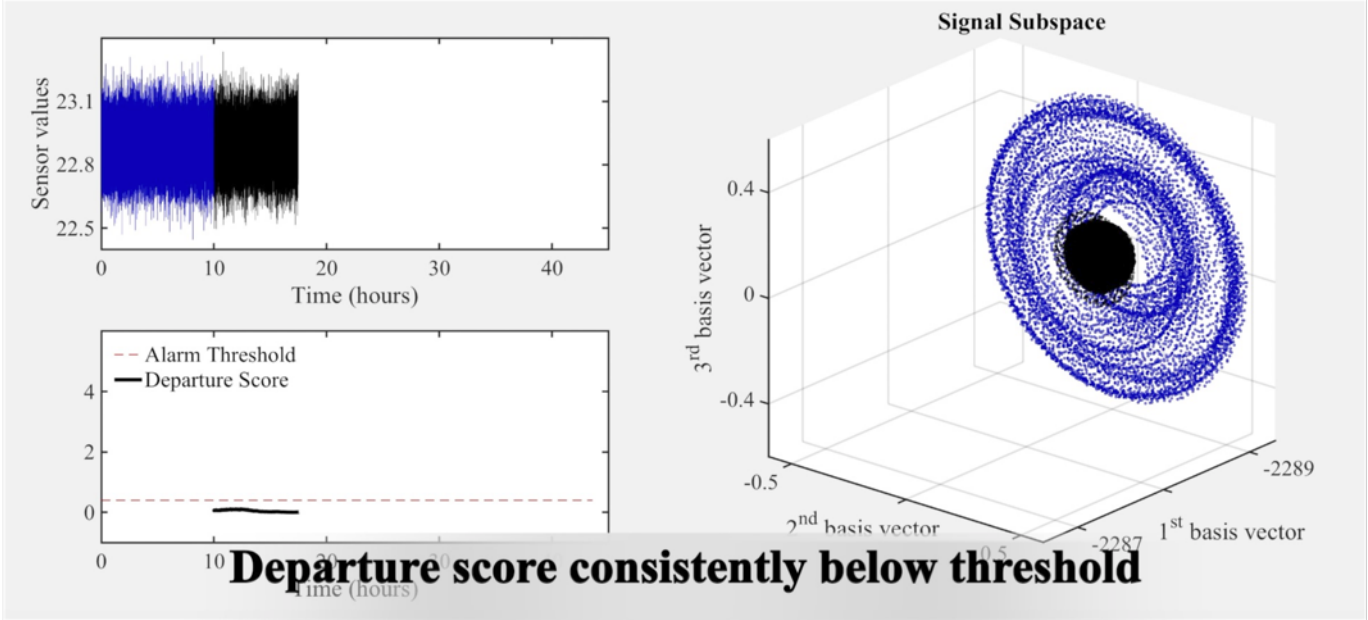
Visualization



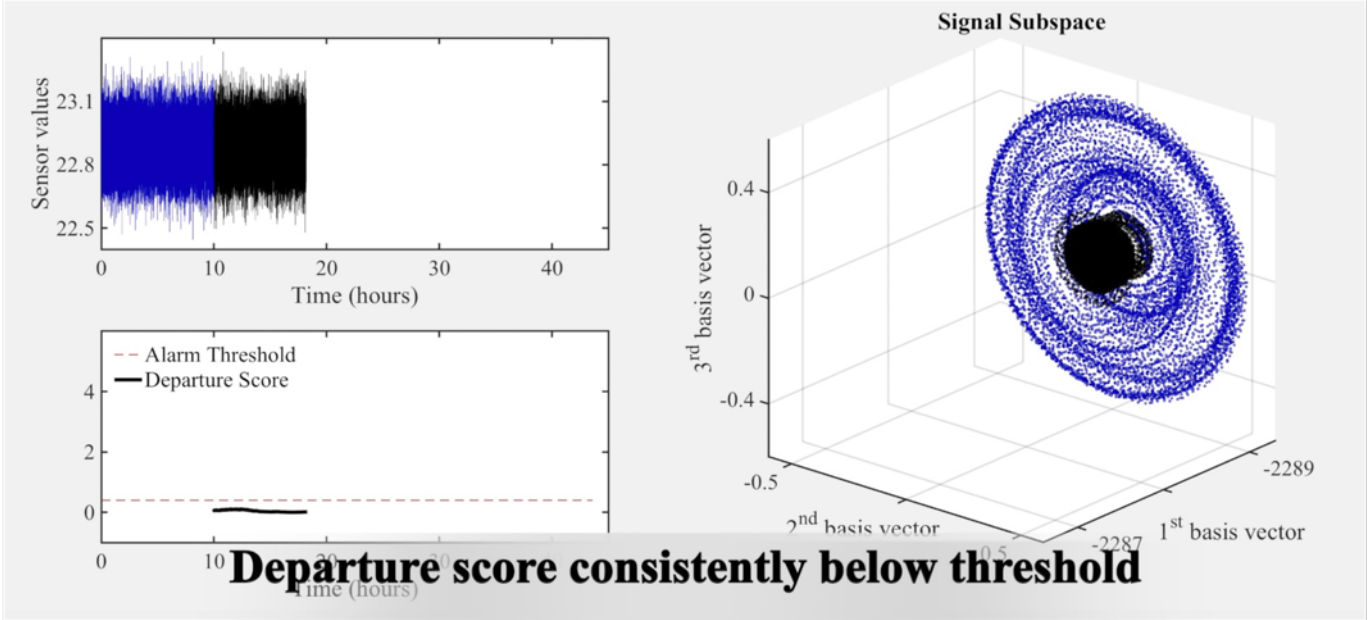
Visualization



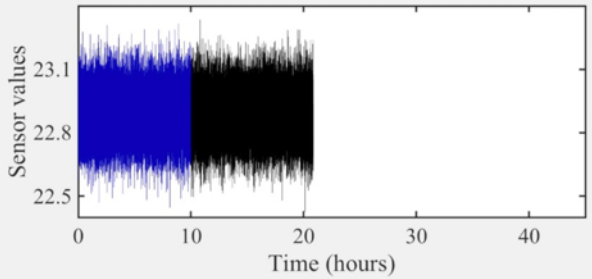
Visualization

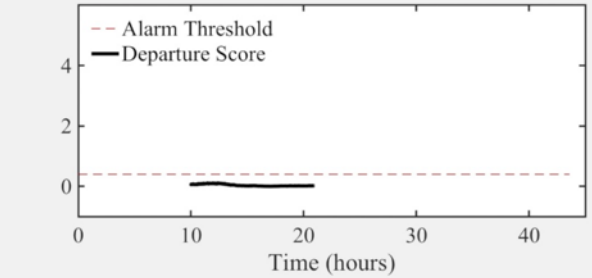


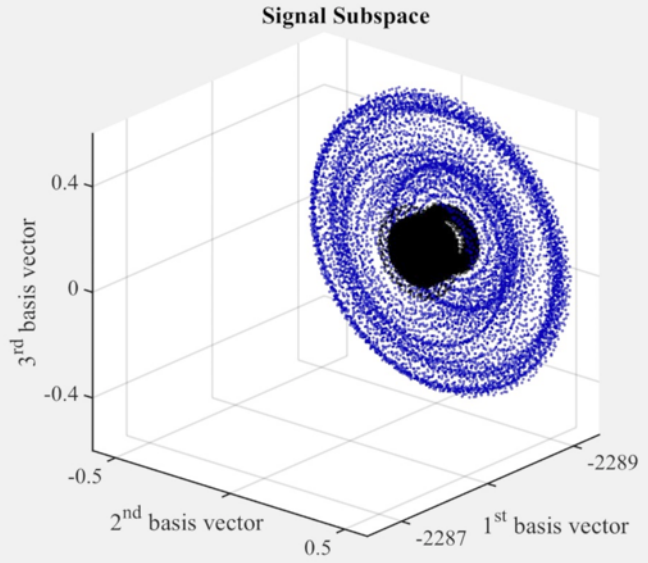
Visualization



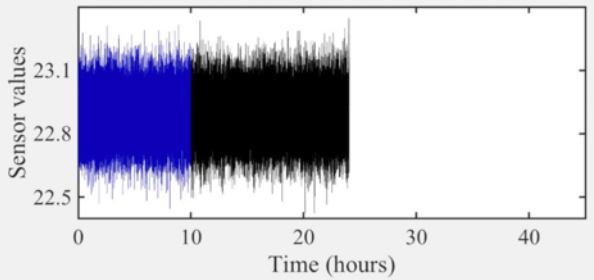
Visualization

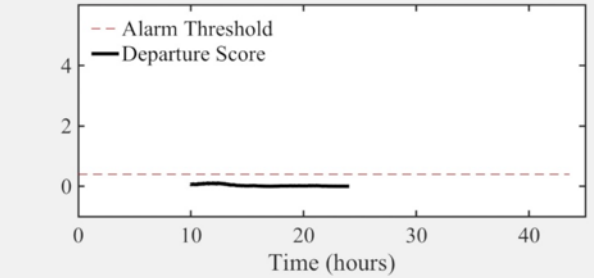


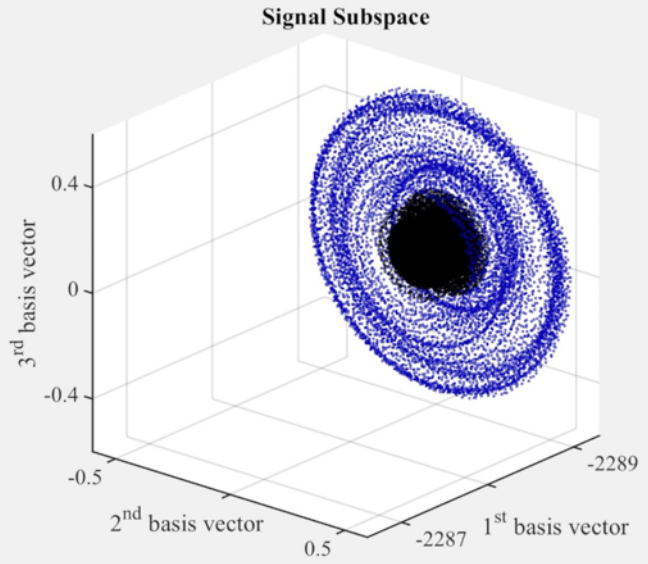




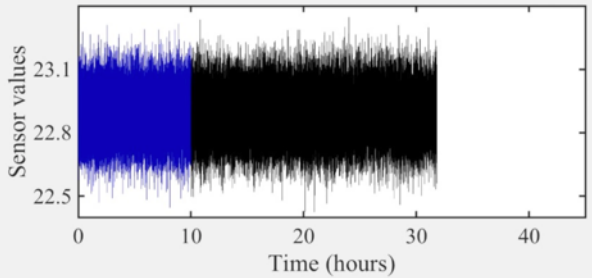
Visualization

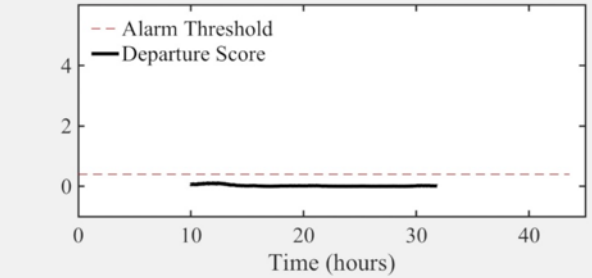


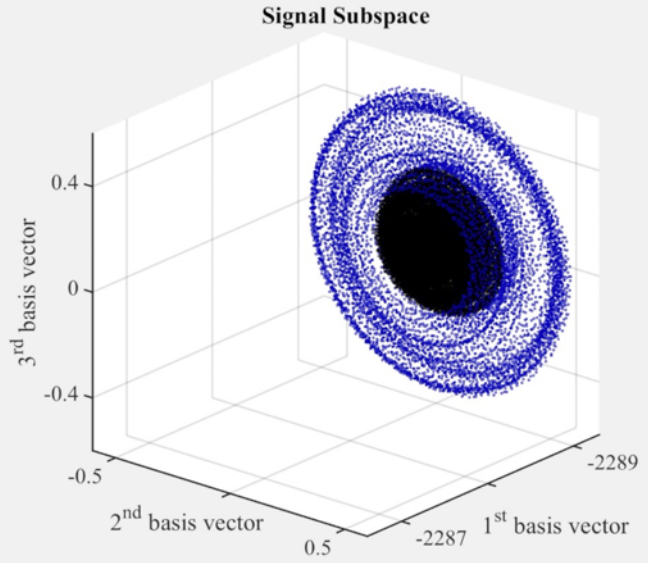




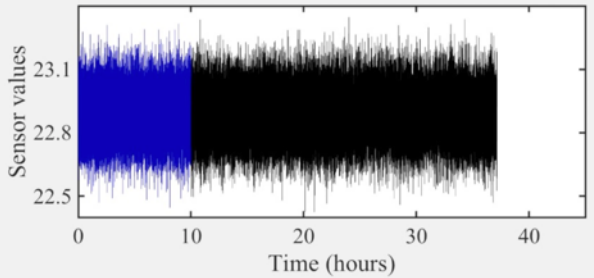
Visualization

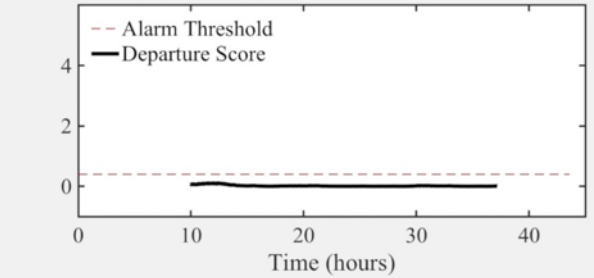


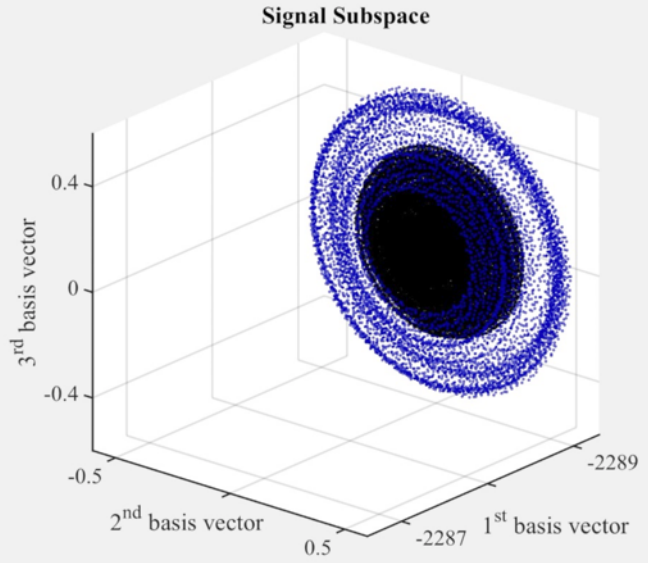




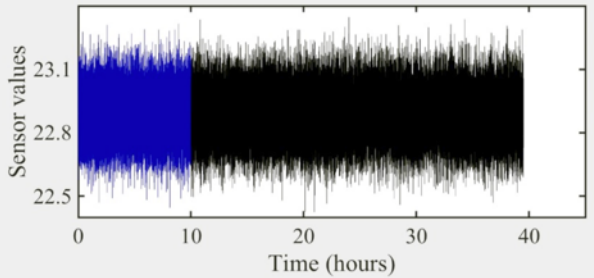
Visualization

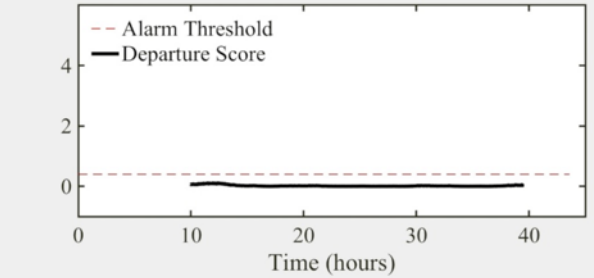


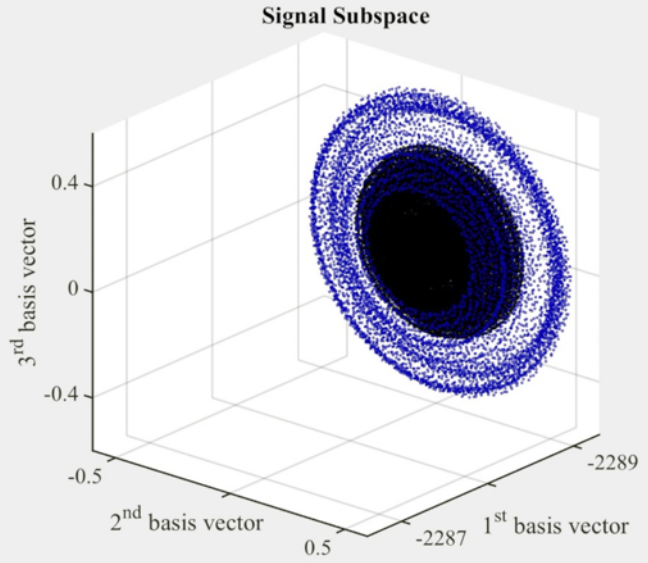




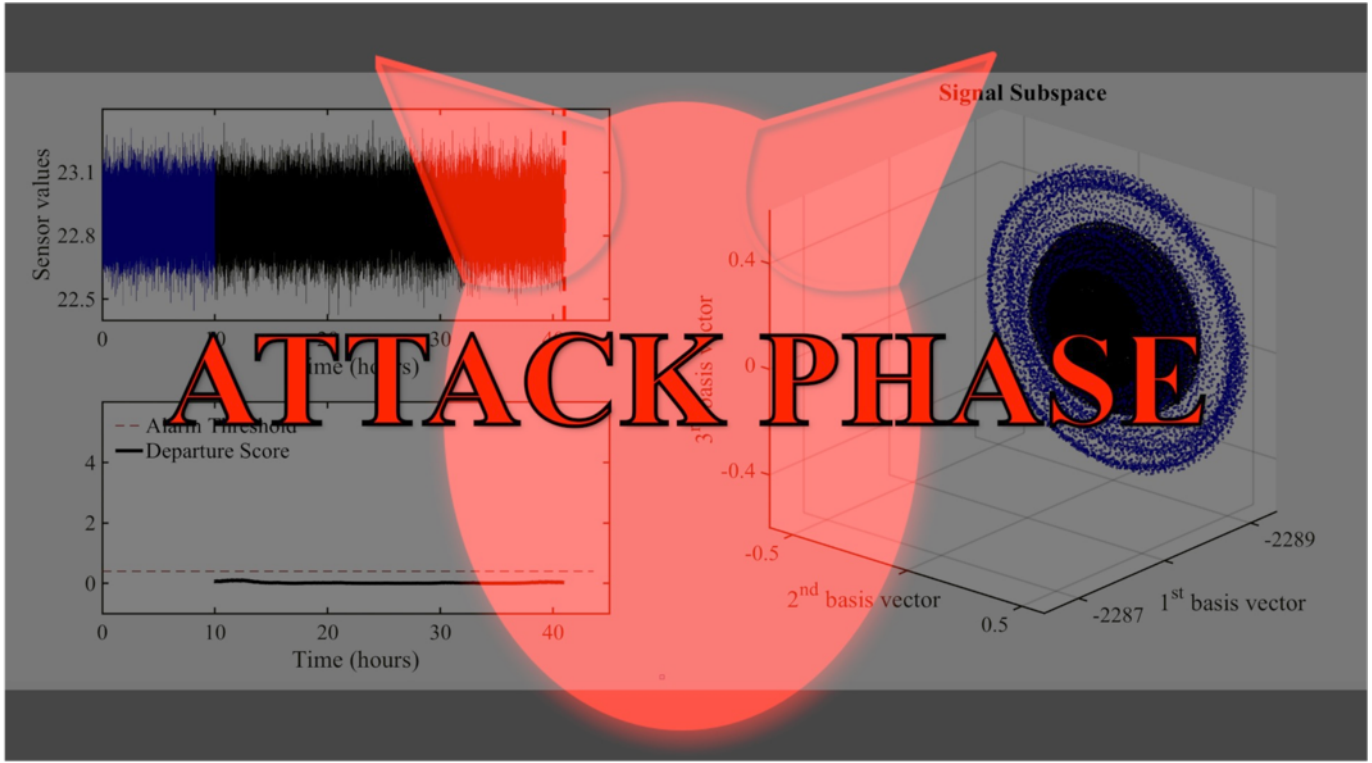
Visualization



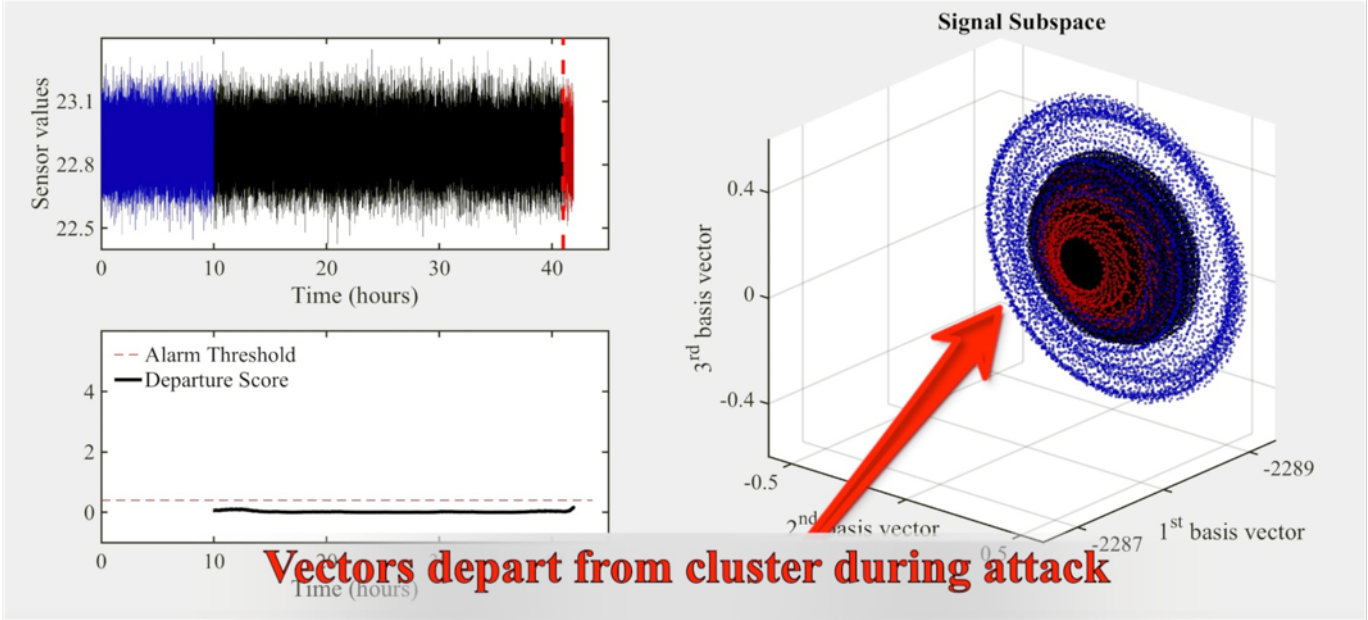




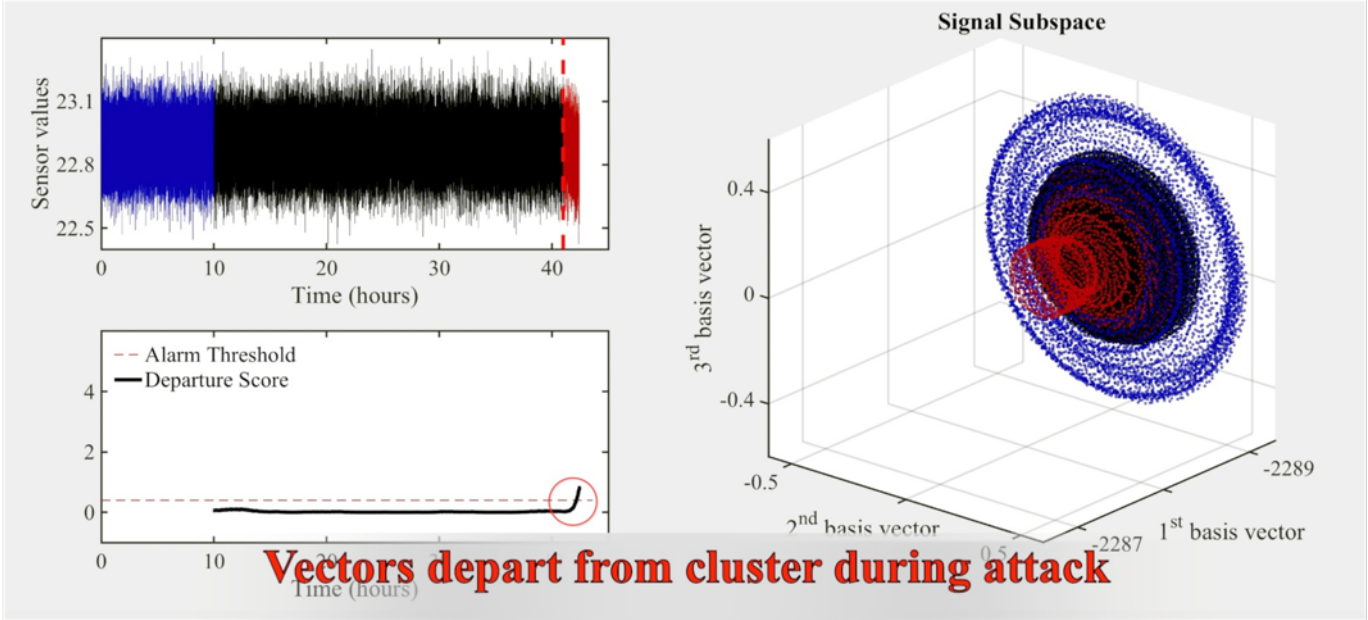
Visualization



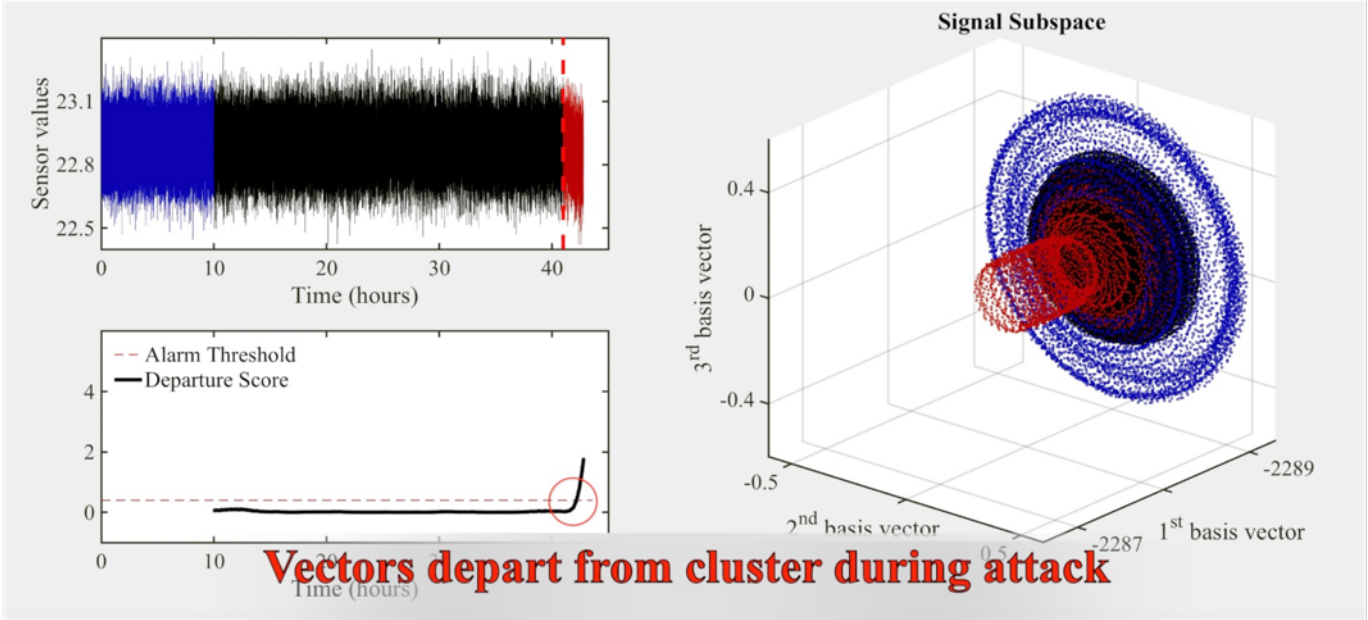
Visualization



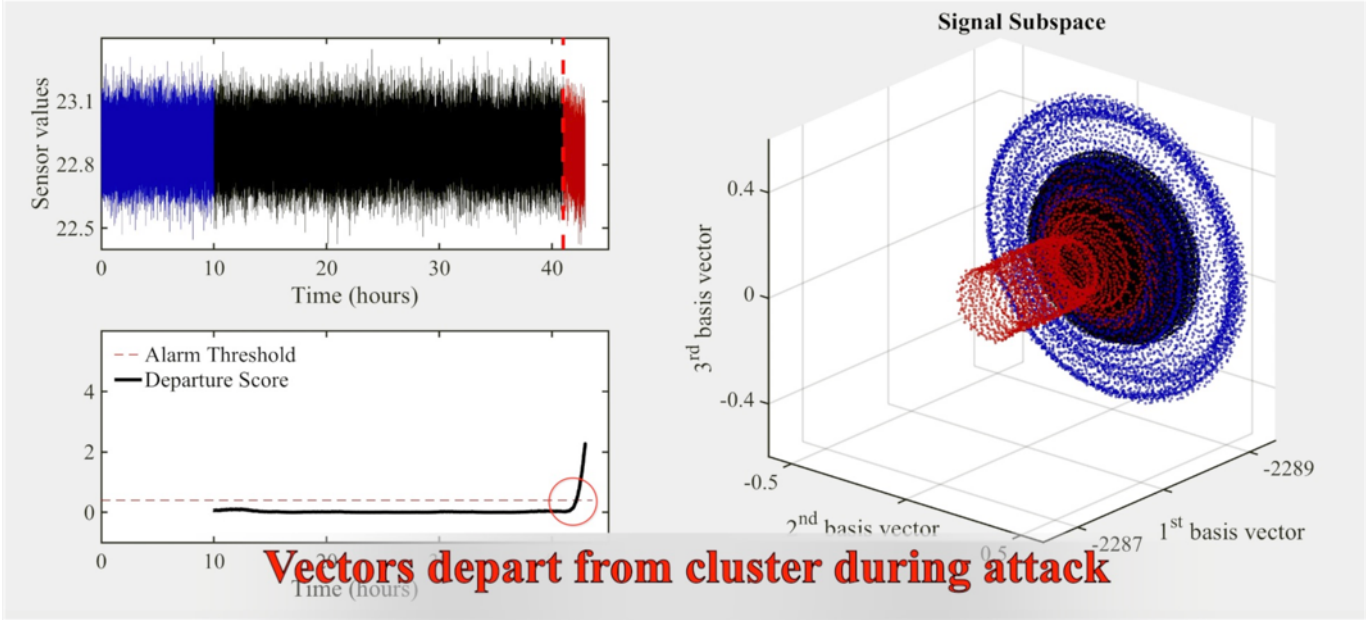
Visualization



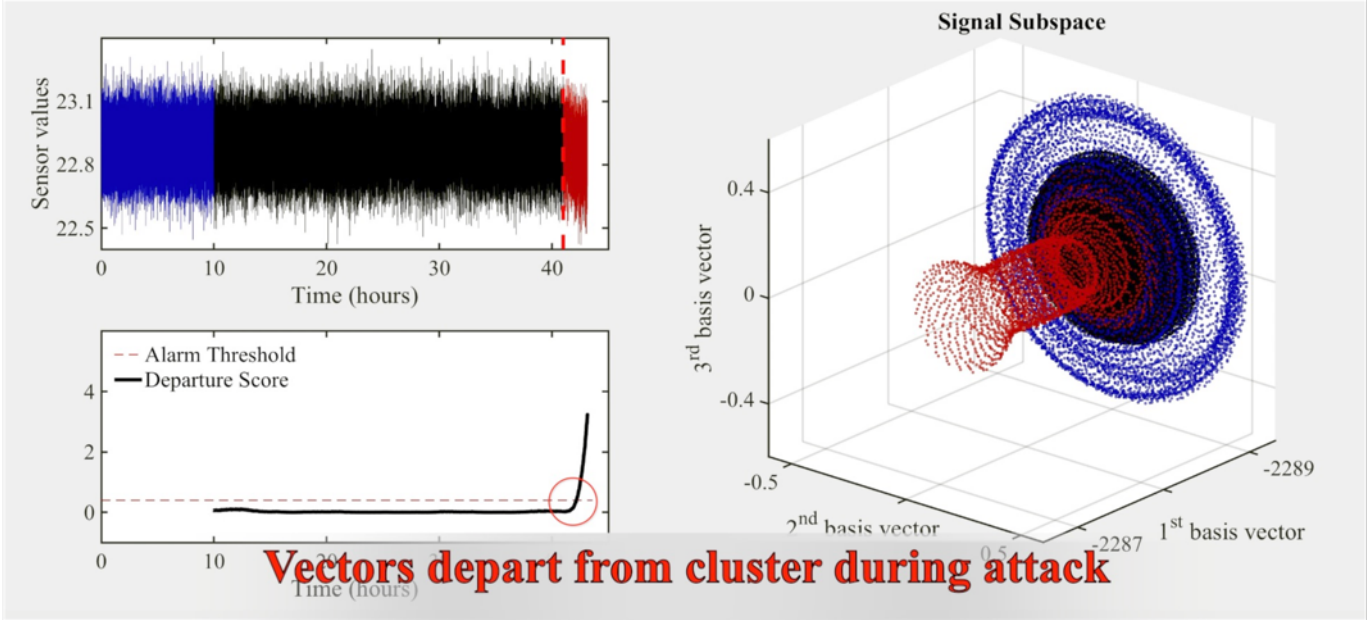
Visualization



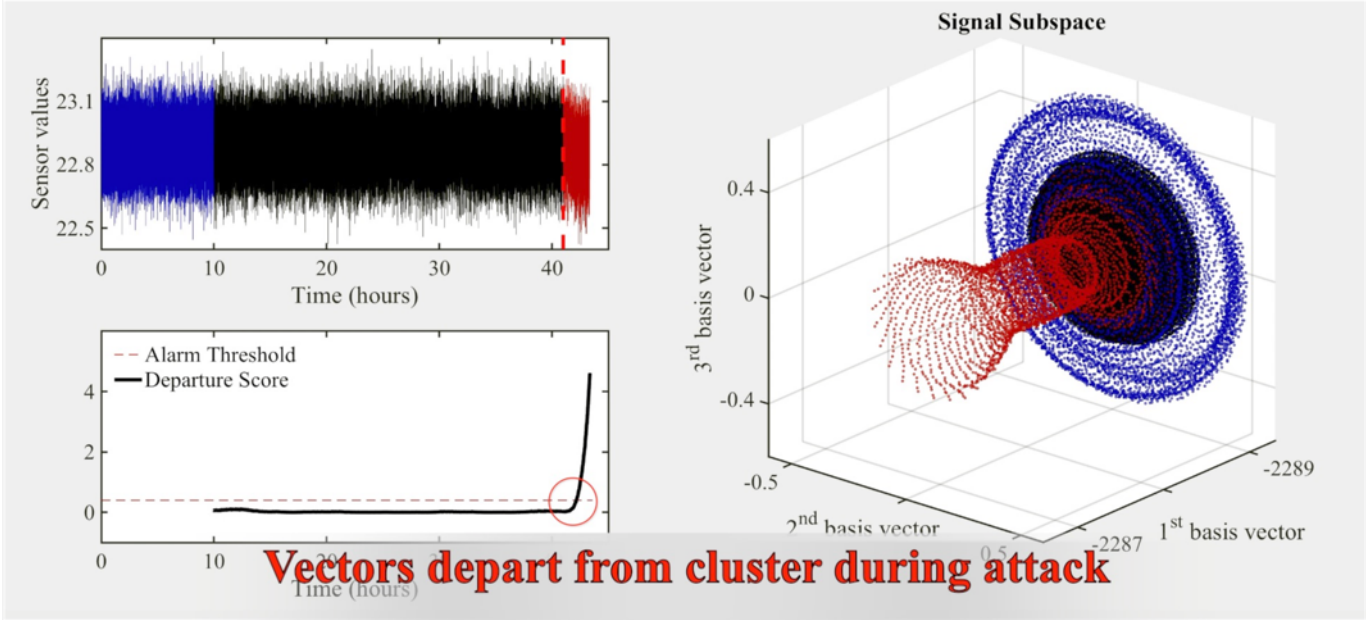
Visualization



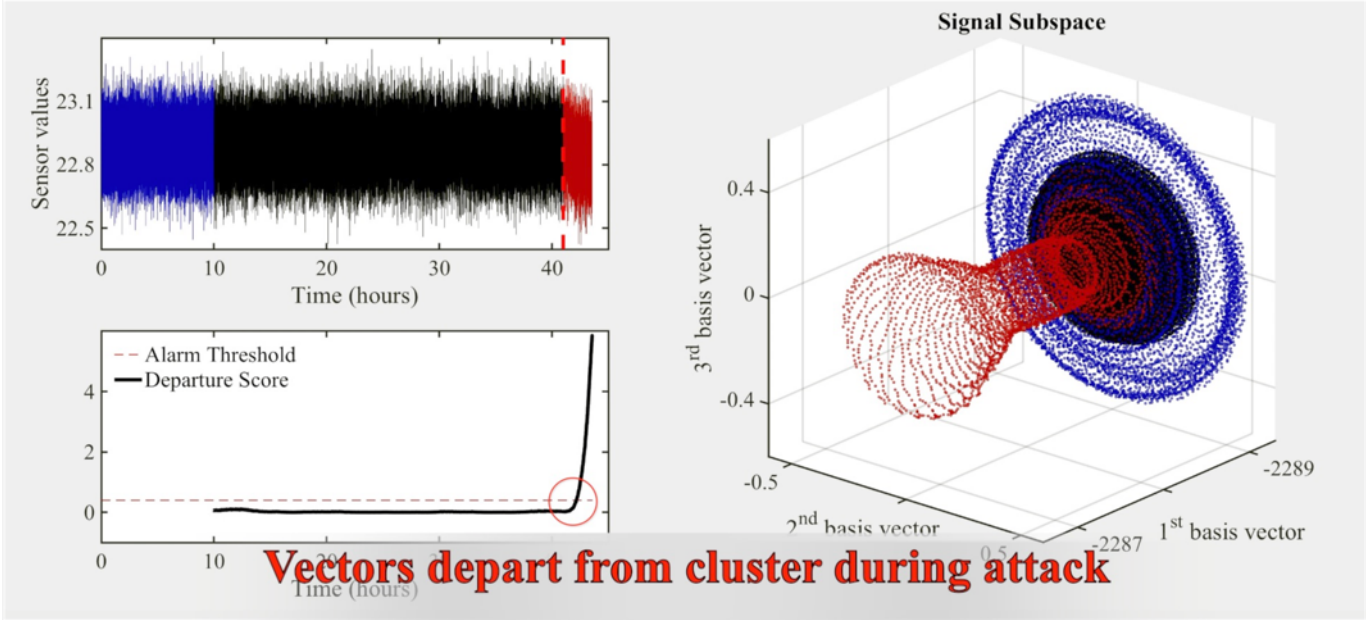
Visualization



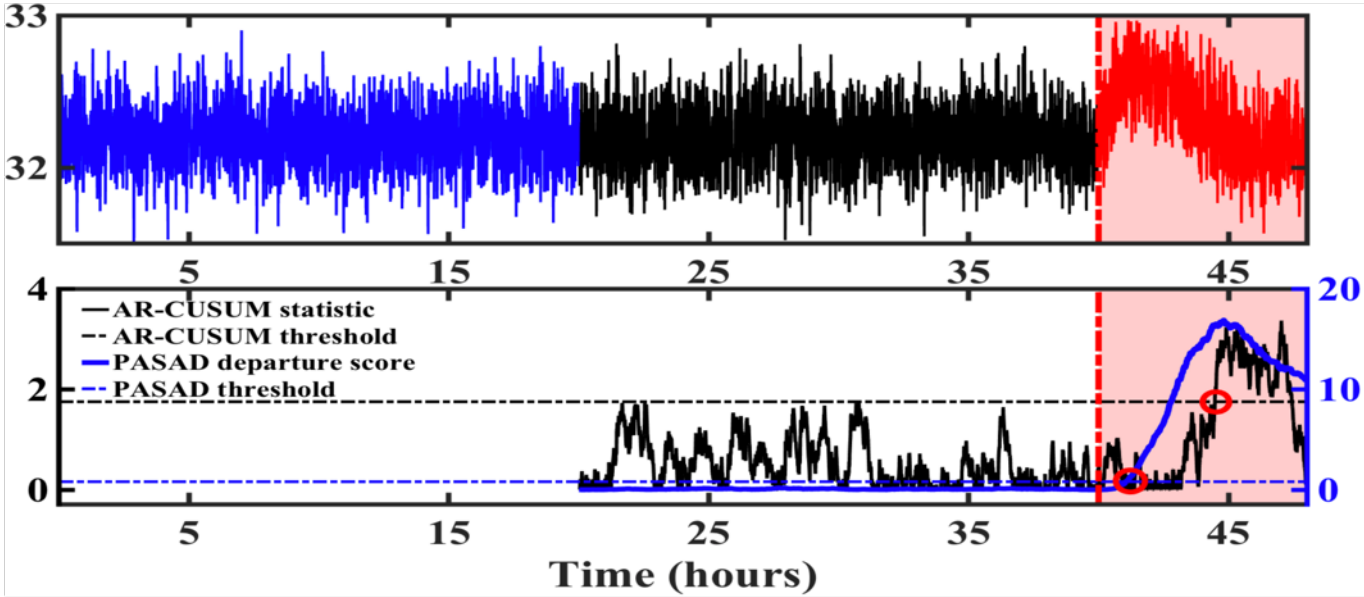
Visualization



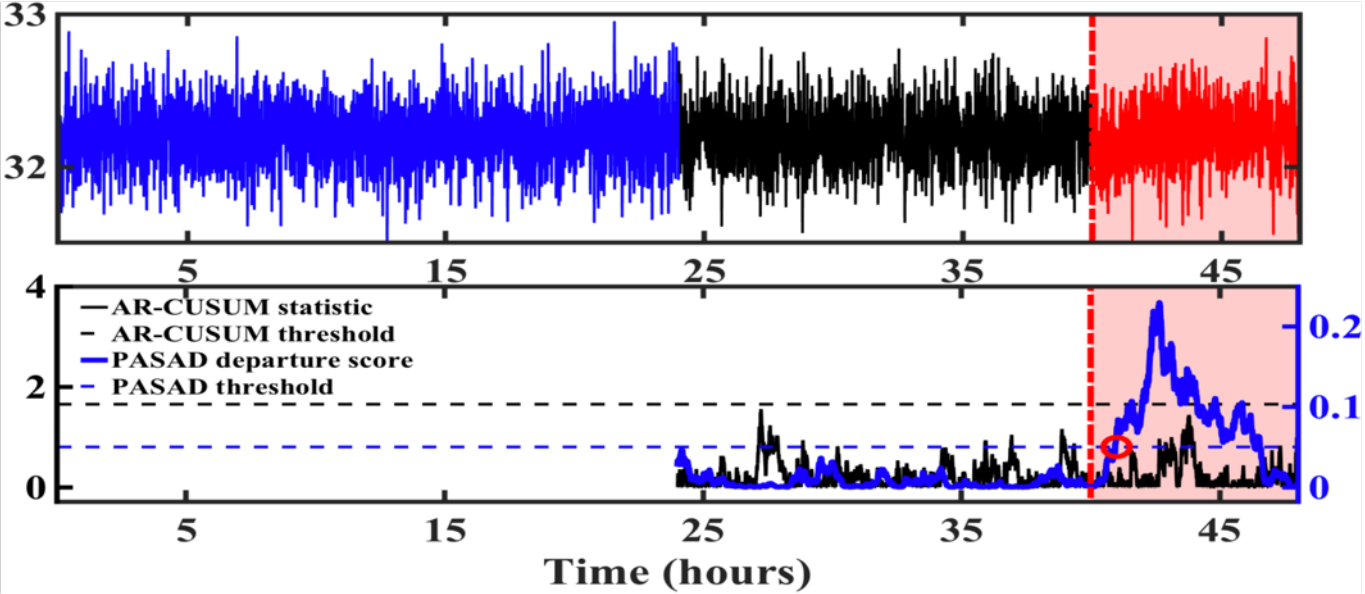
Visualization



Experimental Results



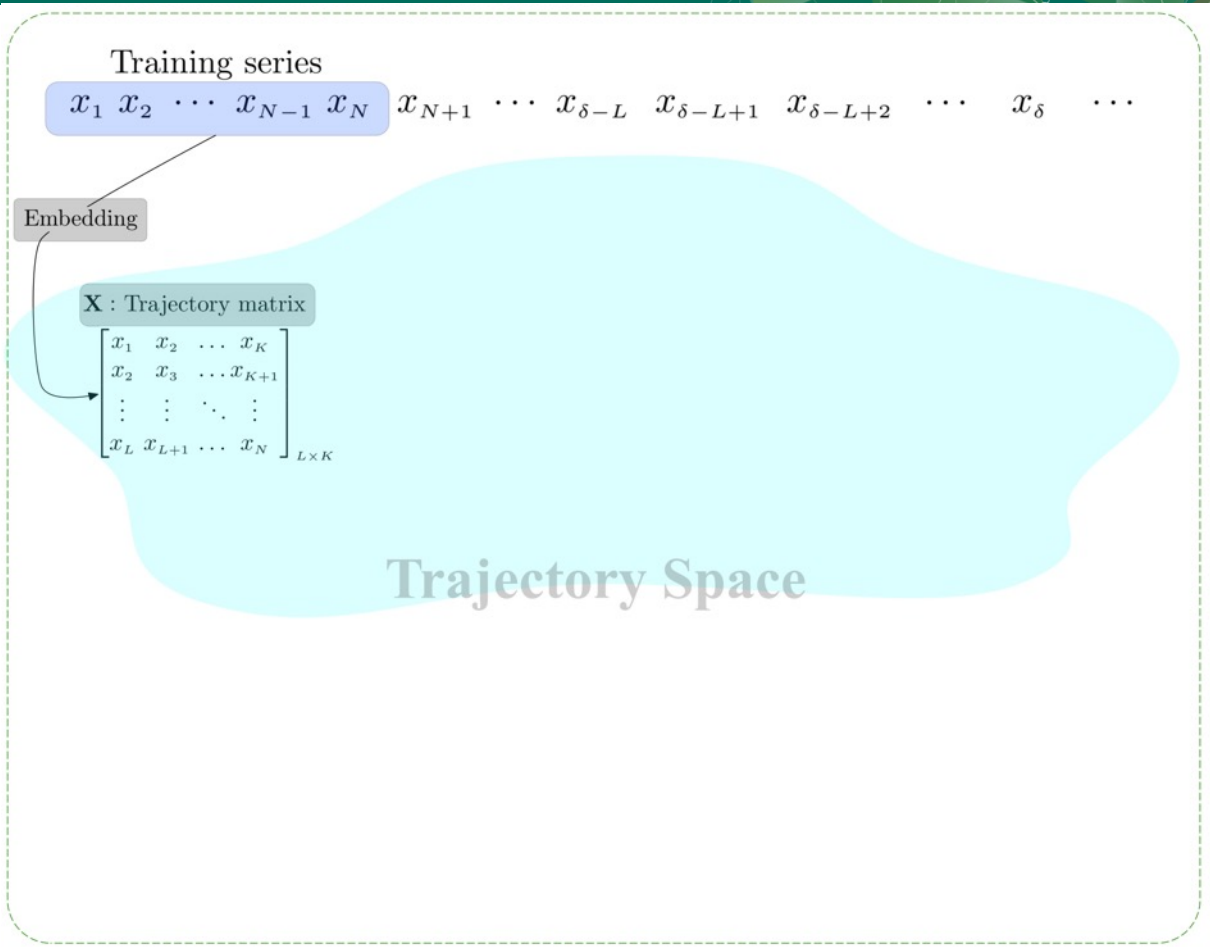
Experimental Results

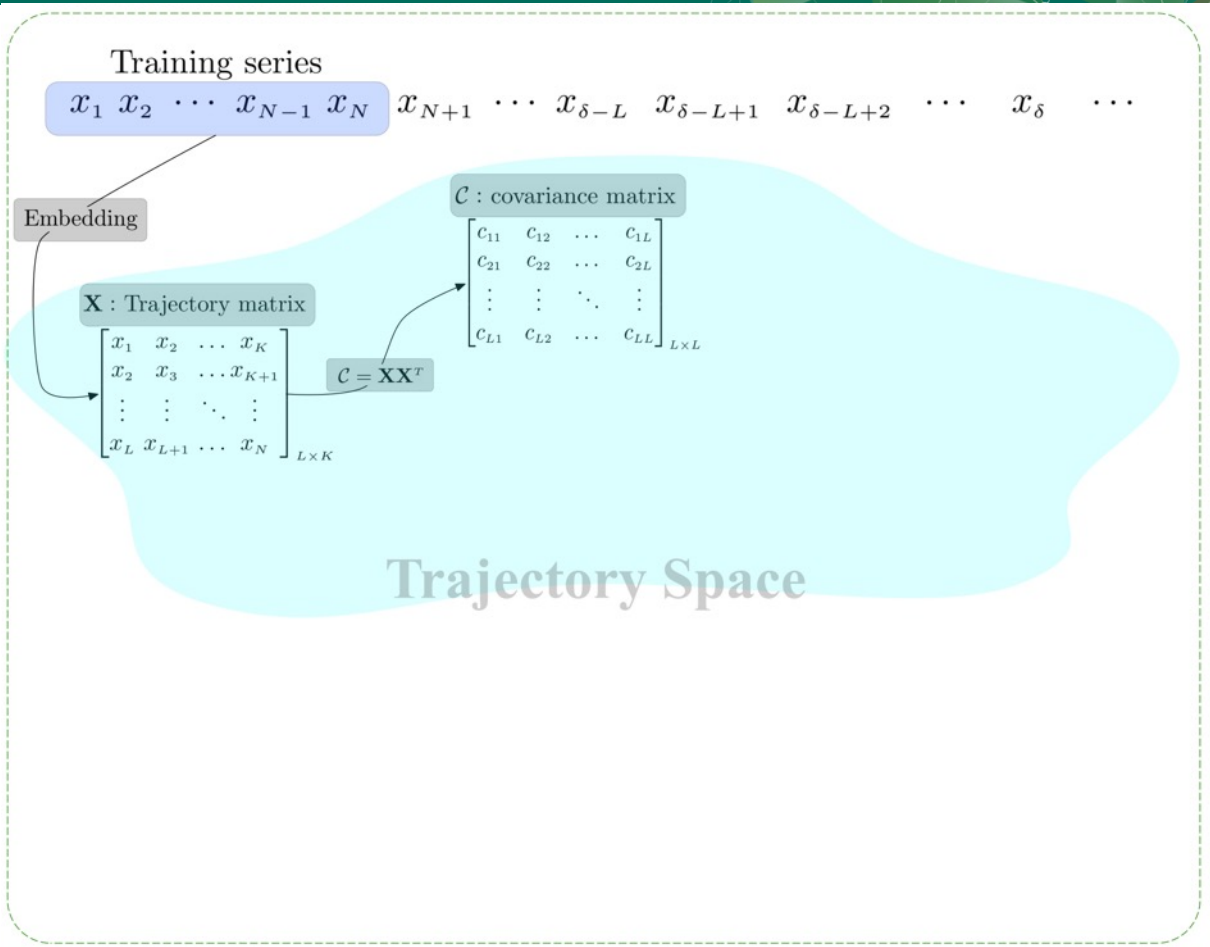


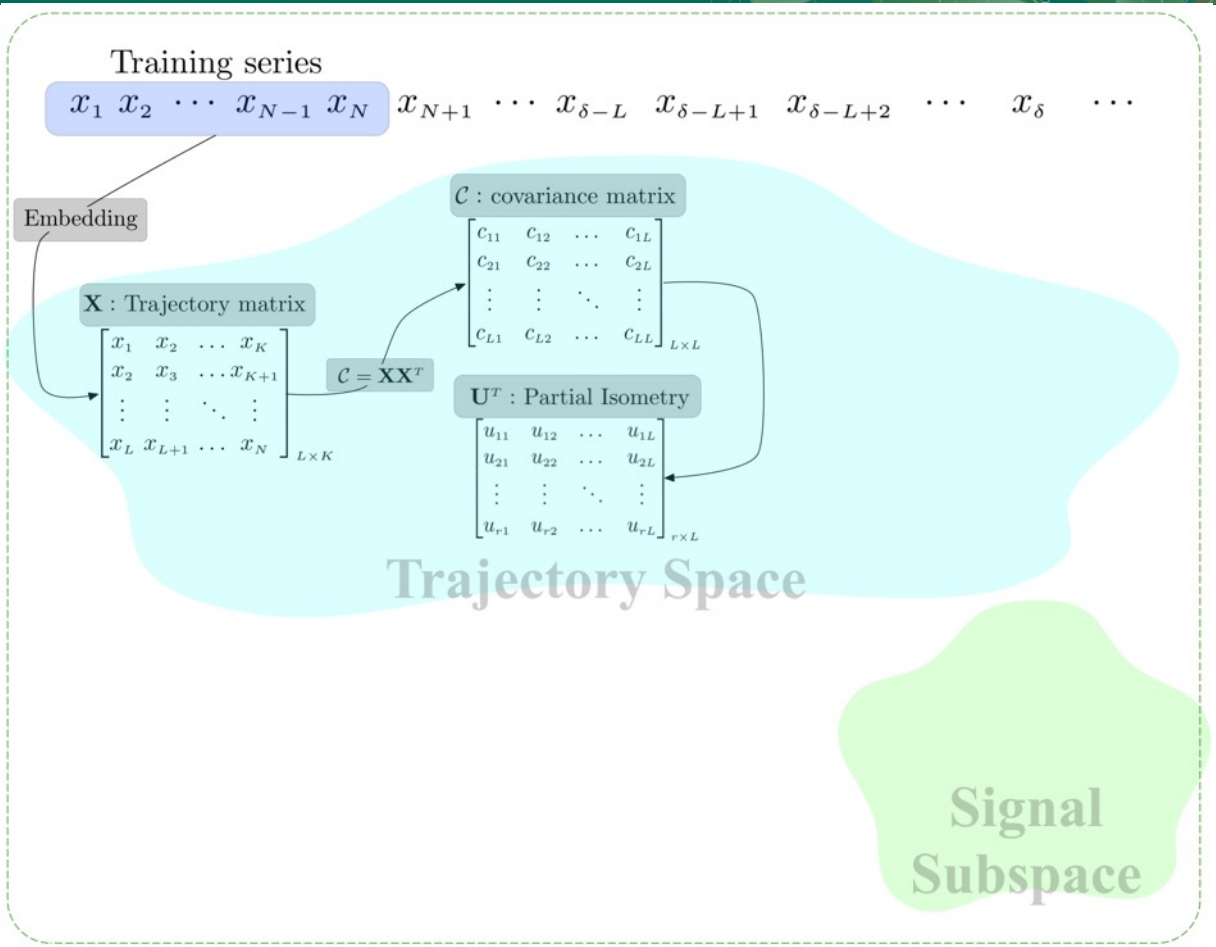
$$x_1 \; x_2 \; \cdots \; x_{N-1} \; x_N \; x_{N+1} \; \cdots \; x_{\delta-L} \; x_{\delta-L+1} \; x_{\delta-L+2} \; \cdots \; x_\delta \; \cdots$$

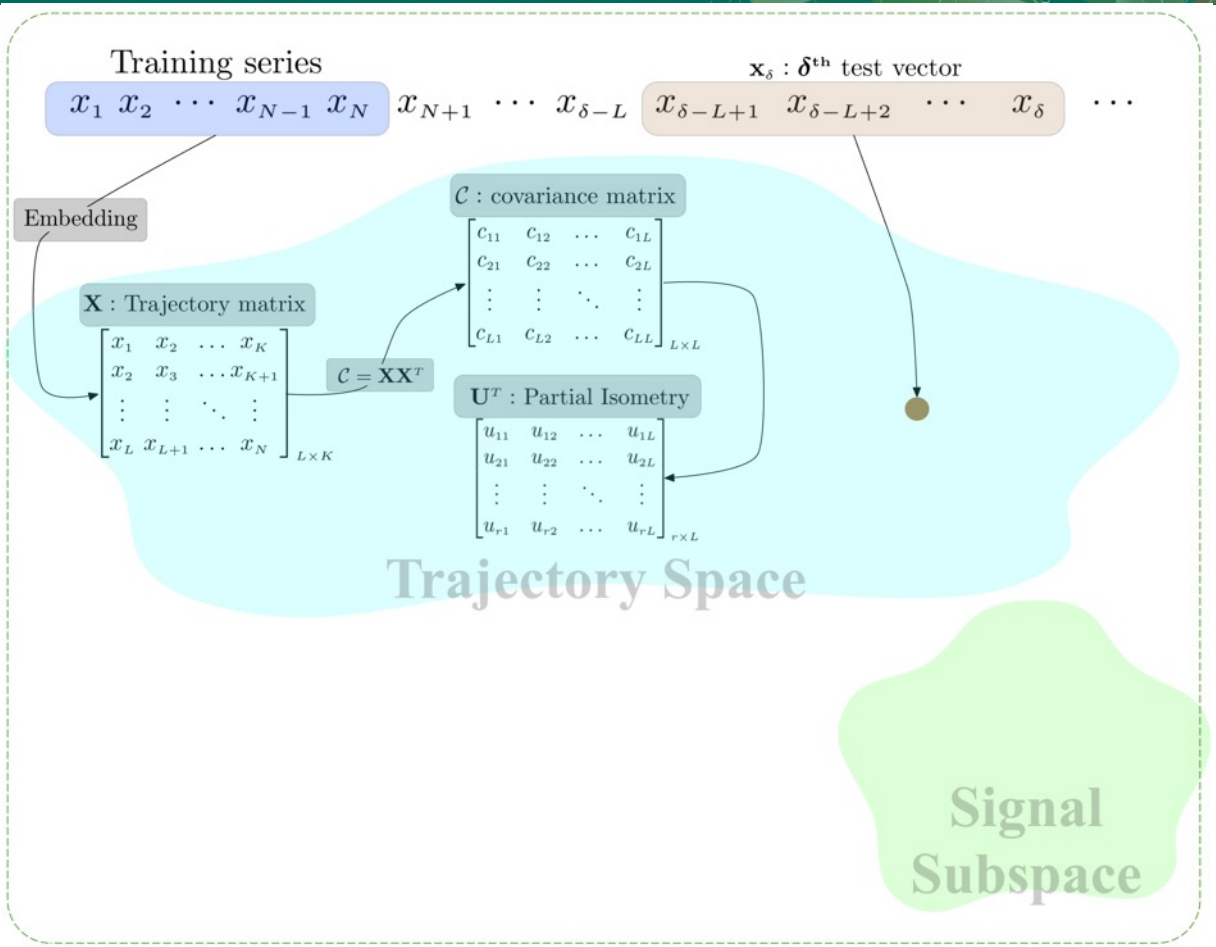
Training series

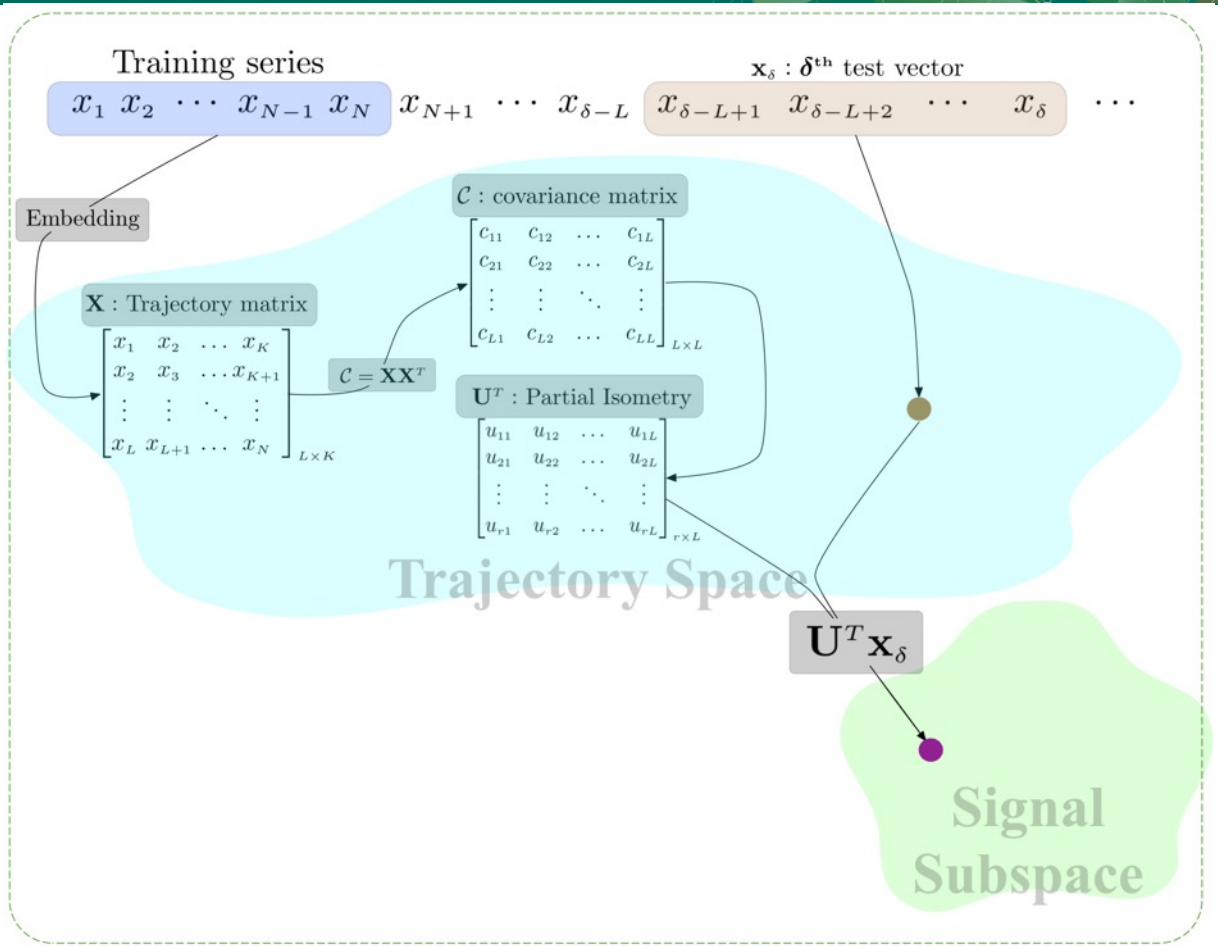
$$x_1 \; x_2 \; \cdots \; x_{N-1} \; x_N \; x_{N+1} \; \cdots \; x_{\delta-L} \; x_{\delta-L+1} \; x_{\delta-L+2} \; \cdots \; x_\delta \; \cdots$$

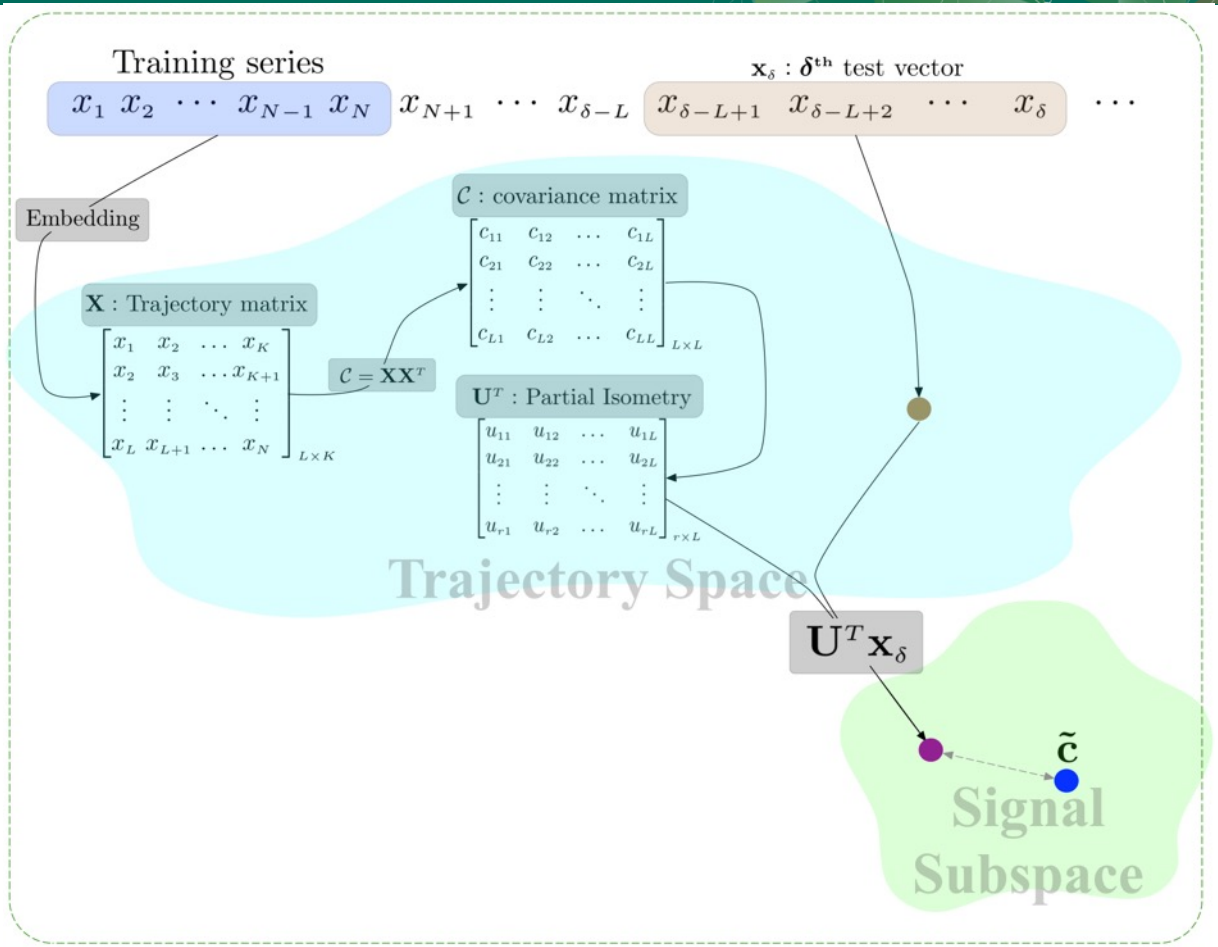

Training series
$x_1\ x_2\ \cdots\ x_{N-1}\ x_N\ x_{N+1}\ \cdots\ x_{\delta-L}\ x_{\delta-L+1}\ x_{\delta-L+2}\ \cdots\ x_\delta\ \cdots$
Embedding
X : Trajectory matrix
$\begin{bmatrix} x_1 & x_2 & \dots & x_K \\ x_2 & x_3 & \dots & x_{K+1} \\ \vdots & \vdots & \ddots & \vdots \\ x_L & x_{L+1} & \dots & x_N \end{bmatrix}_{L\times K}$
Trajectory Space

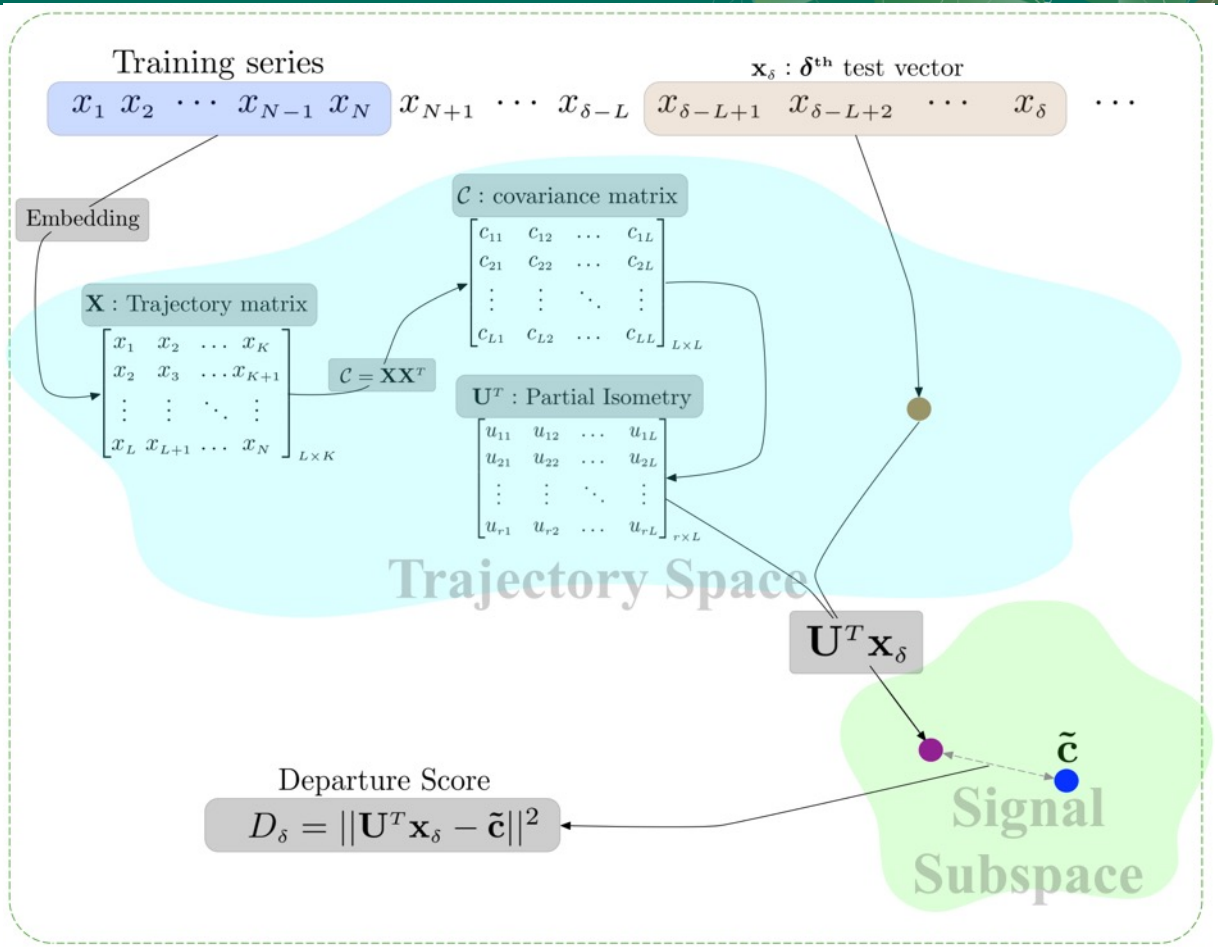

Training series
$x_1\ x_2\ \cdots\ x_{N-1}\ x_N\ x_{N+1}\ \cdots\ x_{\delta-L}\ x_{\delta-L+1}\ x_{\delta-L+2}\ \cdots\ x_\delta\ \cdots$
Embedding
$\mathcal{C}$: covariance matrix
$\begin{bmatrix} c_{11} & c_{12} & \dots & c_{1L} \\ c_{21} & c_{22} & \dots & c_{2L} \\ \vdots & \vdots & \ddots & \vdots \\ c_{L1} & c_{L2} & \dots & c_{LL} \end{bmatrix}_{L\times L}$
$\mathbf{X}$: Trajectory matrix
$\begin{bmatrix} x_1 & x_2 & \dots & x_K \\ x_2 & x_3 & \dots & x_{K+1} \\ \vdots & \vdots & \ddots & \vdots \\ x_L & x_{L+1} & \dots & x_N \end{bmatrix}_{L\times K}$
$\mathcal{C} = \mathbf{X}\mathbf{X}^T$
Trajectory Space


Training series
$x_1\ x_2\ \cdots\ x_{N-1}\ x_N\ x_{N+1}\ \cdots\ x_{\delta-L}\ x_{\delta-L+1}\ x_{\delta-L+2}\ \cdots\ x_\delta\ \cdots$
Embedding
$\mathbf{X}$: Trajectory matrix
$\begin{bmatrix} x_1 & x_2 & \dots & x_K \\ x_2 & x_3 & \dots & x_{K+1} \\ \vdots & \vdots & \ddots & \vdots \\ x_L & x_{L+1} & \dots & x_N \end{bmatrix}_{L\times K}$
$\mathcal{C} = \mathbf{X}\mathbf{X}^T$
$\mathcal{C}$: covariance matrix
$\begin{bmatrix} c_{11} & c_{12} & \dots & c_{1L} \\ c_{21} & c_{22} & \dots & c_{2L} \\ \vdots & \vdots & \ddots & \vdots \\ c_{L1} & c_{L2} & \dots & c_{LL} \end{bmatrix}_{L\times L}$
$\mathbf{U}^T$: Partial Isometry
$\begin{bmatrix} u_{11} & u_{12} & \dots & u_{1L} \\ u_{21} & u_{22} & \dots & u_{2L} \\ \vdots & \vdots & \ddots & \vdots \\ u_{r1} & u_{r2} & \dots & u_{rL} \end{bmatrix}_{r\times L}$
Trajectory Space
Signal Subspace


Training series
$x_1\ x_2\ \cdots\ x_{N-1}\ x_N\ x_{N+1}\ \cdots\ x_{\delta-L}\ x_{\delta-L+1}\ x_{\delta-L+2}\ \cdots\ x_\delta\ \cdots$
$\mathbf{x}_\delta$: $\boldsymbol{\delta}^{\mathbf{th}}$ test vector
Embedding
$\mathcal{C}$: covariance matrix
$\mathbf{X}$: Trajectory matrix
$\mathcal{C} = \mathbf{X}\mathbf{X}^T$
$\mathbf{U}^T$: Partial Isometry
Trajectory Space
Signal Subspace


Training series
$x_1\ x_2\ \cdots\ x_{N-1}\ x_N\ x_{N+1}\ \cdots\ x_{\delta-L}\ x_{\delta-L+1}\ x_{\delta-L+2}\ \cdots\ x_\delta\ \cdots$
$\mathbf{x}_\delta$: $\boldsymbol{\delta}^{\mathbf{th}}$ test vector
Embedding
$\mathcal{C}$: covariance matrix
$\mathbf{X}$: Trajectory matrix
$\mathcal{C} = \mathbf{X}\mathbf{X}^T$
$\mathbf{U}^T$: Partial Isometry
Trajectory Space
$\mathbf{U}^T\mathbf{x}_\delta$
Signal Subspace


Training series
$x_1\ x_2\ \cdots\ x_{N-1}\ x_N\ x_{N+1}\ \cdots\ x_{\delta-L}\ x_{\delta-L+1}\ x_{\delta-L+2}\ \cdots\ x_\delta\ \cdots$
$\mathbf{x}_\delta$: $\boldsymbol{\delta}^{\text{th}}$ test vector
Embedding
$\mathcal{C}$: covariance matrix
$\mathbf{X}$: Trajectory matrix
$\mathcal{C} = \mathbf{X}\mathbf{X}^T$
$\mathbf{U}^T$: Partial Isometry
Trajectory Space
$\mathbf{U}^T\mathbf{x}_\delta$
$\tilde{\mathbf{c}}$
Signal Subspace


Training series
$x_1\ x_2\ \cdots\ x_{N-1}\ x_N\ x_{N+1}\ \cdots\ x_{\delta-L}\ x_{\delta-L+1}\ x_{\delta-L+2}\ \cdots\ x_\delta\ \cdots$
$\mathbf{x}_\delta$: $\boldsymbol{\delta}^{\text{th}}$ test vector
Embedding
$\mathcal{C}$: covariance matrix
$\mathbf{X}$: Trajectory matrix
$\mathcal{C} = \mathbf{X}\mathbf{X}^T$
$\mathbf{U}^T$: Partial Isometry
Trajectory Space
$\mathbf{U}^T\mathbf{x}_\delta$
$\tilde{\mathbf{c}}$
Signal Subspace
Departure Score
$D_\delta = ||\mathbf{U}^T\mathbf{x}_\delta - \tilde{\mathbf{c}}||^2$

CHALMERS

UNIVERSITY OF TECHNOLOGY