Power Systems/Communication System Co-Simulation and Experimental Evaluation of Cyber Security of Power Grid

Yi Deng, Sandeep Shukla,
Hua Lin, James Thorp

February 5, 2014

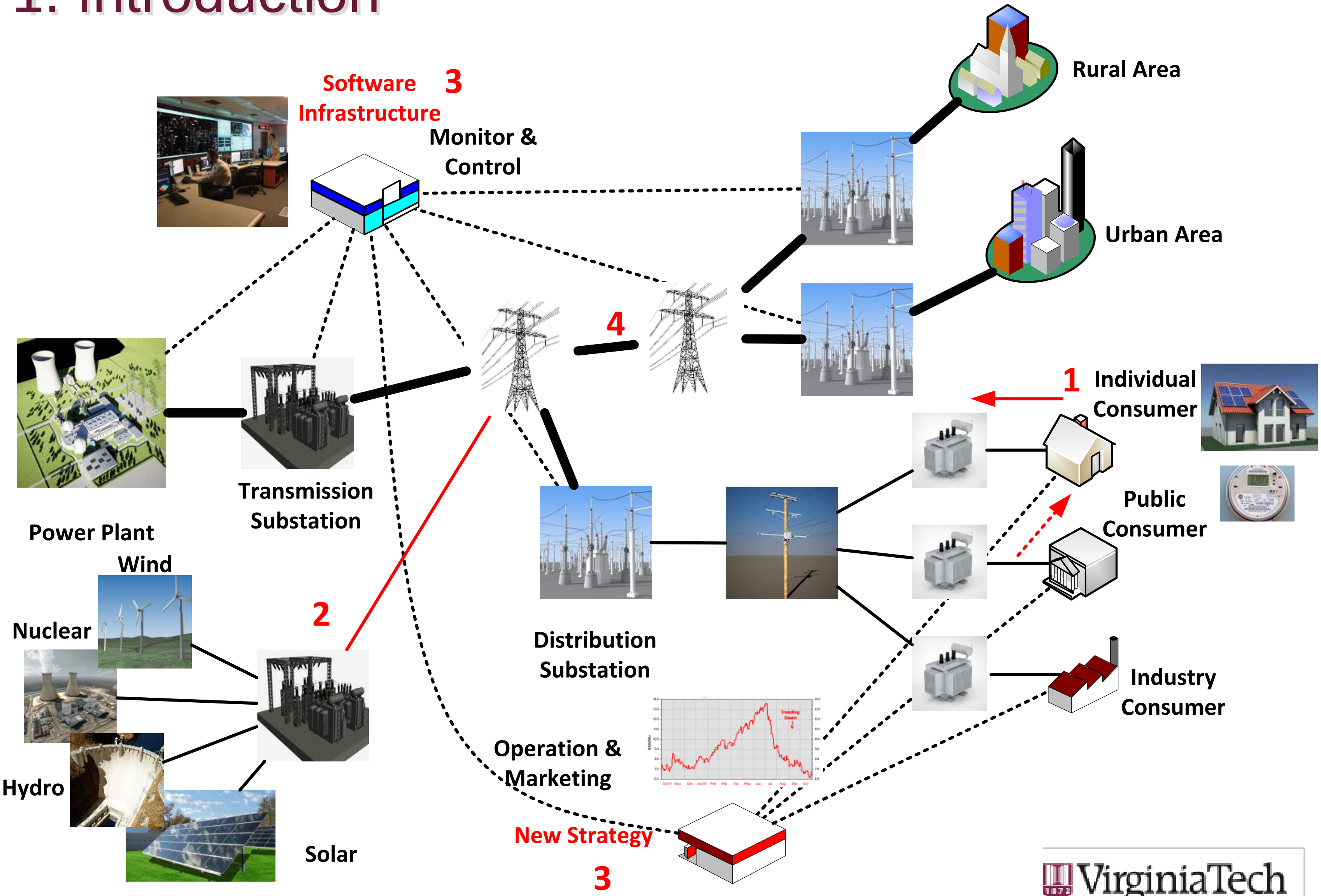
9th Electricity Conference at CMU

VirginiaTech
Invent the Future

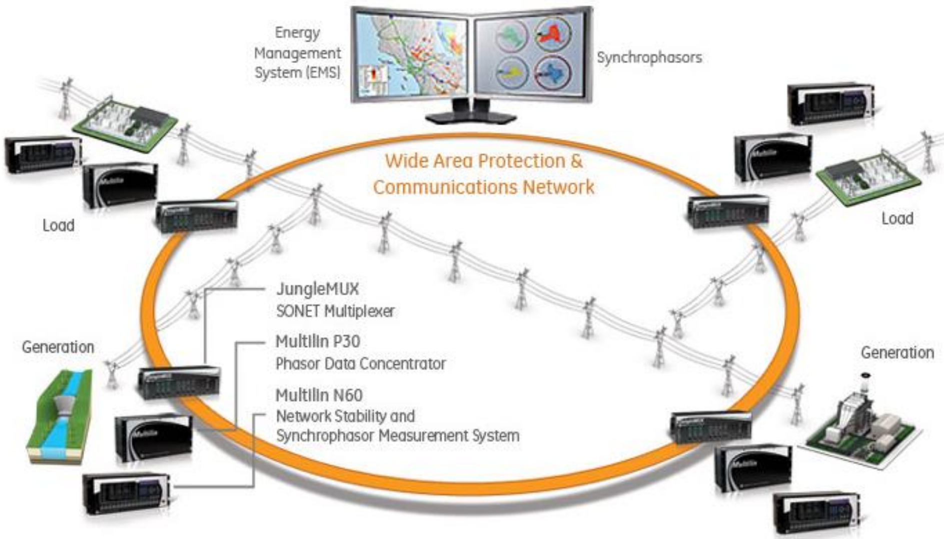
Outline

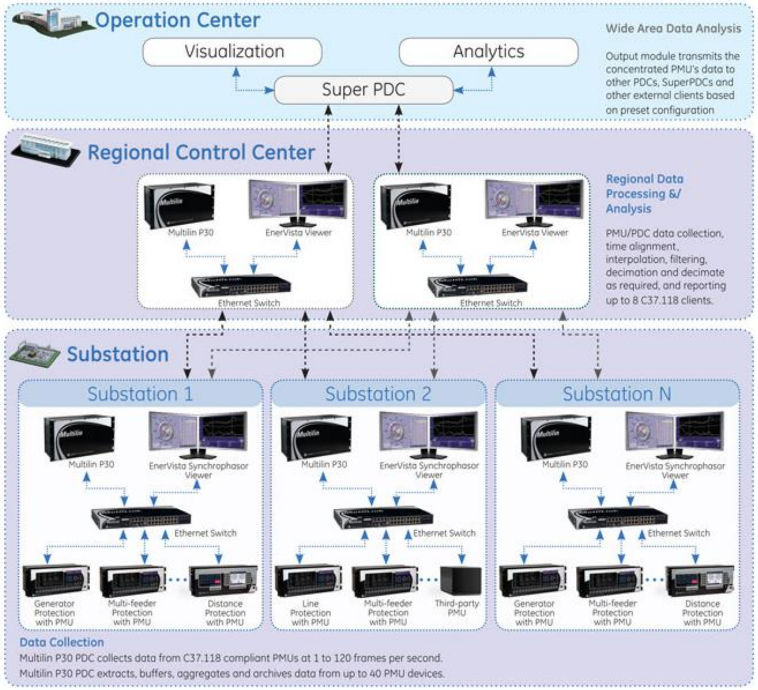
1. Introduction
2. Power Systems and Communication System Co-Simulation: GECO: a Modulized Global Event-driven CO-simulation Platform
3. Cyber Attack Simulation on PMU-based State Estimation
4. Co-simulation Case Study on PMU-based Out-of-step Protection
5. Conclusion & Future Research

1: Introduction



GE’s Solution on Wide Area Monitoring and Control – Synchrophasor Techniques


Energy Management System (EMS)
Synchrophasors
Wide Area Protection & Communications Network
Load
Load
JungleMUX SONET Multiplexer
Multilin P30 Phasor Data Concentrator
Multilin N60 Network Stability and Synchrophasor Measurement System
Generation
Generation

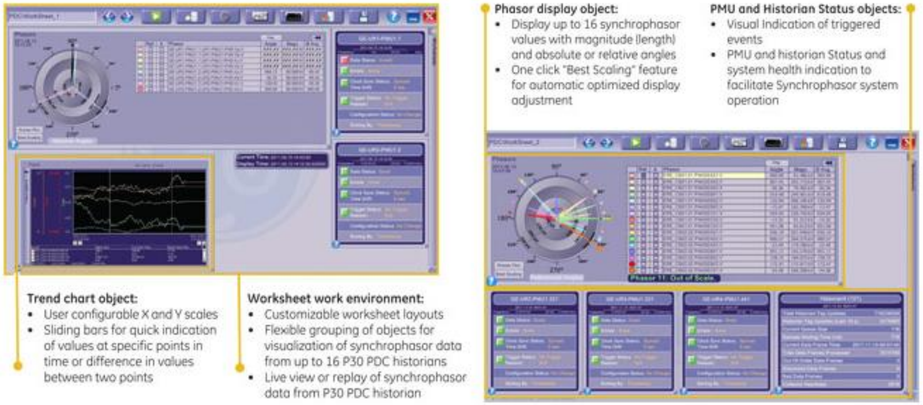


Output module transmits the concentrated PMU's data to other PDCs, SuperPDCs and other external clients based on preset configuration

PMU/PDC data collection, time alignment, interpolation, filtering, decimation and decimate as required, and reporting up to 8 C37.118 clients.

Multilin P30 PDC collects data from C37.118 compliant PMUs at 1 to 120 frames per second.

Multilin P30 PDC extracts, buffers, aggregates and archives data from up to 40 PMU devices.



Phasor display object:
- Display up to 16 synchrophasor values with magnitude (length) and absolute or relative angles
- One click "Best Scaling" feature for automatic optimized display adjustment

PMU and Historian Status objects:
- Visual Indication of triggered events
- PMU and historian Status and system health indication to facilitate Synchrophasor system operation

Trend chart object:
- User configurable X and Y scales
- Sliding bars for quick indication of values at specific points in time or difference in values between two points

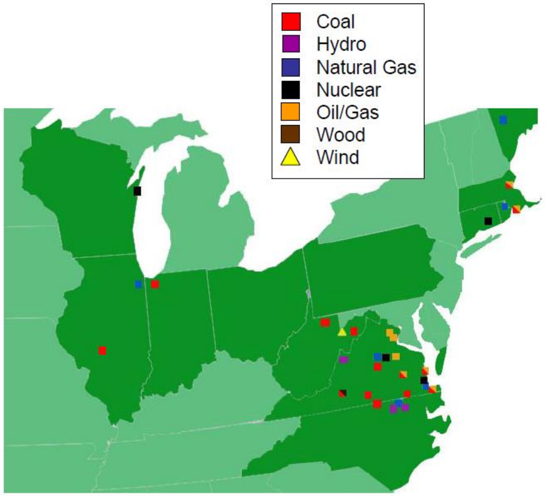
Worksheet work environment:
- Customizable worksheet layouts
- Flexible grouping of objects for visualization of synchrophasor data from up to 16 P30 PDC historians
- Live view or replay of synchrophasor data from P30 PDC historian

* From GE’s Industrial Solution Website

Dominion Synchrophasor Project

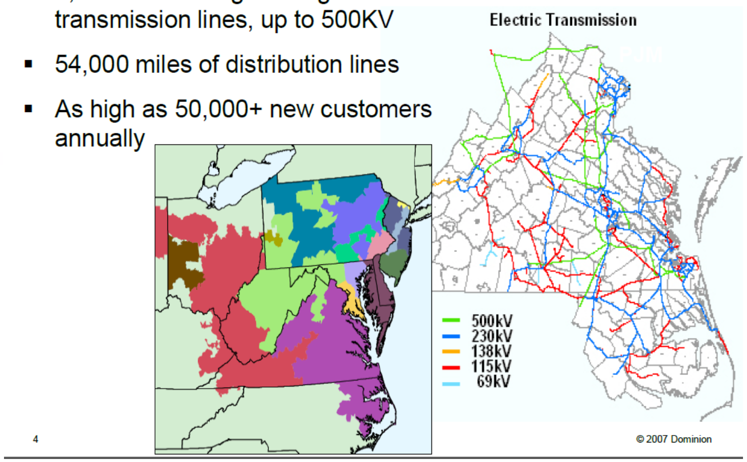
Domination Generation

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



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



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

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

** From Dominion project and VT project report

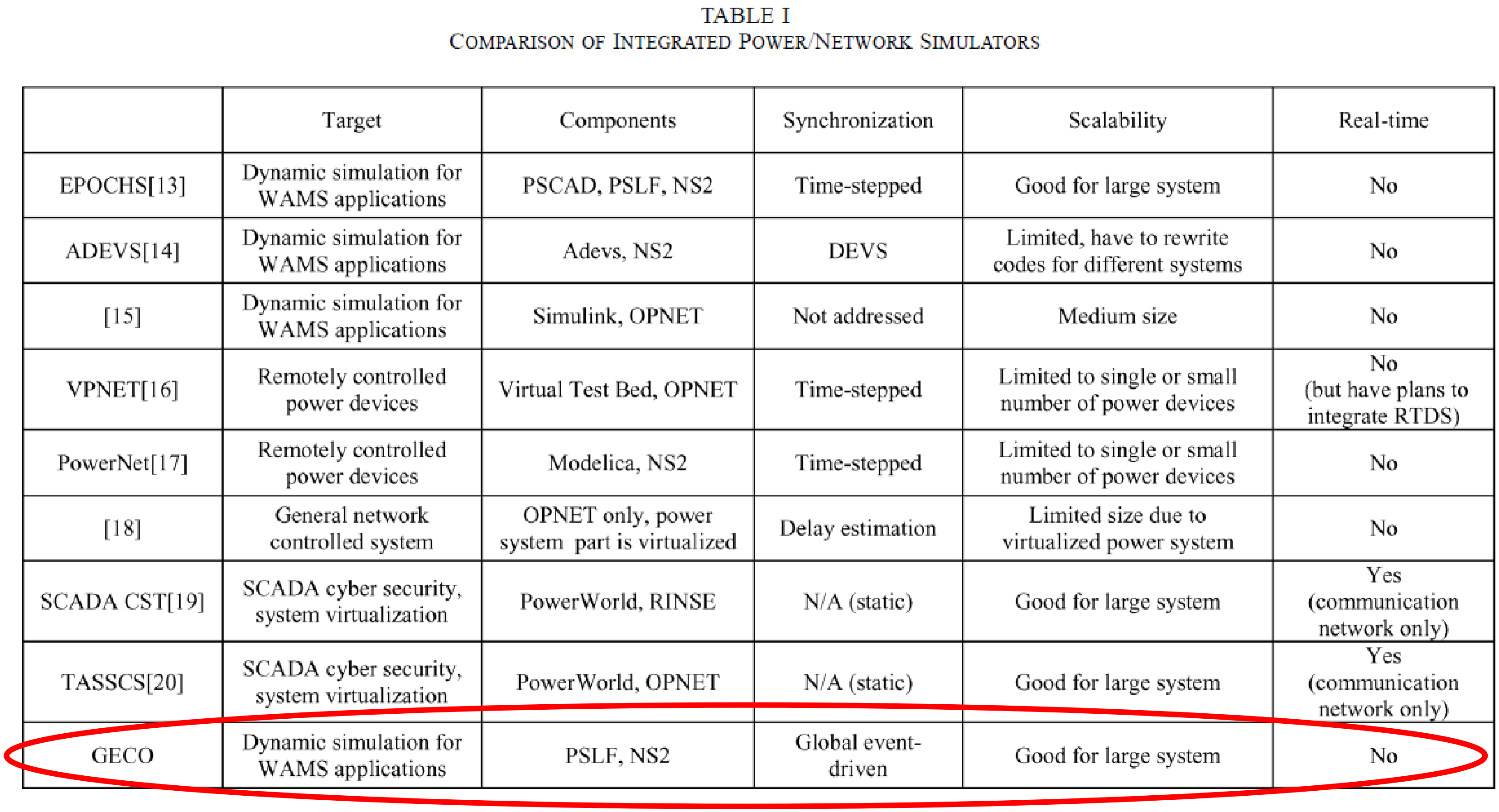
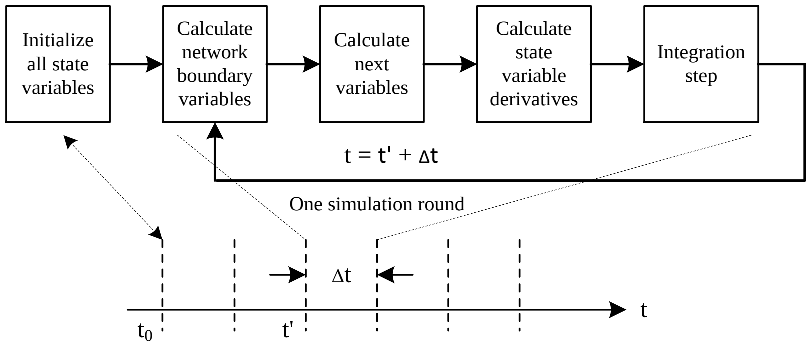


TABLE I
COMPARISON OF INTEGRATED POWER/NETWORK SIMULATORS

	Target	Components	Synchronization	Scalability	Real-time
EPOCHS[13]	Dynamic simulation for WAMS applications	PSCAD, PSLF, NS2	Time-stepped	Good for large system	No
ADEVS[14]	Dynamic simulation for WAMS applications	Adevs, NS2	DEVS	Limited, have to rewrite codes for different systems	No
[15]	Dynamic simulation for WAMS applications	Simulink, OPNET	Not addressed	Medium size	No
VPNET[16]	Remotely controlled power devices	Virtual Test Bed, OPNET	Time-stepped	Limited to single or small number of power devices	No (but have plans to integrate RTDS)
PowerNet[17]	Remotely controlled power devices	Modelica, NS2	Time-stepped	Limited to single or small number of power devices	No
[18]	General network controlled system	OPNET only, power system part is virtualized	Delay estimation	Limited size due to virtualized power system	No
SCADA CST[19]	SCADA cyber security, system virtualization	PowerWorld, RINSE	N/A (static)	Good for large system	Yes (communication network only)
TASSCS[20]	SCADA cyber security, system virtualization	PowerWorld, OPNET	N/A (static)	Good for large system	Yes (communication network only)
GECO	Dynamic simulation for WAMS applications	PSLF, NS2	Global event-driven	Good for large system	No

Hua Lin; Veda, S.S.; Shukla, S.S.; Mili, L.; Thorp, J., "GECO: Global Event-Driven Co-Simulation Framework for Interconnected Power System and Communication Network," Smart Grid, IEEE Transactions on , vol.3, no.3, pp.1444,1456, Sept. 2012

2: Global Event-Driven Synchronization

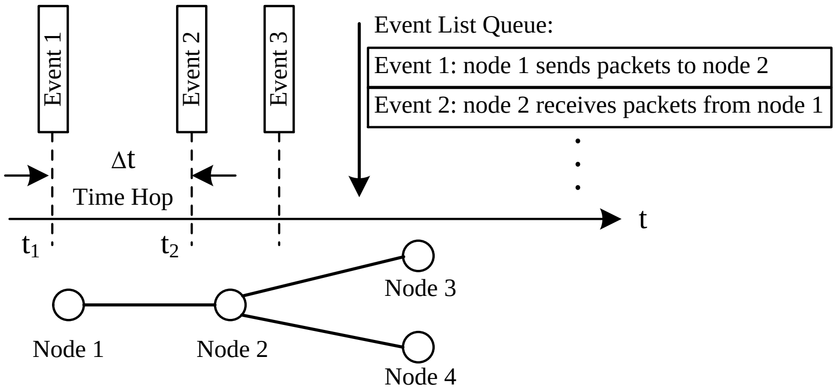


Initialize all state variables → Calculate network boundary variables → Calculate next variables → Calculate state variable derivatives → Integration step

t = t' + Δt

One simulation round

Dynamic Simulation Procedure of Power Systems

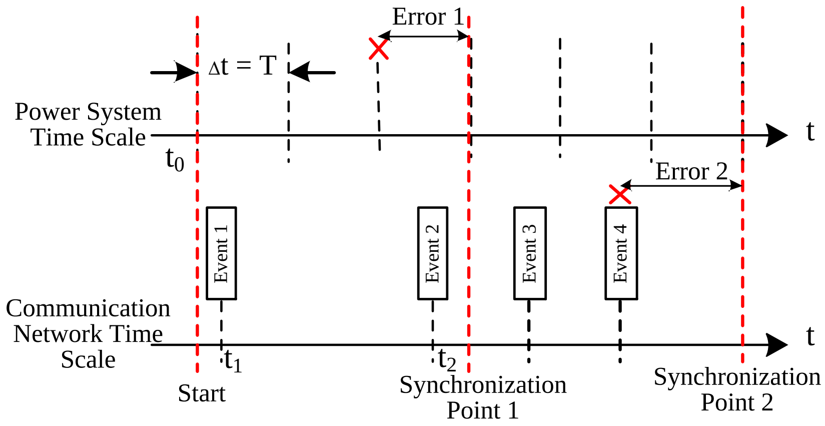


Event List Queue:

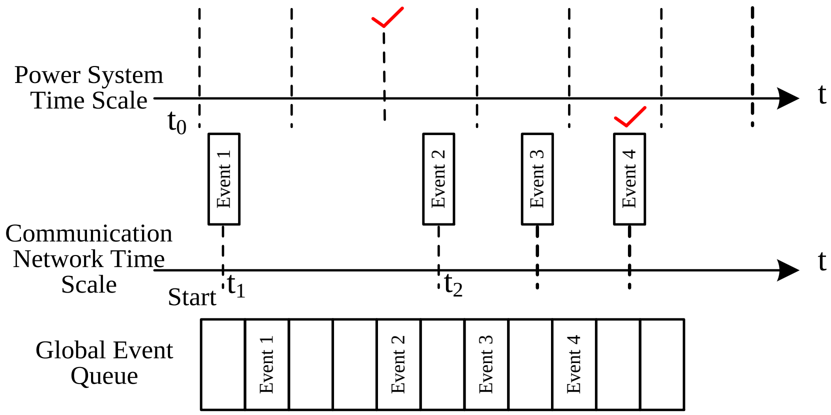
Event 1: node 1 sends packets to node 2

Event 2: node 2 receives packets from node 1

Communication Network Simulation Procedure

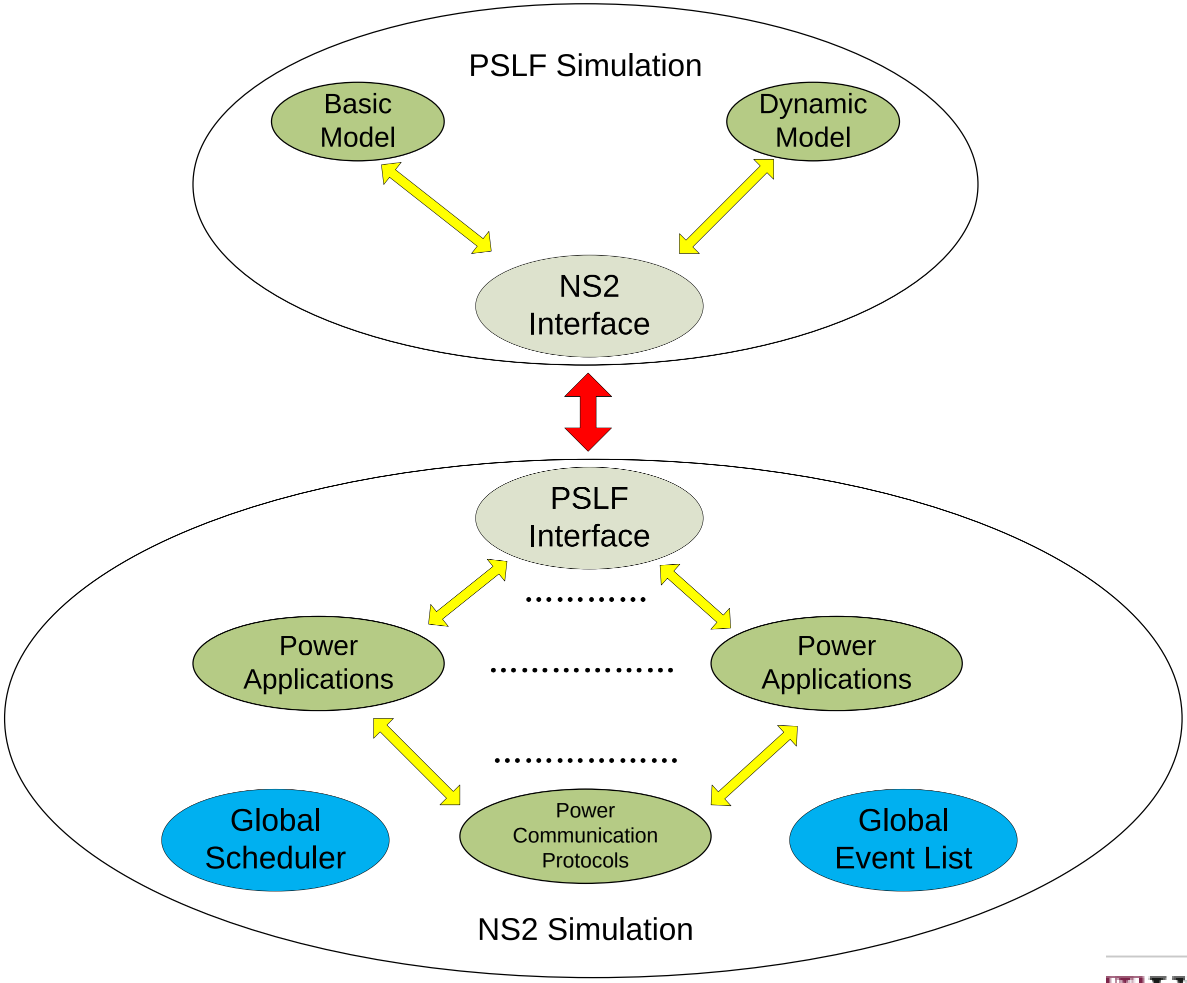


Two types of synchronization errors

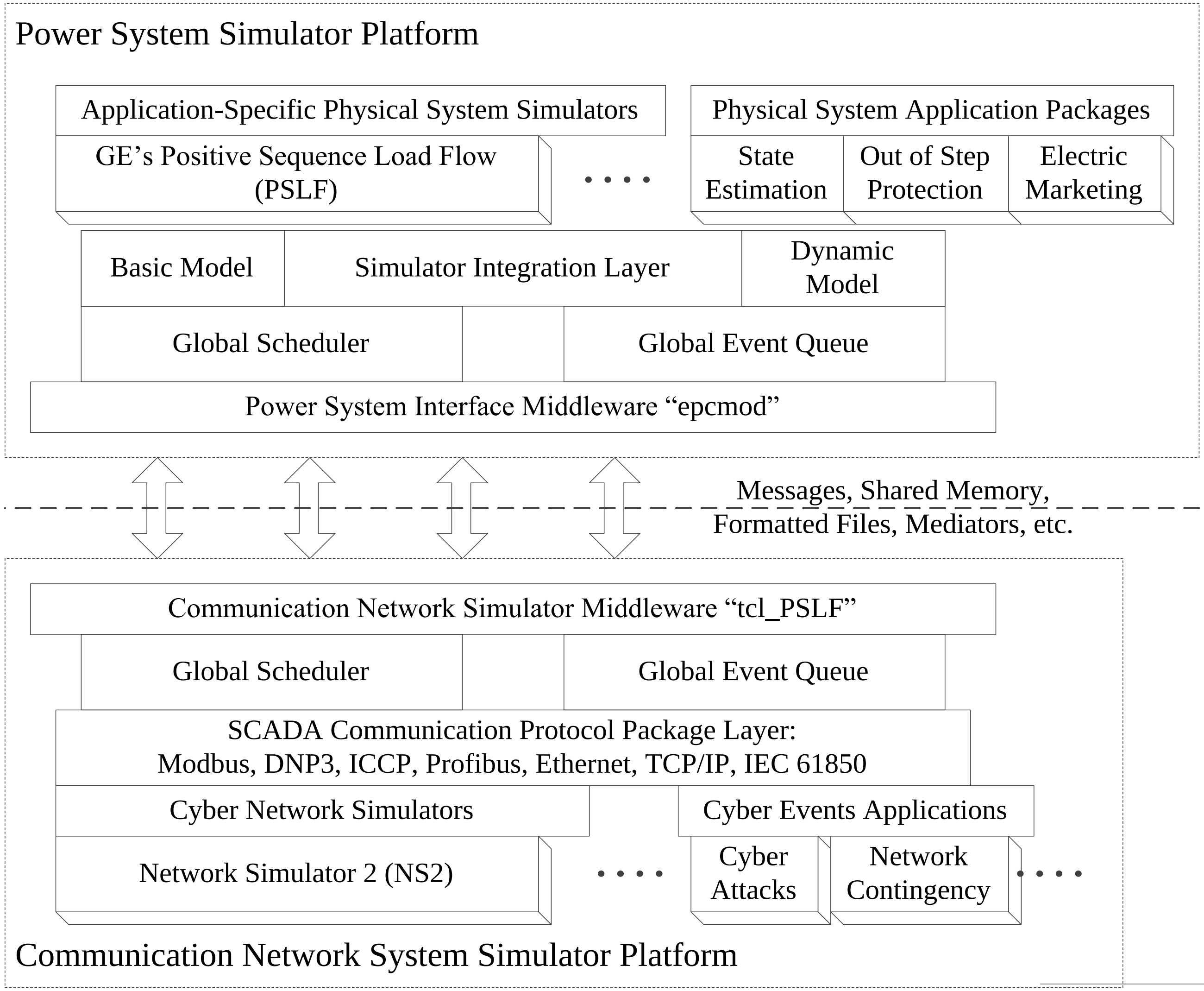


Event-driven synchronization without errors

GECO (Global Event-driven CO-simulation): Platform Structure



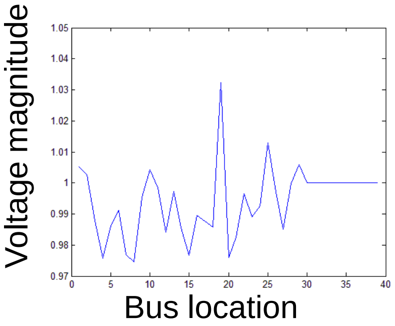
GECO: A Modulized *G*lobal *E*vent-driven *CO*-simulation platform

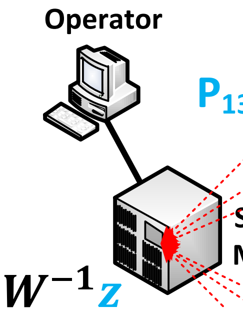


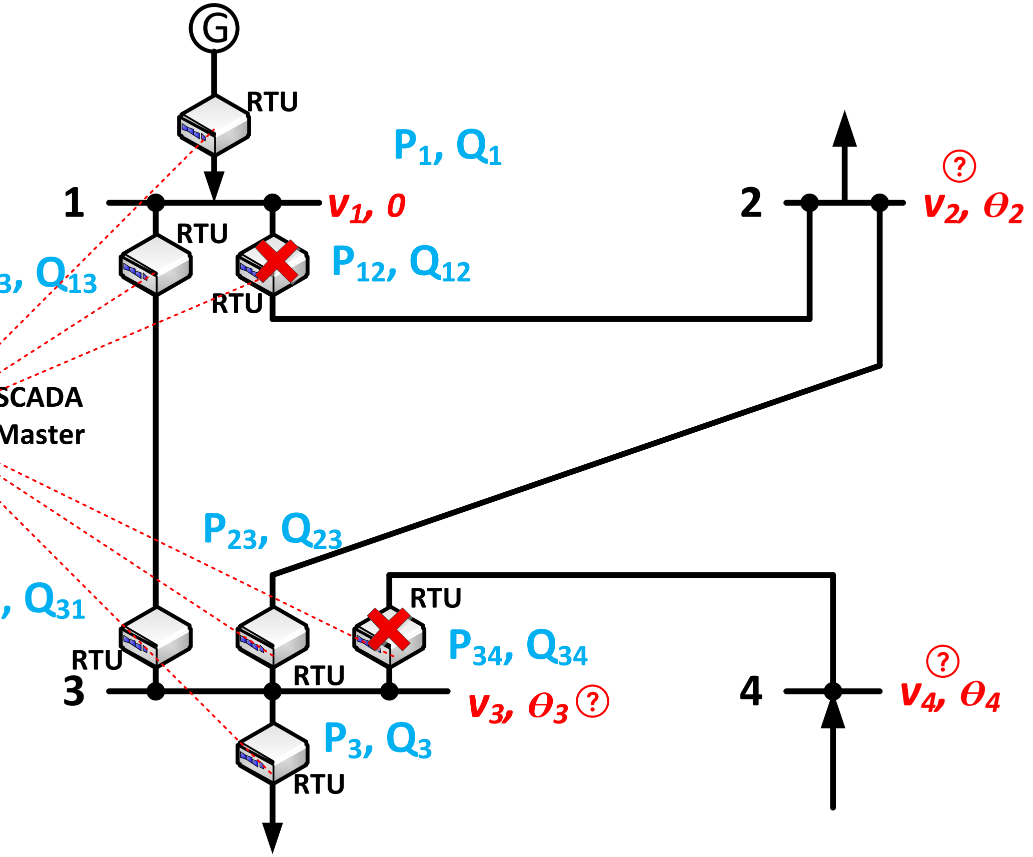
Power System Simulator Platform
Application-Specific Physical System Simulators
GE's Positive Sequence Load Flow (PSLF)
. . . .
Physical System Application Packages
State Estimation
Out of Step Protection
Electric Marketing
Basic Model
Simulator Integration Layer
Dynamic Model
Global Scheduler
Global Event Queue
Power System Interface Middleware "epcmod"
Messages, Shared Memory, Formatted Files, Mediators, etc.
Communication Network Simulator Middleware "tcl_PSLF"
Global Scheduler
Global Event Queue
SCADA Communication Protocol Package Layer:
Modbus, DNP3, ICCP, Profibus, Ethernet, TCP/IP, IEC 61850
Cyber Network Simulators
Network Simulator 2 (NS2)
. . . .
Cyber Events Applications
Cyber Attacks
Network Contingency
. . . .
Communication Network System Simulator Platform

3: Problem Statement: Attack Model

Malicious Data Injection attack on State Estimation







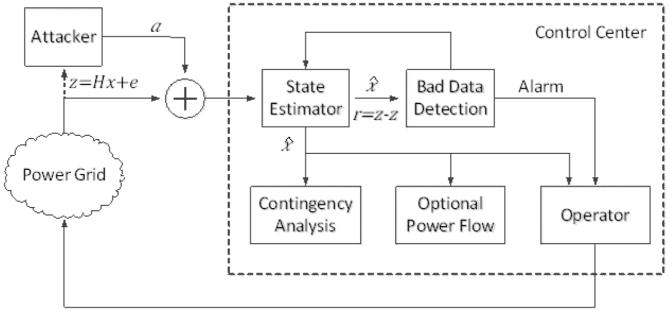
$$z = Hx + e$$

$$\hat{x} = \left(H^T W^{-1} H\right)^{-1} H^T W^{-1} z$$

$$z_a = z + a$$

$$a = Hc$$

$$\left\| z_a - H\hat{x}_f \right\| = \| z - H\hat{x} \| \leq \tau$$



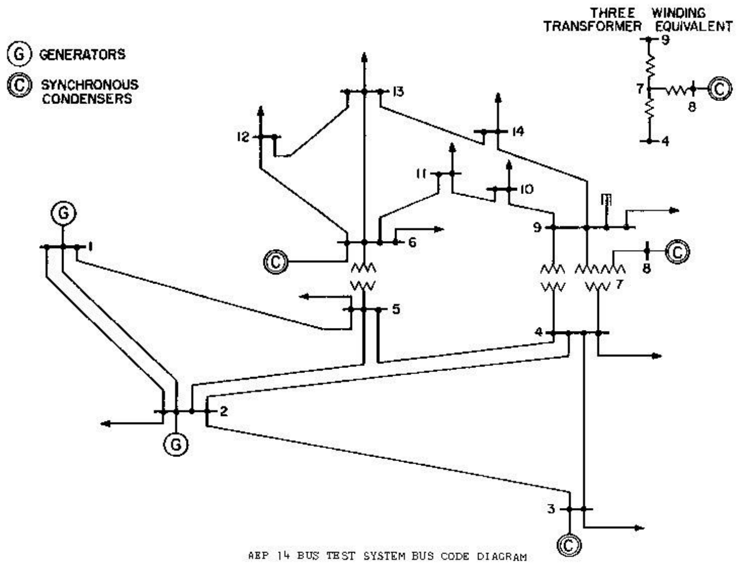
We can't detect the attacks

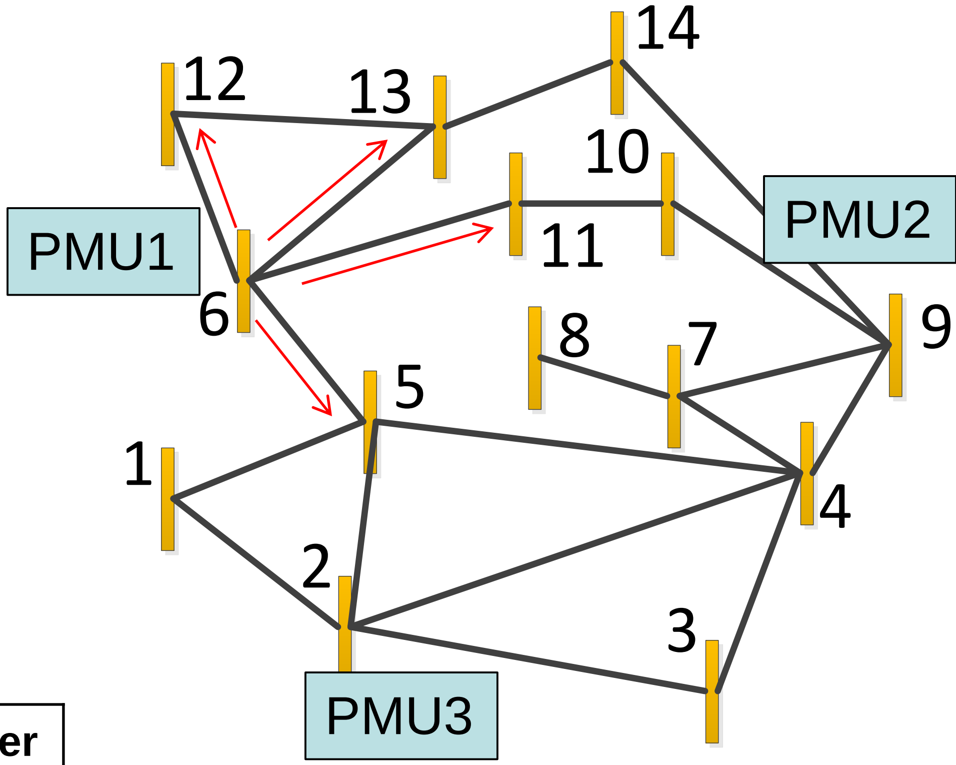
The injected data will modify the state estimation results

VirginiaTech
Invent the Future

The Placement of PMUs

IEEE 14-Bus Example


GENERATORS
SYNCHRONOUS CONDENSERS
THREE WINDING TRANSFORMER EQUIVALENT
1
2
3
4
5
6
7
8
9
10
11
12
13
14
AEP 14 BUS TEST SYSTEM BUS CODE DIAGRAM



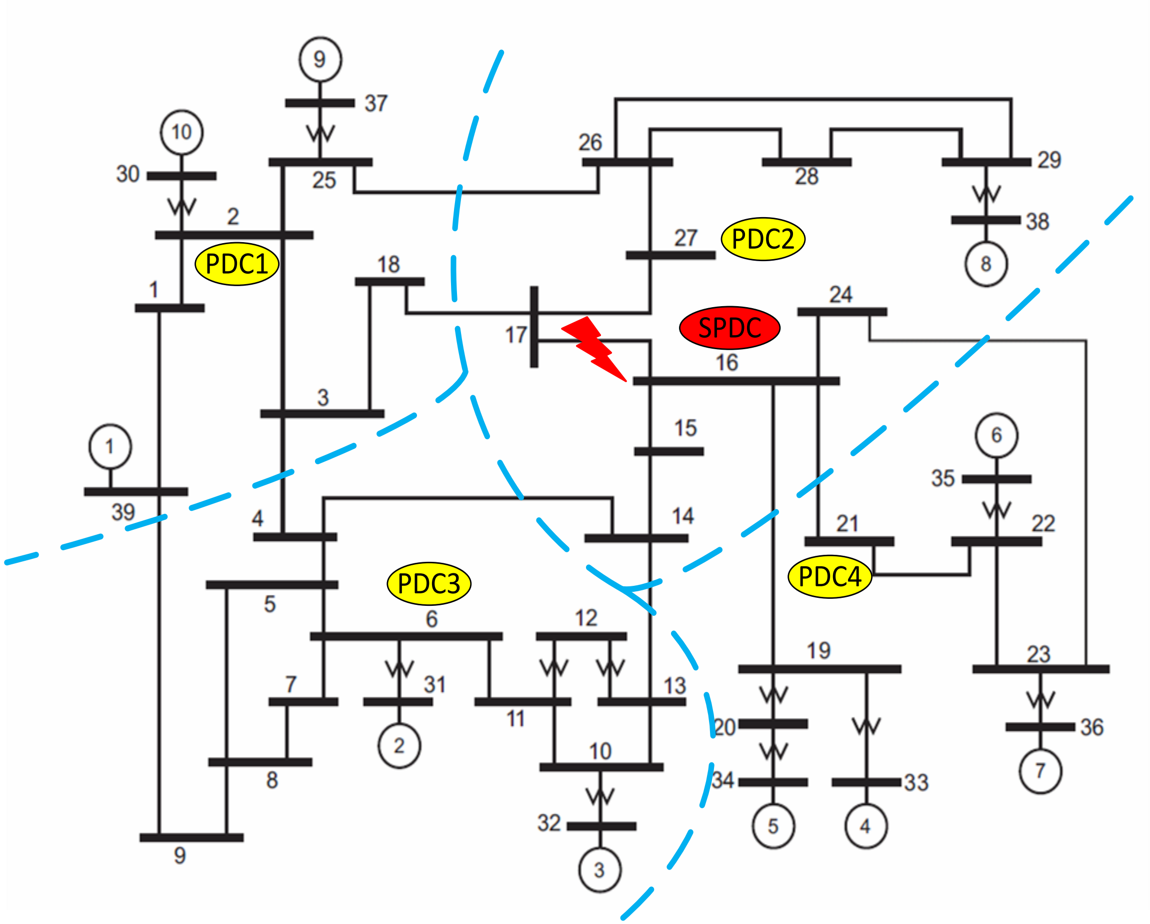
Test system	PMUs Number
IEEE 14-bus	3
IEEE 24-bus	6
IEEE 30-bus	7
New England 39-bus	8
IEEE 57-bus	11

Minimum number of critical places for installing PMUs

Secured PMUs installed in these places make the system observable

Case study:

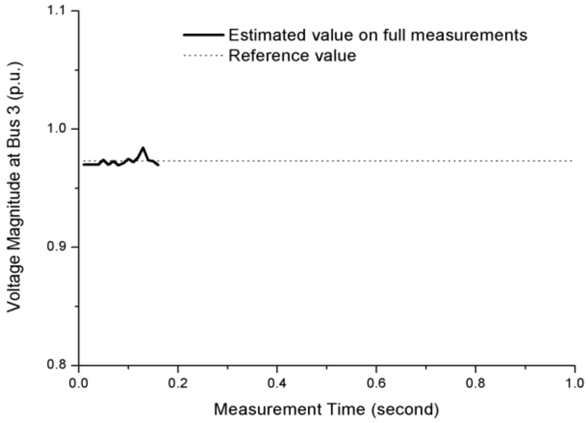
New England 39-bus test system



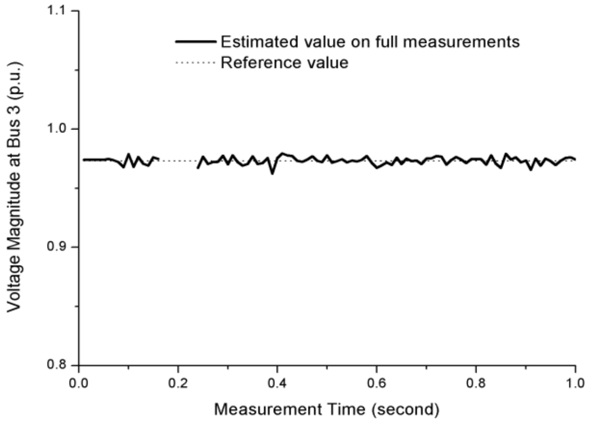
Cyber attack Simulation: on network channels

Single Network Link Failure

Bus16-Bus17 (Tp=50ms)

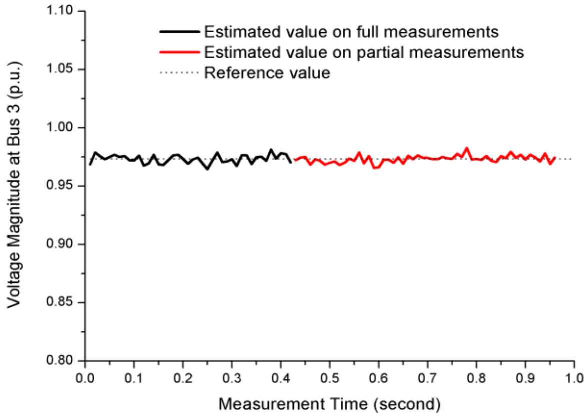


Bus16-Bus17 (Tp=60ms)

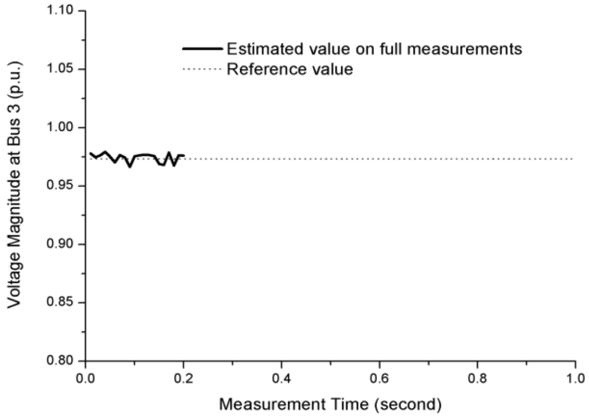


Saturation attacks

Network saturation 50%



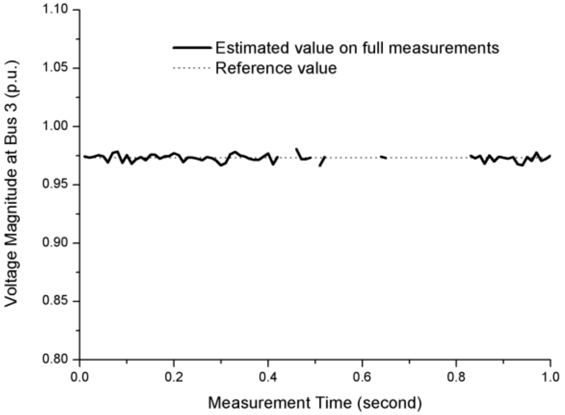
Network saturation 85%



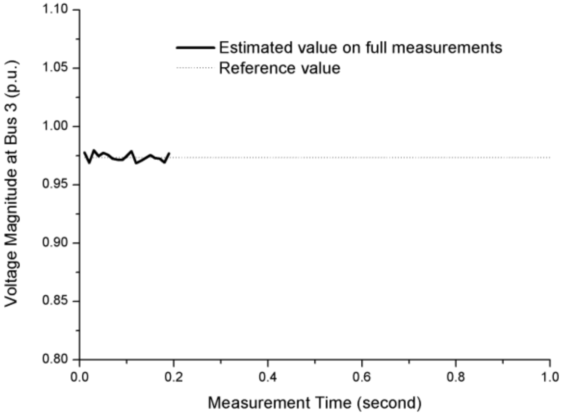
Cyber attack Simulation: on network nodes

Denial of Service Attack

DoS attack on the router at Bus 16

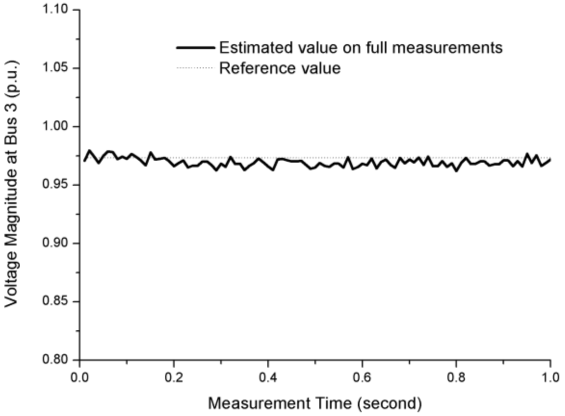


Enhanced DoS attack

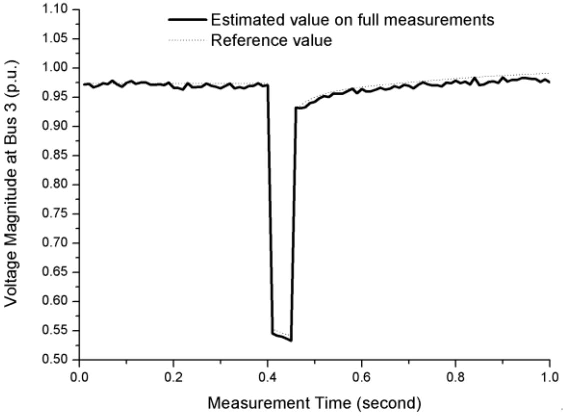


Data Spoofing

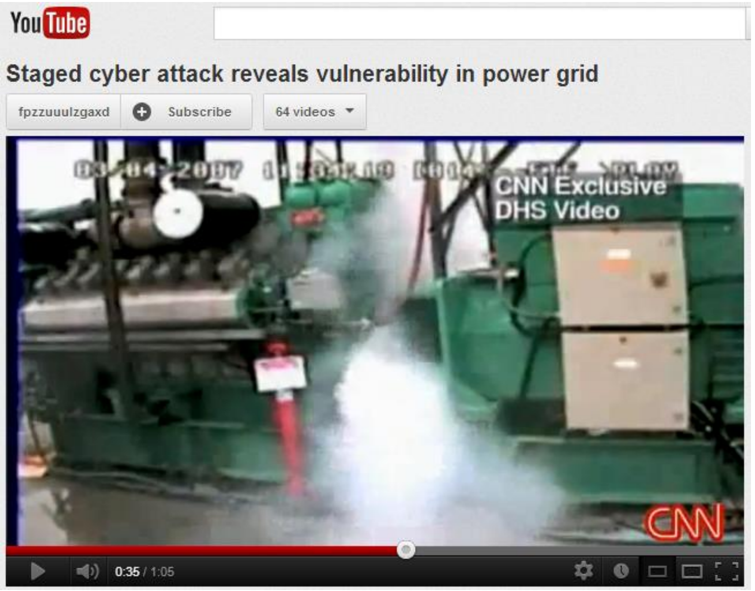
PMU spoofing on Bus 3



PMU spoofing in contingency



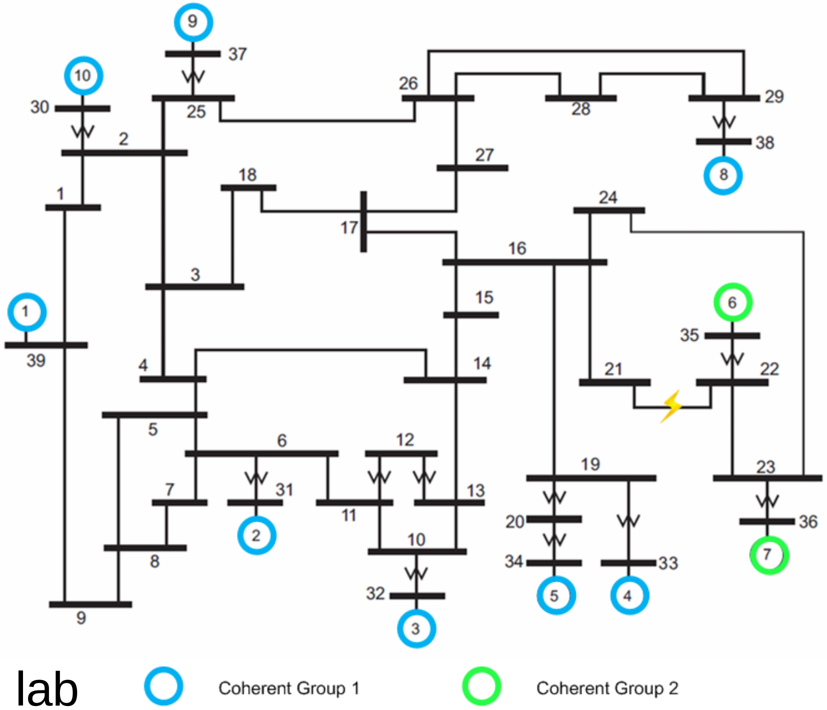
4: Out-of-Step Protection



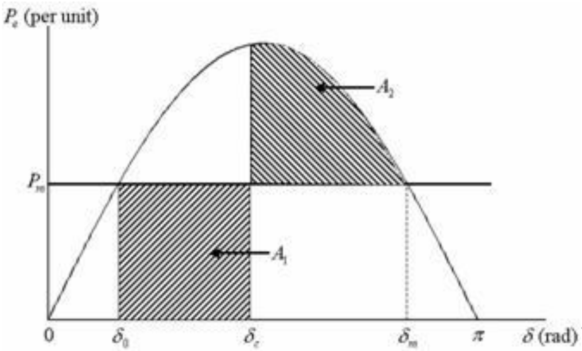
Staged cyber attack reveals vulnerability in power grid

fpzzuuulzgaxd · Subscribe · 64 videos

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.

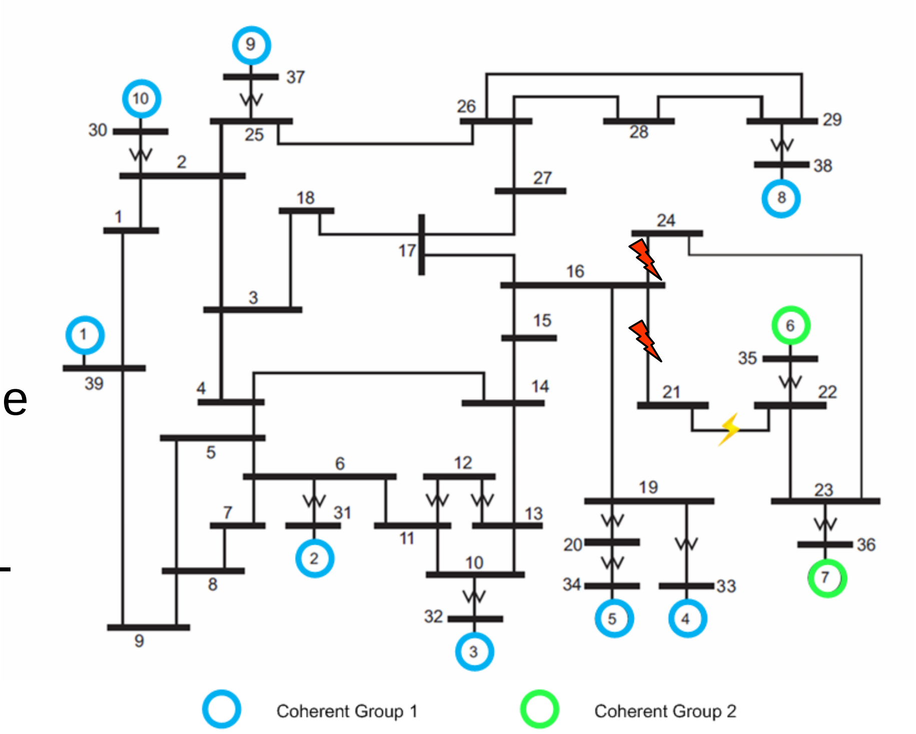


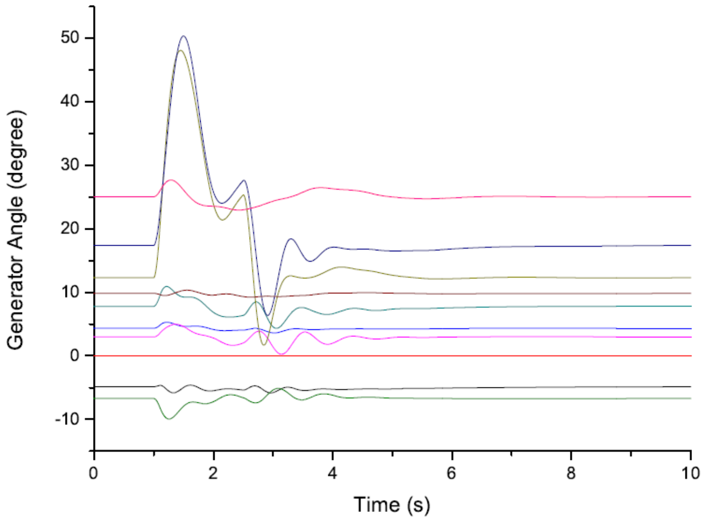
Equal Area Criterion

Out-of-Step Protection

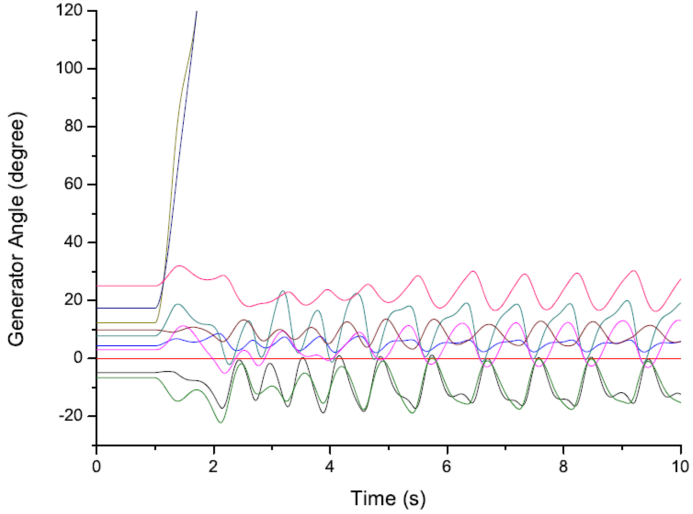
- Out-of-Step (OOS) means a generator or a group of generators lose synchronism with the rest of the system.

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





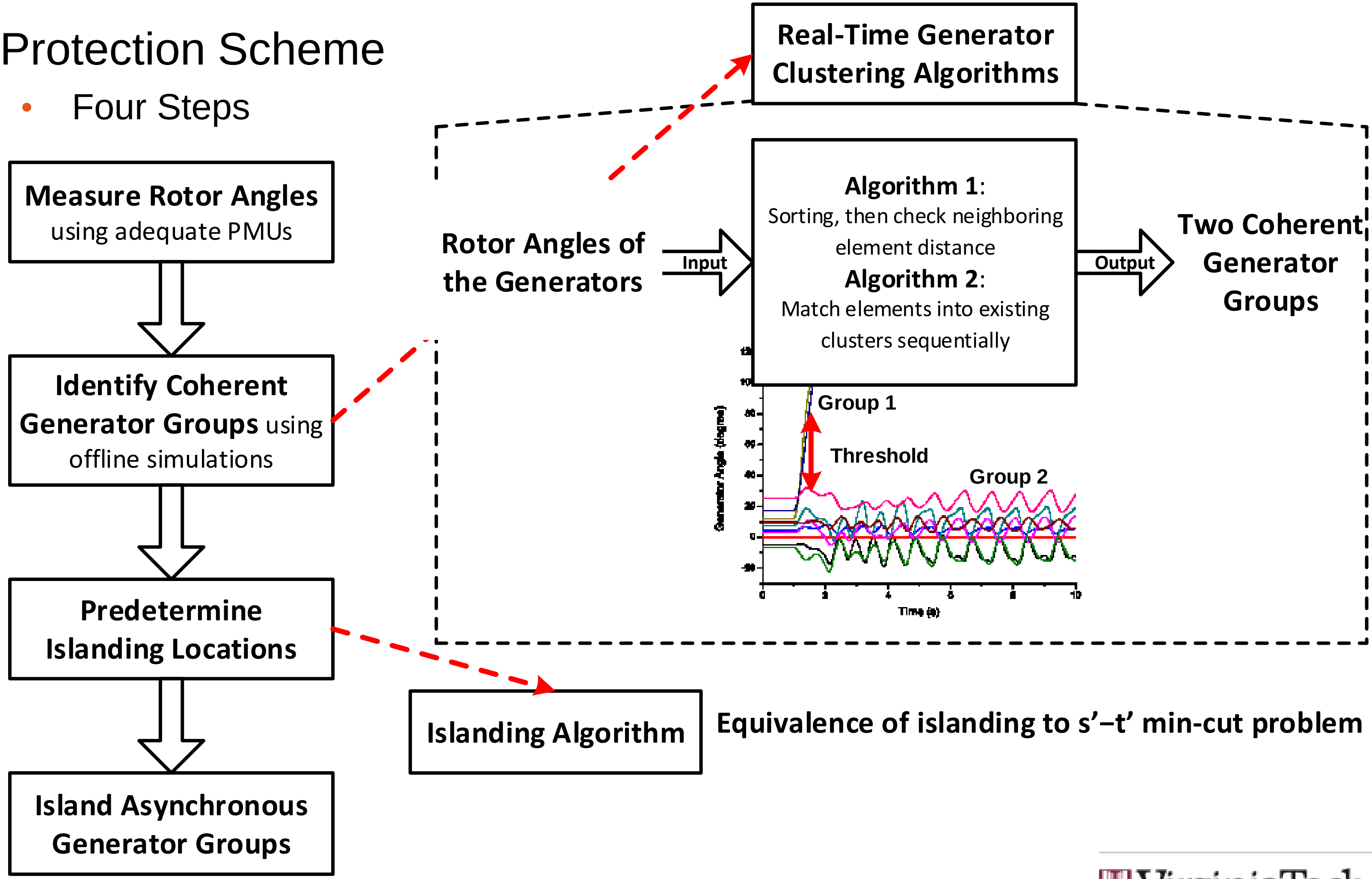
Fault cleared in 0.1 second, system back to normal condition



Fault cleared in 0.3 second, OOS condition is observed

PMU-based Out-of-Step Protection

- Protection Scheme
  - Four Steps



Measure Rotor Angles using adequate PMUs

Identify Coherent Generator Groups using offline simulations

Predetermine Islanding Locations

Island Asynchronous Generator Groups

Real-Time Generator Clustering Algorithms

Rotor Angles of the Generators

Algorithm 1: Sorting, then check neighboring element distance

Algorithm 2: Match elements into existing clusters sequentially

Two Coherent Generator Groups

Islanding Algorithm

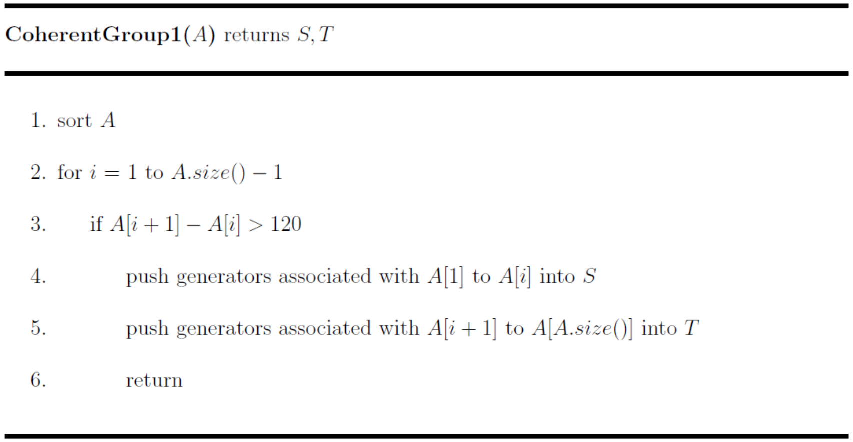
Equivalence of islanding to s'–t' min-cut problem

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.

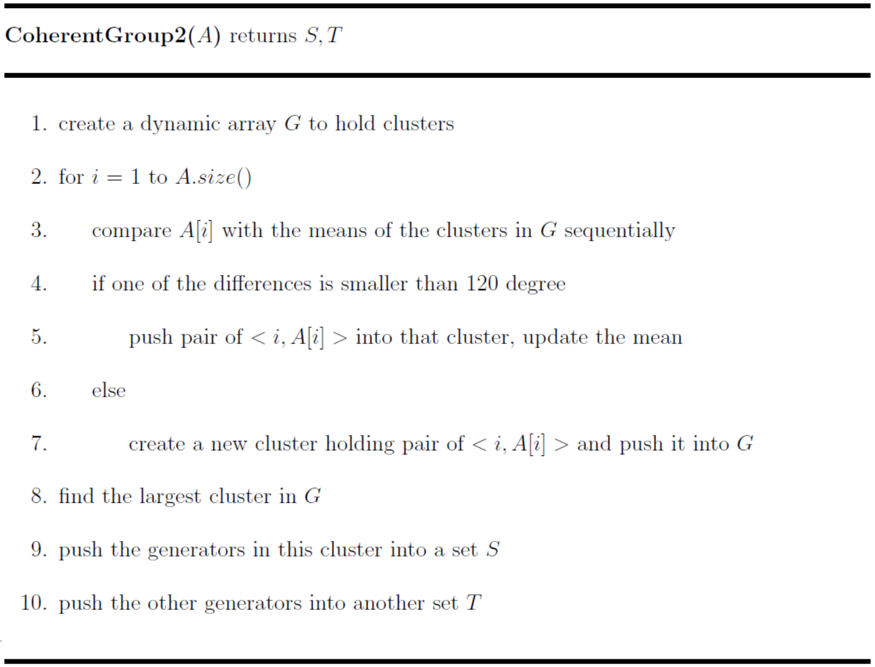
- The first algorithm sorts the measured rotor angle and traverse the measured rotor angle sequentially. If the gap between two neighbors is greater than 120 degrees, then the OOS condition is identified.

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



CoherentGroup1(A) returns S, T

```
sort $A$
for $i = 1$ to $A.size() - 1$
    if $A[i+1] - A[i] > 120$
        push generators associated with $A[1]$ to $A[i]$ into $S$
        push generators associated with $A[i+1]$ to $A[A.size()]$ into $T$
        return
```

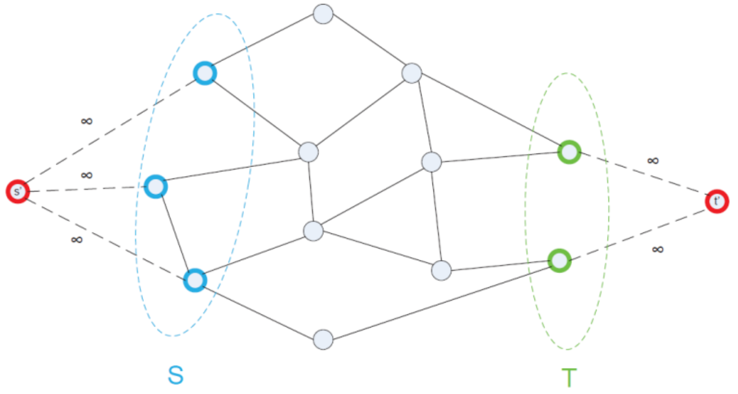


CoherentGroup2(A) returns S, T

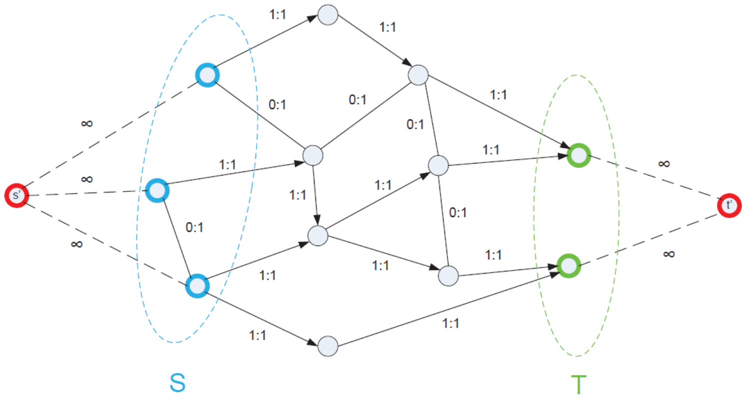
```
create a dynamic array $G$ to hold clusters
for $i = 1$ to $A.size()$
    compare $A[i]$ with the means of the clusters in $G$ sequentially
    if one of the differences is smaller than 120 degree
        push pair of $< i, A[i] >$ into that cluster, update the mean
    else
        create a new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

Islanding Algorithm

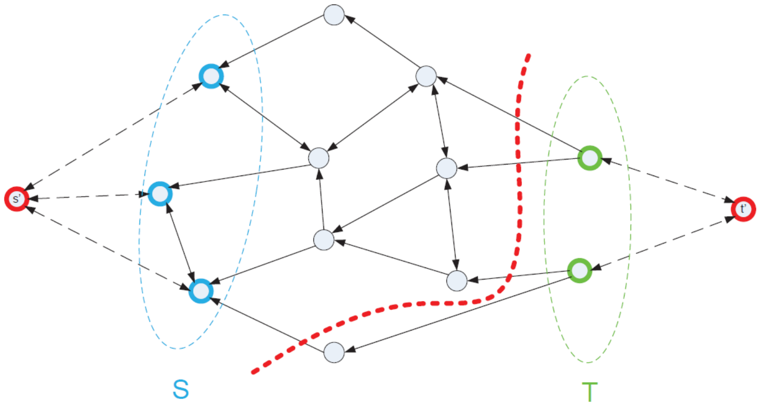
- As long as we have found two coherent generator groups *S* and *T*, the next step is to find a minimum cut of the entire power system that can separate *S* and *T*.
- Edmonds-Karp algorithm which is $O(|V||E|^2)$



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

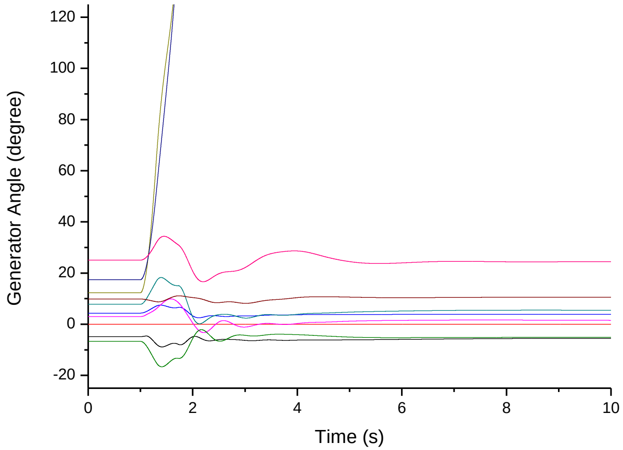


A max-flow example

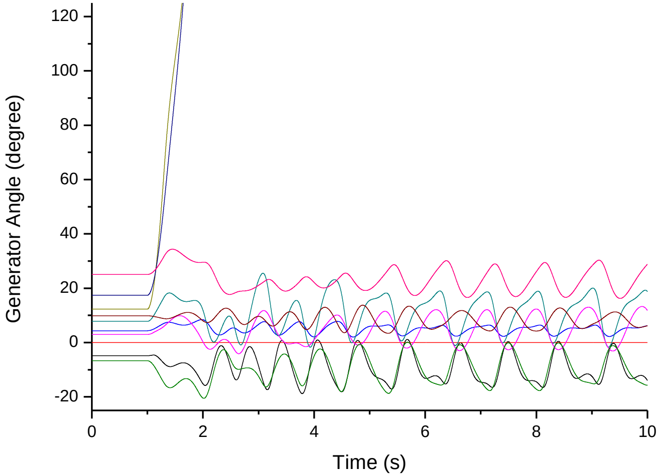


Find the min-cut on the residual network

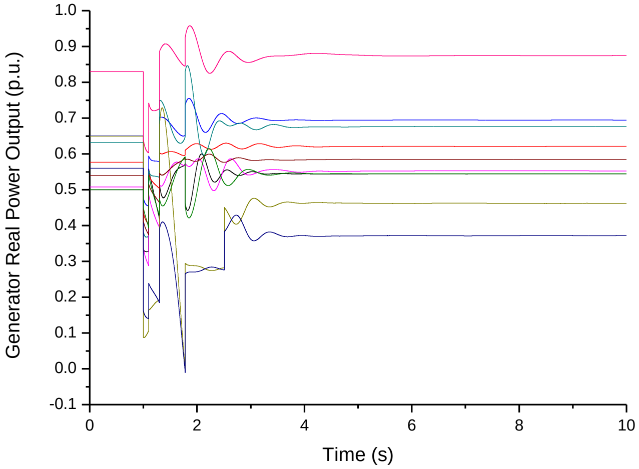
Simulation Results



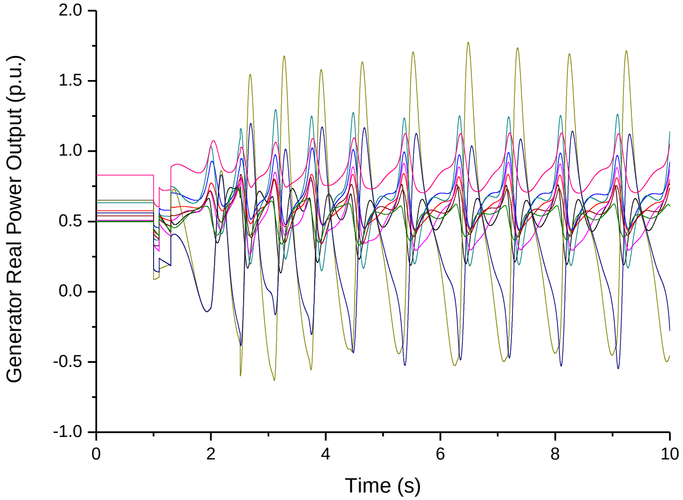
Generator angels showing OOS condition
(BW=1Gbps, D=5ms)



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



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



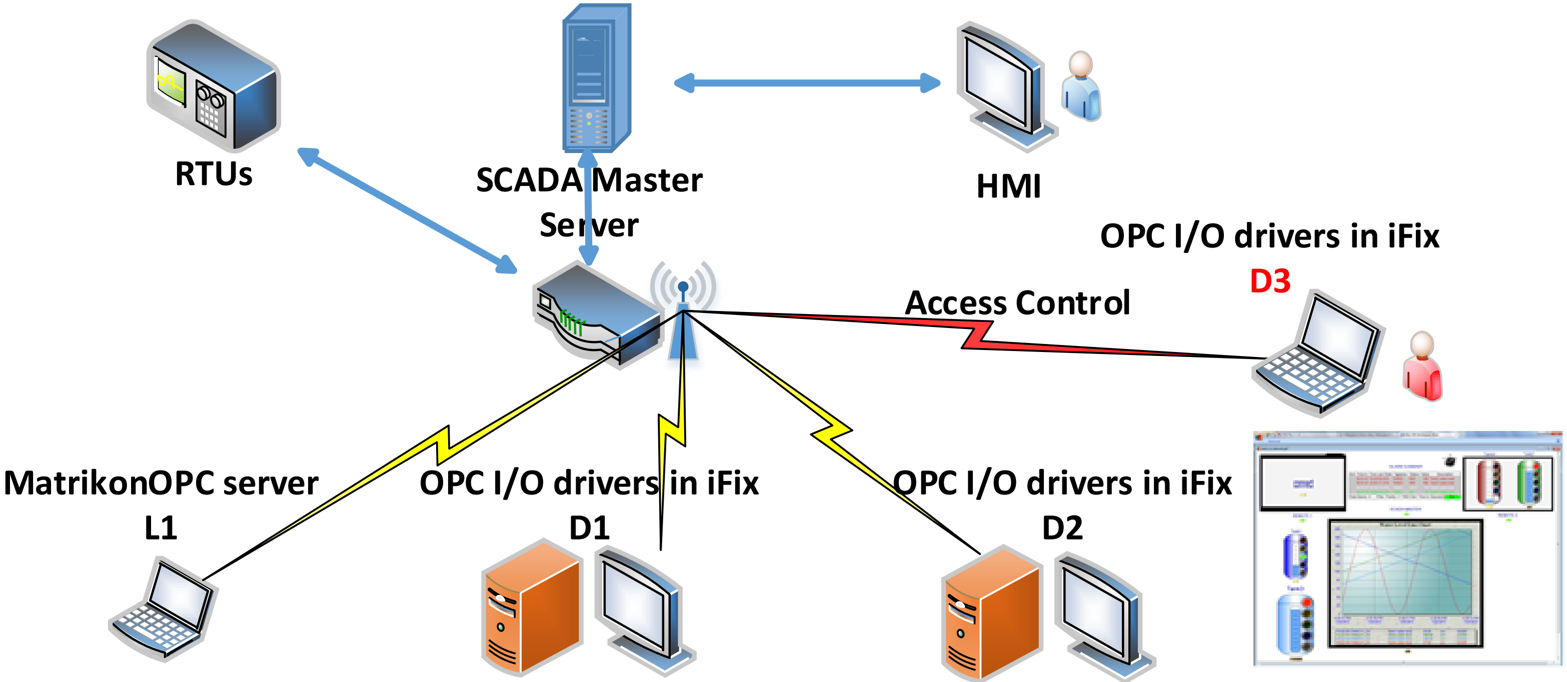
Generator real power outputs with link failure
(BW=100Mbps, D=10ms)

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

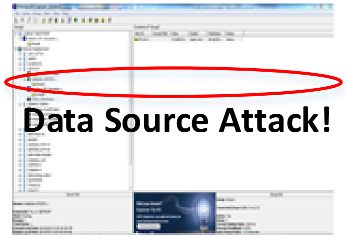
OPC I/O drivers in iFix D3

Access Control

MatrikonOPC server L1

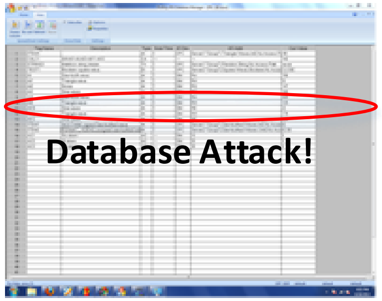
OPC I/O drivers in iFix D1

OPC I/O drivers in iFix D2



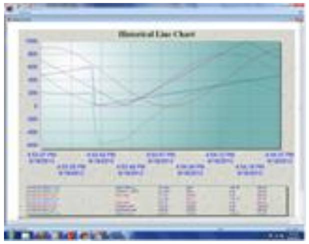
Data Source Attack!

assigns the data to a tag in the iFix database manager

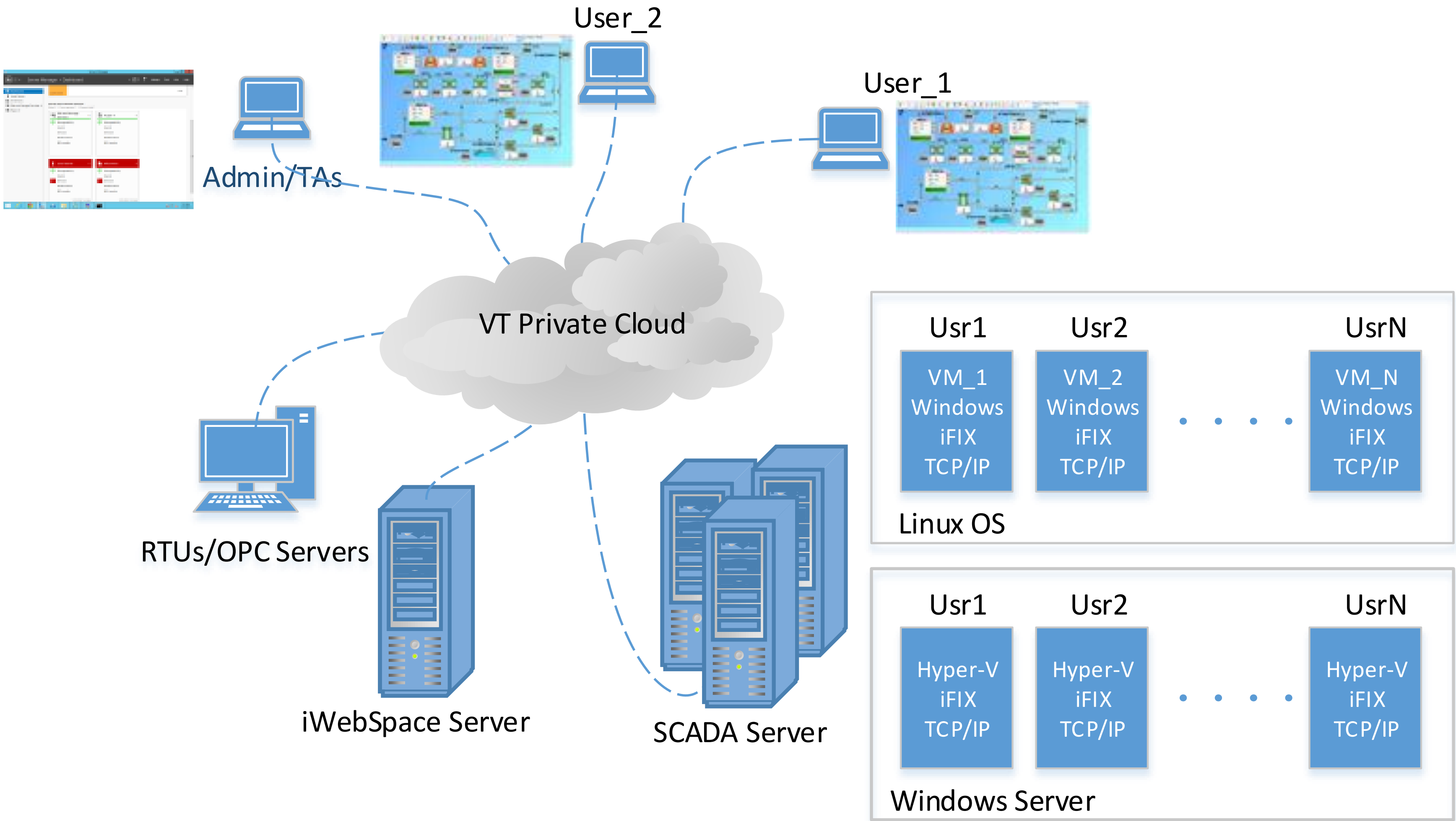


Database Attack!

monitors the tag in D1's database



Cloud-based Virtual SCADA Infrastructure in VT



User_2

User_1

Admin/TAs

VT Private Cloud

RTUs/OPC Servers

iWebSpace Server

SCADA Server

Usr1	Usr2		UsrN
VM_1 Windows iFIX TCP/IP	VM_2 Windows iFIX TCP/IP	. . . .	VM_N Windows iFIX TCP/IP

Linux OS

Usr1	Usr2		UsrN
Hyper-V iFIX TCP/IP	Hyper-V iFIX TCP/IP	. . . .	Hyper-V iFIX TCP/IP

Windows Server

References

1. Hua Lin, Yi Deng, Sandeep Shukla, James Thorp, Lamine Mili. "Cyber Security Impacts on All-PMU State Estimator - A Case Study on Co-Simulation Platform GECO", Third International IEEE Conference on Smart Grid Communications (SmartGridComm), November, 2012, Tainan City, Taiwan.
2. Yi Deng, Sandeep Shukla, “Vulnerabilities and Countermeasures - A Survey on the Cyber Security issues in the Transmission Subsystem of a Smart Grid”, Journal of Cyber Security and Mobility, invited paper, 2012
3. Yi Deng, Hua Lin, Arun G. Phadke, Sandeep Shukla, and James S. Thorp, “Networking technologies for wide-area measurement applications” book chapter, “Smart Grid Communications and Networking” to be published, Cambridge University Press, UK, 2012
4. Yi Deng, Hua Lin, Arun G. Phadke, Sandeep Shukla, James S. Thorp, Lamine Mili, “Communication Network Modeling and Simulation for Wide Area Measurement Applications” IEEE PES Conference on Innovative Smart Grid Technologies, Jan. 2012
5. Yi Deng, Shravan Garlapati, Hua Lin, Santhoshkumar Sambamoorthy, Sandeep Shukla, James Thorp, Lamine Mili, “Visual Integrated Application Development for Substation Automation Compliant with IEC 61850” PAC World Conference 2011, Dublin, Ireland, June 2011
6. H. Lin, S. Sambamoorthy, S. Shukla, L. Mili, J. Thorp, “GECO: Global Event-Driven Co-Simulation Framework for Interconnected Power System and Communication Network”. IEEE Transactions on Smart Grid, accepted, 2012
7. 1: Yi Deng; Hua Lin; Shukla, S.; Thorp, J.; Mili, L., "Co-simulating power systems and communication network for accurate modeling and simulation of PMU based wide area measurement systems using a global event scheduling technique," Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES), 2013 Workshop on , vol., no., pp.1,6, 20 May 2013

Thanks for your attention!

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