
Yi Deng, Sandeep Shukla, Hua Lin, James Thorp

February 5, 2014

9th Electricity Conference at CMU
Outline

1. Introduction
3. Cyber Attack Simulation on PMU-based State Estimation
4. Co-simulation Case Study on PMU-based Out-of-step Protection
5. Conclusion & Future Research
1: Introduction
GE’s Solution on Wide Area Monitoring and Control – Synchrophasor Techniques

* From GE’s Industrial Solution Website

Virginia Tech
Invent the Future
Dominion Synchrophasor Project

Dominion Generation

- 26,500 megawatts of capacity
- 6th largest producer in U.S.

Task
1. Prototype Development Recommendations on synchrophasor infrastructure
2. Commissioning process
3. Algorithms for online determination of Signal to Noise Ratio (SNR) of the PMU data
4. Recommendations for the central PDC architecture design and the ESOC architecture design (ESOC) Emergency System Operation Center
5. Optimized PMU placement scheme

6. Provide algorithms for:
   a) Loss of data from one or several PMUs
   b) Loss of signals in a PMU
   c) Stale (non-refreshing) data
   d) Inconsistent data, data rates and latencies
   e) Off-sets in signal magnitude and phase
   f) Corrupted and drifting signals in a PMU
   g) Corrupted and drifting time reference in one or several PMUs
   h) Combination of several issues described above
   i) Combination of several issues described above
   j) The failure of the topology processor and/or bad/incomplete topology information

T&D Business

- 6,000 miles of high-voltage transmission lines, up to 500KV
- 54,000 miles of distribution lines
- As high as 50,000+ new customers annually

21 500kv station, 5 230kv station, 115kv station

** From Dominion project and VT project report
<table>
<thead>
<tr>
<th>Target</th>
<th>Components</th>
<th>Synchronization</th>
<th>Scalability</th>
<th>Real-time</th>
</tr>
</thead>
<tbody>
<tr>
<td>EPOCHS[13]</td>
<td>Dynamic simulation for WAMS applications</td>
<td>PSCAD, PSLF, NS2</td>
<td>Time-stepped</td>
<td>Good for large system</td>
</tr>
<tr>
<td>ADEV[14]</td>
<td>Dynamic simulation for WAMS applications</td>
<td>Adevs, NS2</td>
<td>DEVS</td>
<td>Limited, have to rewrite codes for different systems</td>
</tr>
<tr>
<td>[15]</td>
<td>Dynamic simulation for WAMS applications</td>
<td>Simulink, OPNET</td>
<td>Not addressed</td>
<td>Medium size</td>
</tr>
<tr>
<td>VPNET[16]</td>
<td>Remotely controlled power devices</td>
<td>Virtual Test Bed, OPNET</td>
<td>Time-stepped</td>
<td>Limited to single or small number of power devices</td>
</tr>
<tr>
<td>PowerNet[17]</td>
<td>Remotely controlled power devices</td>
<td>Modelica, NS2</td>
<td>Time-stepped</td>
<td>Limited to single or small number of power devices</td>
</tr>
<tr>
<td>[18]</td>
<td>General network controlled system</td>
<td>OPNET only, power system part is virtualized</td>
<td>Delay estimation</td>
<td>Limited size due to virtualized power system</td>
</tr>
<tr>
<td>SCADA CST[19]</td>
<td>SCADA cyber security, system virtualization</td>
<td>PowerWorld, RINSE</td>
<td>N/A (static)</td>
<td>Good for large system</td>
</tr>
<tr>
<td>TASSCS[20]</td>
<td>SCADA cyber security, system virtualization</td>
<td>PowerWorld, OPNET</td>
<td>N/A (static)</td>
<td>Good for large system</td>
</tr>
<tr>
<td><strong>GECO</strong></td>
<td>Dynamic simulation for WAMS applications</td>
<td>PSLF, NS2</td>
<td>Global event-driven</td>
<td>Good for large system</td>
</tr>
</tbody>
</table>

2: Global Event-Driven Synchronization

Dynamic Simulation Procedure of Power Systems

- Initialize all state variables
- Calculate network boundary variables
- Calculate next variables
- Calculate state variable derivatives
- Integration step

\[ t = t' + \Delta t \]

One simulation round

Communication Network Simulation Procedure

- Event List Queue:
  - Event 1: node 1 sends packets to node 2
  - Event 2: node 2 receives packets from node 1

Power System Time Scale

- Start
- Synchronization Point 1
- Synchronization Point 2

Communication Network Time Scale

- Start
- t_1
- t_2

Global Event Queue

Two types of synchronization errors

Event-driven synchronization without errors
GECO (Global Event-driven CO-simulation): Platform Structure
GECO: A Modulized **Global** Event-driven **CO**-simulation platform

Power System Simulator Platform

<table>
<thead>
<tr>
<th>Application-Specific Physical System Simulators</th>
<th>Physical System Application Packages</th>
</tr>
</thead>
<tbody>
<tr>
<td>GE’s Positive Sequence Load Flow (PSLF)</td>
<td>State Estimation Out of Step Protection Electric Marketing</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Basic Model</th>
<th>Simulator Integration Layer</th>
<th>Dynamic Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Scheduler</td>
<td>Global Event Queue</td>
<td></td>
</tr>
</tbody>
</table>

Power System Interface Middleware “epcmod”

Communication Network Simulator Middleware “tcl_PSLF”

SCADA Communication Protocol Package Layer: Modbus, DNP3, ICCP, Profibus, Ethernet, TCP/IP, IEC 61850

<table>
<thead>
<tr>
<th>Cyber Network Simulators</th>
<th>Cyber Events Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Simulator 2 (NS2)</td>
<td>Cyber Attacks Network Contingency</td>
</tr>
</tbody>
</table>

Communication Network System Simulator Platform
3: Problem Statement: Attack Model
Malicious Data Injection attack on State Estimation

\[ z = Hx + e \]
\[ \hat{x} = (H^T W^{-1} H)^{-1} H^T W^{-1} z \]
\[ z_a = z + \alpha \]
\[ \alpha = Hc \]
\[ \|z_a - H\hat{x}_f\| = \|z - H\hat{x}\| \leq \tau \]

We can’t detect the attacks
The injected data will modify the state estimation results
The Placement of PMUs

IEEE 14-Bus Example

<table>
<thead>
<tr>
<th>Test system</th>
<th>PMUs Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE 14-bus</td>
<td>3</td>
</tr>
<tr>
<td>IEEE 24-bus</td>
<td>6</td>
</tr>
<tr>
<td>IEEE 30-bus</td>
<td>7</td>
</tr>
<tr>
<td>New England 39-bus</td>
<td>8</td>
</tr>
<tr>
<td>IEEE 57-bus</td>
<td>11</td>
</tr>
</tbody>
</table>

Minimum number of critical places for installing PMUs
Secured PMUs installed in these places make the system observable
Case study:
New England 39-bus test system
Cyber attack Simulation: on network channels

Single Network Link Failure

Bus16-Bus17 (Tp=50ms)

Saturation attacks

Network saturation 50%

Bus16-Bus17 (Tp=60ms)

Network saturation 85%
Cyber attack Simulation: on network nodes

Denial of Service Attack

**DoS attack on the router at Bus 16**

![Graph showing voltage magnitude over time for DoS attack on the router at Bus 16.](image)

**Enhanced DoS attack**

![Graph showing voltage magnitude over time for enhanced DoS attack.](image)

Data Spoofing

**PMU spoofing on Bus 3**

![Graph showing voltage magnitude over time for PMU spoofing on Bus 3.](image)

**PMU spoofing in contingency**

![Graph showing voltage magnitude over time for PMU spoofing in contingency.](image)
4: Out-of-Step Protection

Cyber attack on power generator by Idaho lab

Out-of-Step (OOS) means a generator or a group of generators lose synchronism with the rest of the system.

Equal Area Criterion
Out-of-Step Protection

• Out-of-Step (OOS) means a generator or a group of generators lose synchronism with the rest of the system.

• One effective method is to run time-domain dynamic simulations and monitor the generator angles.

Fault cleared in 0.1 second, system back to normal condition

Fault cleared in 0.3 second, OOS condition is observed
PMU-based Out-of-Step Protection

- Protection Scheme
  - Four Steps

  1. Measure Rotor Angles using adequate PMUs
  2. Identify Coherent Generator Groups using offline simulations
  3. Predetermine Islanding Locations
  4. Islanding Algorithm

- Real-Time Generator Clustering Algorithms
  - Algorithm 1: Sorting, then check neighboring element distance
  - Algorithm 2: Match elements into existing clusters sequentially

- Two Coherent Generator Groups

- Equivalence of islanding to $s'-t'$ min-cut problem
Clustering Algorithm for Coherent Groups

• Clustering algorithm refers to a group of algorithms whose goal is to divide data into subsets based on certain criteria.

• The first algorithm sorts the measured rotor angle and traverse the measured rotor angle sequentially. If the gap between two neighbors is greater than 120 degrees, then the OOS condition is identified.

• An alternative second algorithm processes the measured rotor angle one by one.

---

CoherentGroup1(A) returns S,T

1. sort A
2. for $i = 1$ to $A.size() - 1$
4. push generators associated with $A[i]$ to $A[i]$ into $S$
5. push generators associated with $A[i + 1]$ to $A[A.size()]$ into $T$
6. return

CoherentGroup2(A) returns S,T

1. create a dynamic array $G$ to hold clusters
2. for $i = 1$ to $A.size()$
3. compare $A[i]$ with the means of the clusters in $G$ sequentially
4. if one of the differences is smaller than 120 degree
5. push pair of $<i, A[i]>$ into that cluster, update the mean
6. else
7. create a new cluster holding pair of $<i, A[i]>$ and push it into $G$
8. find the largest cluster in $G$
9. push the generators in this cluster into a set $S$
10. push the other generators into another set $T$
Islanding Algorithm

- As long as we have found two coherent generator groups $S$ and $T$, the next step is to find a minimum cut of the entire power system that can separate $S$ and $T$.

- Edmonds-Karp algorithm which is $O(|V||E|^2)$

Equivalence of islanding to $s - t$ min-cut problem

A max-flow example

Find the min-cut on the residual network
Simulation Results

Generator angels showing OOS condition
(BW=1Gbps, D=5ms)

Generator real power outputs
(BW=1Gbps, D=5ms)

Generator angels with link failure
(BW=100Mbps, D=10ms)

Generator real power outputs with link failure
(BW=100Mbps, D=10ms)
5: Conclusions & Future Research

- Implemented a co-simulation platform GECO, and integrated the dynamic state estimation and the out-of-step protection modules in the platform.
- Launched two case studies (all-PMU based state estimation and PMU based out-of-step protection) to reveal the cyber security vulnerabilities on co-simulation platform.

- Cloud-based virtual SCADA testbed for cyber security research
  - Centralize & Modulize computing and communication resources
  - Replaceable different communication protocols for security research
  - Seamlessly interact with power/control system simulators.
Virtual SCADA Testbed for Cyber Security Research

- RTUs
- SCADA Master Server
- HMI
- OPC I/O drivers in iFix
  - D1: assigns the data to a tag in the iFix database manager
  - D2: monitors the tag in D1’s database
  - D3: Access Control
- MatrikonOPC server L1

Data Source Attack!
Database Attack!
Cloud-based Virtual SCADA Infrastructure in VT

- **User_1**: VM_1, Windows iFIX TCP/IP
- **User_2**: VM_2, Windows iFIX TCP/IP
- **UserN**: VM_N, Windows iFIX TCP/IP

- **iWebSpace Server**
- **RTUs/OPC Servers**
- **Admin/TAs**
- **SCADA Server**
- **VT Private Cloud**

- **Linux OS**: VM_1, VM_2, VM_N
- **Windows Server**: Hyper-V iFIX TCP/IP

- **Usr1**: VM_1, Windows iFIX TCP/IP
- **Usr2**: VM_2, Windows iFIX TCP/IP
- **UsrN**: VM_N, Windows iFIX TCP/IP
References


Thanks for your attention!

{yideng56, birchlin, shukla, jsthorp}@vt.edu