# Blue Waters Fall 2015 Exploratory Allocation: Final Report 2016
**Date: October 21, 2016**

**Title:** Evaluating Data-Driven Detectors of Electricity Theft in Smart Grids.

**PI:** William H. Sanders

Donald Biggar Willett Professor of Engineering and Department Head,
Department of Electrical and Computer Engineering
University of Illinois at Urbana-Champaign

**Co-PI:** Varun Badrinath Krishna

PhD Candidate/Research Assistant
Department of Electrical and Computer Engineering
University of Illinois at Urbana-Champaign

**Collaborator:** Juran Kirihara

Undergraduate Research Assistant
Department of Electrical and Computer Engineering
University of Illinois at Urbana-Champaign

## Executive Summary

Electricity theft is a billion-dollar problem faced by utilities around the world and current measures are ineffective against sophisticated theft attacks that compromise the integrity of smart meter communications. We are devising algorithms that detect such theft attacks, and that are based on mathematical techniques in statistics and machine learning. The goal is to detect and mitigate theft by identifying anomalies in consumption patterns of electricity consumers. We used Blue Waters to evaluate the effectiveness of the ARIMA based approach to detect simulated anomalies in smart meter data. The best parameters for these algorithms need to be found using scanning techniques, and they need to account for a wide range of attack parameters that produce anomalies. Our evaluation is based on a large dataset obtained from a real smart meter deployment.

## Key Challenge

Simulating electricity theft attacks is a challenge because the theft can be done in a variety of ways on a variety of consumers. Each attack method has a wide range of parameters. Each attack target (electricity consumer) has a wide range of consumption behaviors. In order to detect those attacks, we need to evaluate several detectors, each having a wide range of operation parameters. In all, we have a large simulation requirement that requires heavy computational resources.

## Why It Matters

Bloomberg News reported that electricity theft in India contributes to blackouts and costs $17 billion in lost revenue annually [3]. According to the World Bank, electricity theft contributes to a loss in electricity delivery of over 25% of generated supply in India, 16% in Brazil, 6% in China and the U.S., and

5% in Australia [3]. Theft in these countries is almost always achieved by tapping into electric distribution lines. To detect these thefts, utility companies such as BC Hydro have been convincing consumers to install smart meters. However, there has been some push-back as consumers have begun to realize that smart meters are vulnerable to cyber intrusions[10]. In 2010, the Cyber Intelligence Section of the FBI reported that smart meter consumptions were being under-reported in Puerto Rico, leading to annual losses for the utility estimated at $400 million [7]. In 2014, BBC News reported that smart meters in Spain were hacked to cut power bills [8]. Given that smart meters can be compromised, the smart meter roll-out efforts of utilities such as BC Hydro may only increase the attack surface for cyber intrusion-based theft methods.

In [6], we identified seven classes of electricity attacks, some of which distribute the monetary loss across consumers, at no loss to the utility. Therefore, this problem is not only important to utilities, but also consumers around the world.

**Methods & Results**

The methods in this project are detailed in our earlier work [2], where we simulated electricity theft attacks on 500 consumers and tested our detector's false positive and false negative rates on them. The detector fitted an Auto-Regressive Integrate Moving Average (ARIMA) model to the consumption data time series [5], and then flagged outliers using a confidence interval created from the model.

We used methods in [9] to fit the ARIMA time series, but learned from the larger simulation on Blue Waters that these methods do not scale well and are very sensitive to outliers. Also, we found that our results that used Python packages built by third parties were unexpected. Upon further investigation we identified errors in the algorithms coded in those Python packages (specifically the statsmodels.tsa.arima_model.ARIMA package). The algorithms simply do not implement ARIMA models correctly, and use the differencing order term in the ARIMA model in a manner that is inconsistent with the theory. In summary, our experience with Blue Waters helped us identify problems with third party software packages. We are re-developing those packages ourselves and hoping to complete them in time for the September 2016 call for proposals. With the correct algorithms, we hope to discover insights on our electricity theft detector from our use of Blue Waters then.

**Why Blue Waters**

Our earlier work published in [2] was performed at a much smaller scale (500 consumers) on a regular server rack, consuming inordinate amounts of processing time. We wanted to perform evaluation studies of our detector at a larger scale (2900 consumers). In addition, we wanted to try out many parameters for our detector at that scale. Without Blue Waters, it would have taken orders of magnitude longer (years) to complete the tasks.

**Next Generation Work**

Our experience with Blue Waters helped us identify problems with third party software packages. We are re-developing those packages ourselves and hoping to complete them in time for the September 2016 call for proposals. With the correct algorithms, we hope to discover insights on our electricity theft detector from our use of Blue Waters then.

**References**


[1] Varun Badrinath Krishna, Gabriel A. Weaver and William H. Sanders. PCA-Based Method for Detecting Integrity Attacks on Advanced Metering Infrastructure. In Proceedings of QEST 2015. Springer International Publishing.

[2] Varun Badrinath Krishna, Ravishankar K. Iyer and William H. Sanders. ARIMA-Based Modeling and Validation of Consumption Readings in Power Grids. In Proceedings of CRITIS 2015. Springer International Publishing.

[3] R. Katakey and R. K. Singh. (2014, June) India fights to keep the lights on. Bloomberg Businessweek. [Online]. Available: http://www.businessweek.com/printer/articles/205322-india-fights-to-keep-the-lights-on

[4] Cyber Intelligence Section. (2010, May) Smart grid electric meters altered to steal electricity. Federal Bureau of Investigation. [Online]. Available: http://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/

[5] Commission for Energy Regulation smart meter data accessed via Irish Social Science Data Archive at www.ucd.ie/issda

[6] Varun Badrinath Krishna, Kiryung Lee, Gabriel A. Weaver, Ravishankar K. Iyer and William H. Sanders. FDETA- A Framework for Detecting Electricity Theft Attacks in Smart Grids. To appear in Proceedings of IEEE/IFIP DSN 2016 (IEEE/IFIP conference on Dependable Systems and Networks).

[7] Cyber Intelligence Section. (2010, May) Smart grid electric meters altered to steal electricity. Federal Bureau of Investigation. [Online]. Available: http://krebsonsecurity.com/wp-content/uploads/2012/04/FBI-SmartMeterHack-285x305.png

[8] M. Ward. (2014, October) Smart meters can be hacked to cut power bills. [Online]. Available: http://www.bbc.com/news/technology-29643276

[9] Hyndman, R.J., Khandakar, Y.: Automatic Time Series Forecasting: The forecast Package for R. Journal of Statistical Software 27(3), 1–22 (7 2008)

[10] Coalition to Stop Mart Meters in BC. (2014, October) Theft of power through hacking of smart meters. [Online]. Available: http://www.stopsmartmetersbc.com/2014-10-23-theft-of-power-through-hacking-of-smart-meters/