Data-Driven Tools for Cyber-Physical Resiliency of the Electric Grid

A. Srivastava, Washington State University

Associate Professor, Washington State University
Director, Smart Grid Demonstration and Research Investigation Lab
Senior Scientist, Pacific Northwest National Lab (PNNL)
anurag.k.srivastava@wsu.edu

April 2\textsuperscript{nd}, 2020
RESEARCH INTERESTS

- Data-Driven System Operation and Control Algorithms to enable resiliency, voltage stability and security (Transmission Systems with Active Distribution and Microgrids/ DERs)

Keywords: Resiliency, PMUs, Data-driven, Cyber-Power, Voltage Control

ACADEMIC/INDUSTRY EXPERIENCE

- Director, Smart Grid Demonstration and Research Investigation Lab; 2010--
- MIT, PEAC, Aachen University, RTE-France, GE, PNNL, INL, PJM, SEL; 2016-2018
- Mississippi State University; 2005-2010, IIT Kanpur; 1999-2001
- Ph.D. 2005 Illinois Institute of Technology, (IIT), Chicago

RESEARCH SPONSORS

https://sgdril.eecs.wsu.edu
What can we do about it?

- Secure, but not resilient
- Reliable, but not resilient

- Define and measure cyber-physical resiliency
- Change the existing practice for cyber-physical security and resiliency
- Use tools for resiliency monitoring and decision support
This is a picture tracking bullet holes
At first, the military wanted to reinforce those areas, because obviously that’s where the ground crews observed the most damage on returning planes. Until

Abraham Wald pointed out that this was the damage on the planes that *made it* where there are no dots at all, because those are the places where the planes won’t survive when hit. This phenomenon is called bias towards known vulnerability instead of system survivability.
At first, find vulnerabilities and attack surface, patch it and fix it and call it secure.

PJM reports around 4,000+ cyber attacks every month - T. Boston, Former CEO PJM

known as bias towards known vulnerability instead of system survivability or resiliency.
What can we do about it?

- Secure, Attack surface and vulnerabilities
  - Device level vulnerabilities
  - Network vulnerabilities
  - System vulnerabilities and impacts
  - Known vulnerabilities
  - Unknown vulnerabilities

Real time anomaly detection, classification, root cause and control action

- Anomaly detection
- Spatio-temporal classification (physical, cyber, sensor)
- Root cause diagnosis
- Decision support and control actions

But not resilient

- Measuring Resiliency
- Enabling Resiliency

We need Tools
Electric Grid Resiliency

Resilience: The ability to supply its critical load through (and in spite of) limited extreme contingencies
Withstand any sudden inclement weather or human attack on the infrastructure.

Respond quickly, to restore balance in the community as quickly as possible, after an inevitable attack.

Adapt to abrupt and new operating conditions, while maintaining smooth functionality, both locally and globally.

Predict or Prevent future attacks based on patterns of past experiences, or reliable forecasts.
Taxonomy of Resiliency
Can we measure resiliency?

Red – Not Resilient
Purple – Resilient
Green – Super Resilient
Overview of resiliency quantification process

- Network, control, generating sources and critical loads

- Edge Count
- Overlapping Edges
- Switching Operations
- Repetition of Sources
- Centrality
- Probability of Availability
- Penalty Factor

Weights assigned to factors using pairwise comparison, or can be used defined according to requirement

Interaction Index $\lambda$ is determined – models interdependency between factors considered

$$C_{\mu}(f) = \int f d\mu = \sum_{i=1}^{n} (f(x_i) - f(x_{i-1})) \mu(A_i)$$

Choquet Integral to combine the factors into single resiliency value

Decision Making Tool
Measuring Resiliency

CANVASS: Cyber-Attacks and Network Vulnerability Analytics Software for Smart Distribution Grids
CyPhyR: Cyber-Physical Resiliency in Microgrid
CP-SAM: Cyber-Physical Security Assessment Metric
CP-TRAM: Cyber-Physical Transmission Resiliency Metric

- Weather Parameters
- Infrastructure Parameter
GRID MANAGEMENT AND DECISION MAKING DASHBOARD

- Grid Analysis & Management
  - Detailed Logs
  - Grid Analysis & Management
- Situation Awareness & Decision Support
  - Anomaly Detection
  - Root Cause Analysis
  - Criticality Analysis
  - Visualization
  - Proactive Control
  - Classification
  - Remedial Action
  - [ML/AI]
Ensemble Approach for Anomaly/Event Detection

- Real time anomaly detection, classification, root cause and control action
- Anomaly detection
- Spatio-temporal classification (physical, cyber, sensor)
- Root cause diagnosis
- Decision support and metric driven tools
- Control actions (holonic fast and optimal)
- Predictive analytics

Diagram:
- Data Window
- Ensemble
- Outlier Scores
- Base Detectors
- Model $Y_{MLE} (\alpha, \beta)$
- Detection of Transient Window Using Prony Analysis

Legend:
- Data X
- $f_i, f_j, f_k, f_l$
### Results for SyncAED

#### Tests on the RTDS simulated PMU data (1.5 hours)

<table>
<thead>
<tr>
<th>Method</th>
<th>Recall</th>
<th>Precision</th>
<th>False positive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linear Regression</td>
<td>0.9021</td>
<td>0.8565</td>
<td>0.1435</td>
</tr>
<tr>
<td>DBSCAN</td>
<td>0.8821</td>
<td>0.8821</td>
<td>0.1179</td>
</tr>
<tr>
<td>Chebyshev</td>
<td>0.9154</td>
<td>0.8754</td>
<td>0.1246</td>
</tr>
<tr>
<td>LSTM</td>
<td>0.9298</td>
<td>0.8554</td>
<td>0.1446</td>
</tr>
<tr>
<td>MLE ensemble</td>
<td><strong>0.9351</strong></td>
<td><strong>0.8913</strong></td>
<td><strong>0.1087</strong></td>
</tr>
</tbody>
</table>

#### Tests on the RTDS simulated PMU data (1.5 hours, 5% bad data points, 5%-10% range)

<table>
<thead>
<tr>
<th>Method</th>
<th>Recall</th>
<th>Precision</th>
<th>False positive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linear Regression</td>
<td>0.7854</td>
<td>0.7655</td>
<td>0.2345</td>
</tr>
<tr>
<td>DBSCAN</td>
<td>0.7216</td>
<td>0.7015</td>
<td>0.2985</td>
</tr>
<tr>
<td>Chebyshev</td>
<td>0.8125</td>
<td>0.7542</td>
<td>0.2458</td>
</tr>
<tr>
<td>LSTM</td>
<td>0.8298</td>
<td>0.7754</td>
<td>0.2246</td>
</tr>
<tr>
<td>MLE ensemble</td>
<td><strong>0.8912</strong></td>
<td><strong>0.9021</strong></td>
<td><strong>0.0979</strong></td>
</tr>
</tbody>
</table>

#### Tests on the RTDS simulated PMU data (1.5 hours, 10% bad data points, 10%-20% range)

<table>
<thead>
<tr>
<th>Method</th>
<th>Recall</th>
<th>Precision</th>
<th>False positive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linear Regression</td>
<td>0.7854</td>
<td>0.7655</td>
<td>0.2345</td>
</tr>
<tr>
<td>DBSCAN</td>
<td>0.7216</td>
<td>0.7015</td>
<td>0.2985</td>
</tr>
<tr>
<td>Chebyshev</td>
<td>0.8125</td>
<td>0.7542</td>
<td>0.2458</td>
</tr>
<tr>
<td>LSTM</td>
<td>0.8298</td>
<td>0.7754</td>
<td>0.2246</td>
</tr>
<tr>
<td>MLE ensemble</td>
<td><strong>0.8912</strong></td>
<td><strong>0.9021</strong></td>
<td><strong>0.0979</strong></td>
</tr>
</tbody>
</table>
Results with SyncAED using Real PMU Data

Thanks to PNNL/ EPRI for data
Synchrophaosr Anomaly Detection, Event Detection, Classification and Localization

- Being extended with concept drift, Graph based deep learning, microPMU
- PMU based model validation, state estimation, emergency control
SyncAED Tool
SynchroPhasor Anomaly And Event Detection

Anomaly Detection Event Detection

### Anomaly Detection data

<table>
<thead>
<tr>
<th>id</th>
<th>diagnosis</th>
<th>radius_mean</th>
<th>smoothness_mean</th>
</tr>
</thead>
<tbody>
<tr>
<td>842302</td>
<td>M</td>
<td>17.99</td>
<td>0.1184</td>
</tr>
<tr>
<td>842517</td>
<td>M</td>
<td>20.57</td>
<td>0.08474</td>
</tr>
<tr>
<td>84300903</td>
<td>M</td>
<td>19.69</td>
<td>0.1096</td>
</tr>
<tr>
<td>84348301</td>
<td>M</td>
<td>11.42</td>
<td>0.1425</td>
</tr>
<tr>
<td>84358402</td>
<td>M</td>
<td>20.29</td>
<td>0.1003</td>
</tr>
<tr>
<td>843786</td>
<td>M</td>
<td>12.45</td>
<td>0.1278</td>
</tr>
</tbody>
</table>

### Event Detection data

<table>
<thead>
<tr>
<th>id</th>
<th>diagnosis</th>
<th>radius_mean</th>
<th>smoothness_mean</th>
</tr>
</thead>
<tbody>
<tr>
<td>842302</td>
<td>M</td>
<td>17.99</td>
<td>0.1184</td>
</tr>
<tr>
<td>842517</td>
<td>M</td>
<td>20.57</td>
<td>0.08474</td>
</tr>
<tr>
<td>84300903</td>
<td>M</td>
<td>19.69</td>
<td>0.1096</td>
</tr>
<tr>
<td>84348301</td>
<td>M</td>
<td>11.42</td>
<td>0.1425</td>
</tr>
<tr>
<td>84358402</td>
<td>M</td>
<td>20.29</td>
<td>0.1003</td>
</tr>
<tr>
<td>843786</td>
<td>M</td>
<td>12.45</td>
<td>0.1278</td>
</tr>
</tbody>
</table>
### Event Details - Case 1

<table>
<thead>
<tr>
<th>Sno.</th>
<th>Time (s)</th>
<th>Bus</th>
<th>Event</th>
<th>Voltage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>109</td>
<td>9</td>
<td>Cap bank Closed</td>
<td>Up</td>
</tr>
<tr>
<td>2</td>
<td>119</td>
<td>10</td>
<td>3 Phase fault</td>
<td>Down</td>
</tr>
<tr>
<td>3</td>
<td>132</td>
<td>9</td>
<td>Cap bank Removed</td>
<td>Down</td>
</tr>
<tr>
<td>4</td>
<td>147</td>
<td>8</td>
<td>P load decreased</td>
<td>Up</td>
</tr>
<tr>
<td>5</td>
<td>157</td>
<td>9</td>
<td>Cap bank Closed</td>
<td>Up</td>
</tr>
<tr>
<td>6</td>
<td>168</td>
<td>10</td>
<td>3 Phase fault</td>
<td>Down</td>
</tr>
<tr>
<td>7</td>
<td>178</td>
<td>9</td>
<td>Cap bank Removed</td>
<td>Down</td>
</tr>
<tr>
<td>8</td>
<td>188</td>
<td>8</td>
<td>P load increased</td>
<td>Down</td>
</tr>
<tr>
<td>9</td>
<td>198</td>
<td>8</td>
<td>Q load increased</td>
<td>Down</td>
</tr>
<tr>
<td>10</td>
<td>209</td>
<td>8</td>
<td>P load increased</td>
<td>Down</td>
</tr>
<tr>
<td>11</td>
<td>219</td>
<td>8</td>
<td>Q load decreased</td>
<td>Up</td>
</tr>
<tr>
<td>12</td>
<td>229</td>
<td>2</td>
<td>GenDrop</td>
<td>Down</td>
</tr>
</tbody>
</table>
## Results - Case 1

<table>
<thead>
<tr>
<th>S No.</th>
<th>Time (s)</th>
<th>Actual Event</th>
<th>Actual Location</th>
<th>Detection Bus</th>
<th>Classified Event</th>
<th>Normalized Score</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>PMU 1</td>
<td>PMU 2</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>109</td>
<td>Cap Bank Closed</td>
<td>Bus 9</td>
<td>9</td>
<td>10</td>
<td>Reactive Power Event</td>
</tr>
<tr>
<td>2</td>
<td>119</td>
<td>Three Phase fault</td>
<td>Bus 10</td>
<td>10</td>
<td>9</td>
<td>Fault Event</td>
</tr>
<tr>
<td>3</td>
<td>132</td>
<td>Cap Bank Opened</td>
<td>Bus 9</td>
<td>9</td>
<td>10</td>
<td>Reactive Power Event</td>
</tr>
<tr>
<td>4</td>
<td>148</td>
<td>P load decreased</td>
<td>Bus 8</td>
<td>8</td>
<td>-</td>
<td>Active Power Event</td>
</tr>
<tr>
<td>5</td>
<td>158</td>
<td>Cap Bank Closed</td>
<td>Bus 9</td>
<td>9</td>
<td>10</td>
<td>Reactive Power Event</td>
</tr>
<tr>
<td>6</td>
<td>168</td>
<td>Three Phase fault</td>
<td>Bus 10</td>
<td>10</td>
<td>9</td>
<td>Fault Event</td>
</tr>
<tr>
<td>8</td>
<td>179</td>
<td>Cap bank Opened</td>
<td>Bus 9</td>
<td>9</td>
<td>10</td>
<td>Reactive Power Event</td>
</tr>
<tr>
<td>8</td>
<td>188</td>
<td>P load increased</td>
<td>Bus 8</td>
<td>-</td>
<td>-</td>
<td>No Detection</td>
</tr>
<tr>
<td>9</td>
<td>198</td>
<td>Q load increased</td>
<td>Bus 8</td>
<td>8</td>
<td>9</td>
<td>Reactive Power Event</td>
</tr>
<tr>
<td>10</td>
<td>209</td>
<td>P load decreased</td>
<td>Bus 8</td>
<td>8</td>
<td>9</td>
<td>Active Power Event</td>
</tr>
<tr>
<td>11</td>
<td>219</td>
<td>Q load decreased</td>
<td>Bus 8</td>
<td>8</td>
<td>9</td>
<td>Reactive Power Event</td>
</tr>
<tr>
<td>12</td>
<td>229</td>
<td>Gen Drop</td>
<td>Bus 2</td>
<td>2</td>
<td>-</td>
<td>Active Power Event</td>
</tr>
<tr>
<td>Sno.</td>
<td>Time (s)</td>
<td>Bus</td>
<td>Events Details</td>
<td>Voltage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>----------</td>
<td>-----</td>
<td>----------------</td>
<td>---------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>109</td>
<td>9</td>
<td>Cap bank Closed</td>
<td>Up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>119</td>
<td>13</td>
<td>3 Phase fault</td>
<td>Down</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>132</td>
<td>9</td>
<td>Cap bank Removed</td>
<td>Down</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>148</td>
<td>8</td>
<td>P load decreased</td>
<td>Up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>158</td>
<td>9</td>
<td>Cap bank Closed</td>
<td>Up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>168</td>
<td>13</td>
<td>3 Phase fault</td>
<td>Down</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>178</td>
<td>9</td>
<td>Cap bank Removed</td>
<td>Down</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>188</td>
<td>8</td>
<td>P load increased</td>
<td>Down</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>198</td>
<td>8</td>
<td>Q load increased</td>
<td>Down</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>209</td>
<td>8</td>
<td>P load increased</td>
<td>Down</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>219</td>
<td>8</td>
<td>Q load decreased</td>
<td>Up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>229</td>
<td>6</td>
<td>Tap Down</td>
<td>Down</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>240</td>
<td>13</td>
<td>3 Phase fault</td>
<td>Down</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>240</td>
<td>3</td>
<td>Cap Bank closed</td>
<td>Up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>253</td>
<td>6</td>
<td>Tap Up</td>
<td>Up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>263</td>
<td>2</td>
<td>GenDrop</td>
<td>Down</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Results - Case 2

<table>
<thead>
<tr>
<th>S No.</th>
<th>Time (s)</th>
<th>Actual Event</th>
<th>Actual Location</th>
<th>Detection Bus PMU 1</th>
<th>PMU 2</th>
<th>Classified Event</th>
<th>Normalized Score PMU 1</th>
<th>PMU 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>109</td>
<td>Cap Bank Closed</td>
<td>Bus 9</td>
<td>9</td>
<td>7</td>
<td>Reactive Power Event</td>
<td>2.15</td>
<td>2.11</td>
</tr>
<tr>
<td>2</td>
<td>119</td>
<td>Three Phase fault</td>
<td>Bus 13</td>
<td>13</td>
<td>9</td>
<td>Fault Event</td>
<td>26.56</td>
<td>11.09</td>
</tr>
<tr>
<td>3</td>
<td>132</td>
<td>Cap Bank Opened</td>
<td>Bus 9</td>
<td>9</td>
<td>7</td>
<td>Reactive Power Event</td>
<td>1.89</td>
<td>1.84</td>
</tr>
<tr>
<td>4</td>
<td>148</td>
<td>P load decreased</td>
<td>Bus 8</td>
<td>7</td>
<td>-</td>
<td>Active Power Event</td>
<td>2.61</td>
<td>-</td>
</tr>
<tr>
<td>5</td>
<td>158</td>
<td>Cap Bank Closed</td>
<td>Bus 9</td>
<td>9</td>
<td>7</td>
<td>Reactive Power Event</td>
<td>2.26</td>
<td>2.25</td>
</tr>
<tr>
<td>6</td>
<td>168</td>
<td>Three Phase fault</td>
<td>Bus 13</td>
<td>13</td>
<td>9</td>
<td>Fault Event</td>
<td>40.32</td>
<td>12.92</td>
</tr>
<tr>
<td>8</td>
<td>179</td>
<td>Cap bank Opened</td>
<td>Bus 9</td>
<td>9</td>
<td>7</td>
<td>Reactive Power Event</td>
<td>1.58</td>
<td>1.57</td>
</tr>
<tr>
<td>8</td>
<td>188</td>
<td>P load increased</td>
<td>Bus 8</td>
<td>-</td>
<td>-</td>
<td>No Detection</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>9</td>
<td>198</td>
<td>Q load increased</td>
<td>Bus 8</td>
<td>7</td>
<td>9</td>
<td>Reactive Power Event</td>
<td>0.74</td>
<td>0.67</td>
</tr>
<tr>
<td>10</td>
<td>209</td>
<td>P load decreased</td>
<td>Bus 8</td>
<td>7</td>
<td>9</td>
<td>Active Power Event</td>
<td>2.71</td>
<td>0.68</td>
</tr>
<tr>
<td>11</td>
<td>219</td>
<td>Q load decreased</td>
<td>Bus 8</td>
<td>7</td>
<td>9</td>
<td>Reactive Power Event</td>
<td>0.85</td>
<td>0.79</td>
</tr>
<tr>
<td>12</td>
<td>229</td>
<td>Tap Down</td>
<td>Bus 6</td>
<td>6</td>
<td>-</td>
<td>Reactive Power Event</td>
<td>0.62</td>
<td>-</td>
</tr>
<tr>
<td>13</td>
<td>240</td>
<td>Three Phase Fault</td>
<td>Bus 13</td>
<td>13</td>
<td>9</td>
<td>Fault Event</td>
<td>20.72</td>
<td>15.37</td>
</tr>
<tr>
<td>14</td>
<td>240</td>
<td>Cap bank closed</td>
<td>Bus 3</td>
<td>-</td>
<td>-</td>
<td>No Detection</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>15</td>
<td>253</td>
<td>Tap Up</td>
<td>Bus 6</td>
<td>6</td>
<td>13</td>
<td>Reactive Power Event</td>
<td>0.68</td>
<td>0.51</td>
</tr>
<tr>
<td>16</td>
<td>263</td>
<td>Gen Drop</td>
<td>Bus 2</td>
<td>2</td>
<td>-</td>
<td>Active Power Event</td>
<td>2.06</td>
<td>-</td>
</tr>
</tbody>
</table>
Map and Graph Interaction (google map)
Cyber-Physical Security Assessment Metric (CP-SAM)

- Integrate measurements, computed parameters, and weights with Fuzzy Choquet Integral
- Scale resiliency value between (0-100)

**CPS model generation**
- Initial weights assigned to parameters in Shapley value
- Attack graph generated from isomorphic graph of physical system and firewall configurations [Section III B]
- Graph of power system topology, system information including network information, source redundancy and availability [Section III A]

**Measurements (M) and computed parameters from model (CP)**
- CP: Reconfiguration paths ranked by resiliency
- CP: Path length, exploitability, vulnerability ratio
- M: latency, packet monitoring [Section III B]
- M: Voltage, current, switch status, real and reactive power consumption alerts from host based IDS
- CP: Graph theory based topology [Section III A]
CP-SAM for Chaos Monkey (Netflix) and Other Events
Cyber-physical Analytics for Ukraine Attack

1. Phishing email to IT network
2. Privilege escalation
   Obtained admin on DC

3. Ot vpn login
   Stolen credential from DC used to remotely
   login to vpn

4. Install malware
   BlackEnergy malware installed on control systems

5. Remote hmi session
   Created remote operators session to SCADA server

6. Trip breakers
   Operate key circuit breakers, 225,000 customers offline

7. Disable systems
   Wipe SCADA servers, brick serial-ethernet converters
   and control center ups

8. Telephone DDoS
   Telephone DDoS prevents communication about grid state

225,000 customers without power
Hardware Interface/Ethernet Internet
μPMU
PDC
Database
Real Time Communication
Simulator/Emulator
Control Center
Data Archival
Real Time Application
Application Layer
Application Layer
Communication Layer
Sensor and Actuator Layer
Power System Layer
Real Time Power System Simulator
μPMU
PDC
Control
AWR RESILIENCE METRICS
Testbed
Testbed

Power System
- Real-Time emulation tools including RTDS and OPAL-RT
- Offline simulation tools

Communication System
- Emulation tools such as CORE, DeterLab
- Simulation tools such as NS-3, Mininet

Security Tools
- Device and host level attack implementation and analysis
- Network level simulation of attacks

TCP/IP, Remote Encapsulation, Hardware
- IPC, TCP/IP, Remote Encapsulation
- Proxy interface, attack implementations

TCP/IP, libpcap, attack libraries
Simulating Ukraine Attack

1. Attacker sends an e-mail with malware
2. E-mail recipient opens the e-mail and the malware gets installed quietly
3. Using the information that malware gets, hacker is able to take control of the e-mail recipient’s PC and get access of two-level password
4. Analysis IEC 61850 protocol (GOOSE, SMV packet) information and relay setting file
5. Manipulate MMS packet and relay configuration session information
6. Takes control of circuit breaker or change the setting of relay
CyPhyR: Cyber-Physical Resiliency Tool
**CANVASS?**

- Canvass stands for Cyber-Attacks and Network Vulnerability Analytics Software for Smart Grids
- It enables unfavorable physical and cyber event simulation for power systems
- **Free, open-source, platform-independent resiliency-computation toolkit**
- It has default restoration and resiliency computation algorithms – with ability for user to define own metrics and scenarios.
- It enables easy power system modeling and interdisciplinary resiliency engineering research by abstracting lower level (hard-to-learn) open-source:
  - power simulation software [GridLAB-D],
  - network analysis library [NetworkX],
  - OS-based socket libraries [TCP/IP]
  - Packet Manipulation library [ScaPy]
  into a single, easy-to-use Python package.
- Multiple interdependent infrastructure modeling, such as cyber-physical power grid, along with crew transport network.
- It can interface with Real-Time Simulation software through socket programming.

https://sgdril.eecs.wsu.edu/research-interests-and-grants/industrial-grade-products/pycanvass/
Measuring Resiliency in Alaska

- Real-Time Inputs
  - Derived from Weather APIs in JSON format
  - Cyber-physical Power Grid Data
    - Power Flow State variables \((f, P, Q, V, \theta, p, f)\)
    - Network Communication State Variables - Bandwidth, Latency, Round Trip Time, Drop Rate
    - Diesel (DER) Generation Capacity
    - Solar Generation Rate, Battery SOC

- List of Probability of An Event
  - Weather-Related
    - Tropical Storm
    - Wind
    - Hurricane
    - Heavy Rain
    - Flooding
    - Snow
    - Hail
    - Blizzard
    - Freezing Temperature
    - Strong Winds
    - Cyclones
    - Solar Eclipse
  - Cyber
    - Data packet modification
    - Denial of Service
    - Bad Data Injection
    - Eavesdropping

- Data Pre-processing and conversion to logistic variables

- Impact Metric

- Communication Network
  - Substation Router Failure
  - Sub-network failure probability
  - Network Reliability Estimation

- Physical Energy Delivery Infrastructure
  - Transformer Failure
  - Sub-network failure probability
  - Network Reliability Estimation
  - Reliability Score

- Off-Grid (Alternative) Energy Resources
  - Solar Installation
  - Battery-storage
  - Hydro-storage

- Restoration and Outage Management System
  - Number of Tightly Coupled Network Microgrids
  - Automatic Restoration Capability
  - Crew Mobility Capability

- Metrics
  - Reliability Score
  - Cyber Integrity Score
  - Physical Integrity Score

- Operational Resilience Metric
  - 'Anticipate' Metric
  - 'Withstand' Metric
  - 'Recover' Metric
  - Normalization and Standardization
Enabling Resilient Smart Grid

By System Design:
- Redundancy and system approach
- Embedding resiliency concepts in operational and planning practice
- Automation, flexibility, adaptability, and physical network switching and hardening
- Resilient Communication Networking
- Providing incentive for resiliency

By Cyber Security and Weather Resistance Measure:
- Cyber-Physical Threat Detection
- Integrated Defense Plan

By Robust Computing and Data Analytics:
- Distributed coordination
- Centralized, decentralized, distributed

By Robust Mathematical Algorithm and Robust Control:
- Distributed optimization
- Robust convergence and time guarantee
- Distributed coordination for RAS

By Physical System Measure:
- Reconfiguration and resource allocation
- Controlled islanding
Example: Microgrid/DERs based restoration during contingencies

- ML based cold load pickup estimation, behind the meter DER estimation, MEMS and ADMS coordination, proactive/corrective control, centralized/decentralized/distributed voltage control and energy management
Example: Cyber-physical Data Analytics For Event Classification in Protection System

SCADA

- Breaker Status and Topology of the System
- Breaker Status Change

Streaming PMU Data

- PMU Data
- Autoencoder
- Fault Detection (Physical Data)
- IF-Else Conditions based Final Decision
- Cyber Attack
- Physical Fault

Streaming Cyber Data

- Cyber Data
- Signature Based Algorithm
- Intrusion Detection (Cyber Data)
- Cyber-Physical

Cyber Physical Security Analytics for Anomalies in Transmission Protection Systems
Example: Cyber-physical Data Analytics in Protection Failure

- Protection Mal-operation is #1 concern according to NERC
- Protection and associated control is becoming more digital
Example: RAS based Wind Curtailment

Scenario #1
- Low voltage violation at Bus #14
- Normal operation between Bus #3 and #4 (Line Rating set to 50 MVA)
- Line overloaded between Bus #7 and #9 (Line Rating set to 35 MVA)

Scenario #2
- Low voltage violation at Bus #14
- Line overloaded between Bus #3 and #4 (Reset Line Rating to 45 MVA)
- Line overloaded between Bus #7 and #9 (Line Rating set to 35 MVA)
Cyber-Physical-Human Resiliency Analysis for Extreme Events (With PNNL)
Cyber-Physical-Human Resiliency analysis for Extreme Events

**HYPERSIM GRID modeling**

**Protection Relays & Sensors**

**PHYSICAL LAYER**
- SCADA DATABASE
- Protection software
- Network monitoring software
- PMU DATABASE
- 3-phase voltage and current values
- Breaker status

**CYBER LAYER**
- Cyber DATABASE
- Cyber data
- Network packets
- Cyber data
- Network packets

**DATABASE**
- Data driven and AI based learning decision support
- Anomaly flag, Classification and root cause analysis

**ANALYSIS & MANAGEMENT LAYER**
- Data for Training and Validation
- Control Center
- Cyber DATABASE
- EMS
- EMTP (Electromagnetic Transient Program)

**SENSOR LAYER**
- Ping Things

**DECISION MAKING LAYER**
- Operator Visualization Layer
- Communication Model
- Protection Relays & Sensors
Research Problem #1: Shift in Grid Cyber Security Practices

• Murphy’s Law of Security
  o Law 1: “Whatever that can be hacked, will be hacked.”
  o Law 2: “Anything worth hacking has already been hacked (we just don’t know about them yet)”

PJM reports around 4,000+ cyber attacks every month
- T. Boston, Former CEO PJM
Research Problem #2: Resiliency is a Complex Problem

Resiliency is a MCDM problem
Resiliency management system need to be integrated and validated with large scale simulation
Resiliency is characteristics of the system
Data Analytics and machine learning approaches need to be applied after analyzing the power system problem carefully. Finding match between machine learning strength and power system problem to be solved is important.

Machine learning is only applicable in data-rich problems if no system model is available (e.g. forecasting).

If model is available with rich data set, typically it will be two step approach: apply machine learning to narrow down your possible options and refine it with model based approach (e.g. event detection).

Machine learning will not give a good results based on state of the art for highly complex and dynamic problems (e.g. transient stability, contingency analysis).

Validation and metric is important for these evolving solution technologies.

- Physics based model driven and existing power system operational algorithm need to be revisited with power electronics based DERs, active distribution system/ microgrids
- Existing practice of measurements based on SCADA and PMU, waveform capturing
- Not best but best possible evolving solutions

Research Problem #3: Physics-driven Data Analytics/ ML Techniques and finding suitable applications
Most important threat

• The most important threat to the power grid is a force of nature - http://cybersquirrel1.com/

• Humans have to catch up...

<table>
<thead>
<tr>
<th>Agent</th>
<th>Success</th>
</tr>
</thead>
<tbody>
<tr>
<td>Squirrel</td>
<td>1252</td>
</tr>
<tr>
<td>Bird</td>
<td>639</td>
</tr>
<tr>
<td>Snake</td>
<td>117</td>
</tr>
<tr>
<td>Raccoon</td>
<td>115</td>
</tr>
<tr>
<td>Rat</td>
<td>53</td>
</tr>
<tr>
<td>Cat</td>
<td>28</td>
</tr>
<tr>
<td>Marten</td>
<td>25</td>
</tr>
<tr>
<td>Jellyfish</td>
<td>13</td>
</tr>
<tr>
<td>Monkey</td>
<td>12</td>
</tr>
<tr>
<td>Human</td>
<td>3*</td>
</tr>
</tbody>
</table>
Thank You

Acknowledgement: My Research Group, My collaborators, PNNL and my funding agencies.

Anurag K. Srivastava
anurag.k.srivastava@wsu.edu
https://www.youtube.com/channel/UCJvYOVoqP-vM7nmR4qSxpmQ/videos
https://sgdril.eecs.wsu.edu