Cyber-Physical Educational Simulator for Cyber-Power Infrastructure Security

Saman Zonouz, Anurag Srivastava*
Electrical and Computer Engineering,
*Electrical Engineering and Computer Science
University of Miami, *Washington State University
s.zonouz@miami.edu, *asrivast@eecs.wsu.edu*

The bulk electricity delivery system known as the *power grid* is extremely fundamental to most aspects of modern society [4, 5, 7–18]. Power grid critical infrastructures form a vast and interconnected cyber-physical network for delivering electricity from generation plants to end-point consumers. Due to their importance, power control networks have been a very attractive attack surface for malicious attackers and nation-state terrorists to penetrate in the network and consequently cause catastrophic physical damage. Remote malicious cyber attacks caused approximately $100 million of damage cost in 2009 [1]. The most recent control system malware called Stuxnet [2] was crafted to sabotage nuclear power plants. Stuxnet specifically raised new questions about power grid security protection [3] which is strictly recommended by the government as destruction of those systems would have a debilitating impact on national security [6].

Currently, to protect power grid critical infrastructures, expert power system operators, sitting in *control network* rooms, monitor and control the cyber network as well as the underlying physical system in order to guarantee secure energy delivery. Traditionally, power grid operators gain their expertise and experience solely through working with physical system training simulators, which model only the physical systems ignoring the cyber assets, or working with an actual operational power grid where a mistake may result in catastrophic consequences such as large-scale cascading failures and power blackouts. Consequently, a better training and experience transferring solution is needed to make sure that inexperienced operators learn about the potential failures and security incidents as well as how to respond to them and take appropriate recovery actions with minimum effort and without any potential damage on the actual operational power grid. Additionally, there needs to be an assessment method to evaluate whether the operator has gained sufficient amount of expertise and hence can handle real-world conditions before he/she is allowed to work on the actual infrastructure.

Our vision is a conceptual integration of a cyber-attack simulator into the existing simulators, to study the difference in operator response to contingencies with/without the consideration of cyber network configuration. The proposed solution provides a complete simulated power grid infrastructure including the control center environment as well as the physical power system. Additionally, our proposed solution is capable of realistic simulation of malicious cyber-physical attacks that originate at remote cyber assets as well as reactive and proactive corrective control actions to fix cyber exploitations and power contingencies. Furthermore, during an interaction with an expert

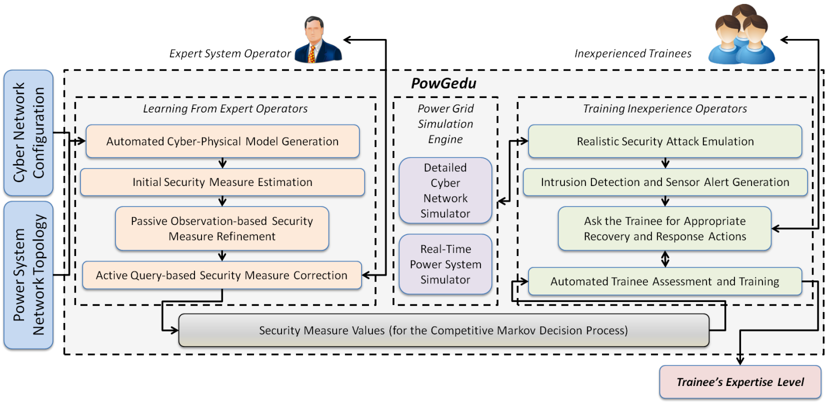
Expert System Operator
Inexperienced Trainees
Cyber Network Configuration
Power System Network Topology
PowGedu
Learning From Expert Operators
Automated Cyber-Physical Model Generation
Initial Security Measure Estimation
Passive Observation-based Security Measure Refinement
Active Query-based Security Measure Correction
Power Grid Simulation Engine
Detailed Cyber Network Simulator
Real-Time Power System Simulator
Training Inexperience Operators
Realistic Security Attack Emulation
Intrusion Detection and Sensor Alert Generation
Ask the Trainee for Appropriate Recovery and Response Actions
Automated Trainee Assessment and Training
Security Measure Values (for the Competitive Markov Decision Process)
Trainee's Expertise Level

Figure 1: Bird's Eye View of the Proposed Architecture

operator, our proposed framework learns appropriate handling of various attack scenarios by creating mathematical behavioral models. Consequently, the framework makes use of those models during an interaction with an inexperienced operator to perform effective knowledge transfer so that inexperienced operators also learn how to handle various attacks appropriately.

The proposed framework consists of several subsystems that achieve its ultimate overall objective cooperatively. Our proposed solution's operation consists of two major phases: 1) learning from simulation; and 2) training operators. During the first phase, the proposed framework is used by expert operators who go through several cyber-physical failure and intrusion scenarios on the user-friendly graphical interface that is backed up with the cyber-physical system and failure simulation engine. During the expert operator interaction. Our proposed solution observes his or her reactions, i.e., corrective control actions, in every system state and calculates a mathematical behavioral model that is a game-theoretic Markov decision process with learned numerical parameters, i.e., state security measures. It is noteworthy that the expert operators could be replaced with a scripted list of appropriate control actions for various system states; such lists are usually composed during the power grid planning efforts in practice nowadays. More specifically, to accelerate the learning model convergence, the introduced framework calculates a rough system model automatically using the power-based impact index. Later on, during the expert operator interaction, the rough values are further refined to represent the expert knowledge precisely.

The second phase aims at training inexperienced operators to consider both cyber and power networks while selecting the corrective control actions. The ultimate goal is to achieve this objective using a simulated environment without the need for interaction with the actual operational critical infrastructure. In particular, the proposed solution with the learned set of system models and parameters can be downloaded and used simultaneously by several (possibly remote) inexperienced trainees. Our introduced framework makes use of its hybrid cyber network and power system simulation engines to emulate realistic attack and failure scenarios for the inexperienced who should observe the situation on their screen and decide upon the optimal control action from the list provided by the introduced framework. In the meanwhile, our proposed solution emulates an expert operator internally by implementing a game-theoretic optimization solution to pick the optimal control action according to the created learned system models. Consequently, the presented engine compares the sequence of actions provided by each trainee and the calculated optimal action sequence, and verifies whether those two sequence match.

References

[1] Electricity grid in U.S. penetrated by spies, available online at `http://online.wsj.com/article/SB123914805204099085.html`, 2009.

[2] Nicolas Falliere, Liam O. Murchu, and Eric Chien. W32.Stuxnet Dossier. Technical report, Symantic Security Response, October 2010.

[3] Patrick McDaniel and Stephen McLaughlin. Security and privacy challenges in the smart grid. *IEEE Security and Privacy*, 7:75–77, 2009.

[4] Stephen McLaughlin, Brett Holbert, Ahmed Fawaz, Robin Berthier, and Saman Zonouz. A multi-sensor energy theft detection framework for advanced metering infrastructures. *IEEE Journal on Selected Areas in Communications*, 2013.

[5] Stephen McLaughlin, Pohly Devin Zonouz, Saman, and McDaniel Patrick. A trusted safety verifier for process controller code. In *Networks and Distributed Systems Symposium (NDSS)*, 2014.

[6] Keith Stouffer, Joe Falco, and Karen Kent. Guide to supervisory control and data acquisition (SCADA) and industrial control systems security. In *SPIN*, 2006.

[7] Saman Zonouz. *Game-Theoretic Intrusion Response and Recovery Engine*. PhD thesis, University of Illinois at Urbana-Champaign (UIUC), 2011.

[8] Saman Zonouz, Robin Berthier, Himanshu Khurana, William Sanders, and Tim Yardley. Seclius: An information flow-based, consequence-centric security metric. *IEEE Transactions on Parallel and Distributed Computing*, 2013.

[9] Saman Zonouz, Charles Davis, Kate Davis, Rakesh Bobba, Robin Berthier, Peter Sauer, and William Sanders. SOCCA: A Security-Oriented Cyber-Physical Contingency Analysis in Power Infrastructures. *IEEE Transactions on Smart Grid*, 2012.

[10] Saman Zonouz and Parisa Haghani. Cyber-physical security metric inference in smart grid critical infrastructures based on system administrators responsive behavior. *Elsevier Computers & Security*, 2013.

[11] Saman Zonouz, Amir Houmansadr, and Robin Berthier. Secloud: A cloud-based comprehensive and lightweight security solution for smartphones. *Elsevier Computers & Security*, 2013.

[12] Saman Zonouz, Amir Houmansadr, and Parisa Haghani. EliMet: Security metric elicitation in power grid critical infrastructures by observing system administrators' responsive behavior. In *42nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pages 1–12, 2012.

[13] Saman Zonouz, Kaustubh R. Joshi, and William H. Sanders. Cost-aware systemwide intrusion defense via online forensics and on-demand detector deployment. In *Proceedings of CCS-SafeConfig: the 3rd ACM Workshop on Assurable & Usable Security Configuration*, pages 71–74, 2010.

[14] Saman Zonouz, Kaustubh R Joshi, and William H Sanders. Floguard: cost-aware systemwide intrusion defense via online forensics and on-demand ids deployment. In *Springer Computer Safety, Reliability, and Security*, pages 338–354. 2011.

[15] Saman Zonouz, Himanshu Khurana, William Sanders, and Tim Yardley. RRE: A game-theoretic intrusion Response and Recovery Engine. In *Proceedings of the 39th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pages 439–48, 2009.

[16] Saman Zonouz, Himanshu Khurana, William Sanders, and Tim Yardley. RRE: A Game-Theoretic Intrusion Response and Recovery Engine. *IEEE Transactions on Parallel and Distributed Systems*, 2013.

[17] Saman Zonouz, Katherine M Rogers, Robin Berthier, Rakesh B Bobba, William H Sanders, and Thomas J Overbye. SCPSE: Security-Oriented Cyber-Physical State Estimation for Power Grid Critical Infrastructures. *IEEE Transactions on Smart Grid*, 2012.

[18] Saman Zonouz, Aashish Sharma, HV Ramasamy, Zbigniew T Kalbarczyk, Birgit Pfitzmann, Kevin McAuliffe, Ravishankar K Iyer, William H Sanders, and Eric Cope. Managing business health in the presence of malicious attacks. In *IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshops (DSN-W)*, pages 9–14, 2011.