An Interactive, Extensible Environment for Power System Simulation on the PMU Time Frame with a Cyber Security Application

Thomas J Overbye, Zeyu Mao, Komal S. Shetye
Dept. of Electrical and Computer Engineering
University of Illinois at Urbana-Champaign
Urbana, IL, USA

James D. Weber
PowerWorld Corporation
Urbana, IL, USA

***Abstract*—Power system simulation environments with appropriate time-fidelity are needed to enable rapid testing of new smart grid technologies and for coupled simulations of the underlying cyber infrastructure. This paper presents such an environment which operates with power system models in the PMU time frame, including data visualization and interactive control action capabilities. The flexible and extensible capabilities are demonstrated by interfacing with a cyber infrastructure simulation.**

Keywords—power grid simulation, PMUs, c37.118, visualization, interactive control, cyber security.

I. Introduction

As the smart grid moves forward, there is a need for flexible and interactive power system simulation environments in which new ideas for grid communication, control, analytics, and visualization can be prototyped. A nice description of the role simulators can play in smart grid development is presented in [1]. Power systems have a long history of interactive simulation environments, with key distinctions often associated with the simulation time frame of the associated underlying dynamics. In this paper, an interactive environment for simulating power system dynamics on what we will call the PMU time frame (power system cycles and slower) is presented, along with a cyber security application.

In order to put this in context, Figure 1 (derived from Fig. 1.2 of [2]) shows the wide variety of time frames that might need to be considered in developing simulations for smart grid applications. However, in order to make the simulation computationally tractable and to simplify the modeling, the time frame of interest needs to be considered. Dynamics significantly faster than the time frame of interest can be represented by algebraic constraints and those significantly slower can be considered constant.

The first interactive digital simulations were operator training simulators (OTSs) with [3] providing an early example. With this approach, the power system was assumed to have a uniform, but not constant, frequency. Dynamics with time frames longer than about one second were considered, such as generator boiler-turbine governors and automatic generation control, but the network equations were solved using a power flow. As the name implies, OTSs were often used to train operators. Slightly longer-term simulations, which used a constant frequency power flow assumption, were used to teach students and nontechnical professionals about the operation of the power grid, with [4] providing an example. Such packages often ran substantially faster than real-time to teach concepts such as loop flow and interconnected operation. Because of the lack of dynamics, they could efficiently solve interconnect size systems with tens of thousands of buses. On an even longer time frame, [5] was used to teach market operations, working with a discrete, often one hour simulation step-size. In such market simulations, the power flow was often not explicitly solved.

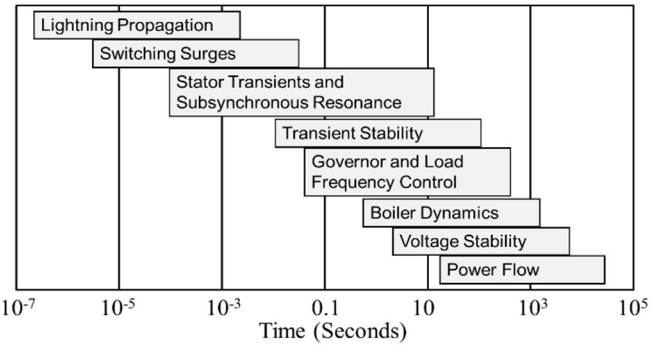


Figure 1: Power System Time Frames

All of the preceding methods assume that even a large network can be modeled as algebraic constraints, with speed of light considerations ignored. To represent very fast dynamics, such as for lightning propagation, switching surges and hardware-in-the-loop, simulations based on the electromagnetic transients approach of [6] have been developed. In this approach, the transmission lines are modeled with the differential equations associated with the voltage and current relationships in inductors and capacitors. By using Trapezoidal integration techniques, the models reduce to a network of coupled current sources and shunt resistances in which transmission line propagation delays can be considered explicitly. However, with simulation step sizes of

This paper was presented in the 2017 IEEE Texas Power and Energy Conference, College Station, Texas, 2017.

microseconds they are often limited to smaller systems, unless large amounts of parallel computation are used.

The interactive simulation environment presented here sits between the extremely short time frame of [6] and the uniform frequency model of [3]. That is, simulating the system with a step size on the order of ¼ or ½ cycles (e.g., 0.004 seconds). In power systems this is known as transient stability time frame, but since it corresponds to the sampling frequency of PMUs, a complementary name is the PMU time frame. Another example of such a simulation package is presented in [7].

In this time frame, the dynamics of the generator machines, exciters, governors and stabilizers can be represented, along with dynamic models for the load (such as for induction motors). Hence during disturbances, each bus has a unique frequency, yet the transmission network equations are still represented as algebraic constraints. This time frame also allows for the detailed modeling of the interaction of the power system with its underlying communication and control systems [8], [9], [10], [11]. Cyber security issues in the communication system can also be considered [12].

The main contributions of this paper are a description of such an interactive PMU time frame simulation environment, along with an example application of the environment to provide a flexible platform that can be used to simulate the interaction of the power system with its cyber infrastructure. The paper is organized as follows. Section II provides a description of the power system simulation environment. Then Section III describes the interaction between this environment and a prototype simulation of a portion of the power grid's cyber infrastructure.

II. A PMU Timeframe Interactive Simulation

While changes to the grid are resulting in more concern about dynamic issues in power system operation, the widespread deployment of PMUs is greatly increasing knowledge about power system dynamics in this PMU time frame, and allowing for the possibility of more closed-loop control. Hence, there is a need for smart grid prototyping and teaching environments modeling these power system dynamics.

In order to avoid the complexity and cost of writing a transient stability simulation from scratch, in an approach similar to what was presented in [10], the dynamics simulation environment described here (abbreviated as DS) utilizes a commercial transient stability package as its simulation engine [13]. This provides the advantages of allowing it to, 1) represent the hundreds of different power system dynamics models commonly found in actual transient stability cases, 2) import and export case models in industry standard formats, and 3) efficiently solve large power system cases. This is in contrast to the approach of [1] of developing a short-term dynamics simulation program with a restricted set of models.

The DS can be configured to run in real-time, or either faster or slower than real-time while solving the power system dynamic models on the PMU time frame, subject to computational limitations. A modest PC can solve systems with several thousand buses in real-time, and can simulate the small systems described here at speeds of several times real-time if desired.

The DS is designed to function in two complimentary modes. First, it can be used as a stand-alone, interactive power system simulation environment. Hence it is very similar to the interactive power flow simulation package of [4]. Second, the stand-alone mode of the DS can be augmented to allow it to also function as a simulation engine server as part of a coupled simulation environment. As is described later in the paper, the DS is able to communicate with other packages using either the C37.118.2 protocol [14], or using the PowerWorld DS protocol (PWDSP) which allows for interactive control. The advantage of using the C37.118.2 protocol is it allows the DS to be immediately connected to existing packages that utilize this protocol. However, C37.118.2 is not designed for interactive control. Rather, interactive control of the DS is accomplished using the PWDSP. Hence, the DS provides for an extensible environment that can be used to simulate both, the power system with its dynamics, and the communication and control systems, such as from [8].

When used in either stand-alone or server mode, the DS is setup to directly open and simulate existing power system transient stability cases, with a strong focus on power system visualization. As an example of the stand-alone mode, Figure 2 shows the one-line diagram for a fictitious 345/138 kV, 42 bus system in which the per unit voltage magnitudes are represented using a color contour [15]. During an interactive simulation, the one-line contour can be updated at a user selected rate of up to about 10 Hz (depending on contour resolution and machine speed), allowing for good visualization of power system voltage effects. By varying this rate, it is possible to compare how a one-line might respond when driven by PMU data, versus one driven by SCADA data in which the refresh rate would be once every few seconds.

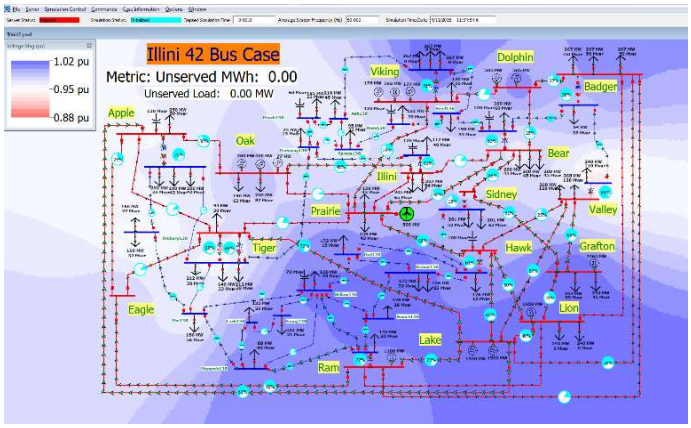


Figure 2: 42 Bus System One-line with Voltage Contour

Another feature of the DS is the ability to display strip-charts of a wide variety of system quantities. Figure 3 demonstrates this functionality on a scenario that takes the Figure 2 case, and over the course of 40 seconds models the impact of a tornado moving through a substation, sequentially opening three 345 kV transmission lines, and taking a 500 MW wind farm off-line. In Figure 3, both strip-charts are displaying one minute of data, with the top chart showing the system frequency and the bottom one showing several of the bus voltage magnitudes. This scenario is setup as sort of a game in which as the simulation progresses in real time, the goal for the user is to interactively modify the system by control actions such as shedding load, to prevent a

voltage collapse. The system oscillations in the PMU time frame are shown in the strip-charts. When the contour is set to refresh at rates of more than several times a second, the system wide impacts of these oscillations can be visualized.

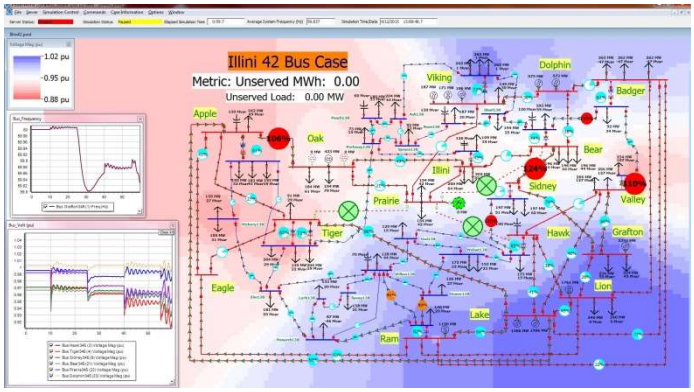


Figure 3: 42 Bus Case with Several Lines Outaged

In the stand-alone mode the system can be monitored and controlled either using the previously mentioned one-lines, or through a variety of tabular displays. Figure **4** shows an example using the 150 bus, 500/230 kV entirely synthetic case from [16]. The figure illustrates a system one-line using a contour to show the substation voltages, a strip-chart showing the system frequency, a tabular display showing all the system generators, and a generator dialog. The dialog can be used to both monitor the generator, and issue controls including changing the exciter setpoint voltage or the governor MW setpoint.

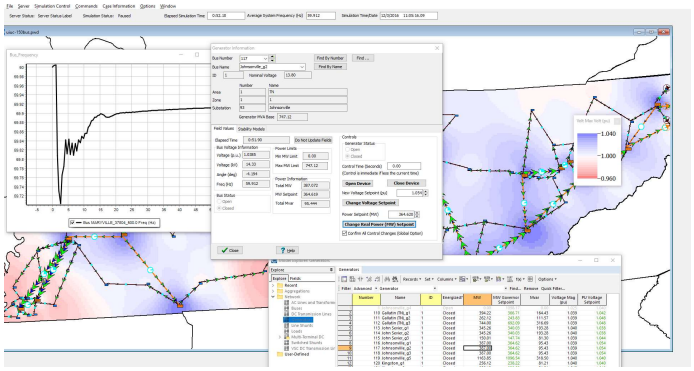


Figure 4: Interactive Control with 150 Bus Case

As noted earlier, when running as a simulation server the DS can communicate using either the C37.118.2 protocol or the PWDSP. C37.118.2 is described in [14], and is intended primarily for a one way transfer of simulation values from the DS to clients. Currently the DS is setup such that each electrical substation is considered as a separate C37.118.2 PMU.

In contrast, the PWDSP allows two-way communication to clients, which may be other simulations. The PWDSP has three major classes of functionality. First, it has dictionary commands that allow the clients to request information about the DS power system model structure. For example, clients can ask for a description of the model structure. In response, the DS returns information about the 21 different object types it uses to represent the power system. Example object types include buses, generators, loads, and ac transmission lines. This allows a client to connect to the DS without a priori knowledge about the particular model.

Second, the PWDSP has commands that allow clients to request simulation values. For example, at a specified rate a client may request all of the per unit voltage magnitudes and angles. Recognizing that clients will commonly be requesting the same sets of values, field sets can be defined by the client and stored on the DS to avoid the communication overhead associated with requesting the same values.

Third, the PWDSP supports commands that modify the underlying power system model. Example commands include opening loads and ac transmission lines, or changing generator setpoints. Eventually all commands used internally by the underlying commercial transient stability engine will be supported. Commands sent by the client are specified to occur at a particular time in the simulation, with a common option to be immediately executed. An example usage of the DS and the PWDSP for cyber security research is described next.

III. A DS Based Toolkit for Cyber Security Research in Power Systems

One application of the DS is to provide a PMU time frame power system simulation as part of a coupled simulation of the power system with some of its cyber infrastructure. This section presents a prototype toolkit of a coupled simulation that consists of three parts: 1) the DS, 2) a synchrophasor network simulation, and 3) a real-time data-sharing and coordination mechanism. The synchrophasor network includes models of phasor measurement units (PMUs), phasor data concentrators (PDCs), and a control center. Communication is done using IEEE C37.118.2-2011 protocol [14] from the DS to the PMUs and then onto the PDCs, and finally to a control center simulation, and using the PWDSP between the control center simulation and the DS for real-time control. This is illustrated in Figure 5. The components of the synchrophasor simulation environment are introduced below. In addition, a cyber security case is set up to demonstrate the interactive simulation of the power system and the cyber infrastructure.

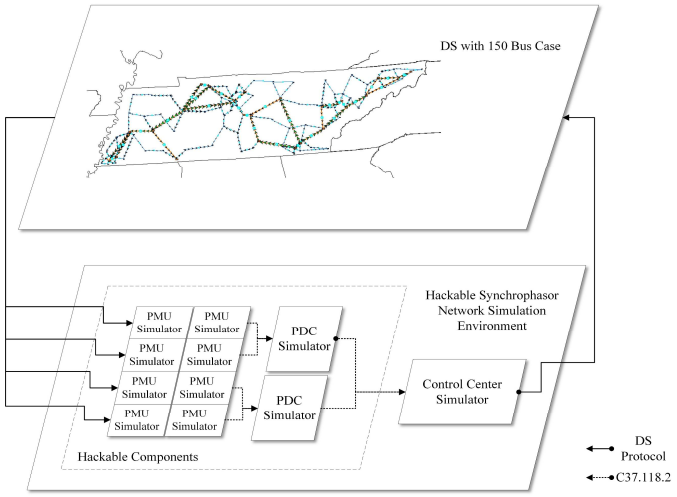


Figure 5: The Interactive Simulation Framework

III.A. Hackable PMU Simulator

The first model represents virtual PMUs that comply with the IEEE standard C37.118.1-2011 [17]. In order to simulate the behavior of PMUs under cyber-attacks, a "hack module" is integrated into the PMU simulator that enables users to choose the cyber-attack events for the selected PMU. This "Hackable PMU simulator" generates multiple virtual PMUs which can have output data rates of up to 120 messages/second. Each PMU is assigned a communication port. The architecture of the PMU simulator is shown in Figure **6**.

At startup, each PMU simulator sends a dictionary command to the DS to obtain information about the model topology. Upon reception of a valid dictionary packet, the packet is decoded and the user interface is updated with the case information. The information obtained for the selected substation is then sent to the PMU generator to build the C37.118.2 configuration frame [14]. Once the configuration frame is ready, the PMU generator is able to accept the request command for the data frame. Similar to the initial procedure used to obtain the model dictionary, the data packet from the DS is first decoded, and then the data corresponding to the selected substations/buses will be sent to the PMU. The hack module is situated between the router and PMU generator, such that the parameters of a data frame can be modified prior to sending out from the router. Data modification is done according to the hack option selected by the user.

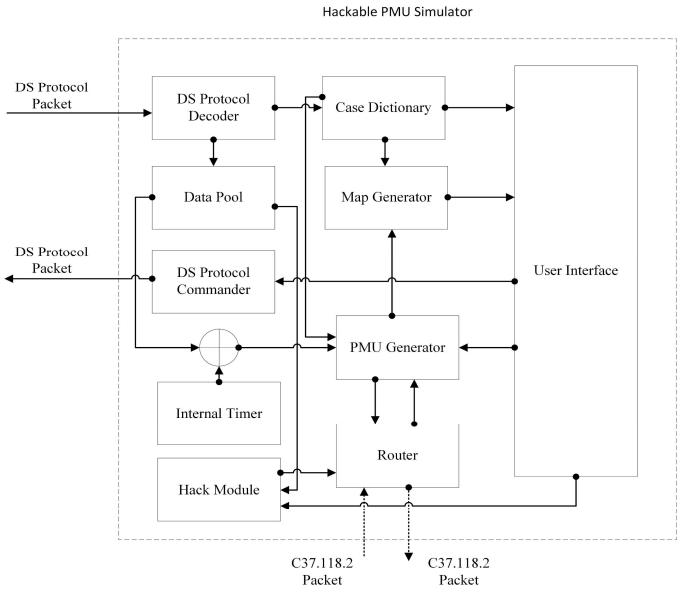


Figure 6: The Hackable PMU Simulator Architecture

In order to generate multiple PMUs for the case, synchronized multi-threads are used in building the simulation. This ensures users not having to run multiple instances of simulators if several PMUs are needed in the system. Instead, the simulator generates as many threads as the number of PMUs. Individual communication ports are then assigned to each PMU for their connection to the PDC simulator. This multi-threaded design supports the optional individual latency for each PMU.

III.B. Hackable PDC Simulator

Like the PMU simulator, the PDC simulator has a hack module that enables the PDCs to be hacked by the cyber-attacks in the simulation. The "Hackable PDC simulator" concentrates the IEEE C37.118.2-2011-formatted data streams from the selected PMU simulators and other data sources specified by the user. It buffers the data stream and waits for a certain time (σ) to receive measurements from all connected PMUs. Multi-threads have also been implemented in the PDC simulator. When the PDC is ready to transmit, it aggregates all the data from the selected PMUs into a single data frame, generates a new time tag for this frame, and outputs at rates up to 120 messages/second. Algorithm 1 illustrates the process of generating the data packets in the PDC simulator.

Algorithm 1 Multi-thread Hackable PDC Algorithm

Input: **D** - Data streams from all connected PMUs; **T**- Algorithm start time; **б** - Waiting period; **H** - Hacked PMU index list
Output: PDC data packet

```
For d in D
    Receive d and record the index i of d
    Decode d
    IF d.time within [T- б, T]
      IF i within H
        d.data = H.type × d.data
      END IF
      Put d.data into O[i]
    ELIF d.time < T- б
      Check d.buffer
      IF d.buffer > 0
        Go back to Step 2
      ELSE
        Put Empty into O[i]
      END IF
    END IF
    END
    While True
      IF current-time >= T + б
        Send out O
        Break
      END IF
    END
```

As is the case with the PMU simulator, the hack module is integrated after the data aggregation, such that the parameters of the newly generated data frame can be modified prior to being sent out. Different types of hack behavior can be achieved by changing the hack option and parameters in the user interface.

III.C. Control Center Simulator

The control center simulator is designed to receive streams from multiple PDC simulators, and to utilize visualization and analysis tools to help users detect anomalous behaviors in the power system and/or its associated synchrophasor cyber infrastructure. Users are able to use command functions, through the connection with the DS, to control the underlying power simulation.

The control center simulator is comprised of four blocks. First, an "operation block" is used to connect to the PDC simulators and the DS. Second, the "dictionary block" shows the details of the running case. Third, the "data visualization block" plots the PMU data and updates the data table. Last, a "map block" shows the geographic information of the power system and the synchrophasor network. As shown in Figure 7d, the geographic map of the given power system case and the sychrophasor network is generated in the map block.

III.D. Bad Data Injection Case

A case study demonstrating the working of the coupled simulation toolkit is implemented. A bad data injection at a single PMU/PDC in the previously mentioned 150 bus case [16] is presented. Prior to the bad data injection, initialization of the interactive simulation is carried out. The steps used for these activities, and the built-in function elements are described below.

1) Interactive Simulation Quick Initialization

1. Open DS to load the 150 bus case. Start the server function in the DS. The server port is 5557.
2. Open the PMU Simulator program. Specify the selected buses (10, 11, 15, 18, 23, 50, 82, 88) in the *PMU Placement* field. Click on the interface "*Start*" button. A port range of 5558-5565 is assigned to these PMUs for connection to the PDC.
3. Open the PDC Simulator program. Specify port numbers 5558-5565 to connect to all 8 PMUs. Here, we also place a PDC in Substation 56, and set its port number to 5566. The PDC is placed in the system and connects to the 8 PMUs.
4. Open the Control Center Simulator program. Connect to both PDC and DS through the port 5566 and 5557. Click on the "*Initialize*" button to receive and decode the dictionary packet from the DS. Afterwards, click on the "*Start*" button to receive data frames from the PDC. Figure 6 shows the procedure of the initialized coupled simulation and the interface of each component in the toolkit.

2) Noise Injection at a single PMU

The process of injecting noise requires switching to the PMU simulator program. In the "*Advance*" tab, select the options "*FreqHz*" and "*Random*" in the combo boxes. Type in the number into the bus field. Random noise injection in the data begins once the "*Start*" button is clicked.

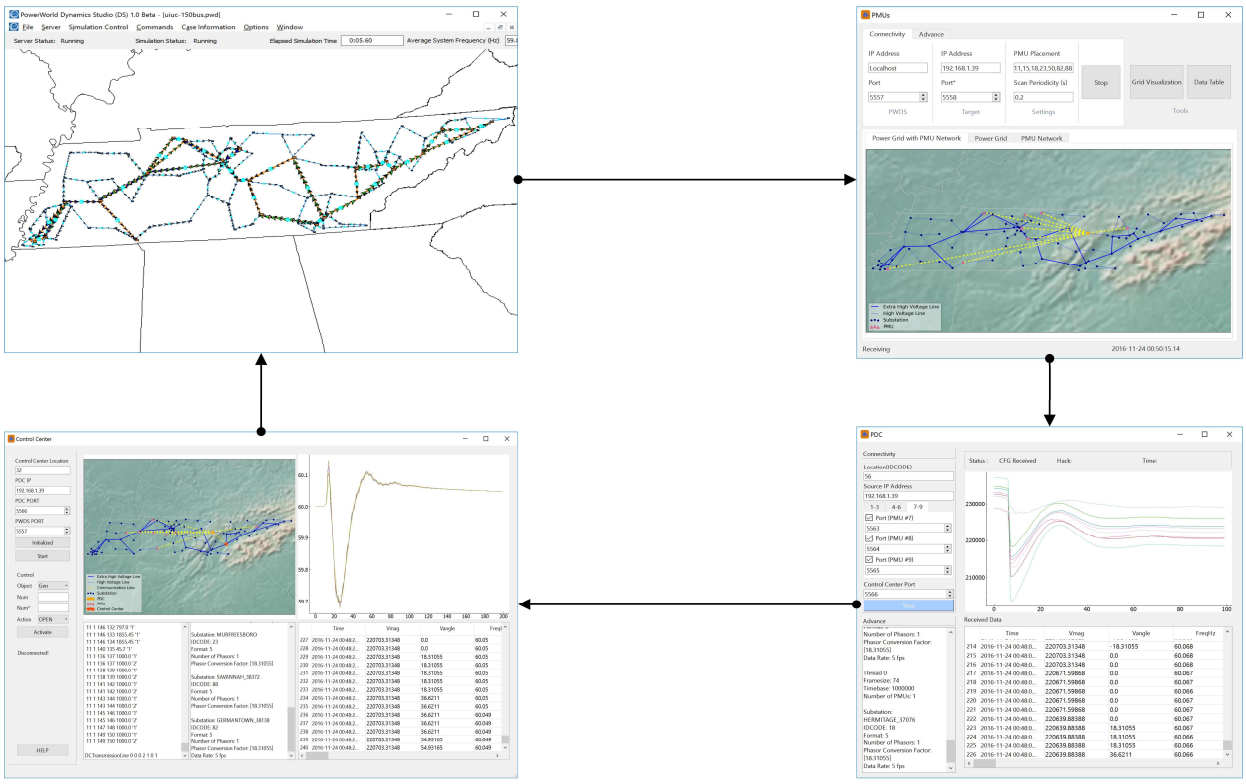
Currently three types of bad data injection have been integrated into the hackable PMU/PDC Simulator. First, the phasor's magnitude/angle/frequency can be added with a specified deviation or a random noise. Second, a time drifting can be injected into the bytes for the time information to lead to the mis-synchronization of the packets. Third, the data output can be locked so that the phasor values will be constant with only time updated.

In this case, data generated by PMU 1, located at Bus 10, is sent over a communication network to the PDC located in Substation 56. The data is then forwarded to the control center. During its transmission, the data passes the PMU/PDC routers and the communication links, and the PMU router is compromised by the cyber attacker. The attacker aims to use a Gaussian noise data injection [18], [19] to manipulate the frequency data that may contaminate the data received by the PDC and consequently affect the frequency monitoring in the control center.

To evaluate the effect of the bad data injection in this coupled simulation, the data stored in all PMUs and the data received by the control center and ready for the frequency monitoring have been extracted and compared. As shown in Figure **8**, significant noise is observed in the control center (Figure **8**b) when compared to the frequency data stored in the PMU (Figure **8**a), which illustrates three points: 1) the bad data is injected into the router

(a) PWDS

(b) PMU Simulator



(d) Control Center Simulator

(c) PDC Simulator

Figure 7: Initialized Interactive Simulation

of PMU 1, thus no noise is found in the data stored in the PMU, 2) the bad data from the PMU 1 router has been aggregated by the PDC and then forwarded to the control center, and 3) the frequency monitoring in the control center will be affected by the bad data injection, and hence wrong decisions might be made by operators based on the attacked data.

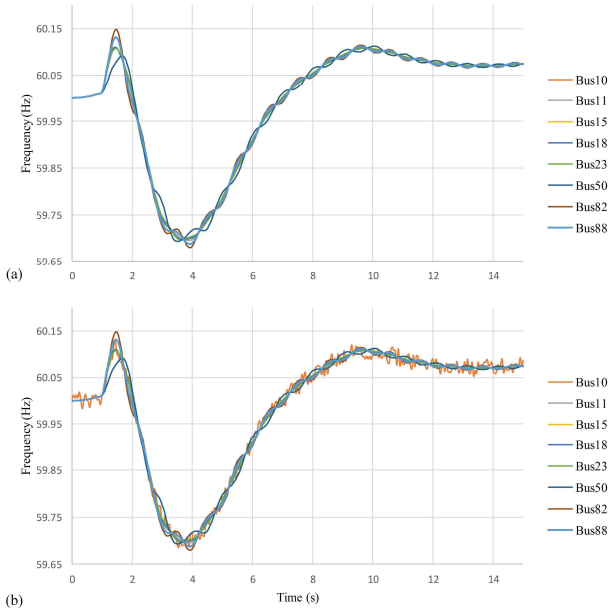


Figure 8: Effect of the bad data injection on the PMU network

IV. Summary and Future Directions

This paper has presented an interactive simulation package that can be used for either stand-alone PMU timescale simulations, or as a simulation engine that can be used for either multi-user simulations, and/or as part of a coupled simulation environment. Based on the real-time data output features of this package a coupled simulation toolkit is developed to simultaneously model both a power system and the synchrophasor cyber infrastructure. Using a 150 bus case the toolkit has been demonstrated to co-simulate the power system and its underlying synchrophasor infrastructure, for cyber security research applications. By showing the procedure of building the synchrophasor network for the 150 bus case, it is clear that other power system cases can be used in this environment by following the same steps.

For future work, we intend to use this interactive system to develop new visualization and analysis methods to detect cyber security events, and other issues in power systems. More cyber-attack scenarios will be added to the coupled simulation toolkit presented in this paper. Similar to the cyber security application shown in this paper, other applications, clients, scenarios, and control actions will be investigated for coupling with the DS.

V. Acknowledgments

The work described here is supported in part by the U.S. Department of Energy under Award Number DE-OE0000780.

References

[1] R. Podmore, M. R. Robinson, “The Role of Simulators for Smart Grid Development,” *IEEE Trans. Smart Grid*, vol. 1, September 2010, pp. 205-212

[2] P. W. Sauer, M. A. Pai, *Power System Dynamics and Stability*, 1997

[3] R. Podmore, J. C. Giri, M. P. Gorenberg, J. P. Britton, N. M. Peterson, “An Advanced Dispatcher Training Simulator,” *IEEE Trans. on Power App. and Sys*., Jan 1982, pp. 17-25.

[4] T. J. Overbye, P. W. Sauer, C. M. Marzinzik and G. Gross, "A user-friendly simulation program for teaching power system operations," *IEEE Trans. on Power Sys.*, vol. PWRS-10, pp. 1725-1733, November 1995

[5] R. D. Zimmerman, R. J. Thomas, “PowerWeb: A Tool for Evaluating Economic and Reliability Impacts of Electric Power Market Designs,” *Proc. IEEE Power Systems Conference and Exposition*, December, 2004,

[6] H.W. Dommel, "Digital Computer Solution of Electromagnetic Transients in Single- and Multiphase Networks," *IEEE Trans. Power App. and Sys*., vol. PAS-88, April 1969, pp. 388-399

[7] G. Zheng, F. Howell, L. Wang, “A Synchrophasor System Emulator – Software Approach and Real-time Simulations,” *Proc. IEEE PES General Meeting*, July 2015, Denver, CO

[8] Y. Wang, P. Yemula, A. Bose, “Decentralized Communication and Control Systems for Power System Operation,” *IEEE Trans. Smart Grid*, vol. 6, March 2015, pp. 885-893

[9] K. Mets, J. A. Ojea, C. Develder, “Combining Power and Communication Network Simulator for Cost-Effective Smart Grid Analysis,” *IEEE Communication Surveys and Tutorials*, vol. 16, issue. 3, 2014, pp. 1771-1796

[10] D. Anderson, C. Zhao, C. H. Hauser, V. Venkatasubramanian, D. E. Bakken, A. Bose, “A Virtual Smart Grid*,” IEEE Power and Energy Magazine*, Jan/Feb 2012, pp. 49-57

[11] K. Zhu, S. Deo, A. T. AL-Hammouri, N. Honeth, M. Chenine, D. Babazadeh, L. Nordstrom, “Test Platform for Synchrophasor Based Wide-Area Monitoring and Control Applications,” *Proc. IEEE PES 2013 General Meeting*, July 2013, Vancouver, BC

[12] D. M. Nicol, C. M. Davis, T. J. Overbye, "A Testbed for Power System Security Evaluation," *International Journal of Information and Computer Security*, vol. 3, number 2, pp. 114-131, 2009.

[13] PowerWorld Transient Stability Add-on, http://www.powerworld.com/products/simulator/add-ons-2/transient-stability

[14] IEEE Standard for Synchrophasor Measurements for Power Systems, IEEE Standard C37.118.2-2011

[15] J. D. Weber and T. J. Overbye, "Voltage contours for power system visualization," *IEEE Trans. on Power Systems*, pp. 404-409, February, 2000

[16] A.B. Birchfield, K.M. Gegner, T. Xu, K.S. Shetye, T.J. Overbye, “Statistical Considerations in the Creation of Realistic Synthetic Power Grids for Geomagnetic Disturbance Studies,” to appear *IEEE Trans. Power Systems*

[17] IEEE Standard for Synchrophasor Measurements for Power Systems, IEEE Standard C37.118.1-2011

[18] Ikponmwosa Idehen, Zeyu Mao, Thomas Overbye, “An Emulation Environment for Prototyping PMU Data Errors,” Proc. North American Power Symposium, September 2016, Denver, CO

[19] Michael Brown, Milan Biswal, Sukumar Brahma, Satish J Ranade, Huiping Cao, “Characterizing and Quantifying Noise in PMU data,” Proc. IEEE PES General Meeting, July 2016, Boston, MA