CREDC

Anomaly Detection for Securing Communications in Advanced Metering Infrastructure

Varun Badrinath Krishna, Juran Kirihara, and William H. Sanders

GOAL

To explore and develop mathematical techniques that can be used to detect anomalies (caused by attackers) in meter data that can lead to undesired behavior (often manifested as “failures” that cause loss of resiliency) in power grids.

RESEARCH PLAN

Identify power grid control decisions that are made based on meter data

- Schedule adequate power generation (in a distributed generation context) in response to demand that is predicted based on electricity usage reported by meters.
- Re-configure connections in the grid (breakers and reclosers) to support large increases and reductions in expected demand as measured by meters.
- Respond to faults by reconfiguring the grid to provide backup resources based on the existing utilization of those resources, as estimated from meter data.

Identify what forms of loss of resiliency can result from decisions based on bad data

- Loss of availability due to inadequate scheduled power generation, misconfigured connections in the grid, etc.
- Inability to recover from a fault, as a result of recovery actions based on compromised data that misrepresent available backup resources.

Understand the data used to make decisions, which could lead to loss of resiliency if the data were bad

- Features of the meter data reveal trends and correlations. These trends may vary across different sources of data (consumers).
- Machine-learning techniques can be used to classify and group different kinds of data sources and model behaviors.

Develop algorithms that can detect bad data that may indicate attacks on data integrity

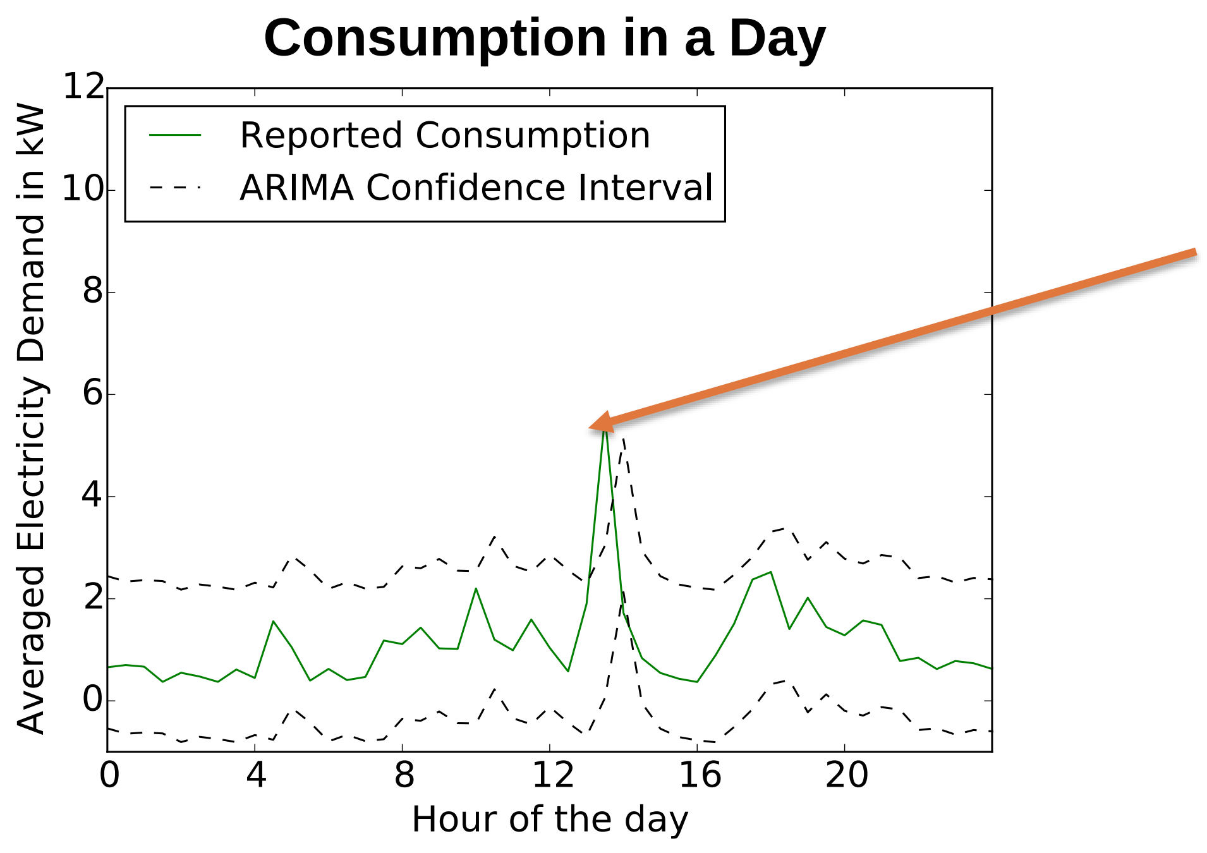
- Anomaly detection algorithms automatically process large datasets and identify anomalies based on models of normal data patterns.
- All control decisions are associated with real-time constraints that must be considered while the algorithms are being developed.
- Methods to reduce false positive rate must be integrated into the anomaly detection algorithms.

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.**

EXAMPLES OF ANOMALY DETECTION METHODS

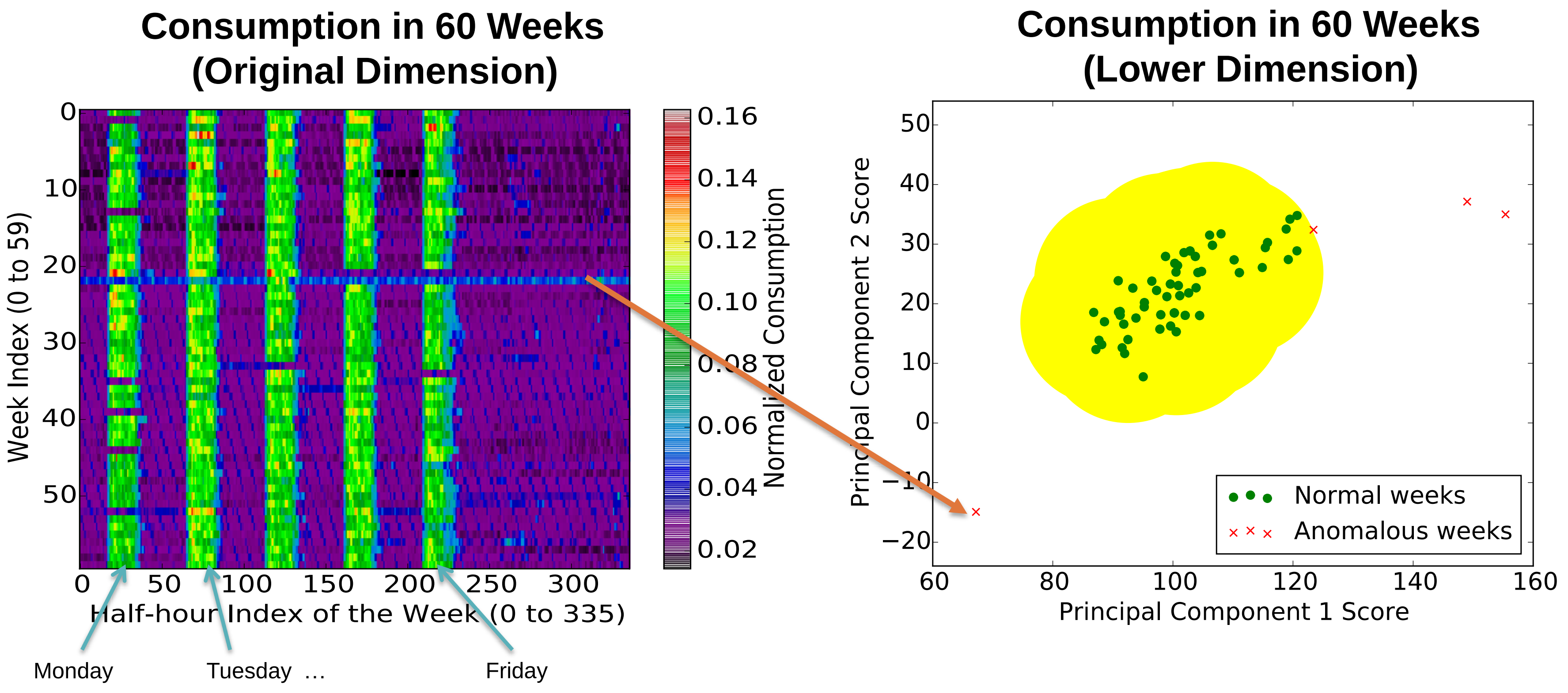
1. For anomalies in individual measurements:
   - Example detection method: Using confidence intervals generated from an Auto-Regressive Integrated Moving Average (ARIMA) model.



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.



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.

RELATED PROJECT (FORMERLY UNDER TCIPG)

- Title: “Design and evaluation of methods to detect electricity theft in Advanced Metering Infrastructure.”
- Funding source: **Siebel Energy Institute Award**, 2015.
- Relationship: Anomaly detection techniques that are similar to those used to detect theft can be used to detect attacks on resiliency.
- Accomplishments:
  - Blue Waters Exploratory Allocation Award, 2015.
  - Publication: V. B. Krishna, K. Lee, G. A. Weaver, R. K. Iyer, and W. H. Sanders. “F-DETA: A Framework for Detecting Electricity Theft Attacks in Smart Grids.” To appear in Proceedings of the 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2016).

Contact: varunbk@illinois.edu

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM | CRED-C.ORG

FUNDING SUPPORT PROVIDED BY THE DEPARTMENT OF ENERGY, OFFICE OF ELECTRICITY DELIVERY & ENERGY RELIABILITY