
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

- Power Plant
- Transmission Substation
- Distribution Substation
- Individual Consumer
- Public Consumer
- Industry Consumer
- Urban Area
- Rural Area
- Monitor & Control
- Operation & Marketing
- New Strategy
- Software Infrastructure
- Wind
- Nuclear
- Solar
- Hydro

Rural Area
Urban Area

Individual Consumer
Public Consumer
Industry Consumer

Software Infrastructure
New Strategy
GE’s Solution on Wide Area Monitoring and Control – Synchrophasor Techniques

* From GE’s Industrial Solution Website
### TABLE I
COMPARISON OF INTEGRATED POWER-NETWORK SIMULATORS

<table>
<thead>
<tr>
<th></th>
<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>
<td>No</td>
</tr>
<tr>
<td>ADEVS[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>
<td>No</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>
<td>No</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>
<td>No (but have plans to integrate RTDS)</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>
<td>No</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>
<td>No</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>
<td>Yes (communication network only)</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>
<td>Yes (communication network only)</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>
<td>No</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

\[ t_0 \rightarrow t' \rightarrow t \]

Two types of synchronization errors

- Error 1
- Error 2

Communication Network Simulation Procedure

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

Event List Queue:

- Event 1
- Event 2
- Event 3
- Event 4

Start

Global Event Queue

- Event 1
- Event 2
- Event 3
- Event 4

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</td>
</tr>
<tr>
<td></td>
<td>Out of Step Protection</td>
</tr>
<tr>
<td></td>
<td>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></td>
<td>Global Event Queue</td>
</tr>
</tbody>
</table>

Power System Interface Middleware “epcmod”

Communication Network Simulator Middleware “tcl_PSLF”

<table>
<thead>
<tr>
<th>SCADA Communication Protocol Package Layer: Modbus, DNP3, ICCP, Profibus, Ethernet, TCP/IP, IEC 61850</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Network Simulators</td>
</tr>
<tr>
<td>Network Simulator 2 (NS2)</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

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

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

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%

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 at Bus 3 (p.u.) over measurement time (second)]

**Enhanced DoS attack**

![Graph showing voltage magnitude at Bus 3 (p.u.) over measurement time (second)]

Data Spoofing

**PMU spoofing on Bus 3**

![Graph showing voltage magnitude at Bus 3 (p.u.) over measurement time (second)]

**PMU spoofing in contingency**

![Graph showing voltage magnitude at Bus 3 (p.u.) over measurement time (second)]
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. Island Asynchronous Generator Groups

Islanding Algorithm

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

Equivalence of islanding to \( s' - t' \) min-cut problem

- Two Coherent Generator Groups

- Input:
  - Rotor Angles of the Generators

- Output:
  - Two Coherent Generator Groups

Virginia Tech
Invent the Future
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[.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 angels with link failure (BW=100Mbps, D=10ms)

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

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

MatrikonOPC server (L1) → OPC I/O drivers in iFix (D1) assigns the data to a tag in the iFix database manager.

SCADA Master Server → OPC I/O drivers in iFix (D3) Access Control

OPC I/O drivers in iFix (D2) monitors the tag in D1’s database.

Data Source Attack!

Database Attack!
Cloud-based Virtual SCADA Infrastructure in VT
References


Thanks for your attention!

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