Federated Simulation for Development of Improved Incident Detection and Management

Website: http://cred-c.org/researchactivity/fedsimidm

Researchers (Illinois): Thomas J. Overbye, Zeyu Mao

Industry Collaboration:

- PowerWorld Corporation

Description of research activity: Absolute security is not possible. Therefore, it is important to improve the ability of the energy delivery sector to detect, effectively intervene, and if necessary recover from cyber incidents. Emerging needs to coordinate among interdependent energy delivery systems in real time lead to further security requirements on the supporting cyber infrastructure. Necessary to the development of security controls in the operational grid is a means of bringing together detailed simulations of the grid's different components, to assess the impact of these controls on the real-time behavior of the system. The activity has three goals. First, the development of federated simulations of the power systems and its underlying cyber infrastructure, coupled with key real-time information-sharing and coordination mechanisms. We will meet this objective in part by leveraging existing commercial packages, such as interactive power system transient stability-level simulations, and in part by developing new prototype packages. Second, the development of publicly available synthetic case models that can be used within these environments. (While models of actual infrastructure are best, NDAs limit the use of such models in cooperative university research; hence the need for the synthetic case models.) Third, to develop compelling case studies and utilize the environment to develop effective analytics and visualizations that can be used to help the energy delivery sector detect security incidents, intervene, and, if necessary, recover.

This activity is scheduled to complete by June 1, 2017.

How does this research activity address the Roadmap to Achieve Energy Delivery Systems Cybersecurity?
This research activity aims to improve the management and detection of cyber incidents by developing an interactive simulation environment. This interactive and expendable environment can be used to study algorithms for real-time incident detection and analysis, test/verify new theories and other cyber security research on energy delivery systems.

Summary of EDS gap analysis: The emerging needs for real-time coordination among interdependent energy delivery systems are creating new security requirements for the supporting cyber infrastructure. To help meet those new requirements, this activity is working to improve capabilities for incident detection and management on energy delivery systems.

Full EDS gap analysis: As the smart grid moves forward, there is a growing need for improved management and detection methods for cyber incidents. As mentioned in the “Roadmap to Achieve Energy Delivery Systems Cybersecurity” [1], managing cyber incidents is becoming increasingly important, because cyber assaults are becoming more sophisticated and common [2], and EDS systems are becoming more vulnerable for cyber attackers. Effective incident management through all its phases, that is, prevention, preparedness, response, recovery and mitigation, presents a number of challenges to the responsible agencies and researchers [3]. One major challenge is to improve the ability of the energy delivery sector to detect, effectively intervene, and if necessary recover from cyber incidents. An individual EDS simulation is not useful for solving such events in the cyber-physical system.

With the large-scale implementation of smart devices in the energy system, emerging needs to coordinate among interdependent energy delivery systems in real time lead to further security requirements on the supporting cyber infrastructure. Necessary to the development of security controls in the operational grid are means of bringing together detailed simulations of the grid's different components and to assess the impact of these controls on the behavior of the system.

Interactive simulations have a long history in the EDS field; however, the key distinctions are often associated with the simulation time frame. In order to make such simulations computationally tractable and to simplify the modeling, the time frame of interest needs to be considered. The first interactive digital simulations were operator training simulators (OTSs) with [4] 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 [5] 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 interconnected systems with tens of thousands of buses. On an even longer time frame, [6] 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. 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 [7] 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 microseconds they are often limited to smaller systems, unless large amounts of parallel computation are used.

In order to simulate different components in the EDS system, the interactive simulation environment should sit between the extremely short time frame of [9] and the uniform frequency model of [6]. That is, simulating the system with a step size on the order of ¼ or ½ cycles (i.e., 0.004-0.008 seconds). In power systems this is known as the 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 [8]. 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 [9], [10], [11], [12]. Thus, cyber security issues in the EDS system can be considered [13].

To meet the need for improving the cyber incident detection and management in the EDS, this activity is designed to develop an interactive, expandable and coupled simulation, which can be extremely useful for incident management research and other cyber security research.

Bibliography:

[1] Energy Sector Control Systems Working Group, “Roadmap to Achieve Energy Delivery Systems Cybersecurity,” available at https://energy.gov/oe/downloads/roadmap-achieve-energy-delivery-systems-cybersecurity-2011.

[2] ICS-CERT MONITOR, available at https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Apr-Jun2013.pdf

[3] S. Jain, C. R. McLean, “An Integrated Gaming and Simulation Architecture for Incident Management Training,” NISTIR 7295, 2006.

[4] 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.

[5] 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

[6] 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

[7] 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

[8] 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

[9] 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

[10] 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

[11] 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

[12] 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

[13] 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.