



Attack-Resilient and Secure EMS: Design, Algorithms, Operational Protocols, and Evaluation

Final Project Report

S-72

Power Systems Engineering Research Center
*Empowering Minds to Engineer
the Future Electric Energy System*

A large, stylized yellow star graphic is positioned in the bottom right corner of the page. It is a five-pointed star with a circular center, rendered in a thick yellow line.

Attack-Resilient and Secure EMS: Design, Algorithms, Operational Protocols, and Evaluation

Final Project Report

Project Team

Lalitha Sankar, Project Leader

Oliver Kosut

Arizona State University

Manimaran Govindarasu

Iowa State University

Graduate Students

Zhigang Chu

Roozbeh Khodadadeh

Andrea Pinceti

Jiazi Zhang

Arizona State University

Vivek Kumar Singh

Pengyuan Wang

Iowa State University

PSERC Publication 18-06

September 2018

For information about this project, contact:

Lalitha Sankar
Arizona State University
School of Electrical, Computer, and Energy Engineering
Engineering Research Center
551 E. Tyler mall, Room 585
Tempe, AZ 85281
Phone: 480-965-4953
Email: lalitha.sankar@asu.edu

Power Systems Engineering Research Center

The Power Systems Engineering Research Center (PSERC) is a multi-university Center conducting research on challenges facing the electric power industry and educating the next generation of power engineers. More information about PSERC can be found at the Center's website: <http://www.pserc.org>.

For additional information, contact:

Power Systems Engineering Research Center
Arizona State University
527 Engineering Research Center
Tempe, Arizona 85287-5706
Phone: 480-965-1643
Fax: 480-727-2052

Notice Concerning Copyright Material

PSERC members are given permission to copy without fee all or part of this publication for internal use if appropriate attribution is given to this document as the source material. This report is available for downloading from the PSERC website.

© 2018 Arizona State University. All rights reserved.

Acknowledgements

We wish to thank Dr. Kory Hedman and his students from Arizona State University for their continuous support with the implementation and integration of software tools into the EMS platform.

We would also like to thank each and every one of our industry advisers. In particular we wish to thank the following people for their helpful suggestions and insightful comments: Evangelos Farantatos (EPRI), Benjamin Kroposki (NREL), Eugene Litvinov (ISONE), Harvey Scribner (SPP), and Mark Westendorf (MISO).

Executive Summary

During the past decade, the electric utility industry has increasingly used a combination of Energy Management System (EMS) and Supervisory Control and Data Acquisition (SCADA) systems to analyze, manage, and control the power system. The use of these monitoring and computing systems has helped power systems operators and utilities (stakeholders) run more efficiently, securely, and economically. Harnessing the processing power of modern computers and advances in telecommunication and information technology, these EMSs ensure that the systems operators have an accurate understanding of the network health and real-time status while ensuring wide-area control and situational awareness.

The increased reliance on information technology (IT) necessitates addressing the associated cybersecurity risks which are inherent to any cyber-physical system (CPS). The Department of Energy (DOE), Department of Homeland Security (DHS), and the North American Electric Reliability Corporation (NERC) have identified concerns that the grid is vulnerable to sophisticated coordinated cyber-attacks. With this project we addressed the following fundamental question: can reasonably realistic (i.e., attackers with limited capabilities) cyber-attacks be modeled and tested on electric power system (EPS) simulation platforms to evaluate: (a) attack severity and consequences, and (b) resiliency of energy management systems (EMSs) to such attacks?

In Part 1 of the project, the ASU team developed a software EMS platform on which sophisticated attacks and countermeasures were tested, validated, and demoed. The work of the ISU team in building a hardware testbed for cybersecurity studies is described in Part 2.

Part 1: Development of commercial grade energy management system and testing of cyber-attacks and countermeasures

The goal of this project is to identify realistic cyber-threats and vulnerabilities of modern EMSs as well as to propose countermeasures that system operators can implement in their systems. To obtain the most representative and accurate assessments possible, we developed a software platform which very realistically mimics the functions and operation of real world energy management systems. This java-based EMS platform, developed in collaboration with IncSys, includes a state estimator (SE) with bad data detector, real-time contingency analysis (RTCA), and security constrained economic dispatch (SCED). This complex tool allowed us to both verify how stealthy cyber-attacks are not detected by the EMS as well as observing the resulting physical consequences in a precise way. The platform has been used to observe the resiliency of systems of different sizes, varying from 200 to over 2000 buses, against a diverse number of attacks ranging from line overloads, to hiding post-contingency violations and stability limit violations.

Intelligently designed false data injection (FDI) attacks have been shown to be able to by-pass the state estimation bad data detector present in an energy management system (EMS) and to introduce arbitrary errors in the states of the system under attack. These false measurements can be computed so that they will create unobservable physical consequences, such as line overflows. As part of the analysis of the vulnerability of real power systems to these types of attacks, in this project we have

formulated four computationally efficient problems that can be used to design attacks on realistic, large scale systems.

The first two methods are based on row and column generation techniques which are useful to solve large linear programs which would otherwise be intractable. Row generation, which reduces the number of constraints, is used on line flow limits: we exclude all the constraints corresponding to lines which have a small power flow, as those are unlikely to be active in the optimal solution. If any of the constraints which have been omitted are violated in the final solution, they are added back to the problem and a new solution is calculated. The second algorithm uses both row generation and column generation. In this case, generators which are unlikely to modify their output as a consequence of the attack are removed from the problem, reducing the number of binary variables. The third method is based on the difference maximization algorithm, and in addition to being a linear program it also provides upper and lower bounds on the solution. The last algorithm uses Benders' decomposition, in which the problem is divided into two sub-problems which are solved iteratively.

These four algorithms have been tested on different test systems to compare their performance from a computational efficiency point of view as well as efficacy of the computed attacks. Moreover, the results have been used to assess the vulnerability of the systems. In general, every time a line is congested it is possible to create an attack which will lead to an overflow on such line. Lastly, the results are not only dependent on the level of congestion of the target line but also on the overall congestion of the system.

One of the assumptions of the attacks described is that the attacker has knowledge of system-wide information such as topology, generation data, etc. As we are looking at large scale test cases, it is reasonable to assume that it would be hard for an attacker to be able to gather full system data. For this reason, in this project we look at the possible physical consequences resulting from attacks designed with limited information. Specifically, we assume that the attacker has knowledge of only a small subgraph of the network and absolutely no knowledge of the outside system. This requires the attacker to be able to model the system response without any knowledge on its topology, generation, and loads; to this end, multiple linear regression can be used to predict the power injection at the boundary buses of the attack subgraph. This modified attack model is tested on the IEEE 24 and IEEE 118 bus systems, showing that successful attacks can be computed, even though the magnitude of the overflows is lower than the case in which the attacker has full knowledge of the system.

Network topology is important system data used in various data processing modules in the EMS. Changes in topology can result from either system incidents or malicious physical attacks; but, in general, such topology alterations can be detected in the cyber layer. However, a sophisticated attacker can launch cyber-attacks that alter the topology information in an unobservable manner; furthermore, they can also mask a physical attack via a cyber-attack to create a more coordinated attack. This type of unobservable cyber-attacks on topology can be of two types: line-maintaining and line-removing. For a line-maintaining attack, the attacker changes measurements and line status information to make it appear that line that is not in the system is now shown as active at the control center via SCADA data; the opposite is achieved by a line-removing attack. Using similar techniques as the attacks described above, we have shown that this type of coordinated

attacks is feasible and cannot be detected by current EMS technology. As per our results on the IEEE 24 bus system, large unobservable overloads of transmission lines can be achieved.

After having identified vulnerabilities of large scale systems that can be exploited by gaining access to the EMS, we focus our attention on possible countermeasures to protect the system from cyber-attacks. The FDI attacks described in the previous paragraphs create physical consequences by injecting false measurements from which the system operator gathers a wrong representation of the system loads. It is the mismatch between the real loads and the generation redispatch resulting from the fake loads which lead to the overloading of transmission lines. Based on this observation we designed three detectors, each relying on a different machine learning algorithm, to analyze and validate the observed loads in real time. The detectors are designed and trained to learn the patterns which exist between real system loads; when a new set of measurements is processed by the state estimator, the resulting loads are checked for the previously learnt patterns to understand if they represent normal or anomalous data. The three machine learning techniques used are: nearest neighbor, support vector machine, and replicator neural network. From the tests performed on the IEEE 30 bus system and on the synthetic Texas system, we have verified the high detection capabilities of the three detectors. Besides the very satisfactory performance of the algorithms designed, the importance of this approach lies in the fact that this countermeasure relies on data which is already being collected at the control center. Implementing these detectors in a real EMS would be fairly easy and accessible to any system operator.

Part 2: Anomaly detection for wide-area protection and control in smart grid

This research has focused on the design, development, and evaluation of robust algorithms for anomaly detection and mitigation for a couple of key applications in wide-area protection and control. The central theme of this research is to leverage Cyber-Physical System (CPS) properties of the grid and machine-learning algorithms to design robust Anomaly Detection System (ADS) that detects anomalies beyond the traditional information technology-based intrusion detection solutions. The following are the two key contributions. (1) The development of anomaly detection algorithm for Remedial Action Scheme (RAS), a wide-area protection scheme using a multi-agent based framework with machine-learning algorithms to distinguish attack behaviors from normal and fault behaviors, which in turn helps to achieve optimal protection decisions, such as load shedding. (2) The development of two anomaly detection algorithms for Automatic Generation Control (AGC): (a) model-based ADS and machine learning-based AGC. The former leverages the historical data as the redundant measurement to create different types of bounds/rules to detect attacks. The machine learning-based ADS deploys semi-supervised clustering algorithm for detecting cyber-attacks. The performance of the proposed anomaly detection and mitigation algorithms were evaluated through a combination of simulation and testbed-based experimental studies with realistic system models, datasets, and use-case scenarios. The results and testbed-based evaluations show that these algorithms achieve detection accuracies to the extent that they are ready for pilot deployment and evaluations. The research has also advanced the state-of-the-art research in CPS security for the power grid and the innovative use of machine-learning algorithms. This project also contributed to the workforce development in training several graduate students in research and also offering a couple of industry short courses for the utility industry.

Project Publications:

- [1] J. Zhang, Z. Chu, L. Sankar and O. Kosut, "Can Attackers with Limited Information Exploit Historical Data to Mount Successful False Data Injection Attacks on Power Systems?," in *IEEE Transactions on Power Systems*.
- [2] A. Pinceti, L. Sankar, and O. Kosut, "Load Redistribution Attack Detection using Machine Learning: A Data-Driven Approach", 2018 *IEEE Power & Energy Society General Meeting*, August 5-9, 2018, Portland, Oregon, USA, 2018
- [3] Z. Chu, J. Zhang, O. Kosut and L. Sankar, "Evaluating power system vulnerability to false data injection attacks via scalable optimization," *2016 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Sydney, NSW, 2016, pp. 260-265.
- [4] Z. Chu, J. Zhang, O. Kosut and L. Sankar, "Vulnerability Assessment of Large-scale Power Systems to False Data Injection Attacks," [Online]. Available: <https://arxiv.org/abs/1705.04218>
- [5] V. Singh, A. Ozen, M. Govindarasu, "A Hierarchical Multi-Agent Based Anomaly Detection for Wide-Area Protection in Smart Grid," Resilience Week 2018, August 20-23, Denver, Colorado, USA, 2018, (accepted for publication).
- [6] K. Sarangan, V.K. Singh, M. Govindarasu, "Cyber Attack-Defense Analysis for Automatic Generation Control with Renewable Energy Sources," *North American Power Symposium (NAPS) 2018*, September 9-11, Fargo, North Dakota, USA, 2018, (accepted for publication).
- [7] V.K. Singh, H. Ebrahim, M. Govindarasu, "Security Evaluation for Two Intrusion Detection Systems in Smart Grid SCADA Environment," *North American Power Symposium (NAPS) 2018*, September 9-11, Fargo, North Dakota, USA, 2018, (accepted for publication).
- [8] P. Wang, M. Govindarasu, "Anomaly Detection for Power System Generation Control based on Hierarchical DBSCAN," *North American Power Symposium (NAPS) 2018*, September 9-11, Fargo, North Dakota, USA, 2018, (accepted for publication).
- [9] V. Singh, M. Govindarasu, "Decision Tree Based Anomaly Detection for Remedial Action Scheme in Smart Grid using PMU Data," *IEEE Power and Energy Society 2018 General Meeting*, August 5-9, 2018, Portland, Oregon, USA, 2018.

Student Theses:

- [1] Jiazi Zhang. *Vulnerability Analysis of False Data Injection Attacks on Supervisory Control and Data Acquisition and Phasor Measurement Units*. PhD Dissertation, Arizona State University, Tempe AZ, 2017