Third-Party Measurement of Network Outages in Hurricane Sandy*

John Heidemann, USC/Information Sciences Institute, johnh@isi.edu

We are interested in understanding Internet outages. In our work, we have been developing the use of active probing of destination networks to detect network outages [7]. We probe networks with ICMP echo request messages ("pings"), and interpret networks that cease responding as down. We know that active probing provides an incomplete view of the network, since it can only see networks that agree to respond (those that are not firewalled), however, we have previously shown that this approach provides a reasonable picture of more than half of the active Internet [2]. We therefore believe that our approach can effectively evaluate network outages.

The key unique characteristics of our work is that it provides a third-party view of edge-network resiliency taken on-demand. Considering each of these aspects: We believe a *third-party* viewpoint is important. Individual network operators and ISPs have the capability to track the resiliency of their own networks. But a third party viewpoint is clearly independent of any business motivations of individual ISPs, and a third party can provide consistent, unbiased observations over many different ISPs.

Use of *on-demand* probes of *edge-networks* is important to evaluate outages as seen by end-users, not just ISPs, and to detect problems that are independent of the routing system. Prior work has used passive observations [1] or focused on identifying routing problems [4, 5]. We see active probing of edge networks as essential to provide timely, precise observations of what users experience.

We have recently described network outages that occurred during Hurricane Sandy [3] at the end of October, 2012. There are always occasional network outages in a network the size of the Internet. However, we show that the U.S. network outage rate approximately doubled when the hurricane made landfall, and that it took about four days to recover to prior levels.

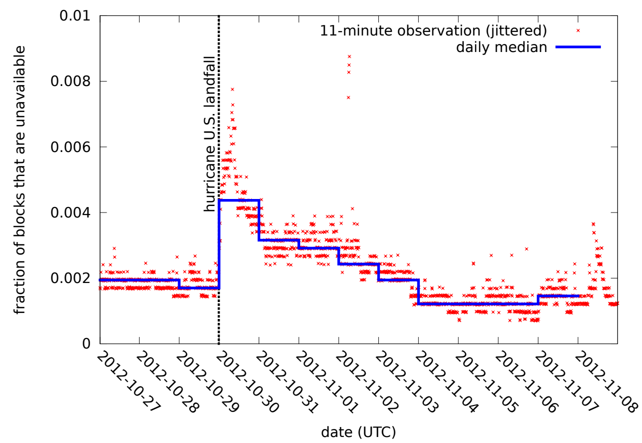

Figure 1: Median daily outages (solid line) for /24 blocks geolocated to the United States, with jittered individual readings (dots). (Dataset: [8]).

Figure 1 shows U.S. networks had an outage rate of about 0.2% before landfall. (This rate seems somewhat better than the global average.) This rate jumps to 0.43%, more than double the prior U.S. baseline, for the 24-hours following landfall. The outage level drops slowly over the next four days, first to around 0.3% and finally returning to the baseline on 2012-11-03.

We did additional analysis to identify the location of these outages. Figure 2 focuses on the northeastern seaboard, showing outages by network location (as determined by MaxMind GeoLite City [6]). Circles in this figure are weighted by outage size and duration (as in Figure 2). While we see some outages elsewhere in the U.S., this figure shows the localized and long-lasting outages in the New York/New Jersey area at and immediately following landfall.

We are continuing to develop our outage detection methods, and we believe a third-party system can monitor outages over the global IPv4 address space with minimal traffic overhead.

Raw and processed datasets from this abstract are available at no cost to researchers through the U.S. DHS PREDICT program and by request from the authors. This work was reviewed by USC's IRB (IIR00000975) and identified as non-human subjects research.

*This material is based on research sponsored by the Department of Homeland Security (DHS) Science and Technology Directorate, Homeland Security Advanced Research Projects Agency, Cyber Security Division BAA 11-01-RIKA and Air Force Research Laboratory, Information Directorate under agreement number FA8750-12-2-0344, and under DHS contract number D08PC75599. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the Department of Homeland Security or the U.S. Government.

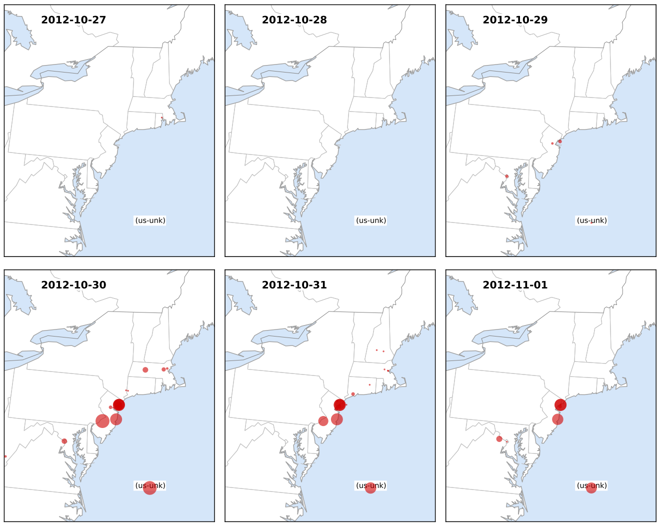

Figure 2: Geographic location of observed outages in the Northeastern U.S., by day. Top row: 3 days before landfall, second: 3 days after landfall. Circle area represents the block-rounds of outage at each location. (The point in the mid-Atlantic represents U.S. networks with unknown cities.; dataset: [8]).

Biography

John Heidemann received his B.S. from University of Nebraska-Lincoln (1989) and his M.S. and Ph.D. from the University of California, Los Angeles (1991 and 1995). He is a senior project leader at the University of Southern California/Information Sciences Institute (USC/ISI) and a research professor at USC in Computer Science. At ISI he leads the ANT (Analysis of Network Traffic) Lab (`http://www.isi.edu/ant/`), studying how large Internet topology and traffic data inform network reliability, security, and architecture. He is a senior member of ACM and IEEE.

References

[1] Alberto Dainotti, Claudio Squarcella, Emile Aben, Marco Chiesa, Kimberly C. Claffy, Michele Russo, and Antonio Pescapé. Analysis of country-wide Internet outages caused by censorship. In *Proceedings of the ACM Internet Measurement Conference*, pages 1–18, Berlin, Germany, November 2011. ACM.

[2] John Heidemann, Yuri Pradkin, Ramesh Govindan, Christos Papadopoulos, Genevieve Bartlett, and Joseph Bannister. Census and survey of the visible Internet. In *Proceedings of the ACM Internet Measurement Conference*, pages 169–182, Vouliagmeni, Greece, October 2008. ACM.

[3] John Heidemann, Lin Quan, and Yuri Pradkin. A preliminary analysis of network outages during hurricane sandy. Technical Report ISI-TR-2008-685, USC/Information Sciences Institute, November 2012.

[4] Ethan Katz-Bassett, Colin Scott, David R. Choffnes, Ítalo Cunha, Vytautas Valancius, Nick Feamster, Harsha V. Madhyastha, Tom Anderson, and Arvind Krishnamurthy. LIFEGUARD: Practical repair of persistent route failures. In *Proceedings of the ACM SIGCOMM Conference*, pages 395–406, Helsinki, Finland, August 2012. ACM.

[5] Doug Madory. Hurricane Sandy: Initial impact. Renesys blog `http://www.renesys.com/blog/2012/10/hurricane-sandy-initial-impact.shtm%l`, October 2012.

[6] Maxmind. Geolite city. Web page `http://dev.maxmind.com/geoip/geolite`, 2012.

[7] Lin Quan, John Heidemann, and Yuri Pradkin. Detecting internet outages with precise active probing (extended). Technical Report ISI-TR-2012-678b, USC/Information Sciences Institute, February 2012. (updated May 2012; this TR superceeds ISI-TR-2011-672.).

[8] USC/LANDER project. Internet address survey dataset, predict id `usc-lander/internet_address_survey_reprobing_it50j`. web page `http://www.isi.edu/ant/lander`, November 2012.