Integrated Smart Grid Analytics for Anomaly Detection

Maxwell Morgan (UMich), Davis Vorva (UMich), Michael G. Kallitsis (UMich, Merit)

Abstract

Now and in the future, many homes and smart homes are and will be connected to the central power grid with two way communications in order for power distributors to gain energy readings and other pertinent data. This approach is efficient for the power distributors because it enables real-time monitoring that can be used for more accurate pricing, capacity planning, and faster outage detection. However, this interconnectivity also poses a threat to the homes and smart homes. Anomalies may accrue within the home due to malfunctioning, compromised, or hacked appliances or energy meters. The purpose of our project is to design and optimize algorithms to detect anomalies that may occur in a smart home environment.

The methodology of our project consists of two phases: experimental and analytical. During the experimental phase, data is collected and stored using an integrated system of Z-Wave sensors and Raspberry Pi micro-controllers. Types, or features, of data collected include: temperature, humidity, luminescence, motion, power, water use, and energy consumption. During the analytical phase, the collected data is analyzed offline using a variety of algorithmic methods. We then compare the accuracy of the different methods in order to find the most efficient. The most efficient algorithms are then implemented in an online fashion where streaming data is analyzed in real-time.

We hypothesize that the more data features we collect will have a significant effect on the accuracy of the algorithms produced. Although we believe this correlation to be present, there is a trade-off between the quantity of features analyzed and the computational capacity of the microprocessor being used. As more features are added, more processing power is necessary in order to analyze the data using the designed algorithms.

Introduction and Threat Model

The electric grid is a "system of systems" that has experienced an expansion of technological capabilities in past years. The modernized grid's key characteristics include [2]:

- Two-way communication technologies in an integrated fashion across electricity generation, transmission, distribution and consumption;
- Incorporating variable renewable energy sources such as solar and wind;
- Handling the power capacity for charging electric vehicles;
- Accommodating distributed, small-scale generators and new technologies that ensure grid reliability and efficiency.

While this means that the grid is facing a number of important challenges, its new technologies present valuable opportunities for addressing them [3]. One of the modern technologies that enhances the system is the two-way data communication potential offered by advanced metering infrastructures (AMI). Comprised of a plethora of "smart" digital meters, the smart grid would allow development of *demand response* mechanisms, real-time monitoring of grid status, etc. [3]. It is, hence, of paramount importance to ensure AMI secure communications and be able to quickly detect nefarious activity.

Figure 1: Smart meter capable of being hacked.

It has been reported that these enhanced digital meters, shown in Figure 1, are capable of being hacked in order to spoof messages being sent to a utility company. After a successful penetration of the meter, the attacker would have the ability to under-report or even get someone else to pay their bill by changing the meter ID encapsulated in the message [4].

These types of attacks can even be harmful to users outside the smart meter network. An orchestrated attack targeting industrial control systems (ICSs) on a cluster of meters could be detrimental to the entire power grid. Malware of this variety is capable of affecting ICSs by altering code on programmable logic controllers (PLCs) that control the ICSs. An infamous program named Stuxnet.W32 did just that to control and disable Iranian centrifuges involved in refining uranium for nuclear weapons [1].

Purpose

There are both educational and security based objectives for this project.

1. The educational purpose of this project is to develop a cost-effective measuring infrastructure based on Z-Wave sensors and Raspberry Pis that would monitor for anomalies in a home area network. Graduate level curriculum development at EMU would incorporate the outcomes of our research in this area.
2. The security based purpose of this project is to design algorithms that quickly detect anomalies that may occur in a smart home or smart grid environment. These predictive algorithms can be used to notify users of possible anomalies or malicious activity.

Methodology

Our project consists of two phases: experimental and analytical. During the experimental phase, data is collected and stored using an integrated system of Z-Wave sensors and Raspberry Pi micro-controllers.

Each of the sensors will be connected to a Raspberry Pi microcrontroller hosting Z-Way server software. An additional Raspberry Pi can be used to request and store sensor data. A diagram of the network, including the sensors, is shown in Figure 2.

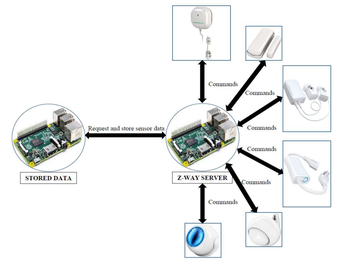

Figure 2: Sensor network diagram. (clockwise, starting at top) water sensor, door/window sensor, energy meter, energy switch, motion luminescence humidity and temperature sensor, motion luminescence and temperature sensor (middle and left) raspberry pi 2 model B

This integrated system of sensors and microcontrollers will be inserted into the NextEnergy testbed, a smart apartment, controlled environment. There it will collect real world data. Types, or features, of data collected include: temperature, humidity, luminescence, motion, power, water use, and energy consumption. In addition to collecting our own data from the Z-Wave sensor network, we also have access to other real-world datasets through project collaborators. These data sets include:

1. University of Michigan Power Plant data historian; access to database and smart metering tree topology. Recorded data features include frequency, real, reactive and total power, power factor, current and voltage.
2. Washington State University CASAS datasets.
3. University of Massachusetts datasets.

A plot of the data types used, taken in real-time, can be seen in Figure 3.

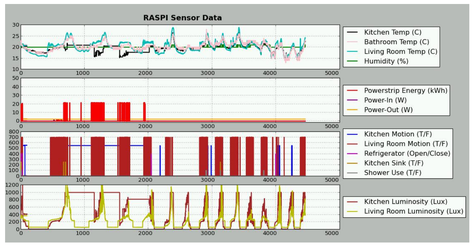

Figure 3: Real-time graph of sample data types.

During the analytical phase, the collected data is processed using regression analysis techniques to detect differences in predicted and actual power consumption. To optimize this process, a number of algorithms will be examined in order to identify the methods that minimize false-positives. The most efficient of these will be implemented in the proposed model, which will stream and analyze data in real-time.

Home-Area Network Event Detection

Our correlative monitoring approach aims at collecting various types of measurements from sensors deployed in a HAN network, and using appropriate supervised or unsupervised learning techniques to detect whether deviations from normal power usage patterns occur. As an example, consider the prediction technique depicted in Figure 4.

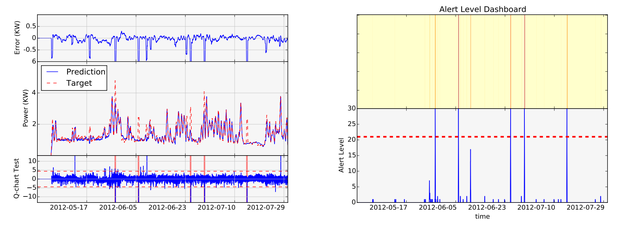

Figure 4: (L) Outputs from prediction, error and detection models. (R) Alert heat-map.

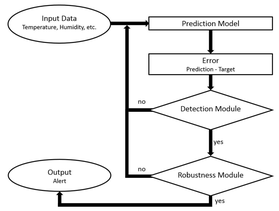

Figure 5: Flow chart outlining even detection process.

One could train the network using real-time measurements and use a regression model to predict the electricity usage given the sensor readings at any given instance. The predicted value is then put through an error analysis to determine the deviation from the actual smart meter power indication. During the detection module, a detection range based on the stringency of the test environment is implemented. This range is indicated by the dashed lines of the Q-chart Test in Figure 4. If the deviation of the prediction is outside that range, the process proceeds to the robustness module, otherwise it is not considered an anomaly. During the robustness module, an alert level is recorded as alerts per half hour. If the alert level is greater than 70%, a marker is placed on the alert level dashboard shown in Figure 4. This process is depicted in the flow chart in Figure 5.

References

[1] Nicolas Falliere, Liam O Murchu, and Eric Chien. W32.stuxnet dossier, February 2011. [Symantec Corporation].

[2] Hamid Gharavi and Reza Ghafurian. Smart Grid: The Electric Energy System of the Future. *Proceedings of the IEEE*, June 2011.

[3] Massachusetts Institute of Technology. *The Future of the Electric Grid: An Interdisciplinary MIT study*. MIT Energy Initiative, 2001.

[4] Mark Ward. Smart meters can be hacked to cut power bills, October 2014. [Online; www.bbc.com; posted 16-October-2014].