CPS: Synergy: Collaborative Research: A Unified System Theoretic Framework for Cyber Attack-Resilient Power Grid (NSF Award # CNS-1329915)

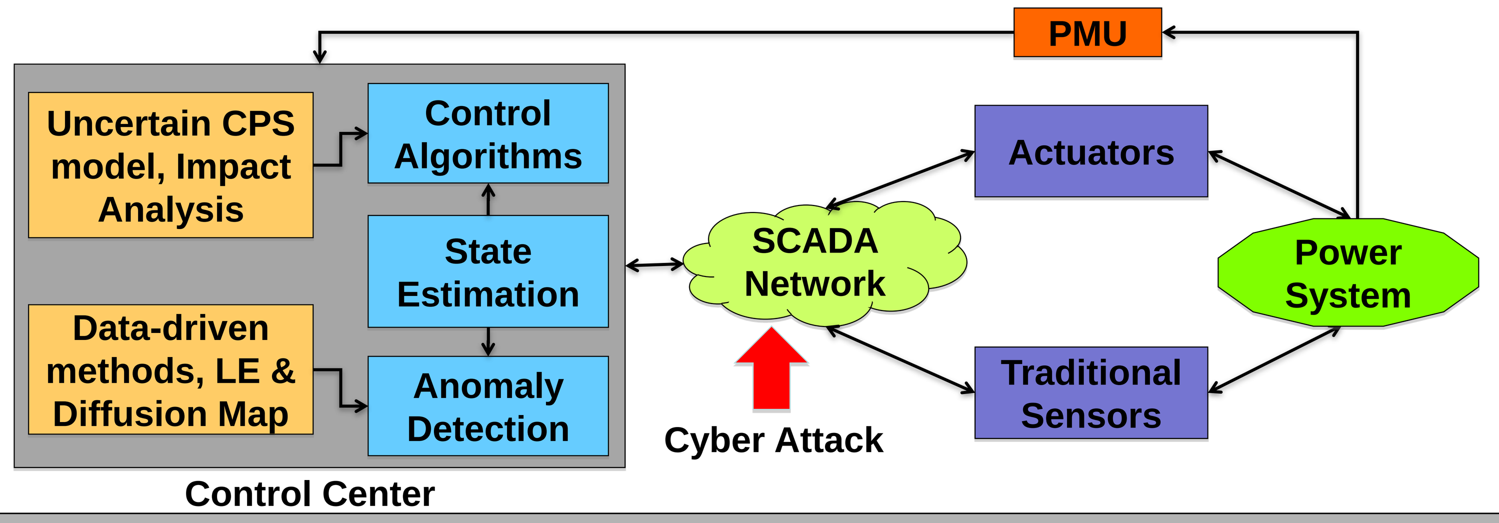
National Science Foundation

Investigators: Umesh Vaidya (PI), Manimaran Govindarasu (Co-PI), Venkataramana Ajjarapu (Co-PI) – *Iowa State University*
Makan Fardad (PI) – *Syracuse University*

Background and Motivation

- Modern power grid is a highly automated cyber-physical system afflicted by instability and uncertainty from network interaction and attacks.
- New analysis tools required to monitor and maintain system performance, detect and mitigate vulnerability to faults and attacks.

Schematic of cyber-physical security framework

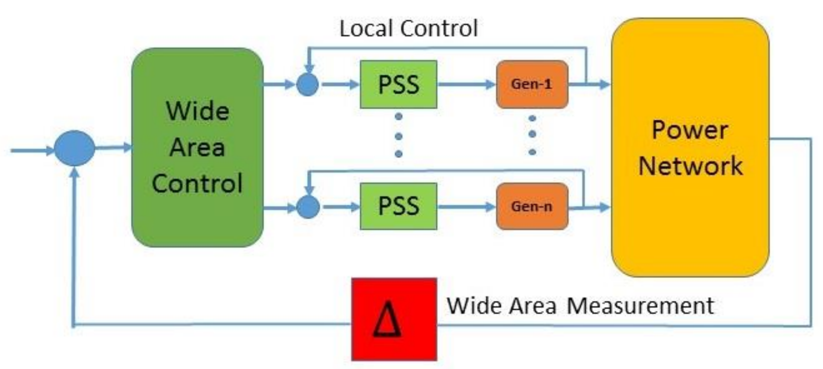


Goals:

- To develop a modeling framework that quantifies the impacts of cyber attacks on wide-area control and monitoring applications of the power grid
- To provide a scientific foundation and develop system resiliency against attacks

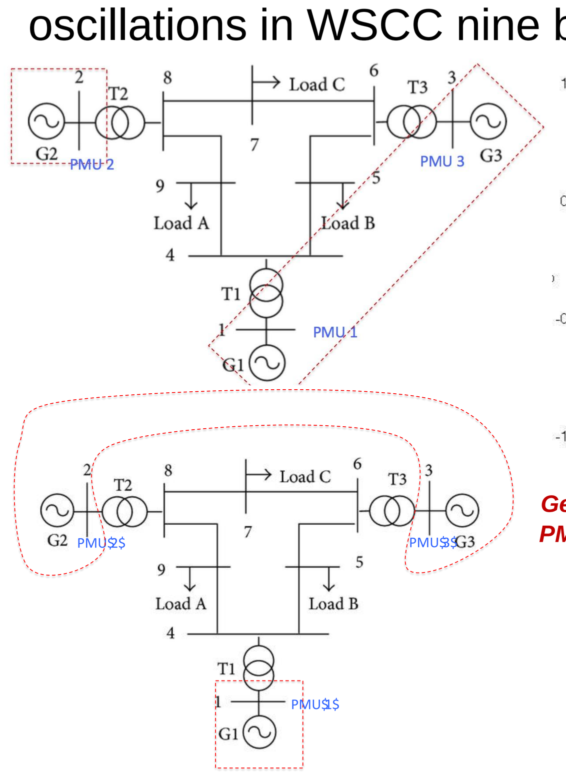
Vulnerability Analysis and Mitigation of Attacks on Phasor Measurement Units for Wide Area Monitoring and Control

- Discovered systematic analytical and computational framework to analyze vulnerability of power network to data integrity attacks on Phasor Measurement Units used for wide area monitoring and control.

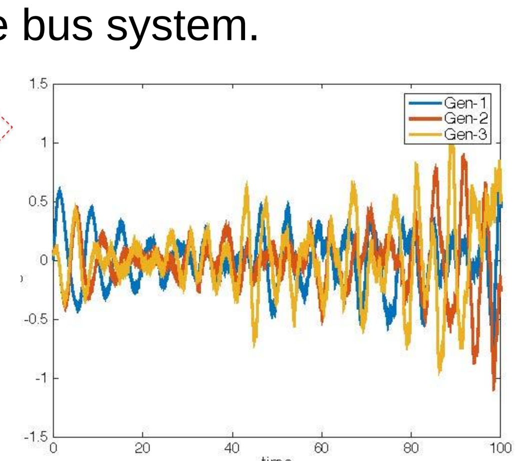


- Data from PMUs is used in feedback loop for wide area control of interarea oscillation.
- Data integrity attacks on PMU is modeled as stochastic multiplicative uncertainty.

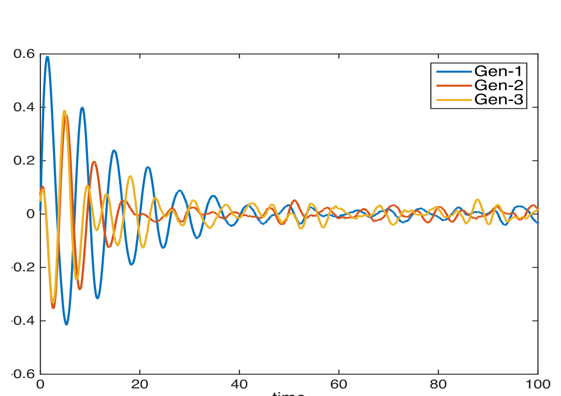
- Framework can be used to identify most critical PMU measurement for feedback control that can tolerate least amount of uncertainty.
- Analytical and computational framework based on Linear Matrix Inequalities for the design of controller robust to data integrity attacks on PMU.
- Implemented the developed framework for the suppression of inter-area oscillations in WSCC nine bus system.



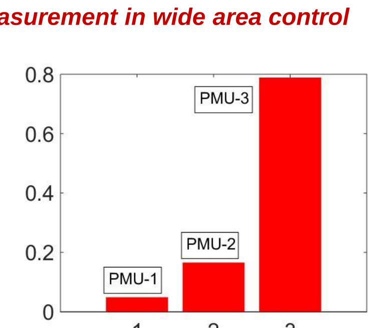
Inter area oscillating generators in WSCC 9 bus system



Generators frequency with noise corrupted PMU measurement in wide area control



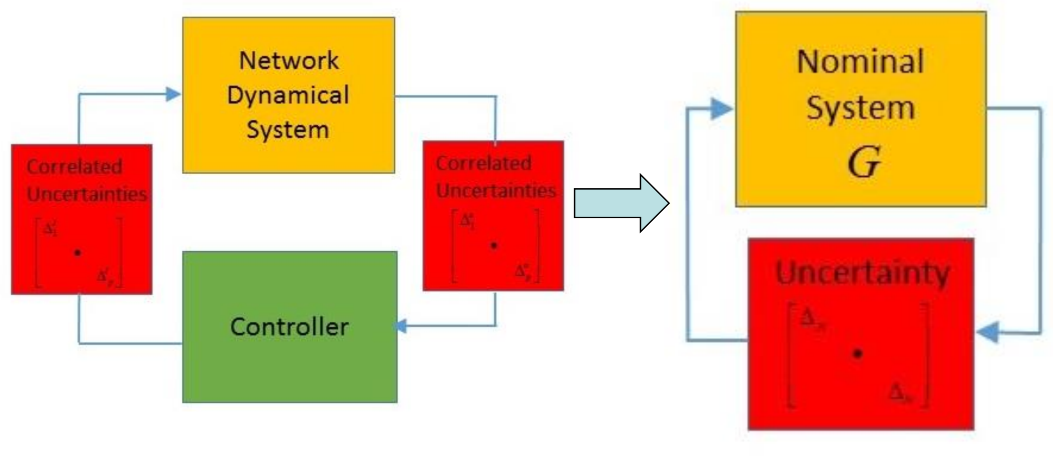
Generators frequency with noise corrupted PMU measurement with attack resilient wide area control



Rank ordering PMU measurements in order of their criticality to maintain network stability

Correlated Attacks on Network Systems: Modeling, Analysis, and Mitigation

- Discovered systematic analytical and computational framework for modeling analysis and mitigation of correlated attacks in network dynamical system.
- Correlated attacks on network dynamical system is modeled as stochastic correlated uncertainties.
- Framework can be used to analyze the impact of spatially correlated attacks on PMUs or spatially coordinated link failure attacks on communication network or transmission lines in power system.



- Spectral radius based condition for stability of network system.

$$\rho(\Sigma G) < 1$$

ρ-Spectral radius,
Σ -Covariance matrix,
G - Nominal system.

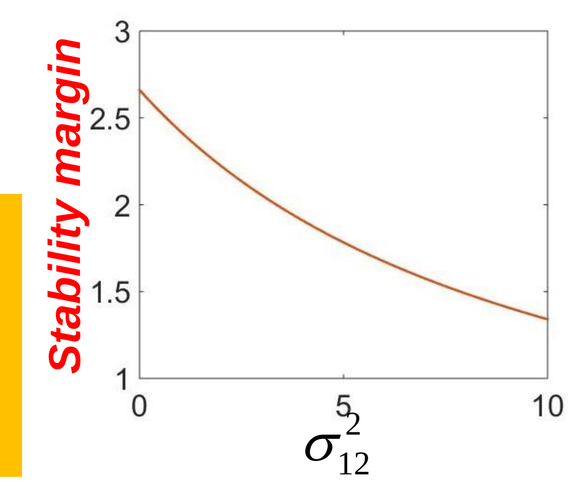
- Optimization-based framework for synthesis of controller robust to correlated attacks.

Impact of correlation of stability margin

- WSCC 9 bus system, two PMU measurements corrupted simultaneously.
- Covariance matrix

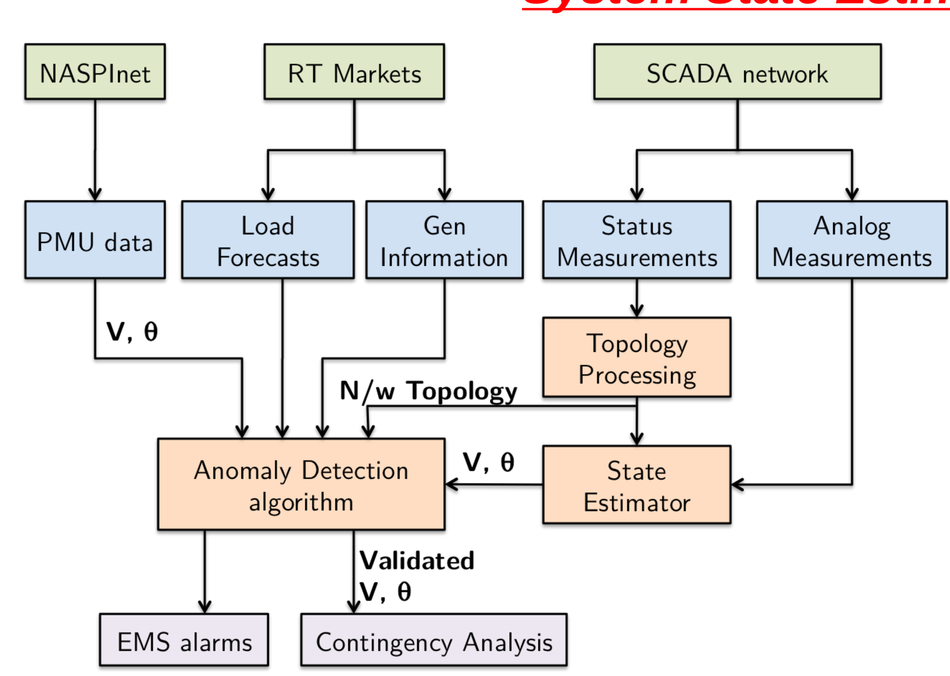
$$\Sigma = \begin{pmatrix} \sigma_{11}^2 & \sigma_{12}^2 \\ \sigma_{12}^2 & \sigma_{22}^2 \end{pmatrix}$$

Decrease in stability margin $\frac{1}{\rho(\Sigma G)}$ with increase in correlation



Wide Area Monitoring, Protection and Control (WAMPAC)

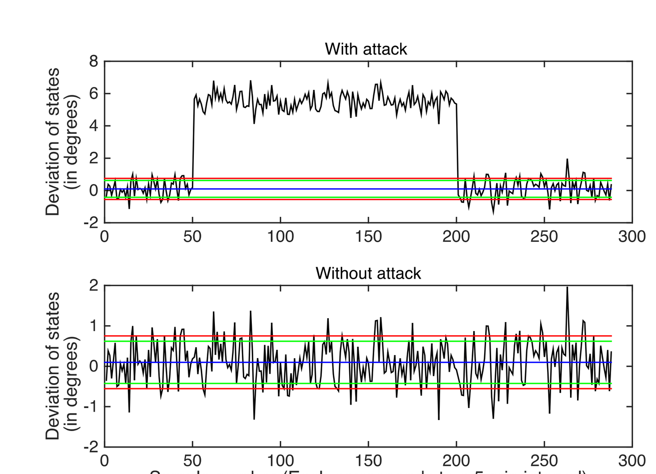
A) Online Detection of Cyber Attacks in Power System State Estimation



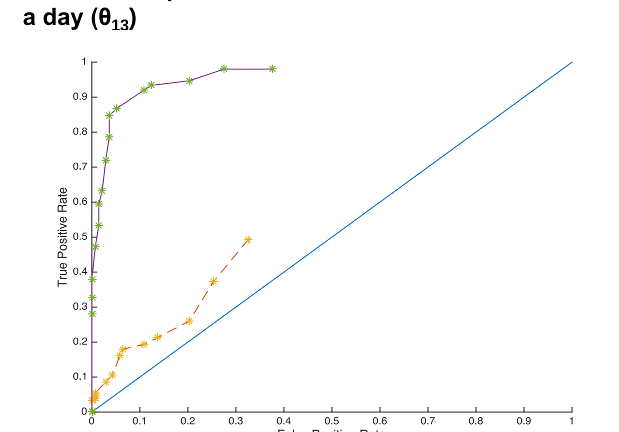
Model-based Anomaly Detection

- Uses information independent from SCADA measurements to detect anomalies.
- Leverages Load Forecast information, Generation Schedules and available PMU measurement data.
- Performs statistical characterization to detect measurement anomalies.

Simulation Results



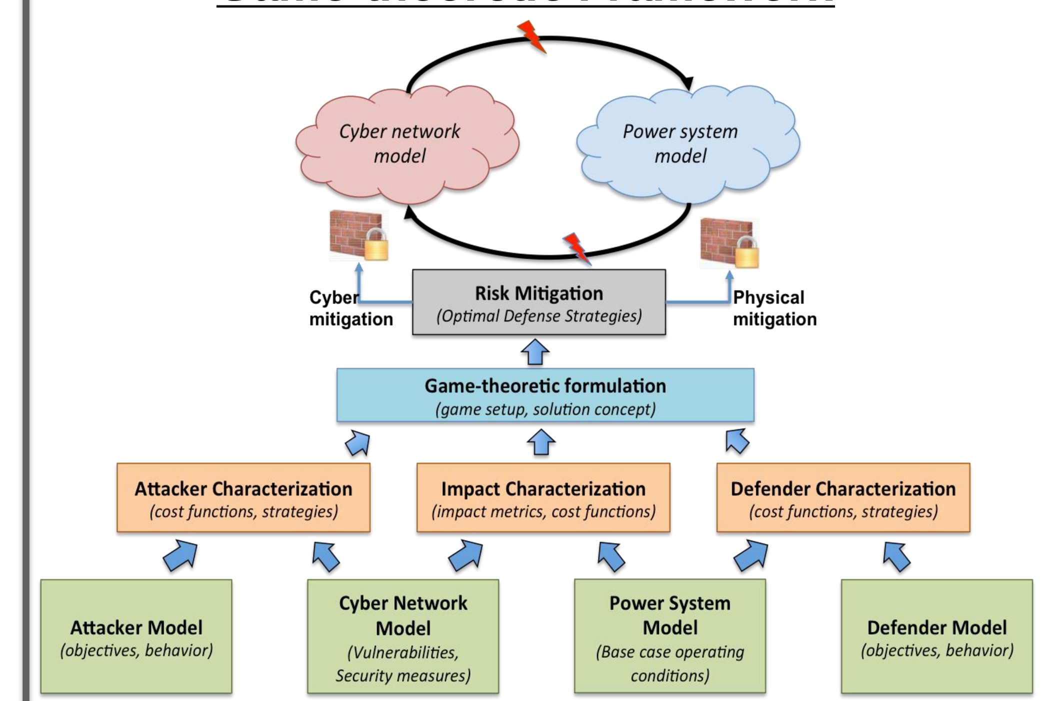
Deviation of predicted and actual state estimates over a day (θ_{13})



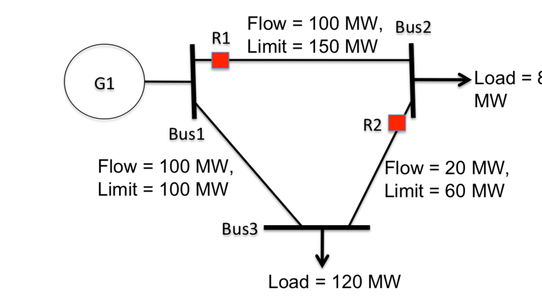
Receiver Operating Characteristic for State Variable(θ_2) Low (dotted) and High (solid) Attack Magnitudes

B) Cyber-Physical Risk Modeling and Mitigation using a Game- theoretic approach

Game-theoretic Framework



Simple Case Study



Scenario 1: Stealthy attacker - Prefers to be stealthy

Attack	$C_{attacker}$	C_{attack_impact}	$C_{defender}$
Attack 1	10	5	4
Attack 2	7	4	3

Scenario 1	D1	D2
A1	-1,1	-2,2
A2	1,-1	0,0

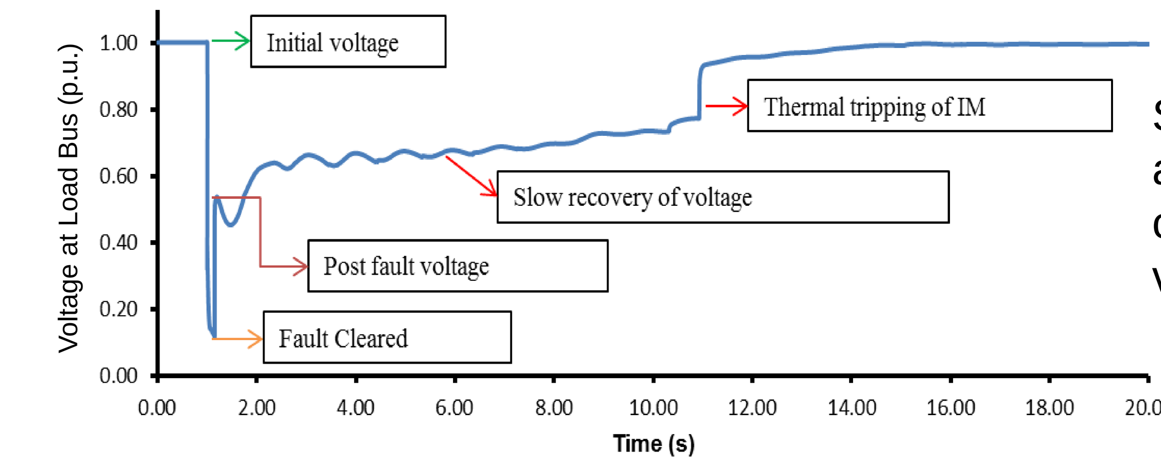
Scenario 2: Determined attacker - Prefers attack with max impact

Attack	$C_{attacker}$	C_{attack_impact}	$C_{defender}$
Attack 1	7	5	4
Attack 2	10	4	3

Scenario 2	D1	D2
A1	-2,2	1,-1
A2	-2,2	-3,3

Fault Induced Delayed Voltage Recovery (FIDVR) monitoring using Lyapunov Exponent (LE)

- Another attack vector is to create faults at loads to induce voltage instability.
- Detecting and controlling the instability in real-time is possible using the LE.
- Positive (negative) LE captures instability (stability) of the system.
- Heavy Induction Motor (IM) loads cause a different kind of voltage problem.

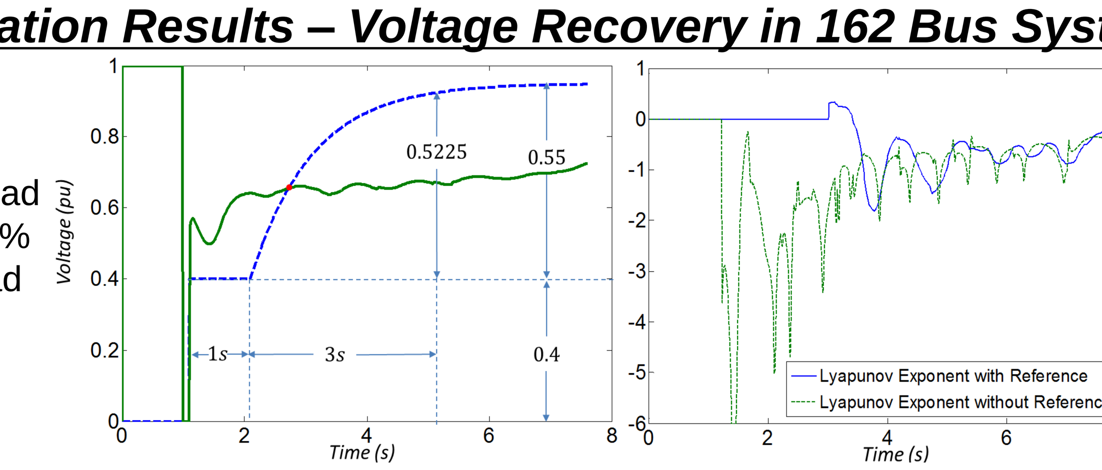


Stalling of IM after fault causes delay in voltage recovery

- FIDVR is a slow phenomenon (~15s) and cannot be detected by LE.
- FIDVR does not cause instability but has large impacts on load performance.
- NERC/WECC have pass/fail criteria to characterize the voltage recovery, but no quantification of the severity level of the deviation from standard.
- LE is modified by using a Reference voltage waveform to quantify deviation.

Simulation Results – Voltage Recovery in 162 Bus System After Fault

FIDVR observed with IM Load around 30% of total load



Voltage (green) for IM loads along with Reference (blue)

LE evolution for IM loads with and without Reference

LE with Reference goes positive **(FIDVR detected and quantified in Real-Time)**

LE without Reference is negative **(FIDVR not detected)**

Publications

1) *Sai Pushpak and Umesh Vaidya, "Control of Inter-Area Oscillation with Noise Corrupted Wide Area Measurement," Submitted to American Control Conference, Boston, 2016.*
2) *Amit Diwadkar and Umesh Vaidya, "Limitations and Tradeoffs in Synchronization of Large Scale Networks with Uncertain Links," Under Review for publication in Scientific Reports, Nature Publication Group.*
3) *Sai Pushpak, Amit Diwadkar and Umesh Vaidya, "Mean Square Based Stability Analysis and Controller Synthesis for Continuous time Network Systems, Under review in IEEE Transactions of Automatic Control, 2015.*
4) *A. Ashok, G. Manimaran, and V. Ajjarapu, "Online Detection of Cyber Attacks in Power System State Estimation," Under review in IEEE Transactions on Smart Grid, 2015.*
5) *A. Ashok, and G. Manimaran, "Cyber-Physical Risk Modeling and Mitigation for the Smart Grid using a Game-theoretic Approach," In Proceedings of IEEE PES Innovative Smart Grid Technologies (ISGT) Conference, Washington, D.C, 2015.*
6) *A. Ramapuram Matavalam, and V. Ajjarapu, "PMU based Real-Time Monitoring for Delayed Voltage Response," in North American Power Symposium (NAPS), 2015, Oct. 2015.*