Poster: Integrating Historical and Real-Time Anomaly Detection to Create a More Resilient Smart Grid Architecture

Extended Abstract

Spencer Drakontaidis, Michael Stanchi, Gabriel Glazer, Antoine Davis, Madison Stark, Caleb Clay, Jason Hussey, Nicholas Barry, Aaron St. Leger, Suzanne J. Matthews
Department of Electrical Engineering & Computer Science
West Point, NY
[spencer.drakontaidis,michael.stanchi,gabriel.glazer,antoine.davis,madison.stark,caleb.clay,jason.hussey,nicholas.barry,aaron.stleger,suzanne.matthews]@usma.edu

CCS CONCEPTS

• **Hardware** → **Smart grid**; • **Computer systems organization** → *Embedded and cyber-physical systems*; • **Security and privacy** → Intrusion/anomaly detection and malware mitigation;

KEYWORDS

Smart Grid, Anomaly Detection, Apache Spark, Raspberry Pi

Ensuring the security of the power grid is critical for national interests and necessitates new ways to detect power anomalies and respond to potential failures. In this poster, we describe our efforts to develop and optimize analysis methodologies for a 1000 : 1 scale emulated smart grid at the United States Military Academy [2]. In contrast to previous work [3, 4], we explore historical analysis using Apache Spark [5] and integrate a Raspberry Pi into our testbed for real-time anomaly detection. We also implement a software controlled physical event and fault generator to induce and measure faults. Figure 1 gives an overview of our system.

Test Bed: USMA's smart grid test bed emulates a large-scale power grid using a controllable load to alter the resistance and inductance of the grid, solar micro-inverters to simulate the power generated from solar panels, and a capacitor bank to correct the reactive power of the load. Our IEEE-compliant Phasor Measurement Units (PMUs) include GPS satellite clocks to ensure measurement data is time synchronized. The test bed includes a fault generator that enables users to create indicators of a grid failure. Data collected by the PMUs is sent to a server running OpenPDC which aggregates the data, time-aligns the measurements, and stores them in a MySQL database.

Web-Based User Interface: To make historical data human readable to grid operators, we develop user interface that combines a jQuery date picker module with Highcharts [1] (an interactive JavaScript charting library) to enable the grid operator to visualize data in a defined time interval. A date interval is specified using a calendar interface which is fed into a SQL request to the database to query the first 1, 000 readings within that time interval. The data is visualized on a derivative module of Highcharts, High Stocks [1] which enables a user to visualize the data as a whole and "zoom" into a selected interval for more detailed analysis of the data.

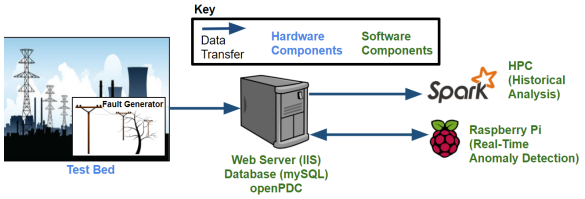

Figure 1: Overview of hardware and software components.

Anomaly Detection: To detect anomalies in historical grid data, we develop a novel MapReduce algorithm that leverages the cluster computing framework Apache Spark [5]. At a high level, the algorithm checks a sliding "window" of data for power fluctuations that meet the criteria of *constraint* and *temporal* anomalies (as described in [3]). Experimentation is performed on a 36-core compute node belonging to the DOD Supercomputer Topaz, and a dataset consisting of 1 million real measurements collected from our test bed. Our preliminary results show that our algorithm is capable of detecting constraint and temporal anomalies simultaneously.

ACKNOWLEDGMENTS

Funding this work is provided by the Office of Naval Research, the U.S. Army Armament Research, Development and Engineering Center (ARDEC) and the High Performance Computing Modernization Program (HPCMP). The opinions in this work are solely of the authors and do not necessarily reflect those of the U.S. Military Academy, the U.S. Army, or the Department of Defense.

REFERENCES

[1] Highcharts. 2017. Highcharts API. (2017). https://api.highcharts.com/highcharts/
[2] A. St. Leger, T. Banwell J. Spruce, and M. Collins. 2016. Smart grid testbed for wide-area monitoring and control systems. In *2016 IEEE/PES Transmission and Distribution Conference and Exposition (T D)*. 1–5.
[3] S. Matthews and A. St. Leger. 2017. Leveraging MapReduce and Synchrophasors for Real-Time Anomaly Detection in the Smart Grid. *IEEE Transactions on Emerging Topics in Computing* (2017).
[4] S. J. Matthews and A. St. Leger. 2017. Leveraging single board computers for anomaly detection in the smart grid. In *2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)*. 437–443. https://doi.org/10.1109/UEMCON.2017.8249031
[5] Matei Zaharia, Reynold S Xin, Patrick Wendell, Tathagata Das, Michael Armbrust, Ankur Dave, Xiangrui Meng, Josh Rosen, Shivaram Venkataraman, Michael J Franklin, et al. 2016. Apache spark: a unified engine for big data processing. *Commun. ACM* 59, 11 (2016), 56–65.

HoTSoS '18, April 10–11, 2018, Raleigh, NC, USA
ACM ISBN 978-1-4503-6455-3/18/04.
https://doi.org/10.1145/3190619.3191683