Failure Diagnosis and Cyber Intrusion Detection in Transmission Protection System Assets Using Synchrophasor Data

Anurag Srivastava, Bo Cui, P. Banerjee

Washington State University

WASHINGTON STATE UNIVERSITY

SGDRIL
Smart Grid Demonstration & Research Investigation Lab, Washington State University, Pullman

NASPI March 2017

Outline

Motivation

Work Plan

- PMUs Data Anomalies Detection
- Physical Failure Detection in Substation Assets
- Cyber Intrusion Detection
- Assets Failure Detection

Test Cases and Modeled Scenarios

- Opal-RT and Computer-Aided Protection Engineering (CAPE)
- Case studies

Simulation Results

- PMU data anomalies detection
- Physical Failure Diagnosis
- Substation level cyber intrusions detection

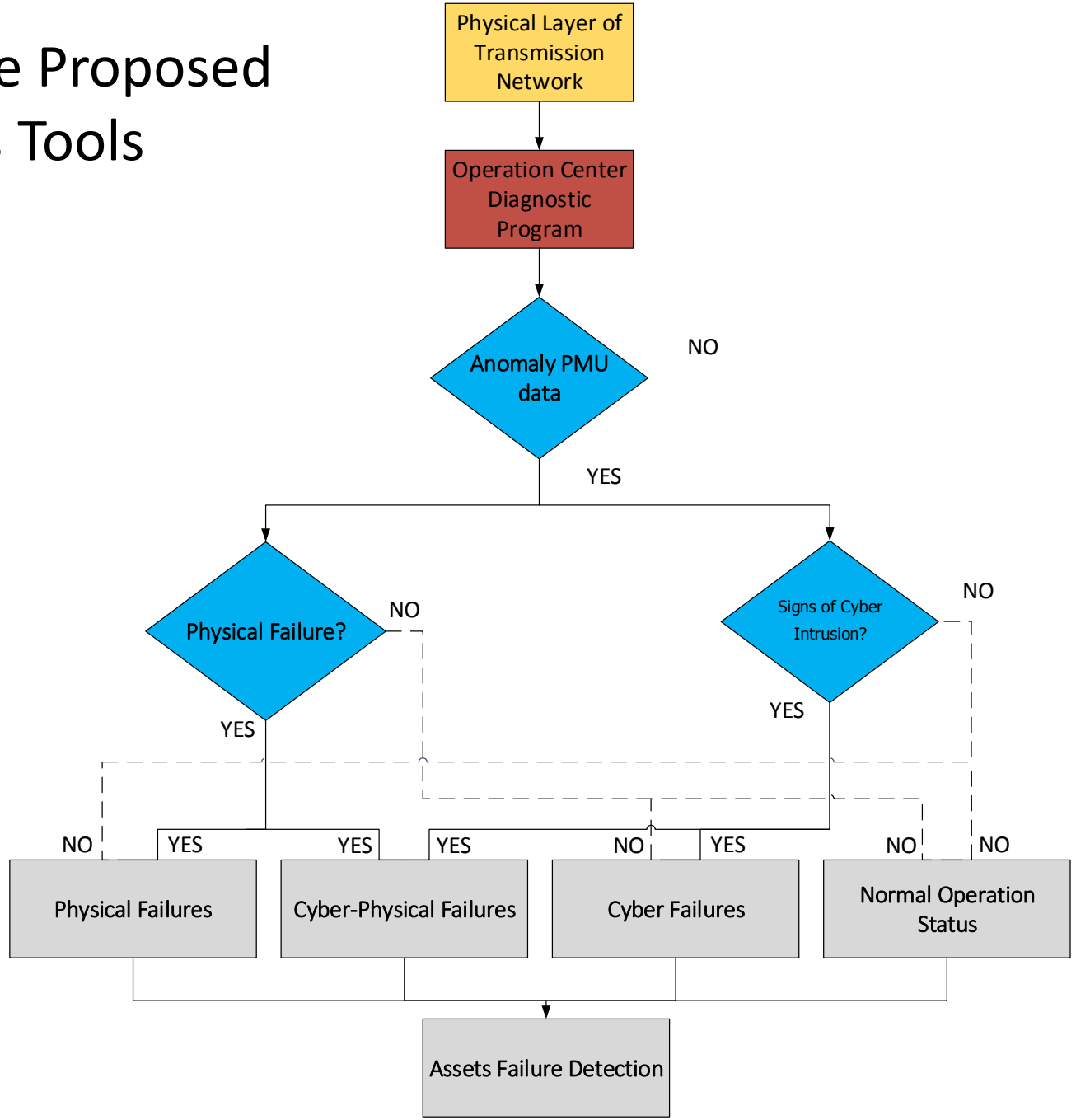
Summary

Motivation

- The outage area in transmission network is significantly extended if malfunctions or failures occurs in the protective devices themselves.
- Protection system mis-operation is a top concern among the priority list by NERC to maintain the grid reliability**.
- The protection system mis-operation can be caused not only by physical devices failure but also substations level cyber intrusions
- The potential threats from substations level cyber intrusions is not well practiced.

- *Based on the NERC report, available at http://www.nerc.com/docs/docs/blackout/NERC_Final_Blackout_Report_07_13_04.pdf
- ** Based on the NERC report, available at http://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/2015%20State%20of%20Reliability.pdf and at http://www.nerc.com/docs/pc/spctf/Redundancy_Tech_Ref_1-14-09.pdf

Work Plan for the Proposed Failure Diagnosis Tools



Goal: Detecting Anomalies in PMU data

Chebyshev bad data detection

- First stage, $k_1 = \frac{1}{\sqrt{P_1}}$
- Then the upper and lower bounds for stage 1 can be developed as
- $\mathrm{ODV}_{1U} = \mu_1 + k_1 * \sigma_1$
- $\mathrm{ODV}_{1L} = \mu_1 - k_1 * \sigma_1$
- Second Stage:$k_2 = \frac{1}{\sqrt{P_2}}$
- And for the upper and lower level bounds for stage 2 can be determined as
- $\mathrm{ODV}_{2U} = \mu_2 + k_2 * \sigma_2$
- $\mathrm{ODV}_{2L} = \mu_2 - k_2 * \sigma_2$
- All the data point lies upper than upper bound or lower than lower bound will be identified as an outlier*.

*Help from Mengze Zhou and Dr. Yinghui Wu at WSU for this task is appreciated

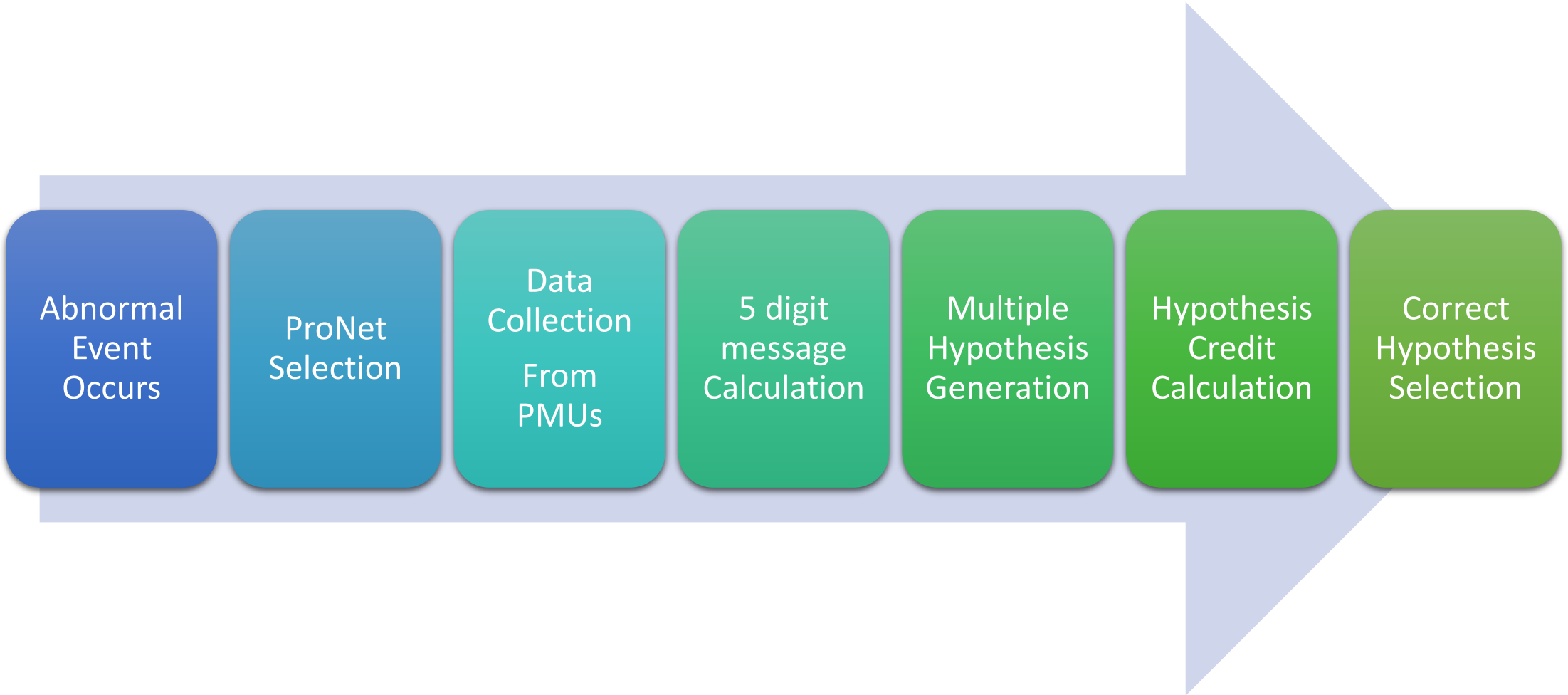
Goal: Detecting Anomalies in PMU data

Detecting Anomalies using Local State Estimation (LSE)

- The local substation level state estimation techniques is proposed to detect anomaly in synchrophasor measurements data.
- The developed LSE go back to predefined database to find the substations with abnormal PMU data based on the bad data in local state estimator.

Failure Diagnosis in Physical System

Goal: Physical Diagnosis



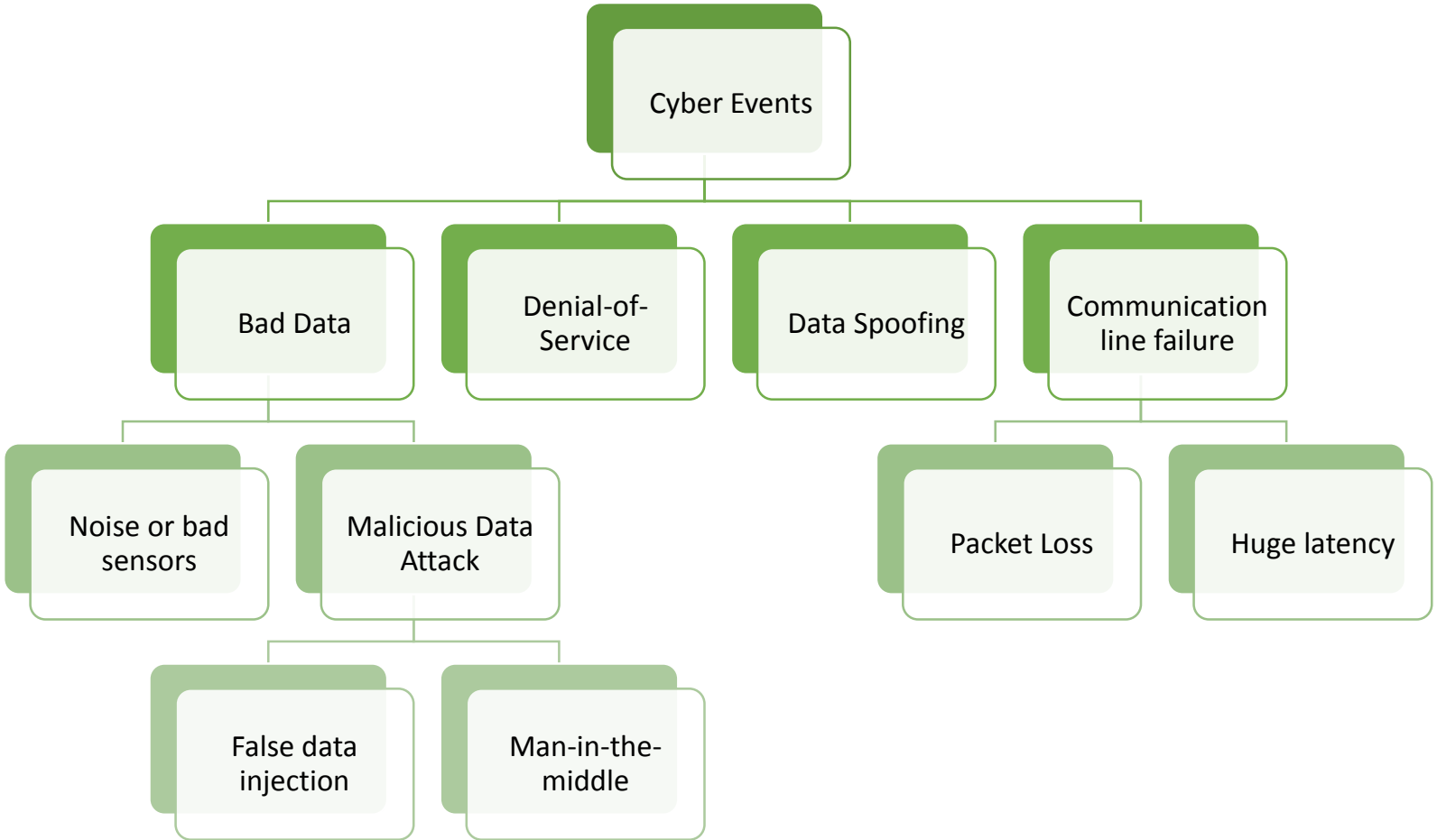
Goal: Cyber Intrusions Detection

Failure Diagnosis in Cyber System

- The existing power grid transmission system is vulnerable to malicious cyber attacks with greater complexity and more communication devices.
- However, the increasing number installation of Phasor Measurement Units (PMUs) improves power grid resilience and reliability by reducing the number and duration of outages.
- So the cyber attacks target on power system transmission system substations has been addressed via PMUs measurement data analysis combined with substations computer network log files.

Goal: Cyber Intrusions Detection

Possible Failures in Cyber part



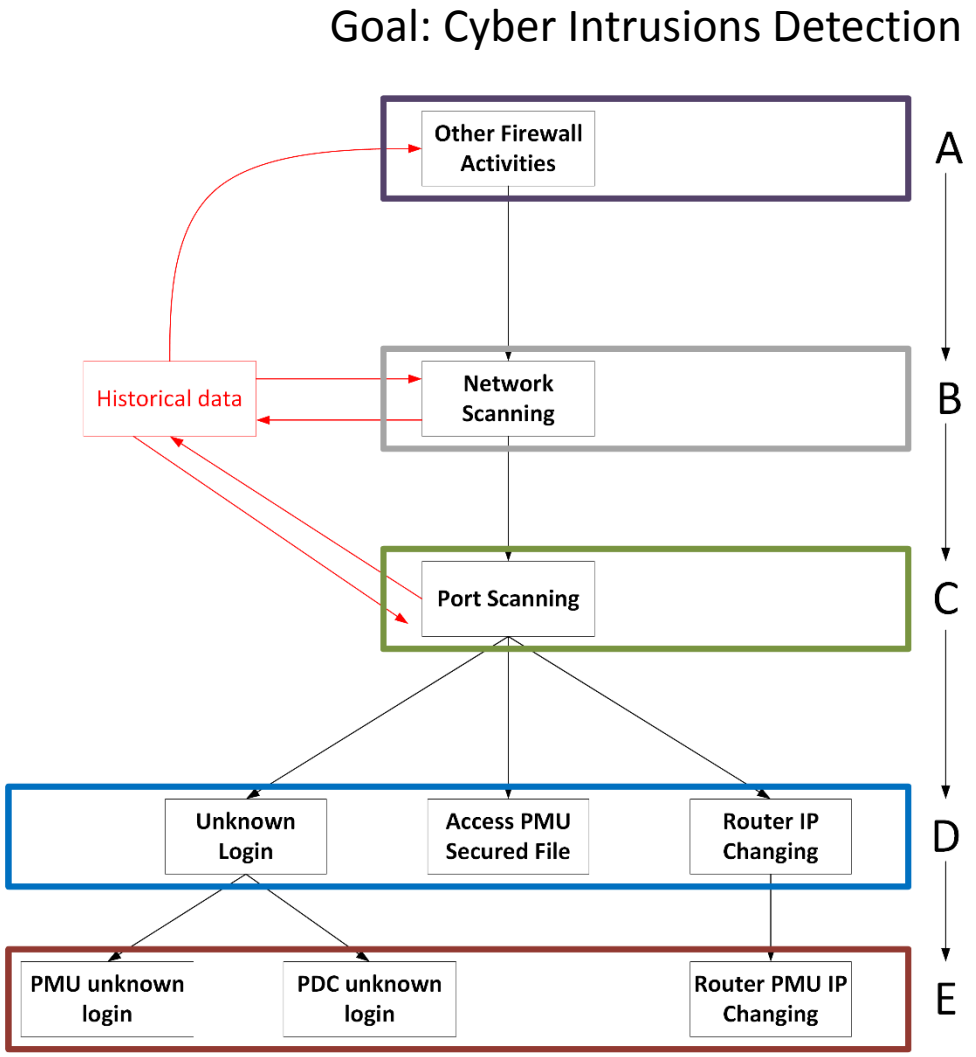
Goal: Cyber Intrusions Detection

Substations Vulnerabilities analysis

- Communication Links Damage: Routers have to rebuild their routing tables following a link failure, therefore all the delays (processing delay, queuing delay, transmission delay, propagation delay) of the communication increase.
- Denial of Service: DoS attack can happen in the all-PMU state estimator if a number of computers or network devices in the Intranet are controlled by Trojans.
- Data Spoofing: It is also possible that the PMUs in the system are hacked by adversaries. Then the adversaries can arbitrarily manipulate the measurement data without being detected.

Application of Communication Network Log Files

- To identify the cyber attack using cyber information, three different similarity calculation methods are employed to calculate the similarity index between real event and typical substation cyber intrusion. The three similarities will vote to determine if the log files are abnormal.



Similarity Calculation

Goal: Cyber Intrusions Detection

- **Cosine Similarity**

- Given two vectors of attributes, A and B, the cosine similarity, cos(θ), is represented using a dot product and magnitude as

- $Similarity = \cos(\theta) = \frac{A \cdot B}{\|A\|\|B\|} = \frac{\sum_{i=1}^{n} A_i B_i}{\sqrt{\sum_{i=1}^{n} A_i^2} \sqrt{\sum_{i=1}^{n} B_i^2}}$

- **Euclidean Distance Similarity**

- In Cartesian coordinates, if p = (p1, p2,..., pn) and q = (q1, q2,..., qn) are two points in Euclidean n-space, then the distance (d) from p to q, or from q to p is given by the Pythagorean formula:

- $Distance(p, q) = \sqrt{(q_1 - p_1)^2 + (q_2 - p_2)^2 + \cdots + (q_n - p_n)^2} = \sqrt{\sum_{i=1}^{n} (q_i - p_i)^2}$

- **Jaccard Index**

- The Jaccard coefficient measures similarity between finite sample sets, and is defined as the size of the intersection divided by the size of the union of the sample sets:

- $J(A, B) = \frac{|A \cap B|}{|A \cup B|} = \frac{|A \cap B|}{|A| + |B| - |A \cap B|}$

Threshold for each similarity calculation method

COSINE SIMILARITY THRESHOLD

Threat Type	Threshold Range
No Threat	$0 \sim 0.5$
Cyber Intrusion	$0.5 \sim 0.65$
PMU Related Cyber Intrusion	$0.65 \sim 1$

EUCLIDEAN DISTANCE SIMILARITY THRESHOLD

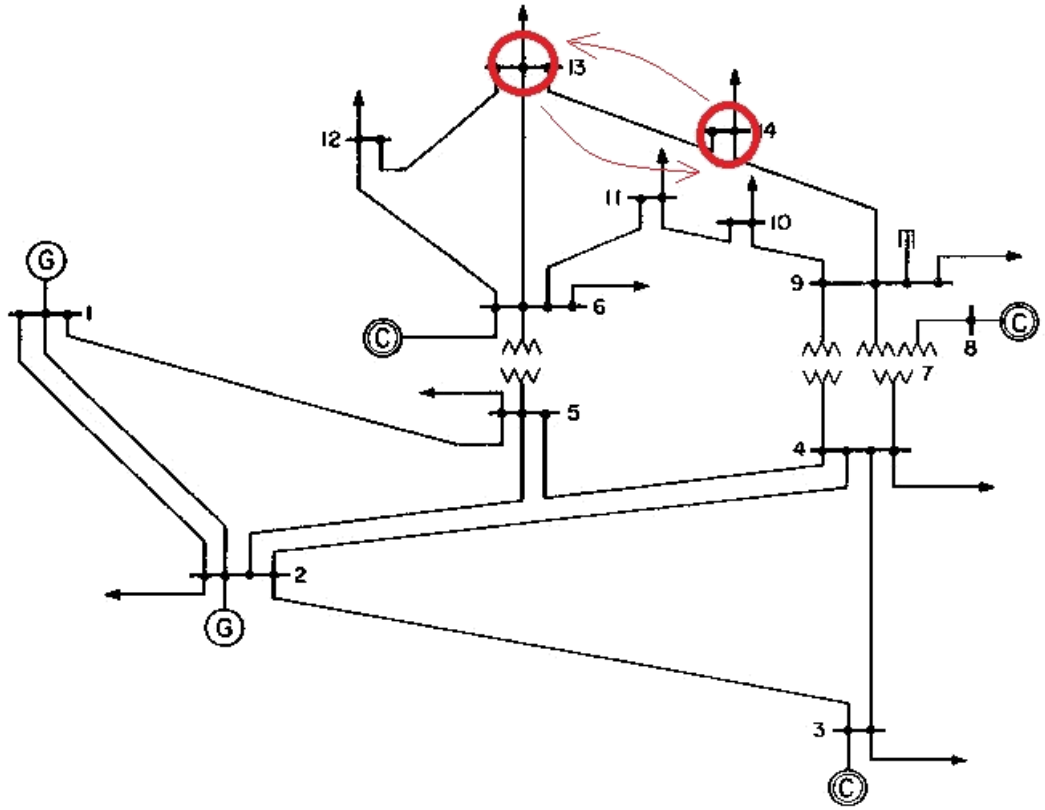
Threat Type	Threshold Range
No Threat	$73 \sim 75$
Cyber Intrusion	$44 \sim 73$
PMU Related Cyber Intrusion	$0 \sim 44$

JACCARD INDEX THRESHOLD

Threat Type	Threshold Range
No Threat	$0 \sim 0.2$
Cyber Intrusion	$0.2 \sim 0.55$
PMU Related Cyber Intrusion	$0.55 \sim 1$

Simulation Results

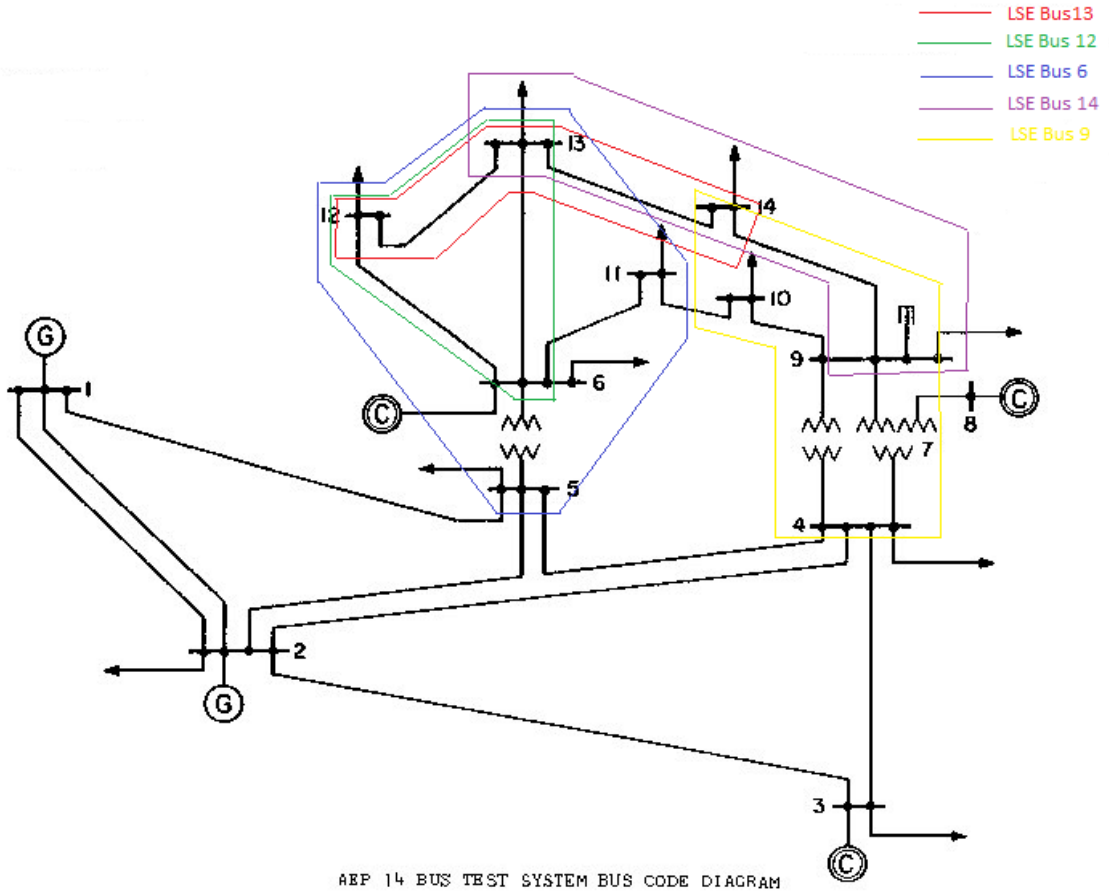
Scenarios: PMU data anomalies detection using local state estimation



- For this scenario, the measurements data from Bus 13 and Bus 14 has been swapped.
- The state estimation for 14 bus system will flag a bad data appearance in the grid.
- Local state estimation (LSE) has been applied and Cyber failure diagnosis program is executed.

Goal: Detecting Anomalies in PMU data

Simulation Example



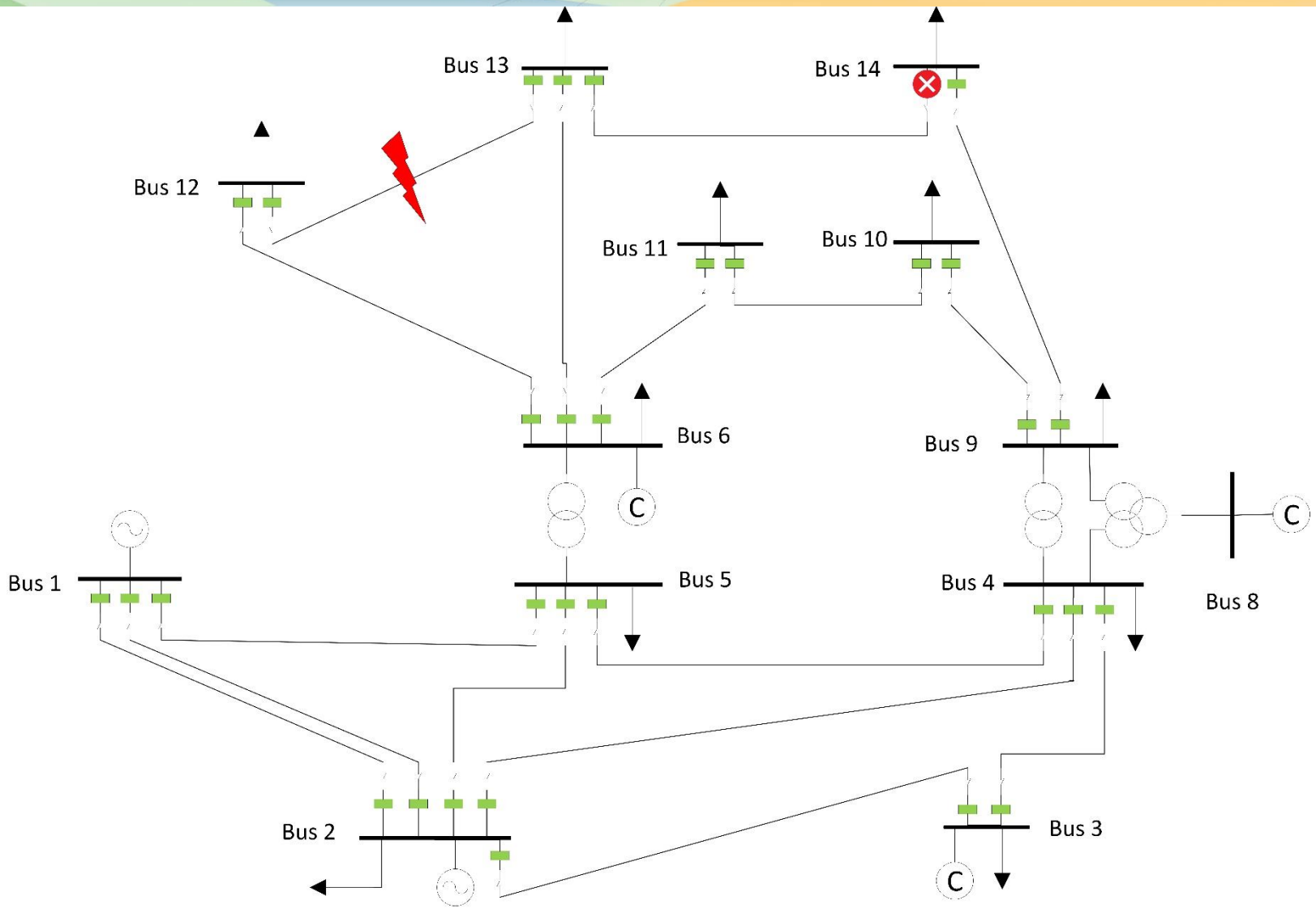
- LSE has been applied to each bus in the system and least square bad data detection is also used.
- For this scenario, the LSE that detects bad data are Bus 6, 9, 12, 13, 14.
- The system will query the pre-defined database for event bus number set {6, 9, 12, 13, 14}, the database returns the corresponding related Bus number {13, 14}

Physical Failure Diagnosis Example

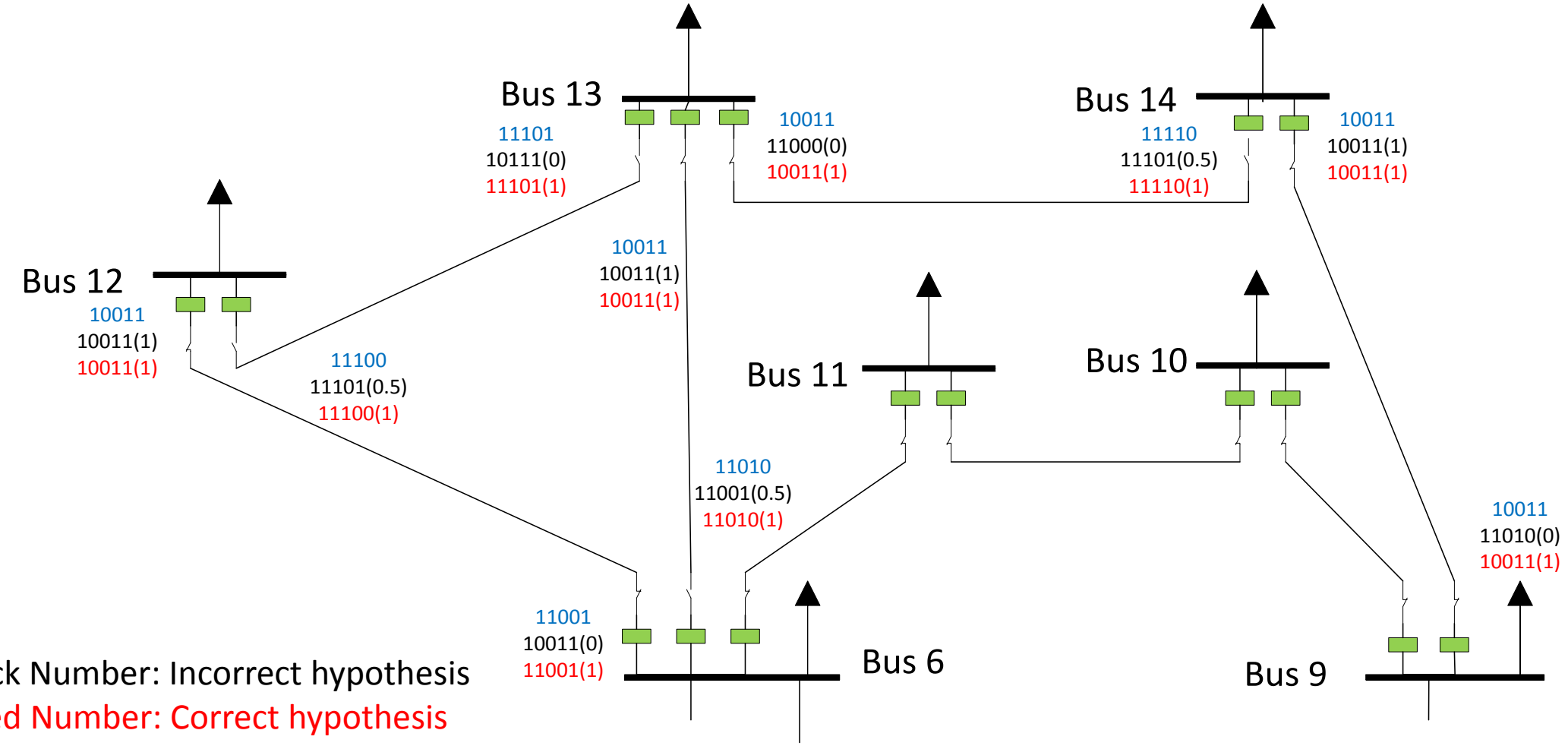
Fault at 12-13,
Breaker 14-13 malfunctioned

Two possible explanations:
1. Fault at 12-13,
Breaker 14-13 malfunctioned

2. Fault at 13-14,
Breaker 13-14 failed
Breaker 13-12 malfunctioned



Physical Failure Diagnosis Results



Black Number: Incorrect hypothesis

Red Number: Correct hypothesis

Simulation Results

Scenarios: Substations Level Cyber Intrusions Detection

Scenario 1:

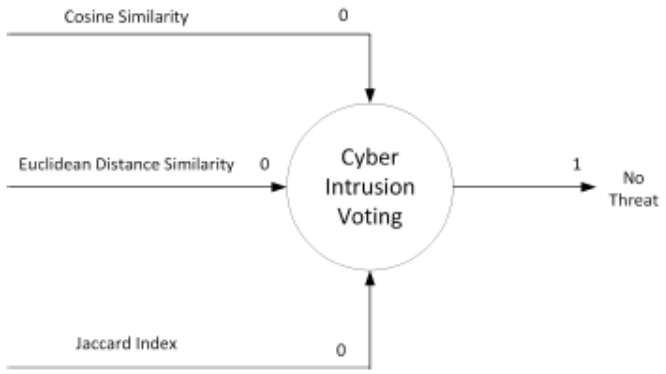
Network Connections Accessed
No further attack

CYBER INTRUSION VECTOR

A	B	C	D	E
1	1	0	0	0

SIMILARITY CALCULATION RESULTS OF SCENARIO 1

Similarity Computing Method	Similarity results
Cosine Similarity	0.2462
Euclidean Distance Similarity	73.6546
Jaccard Index	0.1026



Scenario 2:

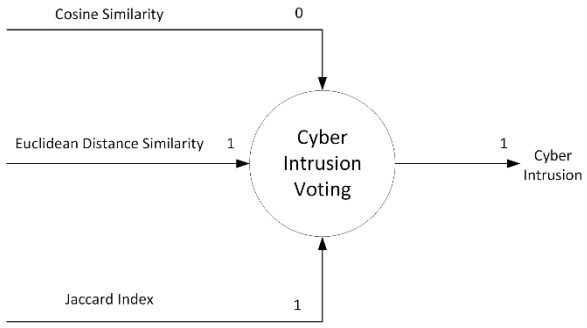
The network connections has been scanned to find potential ports or IP addresses to attack

CYBER INTRUSION VECTOR

A	B	C	D	E
1	1	1	0	0

SIMILARITY CALCULATION RESULTS OF SCENARIO 2

Similarity Computing Method	Similarity results
Cosine Similarity	0.4606
Euclidean Distance Similarity	72.1110
Jaccard Index	0.2308



Scenario 3:

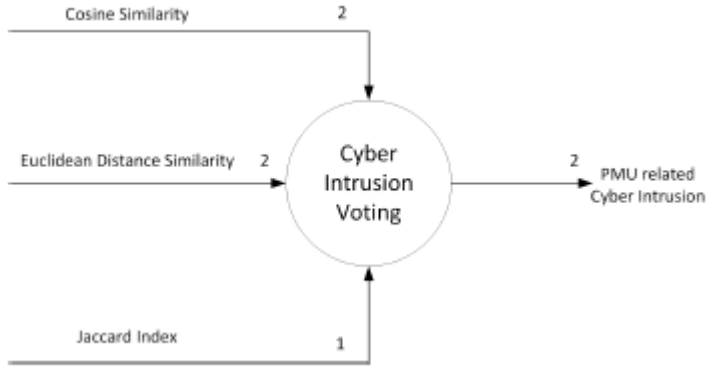
The PMU level data has been accessed by intruders
Past activities has been wiped

CYBER INTRUSION VECTOR

A	B	C	D	E
0	0	0	0	1

SIMILARITY CALCULATION RESULTS OF SCENARIO 3

Similarity Computing Method	Similarity results
Cosine Similarity	0.7006
Euclidean Distance Similarity	43.4741
Jaccard Index	0.5128

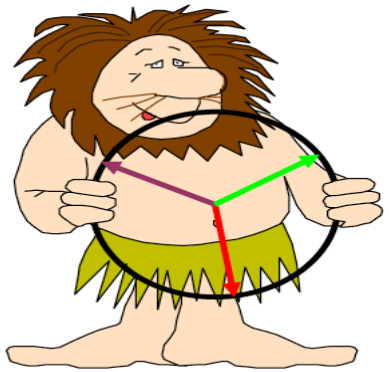


Summary

- An automated failure diagnosis method has been developed for the physical part of the CPS.
- A set of methodologies has been derived for failures detection and identification purpose which can do diagnosis for the cyber part of CPS.
- Developed methods are fast and accurate which can respond to system event quickly.
- The coordination of two methods can be used for failure diagnosis work in CPS.
- The quick results can contribute to failure prognosis and cascading outages prevention (future investigation).

Acknowledgements

- We would like to acknowledge the support from National Science Foundation and related work at WSU.
- We would also like to acknowledge the software support from Electrocon International Inc. for Computer-Aided Protection Engineering (CAPE) and Opal-RT Technologies for Opal-RT.
- Support for Schweitzer Engineering Lab (SEL) is appreciated specially for discussion on GPS spoofing
- Thanks to NASPI community to provide this opportunity to discuss our work



SGDRIL

Smart Grid Demonstration & Research Investigation Lab, Washington State University, Pullman