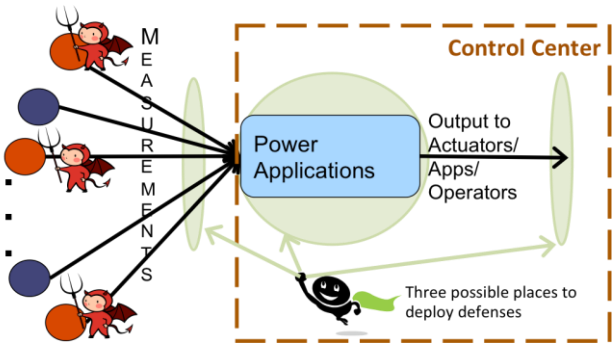
Security and Robustness Evaluation and Enhancement of Power System Applications

Overview and Problem Statement

Power system operations rely on a multitude of sensor data from remote measurement devices at substations and in the field. Sensor data are communicated back to the control center using a variety of protocols (e.g., DNP3, Modbus) and communication media. The remote sensors and the communication channels over which their readings are communicated present an attack surface for adversaries wanting to disrupt power system operations. While power system applications are typically robust against erroneous sensor data and data loss due to accidents and failures, they are typically not robust against coordinated malicious sensor data modification. In this work, we study impacts of malicious sensor data manipulation in power systems, and research mitigation and defense strategies. In general, the integrity of power system operations depends on the underlying cyber infrastructure, and we research ways to explicitly take the state of the cyber system into account in order to improve the robustness of power systems against cyber attacks. A new direction is to study ways to secure power system applications in cloud computing environments.

Research Objectives

- Study the security and robustness of power applications in the face of malicious sensor data manipulation attacks, and develop effective and cost-efficient defenses.
- Develop effective ways to consider the security state of the cyber infrastructure in power system operations to improve their robustness against cyber attacks.
- Develop a process to include security and robustness considerations during the power system application design phase.
- Understand and develop defenses for security issues surrounding the deployment of power applications in cloud environments.
- **Smart Grid Application Area:** Risk and security assessment.



Technical Description and Solution Approach

- Understand the behavior of power system applications and analyze their robustness in the presence of malicious data modification.
- Understand the dependency of power system operations on the security state of the underlying cyber infrastructure.
- Design effective ways to combine and use knowledge about both cyber infrastructure security state and power system electrical state during power system operations for increased robustness against cyber attacks.
- Study ways to protect power system applications for deployment in cloud environments.

Results and Benefits

- Proposed a framework for a security-oriented cyber-physical contingency analysis in power infrastructures. It allows for analyzing the impact of and ranking potential cyber-induced contingencies (*IEEE Transactions on Smart Grid*, 2014).
- Studied security issues surrounding smart distribution grids. Specifically, we looked at data integrity attacks on integrated Volt/VAR control and proposed countermeasures (presented at *American Control Conference*, 2014).
- Developed a scheme to detect malicious data in state estimation that leverages system losses & estimation of (perturbed) parameters (presented at *IEEE SmartGridComm*, 2013).
- Proposed a confidentiality-preserving obfuscation approach for cloud-based power system contingency analysis (presented at *IEEE SmartGridComm*, 2013).
- Studied security issues surrounding the use of cloud computing for the power grid. Specifically, looked at service composition options and assured clouds (presented at *USENIX HotCloud,* 2013).
- Proposed a state estimator that leverages both cyber and power system information and is more robust against false data injection (*IEEE Transactions on Smart Grid*, December 2012).
- Identified ways to inject false data into power flow computations, and investigated defenses (presented at *IEEE SmartGridComm,* 2012).
- Proposed a topology perturbation-based approach for defending against false data injection (*HICSS* 2012).
- For DC state estimation, we showed that protecting a set of *basic measurements*, that is, those necessary for observability, is necessary and sufficient for detecting a class of false data injection attacks (presented at *CPSWeek Workshop on Secure Control Systems,* 2010).
- The outcomes of this project will provide:
    - Robustness characterization of specific power applications with respect to malicious data modification attacks and mechanisms to improve the robustness of those applications.
    - Guidance on where to focus an organization's security budget to secure power grid infrastructure.
- A longer-term benefit of this project would be the evolution of a process that includes security and robustness considerations during application design for future power applications.
- Partnerships and External Interactions: Collaborated with researchers at KTH Royal Institute of Technology in Sweden; collaborated with TCIPG alumni at PowerWorld and the University of Miami.
- **Technology Readiness Level:** This technology is currently in the research and design phase.

Researchers

- Rakesh B. Bobba, rbobba@illinois.edu
- Miao Lu, mlu20@illinois.edu
- Pete Sauer, psauer@illinois.edu
- **External Researchers:** Saman Zonouz (Rutgers), György Dán, Henrik Sandberg, Andre Teixeira, Ognjen Vuković (KTH Royal Institute of Technology), Matt Davis (PowerWorld Corp.)
- **Past Researchers:** Robin Berthier, Roy Campbell, George Gross, Erich Heine, Himanshu Khurana, Kate Morrow, Klara Nahrstedt, Will Niemira, Tom Overbye, William H. Sanders, Al Valdes, Qiyan Wang, and Zheming Zheng

Industry Collaborators

- Matt Davis (PowerWorld), Will Niemira (Sargent & Lundy)

funded by the U.S. Department of Energy and the U.S. Department of Homeland Security