An Eye on the Storm: Tracking Power Outages via the Internet of Things

Kendra Kratkiewicz
MIT Lincoln Laboratory
kendra@ll.mit.edu

ABSTRACT

Assessing the extent of power outages in the wake of disasters is a crucial but daunting challenge. We developed a prototype to estimate and map the severity and location of power outages throughout an event by taking advantage of IoT as a non-traditional power-sensing network. We present results used by FEMA and other responders during multiple major hurricanes, such as Harvey, Irma, and Maria.

AUDIENCE

Level: Beginner
Areas of interest: humanitarian assistance and disaster relief (HADR), electric power grid, Internet of Things (IoT), Internet measurement, cyber security

INTRODUCTION

Emergency response coordinators face daunting challenges in the wake of large-scale disasters, one of which is the vital task of assessing the extent of power outages. Where deployed, Smart Grid technology such as Advanced Metering Infrastructure (AMI) enables utilities to rapidly and automatically assess their customer outages. However, according to recent data from the US Energy Information Administration, only about half of the meters currently deployed in the U.S. possess these capabilities, and they are not evenly distributed; some states have close to full coverage while others have next to none, leaving many utilities with the less efficient method of relying on customers to phone in outages. This can result in significant delays and poor accuracy when determining if power outages exist and which areas are impacted.

Furthermore, In order to understand the impact of widespread power outages on the regional or state level, outage information must be collected and amalgamated from multiple electric utilities. The large number of disparate utilities and the lack of outage data reporting standards make it time consuming and difficult to produce a single product that can provide broad situational awareness.

Researchers from two different groups within MIT Lincoln Laboratory (Cyber Analytics & Decision Systems and Humanitarian Assistance and Disaster Relief Systems) collaborated to develop an alternative method of rapidly estimating the extent and location of power outages, independent of utilities and across geographic boundaries, by taking advantage of signals observed in Internet communications data [1]. The work employs targeted cyber sensing (via active scanning) of local areas, correlated with geographic data, to identify changes in network device availability as an independent indicator of power loss. The method compares IP network scan response rates in an affected area during an event to pre-event norms (a baseline) in order to calculate a "percentage of normal activity" for each town or county in the area. These percentages can be translated to corresponding estimates of customers with or without power. At each observation interval throughout an event, the calculated percentages are displayed on a map using a color scale corresponding to ten percent ranges. The

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited. This material is based upon work supported by the United States Air Force under Air Force Contract No. FA8702-15-D-0001. Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Air Force.

changing map over time reveals where power outages come and go as well as their severity.

IP network geo-location data is obtained from a MaxMind GeoIP2 database [2], which covers over 99% of all allocated IP addresses. The database provides many fields of information associated with each entry, including the geographic location of the IP network and the accuracy radius. Within the U.S., over 90% of IP networks are located to within a 100 km radius.

IP networks are scanned using the highly efficient ZMap Scanner [3], created by the same University of Michigan security researchers who founded Censys [4]. Originally a university-based research effort (now turned commercial company), the Censys project regularly scanned the entire IPv4 address space on multiple ports with the goal of providing data to security researchers. We used their historical scan data to calculate our baseline, pre-event response rates.

OUTCOMES/CONCLUSION

One of the earliest test cases for this approach was Hurricane Matthew in October 2016 as it affected coastal Florida, Georgia, and the Carolinas. Scan response rates were measured over three-hour intervals for more than a week. Figure 1 comprises four snapshots over time from the resulting visualization, which clearly illustrates how Internet device response rates declined along the path of the hurricane. The researchers were able to closely correlate these drops in “percentage of normal activity” with power outages, and increases in activity with power restoration as reported by energy authorities and in Department of Energy situation reports, providing essential data for validating this new technique.

The US Energy Information Administration (EIA) provides hourly electricity operating data for sixty-six balancing authorities that compose the U.S. electric grid [5]. These balancing authorities are responsible for monitoring the grid and ensuring that power supply and demand do not fall out of balance. Accordingly, they track forecasted and actual electricity demand. In the case of a power outage, one would expect actual demand to drop as compared to forecasted demand. Figure 2 presents graphical depictions of the significant correlation between our method and EIA balancing authority data during Hurricane Matthew. The EIA data represents the percent difference between actual and forecasted electricity demand, which is different from but analogous to our calculated percent difference between actual and expected scan response rates.

During emergency situations, such as large-scale hurricanes, the Department of Energy (DOE) typically produces emergency situational awareness reports (situation reports) once a day, which include estimated percentages of customers without power in affected regions [6]. Figure 3 compares our method to DOE situation report data during Hurricane Matthew. In this case we are both trying to estimate the same type of information (percentage of customers without power), and again we demonstrate that the change in Internet device response rates, aggregated across a geographic region, can be used as a reasonable indicator of power status within that region.

During the 2017 hurricane season, this experimental capability provided valuable, supplemental information to FEMA and other responders, such as Air National Guard units, as they assessed which areas were hardest hit by and planned responses to Hurricanes Harvey, Irma, and Maria in Texas, Florida, and the Caribbean. In addition, this capability provided ongoing insight into the prolonged restoration efforts in Puerto Rico.

While to date the team has applied the technique only to the aftermath of expected weather-related disasters, we hope eventually to expand the capability to nationwide monitoring for power outages resulting from any cause, including unexpected cyberattack.

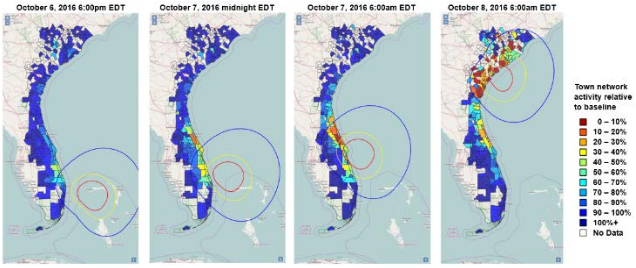
October 6, 2016 6:00pm EDT
October 7, 2016 midnight EDT
October 7, 2016 6:00am EDT
October 8, 2016 6:00am EDT
Town network activity relative to baseline
0 – 10%
10 – 20%
20 – 30%
30 – 40%
40 – 50%
50 – 60%
60 – 70%
70 – 80%
80 – 90%
90 – 100%
100%+
No Data

Figure 1 The "percentage of normal activity" forecasts the location and extent of power outages. Here we see percentages declining along the path of Hurricane Matthew in the southeast coastal US, which correlates closely with reported power outages.

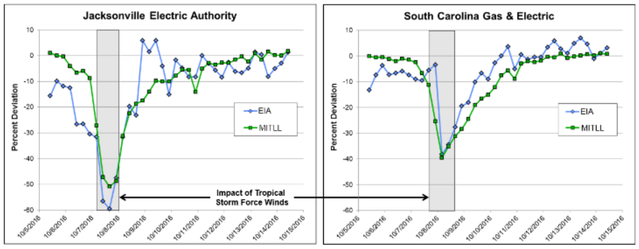

Figure 2 Here the MITLL-calculated percent change in normal activity is compared to US Energy Information Administration (EIA) balancing authority data in the areas covered by Jacksonville Electric Authority and South Carolina Gas & Electric. The EIA data points represent the percent difference between actual and forecasted electricity demand.

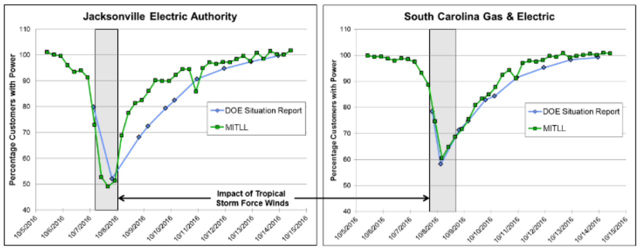

Figure 3 Here we compare the MITLL-calculated "percentage of normal activity" to the percentage of customers with power in the regions served by Jacksonville Electric Authority and South Carolina Gas & Electric as determined from Department of Energy (DOE) situation reports, issued daily during Hurricane Matthew.

PARTICIPATION STATEMENT

I commit to attending the conference if accepted.

REFERENCES/BIBLIOGRAPGHY

[1] K. Kratkiewicz, A. Norige, C. Rose and E. Dantowitz, "Patent Application: System and Method for Cyber Sensing for Power Outage Detection". U.S. Patent 20180241646, 2018.

[2] Maxmind, Inc., "GeoIP2 Databases," 2019. [Online]. Available: https://www.maxmind.com/en/geoip2-databases. [Accessed 5 March 2019].

[3] Z. Durumeric, E. Wustrow and J. A. Halderman, "ZMap: Fast Internet-Wide Scanning and its Security Applications," in *Proceedings of the 22nd USENIX Security Symposium*, 2013.

[4] Censys, "About Censys," 2019. [Online]. Available: https://censys.io/about. [Accessed 5 March 2019].

[5] EIA Staff, "Hourly information on U.S. electricity supply, demand, and flows is now available," 25 July 2016. [Online]. Available: https://www.eia.gov/todayinenergy/detail.php?id=27212. [Accessed 5 March 2019].

[6] U.S. Department of Energy, "Emergency Situation Reports," [Online]. Available: https://www.energy.gov/ceser/activities/energy-security/monitoring-reporting-analysis/emergency-situation-reports. [Accessed 5 March 2019].

BIO

Kendra Kratkiewicz holds bachelor's and master's degrees in computer science from MIT and Harvard, and currently works within the Cyber Security & Information Sciences division of MIT Lincoln Laboratory. There she has contributed to a wide variety of cybersecurity programs, and particularly enjoys using her software engineering skills to help transition research into practical applications. She holds one patent (NetSPA: Network Security Planning Architecture), and has applied for another related to the proposed talk (System and Method for Cyber Sensing for Power Outage Detection). She has authored or co-authored numerous publications (which can be found online via Google Scholar), including a Lincoln Laboratory Technical Report surveying data fusion techniques in IoT. Kendra has presented on the proposed topic to significant audiences at Lincoln Laboratory's Homeland Protection Workshop and as part of a homeland protection educational program for the National Guard.