



Synchrophasor Data-Analytics for a More Resilient Electric Power System

Final Project Report

S-74

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



Synchrophasor Data-Analytics for a More Resilient Electric Power System

Final Project Report

Project Team

Anamitra Pal, Project Leader

Lalitha Sankar

Arizona State University

Christopher DeMarco
University of Wisconsin-Madison

Graduate Students

Reetam Sen Biswas

Zhigang Chu

Andrea Pinceti

Arizona State University

Sowmya Acharya
Jong Min Lim
University of Wisconsin-Madison

PSERC Publication 19-02

September 2019

For information about this project, contact:

Anamitra Pal
Arizona State University
School of Electrical, Computer, and Energy Engineering
P.O. BOX 875706
Tempe, AZ 85287-5706
Phone: 480-965-2882
Fax: 480-727-2052
Email: anamitra.pal@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.

© 2019 Arizona State University. All rights reserved.

Acknowledgements

This is the final report for the Power Systems Engineering Research Center (PSERC) research project titled “Synchrophasor data-analytics for a more resilient electric power systems” (project S-74). We express our appreciation for the support provided by PSERC’s industry members. In particular we wish to thank industry advisors Alan Engelmann (ComED), Blake Buescher (MISO), Zhongyu Wu (MISO), Di Shi (GEIRI North America), Jay Giri (GE Energy), Reynaldo Nuqui (ABB), Evangelos Farantatos (EPRI), Mahendra Patel (EPRI), Dejan Sobajic (NYISO), Curtis Roe (ATC), Emanuel Bernabeu (PJM), Jianzhong Tong (PJM), George Stefopoulos (NYPA), Gordon Matthews (BPA), Qiang Zhang (ISONE), Orlando Ciniglio (Idaho Power Company), Brian Keel (SRP), Atena Darvishi (NYPA), Harvey Scribner (SPP), and Michael Nugent (SPP).

Executive Summary

Deployment of synchrophasor infrastructure is occurring at an exceptionally fast rate in the US power grid; especially at the transmission and the sub-transmission networks. The world's first three-phase phasor measurement unit (PMU)-only linear state estimator has been developed and is running successfully at Dominion Virginia Power. However, the data obtained from PMUs has been primarily used for *forensics* analysis in the past; i.e., *after* an undesirable event has occurred. This PSERC S-74 project is a step towards the utilization of PMU data in *near-real-time* environment. The main focus of this project is to develop algorithms that can distinguish normal system operations from anomalous system behavior using synchrophasor data; and consequently, enhance situational awareness for operational decision making. In this research, following applications of PMU data have been considered:

- (a) *Power system monitoring application*: faster islanding detection and robust power system asset health monitoring;
- (b) *Power system cyber-protection application*: evaluating the efficacy of PMUs to combat cyber-attacks on the SCADA system and developing data analytics algorithm using synchrophasor data to enhance resiliency against cyber-attacks;
- (c) *Power system control application*: Predicting system stability in presence of renewable generation.

To be able to produce the research deliverables with respect to the three above-mentioned applications of synchrophasor technology, the tasks were distributed among the three researchers in the following way: *Task 1*- power system monitoring application (led by Anamitra Pal and his students, and supported by Lalitha Sankar and her students), *Task 2*- power system cyber-protection application (led by Lalitha Sankar and her students, and supported by Anamitra Pal and his students), and *Task 3*- power system control application (led by Christopher DeMarco and his students, and supported by Anamitra Pal and his students).

The first sub-task (Task 1.1) of the monitoring application of this project was power system islanding detection. Synchrophasor measurement based wide-area power system islanding detection has mostly relied on voltage phase angle differences between two buses across the islanded systems. However, *noise due to instrument transformers* can severely degrade the measurement quality and in turn *alter the accuracy of the detection technique*. The errors in the voltage angles could be as high as $\pm 4^\circ$ with respect to existing standards. Such high errors in the PMU data due to the instrumentation channel errors, could result in considerable misclassification in islanding detection. Therefore, a new PMU-based passive islanding detection technique is proposed *which is immune to instrumentation channel errors*. The proposed islanding detection technique monitors the *voltage phase angle difference trajectory* measured from the same PMU as a means to counter the instrumentation channel errors. The voltage phase angle difference is accumulated over a window of PMU samples to minimize misclassification. This approach is termed “cumulated sum of voltage phase angle difference (CUSPAD)”.

The second sub-task (Task 1.2) of the monitoring application of this project was power system asset health monitoring. One of the biggest challenges faced by the electric power industry is the successful management of its aging infrastructure. Untimely loss of a power system's critical equipment, e.g., large power transformer (LPT) could be catastrophic to the grid operations. Power system equipment provide information about their health through the sensors that monitor them.

The data captured by these sensors is a treasure-house of knowledge because it contains information about actual as well as potential failures. The sensors for LPTs include online dissolved gas analyzers (DGAs), power quality (PQ) meters, potential discharge (PD) testers, and bushing monitors, amongst others. *However, the output generated by many of these sensors are not monitored continuously.* It is only when they generate an alarm that their outputs are considered for decision-making. Now, it is possible that the sensors generate alarms when the device is very close to an imminent failure, and no possible intervention (at that stage) can prevent the failure and/or subsequent disruption from occurring. PMUs provide time-synchronized measurements of voltage and current phasors at the timescale of 30 to 60 samples per second. The main research question being explored in this sub-task is as follows: *could PMU measurements capture the deteriorating health of an LPT?* The research done in the course of this sub-task has found that the *signal-to-noise ratio* (SNR) of PMU measurements is a robust metric that can quantify transformer health in real-time. SNR is a statistical measure of the strength of the desirable components to that of undesirable components present in a signal. When an equipment is malfunctioning and is close to failure, noise component in the signal tends to increase, resulting in a wider SNR bandwidth. The asset health monitoring scheme proposed in this research utilizes data-driven methods to monitor the SNR bandwidth obtained from PMU measurements for real-time assessment of equipment health.

One of the sub-tasks (Task 2.1) of the power system cyber-protection application was to create a realistic synthetic test system that can be used to verify the performance of different PMU-based applications as well as to test cyber-attacks and countermeasures. A crucial aspect in designing a testbed that can be used to observe system behaviors at PMU sampling speeds is to accurately model the behavior of the system loads. In fact, not considering faults or other such unpredictable events, the dynamics of the system are mostly governed by the variation of loads over time and how the generators respond to such changes. The power system cyber-protection application of this project proposed a new data-driven algorithm for the generation of synthetic bus-level time series load data at 30 samples per second that can be applied to any system model. The proposed data-driven algorithm is unique because it can learn the spatial and temporal correlation from a dataset of real system loads and use the learnt model to generate new synthetic data that retains the same characteristics. A utility in the Western Interconnection (WI), which is also a part of PSERC provided the data that was used to investigate the spatio-temporal correlation in the utility scale PMU data. We have used singular value decomposition (SVD) to screen out the dominant load patterns in the real PMU data and proposed a generalized scheme to create synthetic data in a test system that retains the spatio-temporal attributes of real PMU data.

The second sub-task (Task 2.2) of the power system cyber-protection application was to investigate the vulnerability of PMUs to cyber-attacks. One of the simplest ways in which PMU data can be compromised by a cyber-attacker is via false data injection (FDI). FDI attacks involve an intelligent attacker who replaces a subset of measurements with counterfeits. Prior research had shown that a sub-class of cyber-attacks can bypass the conventional bad data detector, that does not consider the *temporal correlation* in PMU measurements to detect an anomaly. This PSERC project was the first effort to investigate if *predictive-filters* could be used to identify a cyber-attack. Predictive filters study the temporal correlations in PMU measurements from prior data to predict the future measurements. If the predicted measurements do not correspond to the actual measurements, it indicates an anomaly. Two types of cyber-attacks have been investigated in this research: *sudden attack* and *ramping attack*. A *sudden cyber-attack* refers to the situation when an

attacker injects false measurements suddenly at a specific time. A *ramping cyber-attack* refers to the scenario, when the attacker injects the false measurements slowly over a period of time. Our research findings have shown that the sudden *cyber-attacks* could be detected by predictive filters. However, it is more challenging to detect an intelligently designed *ramping cyber-attack*.

The power system control application (Task 3) of this project involved analysis of power system voltage stability using synchrophasor data. Major power system outages take place when a range of different phenomena occur in quick succession. However, it has often been found that the loss of voltage stability, and ultimately voltage collapse are the immediate precursors of the outage. In current utility practice, operational measures of vulnerability to voltage instability are based on the state estimator that uses a network model to compute the steady state operating point of the grid, with typical update rates in the order of several minutes. The dependence on accurate knowledge of network parameters and topology, and relatively infrequent update rate may be viewed as shortcomings of the existing practice. Among advances that can support new approaches has been a proliferation of vastly improved measurement technology in the grid. In the bulk transmission system, these improved measurements have predominantly taken the form of synchrophasor measurements via PMUs. Typical reporting rates for such measurements are 30 or 60 samples per second (25 or 50 for 50 Hz-based networks). The much higher reporting rate from PMUs suggests the value of developing efficient PMU-based metrics of system performance, which may be computed in near real-time. The metric employed here was based on SVD, alternately known as Karhunen-Loeve decomposition, principal component analysis (PCA), or proper orthogonal decomposition (POD). In power system engineering, SVD has been employed in the context of “full-model-based” analysis to assess voltage stability by examination of the smallest singular value of the power flow Jacobian. Most of the research on voltage stability had relied on full dynamic models. On the contrary, the work presented here could be viewed as an evolution of a model-free approach for voltage stability assessment; which pre-dominantly relies on PMU data. The proposed work also involved precise identification of “noise dominated” measurement channels that contributes no useful information to the SVD calculation and are therefore considered good candidates for removal from the measurements set.

Project Publications:

- [1] R. Sen Biswas, and A. Pal, “A robust techno-economic analysis of PMU-based islanding detection schemes,” in *Proc. IEEE Texas Power and Energy Conf. (TPEC)*, College Station, TX, pp. 1-6, 9-10 Feb. 2017 [**Third Best Paper Award**].
- [2] M. Barkakati, R. Sen Biswas, and A. Pal, “A PMU based islanding detection scheme immune to additive instrumentation channel errors”, *accepted 2019 North American Power Symposium (NAPS)*, Wichita, Kansas, USA.
- [3] K. Basu, M. Padhee, S. Roy, A. Pal, A. Sen, M. Rhodes, and B. Keel, “Health monitoring of critical power system equipment using identifying codes,” in *Proc. CRITIS 2018 Conf.* [**PI Pal received the 2018 Young CRITIS Award for this research**].
- [4] M. Padhee, R. Sen Biswas, A. Pal, K. Basu, and A. Sen, “Identifying unique power system signatures for determining vulnerability of critical power system assets,” *submitted to ACM sigmetrics performance evaluation review (PER)*.
- [5] A. Pinceti, O. Kosut, and L. Sankar, “Data-driven generation of synthetic load datasets preserving spatio-temporal features,” *accepted 2019 IEEE Power & Energy Society General Meeting (PESGM)*, Atlanta, GA.

- [6] Z. Chu, J. Zhang, O. Kosut, and L. Sankar, "Unobservable false data injection attacks against PMUs: feasible conditions and multiplicative attacks," in *Proc. IEEE SmartGridComm* 2018, Aalborg, Denmark, Oct. 2018.
- [7] Z. Chu, A. Pinceti, R. Sen Biswas, O. Kosut, A. Pal, and L. Sankar, "Can predictive filters detect gradually ramping false data injection attacks against PMUs?" accepted *IEEE SmartGridComm* 2019, China.
- [8] J. Zhang, Z. Chu, L. Sankar and O. Kosut, "False data injection attacks on phasor measurements that bypass low-rank decomposition," in *Proc. 2017 IEEE Intl. Conf. Smart Grid Comm. (SmartGridComm)*, Dresden, pp. 96-101, 2017.
- [9] S. Acharya, and C.L. DeMarco, "Exploiting Network-induced Correlation for Efficient Compression of PMU Data," in *Proc. 2018 North American Power Symposium (NAPS)*, Fargo, ND, 2018.
- [10] M. Lim, and C.L. DeMarco, "SVD-based voltage stability assessment from phasor measurement unit data," *IEEE Trans. Power Syst.*, vol. 31, no. 4, pp. 2557-2565, Jul. 2016.

Student Theses:

- [1] M. Barkakati, "Transmission system reliability: monitoring and analysis", M.S. Thesis, Arizona State University, 2018.