Anomaly Detection for Securing Communications in Advanced Metering Infrastructure

Varun Badrinath Krishna, Abhideep Dasgupta and Prof. William H. Sanders, University of Illinois

GOAL — **To explore and develop techniques that can be used to detect anomalies (caused by attackers) in AMI communications that can lead to undesired behavior (often manifested as "failures" that cause loss of resiliency) in power grids.**

IDENTIFY ATTACKS ON ADVANCED METERING INFRASTRUCTURE (AMI)

1) Attacks on AMI Communications

- E.g., DDoS Attacks
- **Industry Partner: Cisco Inc.**

2) Attacks on Distributed Energy Resource (DER) Dispatch

- E.g., Data Spoofing Attacks
- **Industry Partner: IBM Research**

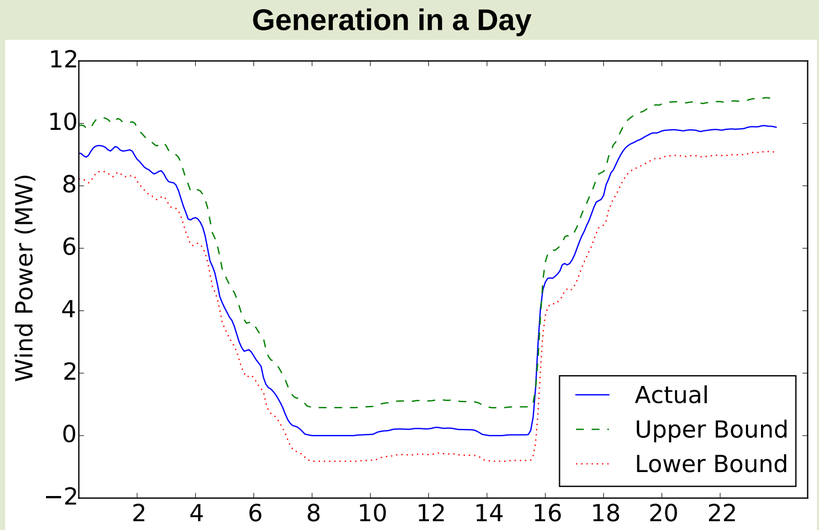
CREATE MODELS FOR NORMAL BEHAVIOR

Example: Improved models for DER generation output

Related US Patent applications filed with IBM Research:

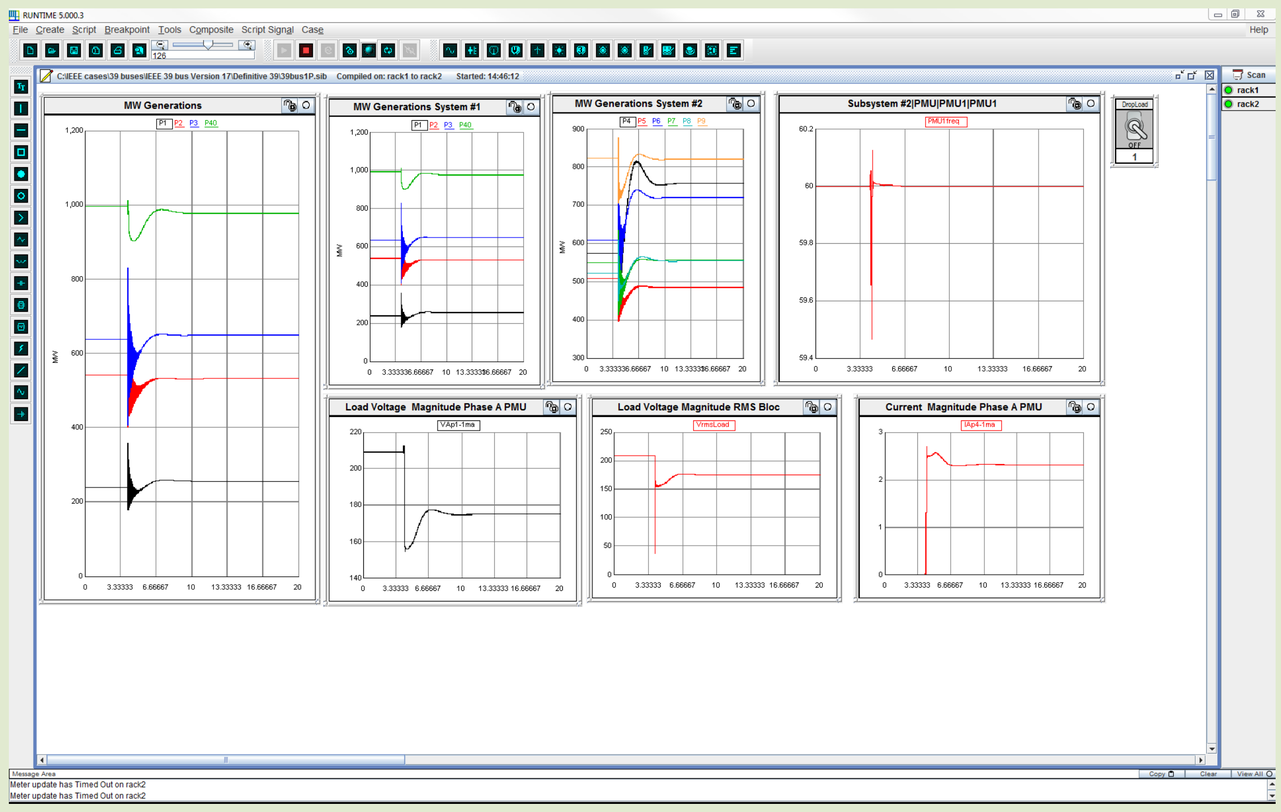
- *Reducing curtailment of wind power generation by improving wind power prediction accuracy.*
  - US Patent application 15/426,524 filed on 2nd Feb 2017.
- *Reducing curtailment of wind power generation by improving wind speed prediction accuracy.*
  - US Patent application 15/426,544 filed on 2nd Feb 2017.

Generation in a Day



MODEL ATTACKS AND REAL-TIME DEFENSES

Example: Create loss of resiliency scenarios with the Real-Time Digital Simulator (RTDS) and evaluate detection and response effectiveness.

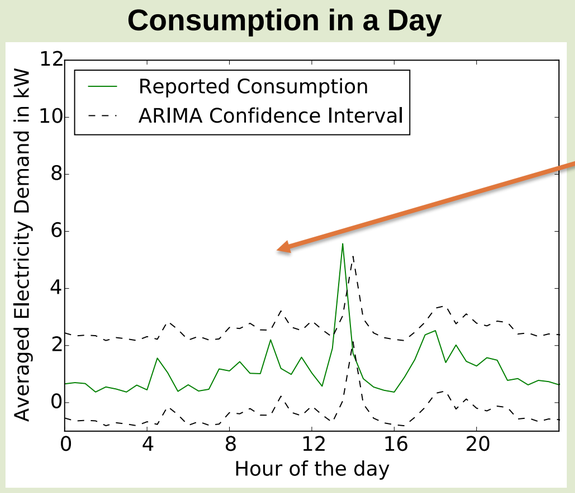


DEVELOP DATA-DRIVEN ANOMALY DETECTION METHODS

1) For anomalies in individual measurements

– Example detection method: Using confidence intervals generated from an Auto-Regressive Integrated Moving Average (ARIMA) model.

Consumption in a Day



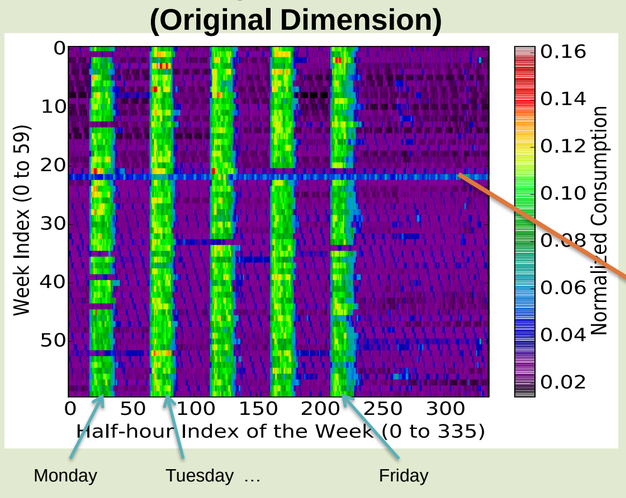
Anomalous measurement as per ARIMA model.
May be indicative of an attack.

More details available in publication: V. B. Krishna, R. K. Iyer and W. H. Sanders. *ARIMA-Based Modeling and Validation of Consumption Readings in Power Grids*. 10th International Conference on Critical Information Infrastructure Security (CRITIS) 2015. **Winner, 2015 Critical Infrastructure Preparedness and Resilience Network (CIPRNet) Young CRITIS Award.**

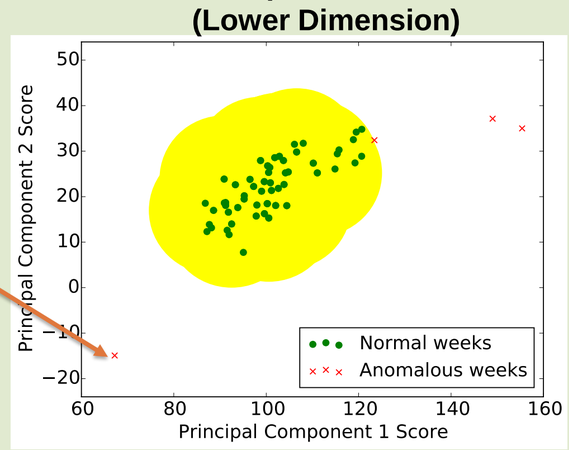
2) For sets of measurements (grouped temporally or spatially) that are collectively anomalous, but not individually anomalous

– Example detection method: Reducing the dimensionality of the set using Principal Component Analysis (PCA), and performing detection in lower dimensions using density-based clustering.

Consumption in 60 Weeks (Original Dimension)



Consumption in 60 Weeks (Lower Dimension)



More details available in publication: V. B. Krishna, G. A. Weaver and W. H. Sanders. *PCA-Based Method for Detecting Integrity Attacks on Advanced Metering Infrastructure*. 12th International Conference on Quantitative Evaluation of Systems (QEST) 2015. **Winner Best Paper Award**

The above plots are based on real data obtained from Ireland's Commission for Energy Regulation (CER) smart meter deployment. The providers of this data bear no responsibility for the further analysis or interpretation of it.

FURTHER INDUSTRY ENGAGEMENT OPPORTUNITIES

- Development and evaluation of new detection algorithms that improve on existing algorithms in terms of
  - Trade-off between detection rate and false-positive rate.
  - Processing time (computational complexity) to meet real time constraints.
- **Engagement with electric utilities to implement anomaly detection algorithms on real meter data**

Prosper Panumpabi and Matthew Backes from Illinois are also contributors to this project

Contact: varunbk@illinois.edu

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM | CRED-C.ORG

FUNDING SUPPORT PROVIDED BY THE U.S. DEPARTMENT OF ENERGY AND THE U.S. DEPARTMENT OF HOMELAND SECURITY