TCIPG

Security and Robustness Evaluation and Enhancement of Power System Applications

State Estimation and Contingency Analysis in a Cyber Adversarial Environment

R. Berthier, R. B. Bobba, C. M. Davis*, K. R. Davis*, T. J. Overbye, W. H. Sanders, S. A. Zonouz$

Goals

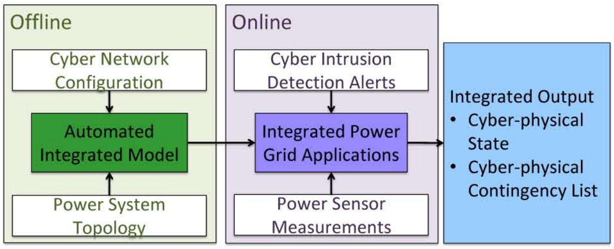
- Study the dependence of power grid applications on cyber infrastructure.
- Understand the impact of cyber attacks on power grid operations.
- Study the use of cyber sensor information and state along with power system measurements to improve power grid operations.
- Design power grid applications that can leverage cyber sensor information to improve power grid operations.

Fundamental Questions/Challenges

- How does the state of cyber infrastructure impact power grid applications?
- How do attacks on cyber infrastructure impact power grid operations?
- Is it feasible to jointly utilize cyber and power sensor information to improve operational reliability of the power grid?
- How can we design power grid applications that can utilize both cyber and power sensor information?

Research Plan

- Study the design of integrated cyber-physical state estimation.
- Study the design of integrated cyber-physical contingency analysis.


Offline

Cyber Network Configuration

Automated Integrated Model

Power System Topology

Online

Cyber Intrusion Detection Alerts

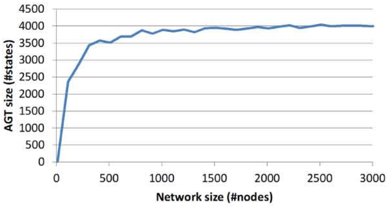
Integrated Power Grid Applications

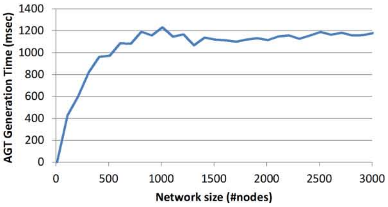
Power Sensor Measurements

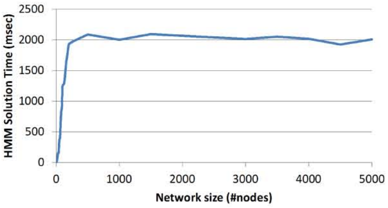
Integrated Output
- Cyber-physical State
- Cyber-physical Contingency List

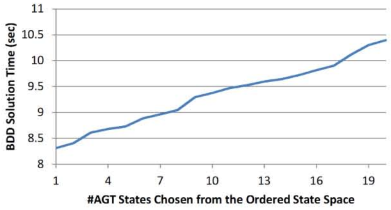
Cyber-Physical State Estimation

- Co-utilize information from cyber and power networks to (more precisely) determine the state of the cyber-physical system.
- Use combined information state to provide a scalable approach to detecting bad data caused by a cyber event.
- Step 1: Estimate probabilistic state (corrupted vs. non-corrupted) of cyber infrastructure components from IDS alerts using hidden Markov modeling (HMM) and attack graph template (AGT).
- Step 2: Identify impacted power system measurements.
- Step 3: Exclude combinations of most likely corrupted measurements from state estimation and compute residual error.
- Step 4: Identify most likely set of corrupted measurements based on residual error.



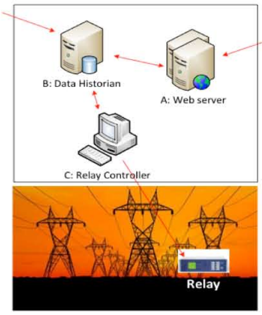


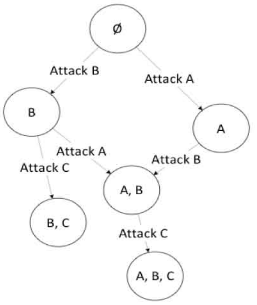




Cyber-Physical Contingency Analysis

- Includes cyber component/infrastructure outages during contingency analysis.
- Takes cyber adversarial events into account.
- Increases the complexity of contingency analysis, especially for *N-x* criterion.
- Step 1: Using knowledge about cyber and power systems, compute a security index for potential cyber contingencies, considering both likelihood of contingency and its impact.
- Step 2: Estimate probabilistic state (corrupted vs. non-corrupted) of cyber infrastructure components from IDS alerts.
- Step 3: Rank cyber contingencies considering the current probabilistic cyber and physical state and the computed security index.





Broader Impact

- Provide situational awareness about underlying cyber infrastructure.
- Improve resiliency of power grid operations by explicitly taking the state of cyber infrastructure into account.

Interaction with Other Projects

- Specification-based IDSes being developed for power grid infrastructure can feed into this framework.
- Security and robustness analysis of power system applications can feed into this framework as dependency information.

Future Efforts

- Consider impacts of false data injection on power system topology processing.

S. A. Zonouz, K. M. Rogers, R. Berthier, R. B. Bobba, W. H. Sanders, T. J. Overbye, "SCPSE: Security-Oriented Cyber-Physical State Estimation for Power-Grid Critical Infrastructures," accepted for publication in *IEEE Transactions on Smart Grid*.

S. A. Zonouz, C.M. Davis, K. R. Davis, R. Berthier, R. B. Bobba, W. H. Sanders, T. J. Overbye, "SOCCA : A Security-Oriented Cyber-physical Contingency Analysis in Power Infrastructures," submitted to *IEEE Transactions on Smart Grid*.

*TCIPG alumni now with PowerWorld Corporation
$TCIPG alumni now with University of Miami.

Trustworthy Cyber Infrastructure for the Power Grid • www.tcipg.org

University of Illinois • Dartmouth College • Cornell University • UC Davis • Washington State University