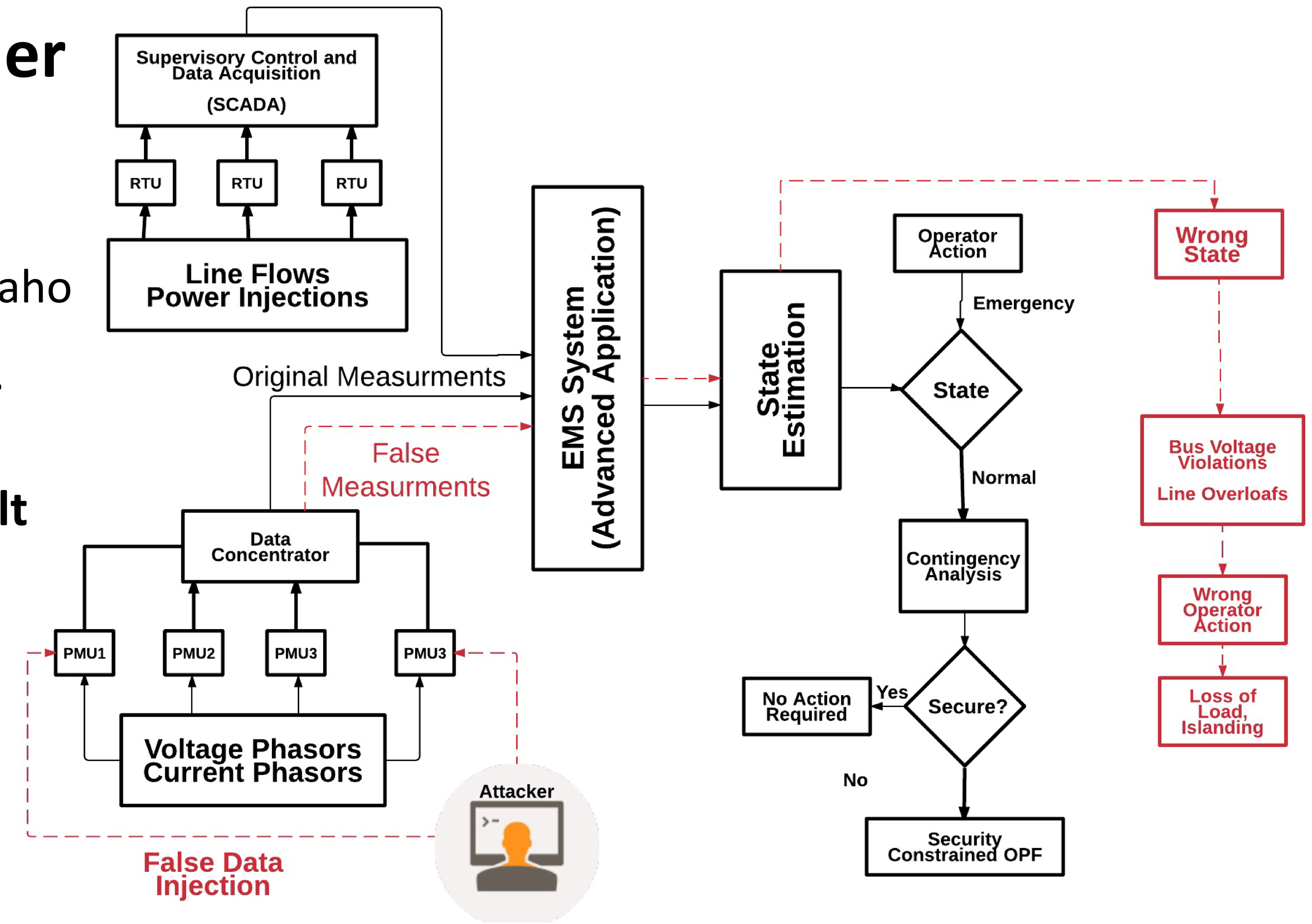
Anomaly Detection and Risk assessment in Power Grids under Data Measurement Threats

https://seftekha.expressions.syr.edu/research-projects/

Sara Eftekharnejad, Syracuse University ; Brian Johnson, James Alves-Foss, University of Idaho

Project Objective: Investigating the impact of false-data injection attacks on PMU-based power system state estimation; quantifying the cyber-physical risks of PMU measurement attacks; developing methods to detect these attacks before they result in cascading failures; proposing methods to prevent wide-spread blackouts.



Challenges

- Existing means for real-time power system monitoring are vulnerable to various types of cyber-attacks. However, the extent of the impact of cyber-attacks on power systems are unknown.
- Malicious PMU false data injections can be formulated to be undetectable by existing bad data detection methodologies.
- The existing grid mitigation solutions do not take dependencies between the cyber and physical layers into consideration.

Technical Approach:

1. Estimate the impact severity of cyber-attack on PMU devices on power systems (challenge 1)
2. Classify real-time event in power systems based on time-series PMU data and identify fake events from real event (challenge 2)
3. Identify critical PMUs that are best candidates for measurement redundancies (challenge 3)
4. Introduce a comprehensive framework for effective mitigation against cyberattacks on PMU systems (challenge 3)

Key Innovations:

1. **Development of a new cascading failure model for power systems based on real-time operating conditions**
2. **Power system islanding methodology under measurement uncertainties**
3. **Methodology to secure RAS schemes against data injection attacks**

Impacts on Society:

This work enhances the reliability and resiliency of the power grids against cyber attacks, and leads to a more secure electricity delivery infrastructure.

Education and Outreach:

- This study has been integrated into courses at both institutions.
- Broad participation of undergraduate students in research.

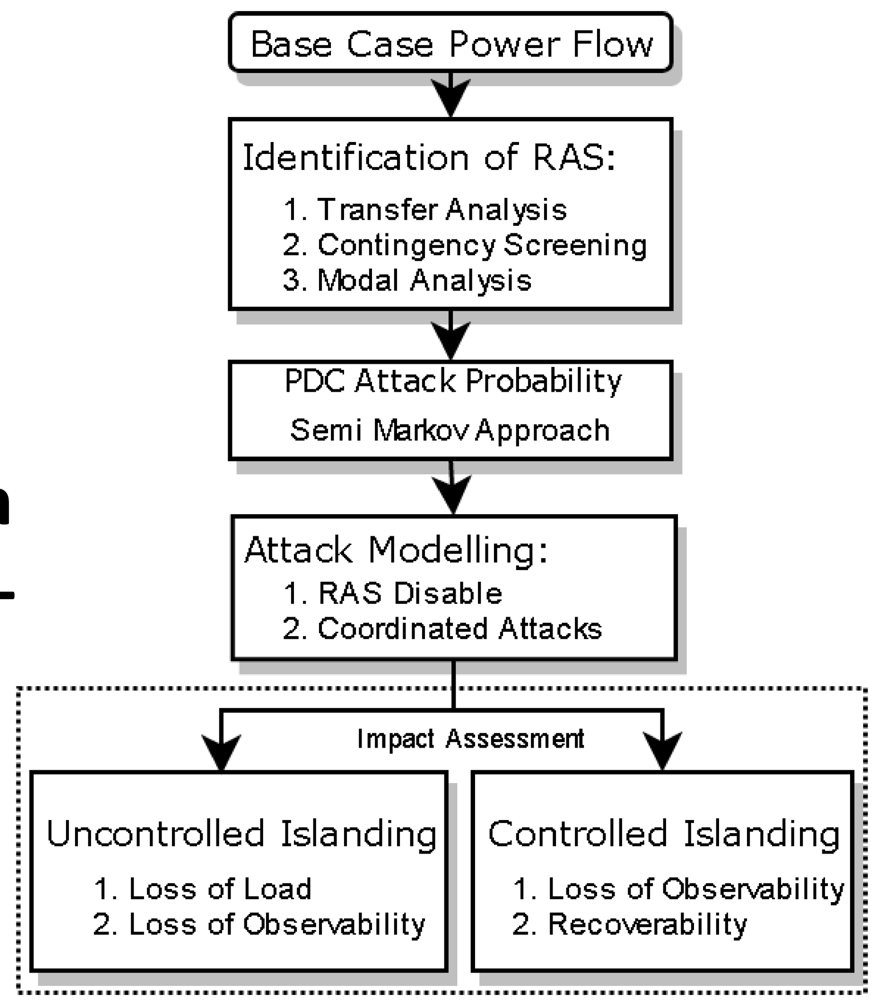
Impact Quantification:

- The results of this project have been disseminated in multiple conferences and peer-reviewed journals.
- The project directly engaged a diverse team of students in research including six graduate students, five undergraduate students, and two high school students.

Scientific Impact

- Quantification of the false data injection impacts in terms of causing cascading failures
- Developing new anomaly detection techniques using time-series data
- Developing new methodologies to predict the failure probability of each power system component under real-time operating conditions
- Developing possible countermeasures to mitigate successful cyber attacks on PMU measurements and prevent cascading blackouts

New Contributions



- ✓ **Development of new risk Quantification metrics of coordinated cyber-physical attacks against power systems and PMU devices**
- ✓ **Development of a new event detection methodology based on large scale real-time data. Using machine learning algorithms, the developed method compresses data and extracts features for accurate event classification.**
- ✓ **A methodology to identify critical PMU measurements for ensuring grid reliability**
- ✓ **Introduction of a new decentralized control strategy to ensure system reliability under evolving cascades**
- ✓ **Modifications to the existing grid islanding techniques to consider measurement uncertainties and implementing dynamic islanding**
- ✓ **Development of scheme to detect and mitigate false data injection attacks against remedial action schemes**