# Communication Infrastructure for the Smart Grid: A Co-Simulation Based Study on Techniques to Improve the Power Transmission System Functions with Efficient Data Networks

Hua Lin

Dissertation submitted to the Faculty of the
Virginia Polytechnic Institute and State University
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy
in
Computer Engineering

Sandeep Shukla
Lamine Mili
A. Lynn Abbott
Yaling Yang
Christian Wernz

September 27, 2012
Blacksburg, Virginia

Keywords: Co-Simulation, Wide Area Measurement System, Smart Grid, Remote Backup Relay, All-PMU State Estimation, Out-of-Step Protection

# Communication Infrastructure for the Smart Grid: A Co-Simulation Based Study on Techniques to Improve the Power Transmission System Functions with Efficient Data Networks

Hua Lin

(ABSTRACT)

The vision of the smart grid is predicated upon pervasive use of modern digital communication techniques in today's power system. As wide area measurements and control techniques are being developed and deployed for a more resilient power system, the role of communication networks is becoming prominent. Advanced communication infrastructure provides much wider system observability and enables globally optimal control schemes. Wide area measurement and monitoring with Phasor Measurement Units (PMUs) or Intelligent Electronic Devices (IED) is a growing trend in this context. However, the large amount of data collected by PMUs or IEDs needs to be transferred over the data network to control centers where real-time state estimation, protection, and control decisions are made. The volume and frequency of such data transfers, and real-time delivery requirements mandate that sufficient bandwidth and proper delay characteristics must be ensured for the correct operations. Power system dynamics get influenced by the underlying communication infrastructure. Therefore, extensive integration of power system and communication infrastructure mandates that the two systems be studied as a single distributed cyber-physical system.

This dissertation proposes a global event-driven co-simulation framework, which is termed as GECO, for interconnected power system and communication network. GECO can be used as a design pattern for hybrid system simulation with continuous/discrete sub-components. An implementation of GECO is achieved by integrating two software packages: PSLF and NS2 into the framework. Besides, this dissertation proposes and studies a set of power system applications which can be only properly evaluated on a co-simulation framework like GECO, namely communication-based distance relay protection, all-PMU state estimation and PMU-based out-of-step protection. All of them take advantage of interplays between the power grid and the communication infrastructure. The GECO experiments described in this dissertation not only show the efficacy of the GECO framework, but also provide experience on how to go about using GECO in smart grid planning activities.

# Contents

# List of Figures

# List of Tables

# Chapter 1

# Introduction

## 1.1 Background

The modern power system has advanced to the point where the system can no longer be operated without wide area control systems [4–6]. The advent of system infrastructure restructuring and the vision of the smart grid have further prompted the concomitant control systems to reach an unprecedented level of sophistication. It can be predicted that more state-of-the-art computational and communication techniques will be integrated into the power system to carry the control system from local to wide area scope. As a result, the power system will be operated and controlled with the help of an underlying communication network where large amount of information will be exchanged. For example, the power system equipped with high-bandwidth communication networks, complex digital processing is a growing trend as a way to improve the resilience and robustness of the transmission subsystem [7]. This new interdependent configuration of the power system and the communication network brings challenges which have not been seen before. The structure of the communication network to be laid out in the national power grid, the communication protocols to be used, the physical media, the distributed algorithms to make decisions on power system state and required control actions, the hierarchy of communication and control network, and many other issues remain unsettled to date. This mandates that we need power system and communication network co-simulation as opposed to only a stand-alone power grid simulator or a stand-alone network simulator. It is prudent that we take into account

these considerations during the design phase.

### 1.1.1 Demand for Co-Simulation Tools

A report prepared by the US Department of Homeland Security [8] advocates the need for a national power grid simulator. It is recommended that such a simulator should allow for modeling various possible disruptive events, studying interdependencies between the power grid and other critical infrastructures, and allow for planning and design of smarter capabilities of the national grid to enhance resilience, robustness, integration of renewable energy sources. Even though this report does not specifically deal with the embedded computational and communication capabilities envisioned for the future smart grid, there are already many efforts worldwide to enable various power grids to communicate data in real-time over wide areas, and use networked and distributed control to avoid various disastrous scenarios including blackouts, unwarranted generation shutdowns, unwarranted frequency excursions, inter-area oscillations, voltage instability, and so on.

If we can implement an effective, scalable and efficient power system and communication network co-simulator, we can design wide-area measurement and control schemes that have hitherto not been considered, and easily simulate its effectiveness and optimize the design and cost. For instance, PMU-based wide area measurement systems (WAMS) would have readily benefited from such a simulator [9]. However, there is a mismatch in the simulation models [10]: power system dynamic simulation uses time-driven methods while communication network simulation uses event-driven methods. These two simulation models must be seamlessly integrated to ensure a reliable synchronization in between.

### 1.1.2 Demand for System Interdependence Study

The infrastructure interdependence of the power system and the communication network may not be obvious [11]. In general, the communication devices need power feeder lines to deliver electrical energy to maintain their normal functions. In the case that a power outage happens, those devices can lose power or be temporarily switched to backup power supplies such as battery, flywheel, etc. If the power delivery can not be recovered on time, communication will be disconnected. On the other hand, WAMS applications highly rely

on the communication networks to collect system measurement data and distribute control decisions. In the case where a communication network outage happens, communication can be terminated or alternative channels can be built up or the WAMS applications can be turned back to the autonomous mode. If the power system and communication network are closely interconnected, in either outage case, the performance of the entire system is expected to be degraded.

Although the interdependence of the two individual systems is very crucial, currently there is no appropriate theoretical model for it. This is partially owing to the uniqueness and complexity of each individual system. Among all the related works, there are basically three ways to study the infrastructure interdependence. The first one is to simply study the communication network as a general network controlled system (NCS). The electrical properties of the power system are ignored. The focus of the study is to examine if the communication network can support a certain amount of data flows [7, 12, 13]. The second one is to study the power system and the communication network separately and sequentially. Examples are [14, 15]. In this case, the communication network is studied first either by theoretical modeling or running simulations. The communication characteristics are extracted and then integrated into the power system model as state variables or functional blocks. By tuning the variables or the blocks, the impacts of the communication network on the power system can be shown. The third method is to study the entire system as a hybrid system with subsystems using distinct models. It is introduced by [16, 17]. This method requires powerful software tools to model and simulate the power systems and communication networks together. But such kind of tools are not widely available. In this dissertation, the third method is favored because it gives the best modeling of the actual system.

The system interdependence also varies among different WAMS applications since every application requires unique interactions between the power system and the communication network. In this dissertation, we propose and study a set of WAMS applications which have distinct communication requirements. Thus, instead of giving unanimous solutions or conclusions, we study the system interdependence case by case based on co-simulation results.

## 1.2 Contributions

In response to the demands for co-simulation tools and system interdependence study, this dissertation makes several contributions as follows:

### 1.2.1 Design of a GECO Framework for Reliable Power System and Communication Network Co-Simulation

This dissertation proposes a power system and communication network co-simulation framework called GECO. GECO stands for **G**lobal **E**vent-driven **Co**-simulation which can be seen as a universal design pattern for hybrid system co-simulation. This framework integrates two individual simulators, one for power system and one for communication network. GECO requires a global event queue to store the interleaved simulation events from power system simulation and communication network simulation respectively and the events are processed in chronological order. This framework has been proved to have reliable synchronization between two individual simulators and have better simulation fidelity than other solutions. This dissertation further implements the GECO framework by integrating two software packages: PSLF and NS2. The co-simulation platform enables the study of a set of promising power system applications in which system interdependence is significant.

### 1.2.2 Study of a Communication-based Power System Remote Backup Relay Protection Scheme

This dissertation proposes a communication-based remote backup distance relay protection scheme for transmission subsystems. Traditional backup distance relays work in a time-delayed manner and may erroneously trip due to hidden failures [18]. The proposed protection scheme allows the relays to communicate with each other and coordinate the protection actions via a communication infrastructure. Communication gives relays better system visibility so that global optimal protection action can be achieved. Two modes of communication are integrated into the protection scheme: master-to-slave and peer-to-peer with pros and cons respectively. Then, the reliance on communication infrastructure of the

protection scheme is studied by running simulation cases on GECO.

### 1.2.3 Study of the Impact of Communication Infrastructure on All-PMU State Estimator

This dissertation studies the communication network impact and cyber attack vulnerability of the all-PMU state estimator for power system monitoring. All-PMU state estimator provides linear state estimation and much faster scanning rate than the traditional one. The amount of data collected by PMUs is large and they need to be transferred to regional and global phasor data centers. As a result, having sufficient bandwidth in the communication infrastructure as well as proper delay characteristics will matter in the correct operation of all-PMU state estimator. Therefore, the communication infrastructure of the all-PMU state estimator is studied on GECO using sensitivity analysis. Key network parameters are tuned to find the critical points of reliable power system monitoring. Furthermore, several network contingency scenarios which can be caused by cyber attacks or component failures are considered to stress test the all-PMU state estimator.

### 1.2.4 Study of a PMU-based Out-of-Step Protection Scheme

This dissertation proposes a PMU-based out-of-step protection scheme which intends to identify coherent generator groups and determine islanding locations in real time. Out-of-step protection schemes using PMUs have been discussed in [7, 19]. Properly deployed PMUs measure the rotor angles of the generators in the system and send the measurements to a central controller. Out-of-step condition can be identified by offline simulation and islanding locations are predetermined from simulation results. This dissertation proposes algorithms to identify the out-of-step condition using real-time measurements and determine the islanding locations based on identified coherent generator groups. This out-of-step protection scheme is validated preliminarily on GECO. For large scale power system where offline simulations are not sufficient or a chain of disturbances are placed in the system, the proposed out-of-step protection scheme gives a potential solution.

## 1.3 Dissertation Organization

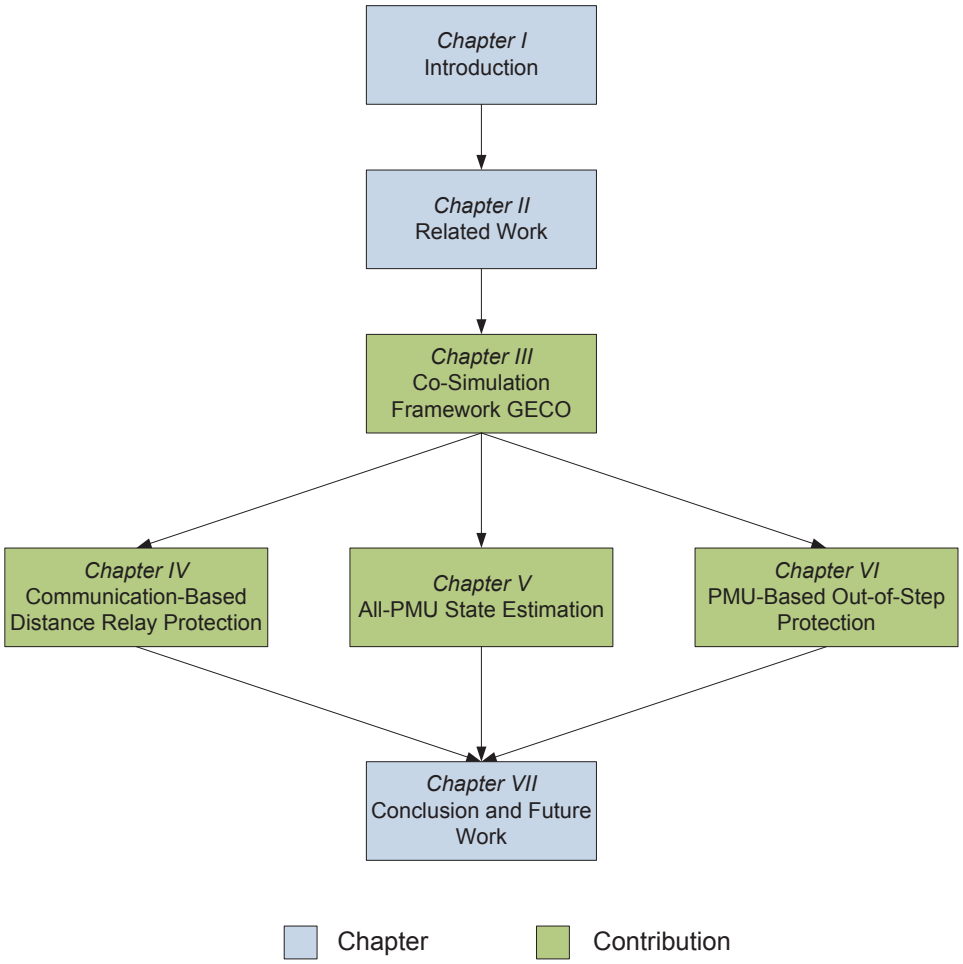


Figure 1.1: Dissertation organization

The organization of this dissertation is shown in Fig. 1.1: In Chapter 2, related works about the power system and communication network co-simulation tools and the relevant studies about the system interdependence are surveyed. Then, Chapter 3 proposes the global event-driven co-simulation framework GECO. The principle of GECO and its advantage over other solutions is shown. The implementation of the GECO framework lays the foundation for the following three chapters where each chapter represents a case study on GECO. Chapter 4 proposes the communication-based distance relay backup protection scheme. Chapter 5 studies the communication infrastructure impact on the all-PMU state estimator. Chapter 6 proposes a real-time PMU-based Out-of-Step protection scheme. Each one of the case studies

requires interplays between the power system and the communication network. The GECO framework helps the design and validation of these promising wide area measurement system applications. The dissertation is concluded and future research works are discussed in Chapter 7.

# Chapter 2

# Related Work

## 2.1 Co-Simulation of Power System and Communication Network

Co-simulation framework for heterogeneous systems which integrate different simulation models is not a rarity in academia [20–23]. There is great need in many research domains to combine different simulations together as a single co-simulation platform [24–30]. However, it is relatively new for communication-based power system applications. There has been some research on power system control analysis with consideration of communication networks [7, 13]. However, owing to the lack of proper modeling tools, the communication characteristics in their research have to be either largely simplified or strong assumptions have to be made [14]. Apparently, neither stand-alone power system simulation nor stand-alone communication network simulation is sufficient to precisely model a fully interconnected power system and communication network. As the restructuring of the power system grows, reliable co-simulation tools are expected to be system designers' favorite to study communication-based power system applications. Table. 2.1 summarizes some related works in this direction.

EPOCHS [16] pioneered the efforts to build a power system modeling tool with consideration of the underlying communication network. The EPOCHS approach is based on federated dynamic simulations which integrates sub-components under the high-level architecture (HLA)

Table 2.1: Comparison of co-simulation frameworks

| | Target | Components | Synchronization | Scalability | Real-time |
|---|---|---|---|---|---|
| EPOCHS[16] | Dynamic simulation for WAMS applications | PSCAD, PSLF, NS2 | Time-stepped | Good for large system | No |
| ADEVS[17] | Dynamic simulation for WAMS applications | Adevs, NS2 | DEVS | Limited, have to rewrite codes for different systems | No |
| Zhu et al.[15] | Dynamic simulation for WAMS applications | Simulink, OPNET | Not addressed | Medium size | No |
| VPNET[31] | Remotely controlled power devices | VTB, OPNET | Time-stepped | Limited to single or small number of power devices | No |
| PowerNet[32] | Remotely controlled power devices | Modelica, NS2 | Time-stepped | Limited to single or small number of power devices | No |
| Tong et al.[33] | General network controlled system | OPNET only, power system part is virtual | Delay estimation | Limited size due to virtual power system | No |
| Davis et al.[34] | SCADA cyber security, system visualization | PowerWorld, RINSE | N/A (static) | Good for large system | Yes, Partial |
| TASSCS[35] | SCADA cyber security, system visualization | PowerWorld, OPNET | N/A (static) | Good for large system | Yes, Partial |
| GECO | Dynamic simulation for WAMS applications | PSLF, NS2 | Global event-driven | Good for large system | No |

framework. Three off-the-shelf simulators: PSCAD/EMTDC for transient protection simulation, PSLF for power system stability simulation and NS2 for computer network modeling, are integrated together as a co-simulation platform. A carefully designed software mediator, called "runtime infrastructure" (RTI), is responsible for interfacing and synchronization between the individual simulators. RTI allows the simulators to exchange data periodically via itself. The synchronization algorithm used in EPOCHS is a simple "time-stepped" method. In this method, the individual simulators run independently but will halt at fixed points in time called synchronization points where information can be exchanged among simulators. After exchanging information, the simulators will restart the simulation themselves until the next synchronization point is reached. The simulators will repeat this "run-halt-exchange-restart" cycle until the simulation stop time is met. Basically, the user is free to set the time interval between the synchronization points. However, this synchronization method is not reliable. For example, if a certain system event, which requires interactions among simulators, occurs between the synchronization points, the event has to be buffered temporarily. The event cannot be processed until the next synchronization point. Therefore, simulation errors may be accumulated. In particular, if the WAMS application is latency-sensitive or if it requires extensive interactions between the power system and communication network,

the synchronization method may degrade the simulation fidelity. In that case, the users of EPOCHS will face a dilemma between precision and efficiency when they want to choose a proper synchronization interval.

A work similar to EPOCHS is reported in [17] trying to improve the synchronization method. In this approach, the power system is modeled using DEVS formalism and encapsulated in the *adves* software package. The communication network is modeled in NS2. Then the simulators are integrated under the DEVS framework [36]. Theoretically, this hybrid simulation environment gives better synchronization than EPOCHS since DEVS is suitable for both continuous system modeling and discrete-event system modeling. However, the DEVS package that has been used is designed for general discrete event system rather than power system simulations. Therefore, the users have to implement their own power system dynamic simulation code conforming to the DEVS specification. This customization may affect the reliability of power system simulation and the scalability of the system. Furthermore, since most commercial power system modeling and simulation tools are not DEVS-oriented, this simulation approach cannot be readily applied to other simulators.

In [15], an integration of MATLAB Simulink and OPNET is reported to study the impact of Information & Communication Technology(ICT) architecture on the reliability of WAMS applications. They use OPNET to simulate a detailed hierarchical ICT infrastructure which connects PMUs and PDCs. All the processes pertaining to phasor data measurement, collection and calculation are properly modeled in OPNET. The communication parameters are tuned to study the latency sensitivity of PMU-based applications. Critical operation point of the system can be found in this way. Although this paper presents an interesting approach that uses co-simulation of power system and communication network to study the system interdependence, the synchronization method in their framework and how the simulators are integrated have not been addressed.

In [31], an integration of Virtual Test Bed (VTB) software and OPNET called VPNET is introduced for simulating remotely controlled power electronic devices in the power system. The synchronization method used in this paper is similar to the EPOCHS's method. The co-simulation coordinator samples value periodically from both simulators based on a global simulation time step. Therefore, it accumulates the same kind of system errors as EPOCHS. Moreover, VTB is a software tool for simulating power electronics and energy systems, so it

may not scale well for large scale power systems. If there are only a few power devices of interest in the system, VPNET should be able to handle the simulation since the communication between devices may not be significant. Especially for the case study in this paper, the network infrastructure consists of only two nodes. However, if the power system is large, the limitation of VPNET will be prominent. A similar work called PowerNet is reported in [32] which integrates Modelica and NS2. The synchronization method and scalability feature are all the same.

An extension of OPNET to simulate wide-area communication networks in power system is proposed in [33]. In this framework, the power system dynamic simulation is simplified as a virtual demander. Whenever the demander requests to transmit data on the network, it suspends itself and creates a packet in OPNET. OPNET will simulate the total communication delay of this packet and report it back to the virtual demander. Then, the virtual demander will restart itself and continue to simulate a same amount of time as the communication delay received from OPNET. At this time, the virtual commander will process all the actions associated with the data packet. In this way, no synchronization errors will be accumulated. But this method is only suitable for one agent, one packet request scenario. If there are multiple agents in the system willing to transmit data within the same time period, this framework fails due to its single-threaded implementation. To simulate a complex hybrid system, alternative solutions are necessary. Other similar works are reported in [37–40].

Another category of co-simulation of power system and communication network is reported in [34] where a SCADA cyber security test bed is designed. The research focus of this test bed is to assess the vulnerability of the communication infrastructure of the power system against cyber attacks. This type of study is not latency-sensitive. Therefore, it does not require synchronization considerations between simulators. The test bed runs in a distributed manner on several computers. The power system is simulated in PowerWorld software on an individual server. There are also several computers called network clients which can read data from PowerWorld through a VPN network and a real-time network simulator RINSE. The network attacks can be generated and studied as part of network simulations and the power system dynamics is not a big concern here. A very similar SCADA cyber security test bed is proposed in [35] which integrates PowerWorld and OPNET.

Most of the works reported in Table. 2.1 involve the reuse of existing off-the-shelf software.

This is a natural choice since they are more reliable and scalable as long as they can be properly modified and customized. Rewriting new simulation engines from scratch is costly and time-consuming. Other possible options include software/hardware hybrid emulation environments or hardware testbeds. For example, since the scale of some SCADA systems is smaller than WAMS applications, it is possible to build emulation environments for SCADA testbeds. In [41, 42], a SCADA testbed PowerCyber using scale-down field devices to represent the real system is documented. However, our co-simulation framework aims at the modeling and simulation for the wide area power system monitoring, protection and control schemes. Building hardware emulation system at the national level is prohibitively expensive. Even if it is possible to make assumptions to scale down the system, the fidelity of the emulation cannot be guaranteed. For example, the communication infrastructure dedicated to the power system could be isolated from other overwhelming networks such as Internet. The communication topology, protocols, routing scheme and background traffic at different levels can be significantly different.

Another attractive solution is to use real-time simulators. Real Time Digital Simulator (RTDS) is a well-known real-time power system simulator which is capable of performing closed loop testing of devices [43–45]. RTDS simulation related to IEC 61850 communication has been reported in [46]. However, the scale of the hardware in the closed loop is limited to local scope. Deploying RTDS simulation on a large-scale distributed network is difficult. Therefore, integrating another real-time communication network simulator with RTDS will be a better option. But real-time simulators allowing open access are always rare so that this kind of real-time co-simulation implementation has not been published. Synchronizing two real-time simulators is also a challenging problem as both simulators need to be synchronized to real world clock. This requires that a real-time simulation coordinator be designed to exchange information between the simulators. Nevertheless, it is expected that real-time co-simulation platform will draw more interest in the future.

## 2.2 System Interdependence Study

As mentioned in Section 1.1.2, there are mainly three approaches to study the system interdependence of interconnected power system and communication network. All the research

work described in Section 2.1 use the third approach. In this section, additional research works on system interdependence study will be presented.

Some research uses the first approach mentioned in Section 1.1.2 to study the communication infrastructure for future power systems. In [12], Xie et al. study many power system disturbance reports from NERC and point out the importance of the IT infrastructure for a modern power system. Based on the analysis of the disturbance data, deficiencies of the legacy system are concluded as: lack of real-time system data, limited network facilities and low data bandwidth, frequent communication failure etc. [47]. Accordingly, a new conceptual IT infrastructure is proposed to improve the system performance across all the levels of the power system. The proposal brings in a lot of advanced computer techniques to the power system domain, although some of them are already popular in other network infrastructures like the Internet. In [48] Ericsson elucidates the requirements of the communication network for the power system. However, solutions to fulfill the requirements are not provided. Then in [7], a WAMS study with more communication details is reported. Current implementations of WAMS involve the deployment of PMUs all over the transmission network, promoting the construction of a communication infrastructure an urgent task. [7] proposes several promising WAMS applications which can benefit greatly from an advanced communication infrastructure. The WAMS applications are classified into three categories: monitoring, protection and control. For each WAMS application, the requirements of the network throughput and latencies are calculated and compared on the basis of the IEEE standard C37.118 [49]. This research provides fundamental guidance on how to design a sufficient communication network for future WAMS applications. Later in [13], a hypothetical WAMS network infrastructure is built in OPNET simulation software. The network represents a possible IT solution for PMUs in the Nordic region. Several configurations of wide-area network (WAN) and local-area network are combined to find an optimal solution. The simulation results shows the minimal requirements of the communication delays to support a WAMS in that area.

The second approach in Section 1.1.2 has also been reported in the literature. In [14], the communication latency impact on an inter-area mode damping scheme is studied. First, the communication delays in the system are estimated from four classical delay models. The total delay of a communication path in the system is calculated by summing up the delays of the sub-segments of the path. This estimation of delay is accurate only if there is no

background traffic on the network. Otherwise, the delays on different communication path are not independent from each other any more. The accuracy of the estimations cannot be guaranteed. Then, a control block which represents the contribution of this delay is attached to the remote input of the power system stabilizer (PSS). The simulation results show that the performance of PSS may degrade due to the communication delay. In [50], a similar approach is used to design an inter-area oscillation damping controller using a static var compensator. The controller receives measured signals from a remote location. The time delay of the signal transmission is assumed to be comparable to the time periods of the critical inter-area modes. Therefore, the delay is considered in the controller design. The controller is $H_\infty$-based and a unified Smith predictor (USP) approach is adopted. In this work, the time delay is assumed to be constant and the system performance is validated under different operation conditions. Later in [51], another similar work is proposed. This work not only consider the delay impact on a nonlinear robust integrated controller, but also consider the case when the measurements are not not complete. By running extensive simulations, the results show that the delay-oriented design shows "less settling time, swing times, oscillatory peak value and more critical clear time and better voltage stability performance" than the conventional ones [51].

As for the third approach in Section 1.1.2, other than the works introduced in Section 2.1, there are also many productive research works using EPOCHS as their simulation foundation [52]. In [53], a communication protocol used for substation automation is studied. Hopkinson et al. study the future trend of utility communication infrastructure from the Quality-of-Service point of view in [54]. Coates et al. propose a trust system to improve the cyber security aspect of the SCADA system in [55]. In [56], Giovanini et al. propose a primary and backup protection scheme using wide area relay agents. The agents can cooperate proper protection action via open protocol even if communication fails. The protection scheme is formally studied in [57]. Other similar communication-based relay protection are listed in [39, 58–62] although they are not supported or validated on a co-simulation platform. In [63], a global special protection system is proposed to maintain system stability after contingency. There are agents attached to power system components in the system such as generators and loads. Their roles are to properly reject power generations or shed load consumption when necessary. Their actions are coordinated by a central controller who monitors the system status and assigns control quotas.

To design a new WAMS-based power system application, it is important to know which approach mentioned in Section 1.1.2 should be used in the very beginning. It depends on many factors. But in general, the first approach is suitable for applications with no feedbacks from the power system. One example is power system monitoring. The second approach is suitable for applications where the communication is simple and point-to-point. The third approach is suitable for more general and complicated cases. In this dissertation, we are aiming at WAMS applications which require significant interplays between the power system and the communication network. Therefore, the third approach is favored.

# Chapter 3

# Co-Simulation Framework GECO

The key issue of the design of the power system and communication network co-simulation framework is that it has to accurately synchronize the simulation time in two distinct simulation models. The power system simulation usually uses time-driven method while the communication network simulation usually uses event-driven method. In this chapter, the simulation techniques for power system and communication network will be briefly reviewed. Then, the co-simulation framework will be proposed based on the foundation of the analysis of these simulation techniques and other co-simulation frameworks like EPOCHS.

## 3.1 Power System Dynamic Simulation

Power system dynamic simulation is commonly modeled as a time-driven or continuous-time system simulation. In a time-driven system, the system dynamics are represented by a set of differential equations in which the transitions between continuous state variables are defined. For simple cases, the differential equations can be solved analytically to get closed form solutions. However in most cases such closed form solutions are not available. Instead, numerical algorithms are used for general cases. Usually, the differential equations are discretized and the time base is divided into small steps. The next system state is derived from current system state. Then, the small variations of the state variables are integrated to approximate the system trajectory. The discretized time step is often very small so that the system variables do not have an abrupt transition within the time step.The discretization

and integration process can be represented as:

$$S(t_0) = S_0$$

$$\Delta S_n = F(S_n, X_n, \Delta t_n)$$

$$Y_n = G(S_n, X_n, \Delta t_n)$$

$$S_{n+1} = S_n + \Delta S_n$$

$$t_{n+1} = t_n + \delta t_n$$

where $S$ stands for system state variables; $S_n$ denotes the $n$th sample of $S$ at time $t_n$; $\Delta t_n$ denotes the $n$th time step; $\Delta S_n$ denotes the variations of the state variables at time $t_n$; $X$ denotes the system input variables and $Y$ denotes the system output variables; $F$ denotes the set of differential equations and in the end $G$ denotes the system output functions.

An example of this numerical algorithm for power system dynamic simulation is illustrated in Fig. 3.1. The system is initialized by executing power flow calculations which provide initial system state values. Next, the simulation enters a loop which represents the main body of the algorithm. Within this loop, the network boundary variables for dynamic models connected directly to the system network are calculated. Then, the secondary variables of dynamic models are calculated from system state variables. An iteration in this loop is completed by calculating state variable derivatives. At this point, the system time is advanced by a preset time step or a time calculated from the current system state. The loop is repeated until the simulation reaches the stop time or the system reaches a certain state. Alternatively, the simulation loop can be expanded on a timeline axis as depicted in Fig. 3.1 for better illustration. The algorithm flow is actually a sequence of discrete iteration rounds on the timeline with small time intervals in between. This sequence shows that a time-driven system in fact is numerically solved in a discrete manner.

## 3.2 Communication Network Simulation

Communication network simulations are usually performed using a discrete event-driven method. Discrete event-driven simulation is suitable for systems whose state is only subject to change due to discrete events. The occurrences of events are usually unevenly distributed

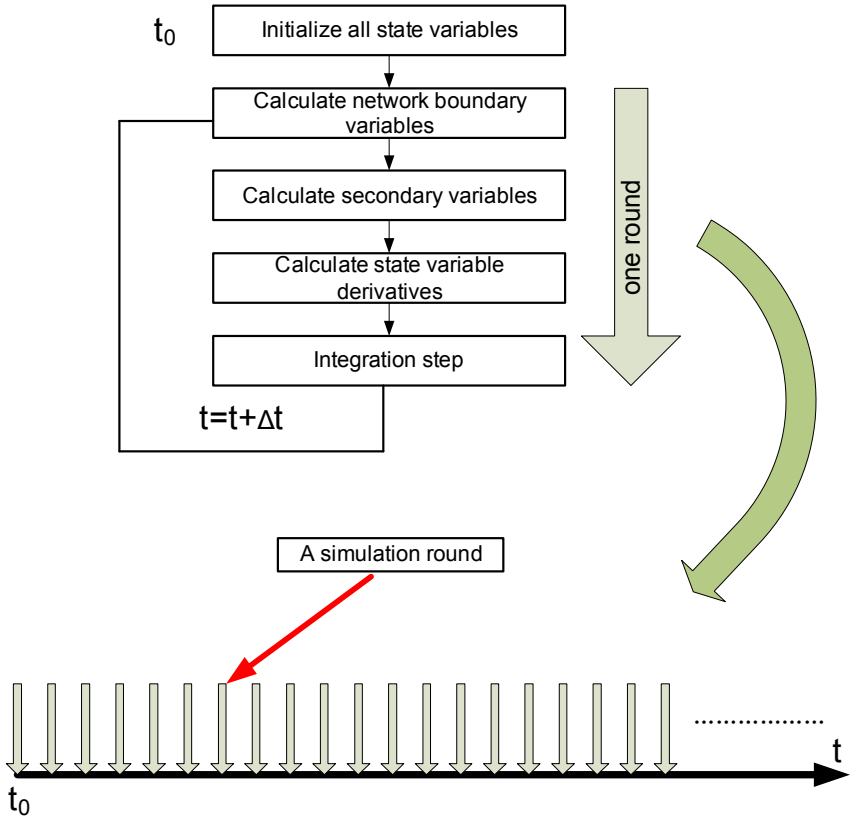


Figure 3.1: Example of the power system dynamic simulation

with respect to time. Time discretization into small time intervals as done in continuous time systems cannot be appropriately applied to discrete event systems since the time step is difficult to select. If the time step is selected too small then it will waste simulation times since system state remains unchanged during many consecutive time steps. If the time step is selected too long, then many events could be missed during a single time step. Instead, in discrete event-driven simulation, the system time directly hops between events. An event scheduler is usually designed to record current system time and process the events in an event list. The event list stores system events with time-stamps in a chronological sequence. This event list can be implemented as a priority queue, an array or a list [10]. The scheduler initializes the system state and the event list in the beginning of the simulation. When the simulation starts, the scheduler processes the event on top of the event list and handles the relevant actions. Then the scheduler adjusts the system time directly to the time of the next event in the list. The entire simulation stops when the system time reaches the stop time or

the system reaches a certain state such as there is no more event in the event list.

Fig. 3.2 shows an example of a communication network simulation that uses event-driven method. When the simulation starts, node 1 sends a packet to node 4 via node 2. The first event in the list should be "node 1 sends a packet to node 2" with an inital timestamp. A receiving event by node 2 is predicted based on the communication link properties. Then the second event "node 2 receives a packet from node 1" will be created and placed in the event list. When the second event is processed, a third event will be created as "nod 2 sends a packet to node4". The occurrence time of the third event can be estimated from the node model and the routing protocol. The network simulation will continue this way until the ending criteria is satisfied.

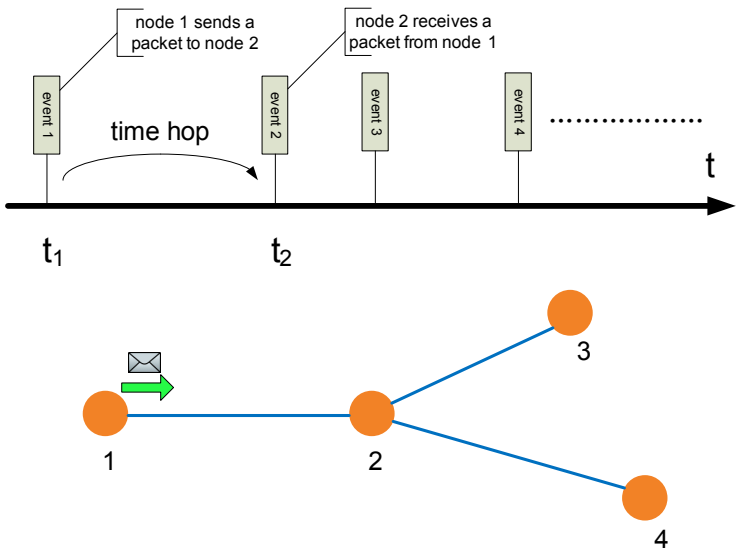


Figure 3.2: Example of the communication network simulation

## 3.3 Co-Simulation Framework GECO

Since the simulation techniques for power system and communication network are different, synchronization mechanism between them is the most crucial issue leading to a successful co-simulation design. An intuitive method is using explicit time-stepped synchronization which is adopted in [16]. This framework is shown in Fig. 3.3. In this method, several syn-

chronization points are predefined. In Fig. 3.3, the top time axis represents the power system dynamic simulation process and the bottom time axis represents the communication network simulation process. When the co-simulation starts, two processes run independently until both of them reach a synchronization point, as denoted by dashed vertical lines in Fig. 3.3. It is the point where two processes suspend the running themselves and start to exchange information. Typical information exchanged includes sending measurements data to the communication network or actuators in the power system receiving remote control commands from the communication network. After the information is exchanged, two processes will restart themselves until the next synchronization point.

This simple synchronization method can easily bring in simulation errors. If an event that requests interaction between the two processes occurs between the synchronization points, it has to be buffered temporarily and wait until the next synchronization point to be processed. If the power system simulation time step is steady, there will be same number of simulation rounds between synchronization points. But there can be any number of network events between synchronization points since they are unevenly distributed. Then, if there is a fault that occurs in the power system between two synchronization points, the power system simulator can not deal with it right away but has to wait to take action. This is indicated by "Error 1" in Fig. 3.3. On the other hand, if a control message is received by a software agent in the network process, it has to wait as well until the next synchronization point to apply it in the power system. This is indicated by "Error 2" in Fig. 3.3. These errors create unwanted time delays in the simulation but they do not exist in a real system. Therefore, the synchronization method used in [16] may accumulate simulation errors over time. Theoretically, each error can be as large as one synchronization time step.

The root of this problem owes to the difficulty to select proper synchronization points. A new co-simulation framework called GECO (**G**lobal **E**vent-driven **Co**-simulation) is accordingly proposed which avoids these synchronization errors. Our co-simulation runs globally in a discrete event driven manner as shown in Fig. 3.4. Since the power system dynamic simulation is in fact solved in discrete manner as shown in Fig. 3.1, each of the iteration rounds is treated as a special discrete event in this framework. A global event scheduler is designed as the global time reference and co-simulation coordinator. A global event list is also prepared by interleaving the power system iteration events with other communication network events according to their timestamps. Therefore, only one event is allowed to be

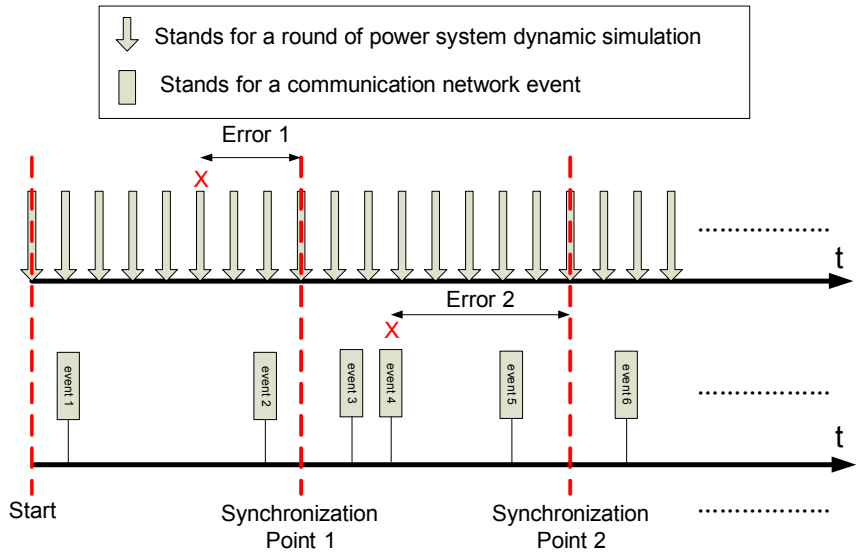


Figure 3.3: Synchronization with errors

processed at the same time. This is illustrated by the single time axis in Fig. 3.1. The global scheduler checks the global event list to identify if the next event is a power system simulation event or a communication network event and yields the control accordingly. More importantly, the simulation processes can suspend themselves after handling each event and yield the control back to the global scheduler. In this way, whenever there is an event that requests interaction, it can be processed immediately by the global scheduler without unnecessary time delay. Both errors in Fig. 3.3 are eliminated in this framework. Therefore the GECO framework has reliable synchronization between the power system simulation and the communication network simulation and has better simulation fidelity than other related works.

## 3.4 Co-Simulation Formalism

It is necessary to show that our global even-driven co-simulation framework does not undermine the simulation integrity in each of the individual simulator since all the events are mixed up. In this subsection, we will verify it using a formal approach. Discrete Event System Specifications (DEVS) is a popular formalism to model and analyze general discrete

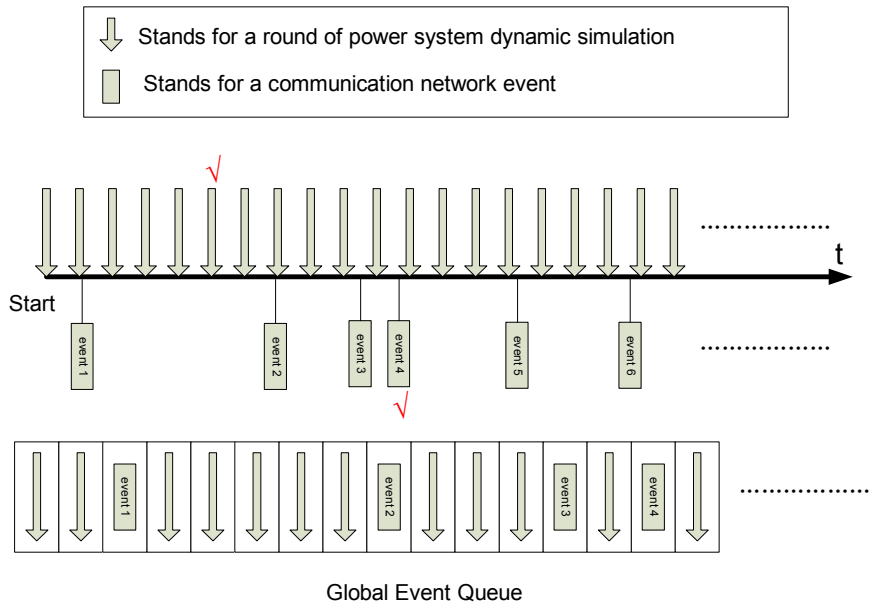


Figure 3.4: Event-driven synchronization without errors

event systems. There are also many other equivalent formalisms but DEVS is more suitable for this co-simulation framework. It is defined as a 7-tuple [36]:

$$M =< X, Y, S, ta, \delta_{int}, \delta_{ext}, \lambda > \tag{3.1}$$

where:
$X$ is the set of input events;
$Y$ is the set of output events;
$S$ is the set of system partial states;
$ta : S \rightarrow T^{\infty}$ is the lifespan function of the partial state;
$\delta_{int} : S \rightarrow S$ is the internal transition function;
$\delta_{ext} : Q \times X \rightarrow S$ is the external transition function;
$\lambda : S \rightarrow Y$ is the output function;
$Q = \{(s, e) \mid s \in S, e \in (T \bigcap [0, ta(s)])\}$ is the set of total states;
$e$ is the time elapsed since last transition;
$T = [0, \infty), T^{\infty} = [0, \infty]$.

The interpretation of (3.1) for a communication network simulation is straightforward where $X, Y$ are the system input/output; $S$ is the system state when a certain discrete event is being processed; $ta$ represents the time delay between the current event and the next event

in the event list. $\delta_{int}$ stands for the relevant processes associated with an event where $\delta_{ext}$ stands for the impact of the input to the system state. Event-driven simulation is commonly used for the system which can be modeled by DEVS.

It has also been shown that the power system dynamic simulation can be modeled by DEVS [17]. For this particular case, $S$ is the set of system state variables (voltage, current, etc.) after each iteration round, $ta$ represents the iteration time step and $\delta_{int}$ stands for the system change after the integration of each time step.

The co-simulation framework in fact couples the power system and communication network together. That is, the output event of the power system simulation is the input event of the communication network simulation and vice versa. From the DEVS formalism point of view, these two atomic DEVS systems actually form a coupled-DEVS which is another 7-tuple [36]:

$$N =< X, Y, D, \{M_i \mid i \in D\}, EIC, ITC, EOC, Select > \tag{3.2}$$

where:
$X$ is the set of input events;
$Y$ is the set of output events;
$D$ is the name set of sub-components;
$\{M_i\}$ is the set of DEVSs that form the coupled-DEVS;
$EIC \subseteq X \times \bigcup_{i \in D} X_i$ is the set of external input couplings;
$ITC \subseteq \bigcup_{i \in D} Y_i \times \bigcup_{i \in D} X_i$ is the set of internal couplings;
$EOC \subseteq \bigcup_{i \in D} Y_i \times Y$ is the set of external output couplings;
$Select$ is a tie-breaker function for time conflict of events.

The couplings define how the atomic DEVSs are connected to form a coupled-DEVS. For the co-simulation framework, $D$ denotes $\{P, C\}$ which represents power system and communication network respectively. $M_p, M_c$ denotes the DEVS models for them. $EIC$ and $EOC$ denotes both empty and $ITC$ denotes $(Y_p, X_c) \cup (Y_c, X_p)$.

It has been proved that DEVS is closed under coupling which means a coupled-DEVS $N$ is equivalent to a DEVS $M'$. The proof can be done by construction [36] where:
$X_{M'} = X_N$;
$X_{M'} = X_N$;
$S_{M'} = \times_{i \in D} Q_i$ ($Q_i$ is the total state set of each component);

$ta_{M'}(S_{M'}) = min\{ta_i(S_i) - e_i | i \in D\}$;
$\delta_{ext_{M'}} = (\ldots, (s_i, e_i), \ldots)$ when $EIC$ is empty;
$\delta_{int_{M'}} = (\ldots, \delta_{ext_i}, \ldots)$ if it is an internal coupling or
$\delta_{int_{M'}} = (\ldots, (s_i, e_i), \ldots)$ for other cases;
$\lambda_{M'} = EOC(\lambda_i(s_i))$.

The new $ta_{M'}$ is the lifespan of the new partial state considering that event from other DEVSs can potentially reduce its own original lifespan. This equivalent DEVS $M'$ can also be simulated using event-driven method. Therefore, the integrity of the individual simulators still holds under our co-simulation framework. The proof also indicates that global event-driven simulation is an effective approach for the interconnected power system and communication network.

## 3.5 Co-Simulation Implementation

The co-simulation framework GECO is implemented by carefully integrating two individual simulators: namely GE's Positive Sequence Load Flow (PSLF) and Network Simulator 2 (NS2). The integration involves major modifications and extensions on both parts. The simulators we choose are the same with EPOCHS [16], but our internal design is different and the difference will be shown in later chapters through comparison of simulation results.

PSLF is a power system simulator designed by GE which provides both steady-state and dynamic power system simulations capabilities. PSLF is able to simulate a system with up to 60,000 buses and is equipped with a rich library of power system dynamic models. The software is written in Java and provides numerous APIs via a script language called EPCL for customized extensions. User-defined models written in EPCL can be integrated into the existing software package. EPCL can also access the runtime simulation data and change the simulation settings as needed. Although PSLF is not an open-source software, its design feature enables users to build flexible extensions.

NS2 is a well-known communication network simulator aiming at the evaluation of network protocols' performance. It is open-source and is widely used in networking research domain. NS2 is a general discrete event simulator with a rich library of network models which covers

four protocol layers except the physical layer in the network reference model. The core of NS2 consists of a set of complex subroutines written in C++. Therefore a script language called Object Tcl (OTcl) is provided to users for easier simulation configuration and reuse. A framework called "OTcl linkage" links the OTcl codes to C++ codes implemented in the background. Flexibility and efficiency of the simulation is balanced in this framework. Since NS2 is open-source, users is free to add new network protocols or models in C++ and configure them in OTcl with a proper mapping.

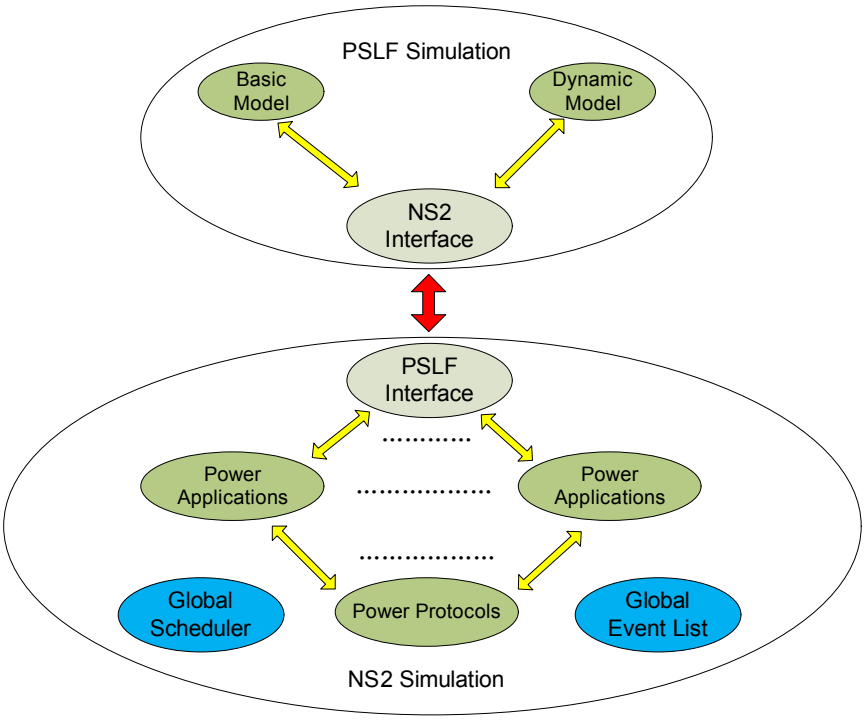


Figure 3.5: The structure of the co-simulation implementation

Fig. 3.5 shows the structure of our co-simulation framework implementation. The global scheduler and global event list are derived directly from the scheduler and the event list used in NS2. Therefore, the co-simulation is controlled by a customized component in NS2. A bi-directional interface is designed connecting PSLF and NS2 to exchange information in between.

On the PSLF side, a dummy dynamic model "epcmod" is added to the power system. It only works as an interface to NS2 and does not affect the power system dynamics. In every power system iteration round, this model updates all the power system data for NS2 and

receives feedbacks from NS2 to change the simulation settings or the topology of the power system accordingly. After every power system iteration round, it is also able to suspend the PSLF simulation, yield the control to the global scheduler and wait for the command to run the next round.

On the NS2 side, a new C++ class "tcl_PSLF" is created to coordinate the simulations of PSLF and NS2 itself. This customized class is independent from all the other networking classes and it is compiled together with other components in NS2. When the co-simulation starts, this class pre-allocates a sequence of power system iteration rounds in the global event list. This step is virtully realized by the Tcl codes in Fig. 3.6. When a power system iteration round needs to be processed, it sends a command to PSLF to restart the suspended simulation. Potential communication-based power system applications are designed in NS2. The power system application classes are usually derived from the class "Application" in NS2. These classes model the functions of the software agents in the power devices such as digital relays, Phasor Measurement Units (PMUs) and Intelligent Electronic Devices (IEDs). The power system data updated from PSLF will be distributed to these classes for further analysis. The software agents are able to communicate with each other via the communication infrastructure in NS2 and control decisions are also made by some of them. The communication protocols used by the power system applications are variants of existing network protocols like UDP and TCP. Minor changes are applied to the UDP and TCP classes to enable them to carry power system data.

```
#Initialize power system integration events
set time 0.0
for {set i 0} {$i <= $round} {incr i} {
    $ns at $time "$pslf_iterate"
    set time [expr {$time+$timestep}]
}
```

Figure 3.6: Allocating power system integration events in the OTcl script

In the following chapters, several WAMS-based power system applications will be propoased as case studies on the co-simulation framework GECO, namely communication-based distance relay protection, all-PMU state estimation and PMU-based out-of-step protection.

The case studies will show a family of power system applications that can be only properly studied using a co-simulation framework like GECO. The co-simulation results can also show the system interdependence between the power system and the communication network and how to design a proper communication infrastructure for future power system applications using GECO.

# Chapter 4

# Communication-Based Distance Relay Backup Protection

Relays are widely deployed in the power system to protect the system from short circuit faults. There is a large variety of relays in service for different protection purposes. For example, on the transmission level, directional distance relays play the leading role to protect the transmission lines. The trend of relay protection is that digital relays which uses advanced microprocessor techniques are being used to gradually phase out traditional mechanical relays. However, the computation capability of current digital relays has not been fully utilized. In this chapter, a new backup relay protection scheme which non-intrusively makes use of the current infrastructure of digital distance relays and an underlying communication network will be introduced. The relays in this scheme communicate and coordinate with each other via the communication network to make global optimal protection decisions. Two communication modes will be covered: supervisory and ad-hoc. In the following sections, the principle of this scheme will be investigated in detail.

## 4.1 Background

Distance (impedance) relays are usually deployed on the transmission level of the power system. The operation of the distance protection relays is governed by the ratio of the

magnitudes of current and voltage (impedance) measured by the relay. When a short-circuit fault occurs, the measured impedance drops dramatically therefore revealing the fault. Also the measured impedance indicates the distance from the fault to the distance relay.

As shown in Fig. 4.1, it is a common practice to assign three protection zones for the distance relays. Zone 1 protection is the primary protection for each distance relay. It covers about 80% – 90% of the length of the first transmission line as shown in Fig. 4.1. Zone 2 protection covers a little bit longer than zone 1, extending beyond the adjacent bus which is about 120% of the length of the first transmission line. Zone 3 protection provides the longest coverage which includes the entire first transmission line and about 80% of the second transmission line. By properly adjusting zone 1, zone 2 and zone 3 settings, the distance relays can achieve overlapped primary and backup protection of the transmission lines. Usually zone 1 protection is the primary protection and it operates instantaneously if a fault is observed. Zone 2 and zone 3 protections are backups and they are operated with intentional time delays. It is common practice to use longer time delay for longer protection reach of the distance relays so that they can provide effective system protection without unnecessary tripping. The time delay can be as long as 1 second for zone 3 relays.

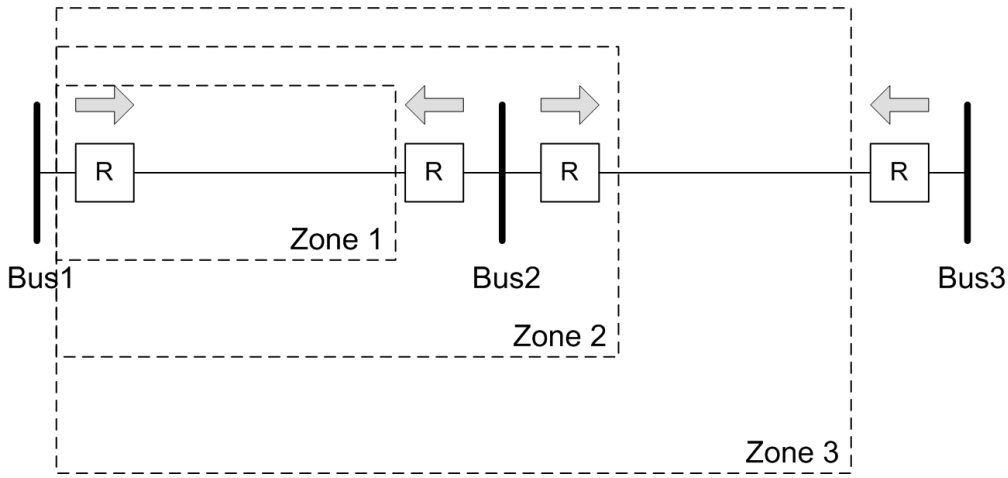


Figure 4.1: Distance relay protection zones

Fig. 4.2 shows the trip and block regions of the distance relays. The decision is made based on the measured impedance. The trip regions are usually three internal tangent circles. If the measured impedance falls in one of the circles, the corresponding protection action will be taken. The circles can be adjusted for different protection purposes.

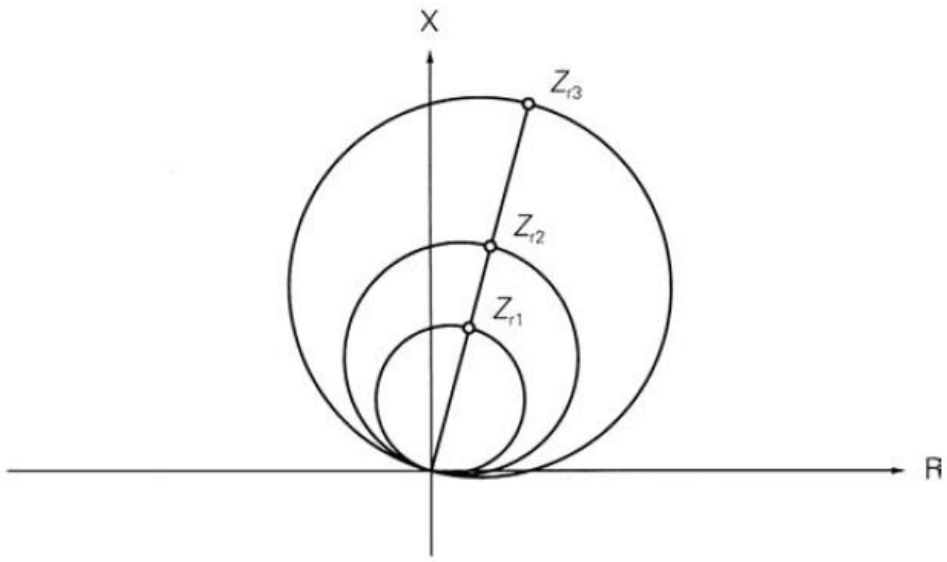


Figure 4.2: Distance relay trip and block regions [1]

## 4.2 Communication-Based Distance Relay Backup Protection

Although the transmission systems with protective relaying typically have the redundancy in the form of backup relays, it is reported that such a system still may suffer from different types of failures. For instance, zone 3 backup relays work in a time-delayed manner, the system may encounter instability issues during the delay. It is also known that zone 3 relays can actually erroneously trip or not trip due to hidden failures [64]. A hidden failure is usually rare but could happen due to software or hardware errors in zone 3 relays. It may go unidentified for a long time. However, such problems may manifest itself as extra sensitivity of a zone 3 relay to even remote line overloading. Even though such an overloading might be transient, or might not have reached a level where the zone 1 and zone 2 relays need to take action, an over active zone 3 relay may trip, starting a sequence of other trips which may lead to a cascading failure [65, 66]. New protection techniques are being sought out to solve this problem [39, 56, 58–62].

Accordingly a new communication-based distance relay backup protection scheme is introduced in this section that leverages the present distance relay protection infrastructure with

the addition of an underlying communication network. Modern microprocessor-based digital relays are more reliable and efficient than traditional electromechanical ones, thus it is possible to enhance them with software agents in order to design more elaborate protection schemes. If the distance relays can communicate with each other through their software agents then a coordinated protection scheme system can be formed. By virtue of extensive communication, new protection schemes could have faster backup relay protection and additional robustness to prevent false tripping. Based on the communication mode, two communication-based protection schemes are discussed: supervisory (master to slave) and ad-hoc (peer to peer).

### 4.2.1 Supervisory Protection

In the supervisory protection scheme, distance relays are interconnected as a network using a communication infrastructure and their functioning is coordinated through extensive communication. A central protection controller called "Master Agent" coordinates the operations of the digital relays in the system. Each distance relay has a software agent (Slave Agent) associated with it. This software agent works as an interface for information exchange between the Master and the corresponding distance relay. In this mode, the protection scheme system is able to provide more secure protection by avoiding hidden failure induced false tripping.

The primary protection for the distance relays remains the same as the traditional distance protection scheme, while the backup protection is different. In this scheme, when a backup relay sees zone 2 or zone 3 faults, instead of waiting for a pre-set time delay to trip, the relay proactively collects information from other relays to evaluate the status and make the decision. This procedure is done by communication between slave agents and the master agent. Firstly, the slave agent whose associated relay sees a remote fault submits a request to the master agent for decision. The master agent then asks other slave agents in the fault zone to see if others see the fault as well. Based on the feedback from other slave agents, the master agent sends the final decision to the original slave agents. The entire communication process in this scheme is shown in Fig. 4.3

Detailed operations of this master-slave mode supervisory protection scheme are shown in

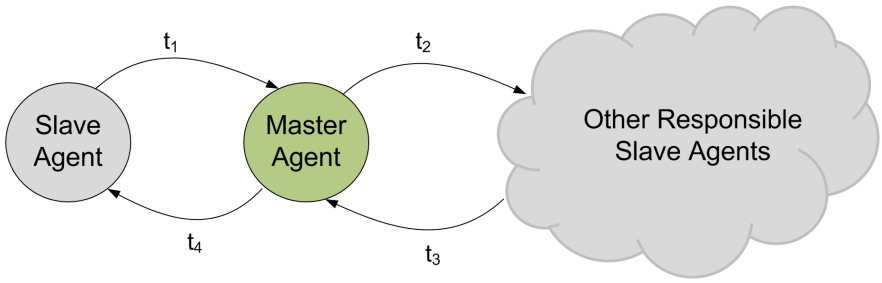


Figure 4.3: Supervisory protection communication

Fig. 4.4 and Fig. 4.5 using a finite state machine (FSM) representation. In the FSM, a circle represents a certain state. An arrow line represents a transition from one state to another. There is a fraction associated with each transition. The numerator position shows the event which causes the transition and the denominator position shows the action taken due to that event.

On the slave agent side, the relay starts from the "normal monitoring" state and keeps monitoring the transmission line. If a zone 1 (local) fault is observed the relay should trip the transmission line immediately. If a zone 2 or zone 3 fault (remote) is observed, the slave agent sends a decision request to the master agent and enters the "wait for decision" state. If the fault disappears during the wait state, the slave agent would go back to the normal state and block whatever decision received from the master agent since this condition indicates the fault may have been cleared by its own primary protection. If the fault persists and the slave agent receives a trip decision from the master agent, the relay should trip the line since the primary protection may have failed. If the slave agent receives a block decision from the master agent but still sees the fault, this indicates the relay may have a hidden failure or wrong setting. Then the slave agent should put the relay out of service and call for maintenance. In this manner, the slave agents can both expedite the backup protection and prevent hidden failure induced false tripping.

On the master agent side, when it receives a decision request from a slave agent, it enters the "processing decision request" state. A group of relays which are entrusted with the fault area are selected and queried by the master agent. When the software agents of the selected relays receive the queries, no matter which state they are in, they should report if they see a fault back to the master agent. The master agent will try to make the final decision when it receives a feedback. As long as a final decision could be made, the master should send it

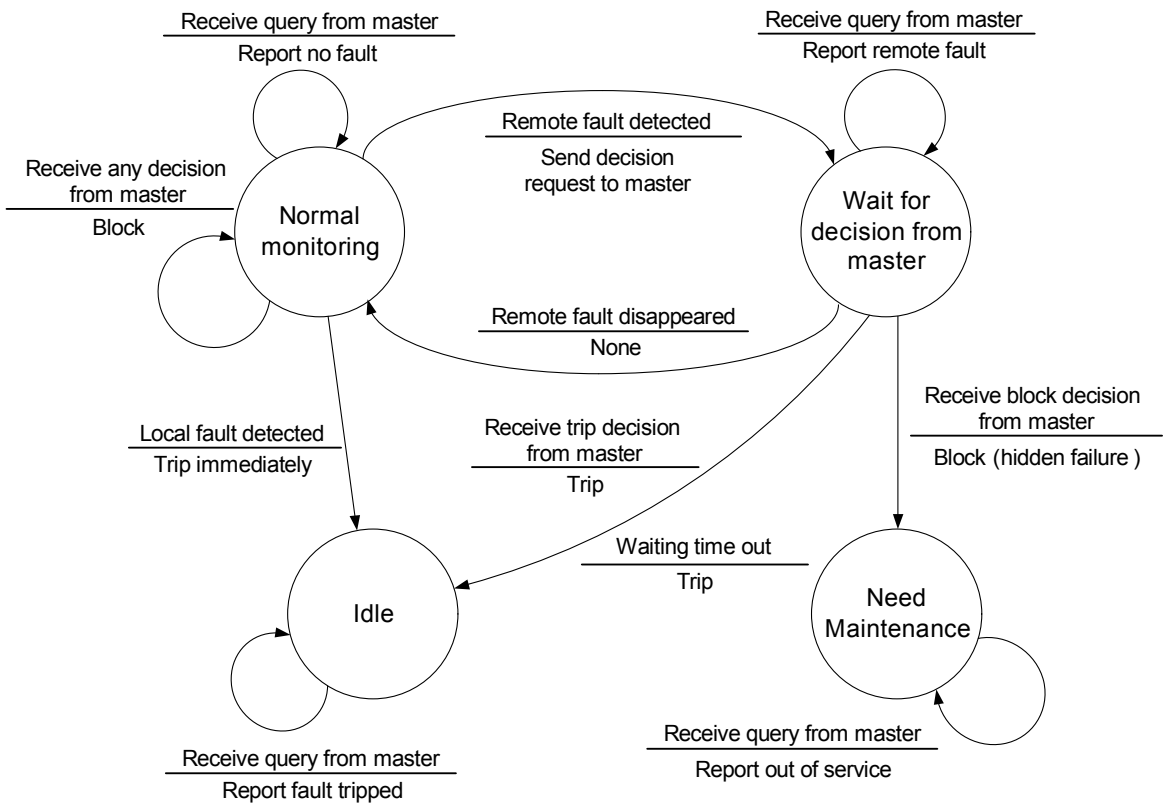


Figure 4.4: FSM of supervisory protection: slave agent

to the original slave agent to take action. Fig. 4.5 only shows the master agent operation for one slave agent. Actually, when a fault happens in the system, multiple slave agents could send request to the master agent. Therefore, the master agent should be a multi-threaded program which can handle all the requests simultaneously.

Although there is extensive communication, the total communication time could still be shorter than the traditional time delay settings for the zone 2 or zone 3 protections. However, the time delay associated with zone 2 or zone 3 should not be eliminated since the network itself may fail. Either link failure or traffic congestion may significantly increase the communication delay or even result in messages dropping. Hence if the communication-based protection cannot complete within a certain time, the relays would revert to the traditional distance protection mode as shown in Fig. 4.4.

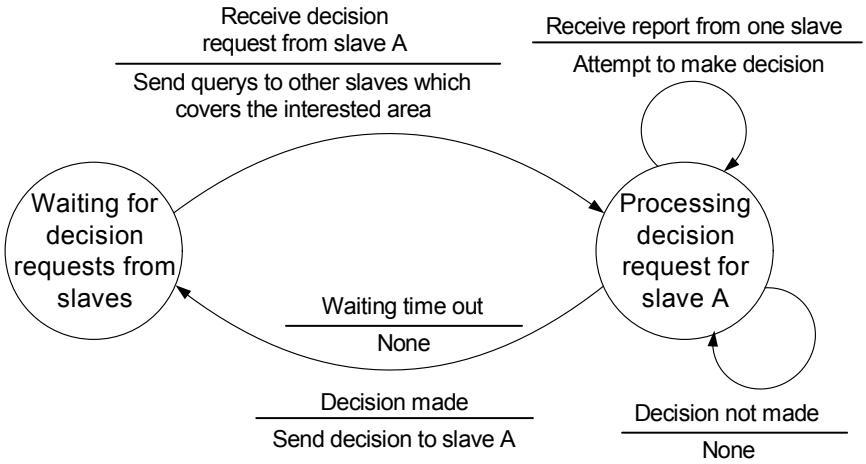


Figure 4.5: FSM of supervisory protection: master agent

### 4.2.2 Ad-hoc Protection

In the supervisory protection scheme, the master agent is the most crucial component since it coordinates all the slave agents. If the master agent fails, the entire protection scheme fails. Another issue of the supervisory scheme is that the slave agents always communicate with the master agent. This could lead to long and unstable communication times, depending on how far the slave agent is from the master agent. In order to overcome these difficulties, an ad-hoc protection scheme is considered. In this scheme, the master agent is removed and its functions are duplicated in every slave agents. Now, the slave agents can directly communicate with each other in a peer-to-peer manner as shown in Fig. 4.6.

Fig. 4.7 shows the FSM representation of the ad-hoc protection operations. The only type of agent in this scheme is the peer agent. Each peer agent actually combines the operations of the slave agent and the master agent. The main difference is that when a peer agent sees a remote fault, it queries other peer agents in its zone directly. On receiving a report from other peer agents, the peer agent makes the decision on its own. Hence, this is a fully distributed and autonomous application based on ad-hoc communication.

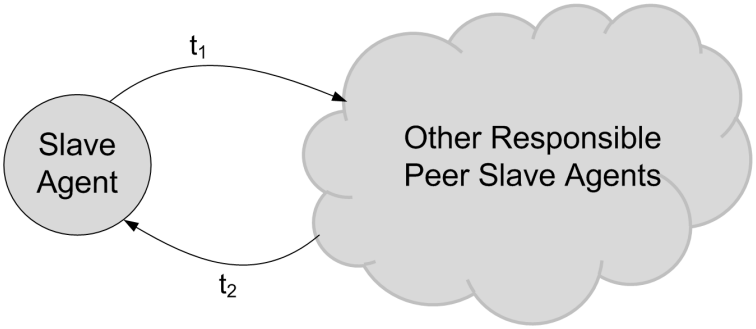


Figure 4.6: Ad-hoc protection communication

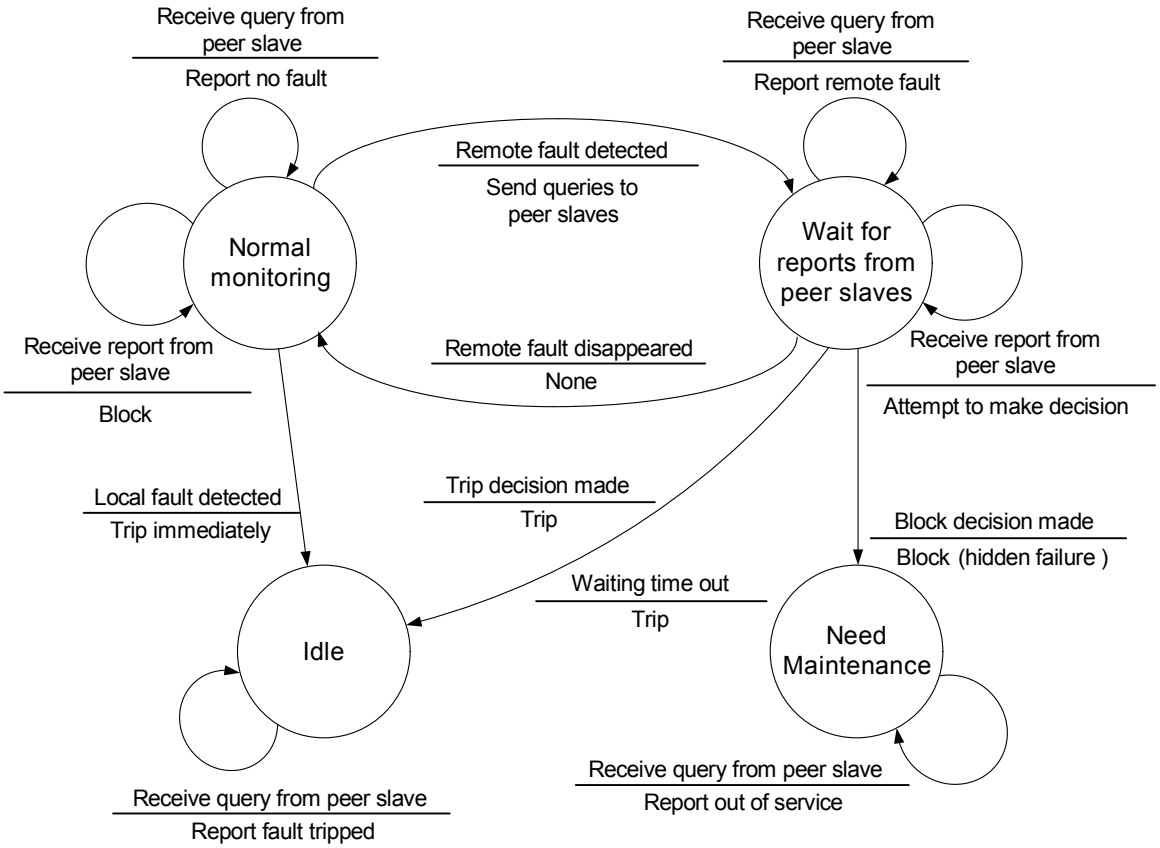


Figure 4.7: FSM of ad-hoc protection

### 4.2.3 Relay Searching and Decision Making

In both protection schemes, a relay search procedure is required for the agents to determine the responsible relay group when a fault is observed. A relay searching algorithm is imple-

mented on a graph abstraction of the power system topology. The step-by-step instruction of this algorithm is shown in Fig. 4.8. The power system topology is represented by an undirected graph $G(V, E)$. All the transmission lines are represented by edges and the buses connecting to transmission lines are represented by vertices. The relay in this graph can be represented by an ordered pair $((m, n), m)$, which means the relay locates at the side of bus $m$ of the transmission line $(m, n)$. The algorithm basically consists of two major steps. First, based on the relay that submits the decision request, the algorithm finds out the possible faulted lines. Then, for each possible faulted line, the algorithm finds out two primary protection relays and all the backup relays for this line.

---

**Algorithm**

---

**Input:** A modified undirected system graph $G(V, E)$; A relay represented by $((m, n), m)$

**Output:** A relay set $R$

**Steps:**

1. Find the possible faulted lines set $L$: for each edge $(u, v) \in E$ except $(m, n)$, if $n = u$ or $n = v$, add $(u, v)$ to $L$
2. Find the responsible relays for each line in $L$:
   a. For each $(u', v') \in L$, add $((u', v'), u')$ and $((u', v'), v')$ to $R$
   b. If $n = u'$, for each edge $(u'', v'') \in E$ except $(u', v')$, if $v' = u''$ add $((u'', v''), v'')$ to $R$, if $v' = v''$ add $((u'', v''), u'')$ to $R$
   c. If $n = v'$, for each edge $(u'', v'') \in E$ except $(u', v')$, if $u' = u''$ add $((u'', v''), v'')$ to $R$, if $u' = v''$ add $((u'', v''), u'')$ to $R$

---

Figure 4.8: The relay searching algorithm

An example is presented here to better illustrate this algorithm. This algorithm is implemented for the New England 39-bus system as shown in Fig. 4.9. It is assumed that there is a fault on transmission line $(4, 14)$ and its backup protection relay $((14, 15), 15)$ senses the

fault. We then find all the responsible relays for relay $((14, 15), 15)$ following the steps in Fig. 4.8. In step 1, we can find all the lines connected to bus 14 except $(14, 15)$ where we get lines $(4, 14)$ and $(13, 14)$. These two lines are all possible faulted lines although the real fault should be located at only one line. Then within step 2, for line $(4, 14)$, in step 2.a we find its primary protection relays $((4, 14), 4)$ and $((4, 14), 14)$. Next, in step 2.b or 2.c we find all the lines connected to bus 4 except $(4, 14)$ which are $(3, 4)$ and $(4, 5)$ and then find out the backup protection relays $((3, 4), 3)$ and $((4, 5), 5)$. For line $(13, 14)$, following the similar steps we find the final relay set for $((14, 15), 15)$, which are $((4, 14), 4)$, $((4, 14), 14)$, $((3, 4), 3)$, $((4, 5), 5)$, $((13, 14), 13)$, $((13, 14), 14)$ and $((10, 13), 10)$.

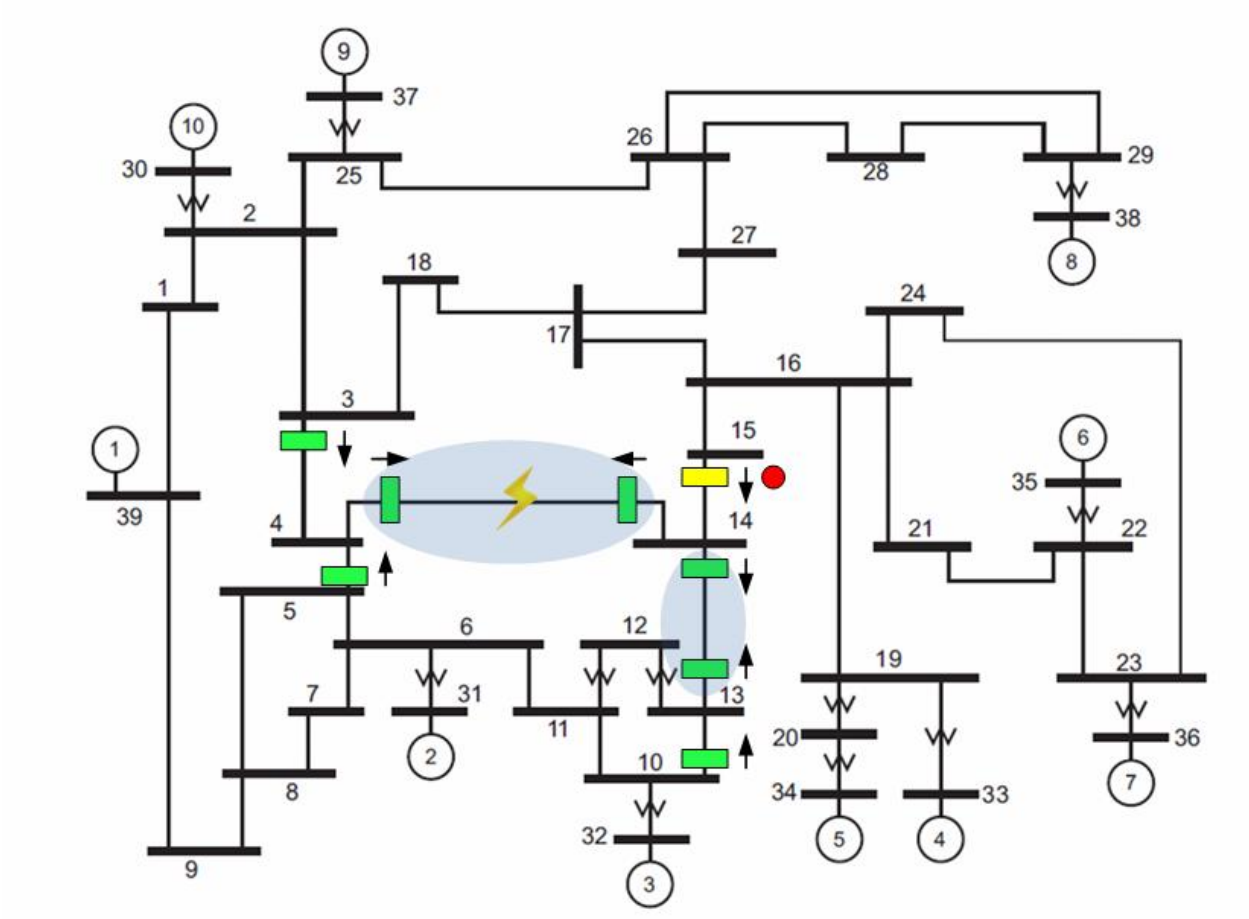


Figure 4.9: Relay searching on 39-bus system [2]

As long as the responsible relay group is determined, the protection decision will be made based on the feedbacks from this group. Since relay protection is a time-critical application,

a simple but effective decision making method is applied to the agents. The decision is made based on the feedbacks from the slave agents or the peer agents, which are selected using the relay searching algorithm. Based on the FSM in Fig. 4.4, 4.5 and 4.7 there are totally four types of feedback reports that can be received from the agents: "remote fault", "no fault", "fault tripped" and "out of service". Note that there is no "local fault" feedback report because if the primary protection relay works normally, a local fault should be tripped immediately. Our decision making works as follows:

a. If the agent receives a "remote fault" report, the trip decision can be made immediately. Since the possibility of two relays have hidden failure simultaneously is very low, there is no need to keep waiting for other reports in this condition.

b. If the agent receives a "no fault" report, it should first check if all the relays in the responsible relay set have reported back. If so the block decision can be made because none of other relays see a fault implying a potential hidden failure. Otherwise, the agent should keep waiting for other reports.

c. If the agent receives a "fault tripped" report, no decision should be made. But the agent should remove this reporting relay from the responsible relay set since this report won't affect the decision any more.

d. If the agent receives an "out of service" report, no decision should be made and the reporting relay should also be removed as well.

## 4.3 Co-Simulation on GECO

In this section, the proposed communication-based distance relay backup protection schemes will be studied in detail on GECO. The protection schemes are applied to the New England 39-bus system as shown in Fig. 4.10. In this benchmark, there are in total 10 generators, 39 buses, 12 transformers and 34 transmission lines. Consequently, 68 distance relay agents are placed in the system - two agents for each transmission line. To better explain the co-simulation results, the 34 transmission lines are numbered in red circles in Fig. 4.10. The 68 relay agents are also sequentially numbered based on which transmission line they are

attached to. For example, the two relay agents on transmission line 1 has id 1 and 2 and the two relay agents on transmission line 34 has id 67 and 68. The 10 generators in the system are cylindrical rotor machines represented by equal mutual inductances on the direct and quadrature axes. Each generator is equipped with an IEEE type 1 excitation system model with added speed multiplier and basic steam turbine and governor. The detailed parameters of these power system devices are configured in PSLF. The PSLF simulation time step is set as 1ms.

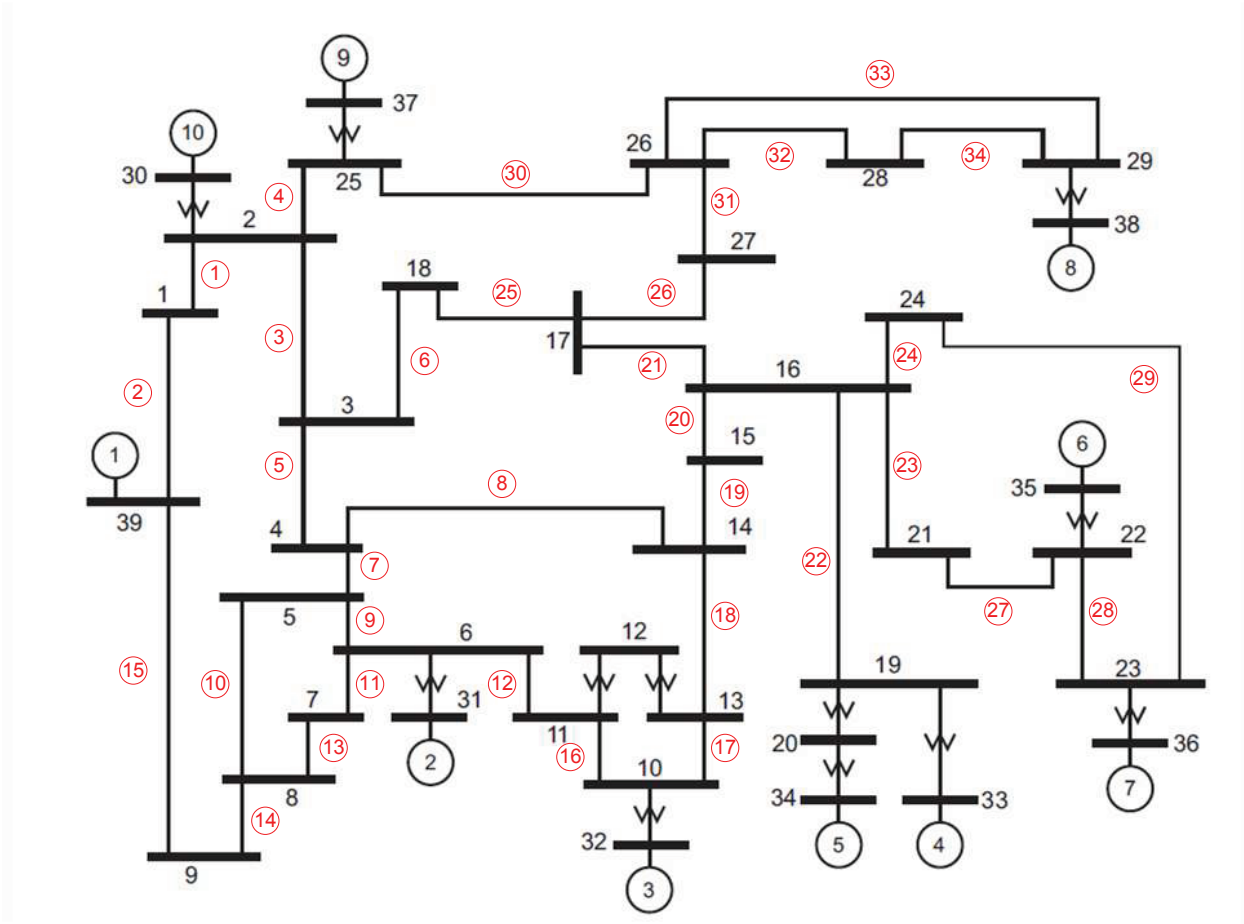


Figure 4.10: New England 39-bus system [2]

The relay agents are connected with each other by a communication infrastructure which is modeled in NS2. This communication infrastructure consists of two levels: substation level and wide area level. Ethernet is used as the layer-2 protocal for the local area network (LAN) in each substation. Then at the substation level, all the relay agents in the same

substation are assumed to share a 100Mbps Ethernet. For example, there are 5 transmission lines connected to bus 16, then 5 distance relay agents on this side should be placed in bus 16 and connected by an Ethernet. In NS2, these relay agents are represented by individual network nodes set as working in the Ethernet model. The relay agents can communicate with other relay agents at different substations via a gateway router. On the wide area level, the substations are connected by high speed direct communication links. These links follow the same routes as the transmission lines. Each communication link has 1Gbps bandwidth and 5ms communication delay. Since the size of messages exchanged among relay agents are small [7] and can be encapsulated in a single packet, UDP is selected as the main transport protocol for relay agent communication. The network is assumed to be dedicated to the protection scheme so that no background traffic is considered at this stage. However, its effect can be easily evaluated in NS2 as long as the detailed traffic model is available.

### 4.3.1 Supervisory Protection

In the supervisory protection scheme, the master agent is placed at Bus 16 since this bus has the highest connection degree in the system. Two different protection scenarios are co-simulated respectively:

1. There is a real fault on a transmission line but its primary relay fails;
2. There is no fault on a transmission line but the backup relay has false reading.

First, a real short circuit fault is created at 0.1 second of the simulation time on transmission line 8 which is between Bus 4 and Bus 14. This fault is shown in Fig. 4.11. The primary relay covering this line on the side of Bus 14 is assumed to work properly but the relay on the side of Bus 4 is assumed to fail. In this condition, its zone 3 backup protection relays must take action instead. In this example, the backup relays are number 9 at Bus 3 and number 14 at Bus 5. They will submit requests to the master agent and wait for decision. The master agent will collect information from all the responsible relays to make a decision and send it back to the backup relays at Bus 3 and Bus 5.

This scenario is simulated on GECO. The simulated voltage magnitude at Bus 3 is used as an indicator to validate the protection scheme. It is plotted in Fig. 4.12. The voltage

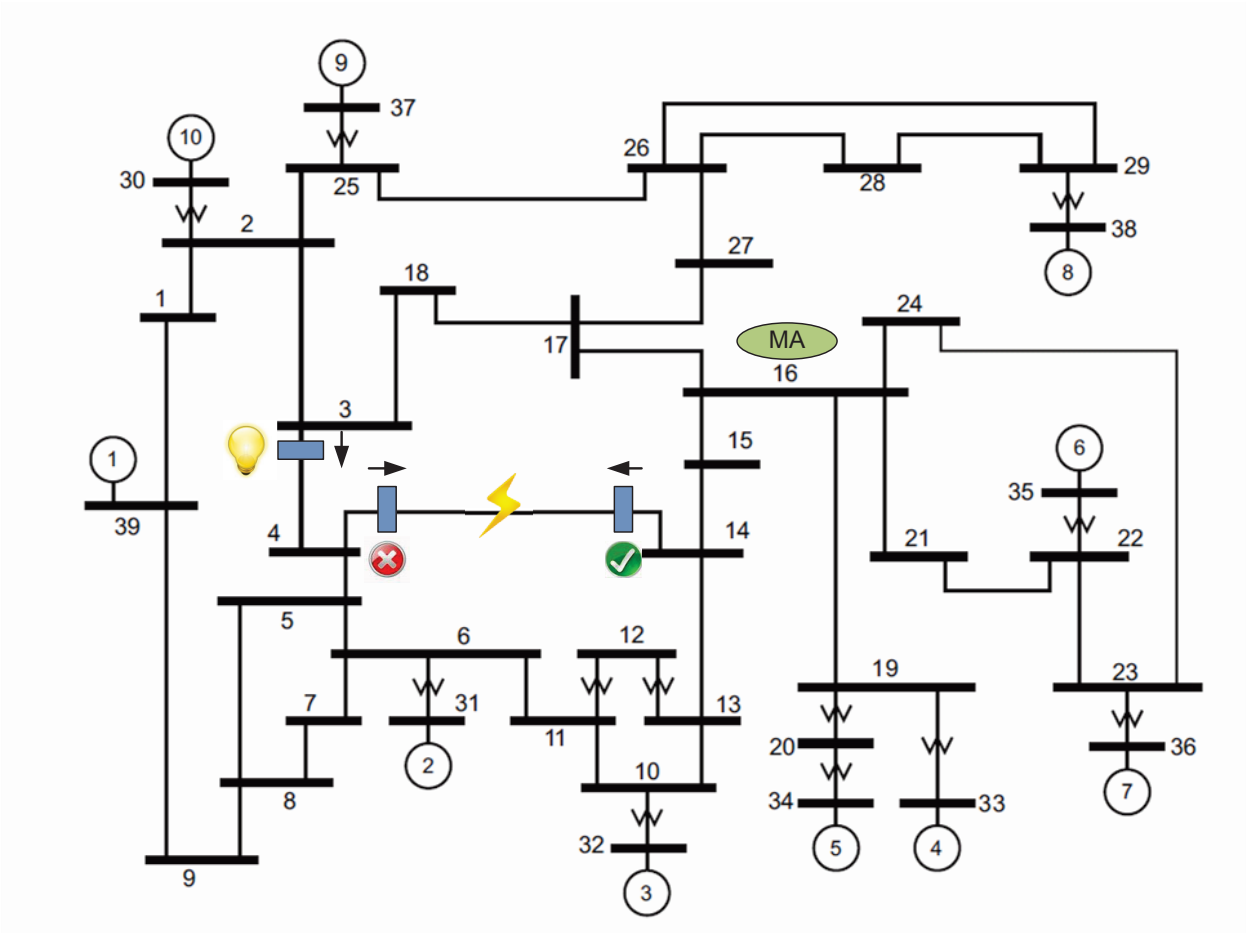


Figure 4.11: Supervisory protection when there is a real fault [2]

drops in the beginning since one of the primary protection relay fails to isolate this fault and it significantly affect the rest part of the system. At this time the backup relays kick in and start to communicate with the master agent for decision. Then, the voltage magnitude comes back after the fault is identified by the master agent and the fault is cleared at both sides of the transmission lines. It roughly takes 80ms for the backup relays to clear the fault. Compared to the traditional zone 3 backup protection which has to wait for 1 second to take action, the supervisory protection scheme can save a lot of time.

Second, it is assumed that there is no fault in the system. However, the same backup relay number 9 at Bus 3 is assumed to sense a fake zone 3 fault due to a false reading which is shown in Fig. 4.13. According to the protection scheme, it will send a request to the master agent for decision. However, the master agent will find out this is a false reading based on

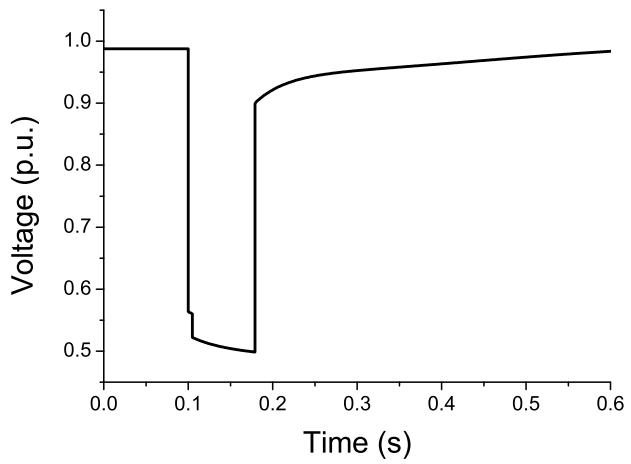


Figure 4.12: Voltage magnitude at Bus 3, real fault, supervisory protection.

the feedbacks it collects and it will notify relay number 9 to block the trip action.

This scenario is also simulated on GECO and the voltage magnitude at Bus 3 is also selected as an indicator to validate the protection scheme. The curve is plotted in Fig. 4.14 where we can find that no action is applied to the transmission line. The protection scheme successfully identify the false fault condition. Compared to the traditional Zone 3 backup protection which will trip the line anyway, the supervisory protection scheme avoids unwanted blackouts.

### 4.3.2 Ad-hoc Protection

Similarly, the ad-hoc protection scheme is applied to the 39-bus system. The master agent is removed and the slave agent (now peer agent) will directly communication with its neighbors. Same real fault and fake fault scenarios in Fig. 4.11 and Fig. 4.13 are repeated for ad-hoc protection. Fig. 4.15 and Fig. 4.16 shows the simulation results in these two scenarios. Again, the ad-hoc protection scheme successfully take the correct actions. Also, based on Fig. 4.15, the communication delay in the ad-hoc protection scheme is only half of that of the supervisory protection scheme.

It is very important that the communication time between agents has to be limited within a certain threshold. The communication time for the four protection scenarios which have been validated so far is shown in Table 4.1. All of the protection actions can be completed within the general Zone 2 time delay of 100ms and the ad-hoc protection scheme takes

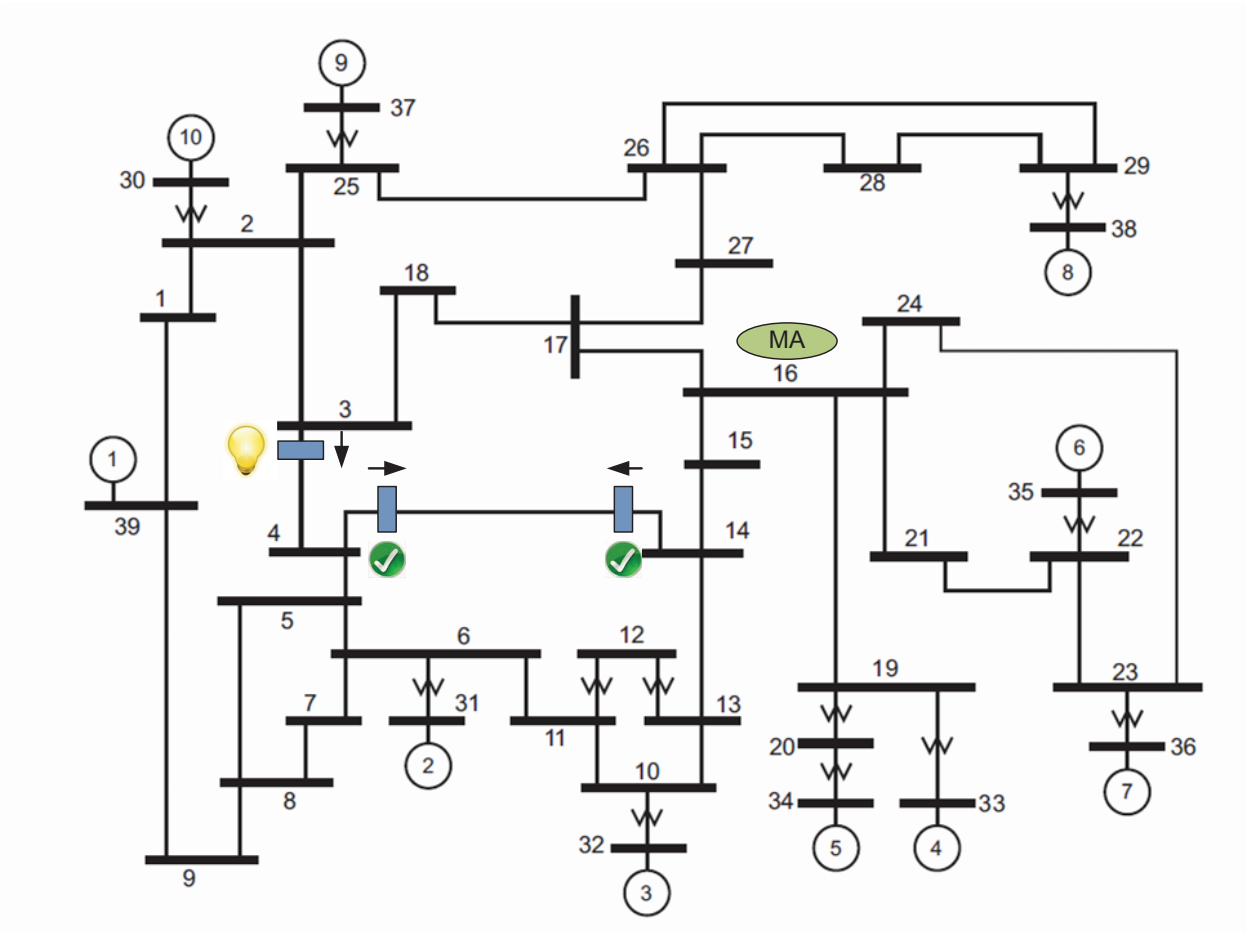


Figure 4.13: Supervisory protection when there is no fault, but false reading. [2]

significantly lesser time than the supervisory protection. Moreover, a block decision always requires longer time than a trip decision which is reasonable considering the decision making mechanism we have adopted.

Table 4.1: Communication time of the protection schemes

| | Trip Decision | Block Decision |
|---|---|---|
| Supervisory Protection | 76.661 ms | 96.635 ms |
| Ad-hoc Protection | 28.290 ms | 38.499 ms |

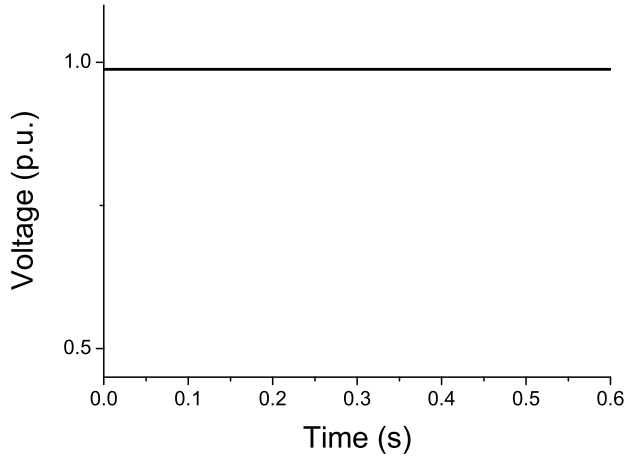


Figure 4.14: Voltage magnitude at Bus 3, fake fault, supervisory protection

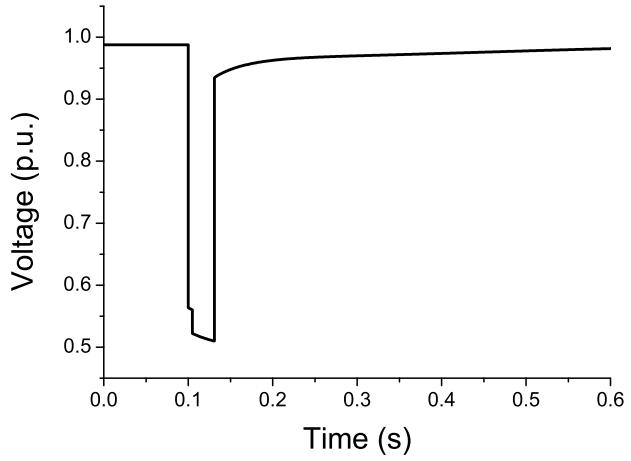


Figure 4.15: Voltage magnitude at Bus 3, real fault, ad-hoc protection

### 4.3.3 Communication Delay Analysis

To further validate and stress test the protection schemes on the entire 39-bus system. Similar fault scenarios in Fig. 4.11 and Fig. 4.13 are repeated for every transmission line and every primary relay in the system. In this set of simulation, the communication link has 100 Mbps bandwidth and 3 ms latency. Similar to the power system, the communication network may suffer from failure as well. Network link failure, node failure and traffic congestion can all undermine the normal communication and affect the applications on top of it. Since our protection schemes highly rely on the network infrastructure, it is also very important to study its robustness again network failure. Therefore, we also consider a scenario in

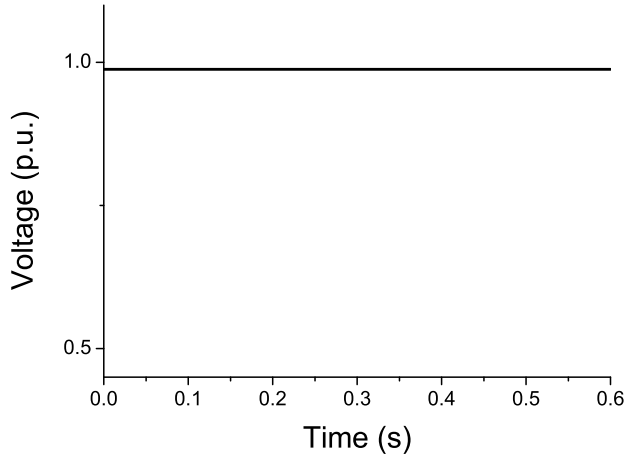


Figure 4.16: Voltage magnitude at Bus 3, fake fault, ad-hoc protection

which the communication link associated with the faulty transmission also fails. This is possible that transmission line and communication link are cut off by the same object. The communication delays in this case expect to increase so we need to validate if the protection scheme can still successfully work.

To better illustrate the communication time distribution for the supervisory protection scheme, the average communication time for all the 68 distance relays is plotted in Fig. 4.17. We can find that the communication time significantly varies depending on the location of the relays. Even so, all the communication can be done within five cycles, which is about 0.0833s in US standard.

For the ad-hoc protection, same experiments are done. The communication time needed for both trip decision and block decision are measured. The trip decision can be made as long as another peer agent sees the fault and the block decision will be made when all the responsible peer agents report back. The average time delay distribution is plotted in Fig. 4.18 where we find immediately that the communication time in ad-hoc protection is less than supervisory protection and very stable. The only exception happens to the relays which are on the transmission line 32,34 and 36. These lines form a small transmission loop so that other responsible peer agents could be very close to the original one. The ad-hoc protection could react very fast: trip decision can be made within one cycle and block decision can also be made within two cycles.

The communication time distributions for both schemes under link failure condition are

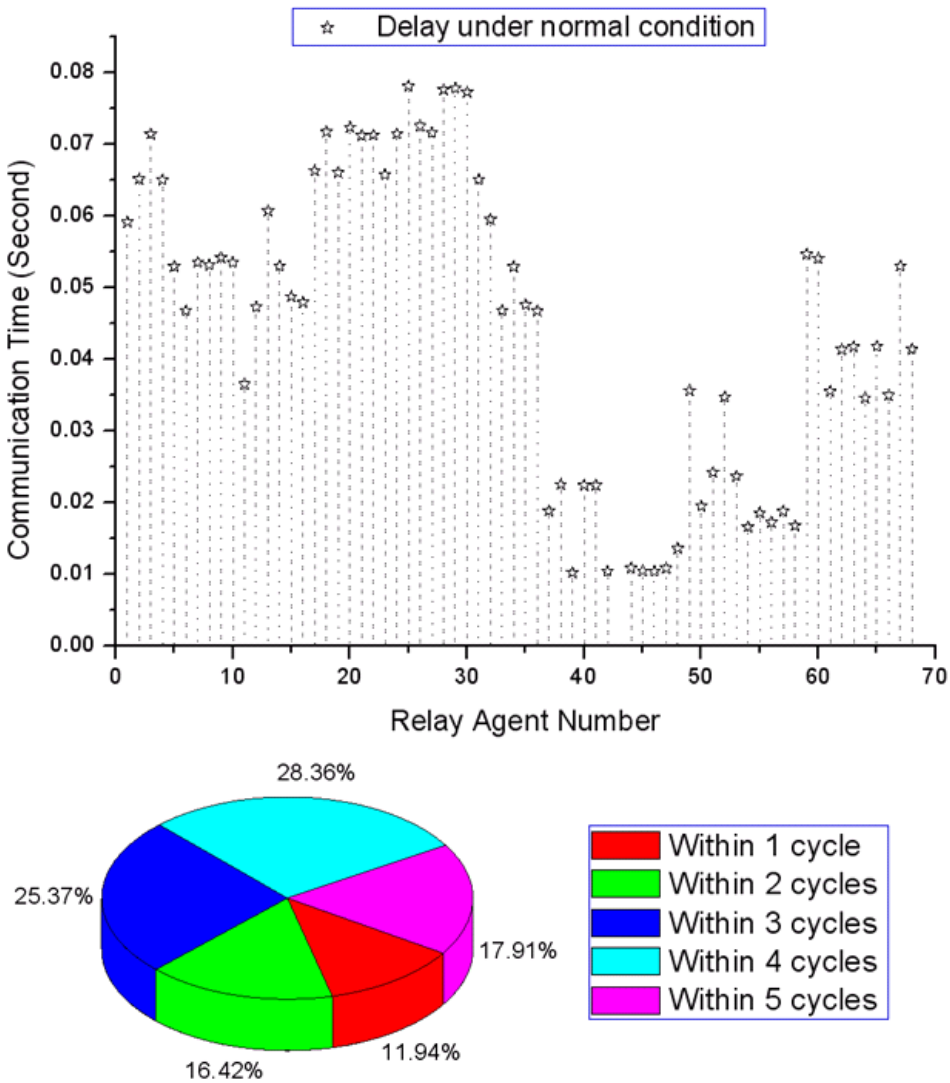


Figure 4.17: Time delay distribution in supervisory protection

shown in Fig. 4.19 and Fig. 4.20. For supervisory protection the distribution is still unstable. The communication time increases a little bit for most of the relays but also increases a lot for several others. Generally speaking, the communication time increases by one cycle on average. For ad-hoc protection, the time distribution becomes unstable. Most of relays need much more communication time to make a trip or block decision. There are also some relays whose decision time doesn't change too much. This is also due to transmission line loops in the system.

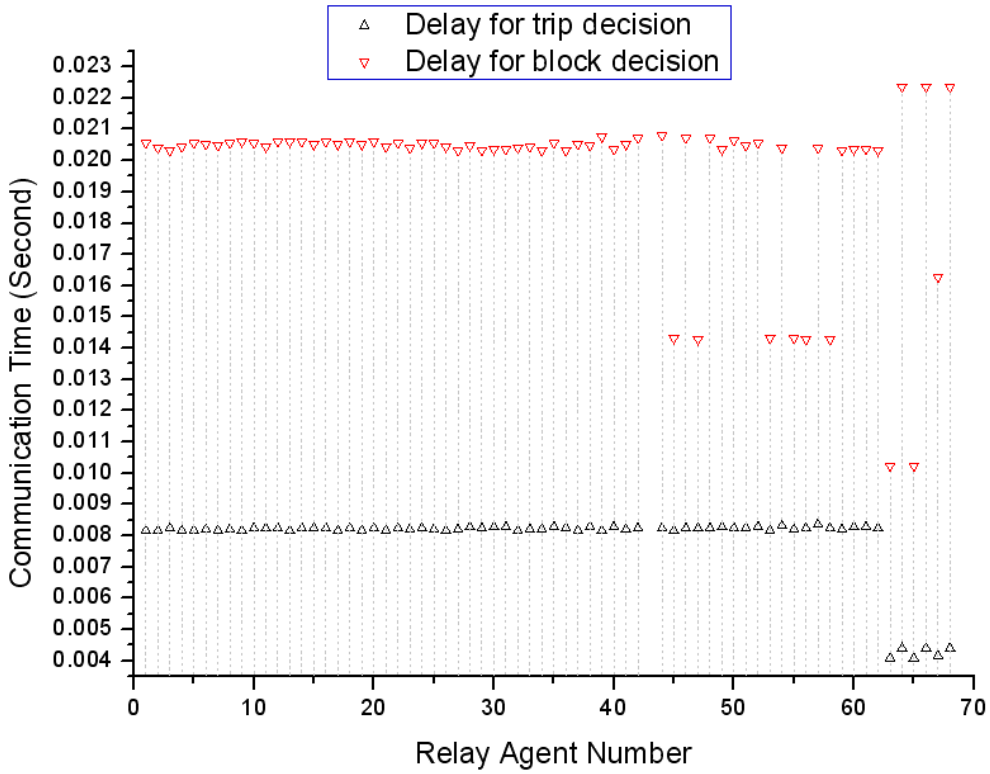


Figure 4.18: Time delay distribution in ad-hoc protection

### 4.3.4 Protection Scheme Comparison

#### 4.3.4.1 Difficulty of Real System Implementation

Most of today's digital relays can be equipped with network interface as an option. International communication standards are being designed to realize compatible communication between devices from different vendors. An underlying communication network could be constructed to connect the relays right away. The cost of a new network infrastructure could be high but the power system may share bandwidth with existing networks like telephone network, cell phone network or the Internet, although security issues need to be considered.

The supervisory protection scheme is a non-intrusive upgrade of existing protection infrastructure and only one extra master agent needs to be designed. The coordination between relays can be realized by slave software agents which will not require any redesign of current digital relays. As long as the digital relays are able to send the fault status and receive trip

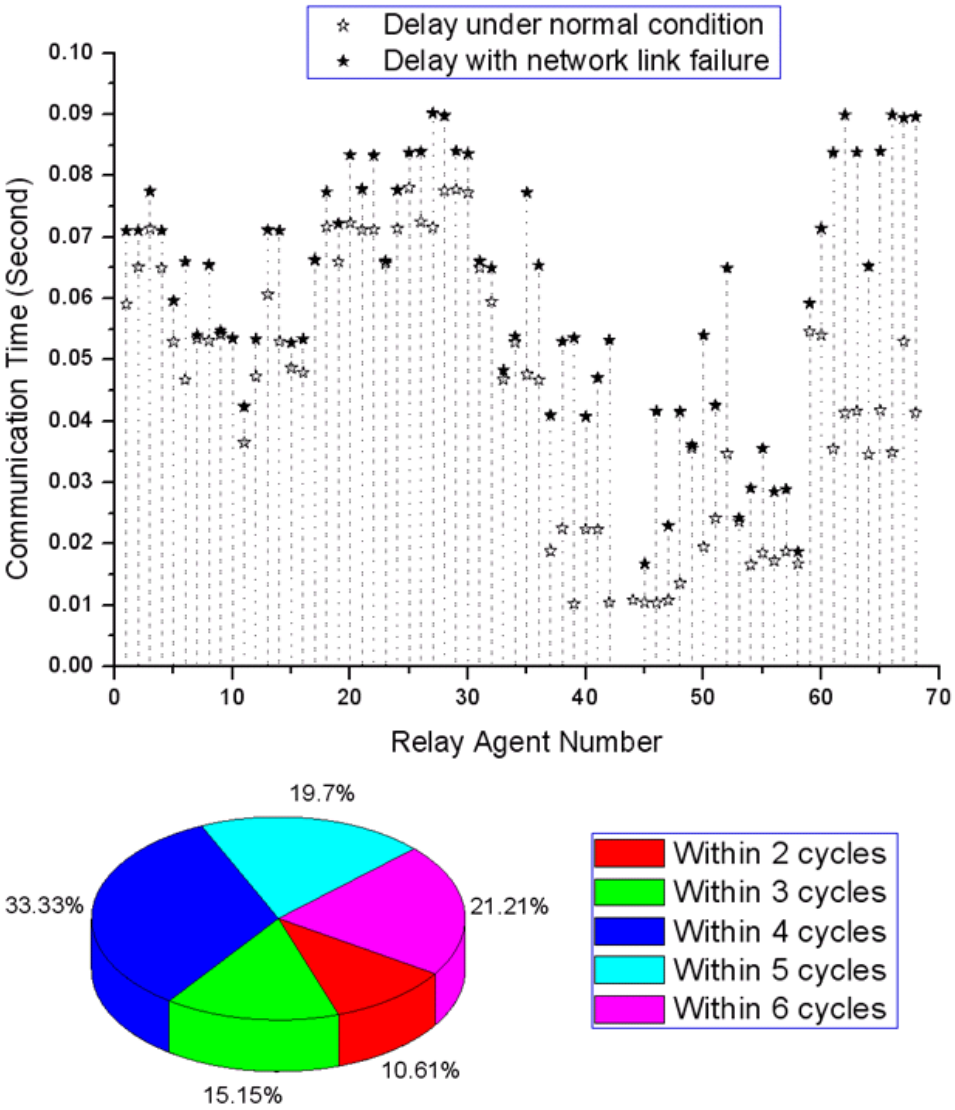


Figure 4.19: Time delay distribution in supervisory protection with communication link failure

or block decisions, all the other work could be completed by slave software agents and the master agent. The power system information should be stored in the master agent only so that the investment for the design of those software agents could be justified.

The ad-hoc protection scheme may need more investment, but only for the design of the peer agents. The existing relays do not have to be replaced either. Since each peer agent operates in an autonomous manner, the system information should be installed in each

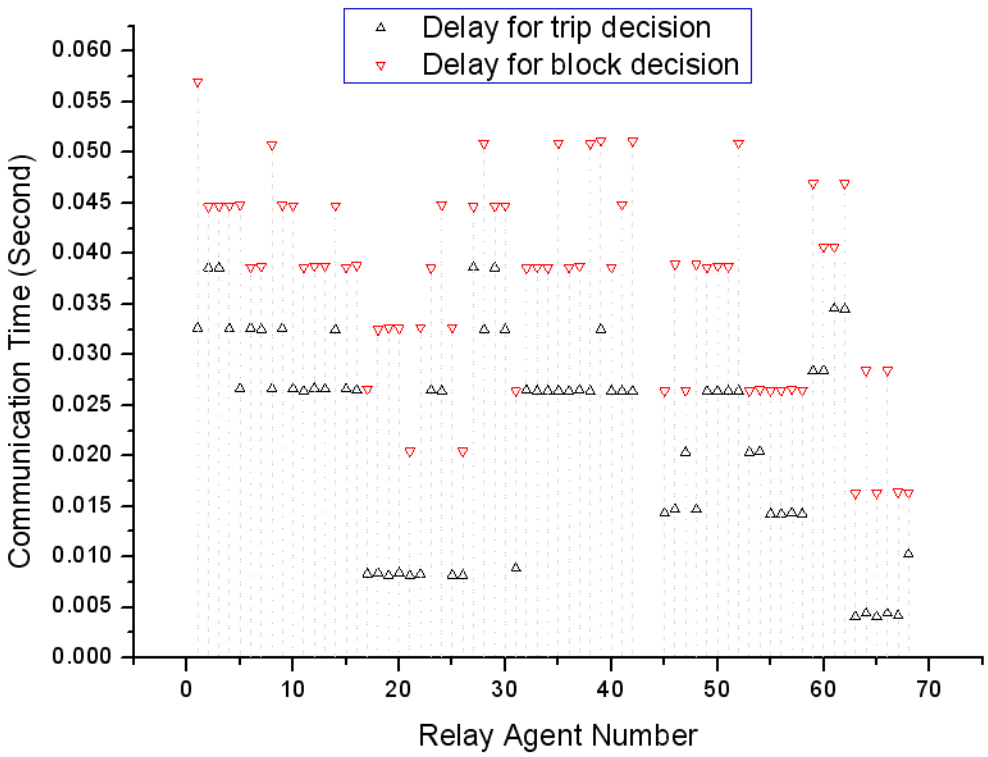


Figure 4.20: Time delay distribution in ad-hoc protection with communication link failure

peer agent to find the responsible peer agents. However if the system topology changes the system information stored in the peer agents have to be updated one by one, which will limit the flexibility of this application. A compromise solution could be using a hybrid protection scheme based on both supervisory and ad-hoc protection. The master agent is still maintained in this hybrid mode to update the system information for each peer agent when necessary. But if a fault is observed in the system the peer agents still communicate with each other in an ad-hoc manner.

#### 4.3.4.2 Reaction Time

From the simulation results in the last section, we find that the ad-hoc protection has much smaller and more stable communication time than the supervisory. This is an advantage indicating that this protection scheme could be deployed in a very large system since the communication time is almost independent of the relay location. In contrary, the supervisory

protection may be limited within a small area to satisfy the communication requirement. When considering the protection of a larger area, multiple master agents may be needed to overlap their reaches. However this may induce unwanted contention and coordination problems.

A fast reaction time of the backup protection may not be always good. In our simulation, the ad-hoc communication can be finished within one cycle. This reaction time may be too fast for a backup relay since the backup relay may trip even faster than the primary protection. More rigorous design specifications could be posed for the relay designer to solve oversensitive issues. We also need to mention that, our simulation results are obtained based on a relatively simple network model and the real network could be more complex and sparse. However, our co-simulation platform provides the users the capability of modeling their own complex networks in NS2.

#### 4.3.4.3 Robustness to Network Failure

The simulation results in the last section show that both of the protection schemes have extra communication delays due to the network link failure. In supervisory protection scheme the average extra delay is about one cycle. Compared to the original communication time this is about 30% increase. However, in the ad-hoc protection, the communication time increases by two or three times which implies the ad-hoc protection performance declines more than the supervisory protection under such kind of failure. Also the time distribution of the ad-hoc protection becomes unstable under link failure, hence it increases the protection design difficulty when considering system fault tolerance.

### 4.3.5 Synchronization and Scalability of GECO

In this section, we will run more simulations on GECO to compare its synchronization method to other solutions and to test the scalability of it. We leverage the proposed communication-based distance relay backup protection schemes as a testbed to show the advantages of GECO.

#### 4.3.5.1 Comparison of Different Synchronization Methods

In the previous chapter, the disadvantages of alternative synchronization method have been discussed. In particular, EPOCHS [16] uses "time-stepped" synchronization and suffers from simulation errors. In this section, we will show the difference of different synchronization methods using a concrete example. We design an alternative co-simulation platform using the synchronization method proposed in EPOCHS [16]. Then, we run simulation cases of the proposed communication-based distance relay backup protection scheme on the alternative platform and GECO using same simulation settings. Then the simulation results from different co-simulation platform will be compared to show the difference.

The protection scenario in this experiment is the supervisory protection with a real fault. The initial fault time, fault location, master agent location and the relay agents involved are all the same on different platforms. This scenario is repeated on the time-stepped synchronization platform using different synchronization steps and the results are compared with GECO. As an indicator, the voltage levels at Bus 3 among all the simulation results are plotted all together in Fig. 4.21. From the figure, we can easily tell the difference among simulations. As the synchronization time step increases, simulation errors are accumulated and the protection action is delayed accordingly. The real system dynamics will be difficult to estimate with these delays. In general, for the "time-stepped" synchronization method, the larger the time step is chosen, the more inaccurate results are expected. However, in the extreme case, if the time step is as small as the power system iteration time step, this method can provide the same simulation fidelity as the GECO framework. In Fig. 4.21, the voltage level of time-stepped synchronization using 0.001s time step is almost the same as GECO. This similarity further proves the advantage and necessity of our co-simulation framework for fully interconnected power system and communication network.

#### 4.3.5.2 Co-Simulation Scalability

The scalability of the co-simulation platform is another important feature considering the actual power system of interest can be much larger than this 39-bus benchmark system. Since GECO integrates two individual simulators, the overall co-simulation scalability will be largely determined by the scalability of the individual simulators themselves and how the

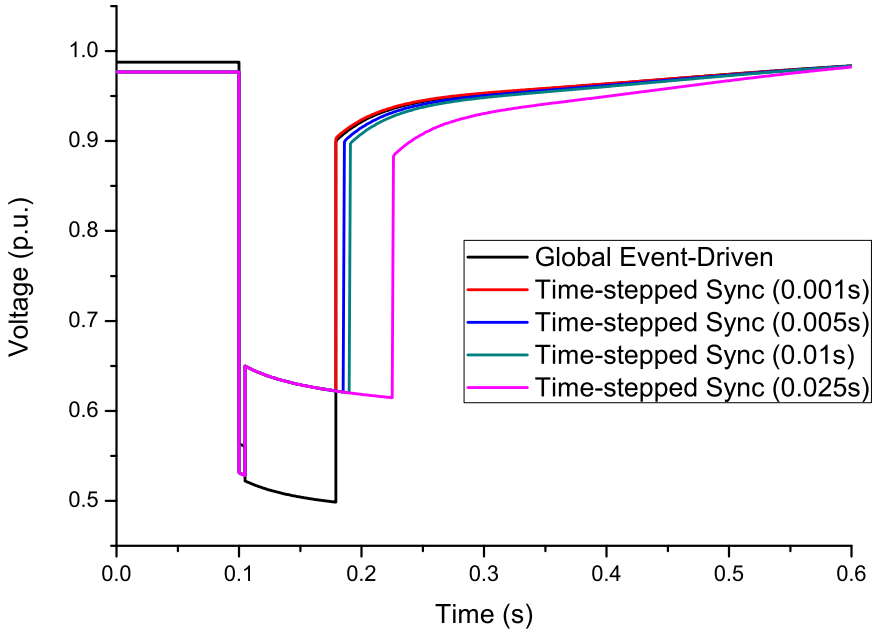


Figure 4.21: Simulation results using different synchronization methods

integration interface is handled. More specifically, in this case, PSLF is able to simulate a system as large as 60,000 buses and NS2 is able to simulate a network with at least 20,000 nodes and the simulation time is on the order of Nlog(N) [67]. Therefore, GECO has the capacity to model and simulate large national systems like WECC. On the other hand, the two simulators are integrated using a bi-directional interface where system information is exchanged. As the system scale grows, the amount of system information through this interface will increase accordingly. The time needed to complete a co-simulation case may also increase depending on the number of interactions between the two simulators.

Table 4.2: Comparison of simulation speed

| Run for 0.5sec | 39-Bus System | 127-Bus System |
|---|---|---|
| Power Step: 0.001sec | 19min16sec | 39min40sec |
| Power Step: 0.01sec | 1min26sec | 2min20sec |

As an example, the same communication-based protection scheme is implemented on a 127-bus WECC system and the co-simulation speed is compared to the 39-bus case. There are 112 transmission lines, 28 generators in this 127-bus system in comparison to 34 lines and 10 generators in the 39-bus system. The co-simulation speeds are shown in Table 4.2. The

stop time in both simulators is set as 0.5 second. Two PSLF simulation time steps, 0.001 second and 0.01 second, are selected for comparison. Smaller PSLF time step results in more discrete power system events and more interactions through the interface between the PSLF and NS2. In Table 4.2, the total simulation time required for different settings are measured on a regular PC. It is clear that co-simulations for larger systems or with smaller power steps both require longer simulation time. However, the latter factor contributes significantly more than the former one.

The co-simulation results in Table 4.2 indicate that the interface between PSLF and NS2 may be a bottleneck for GECO as far as larger scale systems are concerned. This is due to the nature that these two individual simulators are not designed for the purpose of integration with each other. The interface is mainly designed to make information exchange and global event scheduler feasible rather than to optimize the overall co-simulation speed. However, there are many potential ways to improve the co-simulation speed since PSLF and NS2 is not the only solution for GECO. Many other power system and communication network simulators can be readily integrated using GECO framework like PSS/E, InterPSS, OPNET, OMNET++ etc. Depending on the simulators, it is possible to parallel the co-simulation or use distributed resources to expedite the simulation speed [68, 69]. However, it requires great support from the simulators and the coordination between simulators can be much more complicated. In the case of current implementation of GECO, PSLF is not an open source software. Therefore, very limited change can be made to facilitate the speedup.

# Chapter 5

# All-PMU State Estimation

Power system state refers to the complex voltage values at each bus in the system. On the basis of power system state and other known information such as system topology, transmission line impedance, etc., all the other system status can be calculated. As the power system becomes more complicated, it is more crucial for the system operators to know accurate system state in real time. The most likely system state can be estimated from redundant measurement directly or indirectly using a state estimator. Traditionally, a static state estimator is used, assuming that the power system is in quasi-steady state. It collects a redundant collection of measurements on real and reactive power flows, power injections and nodal voltage magnitude. The measurements are collected via Remote Terminal Units (RTUs), A/D converters, modems, communication channels and computers. This system forms the so-called SCADA system. Because the RTUs do not label a time stamp, the metering value recorded at the control center via a planner suffers from time skew, which may include a bias in the state estimator. On the contrary, Phasor Measurement Units (PMUs) are provided with a time stamp, which in principle, prevent the time skew to occur. Given the increased deployment trend of PMUs, it is expected that all-PMU state estimation will eventually replace traditional or mixed state estimators at the control centers of power utilities. Due to the repeated calibration of the voltage and current transformers at the measurement sites, and direct time-synchronized measurement of phasors, the estimated state by an all-PMU state estimator is not only accurate, but also available at a rapid rate, leading to the use of the system state for protection, stabilization, and even calibration of the

measuring devices. However, due to high reliance on an advanced communication network infrastructure for the delivery of large amount of measurements in real-time, the cyber attack surface of the power system is increased. Deliberate cyber attacks or unintentional network failures can affect the state estimator leading to misoperations of the power system.

## 5.1 Background

State estimation lays the foundations of key applications in a modern wide-area measurement system (WAMS) such as system visualization, contingency analysis, optimal power flow, corrective actions required, alarms, real-time pricing, etc [70]. It is also expected to play a crucial role in instrument calibration, system integrity protection schemes (SIPS), remedial action schemes, system restoration, etc [9].

Traditionally, power meters installed in the system periodically measure unsynchronized power flows and line currents for the state estimator and the measurements are collected via a SCADA system. The scanning rate of the SCADA system is in the range of 3-4 seconds which is slow to accurately capture the system dynamics. The estimation process is usually nonlinear such that the iterative algorithm consumes more computational power and takes the risk of divergence. In addition, traditional SCADA systems built decades ago are vulnerable to cyber attacks.

The all-PMU state estimator can steadily improve the deficiencies in the traditional ones. The PMUs use GPS signals to rigorously synchronize measurements and can directly measure positive sequence voltage and current phasors at selected buses. The accuracy of commercial GPS timing pulse is less than 250 ns, so that in a 60Hz power system, the phase angle error is less than 0.02 degrees. The updating rate of the PMUs is tunable but usually set at 30 times per second which is much faster than the SCADA system. The measurements are collected via an advanced packet-switching data network which is more effective than legacy SCADA system.

To explain why all-PMU state estimation has advantages over the traditional ones, the mathematical background of state estimation is briefly discussed in this section.

### 5.1.1 Weighted Least Squares Estimation

In this section, mathematical background of the method of weighted least squares is briefly introduced [50, 71].

Suppose there are $m$ measurements denoted by $z$, $m$ measurements errors denoted by $e$ and $n$ variables denoted by $x$ to be estimated. The set of measurements and the set of variables are related by a set of functions $h(x)$. Then we will have:

$$[z] = \begin{bmatrix} z_1 \\ \vdots \\ z_m \end{bmatrix} \quad [e] = \begin{bmatrix} e_1 \\ \vdots \\ e_m \end{bmatrix} \quad [x] = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \quad [h(x)] = \begin{bmatrix} h_1(x) \\ \vdots \\ h_m(x) \end{bmatrix} \tag{5.1}$$

and

$$[z] = [h(x)] + [e] \tag{5.2}$$

In the weighted least squares estimator, the estimated values of $x$ are found by minimizing:

$$J(x) = \sum_{i=1}^{m} \frac{(z_i - h_i(x))^2}{\sigma_i^2} = [z - h(x)]^T R^{-1} [z - h(x)] \tag{5.3}$$

where $e \sim N(0, R)$ and $R = diag(\sigma_i^2)$ is the covariance matrix of $e$ assumed to be known.

To minimize Eqn(5.3), the first derivative of Eqn(5.3) should be equal to zero:

$$\frac{\partial J}{\partial x} = -\left[\frac{\partial h(x)}{\partial x}\right]^T [z - h(x)] = -[H(x)]^T R^{-1} [z - h(x)] = 0 \tag{5.4}$$

where $[H(x)]$ is the measurement Jocabian matrix [50, 71].

Eqn(5.4) can be solved using numerical algorithms which yields to an iterative solution given by

$$x_{k+1} = x_k + ([H(x_k)]^T R^{-1} H(x_k))^{-1} [H(x_k)]^T R^{-1} (z - h(x_k)) \tag{5.5}$$

### 5.1.2 Traditional Power System State Estimation

Traditional power system state estimator uses power injections, power flow measurements or voltage magnitudes to estimate the system state (complex voltage at each bus). The power

injections and power flows are related to the nodal voltage magnitudes and phase angles, the so-called state variables, via

$$P_i = V_i \sum_{j=1}^{N} V_j (G_{ij} \cos\theta_{ij} + B_{ij} \sin\theta_{ij}) \tag{5.6}$$

$$Q_i = V_i \sum_{j=1}^{N} V_j (G_{ij} \sin\theta_{ij} - B_{ij} \cos\theta_{ij}) \tag{5.7}$$

$$P_{ij} = V_i^2 (g_i + g_{ij}) - V_i V_j (g_{ij} \cos\theta_{ij} + b_{ij} \sin\theta_{ij}) \tag{5.8}$$

$$Q_{ij} = -V_i^2 (b_i + b_{ij}) - V_i V_j (g_{ij} \sin\theta_{ij} - b_{ij} \cos\theta_{ij}) \tag{5.9}$$

Eqn(5.6) to Eqn(5.9) form the $h(x)$ of the traditional power system state estimator which is non-linear and can lead to slow convergence or divergence. The $H(x)$ for the traditional power system state estimator can be derived from Eqn(5.6) to Eqn(5.9) which is presented in [71].

### 5.1.3 All-PMU Power System State Estimation

In an all-PMU state estimator, the complex voltages at each bus can be directly measured. Therefore, the estimation can be much easier and faster than the traditional ones. To make the measurement set redundant, complex current are usually added to the measurement set as well. Although people have shown that it is not necessary to place PMUs at every bus to have the entire system observability [72], in this chapter, we assume that there is one PMU at every bus. Then the $h(x)$ for all-PMU state estimator will be:

$$V_i = V_i \tag{5.10}$$

$$I_{ij} = \frac{V_i - V_j}{r_{ij} + jx_{ij}} + jV_i \frac{b_{ij}}{2} \tag{5.11}$$

Then the estimation process in the all-PMU state estimator is largely simplified and faster. The system state can be calculated from linear equations [71, 73]:

$$[B] = \begin{bmatrix} II \\ yA + y_s \end{bmatrix} \tag{5.12}$$

$$[z] = \begin{bmatrix} V \\ I \end{bmatrix} \tag{5.13}$$

$$[\hat{x}] = [(B^T B)^{-1} B^T][z] \tag{5.14}$$

where $\hat{x}$ is the estimated system state, $II$ is an identity matrix, $y$ is the series admittance matrix, $A$ is the current measurement-bus incidence matrix, $y_s$ is the shunt admittance matrix and $z$ is the measurements vector.

### 5.1.4 Communication Infrastructure of the All-PMU State Estimator

The all-PMU state estimators are usually built on WAMS which mainly consists of interconnected PMUs and Phasor Data Concentrators (PDCs) in a hierarchical layered architecture as shown in Fig. 5.1. The PMU measurements are synchronized by high precision GPS signals in local substations and periodically sent to a nearby PDC via gateway routers and packet-switching data networks. The transmission format of the measurements follows the IEEE C37.118 standard and either TCP or UDP can be used as the transport protocol. The PDCs collect time-tagged phasor measurements from multiple PMUs and rearrange the data in chronological order. When PDCs have collected all the data with the same time tag, the data will be packed and uploaded to a higher level PDC - the Super PDC. The Super PDC is the final destination for the PMU measurements where the state estimation is done.

Fig. 5.2 shows the details of how the PDCs collect, rearrange and send the phasor measurements. In general, it consists of four main modules. The preprocessing module receives phasor measurements from PMUs and extracts the data from the raw data stream and buffers them into a database. The data processing module is in charge of realigning the received data by time tags. The output interface module uploads data to the Super PDC. The exception handling and diagnostics module maintains a timer and monitors the status of other modules and provides status information to data processing module. The architecture of the Super PDC is very similar, except that the output interface module prepares the collected measurements for the state estimator.

The timer in the PDCs and the Super PDC is very crucial for the entire state estimation

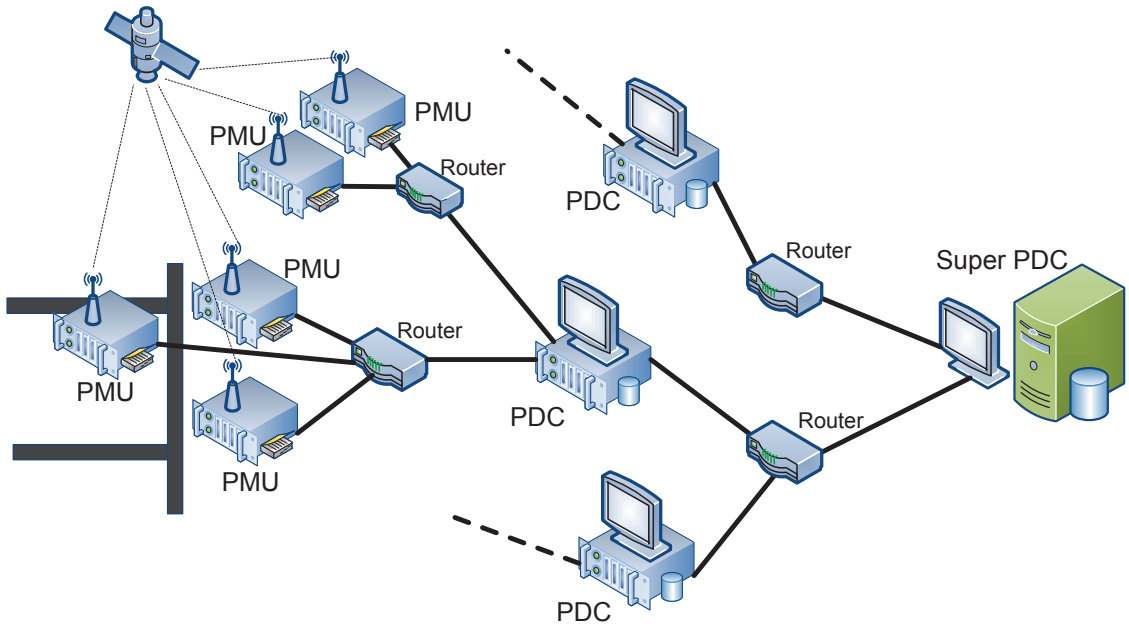


Figure 5.1: A hierarchical architecture of the wide area measurement system

process from a cyber security point of view. A typical timer setting is about 50 ms [15]. The PDC starts a timer when it receives the first packet with a certain time tag. Measurements with the same time tag share the same timer. If the PDC can collect all the needed measurements with that time tag before the timer expires, it will pack all the measurements and upload them to the Super PDC. Otherwise, only the collected measurements will be uploaded and other missing measurements will be discarded. Similarly, the Super PDC will launch the state estimator on a subset of measurements if the timer expires before the Super PDC receives all the measurements. In this situation the accuracy of the state estimation can be hampered and the system may be unobservable.

The main factor which can cause the timer to expire is the communication delay of the measurements data. In a packet-switching data network, the communication delay usually consists of four parts:

$$D = D_t + D_q + D_s + D_p \tag{5.15}$$

where $D_t$ is the transmission delay of a data packet which equals to the packet size divided by link bandwidth; $D_q$ is the queuing delay when the packet waits in the router buffer; $D_s$ is the service processing delay in the router which is used to calculate the next route of a packet; and $D_p$ is the propagation delay of a packet from one end of a link to the other.

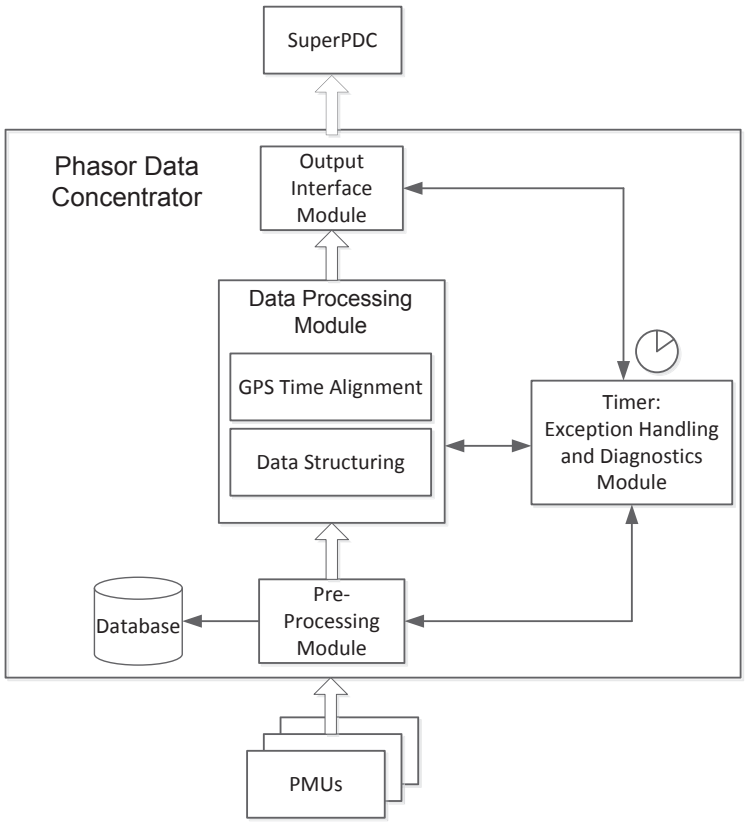


Figure 5.2: The architecture and processing flow in a PDC

Different cyber attacks or network failures can increase one or all of the four parts of the communication delay. It is therefore important to understand how a certain cyber attack can affect a certain part of the communication delay and then affect the timer of PDCs and the Super PDC.

### 5.1.5 Cyber Security Consideration

Time synchronized Phasor Measurement Units (PMUs) are increasingly being deployed in North America, as well as in other countries. The main objective of increased deployment of PMUs is to make the smart grid robust by using the PMU measurements for wide area monitoring and control [9]. PMUs measure voltage and current phasors at a set of buses in the system, and then use those measurements to estimate system state. Every 1/30th of a second, a new measurement is taken and new system state is estimated leading to unprecedented

possibilities in real-time protection and control. However, the all-PMU estimation requires a data network that can deliver PMU data in adequately less than 30 ms, from all the measurement sites to the Phasor Data Concentrators (PDC) and the Super PDC which sorts the data based on time stamps and send to state estimators [7]. Given these requirements of high speed data network, and given the increasing network architectures that use gateways between the enterprise business network and the supervisory control and data acquisition (SCADA) network, the exposure to cyber attack is increased.

We therefore need to understand the threat models, and mitigation techniques. In the recent past a number of researchers have looked into different ways that cyber security attacks can affect the state estimation but we are unaware of any experimental study that creates simulation models to stage cyber attacks on a power system, and its PMU and network infrastructure to assess the effects of attacks [74, 75]. Some of the threat models researchers have thought of are (i) physically cutting network cables; (ii) launch denial of service attacks by blocking the network traffics, overwhelming routers, etc.; (iii) man-in-the middle attack where a perpetrator could intercept PMU data packets in the network, and replace them with fake data packets, leading to wrong state estimation. They can also create replay attack - where the attacker could intercept PMU data traffic and later replay it by blocking the real data traffic, and injecting stored past data traffic; tampering with the PMUs and measuring devices to have wrong measurements; or redirect PMU data to the attacker's own state estimator to construct state information to gain undue advantage in trading in the power exchange market; etc.

Many have proposed to build the data network of WAMS using Internet-compatible technologies. Although for security reasons the network tends to be proprietarily dedicated Intranet and physically isolated from public networks, it does not mean that this network is immune to cyber attacks. Computers in the intranet can be hacked by plug-in USB drives carrying malware. Then these affected computers can be used as sources of collective attacks such as denial of service (DoS). Increasing number of mobile devices can also become a malicious media and we cannot rule out the possibility that utility employees directly implant attacks into the system. Some potential attacks on the all-PMU state estimator are listed below.

**Communication Links Damage:** Some utilities use overhead optical fibers as the main communication links for WAMS. They are placed in parallel with other transmission lines.

Therefore, they are susceptible to physical attacks like cut-off. Natural disasters can interrupt the links as well. Routers have to rebuild their routing tables following a link failure, therefore all the four parts of the communication delay can increase.

**Denial of Service:** DoS attack can happen in the all-PMU state estimator if a number of computers or network devices in the Intranet are controlled by Trojans. The DoS attack generates huge redundant data traffic or inquiries to the target so that the resources of the target may be quickly depleted. In the all-PMU state estimator system, DoS attacks can saturate a critical communication link or a gateway router. In either case, the measurements data can experience longer communication delay or be dropped by the router. In particular, the queuing delay and service processing delay may significantly increase. If a communication is saturated, there will be very limited bandwidth left for the useful data, therefore the transmission delay may also see an increase.

**Data Spoofing:** It is also possible that the PMUs in the system are hacked by adversaries. The latter may arbitrarily manipulate the measurement data without being detected. Let us give a few examples, wrong measurement data can be consistently uploaded to PDCs; The destination of the measurement data can be altered so that the state estimator will never receive the necessary data; The time tag of the GPS signal can be tampered to disorder the synchronization of the measurements; The source ID can be changed so that the state estimator rearranges the data in wrong positions in the measurement matrix. If the PDCs or the Super PDC can be hacked, then the attacker can change the timer settings to make it expire prematurely.

## 5.2 GECO Co-Simulation

In this section, we build a hypothetical all-PMU state estimator on the same New England 39-bus system. Then we run multiple simulation cases on top of GECO to validate the state estimator and study the communication network impact on the state estimator.

### 5.2.1 GECO extension and Simulation Settings

To implement the all-PMU state estimator for this specific system, we add a separated estimator component to our GECO implementation. This new architecture of GECO is shown in Fig. 5.3. When the co-simulation starts, PSLF and NS2 are coordinated by the global scheduler. Power system simulation iterations are modeled as a sequence of discrete events and mixed with other network events in the global event list. The global event scheduler processes the events in the global list according to their chronological order. PMUs, PDCs and Super PDC are modeled as customized applications in NS2. Power system voltages and currents data are simulated in PSLF and sent to the PMU applications in NS2 via an external interface. Phasor measurement data are created by adding random errors to the simulated values. Then these measurements will be time-tagged and sent to PDCs and the Super PDC periodically on the communication network created in NS2. When the Super PDC collects all the measurements with the same time tag, the measurements will be sent to the linear state estimator to calculate the system states.

A hypothetical all-PMU state estimation system is implemented on the New England 39-bus system. The entire system is subdivided into four regions as shown in Fig. 5.4. Each region has one PDC installed to collect measurements from all the local PMUs in its region. The four PDCs are placed at Bus 2, Bus 6, Bus 21 and Bus 27 respectively. A Super PDC is deployed at Bus 16 to collect data from the four PDCs to calculate the final state estimation. The communication infrastructure for this state estimation system is built in NS2. Each bus is represented as a communication node which can send, receive and route measurement data. The communication links are placed in parallel with the transmission lines. The key parameters of the co-simulation are summarized in Table 5.1.

### 5.2.2 Communication Time Analysis

#### 5.2.2.1 Normal Condition Scenario

Under normal conditions, the phasor timer in PDC and SPDC is set as 50ms. Data collected beyond this time will be ignored. The co-simulation results for the normal condition scenario are summarized in TABLE 5.2 where combinations of different link bandwidths and

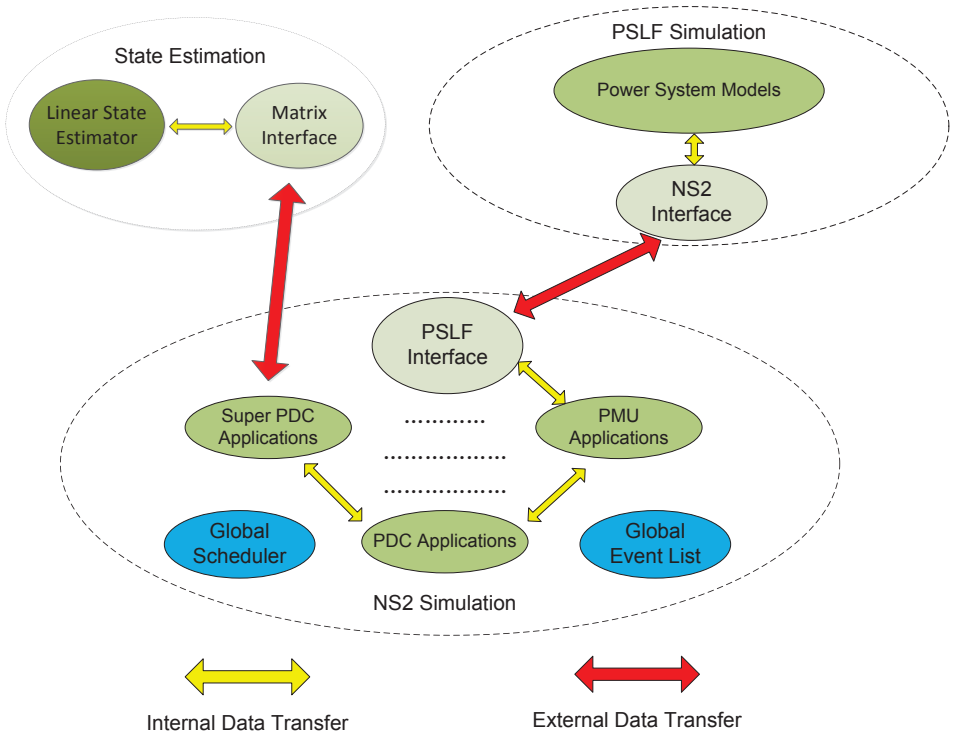


Figure 5.3: The architecture and processing flow in a PDC

Table 5.1: General co-simulation settings

| | | |
|---|---|---|
| Communication Link Bandwidth | $BW$ | 1 Gbps |
| Communication Link Delay | $D$ | 5 ms |
| Measurement Rate | $\lambda$ | 30 times/sec |
| PDC Timer | $T_p$ | 50 ms |
| Super PDC Timer | $T_s$ | 50 ms |
| Phasor Packet Size | $S$ | 500 Bytes |
| PSLF Iteration Step | $Delta$ | 10 ms |
| Measurement Error | $e$ | 1% |

delays are selected. The output of the co-simulation is the average phasor delay and phasor drop rate. The average phasor delay is an index showing how much time a single phasor could spend from the measurement time to the time reaching SPDC. The phasor drop rate calculates the percentage of phasors that are lost during the communication. There are

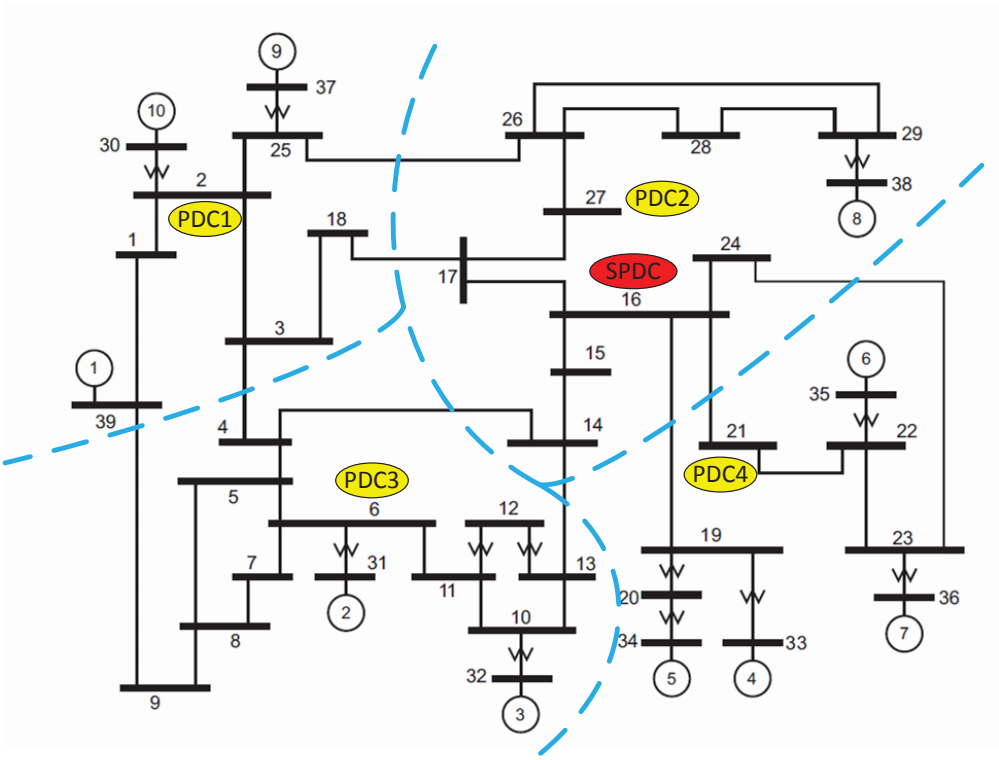


Figure 5.4: All-PMU state estimation on New England 39-bus system [2]

many reasons can lead to the dropping of phasors, for example, network congestion or timer expiration in PDCs.

From TABLE 5.2, we can find that the relationship between the average phasor delay and communication link delay is approximately linear. On the other hand, increasing the bandwidth doesn't give better results. The reason of this is not difficult to reveal. According to IEEE standard C37.118, the packet size of phasor measurements is quite small. If the communication network is dedicated only to this application, there won't be any congestion in the network considering a bandwidth higher than 1Mbps. The total delay is approximately the sum of communication link delays on route. The contribution of bandwidth and queuing delay in this case is trivial. Also in this co-simulation, none of the phasors is dropped during communication.

Table 5.2: Co-simulation results for normal condition

| Parameters | Average Delay | Drop Rate |
|---|---|---|
| BW = 100Mbps, D = 5ms | 55.48ms | 0% |
| BW = 100Mbps, D = 10ms | 110.52ms | 0% |
| BW = 1Gbps, D = 5ms | 55.05ms | 0% |
| BW = 1Gbps, D = 10ms | 110.05ms | 0% |

#### 5.2.2.2 Background Traffic Scenario

From the normal condition co-simulation, we can find that the bandwidths of the communication links are not well utilized since the throughput from one application is small. In the future WAMS implementation, it is very likely to have multiple WAMS applications running simultaneously on the communication network. Some heavy load applications may also be included like video surveillance. Therefore, it is necessary to test the monitoring system under background traffic condition. In this co-simulation, each substation in the system is assumed to send extra communication traffic to the SPDC node. The throughput of this traffic is set as 1Mbps. The co-simulation results are summarized in TABLE 5.3.

From the results, we can easily conclude that the performance of the system is degraded significantly. The linear relationship between the average phasor delay and communication link delay cannot hold any more. This is because the extra background traffic induces network congestion in some part of the system. The phasor data have to be queued in the router buffer and wait for processing. The network congestion not only results in higher communication delay and also forces the timer in the PDCs to expire. Therefore, many phasors will be dropped during communication. Among all the settings in the normal condition co-simulation, the best drop rate is still higher than 24%, which means the communication network cannot sustain such a heavy traffic. The only solution to this problem is to update the communication network. From the last row of TABLE 5.2, we can see that if the bandwidth is increased to 10Gbps and delay is reduced to 1ms, the drop rate will be back to normal again. In practice, optical fibers can reach this specification.

Table 5.3: Co-simulation results for background traffic condition

| Parameters | Average Delay | Drop Rate |
|---|---|---|
| BW = 100Mbps, D = 5ms | 104.95ms | 49.55% |
| BW = 100Mbps, D = 10ms | 140ms | 90.36% |
| BW = 1Gbps, D = 5ms | 83.46ms | 24.14% |
| BW = 1Gbps, D = 10ms | 130.03ms | 41.34% |
| BW = 10Gbps, D = 1ms | 11.02ms | 0% |

#### 5.2.2.3 A Link Failure Scenario

Another scenario to be verified is when the network has communication link failure. It is quite common that the network is put out of work due to hardware failure or software bugs. This happens even more frequently than power system faults. In this co-simulation, the communication link connecting Bus 4 and Bus 14 is assumed to be cut off. Then the co-simulation results are displayed in TABLE 5.4. The results show that when the link delay is low (5ms), after the loss of the link, the system can still work fine only with higher phasor delays. But if the delay is high (10ms), the system has to be re-designed.

Table 5.4: Co-simulation results for link failure condition

| Parameters | Average Delay | Drop Rate |
|---|---|---|
| BW = 100Mbps, D = 5ms | 60.53ms | 0% |
| BW = 100Mbps, D = 10ms | 120.44ms | 31.5% |
| BW = 1Gbps, D = 5ms | 60.05ms | 0% |
| BW = 1Gbps, D = 10ms | 120.04ms | 31.5% |

### 5.2.3 Communication Infrastructure Impact on State Estimator

In this section, four network contingency scenarios are created in GECO to study their impacts on the all-PMU state estimator. We select the estimated voltage magnitude at Bus 3 as an indicator to show the impacts. We will compare the estimated values with the actual reference values (around 0.97 p.u.) which are obtained from PSLF simulation. The reason

to choose Bus 3 is that it is close to the center of the system and it is close to where the contingencies are placed. The durations of all the state estimation results are 1 second.

#### 5.2.3.1 Single Network Link Failure

In this scenario, a single communication link from Bus 16 to Bus 17 is cut off when the co-simulation reaches 0.2 second. The reason to choose this link is because it is close to the SPDC so it carries more measurement data than others. The estimation results are shown in Fig. 5.5 where we can see that the system state becomes unobservable after 0.2 second. The reason of this is that Bus 16-Bus 17 is a critical link. When it is removed, the dynamic routing protocol needs to find an alternative but longer route for the measurements data. After the new route is established, the communication delays for some critical measurements increase such that they cannot arrive at the Super PDC before timer expires. Therefore the system becomes unobservable. The variations of the estimated value are due to randomly simulated measurement errors. The errors follow a normal distribution and the estimated value simply fluctuates around the reference line.

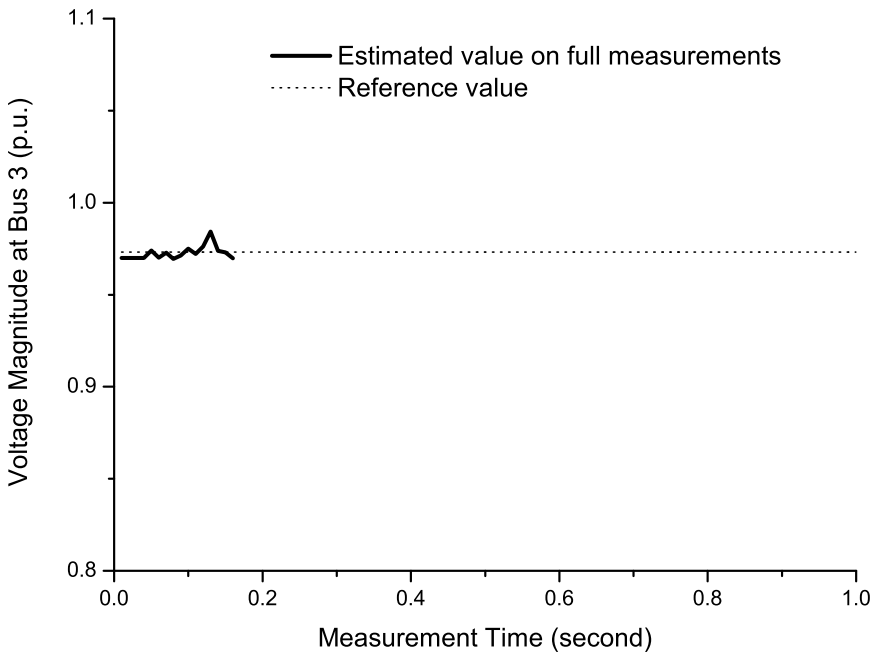


Figure 5.5: Impact of link failure from Bus 16 to Bus 17

The situation can be improved by increasing the timer duration. Fig. 5.6 shows the simulation

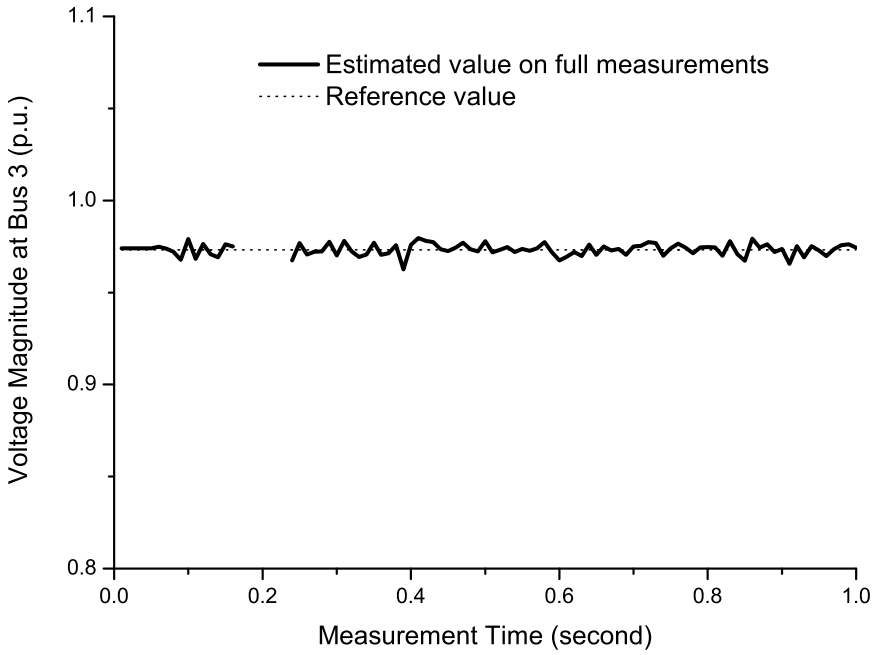


Figure 5.6: Impact of link failure from Bus 16 to Bus 17 when the Super PDC timer increases to 60ms

results of the same scenario except that the timer in the Super PDC is increased to 60ms. We can find that the estimator still lose the system observability for a short period of time. This is because the routers need to re-establish their routing tables after a link failure. During this time, the measurements cannot be sent to the destination properly. But after new routing paths are built, which usually can be done very fast, the state estimator can work normally again. This means increasing the PDC timer duration can effectively mitigate the impact of a link failure. However, if a link failure results in an islanding of the communication network, for instance Bus 16 to Bus 19, this solution will not work.

#### 5.2.3.2 Single Network Link Congestion

In this scenario, malicious traffic is assumed to be created at 0.2 second of the co-simulation and saturate the communication link from Bus 16 to Bus 17. The estimated results are shown in Fig. 5.7. We can find that the malicious traffic does not affect the state estimator immediately. Instead, it gradually saturates the link and the impact starts to show up around 0.42 second. At this point, the communication link is fully saturated and the measurements data

have to be buffered and wait longer to arrive at the Super PDC. Some of the measurements data are discarded due to timer expiration. However, in this particular case, the system state can still be recovered and estimated from other redundant measurements like current phasors. From the curves in Fig. 5.7 we can tell that the accuracy of the state estimation on partial measurements data still holds. But in general, link congestions can make the system unobservable just like the link failure scenario. As shown in Fig. 5.8, enhanced link saturation at the same place can completely blind the state estimator. To counteract this impact, the dynamic routing protocols should be able to detect the saturation level of the communication link and reroute the data proactively.

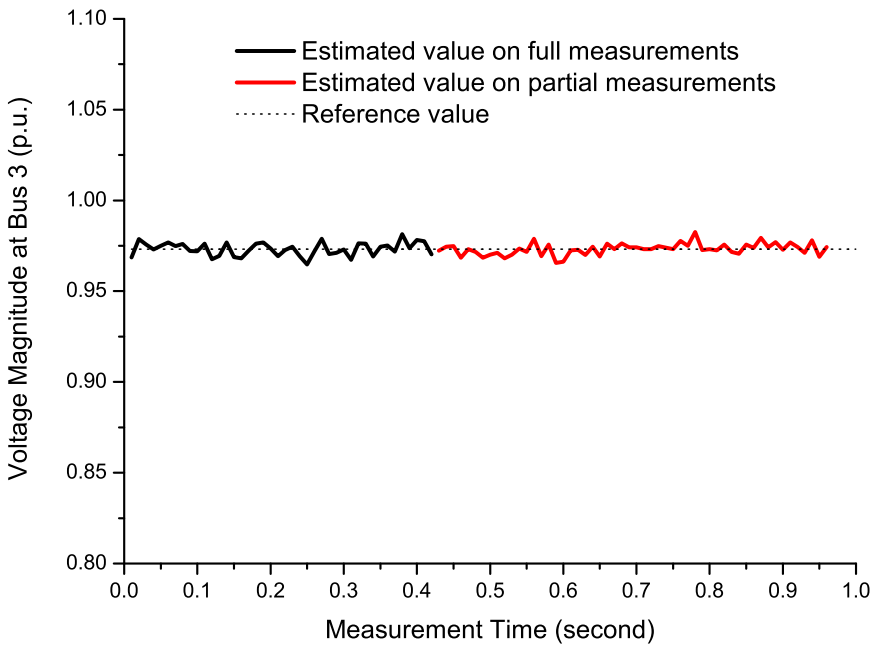


Figure 5.7: Impact of link saturation from Bus 16 to Bus 17

#### 5.2.3.3 Single Router Congestion

DoS attack can aim at a router in the system. Apparently, the most critical gateway router in the 39-bus system is the one which the Super PDC is directly connected to. In this scenario, we assume that at 0.2 second, 10 hacked computers in remote places in the system start to send redundant malicious data to the router at Bus 16 and expect to deplete its resource. The simulation results in Fig.5.9 shows the estimation results in this condition.

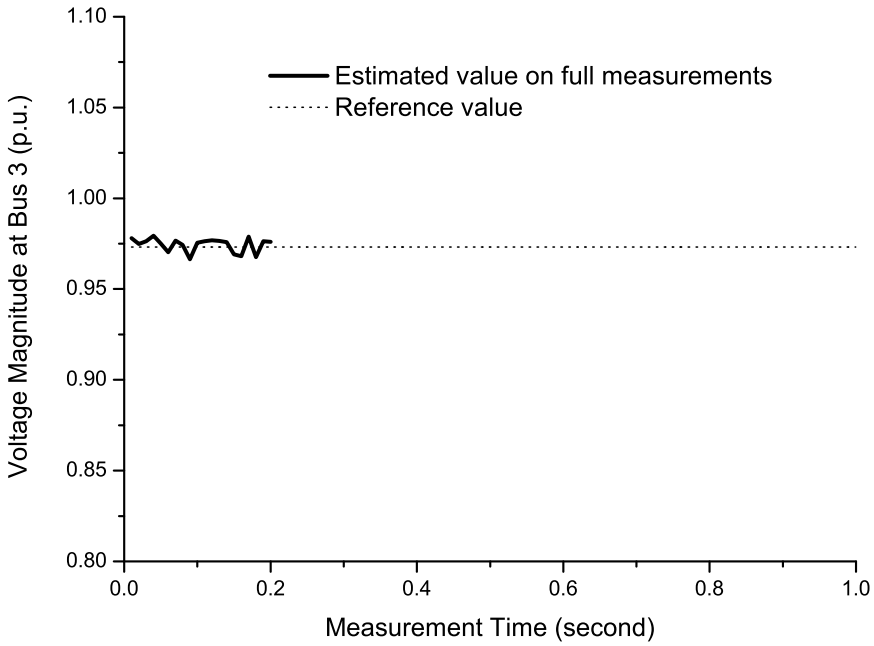


Figure 5.8: Impact of enhanced link saturation from Bus 16 to Bus 17

The behavior of the state estimator obviously becomes unstable and intermittent around 0.4 second. Sometimes the system becomes unobservable, but it may be able to recover for a short time as well. This is because when large amount of redundant data arrive at the router in a short period of time, the router can be overloaded such that the instantaneous input data exceeds the maximum processing throughput, which results in packet dropping. Fig.5.10 shows an enhanced DoS attack on Bus 16, which make the system totally invisible. In this case, backup routers in a dual-router setup can partially offset the impact of the DoS. Malicious traffic filtering or label the data packets with different priorities can also increase the robustness of the system.

#### 5.2.3.4 Data Spoofing in PMU

In this scenario, we assume that the PMUs at Bus 3 are all hacked and the phasors at this bus are all changed to a constant bogus value. More specifically, the hacked voltage magnitude at Bus 3 is fixed at 0.9 p.u., which is far from the reference value. We use co-simulation to see if it can really change the estimation results. Fig. 5.11 shows the estimation results in this condition. We can find that the estimated values at Bus 3 are slightly deviated from

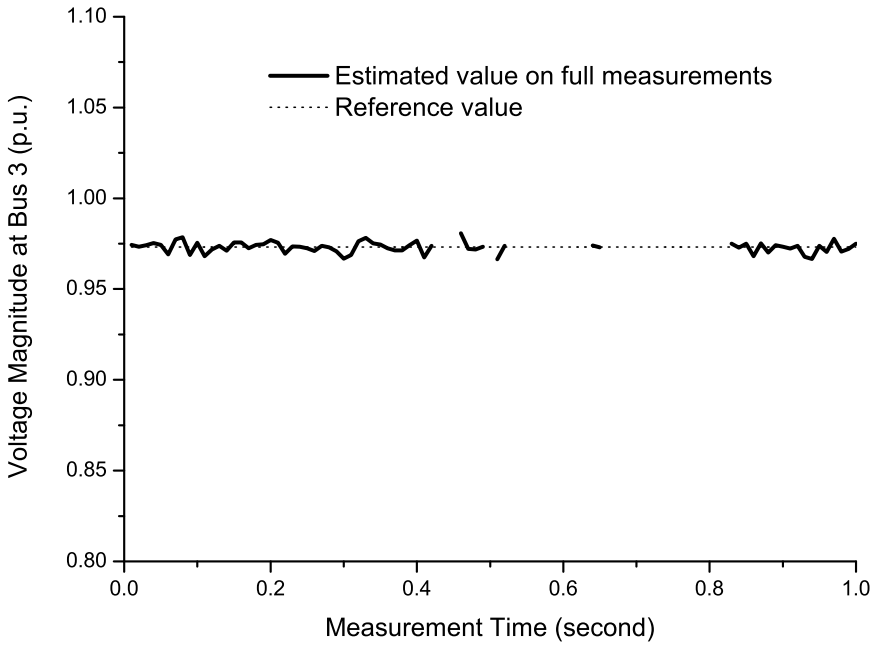


Figure 5.9: Impact of DoS attack on the router at Bus 16

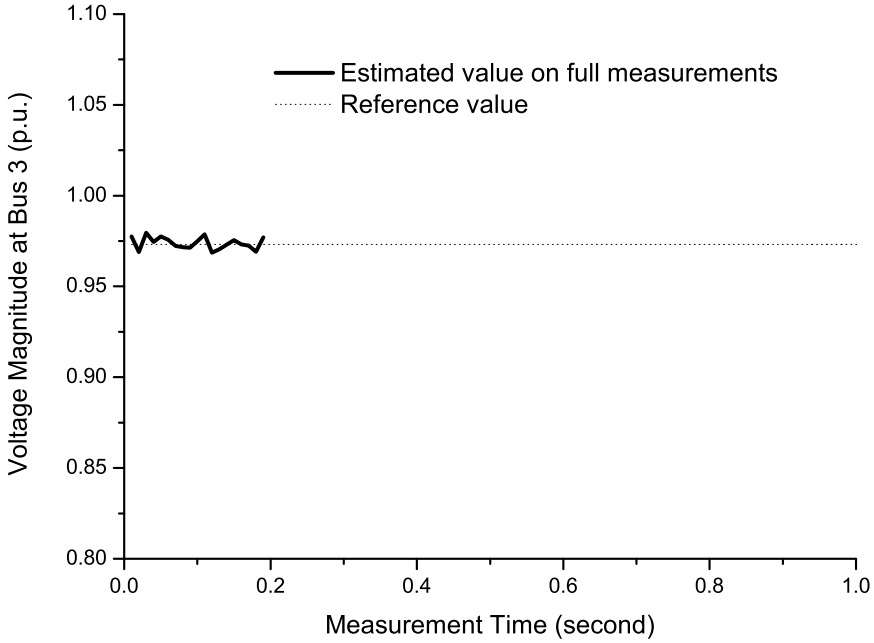


Figure 5.10: Impact of enhanced DoS attack on the router at Bus 16

the reference line but still far from the bogus value 0.9 p.u.. This result indicates that the all-PMU state estimator has some robustness against single PMU data spoofing.

We further test the impact of data spoofing when there is a fault in the power system. Here, a short-circuit short from Bus 4 to Bus 14 is created at 0.4 second and cleared at 0.45 second. The bogus voltage value at Bus 3 is still fixed at 0.9 p.u. The simulation result in Fig. 5.12 shows that the bogus value almost has no impact on the state estimator. This result further proves that the all-PMU state estimator is robust against single PMU data spoofing.

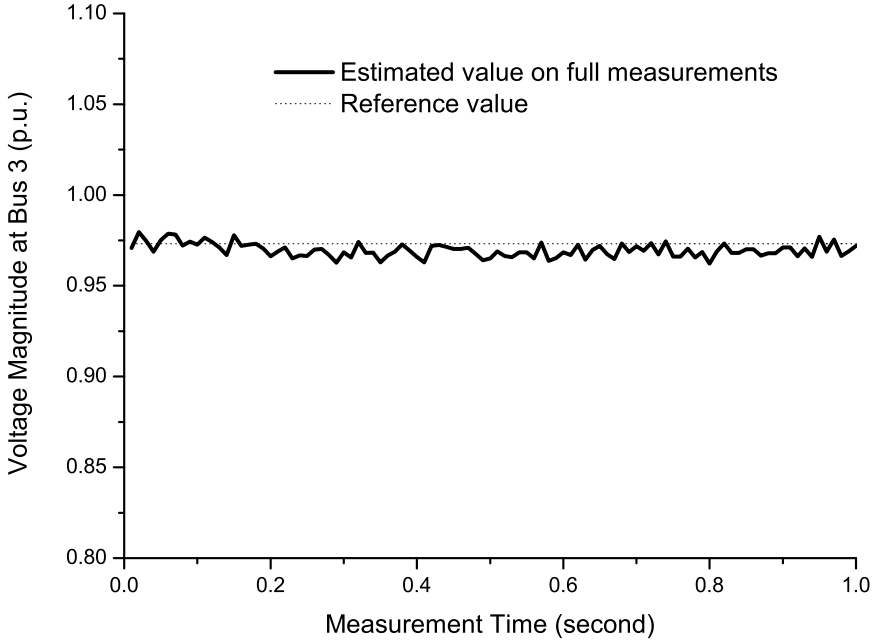


Figure 5.11: Impact of single PMU spoofing at Bus 3

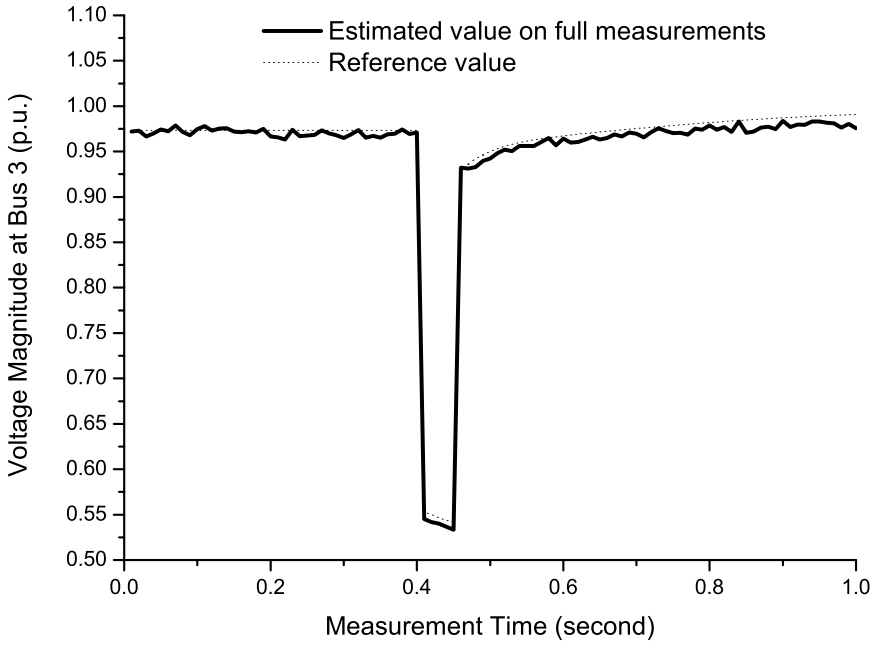


Figure 5.12: Impact of single PMU spoofing at Bus 3 and a short-circuit fault

# Chapter 6

# PMU-Based Out-of-Step Protection

Power system protection refers to the elaborate system of relays and other protection devices that limit damage to the power system equipment and maintain system stability, in the event of occurrence of faults or loss of major elements. The protection schemes are usually designed based on extensive time domain simulations. These systems are expected to detect events and act quickly (sometimes within milliseconds), but at the same time, ensure that such actions are not detrimental to secure and reliable operation of the grid. The advent of WAMS and better inter-substation communication makes it possible to greatly improve existing protection schemes.

One of the most complex protection schemes is the Out-of-Step (OOS) protection. OOS condition occurs when a generator or a group of generators lose synchronism with the rest of the system. Unless such groups of machines are isolated from the grid, it would result in large mechanical vibrations that could potentially damage these generating units. During OOS conditions, huge transient swings are observed at the interface between these out-of-synchronous areas and the rest of the network. Thus, traditional OOS relays detect these swings and open the tie-lines to prevent OOS operation [76]. With the availability of WAMS, these schemes can be made adaptive so that they are both dependable and secure, even in the event of drastic change in operating points due to severely stressed system conditions.

In this chapter, we will study the third case on GECO which is derived from an adaptive OOS scheme based on WAMS proposed in [7, 19].

## 6.1 Background

### 6.1.1 Power System Transient Stability

Power system stability refers to the ability of a power system to restore itself to the normal operating condition after perturbations. There are mainly two large categories of power system stability: voltage stability and angular stability. Voltage stability refers to the ability of the a power system to maintain a desired voltage magnitude. Angular stability refers to the ability of a power system to keep all the generators running in synchronism. Power system transient stability is a special type of angular stability which refers to the ability of the generators in the system to return to synchronism after a major disturbance within a few swings. And OOS protection protects the power system from transient instability.

The dynamic behavior of a generator can be described by the classic swing equation [1]:

$$\frac{2H}{\omega_{\mathtt{syn}}}\omega_{\mathtt{p.u.}}(t)\frac{d^2\delta(t)}{dt^2} = p_{m\mathtt{p.u.}}(t) - p_{e\mathtt{p.u.}}(t) = p_{a\mathtt{p.u.}}(t) \tag{6.1}$$

where
$H$ is the normalized inertia constant of the generator.
$\omega_{\mathtt{syn}}$ is the synchronous electrical radian frequency.
$\omega_{\mathtt{p.u.}}(t)$ is the per-unit electrical frequency.
$p_{m\mathtt{p.u.}}(t)$ is the mechanical power in per unit.
$p_{e\mathtt{p.u.}}(t)$ is the electrical power in per unit.
$p_{a\mathtt{p.u.}}(t)$ is the accelerating power in per unit.

Eqn(6.1) says the angular acceleration of a generator is proportional to the accelerating power. In a normal condition, the mechanical power equals to the electrical power, resulting in zero accelerating power. Therefore, the generator angle doesn't change and keeps in synchronism with others in the system. However, following a major disturbance, for example, a three-phase short-circuit fault, the electrical power output of the generator drops dramatically. Then the generator angle will deviate from its original value and lose synchronism. After the fault is cleared, the generators in the system may or may not be able to return to synchronism. For simple cases, based on the One-Machine-Infinite-Bus (OMIB) system model, the system transient stability can be inferred using the equal area criterion.

### 6.1.2 Equal Area Criterion

In a One-Machine-Infinite-Bus model, the entire power system is reduced to a synchronous machine connected to an equivalent infinite bus as displayed in Fig. 6.1. An infinite bus assumes that its voltage magnitude and phase angle are constant. This angle is set arbitrarily to zero. Then the output electrical power of the generator is

$$p_e = \frac{EV_{bus}}{X' + X} \sin \delta \tag{6.2}$$

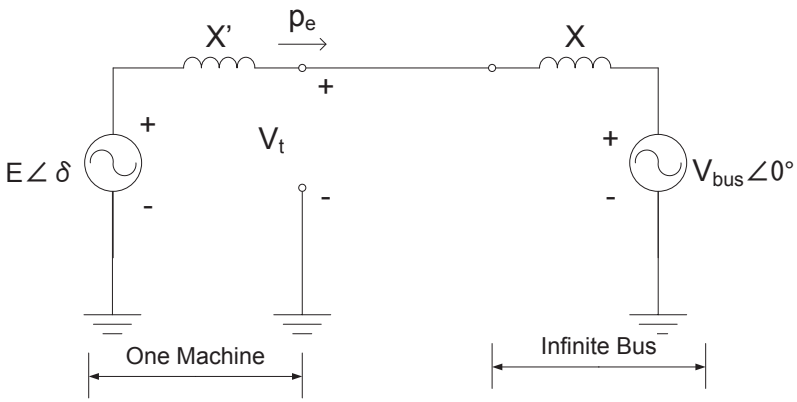


Figure 6.1: The OMIB model

Eqn(6.2) shows the relationship between the output power and the rotor angle of a generator. The plot of this relationship is shown in Fig. 6.2 which is usually called $p - \delta$ plot. Fig. 6.2 also shows a typical behavior of a generator following a major disturbance. The generator is assumed to work in normal condition with a rotor angle $\delta_0$. When a short-circuit fault occurs, the external electrical power drops dramatically and will drive the generator rotor angle to move forward according to Eqn(6.1). The rotor will keep accelerating until the fault is cleared by the tripping of the line circuit breakers and at this point the rotor angle reaches $\delta_c$. Then the rotor will start decelerating until it reaches a maximal value $\delta_m$. The equal area criterion states that, the power system maintains its transient stability if and only if the accelerating area $A1$ in Fig. 6.2 is smaller or equal to the decelerating area $A2$. The proof of equal area criterion can be found in [1].

On the other hand, if the fault is not cleared on time, then $\delta_c$ will move far away from $\delta_0$. In that case, $A1$ cannot be smaller than $A2$. Then the power system cannot hold transient

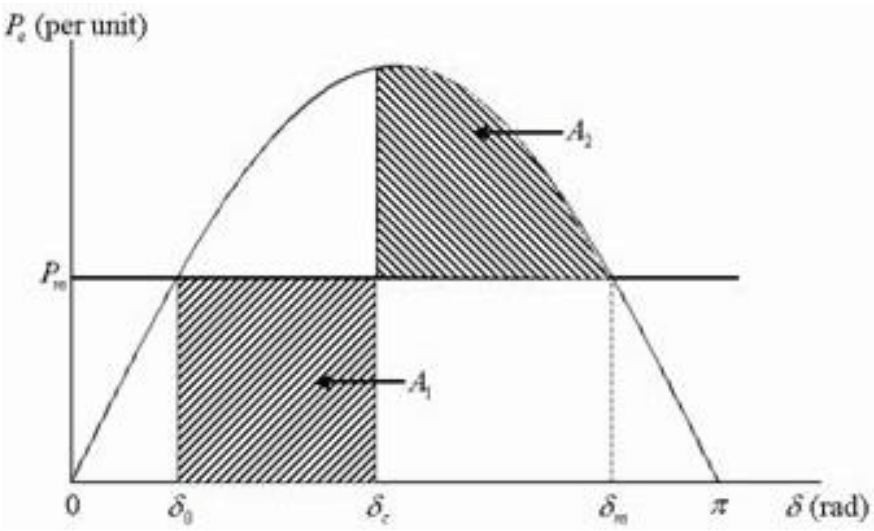


Figure 6.2: The $p - \delta$ plot and the equal area criterion [3]

stability any more. Oscillation between groups of generators which is also called Out-of-Step (OOS) condition can be observed. In a multi-machine system, groups of machines tend to oscillate coherently, against each other. As long as the OOS condition is identified, the oscillating coherent groups must be islanded to prevent further breakdown of the system.

### 6.1.3 Out-of-Step Condition

There are many ways to identify the OOS condition [19]. One effective method is to run time-domain dynamic simulations and monitor the generator angles. If the rotor angles of a group of coherent generators deviate from others up to a threshold, then an OOS condition can be identified. The OOS condition can be better illustrated using an example in the New England 39-bus system as shown in Fig. 6.3. To create an OOS condition, a three-phase short-circuit fault is placed on transmission line 27 which connects Bus 21 and Bus 22 [77]. If the fault is cleared in 0.1 second, then the system can restore to normal condition according to the equal-area criterion. This is shown in Fig. 6.4. However, if the fault is cleared in 0.3 second, an OOS condition is observed in the system, which is depicted in Fig. 6.5. In this condition, the generators at Bus 35 and Bus 36 lose synchronism with other generators in the system. Therefore, two coherent groups of generators are formed, which is shown in Fig. 6.3. The system has to be islanded to avoid further damage or collapse [76].

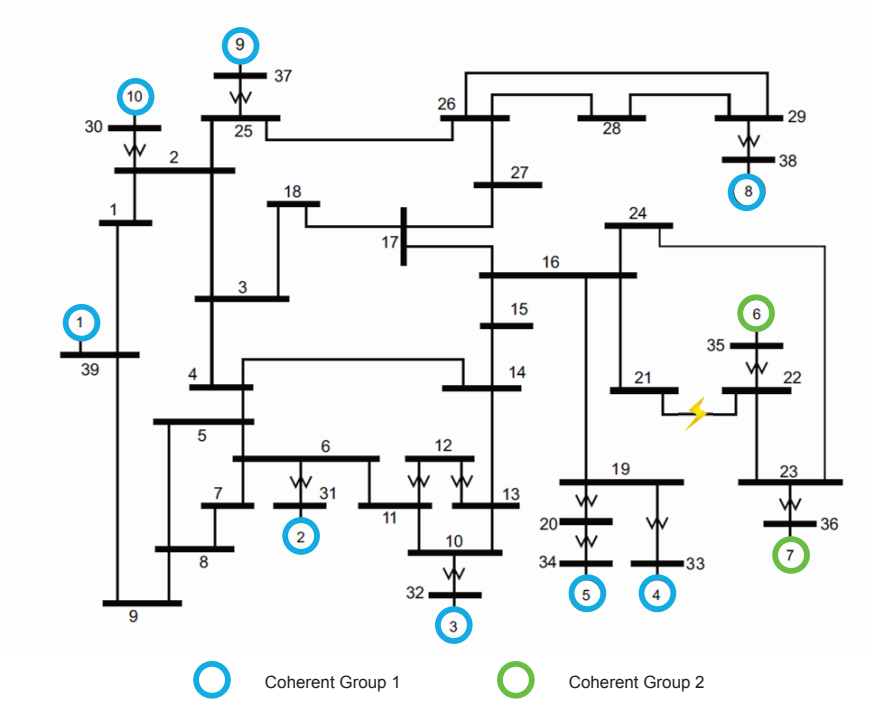


Figure 6.3: OOS condition in the New England 39-bus system [2]

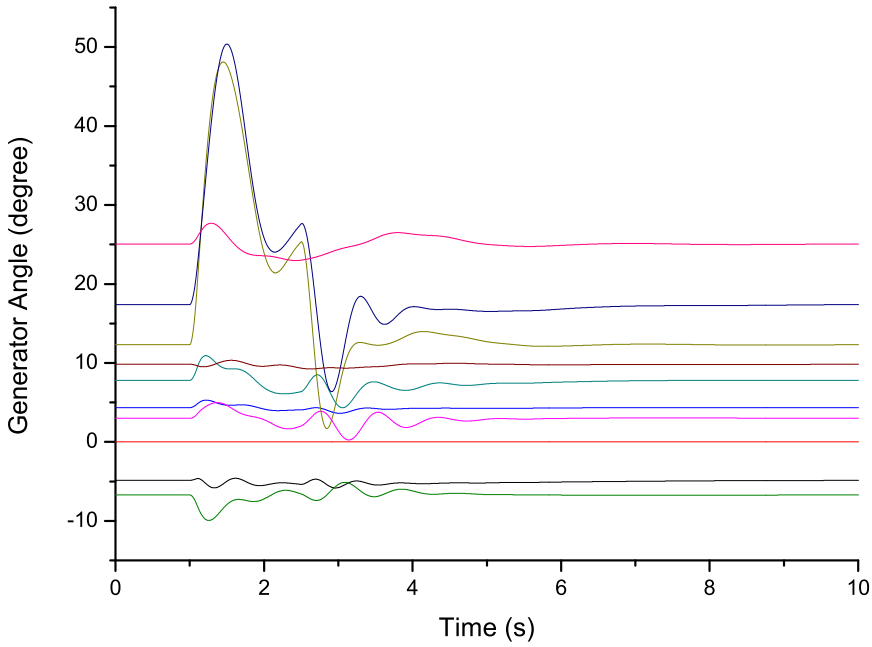


Figure 6.4: Fault cleared in 0.1 second, system back to normal condition

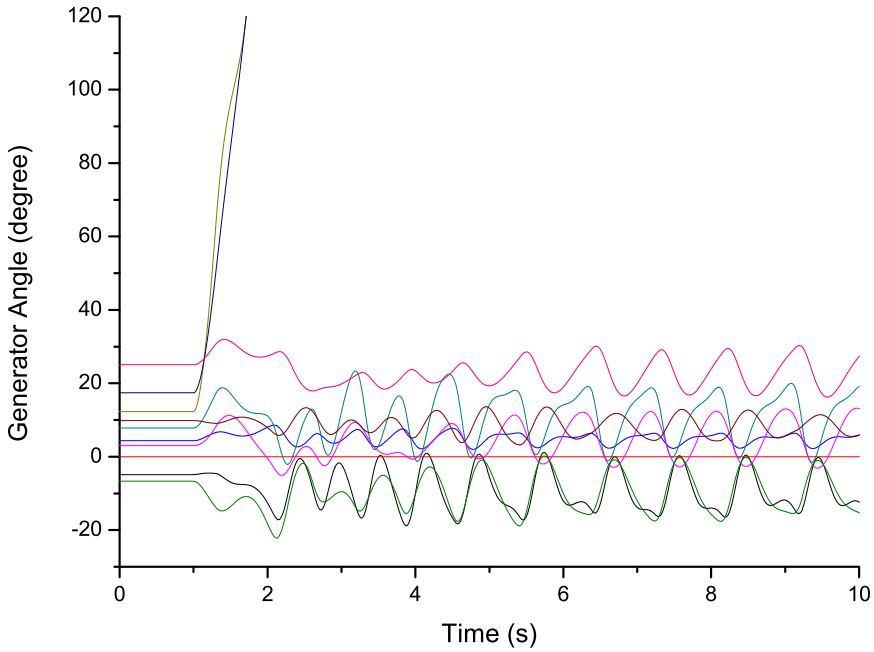


Figure 6.5: Fault cleared in 0.3 second, OOS condition is observed

## 6.2 PMU-Based Out-of-Step Protection

Compared to the traditional OOS protection schemes, the invention of PMU brings great potential to design more effective OOS protection schemes. In [19], a PMU-based OOS protection scheme is proposed. It shows that it is possible to measure the rotor angles by an adequate deployment of PMUs. Therefore, instead of offline dynamic simulation, the rotor angles can be monitored in real time and sent to a central control via wide-area measurement system (WAMS). The central controller then can identify if OOS condition and coherent generator groups is formed based on those direct measurements. OOS condition is determined if the difference in the centers-of-angle exceeds 120 degree [7]. System islanding will be performed if necessary. Although in this scheme, the OOS condition is identified using WAMS, the monitored coherent generator groups and proper islanding locations are still determined by offline simulations or existing plans. In this section, we will propose a PMU-based OOS protection scheme, which can identify OOS condition and perform system islanding in real time.

Our PMU-based OOS protection schemes consist of several steps. First, coherent generator

groups have to be discovered from raw generator rotor angle measurements. Second, given two coherent generator groups, we have to find an optimal islanding solution to divide the system into two parts. Usually we need to find a set of transmission lines and trip them. Third, it is likely that there are more than two coherent generator groups in the system. Then step 1 and 2 have to be called recursively to further island a subsystem. Based on the technique introduced in [19], we will assume that the rotor angles can be directly measured.

### 6.2.1 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. Clustering algorithm is widely used in research areas like: data mining, machine learning, statistics etc.. Hierarchical clustering and k-means clustering are typical clustering algorithms. Hierarchical clustering can be done in bottom-up manner ($O(n^3)$ complexity) or top-down manner($O(2^n)$ complexity) while k-means clustering is usually NP-hard. However, in real power system, the rotor angles of the coherent generators are usually close to each other. Therefore, a simple but efficient algorithm can be used for identifying coherent generator groups which is shown in Fig. 6.6. We assume the measured rotor is stored in an array $A$ whose indices denotes the numbers assigned to the generators. For example, the rotor angle of generator 1 is stored in $A[1]$.

The algorithm in Fig. 6.6 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. The generators in front of this gap is stored in set $S$ and the others is stored in $T$. If no OOS condition is identified, $T$ will be empty. If the number of generators of interest is $n$, then this algorithm runs in $O(n \log n)$.

An alternative algorithm is shown in Fig. 6.7 which processes the measured rotor angle one by one. For each generator, the algorithm tries to match a proper cluster for it by comparing its measured rotor angle and the mean values of existing clusters. If one of the differences is smaller than a threshold, for example 120 degrees, then the algorithm will put this generator into the matching cluster. If not, the algorithm will establish a new cluster holding the current generator. After having processed all the rotor angles, the generators in the largest cluster are placed in $S$ and the others are placed in $T$. This algorithm runs between $\Omega(n)$

**CoherentGroup1**($A$) returns $S, T$

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

Figure 6.6: Coherent group identification algorithm 1

and $O(n^2)$ depends on $A$. The results of these two algorithms can differ slightly. In our case study, we use the first algorithm.

### 6.2.2 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 $T$. Here a cut stands for a set of transmission lines to be tripped and the number of these transmission lines has to be minimized. This problem is closely related to the $s - t$ min-cut problem in graph theory [78]. Fig. 6.8 shows an example of how to convert the coherent generator groups islanding problem to the equivalent $s - t$ min-cut problem on a flow network. The flow network is defined as [78]

**Definition 1** (Flow Network)**.** *A flow network is a digraph $G = (V, E)$ with two distinguished vertices: a source $s$ and a sink $t$. Each edge $(u, v) \in E$ has a non-negative capacity $c(u, v)$. If $(u, v) \notin E$ then $c(u, v) = 0$.*

Then as shown in Fig. 6.8, the power system is first converted to a flow network $G$. The

**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 $T$

Figure 6.7: Coherent group identification algorithm 2

capacity of each edge can be assumed as one for simplicity. Two coherent generator groups is represented by $S$ and $T$, which is obtained from the clustering algorithm in the previous section. Then, a new flow network $G'$ is constructed as follows: two new vertices $s'$ and $t'$ are added to $G$ and new edges connect $s'$ to $S$ and $t'$ to $T$ are added as well. The capacity of the new added edges is assigned to infinity. It is apparent that the $s' - t'$ min-cut in $G'$ is the min-cut for the original islanding problem since the new added edges has infinite capacity and cannot be part of the cut.

The $s - t$ min-cut problem can be solved by first solving the $s - t$ max-flow problem and then the min-cut can be found from the max-flow result since the two problems are closely related according to the max-flow min-cut theorem [78]. The max-flow problem can be efficiently

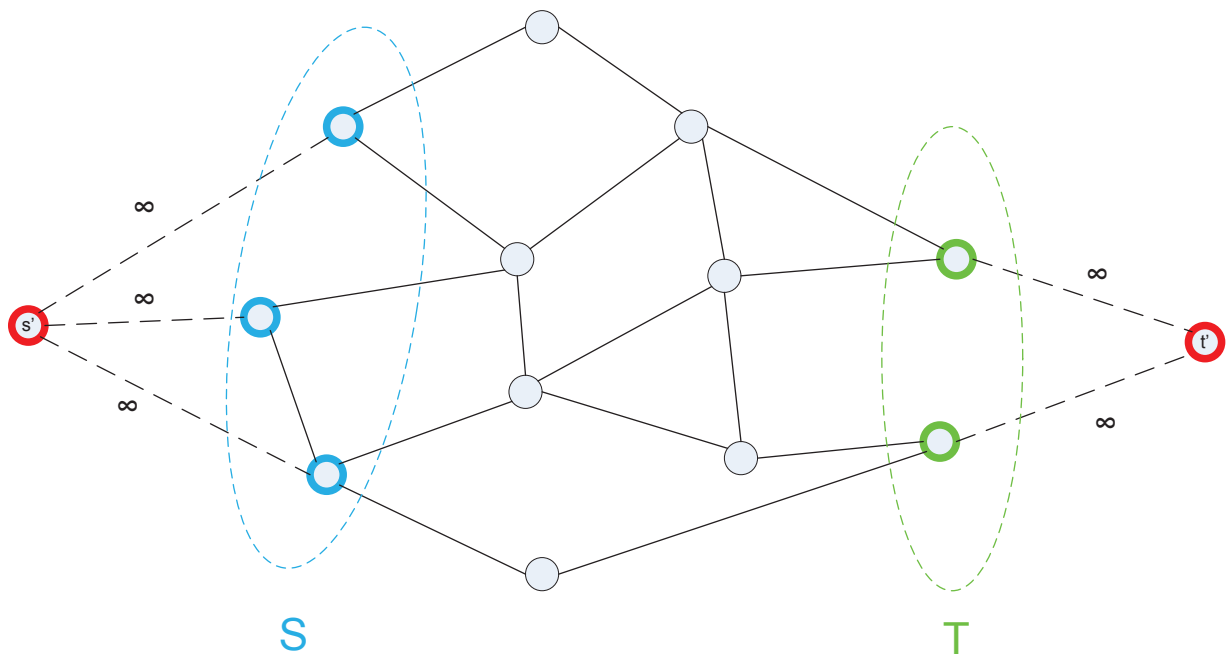


Figure 6.8: Equivalence of islanding to $s-t$ min-cut problem

solved by Edmonds-Karp algorithm [78]. To explain how the algorithm works, we need to introduce several definitions and lemmas first.

**Definition 2** (Net Flow)**.** *A net flow on a flow network $G = (V, E)$ is a function: $f : V \times V \to \Re$ satisfying*

1. *Capacity constraint:* $f(u, v) \leq c(u, v) \quad \forall u, v \in V$
2. *Flow constraint:* $\sum_{v \in V} f(u, v) = 0 \quad \forall u \in V - \{s, t\}$
3. *Stew symmetry:* $f(u, v) = -f(v, u) \quad \forall u, v \in V$

**Definition 3** (Flow Value)**.** *The value of the net flow, denoted by $|f|$, is $|f| = \sum_{v \in V} f(s, v) = \sum_{u \in V} f(u, t)$*

**Definition 4** (Cut)**.** *A cut $(S, T)$ is a partition of $V$ such that $s \in S$ and $t \in T$. The total capacity across this cut is denoted by $c(S, T)$.*

**Lemma 1.** *The flow across a cut $f(S, T) = |f|$ for any cut $(S, T)$.*

**Lemma 2.** *The value of any flow is bounded above by the capacity of any cut:* $f(S,T) \leq c(S,T)$.

**Definition 5** (Residual Network)**.** *Let $f$ be a flow on $G = (V,E))$. The residual network $G_f(V_f, E_f)$ is the graph with strictly positive residual capacities $c_f(u,v) = c(u,v) - f(u,v) > 0$.*

**Definition 6** (Augmenting Path)**.** *Given a flow $f$ on $G = (V,E))$ and its residual network $G_f$, any path $p$ from $s$ to $t$ in $G_f$ is an augmenting path in $G$ with respect to $f$. The flow value can be increased along the augmenting path by $c_f(p) = \min_{(u,v)\in p} \{c_f(u,v)\}$.*

With these knowledge in hand, then the max-flow min-cut theorem can be introduced:

**Theorem 1** (Max-Flow,Min-Cut)**.** *The following statements are equivalent:*

1. $|f| = c(S,T)$ *for some cut* $(S,T)$
2. $f$ *is a max flow*
3. $f$ *admits no augmenting path*

The max-flow min-cut theorem actually suggests a simple algorithm to calculate the maximum flow in a flow network. That is, given an initial flow on $G$, find an arbitrary augmenting path in its residual network $G_f$ and augment the flow along this path. This process will be recursively called until there is no augmenting path. And at this stage, according to the three equivalent statements in max-flow min cut theorem, the current flow is the max flow in the network. This algorithm is called Ford-Fulkerson algorithm. However, this algorithm finds an arbitrary augmenting path and in some cases it can be very slow [78]. The Edmonds-Karp algorithm improves its implementation. The only difference is that the Edmonds-Karp algorithm uses breadth-first-search (BFS) to find an augmenting path and it is proved that Edmonds-Karp algorithm is bounded by $O(|V||E|^2)$ [78].

The Edmonds-Karp algorithm is not the fastest algorithm to solve the max-flow problem. The fastest algorithm so far is proposed in [79] whose complexity is bounded by $O(\min(V^{\frac{2}{3}}, \sqrt{E})E \log \frac{V^2}{E} \log U)$. However, Edmonds-Karp algorithm is easier to implement and the computation time is trivial for small scale systems. Therefore, Edmonds-Karp algorithm is used in our experiments.

As long as the max flow of the network is obtained. The minimum cut can be found by traversing the final residual network starting from $s$. All the vertices that can be reached from $s$ form a min-cut. This can be shown using an example shown in Fig. 6.9. In this figure, the capacities of all the original edges are assumed as 1. Then Fig. 6.9 shows one max-flow solution of this network. Fig. 6.10 shows the residual network for this max-flow. In this figure, the residual capacities are omitted and only the available paths are displayed. We can find a min-cut by traversing from $s'$ and Fig. 6.10 shows a min-cut of four edges.

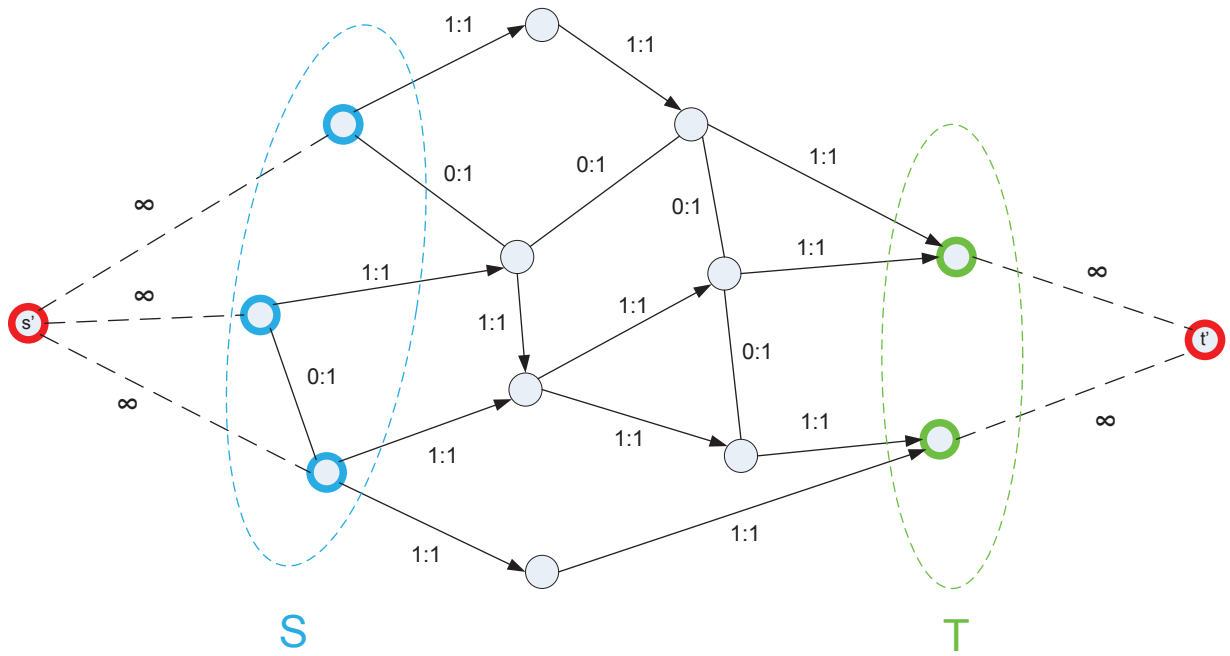


Figure 6.9: A max-flow example

The entire islanding algorithm is summarized in Fig. 6.11. The runtime of this algorithm is bounded by Edmonds-Karp algorithm which is $O(|V||E|^2)$. For power system of 30,000 buses and 45000 lines, this algorithm requires about 2 minutes in the worst case on a 170 GIPS (Giga instructions per second) CPU (Intel Core i7 Extreme Edition 3960X). This time seems too long for OOS protection. However, if the fastest algorithm in [79] is used, the runtime will be expected to be less than 10ms. The calculation speed can also be improved by parallelism. Therefore, the islanding algorithm is possible to find a solution within several swings.

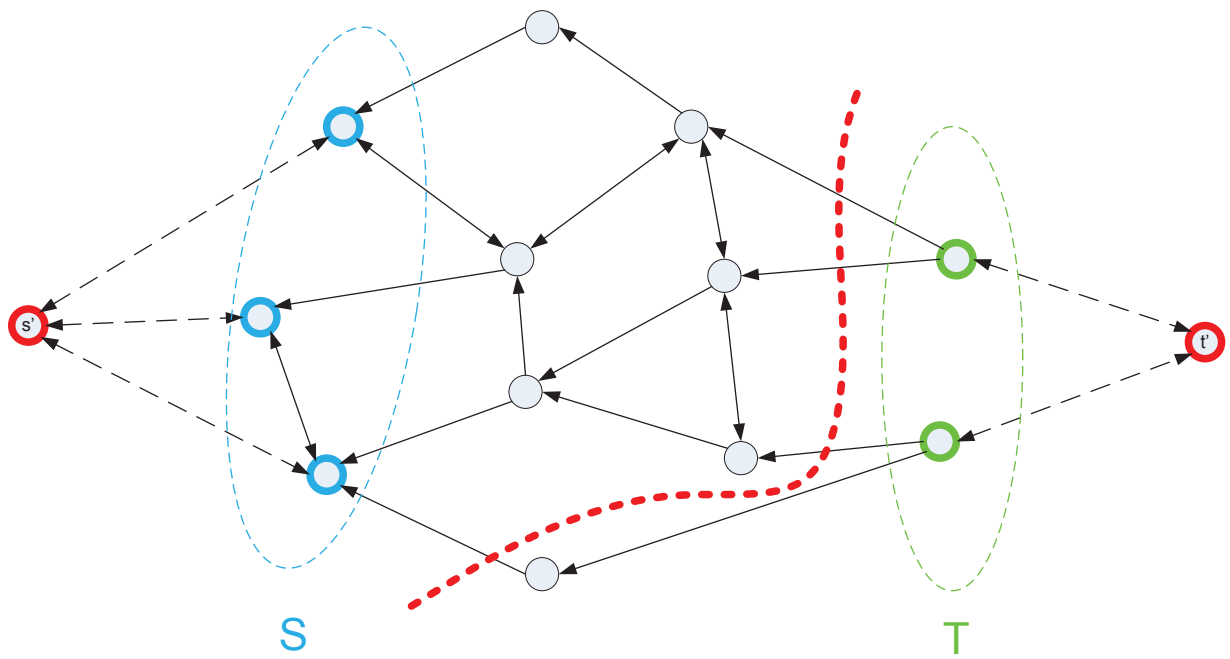


Figure 6.10: Find the min-cut on the residual network

---

**Islanding**($G$,$S$,$T$) returns $G1, G2$

---

1. build a new graph $G'$ by adding new vertices $s', t'$
2. run EdmondsKarp($G'$,$s'$,$t'$) returning max flow $F$
3. find min-cut using $F$ and $G'_F$

---

Figure 6.11: Islanding algorithm

### 6.2.3 Recursive OOS protection

It is possible that there exists more than 2 coherent generator groups in the system [19]. Therefore they must be islanded one by one. The algorithm used in previous sections can be recursively applied to the islanded subsystems until no more OOS condition can be observed. However, this is a very complicated problem which needs more research study.

So far, we equally assign the edge capacity to 1. In a real power system, the weight of each transmission line can be different since the load is distributed. The candidates for weighing the capacity includes real power flow on the transmission line or the current on the transmission line. These values can be collected in real time by the WAMS at the same time with the rotor angles. This can be another potential improvement on the proposed OOS protection scheme.

## 6.3 Co-Simulation on GECO

The OOS protection scheme introduced in the previous section is co-simulated on GECO in this section. Again, we implement the OOS protection scheme on the New England 39-bus system to study the influence of the communication constraints on effective operation of such a scheme. Similar to previous chapters, the communication network is assumed to have the same topology as the power system. PMUs are placed at the generator buses to measure the rotor angles. A central OOS controller is placed at Bus 16 to collectively monitor the rotor angle trajectories. A timer of 50ms is associated with the central controller for the same purpose as the timer in PDCs or the SPDC.

The OOS condition described in Fig. 6.3 is used to test the protection scheme. A three-phase fault is initialized on the transmission line connecting Bus 21 and Bus 22. After the fault is cleared, machines on Bus 35 and Bus 36 lose synchronism. By the nature of their rotor angle trajectory, it is concluded that these two machines form a coherent group of machines. The rotor angles of all the machines are recorded and the centers of angles of all the coherent groups are calculated. When the difference between the centers of angles reaches 120 degrees, existence of OOS conditions is confirmed and the transmission line 23 (connecting Bus 16-24) and 24 (connecting Bus 16-21) are opened, forming an island that consists of generators on Bus 35 and Bus 36. The circuit breaker operating times are not included in this co-simulation. Since the system scale is small, the computation time of the coherent group algorithm and the islanding algorithm is trivial as well.

The response of the generators to the events described above can be observed from the real power outputs and rotor angles of the generators. Fig. 6.12 and Fig. 6.13 show the co-simulation results of the OOS protection scheme. The communication bandwidth is 1Gbps

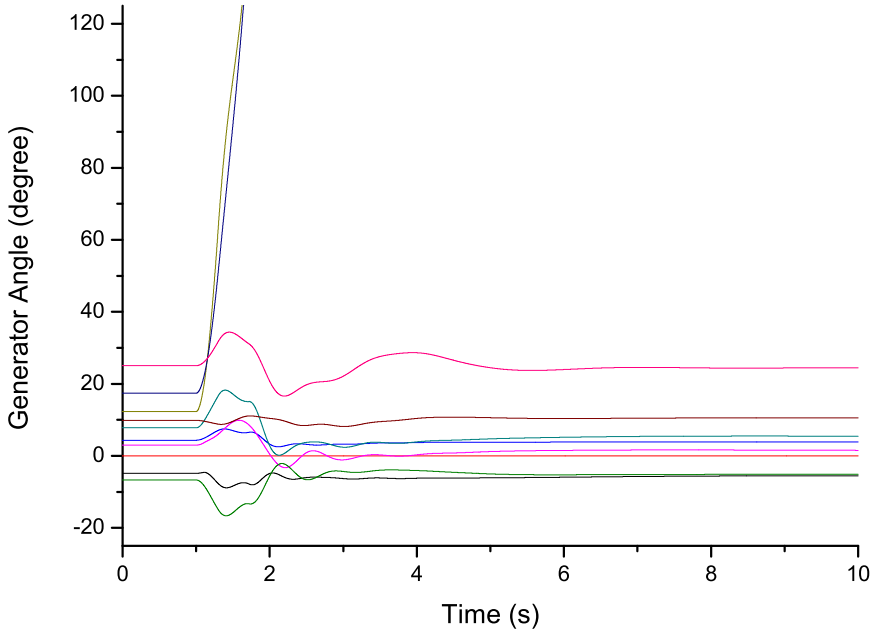


Figure 6.12: Generator angels showing OOS condition (BW=1Gbps, D=5ms)

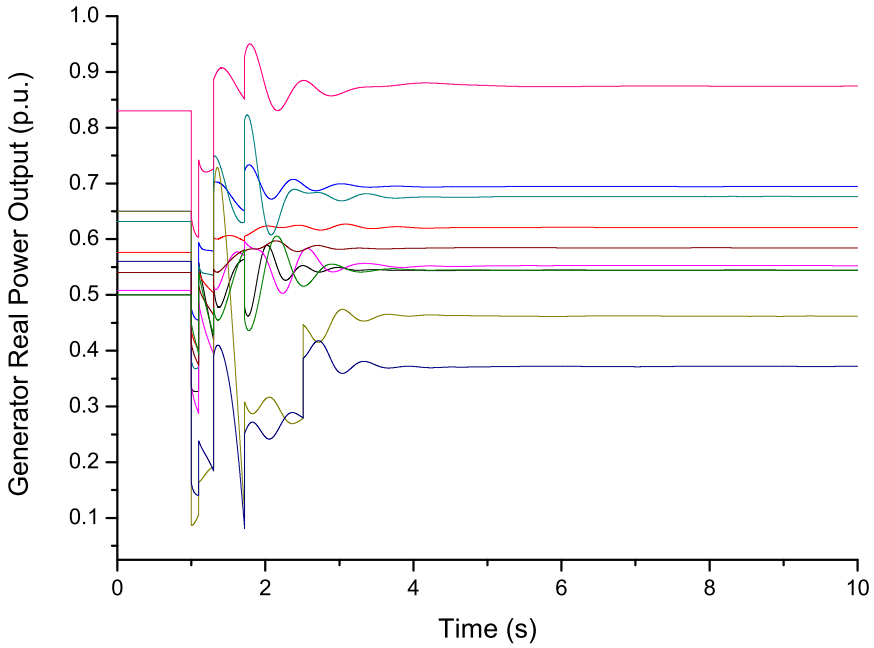


Figure 6.13: Generator real power outputs (BW=1Gbps, D=5ms)

and delay is 5ms. A three-phase fault is placed at 1.0 second on the line and the fault is cleared around 1.3 second by opening the circuit breakers on the line. Then, the generators

experience transient oscillations. The rotor angles in Fig. 6.12 show that the generators on Bus 35 and Bus 36 split from the rest of the generators, while remaining together themselves. The phenomenon is sensed by the central controller and islanding commands are issued to the circuit breakers at the line connecting Bus 16 and Bus 24 and the line connecting Bus 16 and Bus 21. These two lines are finally open around 1.71 second. After the out-of-step split, the rotor angle trajectories of these two generators separate faster from the rest of the system. This event can be observed in the power output of the generators as a spike at the same time as shown in Fig. 6.13. The real output of the power will come back to a stable condition at 4.95 seconds after a series of oscillations. After the split, the bigger island operates at a reduced frequency of 59.87Hz while the smaller island is over-generated, resulting in a frequency of 60.6 Hz.

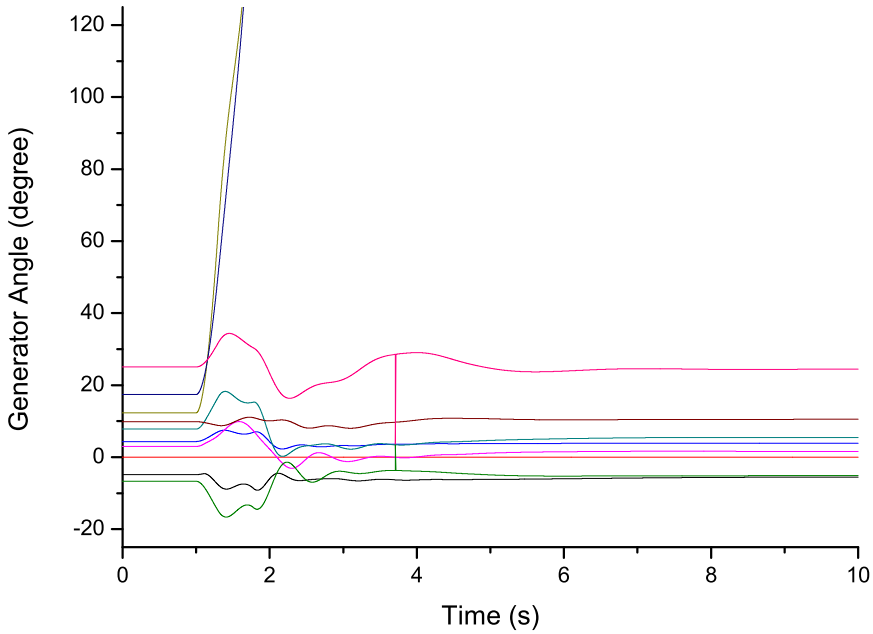


Figure 6.14: Generator angels showing OOS condition (BW=100Mbps, D=10ms)

The OOS protection scheme is further stress tested on an inferior communication network where the bandwidth is 100Mbps and the delay is 10ms for each link. The co-simulation results in this condition are plotted in Fig. 6.14 and Fig. 6.15. The results show that the scheme can still restore the system, but with a slower response. The OOS separation is at 1.77 seconds and the system return to stability around 5.02 seconds. This slower response results in larger spike compared to Fig. 6.13, which could potentially damage system devices

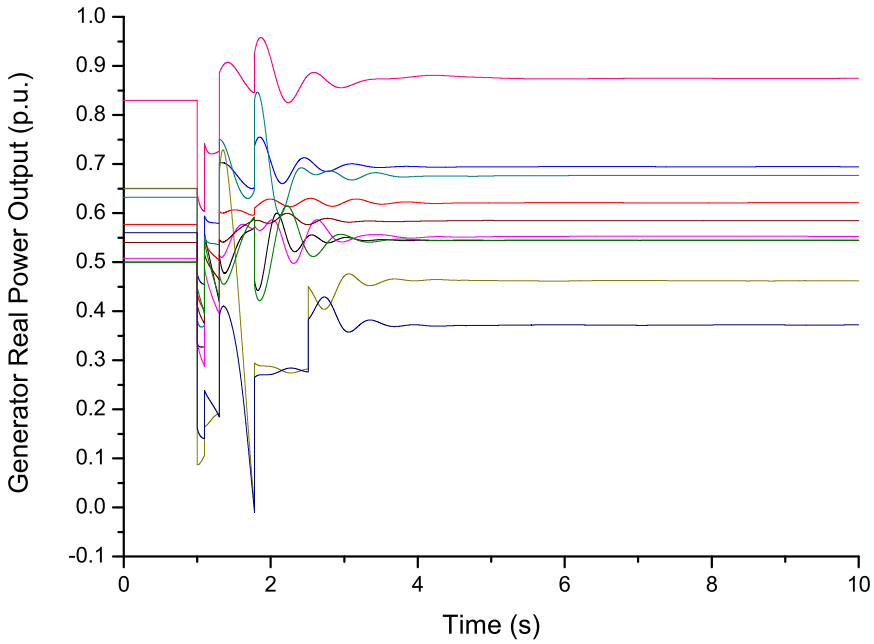


Figure 6.15: Generator real power outputs (BW=100Mbps, D=10ms)

in practice.

For the same network, if a communication link failure is also considered in the co-simulation, the results will be totally different. The rotor angles and real power outputs of the generators, after a communication link failure occurs following the short-circuit fault, are plotted in Fig. 6.16 and Fig. 6.17. It can be concluded that the OOS protection scheme fails to form the islands. This is because the average phasor transmission delay will be increased after the network loses an critical path. Some of the angle measurements cannot reach the central controller before its timer expires. Therefore, better communication network or longer timer is required to secure the protection scheme in this scenario.

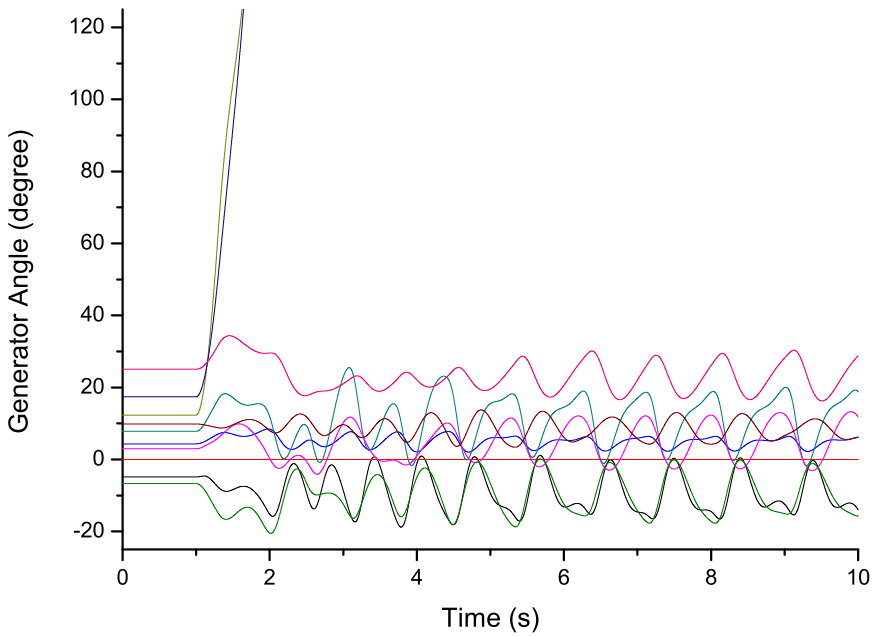


Figure 6.16: Generator angels with link failure (BW=100Mbps, D=10ms)

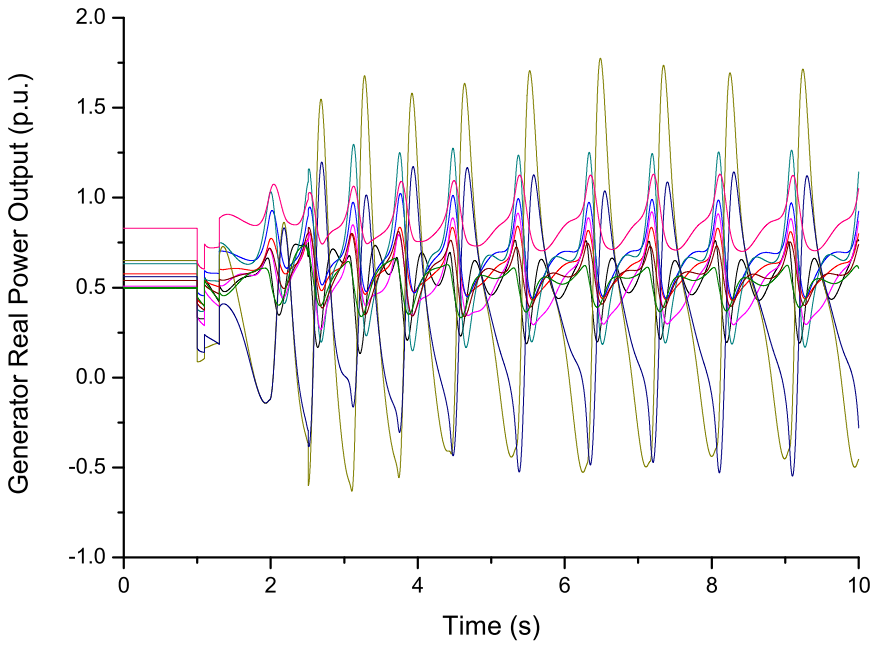


Figure 6.17: Generator real power outputs with link failure (BW=100Mbps, D=10ms)

# Chapter 7

# Conclusion and Future Work

This dissertation studies the problem of power system and communication network co-simulation, which is in great need in the smart grid research area. This dissertation proposes a new co-simulation framework GECO using a global event-driven mechanism. GECO can be seen as a universal design pattern for hybrid system simulation. It accurately synchronizes the simulation time across several simulator processes, therefore providing better simulation fidelity. Using a global priority queue to hold the simulation events from power system simulator and communication network simulator is the key for implementing the framework. The implementation of GECO in this dissertation consists of PSLF and NS2.

In addition, communication-based power system applications are proposed and studied on GECO. First, a communication-based distance relay protection scheme is proposed. Via real time communication among relay agents, the proposed protection scheme achieves faster backup remote protection than traditional schemes and is robust against hidden failure. The proposed protection scheme is also non-intrusive so that it can improve the current relaying infrastructure with modest upgrade. Then, the impact of communication infrastructure on the all-PMU state estimator is studied on GECO. Critical conditions for reliable system monitoring are found using sensitivity analysis on key network parameters. The results show the vulnerability of the all-PMU state estimator. Last, a new PMU-based Out-of-Step protection scheme is proposed. The proposed scheme can automatically identify coherent groups of machines, identify OOS condition and apply islanding strategy using proposed clustering algorithm and islanding algorithm. The scheme has the potential to be applied to

large-scale complex power systems when offline simulations are not sufficient to include all kinds of system contingencies.

The proposed power system applications requires a wide-area infrastructure which consists of interconnected power system and communication network. Without a co-simulation platform like GECO, the applications cannot be properly investigated. This dissertation fills the gap and enables the study of WAMS applications which have not been seen before.

The research work introduced in this dissertation can be extended in multiple directions:

1. **Improvement on GECO**
   The current implementation of GECO integrates PSLF and NS2. There are many other available simulators in the market that are potentially better than PSLF and NS2. For example, as for power system simulators, there are PSS/E, PSCAD/EMTDC, InterPSS etc.. As for communication network simulators, there are NS3, OPNET, QualNet etc.. These candidates have better user interface and richer libraries. Therefore, integrating them into GECO framework can potentially improve the user experience. Furthermore, the current implementation requires two independent processes busy-waiting for each other which makes the simulation very slow. Better inter-process communication method should be studied to improve the simulation speed.

2. **Improvement on Case Study I**
   Current decision making in the communication-based distance relay protection scheme is simple. More complete and convincing real time decision making policy is desired. When a fault happens in the system, multiple backup relays can sense the fault and each of them is likely to communicate with the master agent or peer agent to make protection decision. It is important to learn how to limit the tripping cost when only one tripping among the relay agents is sufficient.

3. **Improvement on Case Study II**
   Current simulation cases consider single network contingencies. More complex contingency or cyber attacks should be evaluated for further test the vulnerability of the estimator. The network infrastructure in the simulation cases is hypothetical. It is better to include real networks used in utilities to enhance the simulation fidelity. Also, different system topologies can be considered.

4. **Improvement on Case Study III**

   The proposed scheme is validated on a small scale system with exact two coherent groups. To further study the proposed scheme, much larger system should be considered. The ability to handle more than two coherent groups of the protection scheme needs to be verified. It is important to know if recursively applying the islanding algorithm can properly maintain the system stability. Also, real time transmission line weight should be considered. For example, real time power flow or current value can be used as the line weight in the islanding algorithm.

# Bibliography


[1] J. Duncan Glover, Mulukutla S. Sarma, and Thomas J. Overbye. *Power System Analysis and Design*. Cengage Learning, 2011.

[2] I. Hiskens. Significance of load modeling in power system dynamics. In *the x symposium of specialists in electric operational and expansion planning*, 2006.

[3] *http://nptel.iitm.ac.in/courses/Webcourse-contents/IIT-KANPUR/power-system/chapter_9/9_4.html*.

[4] A. G. Phadke and R. M. de Moraes. The wide world of wide-area measurement. *IEEE Power and Energy Magazine*, 6(5):52–65, 2008.

[5] D. Karlsson, M. Hemmingsson, and S. Lindahl. Wide area system monitoring and control - terminology, phenomena, and solution implementation strategies. *IEEE Power and Energy Magazine*, 2(5):68–76, 2004.

[6] Wei Zhang, M. S. Branicky, and S. M. Phillips. Stability of networked control systems. *IEEE Control Systems Magazine*, 21(1):84–99, 2001.

[7] A. G. Phadke and J. S. Thorp. Communication needs for wide area measurement applications. In *Proc. 5th Int Critical Infrastructure (CRIS) Conf*, pages 1–7, 2010.

[8] National power grid simulator workshop report. Technical report, U.S Department of Homeland Security, 2008.

[9] J. De La Ree, V. Centeno, J. S. Thorp, and A. G. Phadke. Synchronized phasor measurement applications in power systems. *IEEE Transactions on Smart Grid*, 1(1):20–27, 2010.

[10] Harry Perros. *Computer Simulation Techniques - The Definitive Introduction.* 2009.

[11] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly. Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, 21(6):11–25, 2001.

[12] Zhaoxia Xie, G. Manimaran, V. Vittal, A. G. Phadke, and V. Centeno. An information architecture for future power systems and its reliability analysis. *IEEE Transactions on Power Systems*, 17(3):857–863, 2002.

[13] M. Chenine and L. Nordstrom. Modeling and simulation of wide-area communication for centralized PMU-based applications. *IEEE Transactions on Power Delivery*, 26(3):1372–1380, 2011.

[14] J. W. Stahlhut, T. J. Browne, G. T. Heydt, and V. Vittal. Latency viewed as a stochastic process and its impact on wide area power system control signals. *IEEE Transactions on Power Systems*, 23(1):84–91, 2008.

[15] Kun Zhu, M. Chenine, and L. Nordstrom. ICT architecture impact on wide area monitoring and control systems' reliability. *IEEE Transactions on Power Delivery*, 26(4):2801–2808, 2011.

[16] K. Hopkinson, Xiaoru Wang, R. Giovanini, J. Thorp, K. Birman, and D. Coury. EPOCHS: a platform for agent-based electric power and communication simulation built from commercial off-the-shelf components. *IEEE Transactions on Power Systems*, 21(2):548–558, 2006.

[17] J. Nutaro, P. T. Kuruganti, L. Miller, S. Mullen, and M. Shankar. Integrated hybrid-simulation of electric power and communications systems. In *Proc. IEEE Power Engineering Society General Meeting*, pages 1–8, 2007.

[18] Arun G. Phadke. Hidden failures in electric power systems. *International Journal of Critical Infrastructures*, 1:64–75, 2004.

[19] Francisco G. Velez Cedeno. *Multiple Swing Out-of-Step Relaying.* PhD thesis, Virginia Tech, 2010.

[20] M. C. D'Abreu and G. A. Wainer. Models for continuous and hybrid system simulation. In *Proc. Winter Simulation Conf*, volume 1, pages 641–649, 2003.

[21] F. Bouchhima, M. Briere, G. Nicolescu, M. Abid, and E. M. Aboulhamid. A SystemC/Simulink co-simulation framework for continuous/discrete-events simulation. In *Proc. IEEE Int. Behavioral Modeling and Simulation Workshop*, pages 1–6, 2006.

[22] J. H. Taylor and Jie Zhang. Rigorous hybrid systems simulation with continuous-time discontinuities and discrete-time components. In *Proc. Mediterranean Conf. Control & Automation MED '07*, pages 1–6, 2007.

[23] J. Eker, J. W. Janneck, E. A. Lee, Jie Liu, Xiaojun Liu, J. Ludvig, S. Neuendorffer, S. Sachs, and Yuhong Xiong. Taming heterogeneity - the Ptolemy approach. *Proceedings of the IEEE*, 91(1):127–144, 2003.

[24] A. Bottcher, A. Jahn, and M. Lazzari. Performance evaluation of channel-sensitive, stabilized multiple access schemes for land-mobile satellite services using a hybrid simulation tool. *IEEE Journal on Selected Areas in Communications*, 11(3):443–453, 1993.

[25] T. Hayashi, K. Katsura, and H. Tsunetsugu. New hybrid integrated laser diode-drivers using microsolder bump bonding: SPICE simulation of high-speed modulation characteristics. *IEEE/OSA Journal of Lightwave Technology*, 12(11):1963–1970, 1994.

[26] L. Ferrarini, G. Ferretti, C. Maffezzoni, and G. Magnani. Hybrid modeling and simulation for the design of an advanced industrial robot controller. *IEEE Robotics & Automation Magazine*, 4(2):45–51, 1997.

[27] H. T. Su, K. W. Chan, and L. A. Snider. Parallel interaction protocol for electromagnetic and electromechanical hybrid simulation. *IEE Proceedings-Generation, Transmission and Distribution*, 152(3):406–414, 2005.

[28] M. Carr and J. L. Volakis. A generalized framework for hybrid simulation of multi-component structures using iterative field refinement. *IEEE Antennas and Propagation Magazine*, 48(1):22–32, 2006.

[29] A. Muttreja, A. Raghunathan, S. Ravi, and N. K. Jha. Hybrid simulation for energy estimation of embedded software. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 26(10):1843–1854, 2007.

[30] Yong Li, Wei Li, and Yongping Lu. Computer-aided simulation analysis of a novel structure hybrid magnetic bearing. *IEEE Transactions on Magnetics*, 44(10):2283–2287, 2008.

[31] W. Li, A. Monti, M. Luo, and R. A. Dougal. VPNET: A co-simulation framework for analyzing communication channel effects on power systems. In *Proc. IEEE Electric Ship Technologies Symp. (ESTS)*, pages 143–149, 2011.

[32] V. Liberatore and A. Al-Hammouri. Smart grid communication and co-simulation. In *Proc. IEEE Energytech*, pages 1–5, 2011.

[33] Xiaoyang Tong. The co-simulation extending for wide-area communication networks in power system. In *Proc. Asia-Pacific Power and Energy Engineering Conf. (APPEEC)*, pages 1–4, 2010.

[34] C. M. Davis, J. E. Tate, H. Okhravi, C. Grier, T. J. Overbye, and D. Nicol. SCADA cyber security testbed development. In *Proc. 38th North American Power Symp. NAPS 2006*, pages 483–488, 2006.

[35] Malaz Mallouhi, Youssif Al-Nashif, Don Cox, Tejaswini Chadaga, and Salim Hariri. A testbed for analyzing security of SCADA control systems (TASSCS). In *Second IEEE PES Innovative Smart Grid Technologies Conference*, 2011.

[36] B. P. Zeigler. *Theory of Modeling and Simulation.* Academic Press, 2000.

[37] Mesut Baran, Raghuram Sreenath, and Nikhil Mahajan. Extending EMTP for simulating agent based distributed applications. In *14th PSCC*, 2002.

[38] T. S. Sidhu and Yujie Yin. Modelling and simulation for performance evaluation of IEC61850-based substation communication systems. *IEEE Transactions on Power Delivery*, 22(3):1482–1489, 2007.

[39] Tianqi Xu, Xianggen Yin, Dahai You, Yan Li, and Yangguang Wang. A novel communication network for three-level wide area protection system. In *Proc. IEEE Power*

*and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century*, pages 1–8, 2008.

[40] N. Higgins, V. Vyatkin, N.-K. C. Nair, and K. Schwarz. Distributed power system automation with IEC61850, IEC61499, and intelligent control. *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews*, 41(1):81–92, 2011.

[41] A. Hahn, B. Kregel, M. Govindarasu, J. Fitzpatrick, R. Adnan, S. Sridhar, and M. Higdon. Development of the PowerCyber SCADA security testbed. In *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*, 2010.

[42] A. Ashok, A. Hahn, and G. Manimaran. Cyber-physical security testbed: System architecture and studies. In *Proceedings of Cyber Security and Information Intelligence Research (CSIIR) Workshop*, 2011.

[43] T. Chiocchio, R. Leonard, Y. Work, R. Fang, M. Steurer, A. Monti, J. Khan, J. Ordonez, M. Sloderbeck, and S. L. Woodruff. A co-simulation approach for real-time transient analysis of electro-thermal system interactions on board of future all-electric ships. In *Proceedings of the 2007 summer computer simulation conference*, 2007.

[44] I. Leonard, T. Baldwin, and M. Sloderbeck. Accelerating the customer-driven microgrid through real-time digital simulation. In *Proc. IEEE Power & Energy Society General Meeting PES '09*, pages 1–3, 2009.

[45] C. Zhang, V. K. Vijapurapu, A. K. Srivastava, N. N. Schulz, J. Bastos, and R. Wierckx. Hardware-in-the-loop simulation of distance relay using RTDS. In *Proceedings of the 2007 summer computer simulation conference*, 2007.

[46] R. Kuffel, D. Ouellette, and P. Forsyth. Real time simulation and testing using IEC61850. In *Proc. Int Modern Electric Power Systems (MEPS) Symp*, pages 1–8, 2010.

[47] D. J. Marihart. Communications technology guidelines for EMS/SCADA systems. *IEEE Transactions on Power Delivery*, 16(2):181–188, 2001.

[48] G. N. Ericsson. On requirements specifications for a power system communications system. *IEEE Transactions on Power Delivery*, 20(2):1357–1362, 2005.

[49] Ieee standard c37.118-2005.

[50] Ali Abur and Antonio Gomez Exposito. *Power System State Estimation: Theory and Implementation.* CRC Press, 2004.

[51] G. L. Yu, B. H. Zhang, H. Xie, and C. G. Wang. Wide-area measurement-based nonlinear robust control of power system considering signals' delay and incompleteness. In *Proc. IEEE Power Engineering Society General Meeting*, pages 1–8, 2007.

[52] K. P. Birman, J. Chen, E. M. Hopkinson, R. J. Thomas, J. S. Thorp, R. Van Renesse, and W. Vogels. Overcoming communications challenges in software for monitoring and controlling power systems. *Proceedings of the IEEE*, 93(5):1028–1041, 2005.

[53] Guodong Liao, K. M. Hopinson, Jun Tang, Li Ding, and Xiaoru Wang. A simulation study on the ethernet communication of a substation automation system based on EPOCHS. In *Proc. Int. Conf. Power System Technology PowerCon 2006*, pages 1–7, 2006.

[54] K. Hopkinson, G. Roberts, Xiaoru Wang, and J. Thorp. Quality-of-service considerations in utility communication networks. *IEEE Transactions on Power Delivery*, 24(3):1465–1474, 2009.

[55] G. M. Coates, K. M. Hopkinson, S. R. Graham, and S. H. Kurkowski. A trust system architecture for SCADA network security. *IEEE Transactions on Power Delivery*, 25(1):158–169, 2010.

[56] R. Giovanini, K. Hopkinson, D. V. Coury, and J. S. Thorp. A primary and backup cooperative protection system based on wide area agents. *IEEE Transactions on Power Delivery*, 21(3):1222–1230, 2006.

[57] Xiaoyang Tong, Xiaoru Wang, and K. M. Hopkinson. The modeling and verification of peer-to-peer negotiating multiagent colored Petri Nets for wide-area backup protection. *IEEE Transactions on Power Delivery*, 24(1):61–72, 2009.

[58] W. R. Lachs. A new horizon for system protection schemes. *IEEE Transactions on Power Systems*, 18(1):334–338, 2003.

[59] Song Shaoqun, Zhu Yongli, Huang Min, and Yu Hong. Multiagent and WAN based adaptive coordinated protection system. In *Proc. IEEE/PES Transmission and Distribution Conf. and Exhibition: Asia and Pacific*, pages 1–6, 2005.

[60] T. Shono, K. Sekiguchi, T. Tanaka, and S. Katayarna. A remote supervisory system for a power system protection and control unit applying mobile agent technology. In *Proc. Transmission and Distribution Conf. and Exhibition 2002: Asia Pacific. IEEE/PES*, volume 1, pages 148–153, 2002.

[61] Dong qing Wang, Shi hong Miao, Xiang ning Lin, Pei Liu, Ying-Xin Wu, and Dan Yang. Design of a novel wide-area backup protection system. In *Proc. IEEE/PES Transmission and Distribution Conf. and Exhibition: Asia and Pacific*, pages 1–6, 2005.

[62] M. M. Eissa, M. E. Masoud, and M. M. M. Elanwar. A novel back up wide area protection technique for power transmission grids using phasor measurement unit. *IEEE Transactions on Power Delivery*, 25(1):270–278, 2010.

[63] L. A. O. Class, K. M. Hopkinson, Xiaoru Wang, T. R. Andel, and R. W. Thomas. A robust communication-based special protection system. *IEEE Transactions on Power Delivery*, 25(3):1314–1324, 2010.

[64] A. G. Phadke and J. S. Thorp. Expose hidden failures to prevent cascading outages [in power systems]. *IEEE Computer Applications in Power*, 9(3):20–23, 1996.

[65] H. Wang and J. S. Thorp. Optimal locations for protection system enhancement: a simulation of cascading outages. *IEEE Transactions on Power Delivery*, 16(4):528–533, 2001.

[66] J. De La Ree, Y. Liu, L. Mili, A. G. Phadke, and L. DaSilva. Catastrophic failures in power systems: Causes, analyses, and countermeasures. *Proceedings of the IEEE*, 93(5):956–964, 2005.

[67] S. Bak. Large-scale network simulation scalability and an FPGA-based network simulator. Technical report, 2008.

[68] S. Kristiansen and T. Plagemann. NS2 distributed clients emulation: accuracy and scalability. In *Proceedings of the 2nd International Conference on Simulation Tools and Techniques*, 2009.

[69] G. Carl. *Towards Large-Scale Testing of Policy-Based Routing via Path Algebraic and Scaled-Down Topological Modeling.* PhD thesis, Pennsylvania State University, 2008.

[70] Ming Zhou, V. A. Centeno, J. S. Thorp, and A. G. Phadke. An alternative for including phasor measurements in state estimators. *IEEE Transactions on Power Systems*, 21(4):1930–1937, 2006.

[71] K. Jones. Three-phase linear state estimation with phasor measurements. Master's thesis, Virginia Tech, 2011.

[72] Bei Xu and Ali Abur. Optimal placement of phasor measurement units for state estimation. Technical report, Texas A&M University, 2005.

[73] A.G. Phadke and J. S. Thorp. *Synchronized Phasor Measurements and Their Application.* Springer Science + Business Media, 2008.

[74] M. E. Kuhl, J. Kistner, K. Costantini, and M. Sudit. Cyber attack modeling and simulation for network security analysis. In *Proc. Winter Simulation Conf*, pages 1180–1188, 2007.

[75] Yilin Mo, T. H. J. Kim, K. Brancik, D. Dickinson, Heejo Lee, A. Perrig, and B. Sinopoli. Cyber physical security of a smart grid infrastructure. *Proceedings of the IEEE*, 100(1):195–209, 2012.

[76] Li Li and Yutian Liu. Out-of-step splitting framework based on adaptive separation detecting criterion. In *Proc. Transmission & Distribution Conf. & Exposition: Asia and Pacific*, pages 1–5, 2009.

[77] A. Sauhats, J. Kucajevs, L. Leite, G. Bockarjova, and A. Utans. Out-of-step automation device model validation methodology. In *Proc. 10th Int Environment and Electrical Engineering (EEEIC) Conf*, pages 1–6, 2011.

[78] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. *Introduction to Algorithms.* The MIT Press, 2009.

[79] A. V. Goldberg and S. Rao. Beyond the flow decomposition barrier. In *Proc. th Annual Symp Foundations of Computer Science*, pages 2–11, 1997.

[80] R. Chabukswar, B. Sinopoli, and G. Karsai. Simulation of network attacks on SCADA systems. In *First Workshop on Secure Control Systems*, 2010.

[81] B. Chaudhuri, R. Majumder, and B. C. Pal. Wide-area measurement-based stabilizing control of power system considering signal transmission delay. *IEEE Transactions on Power Systems*, 19(4):1971–1979, 2004.

[82] Yi Deng, Shravan Garlapati, Hua Lin, Santhoshkumar Sambamoorthy, Sandeep Shukla, James Thorp, and Lamine Mili. Visual integrated application development for substation automation compliant to iec 61850. In *Proceedings of the PAC World Conference*, 2011.

[83] Yi Deng, Hua Lin, A. G. Phadke, S. Shukla, J. S. Thorp, and L. Mili. Communication network modeling and simulation for wide area measurement applications. In *Proc. IEEE PES Innovative Smart Grid Technologies (ISGT)*, pages 1–6, 2012.

[84] Xueyuan Dong, K. Hopkinson, Xiaoyang Tong, Xiaoru Wang, and J. Thorp. IP-based communication systems for wide-area frequency stability predictive control. In *Proc. 5th Int Critical Infrastructure (CRIS) Conf*, pages 1–7, 2010.

[85] S. Garlapati, Hua Lin, S. Sambamoorthy, S. K. Shukla, and J. Thorp. Agent based supervision of zone 3 relays to prevent hidden failure based tripping. In *Proc. First IEEE Int Smart Grid Communications (SmartGridComm) Conf*, pages 256–261, 2010.

[86] R. Giovanini, D. V. Coury, K. M. Hopkinson, and J. S. Thorp. Improving local and backup protection using wide area agents. In *Proc. Eighth IEE Int Developments in Power System Protection Conf*, volume 2, pages 738–741, 2004.

[87] T. Godfrey, S. Mullen, R. C. Dugan, C. Rodine, D. W. Griffith, and N. Golmie. Modeling smart grid applications with co-simulation. In *Proc. First IEEE Int Smart Grid Communications (SmartGridComm) Conf*, pages 291–296, 2010.

[88] M. Haffar, F. Clavel, J. M. Thiriet, H. Ziade, and K. Mouchref. Performance evaluation of a hybrid communication architecture using an operational co-simulation platform.

In *Proc. IEEE PES Conf. Innovative Smart Grid Technologies - Middle East (ISGT Middle East)*, pages 1–6, 2011.

[89] Kenneth Mark Hopkinson. *Overcomming Communication, Distributed Systems , and Simulation Challenges: A Case Study Involving the Protection and Control of the Electric Power Grid using A Utility Intranet Based on Internet Technology.* PhD thesis, Cornell University, 2004.

[90] S. H. Horowitz and A. G. Phadke. Third zone revisited. *IEEE Transactions on Power Delivery*, 21(1):23–29, 2006.

[91] Hua Lin, Yi Deng, Sandeep Shukla, James Thorp, and Lamine Mili. Cyber security impacts on all-pmu state estimator - a case study on co-simulation platform GECO. In *Proceedings of the Third International IEEE Conference on Smart Grid Communications*, 2012.

[92] Hua Lin, Santhoshkumar Sambamoorthy, Sandeep Shukla, James Thorp, and Lamine Mili. A study of communication and power system infrastructure interdependence on pmu-based wide area monitoring and protection. In *Proceedings of the IEEE Power & Energy Society General Meeting*, 2012.

[93] Hua Lin, S. Sambamoorthy, S. Shukla, J. Thorp, and L. Mili. Power system and communication network co-simulation for smart grid applications. In *Proc. IEEE PES Innovative Smart Grid Technologies (ISGT)*, pages 1–6, 2011.

[94] Hua Lin, Santhoshkumar Sambamoorthy, Sandeep Shukla, James Thorp, and Lamine Mili. Ad-hoc vs. supervisory wide area backup relay protection validated on power/network co-simulation platform. In *Proceedings of the 17th Power Systems Computation Conference*, 2011.

[95] Hua Lin, S. S. Veda, S. S. Shukla, L. Mili, and J. Thorp. GECO: Global event-driven co-simulation framework for interconnected power system and communication network. *IEEE Transactions on Smart Grid*, 3(3):1444–1456, 2012.

[96] J. S. Thorp and A. G. Phadke. Protecting power systems in the post-restructuring era. *IEEE Computer Applications in Power*, 12(1):33–37, 1999.

[97] Xiaoyang Tong. A web services based wide-area corporation multi-agent system platform for power system. In *Proc. IEEE Conf. Cybernetics and Intelligent Systems*, pages 666–671, 2008.

[98] Xiaoyang Tong, Xiaoru Wang, and Li Ding. Study of information model for wide-area backup protection agent in substation based on IEC61850. In *Proc. Third Int. Conf. Electric Utility Deregulation and Restructuring and Power Technologies DRPT 2008*, pages 2212–2216, 2008.

[99] X.R. Wang, Hopkinson K.M., and J.S. Thorp. Developing an agent-based backup protection system for transmission networks. In *First International Conference on Power Systems and Communication Systems Infrastructures for the Future*, 2002.

[100] *http://www.dhs.gov/files/programs/gc_1189168948944.shtm.*

[101] *http://www.isi.edu/nsnam/ns/.*

[102] *PSLF Users Manual for Version 16.1.*

[103] Rationale for the use of local and remote (zone 3) protective relaying backup systems. Technical report, North American Electric Reliability Council, 2005.