Towards Attack Resilient Data Analytics for Power Grid Operations

Travis Hagan, Shashini De Silva
Advisors: Dr Eduardo Cotilla-Sanchez, Dr. Jinsub Kim
April 27, 2018
Motivation

• Modernizing power grid
• Bad data = bad decisions
• Blackouts
• Why GPS attacks?
Project Description

- Power System Solver
- PMU data correction
- Protective algorithms
Overview of Approach

Control Actions:
- Update relay settings
- Load shedding
- Line/Generator disconnect
Realistic attacks on PMU devices

• Removing from service
• Hacking PMU to PDC connection
• GPS Jamming
• Spoofing
Case Study: Chicoasen-Angostura transmission line

- Carry away clock
- If PMU data goes through PDC, max error is 200 ms
Overview of Approach

Control Actions:
- Update relay settings
- Load shedding
- Line/Generator disconnect
PSS®E Simulation

- RTS 1996
- Creating a realistic power grid
  - Primarily based on BPA recommendations and current grid operations
  - Implementing an angle change attack
Overview of Approach

Protection and Control algorithms

Protection and Control algorithms

Protective device settings

PSSE Dynamic Simulation

Python API

PMU data Correction

PMU data

Control Actions:
- Update protection settings
- Load shedding
- Line/Generator disconnect
Simulation - Protective devices

- Overcurrent relay
- Frequency/voltage relay
- Distance relay
- Volts/Hertz relay
- Load shedding relay
- No differential relay in PSSE

<table>
<thead>
<tr>
<th>Devices</th>
<th>Count</th>
<th>Protective devices (typ)</th>
<th>Protective device (sim)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buses</td>
<td>73</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Loads</td>
<td>51</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Generators</td>
<td>99</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>Branches</td>
<td>105</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Transformers</td>
<td>16</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Total: 772
Simulation – Rollout Policy

1. Start simulation and run to contingency
2. Pause Simulation, test ALL possible actions
3. Apply load shed in simulation
4. Determine effectiveness of decision
5. Determine most effective solution and shed load
6. Evaluate if further action is necessary
Connection to real devices

- PMUs and relays
- Six settings groups
- USB, Ethernet, Serial
Overview of Approach

Control Actions:
- Update protection settings
- Load shedding
- Line/Generator disconnect

PMU data → PMU data Correction → Protection and Control algorithms → Protective device settings

PMU data Correction → Python API → PSSE Dynamic Simulation

Python API
Motivation

- Observing a low dimensional subspace for real time PMU data
• Measurements collected from the power network are constrained by Kirchoff laws.
**High-level Idea**

- Use the knowledge of the solution space to detect and mitigate the effect of data attacks.
PMU Measurement model

- Voltage phasor and outgoing power flow measurements collected from sparsely deployed PMUs

\[ y = h(\theta) + e + \alpha \]

- \( y \) = PMU measurement vector
- \( \theta \) = State vector
- \( \alpha \) = Attack vector
- \( h(.) \) = Nonlinear measurement function
- \( e \) = Gaussian random noise vector
SCADA Measurement model

• Outgoing power flow and power injection measurements collected from a **trustworthy** set of SCADA meters

\[ b = g(\theta) + e \]

- **b** = SCADA measurement vector
- **\theta** = State vector
- **g(.)** = Nonlinear measurement function
- **e** = Gaussian random noise
Data Correction Approach

• Leverage both PMU and SCADA measurements

\[ \theta^* = \text{argmin}_\theta \| \begin{bmatrix} y \\ b \end{bmatrix} - \begin{bmatrix} h(\theta) \\ g(\theta) \end{bmatrix} \|_2 \]

\[ \hat{y} = h(\theta^*) \]
Simulation Setting
Simulation Results
Future Steps

• Validate protection settings
• Integrated framework
Questions