Online Robust PCA for Malicious Attack-Resilient Wide Area Monitoring

Student: Kaveri Mahapatra[1], Co-PI: Nilanjan Ray Chaudhuri[1], PI: Rajesh Kavasseri[2], Co-PI: Sukumar Brahma[3]

[1]The Pennsylvania State University, University Park, PA, [2]North Dakota State University, Fargo, ND, [3]Clemson University, Clemson, SC

https://www.nsf.gov/awardsearch/showAward?AWD_ID=1544621

PROBLEM/CONTEXT

One wrong move by a protective relay during stressed operation can spell disaster for the power grid; Eg: 2003 NE Blackout.

Spurious or maliciously injected sensor data can seriously jeopardize the monitoring and stabilization controls of power grids

CHALLENGE

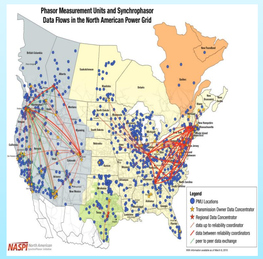
- *Can we leverage the physical system's expansive dynamic behavior to distinguish disturbances from data anomalies by extracting event fingerprints from wide area measurements? (NDSU + CU goals)*
- *How to ensure detection of data anomaly in such wide area measurements ? (PSU goals) To that end, the aim is to bridge the gap between developments in the area of Robust Principal Component Analysis (RPCA) – traditionally focused on the 'signals' side of the CPS, with the intrinsic properties of the system in terms of a Subspace Library from the 'systems' side of the CPS*

KEY IDEAS

- Identify the corrupted signals among a set of signals and quantify the amount of corruption present at any sampling instant by using an efficient convex optimization algorithm
- Leverage the physical system's expansive dynamic behavior to distinguish disturbances from data anomalies by extracting the lower dimensional property of wide area measurements in a subspace library representing system events
- Explore the effects of intelligent cyberattacks on PMU measurements to separate the anomalous signatures and correct the data for real-time applications

CONTRIBUTIONS

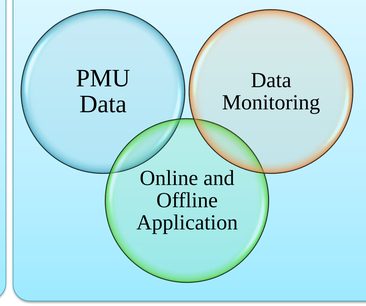
- Improved Data-driven supervisory intelligence with PMUs
- Fusion of sensory data with dynamic properties of physical system will help gaining fundamental insight into coupling between cyber and physical layer and use this knowledge to detect and separate spurious signals or malicious data manipulations originating from cyber-attacks



MAIN TASKS & DEVELOPMENTS

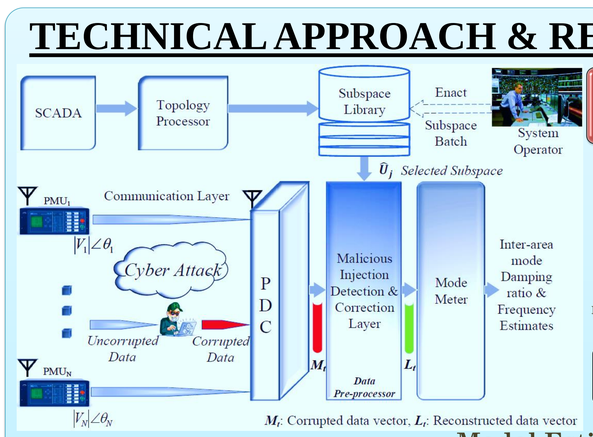
- A framework is established to analyze **dynamical response from a system using Synchrophasor data** under nominal and off-nominal (e.g. faulted) conditions
- An approach for **bad data detection in PMU measurements** during disturbances is proposed. The proposed approach can **distinguish between the outlier caused by bad data from those caused by disturbances**
- **A Principal component pursuit (PCP) technique** is proposed with an overlapping window framework of PMU measurements for anomalies in PMU data
- **An Online Robust PCA based architecture is proposed for malicious corruption-resilient wide-area mode metering application using a library of event subspaces**

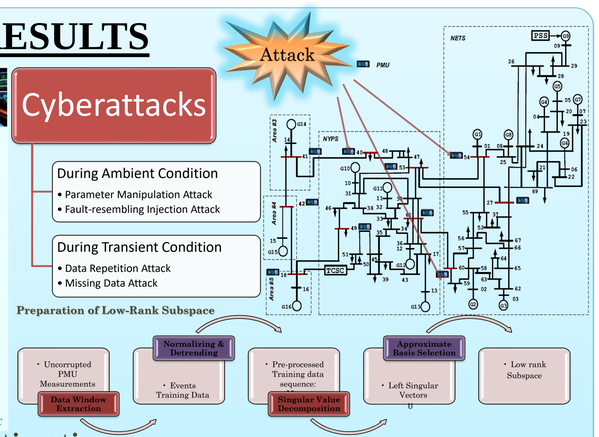
SCIENTIFIC IMPACT

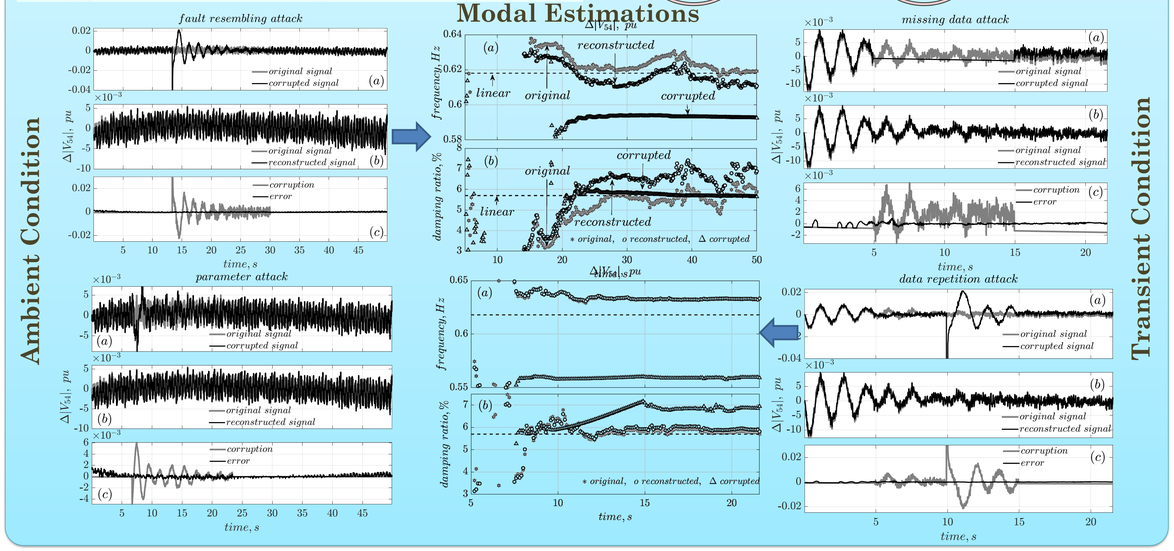


- An Architecture for Detection & Correction of Anomalies in PMU Data
- Improvised Event Detection in Power Systems
- Resiliency Against Malicious Injections caused by Cyberattacks
- Improved PMU Data Quality
- Subspace Library for Power System Events
- Improved Interarea Oscillation Monitoring
- Prevent System wide Blackouts

TECHNICAL APPROACH & RESULTS







EDUCATION & OUTREACH

- A new course on Advanced Power System Protection with digital relaying and wide area protection schemes will be introduced
- Module on applications of PMUs and findings from this project from this project will be introduced in courses

IMPACT ON SOCIETY

A reliable power system secure from cyberattacks reduces the enormous financial and societal costs associated with large scale outages and helps create an energy-infrastructure that is beneficial to the society and improves the quality of services along with better management of stresses in power systems

POTENTIAL IMPACT

- Protect critical infrastructures from cyber-attacks and facilitate improved system diagnosis, lower downtime, better service, and higher resiliency
- Secured sensory information can potentially benefit a wide range of CPS including process control, energy, and probably systems involving robots or even future transportation systems employing autonomous vehicles

PUBLICATIONS

1. *K. Mahapatra, N. R. Chaudhuri and R. G. Kavasseri, S. Brahma,* "Online Analytical Characterization of Outliers in Synchrophasor Measurements: A Singular Value Perturbation Viewpoint", published in IEEE Transactions on Power Systems.
2. *K. Mahapatra, N. R. Chaudhuri and R. Kavasseri,* "Bad data detection in PMU measurements using principal component analysis," *2016 North American Power Symposium (NAPS)*, Denver, CO, 2016.
3. *K. Mahapatra, N. R. Chaudhuri and R. Kavasseri,* "Online Bad Data Outlier Detection in PMU Measurements using PCA Feature-driven ANN Classifier" *2017 IEEE PES General Meeting.*
4. *K. Mahapatra, N. R. Chaudhuri,* "Malicious Corruption-Resilient Wide-Area Oscillation Monitoring using Online Robust PCA," *2018 IEEE PES General Meeting.*
5. *K. Mahapatra, N. R. Chaudhuri, "Online Robust PCA for Malicious Attack-Resilience in Wide-Area Mode Metering Application," submitted in in IEEE Transactions on Power Systems (under second review)*

PennState College of Engineering | ELECTRICAL ENGINEERING AND COMPUTER SCIENCE | EECS

CPS: Breakthrough: Collaborative Research: WARP: Wide Area assisted Resilient Protection

Award ID#: CNS 1544621