Internet Outages:
Reliability and Security

John Heidemann

with Joseph Bannister1, 3*, Genevieve Bartlett1, Christos Papadopoulos2, Yuri Pradkin1, Lin Quan1, 4*, Abdulla Awabel1, Guillermo Baltra1, Dominik Staros1
1: USC/ISI, 2: Colorado State University, 3*: Aerospace Corp, 4*: Bank of China (* work done when at USC/ISI)

23 April 2018

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 FA8750-13-2-0104, and contract number SPAWARR 7060010644. The views expressed in this report do not necessarily reflect the views of the authors and do not necessarily represent those of DHS, its components, or any other sponsoring agency.

The Internet is Important…

Online sales boomed on Black Friday

By Jackie Stasavage

November 24, 2017 11:17:47 AM EST

...record $5 billion [online sales] in 24 hours...

Black Friday 2017 was all about digital sales.

American shoppers spent a record $5 billion in 24 hours. That marks a 25.9% increase in dollars spent online compared to Black Friday 2016, according to data from Adobe Digital Insights, which tracks 80% of online spending at America's 100 largest retail websites.

Digital retail giant Amazon (AMZN, Tech30) said Friday that orders were rolling in "at record levels." More than 100,000 toys were sold in just the first five hours of the day, the company said. Amazon did not provide sales figures for Black Friday.

activities today are only online

...5 hours/day on mobile, half on social media...
The World Is Important

hurricanes, floods, fires, blizzards...

before landfall:

few outages

serious outages (red circles), N. of Corpus Christi

many outages (large circles), in Houston-flooding

Hurricane Harvey, August 2017

animation: (play)
https://ant.isi.edu/outage/ani/harvey/

Outages: Reliability and Security

network reliability as security

the Internet is important: Internet reliability is one aspect of security

communication without intentional network interference

speedy physical recovery to natural disasters

Network Reliability as Security

threats from weaknesses in critical infrastructure
Network Reliability as Security:
Country-level Interference in the Internet

Egypt Cuts Off Most Internet and Cell Service

Jan. 2011
Egyptian Revolution

can we document government-level interference in the Internet?

Physical conduits used by the U.S. Internet.

Network Reliability as Security:
Infrastructure Resilience and Points-of-Failure

can we discover hidden dependences in the Internet’s infrastructure?

Clustering algorithms discovering Time Warner’s network from their Sept. 2014 outage.
Network Reliability as Security: Safety in the Physical World

hurricanes, floods, fires, blizzards…

Hurricane Harvey, August 2017

animation:  
https://ant.isi.edu/outage/ani/harvey/

Three Steps

• network reliability is a security problem

• measuring the Internet… Censuses  
  – how big is it?

• measuring Internet outages  
  – they say something about the real world, too!

• years of outages  
  – revealing hidden dependencies
Three Steps

• network reliability—a security problem
• measuring the Internet uses
  – how big is it?
• Internet outages
  – revealing hidden dependencies
• years of outages
  – new questions

results with
scientific rigor

knowledge and data
that others build on

Who We Are

outage detection and visualization

Christos Papadopoulos, CSU co-PI
Guillerme Bahra, USC/ISI
Hang Guo, USC/ISI
Abdul Qadeer, USC/ISI
Wei Lan, USC/ISI
Han Zhang, CSU
Liang Zhu, USC/ISI
Yuri Pradkin, USC/ISI (now: Bank of China)
John Heidemann, USC/ISI, PI
Dominik Stamos, USC/ISI and imaginewc.com

part of the LACANIC project: https://ant.isi.edu/lacanic/

with hosting from
USC/ISI—Marina del Rey and Arlington, VA
CSU
Keio University, Japan
Athens U. of Economics and Business
SurfNet, Netherlands

and ongoing collaboration with
FCC to evaluate technology

LACRENDE is part of the
DHS IMPACT program

www.impactcybertrust.org
Three Steps

• network reliability is a security problem

• **measuring the Internet… Censuses**
  – how big is it?

• measuring Internet outages
  – they say something about the real world, too!

• years of outages
  – revealing hidden dependencies

The Internet

[Jon Postel, Dec. 1969]

[map by CAIDA; data from Cheswick and Burch; 2000]

[Cable and Wireless (only); 1999, by Ramesh Govindan]

[AS-level map; CAIDA, Aug. 2007]
The Internet

[Jon Postel, Dec. 1969]

(map by CAIDA; data from Cheswick and Burch; 2000)

[AS-level map; CAIDA, Aug. 2007]

[Cable and Wireless (only); 1999, by Ramesh Govindan]

The Internet

[map by CAIDA; data from Cheswick and Burch; 2000]

[AS-level map; CAIDA, Aug. 2007]
Prior Work: Studying Only The Core

map all edge hosts
(each public, unicast IPv4 addr)

and scale to the size of today’s Internet

just the network core

traceroute to each network; map routers and links
(Cheswick and Burch 2000; Tangmunarunkit et al, 2001; Spring et al, 2002)

observe routing tables
(Huffaker et al, 2001; Meng et al, 2001; Francis et al, 2001)

Us: Study All of Today’s Internet

map all edge hosts
(each public, unicast IPv4 addr)

and scale to the size of today’s Internet

our approach:
ping all addresses once (census)
some addresses many times (survey)
quantify sources of error

goal: scientific impact
(ex: Q: how big is the Internet?)
Active Measurement of the Internet

we ping (ICMP echo request) all IPv4

192.0.2.1

192.0.2.2

192.0.2.3

192.0.2.4

192.0.3.1

we find computers and unused space temporarily unused: (sleeping)

intentionally silent (firewalled)

and network problems

Our Insight:
Observing the Internet Informs

we can probe the whole Internet (the public, unicast, IPv4 Internet)

“only” 4 billion possible addresses we probe blocks: adjacent 256 addr (like 192.0.2.0 to 192.0.2.255) a census: all 12 million blocks

challenge: interpreting the results and probing sustainably}

scientifically rigorous results (known accuracy!)

minimal traffic for 24x7 coverage no harm to the net (or annoying users!)
IPv4 addresses
(today’s Internet)
$2^{32}$ addresses (~4 billion)
usually written: 4 parts, each 8-bits
192.0.2.1

map linear addresses

to 2D
Hilbert Curve

address blocks: adjacent addresses with same first $n$ bits
192.0.*.* /16
or just 192.0/16
(prefix=192.0, n=16)
blocks are squares on map
The Internet

- each pixel is 65k IP addresses (a /16)
- 65k pixels = all $2^{32}$ addresses
- brightness: responsiveness
- green/red-ness: degree of positive vs. negative replies
- blue: reserved, not probed
- cyan: private or multicast, not probed
- layout: Hilbert Curve

The Whole Internet

- here, 1 pixel is 1 address
- 2.8x2.8m (9x9') at 600dpi
- green: positive, red: negative; white: no resp.
But Does This Mean Anything? (validation!)

- not a perfect statement of truth
  - misses NAT’ed hosts (Network Address Translation)
  - misses non-ping-responsive hosts (from firewalls)
  - some pings are lost (we estimate <5%)
- the best current view of the Internet; and a new methodology to refine data suggesting new questions

Sources of Error

- overcounting
  - routers and multi-homed hosts: estimated at <6% in paper
- undercounting
  - probe loss: random due to order; use 1-repair process to recover single losses in survey
  - firewalled hosts: coming up
- variance
  - measurement location: doesn’t matter; normal error
  - sampling error:
    - can predict from theory
    - function of probe frequency
    - surveys within 0.4% (with 95% confidence)
  - births/deaths during survey: estimate in paper
  - probe type (ICMP vs. TCP): ICMP consistently more complete
Sources of Error

- **overcounting**
  - routers and multi-homed hosts: *estimated at <6% in paper*

- **undercounting**

- **variance**
  - measurement location: *doesn’t matter; normal error*
  - sampling error:

Validation:
method: compare ICMP (pings), TCP, and observed traffic

- with **USC’s network** (good ground truth, but maybe biased)
- with **million random IP addresses** (weaker ground truth but unbiased)

Validation with USC and a Random Sample

<table>
<thead>
<tr>
<th>USC Survey (82k hosts)</th>
<th>1M Random Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>category:</strong></td>
<td><strong>any</strong></td>
</tr>
<tr>
<td>addresses probed</td>
<td>81,664</td>
</tr>
<tr>
<td>responding any</td>
<td>54,078</td>
</tr>
<tr>
<td>ICMP or TCP</td>
<td>27,586 (100%)</td>
</tr>
<tr>
<td>responding ICMP</td>
<td>19,800 (72%)</td>
</tr>
<tr>
<td>ICMP only</td>
<td>17,054 (62%)</td>
</tr>
<tr>
<td>TCP only</td>
<td>14,764 (57%)</td>
</tr>
<tr>
<td>Passive</td>
<td>25,706 (93%)</td>
</tr>
</tbody>
</table>

responding any:
addresses at our border routers, or in ICMP or TCP scans

Census is *incomplete*, but can *estimate error*
⇒ we see 62% of truth at USC

Both USC and random sample are similar
⇒ 62% or 74% of truth
⇒ USC seems representative
Impact of IPv4 Censuses

• how big is the net?
• complete allocation of IPv4: but are we using it?
• how do we use the net?
• assisting topology discovery?
• what about network reliability?
• do others build on it?


“Understanding Block-level Address Usage in the Visible Internet”, Cai & Heidemann; ACM SIGCOMM, 2010

“Selecting Representative IP Addresses for Internet Topology Studies”, Fan & Heidemann; ACM IMC, Nov. 2010

“Trinocular: Understanding Internet Reliability Through Adaptive Probing”, Quan & Heidemann, SIGCOMM, 2013

datasets use and follow-on work by others
Impact of IPv4 Censuses

- how big is the net?
- complete allocation of IPv4: but are we using it?
- how do we use the net?
- assisting topology discovery?
- what about network reliability?
- do others build on it?

---

How Big is the Internet?

<table>
<thead>
<tr>
<th>address type</th>
<th>count</th>
<th>%IPv4</th>
<th>%unicast</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 addresses</td>
<td>4,293M</td>
<td>100%</td>
<td></td>
</tr>
<tr>
<td>special (multicast, pvt, etc.)</td>
<td>587M</td>
<td>13%</td>
<td></td>
</tr>
<tr>
<td>unallocated</td>
<td>5.9M</td>
<td>10%</td>
<td></td>
</tr>
<tr>
<td>allocated unicast</td>
<td>3,702M</td>
<td>86%</td>
<td>100%</td>
</tr>
<tr>
<td>responsive</td>
<td>419M</td>
<td>9%</td>
<td>11%</td>
</tr>
<tr>
<td>positive</td>
<td>371M</td>
<td>8%</td>
<td>10%</td>
</tr>
<tr>
<td>negative</td>
<td>50M</td>
<td>1%</td>
<td>1%</td>
</tr>
<tr>
<td>non-responsive</td>
<td>3,281M</td>
<td>76%</td>
<td>89%</td>
</tr>
<tr>
<td>best estimate: in-use, allocated unicast</td>
<td>670M-796M</td>
<td>17%</td>
<td>19%</td>
</tr>
</tbody>
</table>

Data: Aug. 2017
(census USC/LANDER internet_address_survey_077w-20170830)
IP Hitlists
(Where Should Topology Studies Probe?)

study series of censuses
(data on all reachability)

look at each /24’s history

find best representative
for each /24 block
over the IPv4 Internet
(best: likely to respond)

hitlists are available for research use; see https://ant.isi.edu/traces/

“Selecting Representative IP addresses for Internet Topology Studies”, Fan & Heidemann, ACM IMC 2010

Others Build On It:
Using Our Data and Redoing Our Code

• we run as service
• sharing with
  – https://www.impactcybertrust/
  – in US, Japan, Australia, UK, Canada, Netherlands, Israel, Singapore
  – directly if IMPACT cannot
• data shared as of 2018-03-31:
  – 1231 datasets (1.3TB compressed)
  – 96 unique researchers

several groups scan IPv4, building on our work

• Carna Botnet (2013-03)
  – anonymous grayhat hacker
  – reused 30k compromised home routers and some of our code
  – also scanned for services
  – (vs. us: ethical collection from known servers, only scans for presence)
• ZMap (2013-08)
  – Dumeric, Wustrow, Halderman (U.Mich), Usenix Security
  – inspired by our work
  – goal: as fast as possible
  – (vs. us: politely, at moderate rate)
• and MassScan (2014)
Three Steps

- network reliability is a security problem
- measuring the Internet… Censuses
  – how big is it?
- measuring Internet outages
  – they say something about the real world, too!
- years of outages
  – revealing hidden dependencies

Network Reliability

- our problem: a glitch in our data
- can we find and fix these
  (to get on with our real work)
  … leads to the next part of this talk
From Censuses to Outages

with interpretation *pinging* the Internet
tells network outages
that tell about real world events
responding and stopping

…says something

**Outages: Reliability and Security**

**Hurricane Harvey, August 2017**

before landfall: *few outages*

**serious outages** (red circles), N. of Corpus Christi

**many outages** (large circles), in Houston-flooding

**Hurricane Irma: Watching Recovery**

before, during and after disasters: Irma, Sept. 2017 in Florida…
good recovery underway 24 hours after landfall

**Irma landfall: 2017-09-10t13:10Z at Cudjoe Key, Florida**

https://ant.isi.edu/url/irma/ (play)
Our Insight: Observing the Internet Informs

we can probe the **whole Internet**
(the public, unicast, IPv4 Internet)

"only" 4 billion possible addresses
we probe **blocks**: adjacent 256 addr
(like 192.0.2.0 to 192.0.2.255)
a census: all **12 million blocks**

challenge: **interpreting the results** and **probing sustainably**

- scientifically meaningful results (known accuracy!)
- minimal traffic for 24x7 coverage
- no harm to the net (or annoying users!)

Outages: Reliability and Security
Active Measurement of the Internet

we ping (ICMP echo request) all IPv4

192.0.2.1

ACK

192.0.2.2

we find computers

192.0.3.1

broken network

challenge for outages: ambiguity in non-replies

we ping (ICMP echo request) all IPv4

Intentionally silent (firewalled) and network problems

we ping (ICMP echo request) all IPv4

we find computers

Observing Blocks to Disambiguate Replies

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

multiple probes address ambiguity

all negative: block is down

(blocks: really have 256 addresses, we show 4 here)
Probing Politely: Just Enough

polite: minimal traffic to your net
positive responses => block is up
but don’t need all 4 to learn

1. instead: probe one by one
2. find **one is up** => **stop early**
3. if **try is down** => **try again**
   => stop less early
4. several fail => block down

adaptive probing uses Bayesian inference
informed by model of block response

probing politely => observing without harm

Key Properties of Trinocular

• Trinocular: active probing to detect Internet edge outages
  – **principled**: probe only when needed
    (informed by Bayesian inference)
  – **precise**: outage duration ±330s
    (half of probing interval)
  – **parsimonious**: only +0.7% background radiation
    (at target /24, per Trinocular instance)

**Principled: Bayesian Inference Interprets Probes**

Model: every responding $|E(b)| = 111$, active $A(E(b)) = 0.515$

This block is sparse but consistent, so only a few probes needed.

**15 probes to confirm down**

---

**Precise: Detect All Outages?**

Experiment:

Controlled outages (random duration, 1 to 36 minutes) in test block, measured from 3 different sites (2 in US, 1 in Japan).
Parsimonious: Probing Rate

Experiment:
Trinocular: post-facto analysis of 48 hours operation; background ration: from [Wustrow et al, ACM IMC 2010]; today it is much higher

Impact of Outage Detection

- quantified impact of hurricanes
- observed world events and policy
- others interested in data
- ongoing collaboration with FCC
Impact of Outage Detection

- quantified impact of hurricanes
  - previously: Harvey (2017) and Irma (2017)
  - next: Maria (2017)
- operational network outages
- relationship to government policy

Hurricane Maria: Watching Recovery

before, during and after disasters: Maria in Puerto Rico

Maria landfall:
2017-09-20T10:15Z
at Yabucoa, P.R.

https://ant.isi.edu/url/maria (play)
Impact of Outage Detection

• quantified impact of hurricanes
  – previously: Harvey (2017) and Irma (2017)
  – next: Maria (2017)
• operational network outages
• relationship to government policy

Outages: Reliability and Security

U.S. Outages: August 2014

animating outages for the whole Internet

• this dataset:
  – 4M blocks
  – all of 2014q3
• events:
  – Time Warner outage on 2014-08-27 starting 9:20Z
  – ~11 million customers

https://ant.isi.edu/outages/ani/tw/(play)

two hour outage affected nearly ~11M customers
Impact of Outage Detection

- quantified impact of hurricanes
  - previously: Harvey (2017) and Irma (2017)
  - next: Maria (2017) and Sandy (2012)
- operational network outages
- relationship to government policy

Does The Internet Sleep?

well known: traffic is diurnal
(seen locally everywhere)

people use computers but not always
computers sleep, too

what about IPv4 address usage?
can we see global view?
is there “more Internet” in the day?
The Internet, Awake and Asleep

Pinging the Internet shows active addresses:
- red: more than typical
- white: typical
- blue: fewer

Parts of the Internet sleep: more active during the day:
- fewer: pre-dawn in South America
- more: afternoon in India

https://ant.isi.edu/diurnal/ani/
(play)

Why Study “Sleep”? 

Sleep reflects policy:
Always-on networks a requirement for “broadband”

Diurnal measures network maturity

Sleep correlates with things:
New approach to policy analysis

Sleep affects outage detection:
Must not confuse sleep with down

How big is the net?
Long-term goal
Diurnal affects estimate
Three Steps

• network reliability is a security problem

• measuring the Internet… Censuses
  – how big is it?

• measuring Internet outages
  – they say something about the real world, too!

• years of outages
  – revealing hidden dependencies

Analyzing Long-Term Data

• outage data, 24x7, since Nov. 2013
• about 40TB (!)
• about 20k observations x 4M blocks:
  80G datapoints (!!)

• how to make sense of it?
  – interactive visualization
  – automated clustering
Geographic Visualization

• on the web: [https://ant.isi.edu/outage/world/](https://ant.isi.edu/outage/world/)

• key features
  – circle size: number of blocks out
  – color: percent of blocks out
  – time selection
  – geographic zoom and pan
  – geography: easy to relate to
    (what operators ask for!)

Non-Geographic Visualizations:
the *Network* in Outages

goal: reveal patterns
find dependencies among networks
(colored areas are outages, color shows location)

Quan, Heidemann, and Pradkin
“Visualizing Sparse Internet Events: Network Outages and Route Changes”, First ACM Workshop on Internet Visualization, Nov. 2012
Global Network Outages: Prominent and Unknown

Outages due to Hurricane Sandy

Global Network Outages: Prominent and Unknown

Outages: Reliability and Security

Mar. 2011 Japanese Earthquake

Jan. 2011 Egyptian Revolution

Jan. 2011 Australian Outage

Verizon (AS19262)

Mexico (AS8151)

AT&T and Comcast

our goal: understand small and big

The Visualization Challenge

here ~1/4th (downsampled to fit the screen) of 1/224th of the space (one /8 of IPv4) and 1/12th of the duration (one quarter of ~3 years) …what’s happening? what trends? what’s new?
Efficient Visualization and Clustering

• **visualization with linear ordering algorithm**
  - runtime: $O(n \log n \log m)$
  - for $n$ blocks and $m$ duration timesteps

• **approach**:
  - map clustering to sorting: $O(n \log n)$ in time
  - sort on *multi-timescale bitmap*: $O(\log m)$ in space

• **event clustering**
  - runtime $O(n^2)$
  - parallelizes with Map/Reduce

• **approach**
  - find blocks that transition at the same time

---

Multi-Timescale for Similarity

• **input**: outage timeseries from 5/24 blocks
  - $b_1$: 1111 1110 1111 1111
  - $b_2$: 1111 1111 1111 1111
  - $b_3$: 1111 1100 1111 1111
  - $b_4$: 1111 1100 0111 1111
  - $b_5$: 1111 1110 1111 1111

  goal: cluster by “similarity”

- **Downsample with mean**: keep fractions internally.
- **Concatenate**: 1 - 11 - 1011 - 1110 0111 - 1111 1100 0111 1111
Multi-Timescale Mapping Results

- input: outage timeseries from 5/24 blocks
  - b1 1111 1110 1111 1111
  - b2 1111 1111 1111 1110
  - b3 1111 1100 1111 1111
  - b4 1111 1100 0111 1111
  - b5 1111 1110 1111 1111
goal: cluster by “similarity”

- apply to all blocks...
  - b1 1 - 11 - 1111 - 1110 1111 - 1111 1110 1111 1111
  - b2 1 - 11 - 1111 - 1111 1110 - 1111 1111 1111 1110
  - b3 1 - 11 - 1111 - 1111 1110 - 1111 1110 1111 1111
  - b4 1 - 11 - 1111 - 1110 0111 - 1111 1110 0111 1111
  - b5 1 - 11 - 1111 - 1110 1111 - 1111 1110 1111 1111

- goal: cluster by “similarity”
define similar as adjacent in multi-timescale vectors

result: better clusters
(Hamming distance from 8 to 4)
The Visualization Challenge

here ~1/4th (downsampled to fit the screen) of 1/224th of the space (one /8 of IPv4) and 1/12th of the duration (one quarter of ~3 years) ...what’s happening? what trends? what’s new?

One Visualization Result

the Time Warner outage (the part in this /8)
Clustering to Discovery Dependencies

- visualization is nice, but humans can’t look at everything
- new clustering algorithms can discover dependencies
  - insight: failure at the same time, multiple times => dependency
  - cluster on similarity of fail/recovery events


One Clustering Result

1/224th of the space (one /8 of IPv4) and 1/12th of the duration (one quarter of ~3 years)

the Time Warner outage (the part in this /8)
Iterative Clustering

Clustering over 3 months shows outages but too much data—big outage is split

solution: re-cluster on 3 days around outage

result: 4 big clusters

1/224\(^{th}\) of the space (one /8 of IPv4) and 1/12\(^{th}\) of the duration (one quarter of ~3 years) now just 3 days of time

the Time Warner outage (the part in this /8)

Clustering from Here

• just released clustering technical report
• from here…
  – does clustering relate to external information? (like power outages)
  – what are “normal” outages?
  – can we evaluate policy <= reliability?
  – what policy questions does this bring?
Next Steps

• can you use our data and approaches to improve Internet reliability and security?
• datasets: [www.ImpactCyberTrust.org](http://www.ImpactCyberTrust.org) and [https://ant.isi.edu/datasets/](https://ant.isi.edu/datasets/)
  – data to inform policy?
  – historical data for long-term analysis?
  – compare to your new methods?
• code and papers: [https://ant.isi.edu/](https://ant.isi.edu/)