Securing Smart Power Grids under Data Measurement Cyber Threats

Challenge:

- Existing means for online system monitoring and estimation are vulnerable to various types of cyber-attacks.
- The extent of impact of cyber-attacks on power systems are unknown
- Existing state estimation bad data detection methods cannot detect cyber-attacks
- Countermeasures to alleviate the impact of cyber-attacks on power systems are primitive.

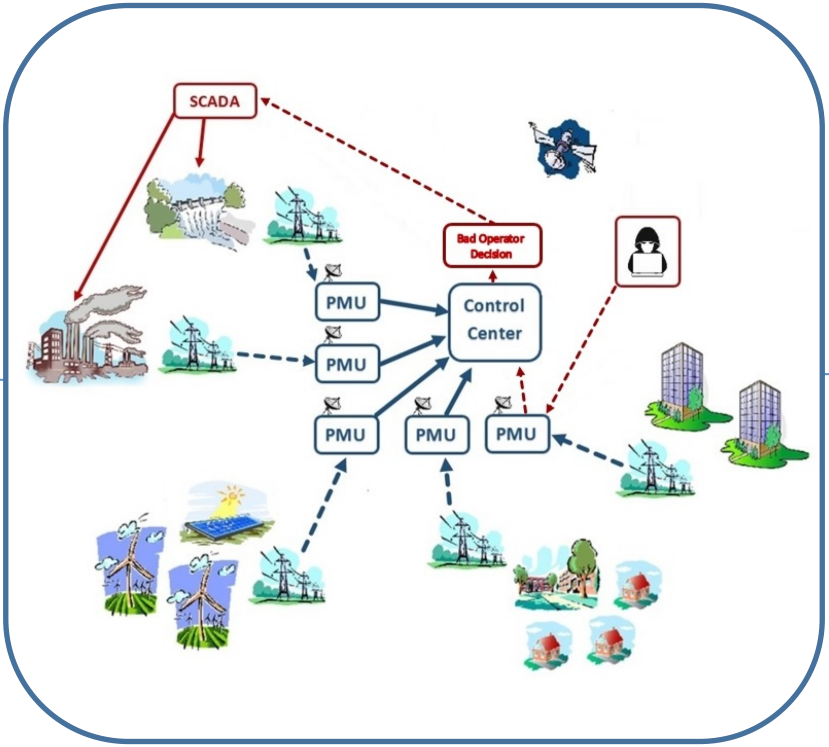
Solution:

- Estimate the impact severity of cyber-attacks on power systems
- Identify compromised PMUs based on real-time system conditions
- Introduce a comprehensive framework for effective mitigation against cyberattacks on PMU systems

NSF Grant No. 1600058.

Sara Eftekharnejad, PI, *Syracuse University*

Brian K. Johnson, James Alves-Foss, *University of Idaho*



Scientific Impact:

- This project helps identify means by which attackers can bypass conventional means to secure power system state estimators
- It also develops possible countermeasures when an attack is identified as remedial actions
- Bad data detection system analyzed to determine effectiveness

Broader Impact:

- This work impacts society by increasing the cyber-security of the power system critical infrastructure.
- By utilizing common software tools and equipment used by utilities, we will ensure our results are directly utilized in practice
- The results of this study can be integrated into a Resilient Controls course, which is a multi-university course jointly taught by the PIs of this project