

Lessons learned by “measuring” the Internet during/after the Sandy storm

E. Aben - RIPE NCC, A. King, K. Benson, Y. Hyun, A. Dainotti, K.C. Claffy - CAIDA, UC San Diego

After causing extensive damage in the Caribbean, superstorm Sandy had devastating effects on the US East Coast, including heavily affecting Internet infrastructure in the region. Researchers at CAIDA have been developing techniques for the detection and analysis of large-scale Internet outages, through correlation of a variety of network measurements, including control-plane signaling, passive traffic collection, and distributed active probing [1,2]. Experiments with correlating different sources of data have inspired our current pursuit of new methodologies [3], with the ultimate goal to develop an operational capability to detect and monitor Internet outages in real-time [4]. [This work is partly funded by the NSF SaTC program CNS-1228994.]

However, Sandy was a significantly different type of disruption than those we have studied thus far, with characteristics that limited and in some cases prevented us from being able to thoroughly analyze the event. These characteristics include:

- Movement over a large area, with no fixed epicenter like an earthquake has.
- High level of Internet penetration in the affected region, including major hubs for international Internet connectivity.
- Disruption was limited to only a subset of networks/hubs in the affected region, making it harder to identify geographic areas of massive impact.

Nonetheless, we were able to observe some of the impacts of Sandy through Internet measurements, and we also learned some lessons that will allow us to improve our methodologies for studying similar events in the future. We would report on both these aspects at the workshop.

The measurements we would discuss include: analysis of changes in Internet routing to Europe and Asia inferred from traceroutes conducted using the RIPE Atlas network [5, 6]; analysis of traffic reaching the UCSD Network Telescope that originated from the areas affected; and traceroute (forward path) measurements through CAIDA's Archipelago infrastructure.

[1] A. Dainotti, C. Squarcella, E. Aben, K. C. Claffy, M. Chiesa, M. Russo, A. Pescapé, “Analysis of Country-wide Internet Outages Caused by Censorship”, ACM SIGCOMM Internet Measurement Conference IMC 2011 - November 2011

[2] A. Dainotti, R. Amman, E. Aben, K. C. Claffy, “Extracting Benefit from Harm: Using Malware Pollution to Analyze the Impact of Political and Geophysical Events on the Internet”, ACM SIGCOMM Computer Communication Review, January 2012

[3] K. Benson, A. Dainotti, K. C. Claffy, E. Aben, “Gaining insight into AS-level outages through analysis of internet background radiation”, Proceedings of the 2012 ACM conference on CoNEXT student workshop, 63-64

[4] <http://www.caida.org/funding/dals-satc/>

[5] E. Aben, “RIPE Atlas - Superstorm Sandy”, <https://labs.ripe.net/Members/emileaben/ripe-atlas-superstorm-sandy>

[6] E. Aben, “RIPE Atlas: Hurricane Sandy and How the Internet Routes Around Damage”, <https://labs.ripe.net/Members/emileaben/ripe-atlas-hurricane-sandy-global-effects>