


Active Probing of Edge Networks: Outages During Hurricane Sandy

John Heidemann
joint work with Lin Quan and Yuri Pradkin

5 February 2013
NANOG, Orlando, Florida

Copyright © 2013 by John Heidemann
Release terms: CC-BY-NC 3.0 unported

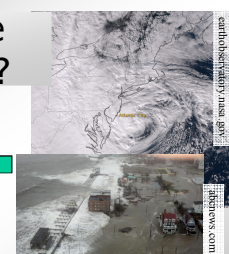
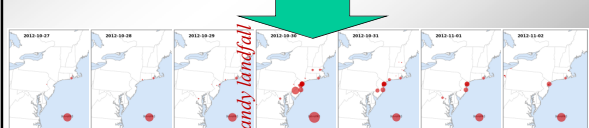


USC Viterbi School of Engineering ANT Outage Detection / 5 February 2013 1

Can Pings Measure Hurricane Damage?

PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_req=1 ttl=251 time=89.6 ms
64 bytes from 8.8.8.8: icmp_req=2 ttl=251 time=83.6 ms
64 bytes from 8.8.8.8: icmp_req=3 ttl=251 time=86.6 ms
^C

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 83.602/86.627/89.641/2.465 ms

USC Viterbi School of Engineering ANT Outage Detection / 5 February 2013 2

Goal: Tracking Outages in Edge Networks

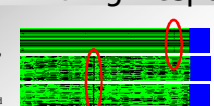
- quickly know the impact of **natural disasters**
 - Hurricane Sandy, Tōhoku Earthquake 2011, etc.
 - and human ones :- (like Egypt 2011, etc.
- evaluate **wide and long outages**
 - many people vs. long duration (vs. both)
- in edge networks**: /24s
 - not just routable prefixes
 - most outages are small, *inside* ISPs, *not* from routing
 - e.g.: [Bush et al, IMC 2007]; us: ~70% smaller than rtg pfx

USC Viterbi School of Engineering ANT Outage Detection / 5 February 2013 3

Approach: Detect Changes in Ping Response

1. probe multiple addresses in each block frequently

green: positive response
black: no response
blue: not probed; each band is a /24 block



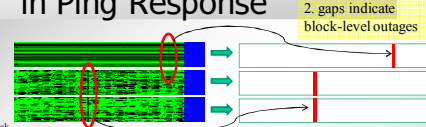
USC Viterbi School of Engineering ANT Outage Detection / 5 February 2013 4

Approach: Detect Changes in Ping Response

1. probe multiple addresses in each block frequently

green: positive response
black: no response
blue: not probed; each band is a /24 block

2. gaps indicate block-level outages



USC Viterbi School of Engineering ANT Outage Detection / 5 February 2013 5

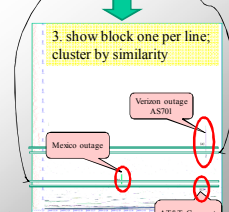
Approach: Detect Changes in Ping Response

1. probe multiple addresses in each block frequently

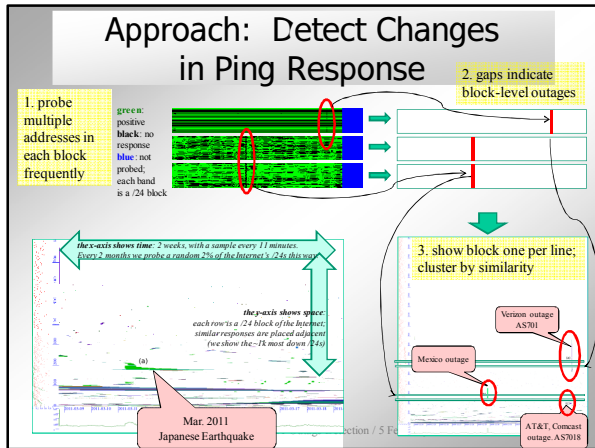
green: positive response
black: no response
blue: not probed; each band is a /24 block

2. gaps indicate block-level outages

3. show block one per line; cluster by similarity



USC Viterbi School of Engineering ANT Outage Detection / 5 February 2013 6



Details: Sandy Analysis

- Sandy-specific methodology
 - re-analyzed existing data
 - moderate traffic: 1400 probes/hour to each /24 block (= 1 probe every 3 s)
 - details in ISI-TR-678b: <http://www.isi.edu/~johnh/PAPERS/Quan12a.html>
 - data available: <http://www.isi.edu/ant/traces/>
- work in progress:
 - custom, outage-specific probing
 - expect <15 probes/hour per /24 (~1% above)

USC Viterbi School of Engineering

ANT Outage Detection / 5 February 2013

9

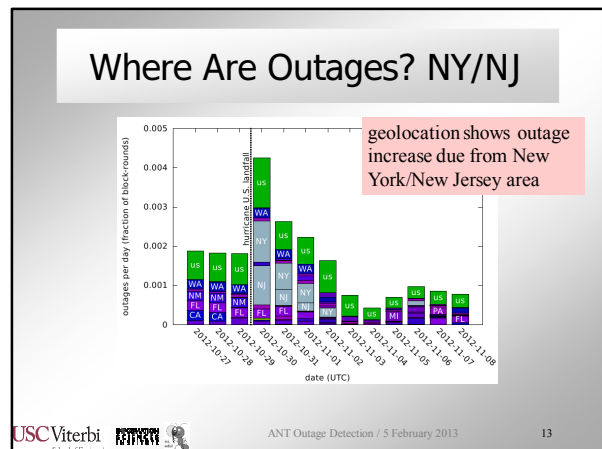
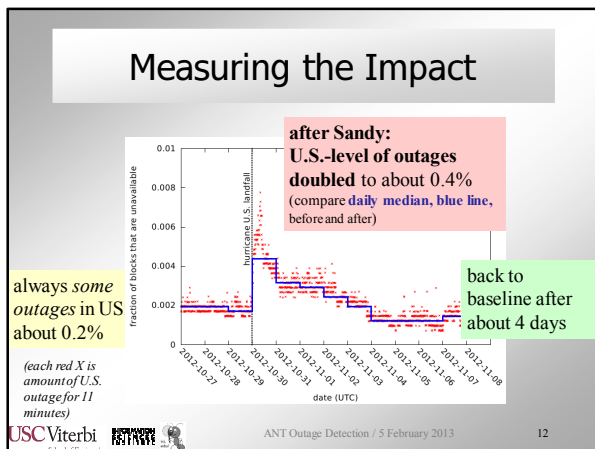
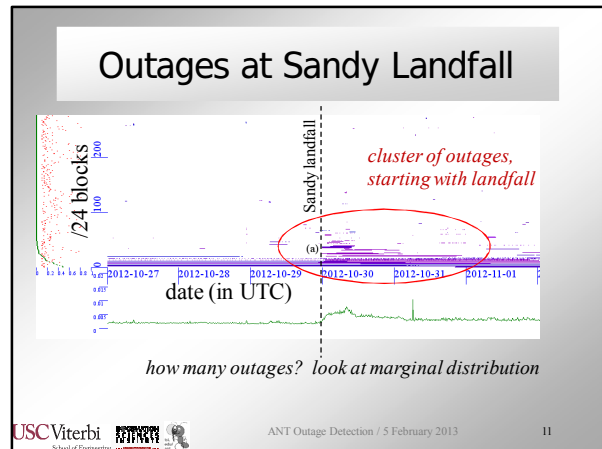
Data About Sandy

- look at one dataset: internet_address_reprobing_it50j-20121027
- 41,582 /24 blocks
- 11,900 geolocate to US
- 4,117 have enough response to analyze
 - 60 of these don't have states

USC Viterbi School of Engineering

ANT Outage Detection / 5 February 2013

10

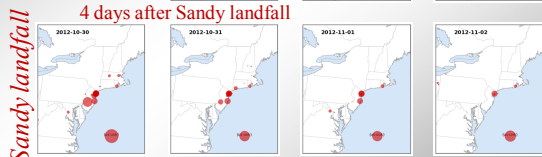


The Northeast, by Day

3 days before Sandy landfall



4 days after Sandy landfall



Sandy landfall

What Next?

- pings *can* detect edge-network outages
- we're working to deploy detection
 - lower probe rate: <15 probes/hour per /24
 - grow coverage: 3.4M blocks
- tech report about Sandy:
<http://www.isi.edu/~johnh/PAPERS/Heidemann12d.html>
- datasets: <http://www.isi.edu/ant/traces>