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

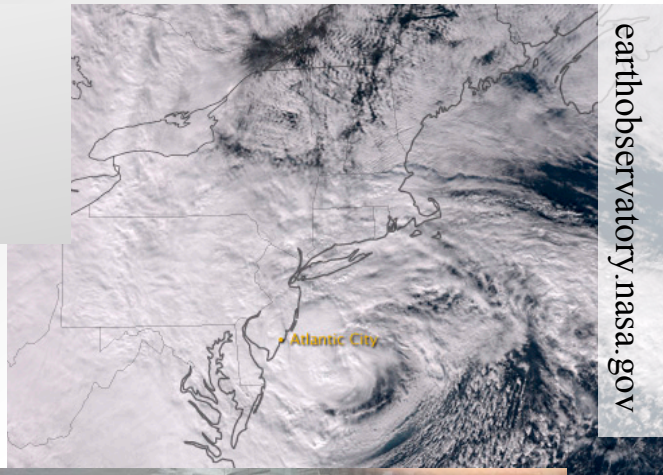
work supported by DHS S&T, Cyber Security Division

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

This research is sponsored by the Department of Homeland Security (DHS) Science and Technology Directorate, HSARPA, Cyber Security Division, BAA 11-01-RIKA and Air Force Research Laboratory, Information Directorate under agreement number FA8750-12-2-0344, and contract number D08PC75599. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. The views contained herein are those of the authors and do not necessarily represent those of DHS or the U.S. Government.

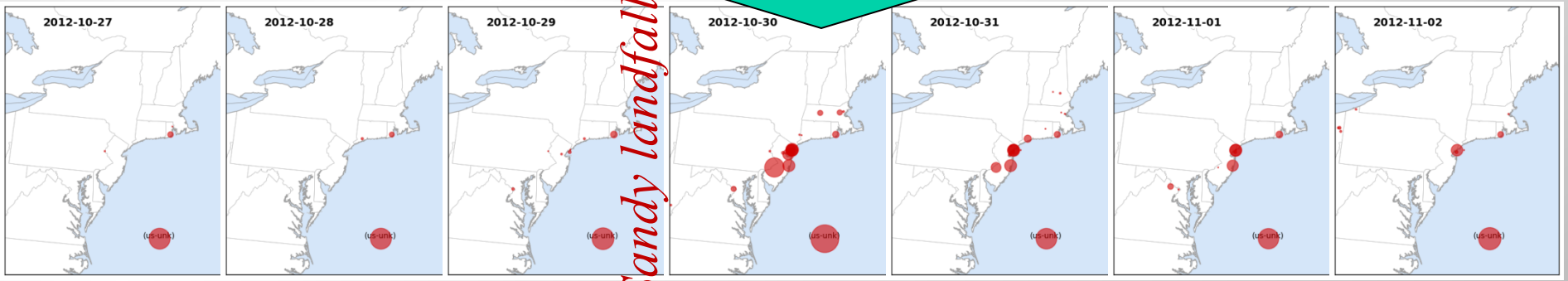
Can Pings Measure Hurricane Damage?

```
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
^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
```



earthobservatory.nasa.gov

abcnews.com



Broader 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.

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

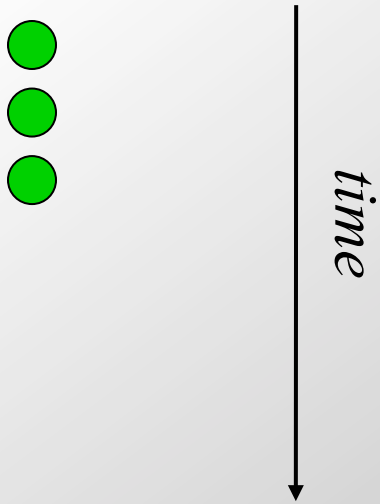
- in ***edge networks*** *(/24* address *blocks,* like 1.2.3.*)
  - most outages are small, *inside* ISPs, *not* from routing
    - e.g.: [Bush et al, IMC 2007]; us: ~70% smaller than routable prefixes
  - want to characterize what people see at home

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(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

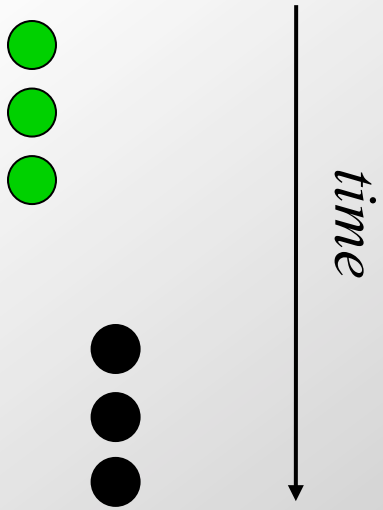
^C
--- 8.8.8.8 ping statistics ---
6 packets transmitted, 3 received, 50% packet loss, time 6001ms
rtt min/avg/max/mdev = 83.602/86.627/89.641/2.465 ms



Background: Active Probing with Pings

pings (ICMP echo request)
draw **positive replies** when an IP address is in use

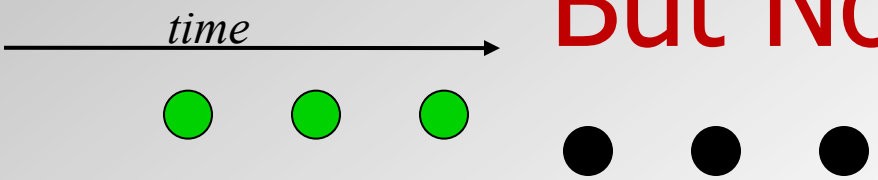
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_req=1 ttl=251 time=89.6 ms
64 bytes from 8.8.8.8: icmp_req=2 ttl=251 time=83.6 ms
64 bytes from 8.8.8.8: icmp_req=3 ttl=251 time=86.6 ms



or get **negative (non-)replies**

no reply from 8.8.8.8: icmp_req=4
no reply from 8.8.8.8: icmp_req=5
no reply from 8.8.8.8: icmp_req=6
^C
--- 8.8.8.8 ping statistics ---
6 packets transmitted, 3 received, 50% packet loss, time 6001ms
rtt min/avg/max/mdev = 83.602/86.627/89.641/2.465 ms

Pings Tell You Something But Not Everything

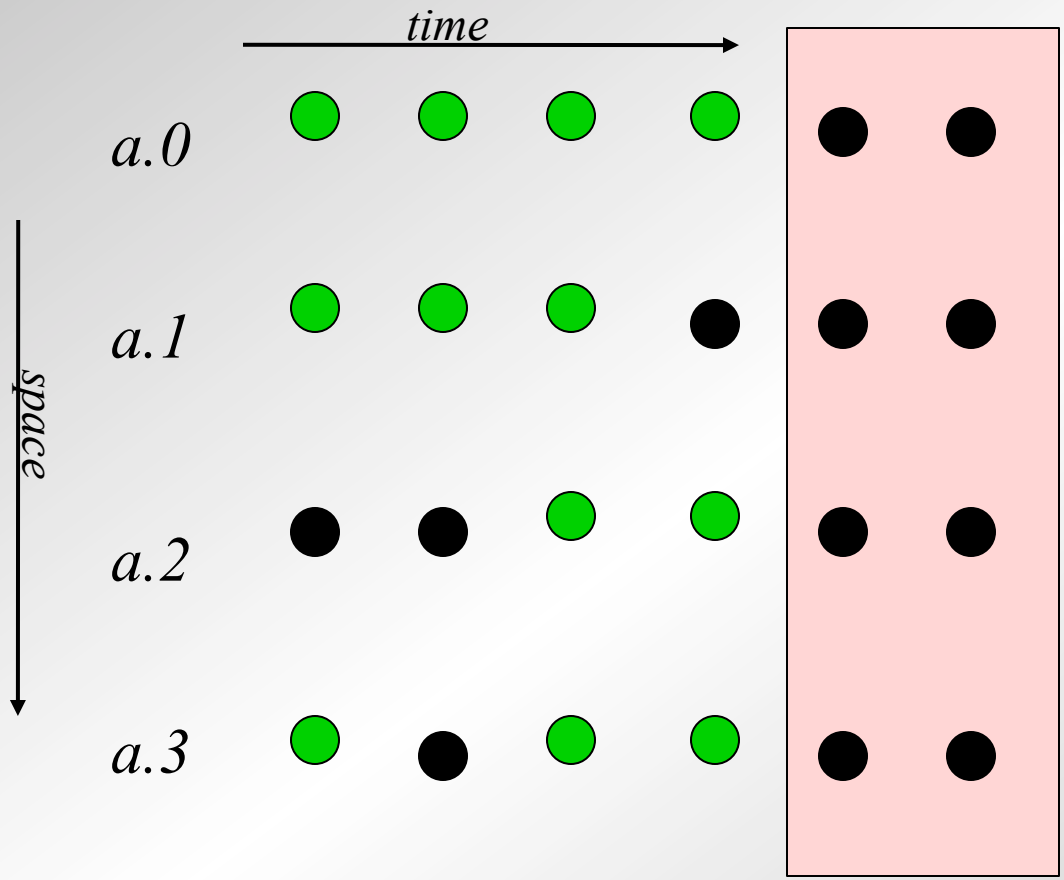


positive:
block is up

negative:
block is down
or
computer crashed
laptop suspended
computer address reassigned
probe or reply lost
firewall enabled

negative replies are ambiguious

So We Probe *Multiple* Addresses

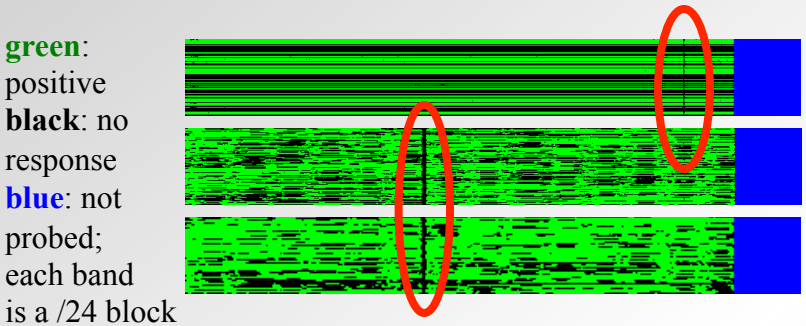


all negative together disambiguates:

network is ***really*** *down*

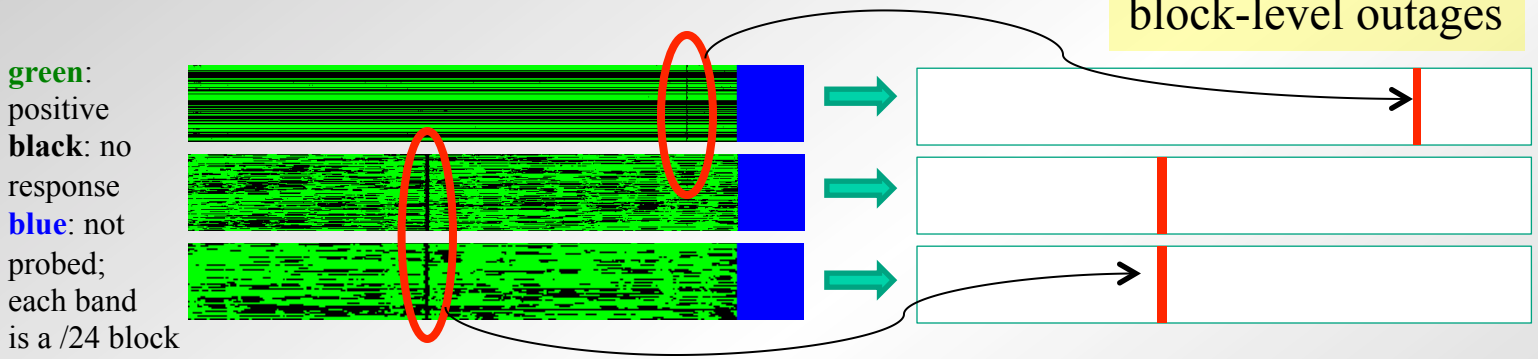
Approach: Detect Changes in Ping Response

1. probe multiple addresses in each block frequently



Approach: Detect Changes in Ping Response

1. probe multiple addresses in each block frequently

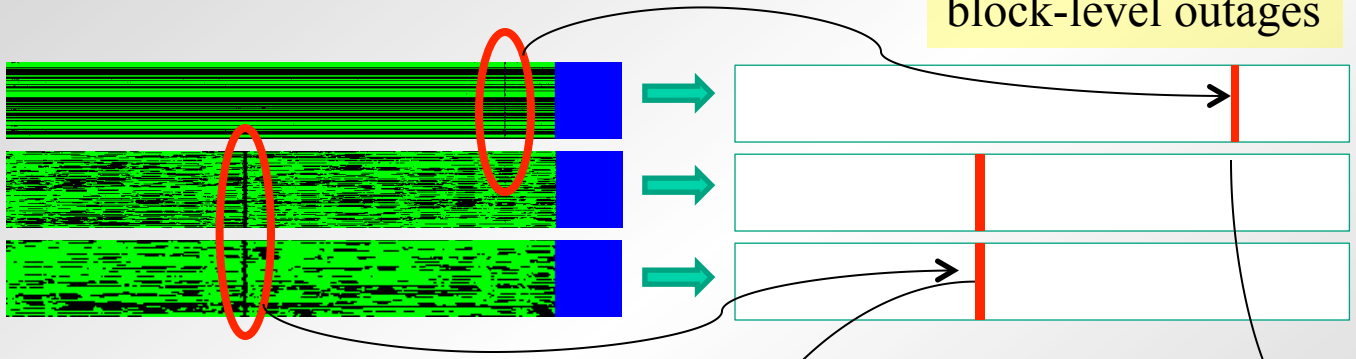


2. gaps indicate block-level outages

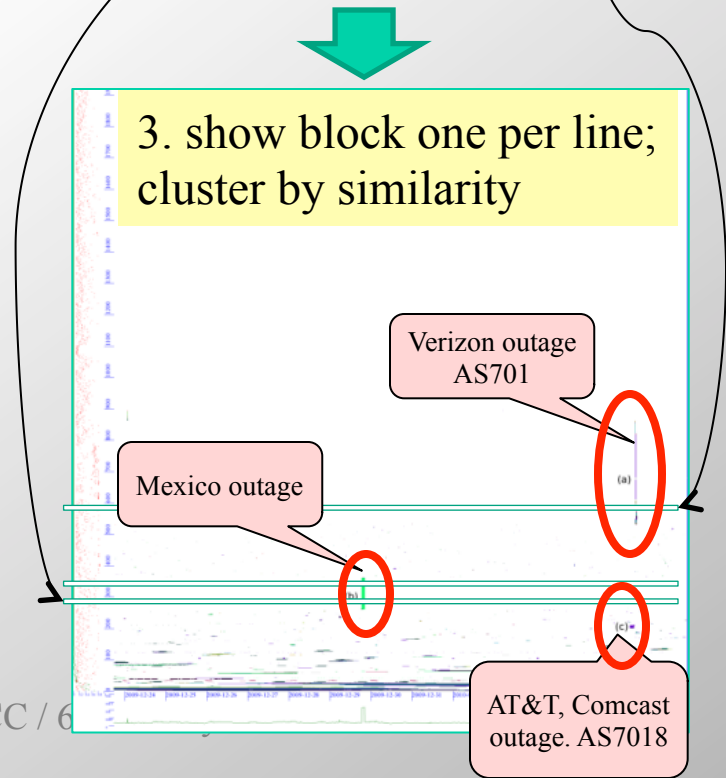
Approach: Detect Changes in Ping Response

1. probe multiple addresses in each block frequently

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



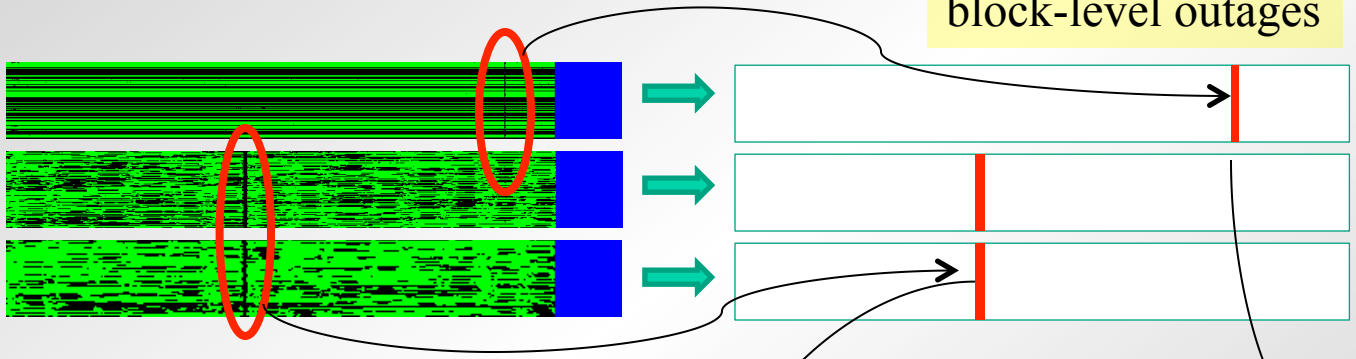
2. gaps indicate block-level outages



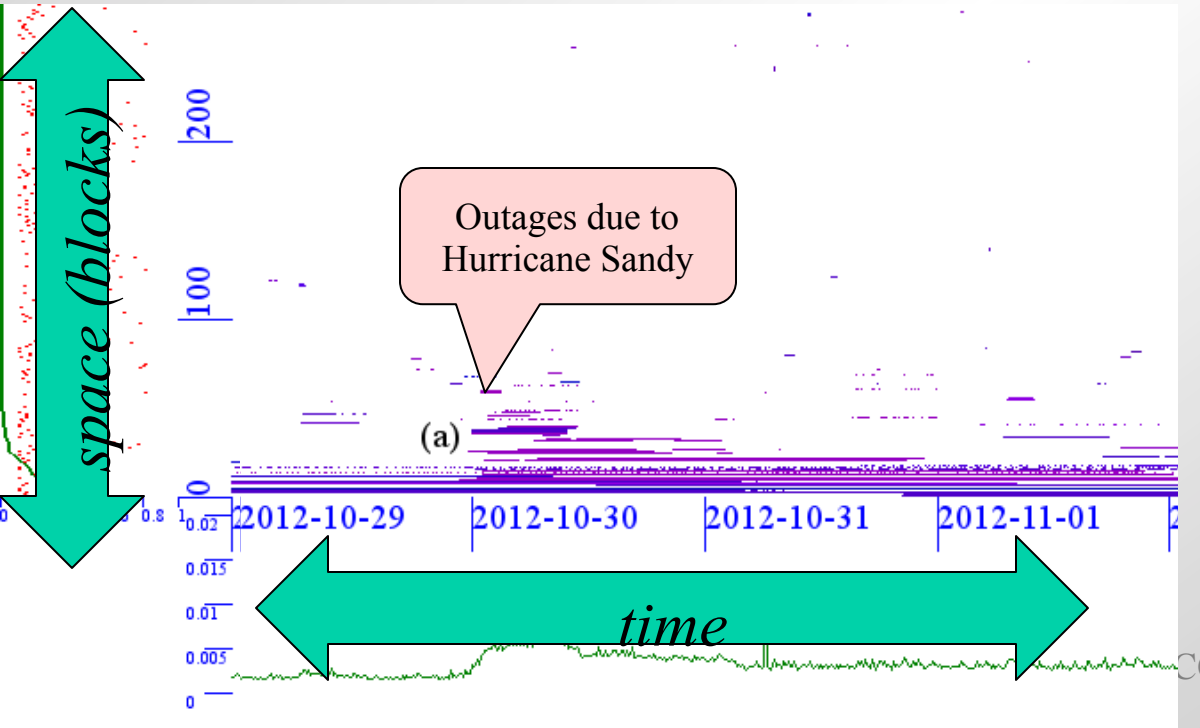
Approach: Detect Changes in Ping Response

1. probe multiple addresses in each block frequently

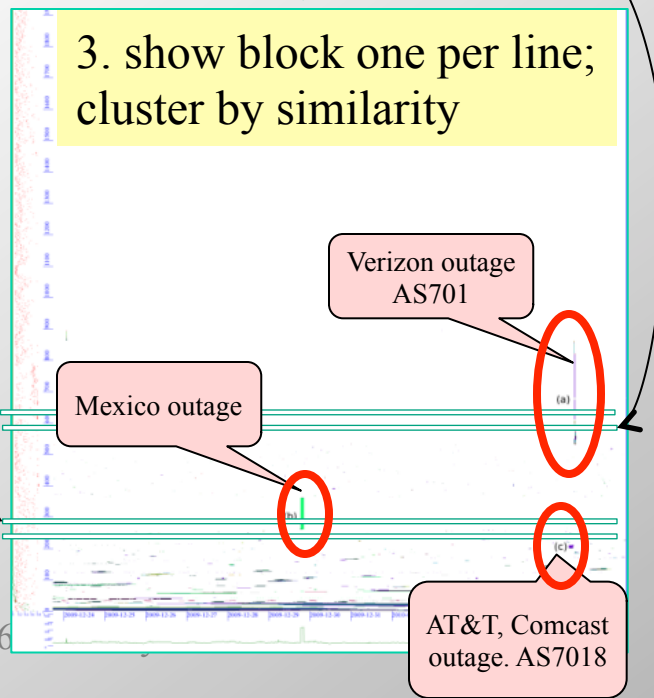
green: positive
black: no response
blue: not probed; each band is a /24 block



2. gaps indicate block-level outages



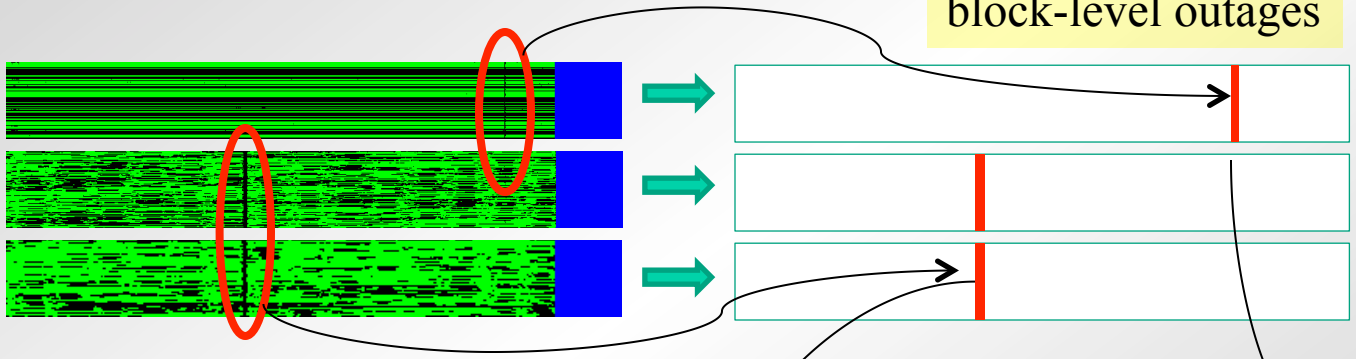
3. show block one per line; cluster by similarity



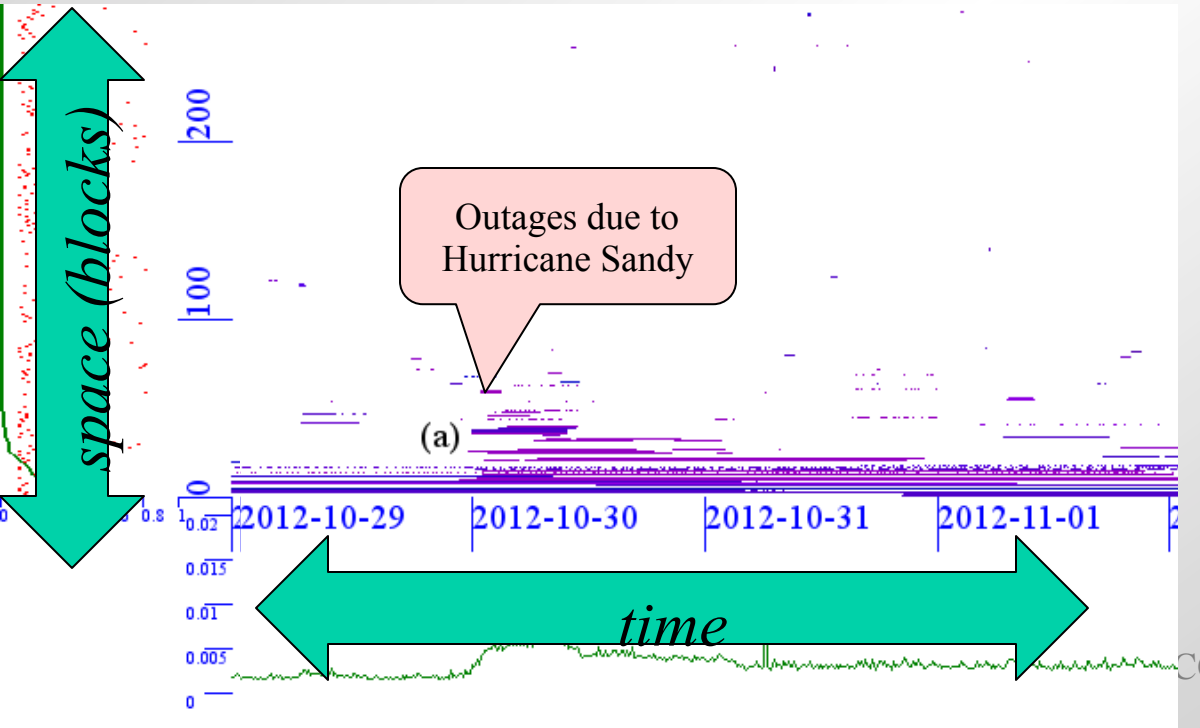
Approach: Detect Changes in Ping Response

1. probe multiple addresses in each block frequently

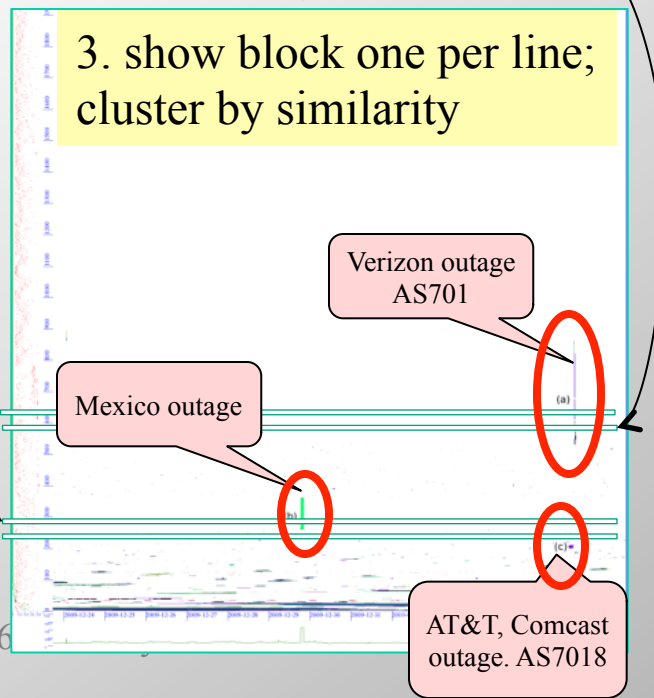
green: positive
black: no response
blue: not probed; each band is a /24 block



2. gaps indicate block-level outages



3. show block one per line; cluster by similarity



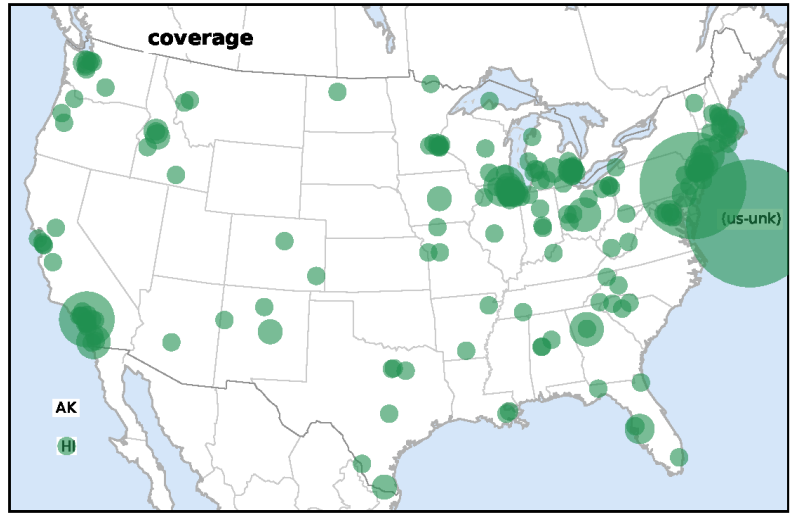
Details: Sandy Analysis

- 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

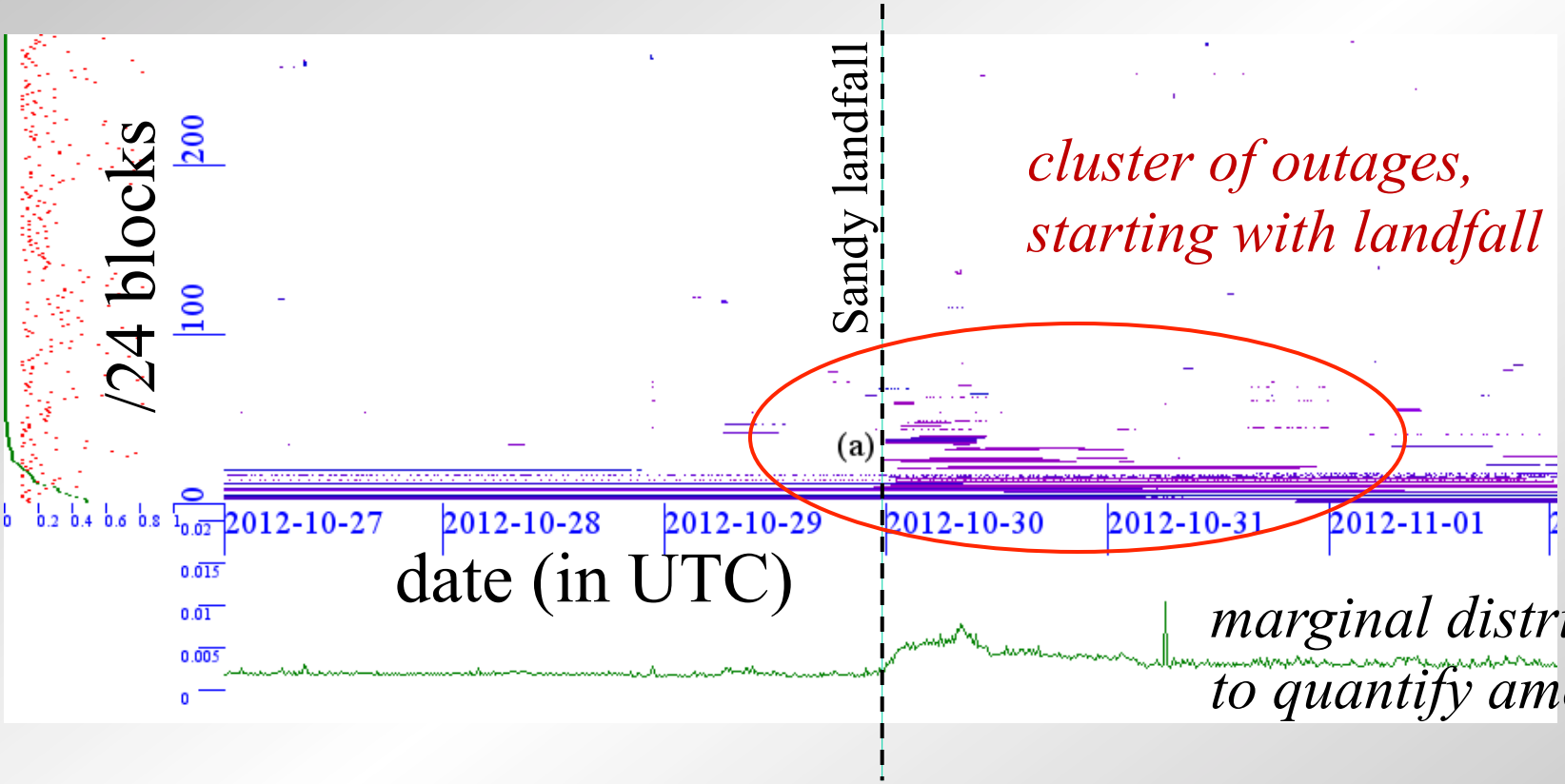
- details and data are available
  - ISI-TR-678b: http://www.isi.edu/~johnh/PAPERS/Quan12a.html
  - data: http://www.isi.edu/ant/traces/

Data About Sandy

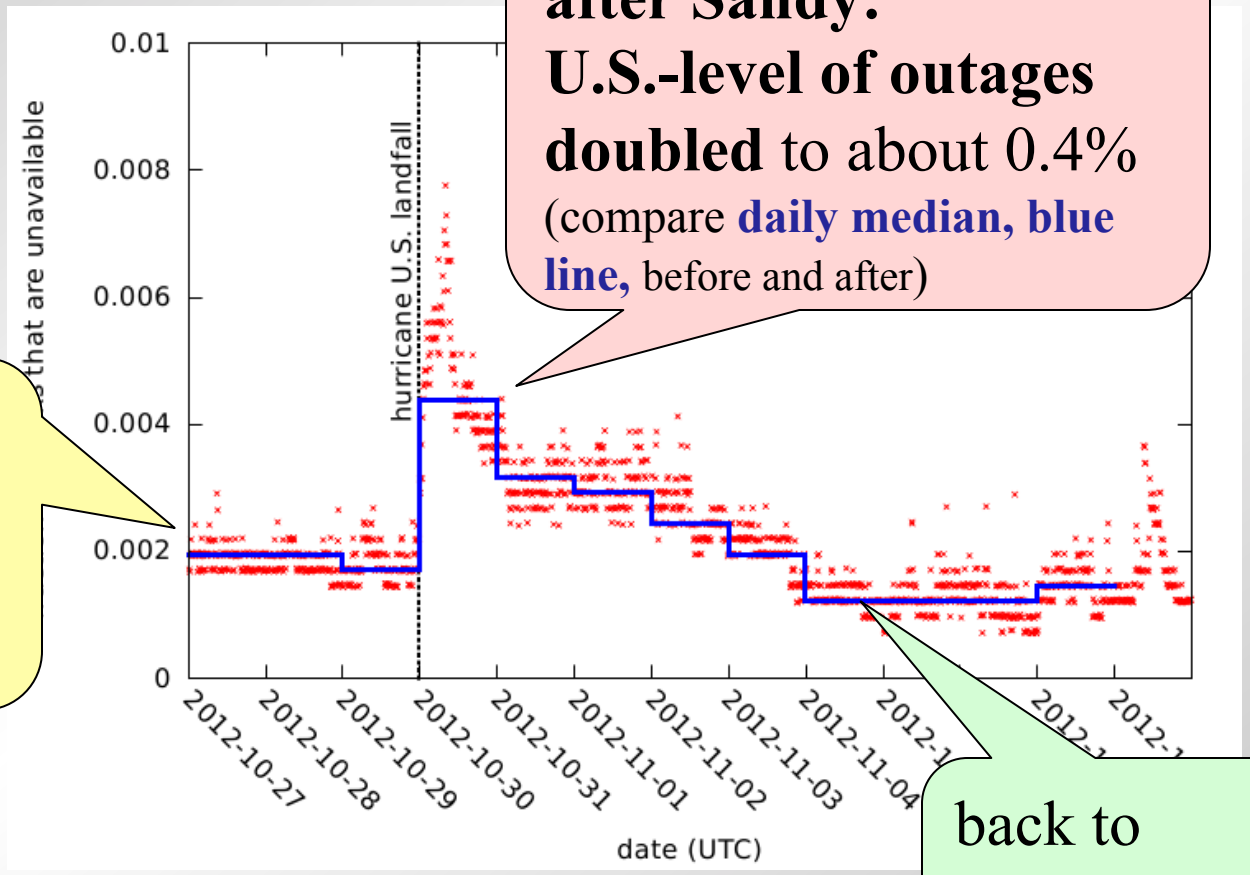
- look at one dataset: internet_address_reprobing_it50j-20121027
- 41,582 /24 blocks
- 11,900 geolocate to US
- 4,117 have enough reponse to analyze
  - 60 of these don't have states



Outages at Sandy Landfall



Measuring the Impact



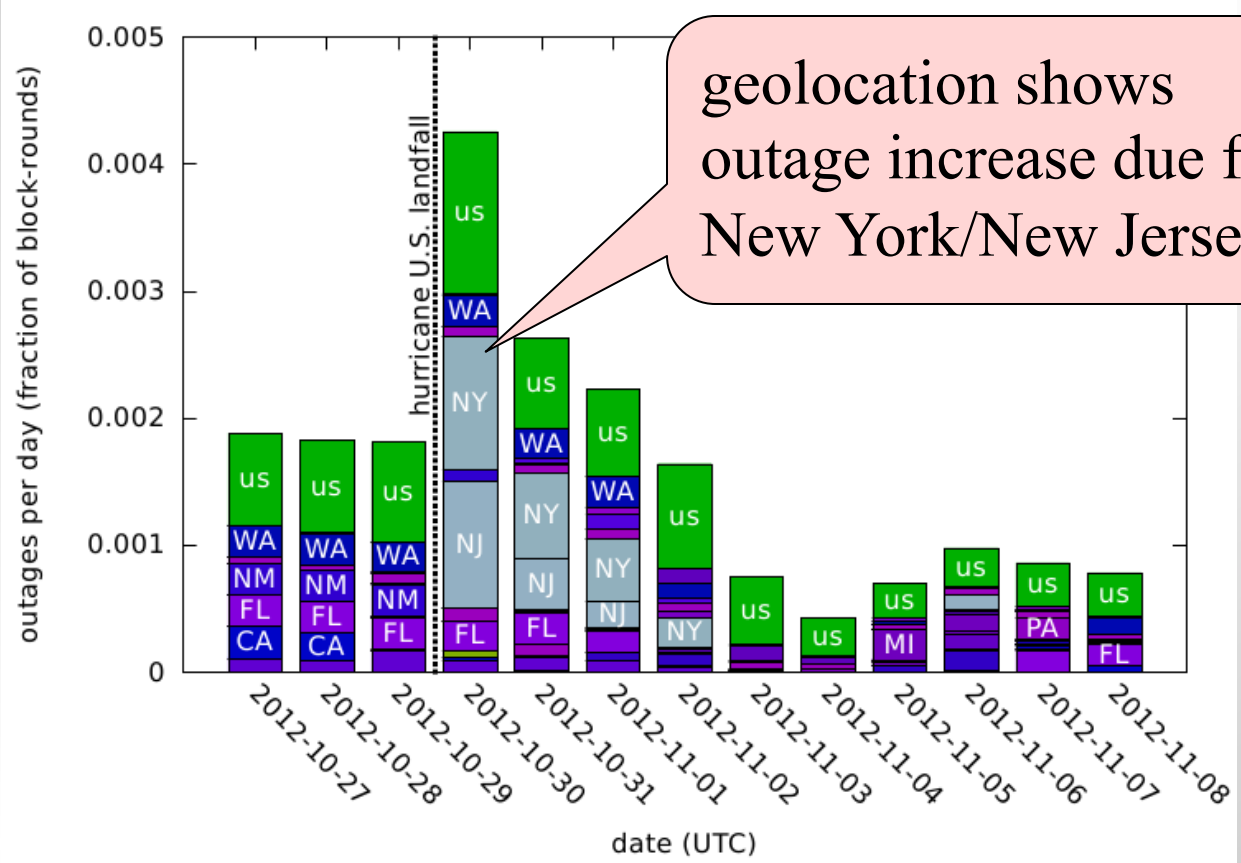
after Sandy:
U.S.-level of outages doubled to about 0.4%
(compare **daily median, blue line,** before and after)

always *some outages* in US:
about 0.2%

(each red X is amount of U.S. outage for 11 minutes)

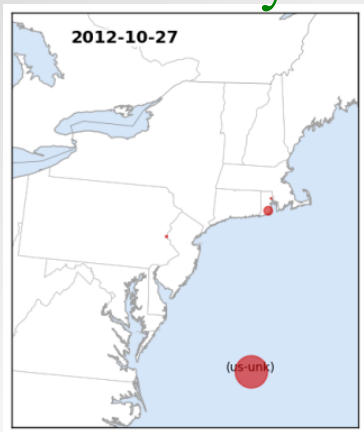
back to baseline after about 4 days

Where Are Outages? NY/NJ



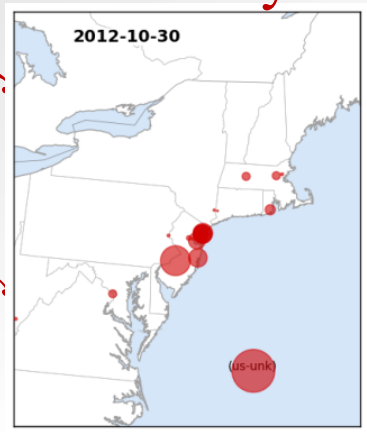
The Northeast, by Day

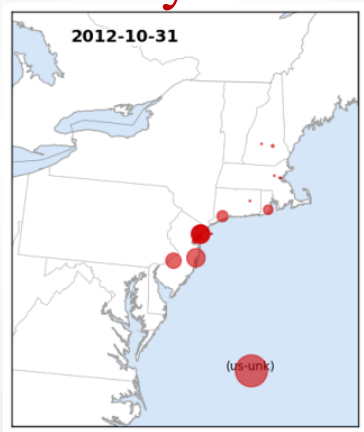
3 days before Sandy landfall



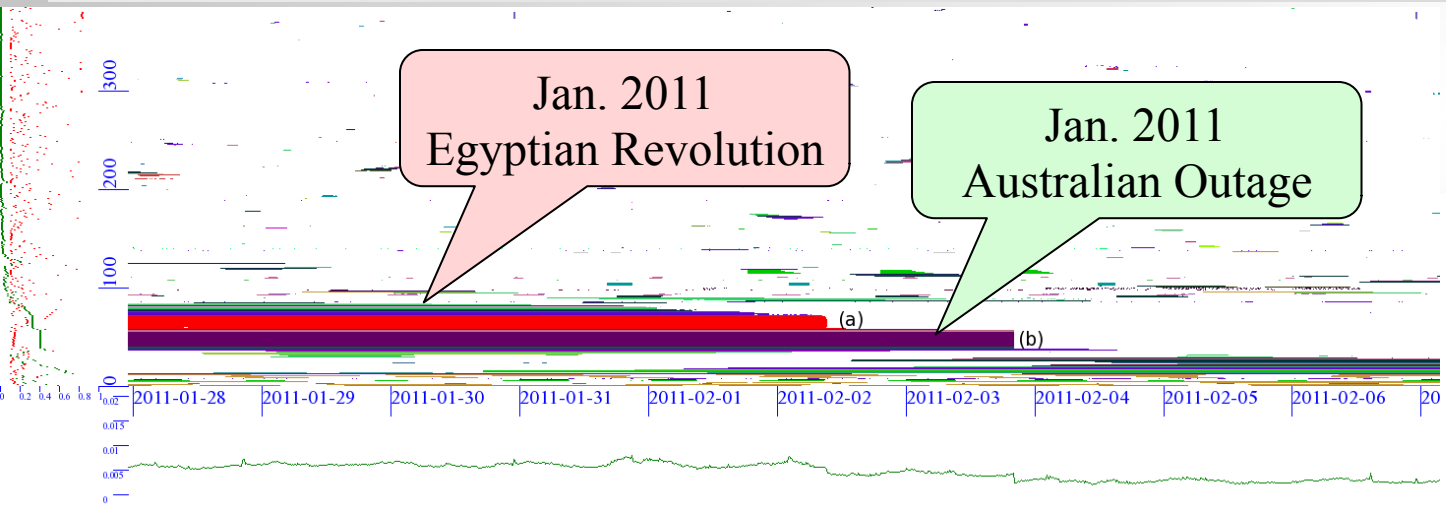
Sandy landfall

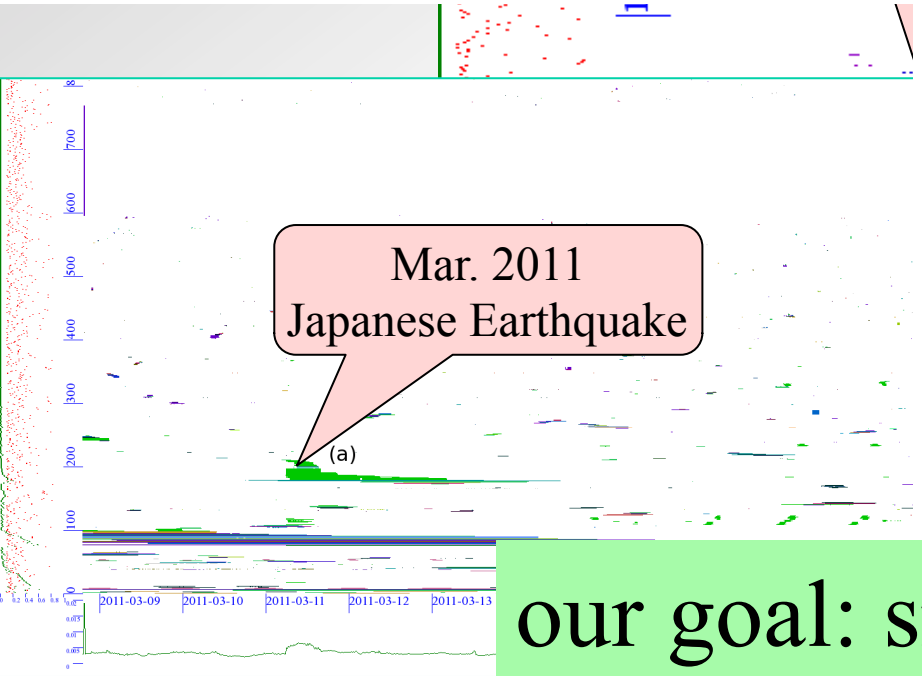
4 days after Sandy landfall

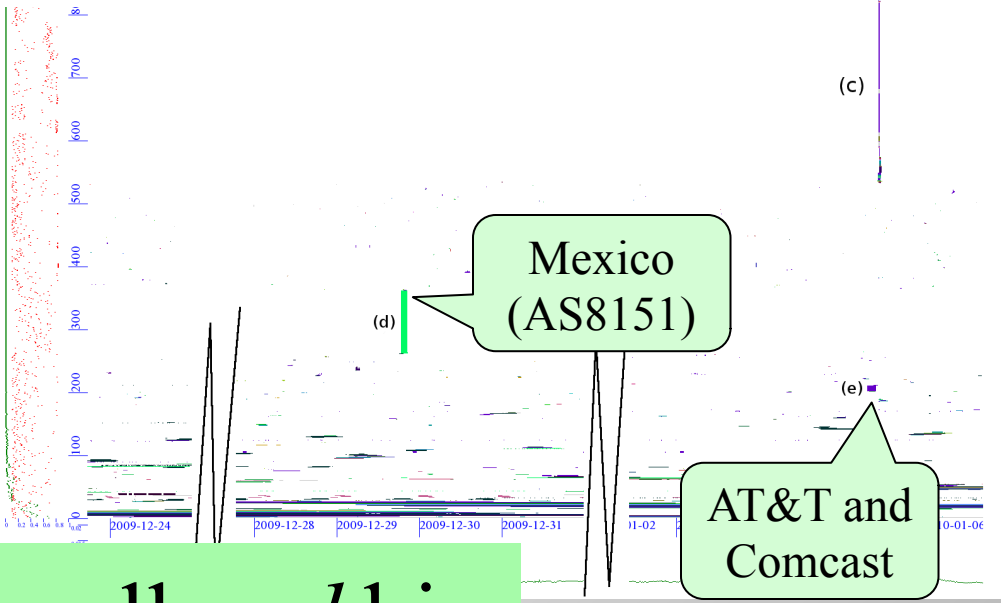




Outages: Prominent and *Unknown*







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