Active Probing of Edge Networks: Hurricane Sandy and Beyond

John Heidemann
joint work with Lin Quan and Yuri Pradkin
6 February 2013
FCC Workshop on Network Resiliency, NYC, NY
work supported by DHS S&T, Cyber Security Division

Broader Goal: Tracking Outages in Edge Networks

• quickly know the impact of natural disasters
  - Hurricane Sandy, Tohoku Earthquake 2011, etc.
  - and human ones; e.g. like Egypt 2011, etc.

• learn about outage shapes
  - wide outages: many people
  - long outages: long time
  - and both

• in edge networks (24 address blocks, like 1.2.3.*)
  - most outages are small, inside ISPs, not from routing
  - e.g. [Bhush et al, DMC 2007]; ~70% smaller than notable prefixes
  - want to characterize what people see at home

Background: Active Probing with Pings

Pings (ICMP echo request)
draw positive replies when an IP address is in use
PING 8.8.8.8 (8.8.8.8) 56(0) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=251 time=89.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=251 time=89.6 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=251 time=89.6 ms

or get negative (non-)replies
no reply from 8.8.8.8: icmp_seq=4
no reply from 8.8.8.8: icmp_seq=5
no reply from 8.8.8.8: icmp_seq=6

--- 8.8.8.8 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 600ms
rtt min/avg/max/mdev = 83.602/86.627/89.641/2.465 ms

Can Pings Measure Hurricane Damage?

PING 8.8.8.8 (8.8.8.8) 56(0) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=251 time=89.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=251 time=89.6 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=251 time=89.6 ms

--- 8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 200ms
rtt min/avg/max/mdev = 83.602/86.627/89.641/2.465 ms

Background: Active Probing with Pings

Pings Tell You Something But Not Everything

positive: block is up
negative: block is down
or computer crashed
laptop suspended
computer address reassigned
probe or reply lost
firewall enabled
negative replies are ambiguous
So We Probe Multiple Addresses

all negative together disambiguates: network is really down

Approach: Detect Changes in Ping Response

1. probe multiple addresses in each block frequently

2. gaps indicate block-level outages

3. show block per line; cluster by similarity

Outages due to Hurricane Sandy

time

Approach: Detect Changes in Ping Response

1. probe multiple addresses in each block frequently

2. gaps indicate block-level outages

3. show block per line; cluster by similarity

Outages due to Hurricane Sandy

time
Details: Sandy Analysis

- for Sandy, we re-analyze existing data
- Internet Surveys
  - sample: 41k blocks (~2% of active address space)
  - probe for 2 weeks
  - every 11 minutes
  - we have been taking surveys since 2006
- details and data are available
  - ISI-TR-678:
    http://www.isi.edu/~johnh/PAPERS/Quan12a.html
  - data: http://www.isi.edu/ant/traces/

Data About Sandy

- look at one dataset:
  internet_address_reprobing_500-20121027
- 41,582 /24 blocks
- 11,900 geolocate to US
- 4,117 have enough response to analyze
  - 60 of these don’t have states

Outages at Sandy Landfall

- cluster of outages, starting with landfall
- date (in UTC)
- marginal distribution to quantify amount

Measuring the Impact

- after Sandy: U.S.-level of outages doubled to about 0.4%
  (compare daily median, blue line, before and after)

Where Are Outages? NY/NJ

- geolocation shows outage increase due from New York/New Jersey

The Northeast, by Day

- 3 days before Sandy landfall
- 4 days after Sandy landfall
Outages: Prominent and Unknown

Jan. 2011 Egyptian Revolution
Jan. 2011 Australian Outage
Mar. 2011 Japanese Earthquake
Verizon (AS1929)
Mexico (AS151)
AT&T and Comcast

our goal: small and big

Outages Everywhere?

• what would it take to track all IPv4?
  – about 3.4M blocks are analyzable
• current surveys: too much traffic
  – 1 probe / 3 seconds (1400 probes/hour) per block
• work in progress: intelligent probing
  – detecting outages at < 20 probes/hour per block
  – a single machine can watch the whole Internet

What Next?

• pings can detect edge-network outages
• Internet-wide detection: work-in-progress

• tech report about Sandy:
  http://www.isi.edu/~johnh/PAPERS/Heidemann12d.html
• datasets: http://www.isi.edu/ant/traces

• feedback or interest? let me know