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

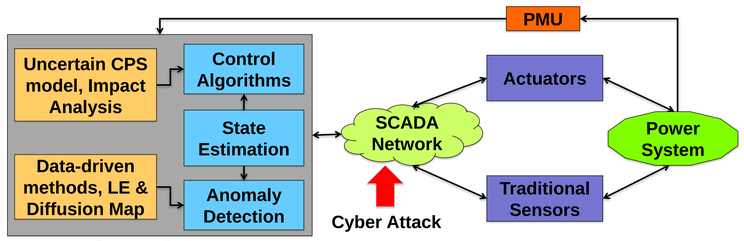
Investigators: Umesh Vaidya (PI), Manimaran Govindarasu (Co-PI), Venkataramana Ajjarapu (Co-PI) – *Iowa State University*
Makan Fardad (PI) – *Syracuse University*

National Science Foundation

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

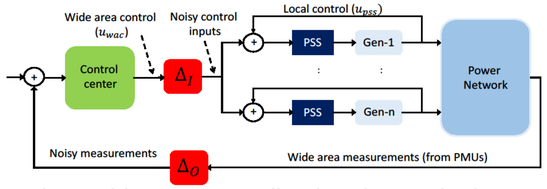


Goals:
- To develop a modeling framework that quantifies the impacts of cyber attacks on wide-area control and monitoring applications of the power grid.
- To provide a scientific foundation and develop system resiliency against attacks.

Resilient Cyber-Physical Power Network in the Presence of Communication Channel Uncertainties

Robust wide-area control with uncertain wide-area measurements

- Developed systematic analytical and computational framework to analyze vulnerability of power network to data integrity attacks on wide-area control inputs and PMU measurements.



- Developed a robust wide-area controller that damps the inter-area oscillations in the presence of uncertain/ noise corrupted wide-area measurements and wide-area control inputs.

Vulnerability of distributed control in power system to attacks on communication network

- Increased research trend towards use of distributed control in power system.
- Developed framework to analyze the vulnerability of decentralized and distributed control from attacks on communication network.
- Decentralized load-side frequency regulation using controllable loads in the presence of data integrity attacks on line voltages.
- System is vulnerable to stochastic voltage fluctuations and critical value of tolerable variance decrease with the increase in cost of controllable loads.
- With stochastic voltages inside the prescribed limits, the frequencies become mean square unstable (Fig. 2, simulation studies on IEEE 68 bus system).

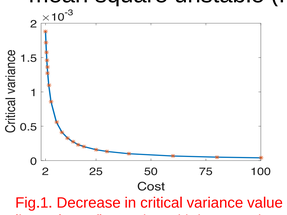


Fig.1. Decrease in critical variance value of stochastic line voltage fluctuation with increase in cost of controllable loads

Vulnerability of distributed load-side frequency control.
Simulation Results
IEEE 68 Bus system

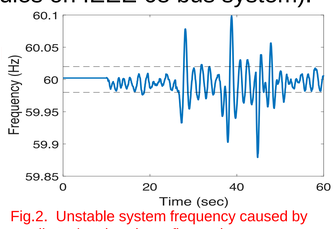
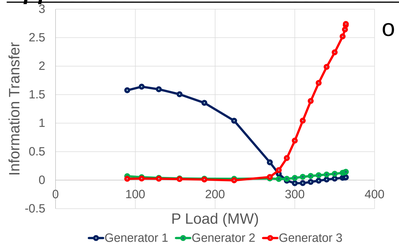


Fig.2. Unstable system frequency caused by small stochastic voltage fluctuations.

Information Transfer Based Approach for Characterizing Causal Interaction in Network Power System

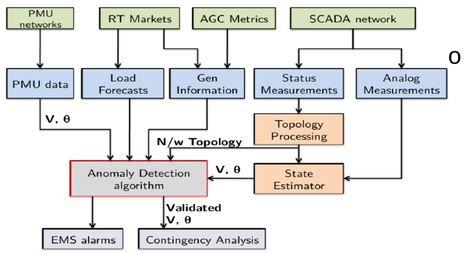
- Identification of causal interactions in network power system for the purpose of influence characterization.
- Identification of causal interaction will be used to determine the source of instability or attacks in the power network, to differentiate the cause of instability as voltage or angle instability, and to determine relative participation of individual generators and loads to overall system instability.
- We use ideas from information theory to define ***information transfer*** between the states in a dynamical system.
- ***Application to an IEEE 9 bus Power System***



- Information transfer from state to mode quantify the participation of individual state in that mode. Initially, generator 1 influences the mode and as system moves on the P-V curve, generator 3 dominates the mode. It validates with the participation factor analysis.

Online Detection of Cyber Attacks in Power System State Estimation

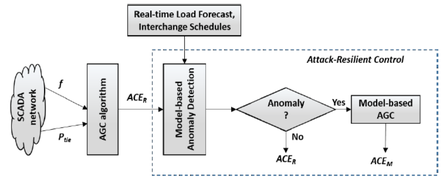
- Developed an online anomaly detection method to detect cyber attacks on State Estimators.



- The proposed algorithm utilizes load forecasts, generation schedules, and synchrophasor data to detect measurement anomalies.
- The anomaly detection algorithm works by obtaining a statistical characterization of the variation between state estimates from traditional SCADA measurements and forecast/synchrophasor- based estimates.
- We evaluated the performance of the proposed algorithm using the IEEE 14 bus power system model for several measures (false positive, false negative, thresholds).
- We observed that the optimal performance of the proposed algorithm depends on finding the balance between the minimum attack magnitude and detection thresholds.

Experimental Evaluation of Cyber Attacks on Automatic Generation Control using a CPS Security Testbed

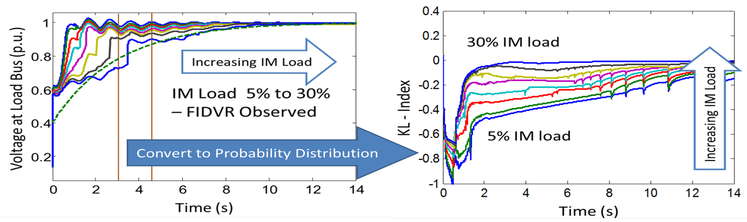
- We show leverage of the PowerCyber CPS testbed to implement and evaluate stealthy cyber attacks on the Automatic Generation Control (AGC) algorithm and also evaluate an Attack Resilient Control (ARC) algorithm to detect and mitigate such attacks.
- ARC is a cyber-physical security solution that combines domain-specific anomaly detection and model-based mitigation.
- We demonstrate the capability of stealthy attack templates to force under-frequency load shedding in a 3-area test system.



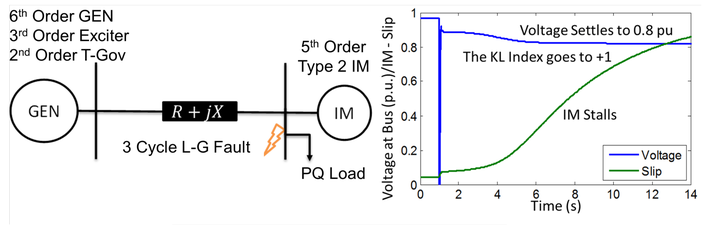
- We also validate the performance of ARC by measuring its ability to detect and mitigate these attacks.
- Our results reveal that ARC is efficient in detecting stealthy attacks and enables AGC to maintain system operating frequency close to its nominal value during an attack.

Novel Synchrophasor based Real-Time Monitoring of Fault Induced Delayed Voltage Recovery (FIDVR)

- FIDVR is caused by stalling of single phase Induction Motors (IM), primarily residential air-conditioners during transmission level faults.
- To quantify FIDVR in Real-Time – Compare the Probability Density Function of the Reference Voltage and the Bus Voltage in a moving window and calculate the Kullback–Leibler (KL) Distance.



- Higher the %IM, the longer it takes to recover to their pre-fault voltage and higher the KL-Index.
- Models are not available in Real-Time test beds that simulate FIDVR.
- We developed an IM model in Open-Modelica & interfaced it with OPAL-RT to demonstrate the IM Stalling.
- The IM motor stalls and its slip goes to 1 and KL index goes to 1.



Publications

1. Sai Pushpak and Umesh Vaidya, "*Fragility of Decentralized Load-side Frequency Control with Stochastic Renewables*," American Control Conference, 2017 Submitted.
2. Sai Pushpak and Umesh Vaidya, "*Resiliency and robust control of power networks against communication channel uncertainties,*" under review in Journal.
3. Subhrajit Sinha and Umesh Vaidya, "*Information-based approach for characterization of causal interactions in network systems with applications*," American Control Conference, Boston, 2016.
4. Aditya Ashok, Manimaran Govindarasu, and Venkataramana Ajjarapu, "*Online Detection of Cyber Attacks in Power System State Estimation,*" in IEEE *Transactions on Smart Grid , vol.PP, no.99.*
5. Aditya Ashok, Siddharth Sridhar, David McKinnon, Pengyuan Wang and Manimaran Govindarasu, "*Testbed-based performance evaluation of Attack Resilient Control for AGC*," *2016 Resilience Week (RWS)*, Chicago, IL, USA, 2016, pp. 125-129.
6. A. R. Ramapuram Matavalam, and V. Ajjarapu, "*Novel Synchrophasor based Real-Time Monitoring and Characterization of Delayed Voltage Recovery*," *2016 PES General Meeting*, Boston, MA, USA, 2016.