The Policy Potential of Measuring Internet Outages

John Heidemann
Yuri Pradkin
Guillermo Baltra
University of Southern California / Information Sciences Institute

ABSTRACT

Today it is possible to evaluate the reliability of the Internet. Prior approaches to measure network reliability required telecommunications providers reporting the status of their own networks, resulting in limits on the precision, timeliness, and availability of the results. Recent work in Internet measurement has shown that network outages can be observed with active measurements from a few sites, and from passive measurements of network telescopes (large, unused address space) or large network services such as content-delivery networks. We suggest that these kinds of *third-party* observations of network outages can provide data that is precise and timely. We discuss early results of Trinocular, an outage detection system using active probing developed at the University of Southern California. Trinocular has been operating continuously since November 2013, and we provide (at no charge) data covering about 4 million network blocks from around the world. This paper describes some results of Trinocular showing outages in a large U.S. Internet Service Provider, and those resulting from the 2017 Hurricane Irma in Florida. Our data shows the impact of the Broadband America policy for always-on networks, and we discuss how it might be used to address future policy questions and assist in disaster planning and recovery.

1 INTRODUCTION

Many public policy questions surround Internet access, including what speeds are available, how widespread access is in society as a whole, and in specific segments of public interest (such as education or first responders), and how Internet access is used and shared (including traffic differentiation and network neutrality). Public policy initiatives such as the 2010 Connecting America plan [9] has centered on policies to broadband access speeds, and the Measuring Broadband America policy has evaluated success towards this goal [10] as measured by the SamKnows platform [31].

Recent work has shown that it is possible for third parties to measure *network outages*. We have been measuring Internet outages continuously since November 2013 [25] with active measurements from multiple vantage points and coverage of about 4 million /24 IPv4 network prefixes around the world. (Our data is available at no cost to researchers [24].) Other groups have shown systems that use active measurements to focus on weather-related Internet reliability [29], and passive observations to detect major (country-wide) Internet disruption [4].

We believe that *network reliability* presents compelling policy questions, and that this recent work shows that we have the technical capabilities to provide data to explore these policy questions. In this paper we will briefly describe our measurement approach and explore potential policy questions one might consider. Some policy questions focus on technical options: do different technologies exhibit different levels of reliability? can we see the effects of different levels of investment on reliability? Others focus on public access: how much does reliability vary across different parts of the country, or between urban and rural areas? In early work we use our system to evaluate to what degree the Internet was always-on in different countries [26]. We believe data on Internet reliability opens up answers to similar questions of public policy.

2 MEASURING INTERNET OUTAGES

We first review approaches to measure Internet outages and compare to current state of the art.

2.1 Current Approaches: Self-Reporting and Routing

Current production approaches fall into two broad categories: self-reported data, and routing information.

Self-reporting: The primary source of data about telecommunications reliability today in the U.S. is by self-reporting from telecommunications companies to the Federal Communications Commission (FCC). The FCC operates NORS (Network Outage Reporting System [7]) at all times. Telecommunications providers are legally required to report outages

TPRC 2018, Sept. 2018, Washington, DC, USA

of a given size, defined by expected number of customer-minutes, or that pertain to a few types of specific critical services.

The FCC's DIRS (Disaster Information Reporting System [8]) is activated during major events (like hurricanes), and coordinates information about outages that telecommunications providers voluntarily provide.

Self-reporting has the huge advantage that it is quite trustworthy because it is provided by the telecommunications operators themselves.

There are two main disadvantages of self-reported data. First, it is proprietary, provided by ISPs only for government review. As a result, it cannot be shared or used for external evaluation. Second, self-reported data is handled manually. Manual processing means it is reported slowly (perhaps 24 or even 72 hours after the event), and it is required only for large outages (900,000 user-minutes).

Internet Routing: Routing between organizations in the Internet (specifically *Autonomous Systems*, ASes) usually uses the BGP protocol [27]. BGP exposes AS paths for each network prefix that is routed, allowing an observer to get information from publicly available observers such as RouteViews [33] and BGPmon [34].

Researchers have studied routing paths using public information, and watched for network outages at the routing layer (for example, with Hubble [16]). Some have used routing changes to trigger either investigation with active probing (for example, with iPlane [18]), or re-routing (for example, with LIFEGUARD [17]).

Routing has a huge advantage that AS PATH information is publicly shared (as required by the protocol), so global data is available.

However, multiple studies have shown that reachability is not necessarily aligned with routable prefixes [1, 25], so routing is often not able to detect non-transit related outages, such as those that happen *inside* a large ISP. Quan et al. suggest that most outages (78% of prefix-rounds) are smaller than routable prefixes [25].

2.2 Recent Approaches: Active and Passive Measurements of the Internet Edge

A number of recent approaches have used active or passive information to observe outages.

Trinocular: Active, Global Outages: We have developed Trinocular, a system that detects network outages as the absence of positive responses to active probes [25]. Trinocular is able to detect outages in blocks (each block is an /24 IPv4 network prefix) where at least 15 IP addresses respond to pings. Currently (as of August 2018) there about 4.3 million blocks in this "measurable" Internet, and Trinocular scans them every 11 minutes.

Trinocular employs several algorithms to accomplish this goal: it requires changes to occur on multiple IP addresses to avoid interpreting single-machine failures as false outages. It uses Bayesian inference to interpret the replies it gets and minimize the number of messages needed for an active decision. Minimizing the number of messages is important to reduce traffic on the targets, thereby reducing the number of abuse complaints we see. In addition, having fewer probes permits faster processing, allowing four parallel processes on a single computer to track outages for the entire measurable IPv4 Internet.

Controlled tests have shown that Trinocular detects all outages that last as long as the probe interval of 11 minutes.

We have been operating Trinocular 24x7 since November 2016, and we make the data available to researchers at no cost [24].

Thunderping: Active, Weather-Triggered: Thunderping was first deployed in 2011 [29]. It uses active probing from PlanetLab [23] to track outages at individual IP addresses. To reduce traffic, it triggers probing based on weather alerts. It has run nearly continuously since deployment, although (to our knowledge) its data is not available.

Thunderping complements Trinocular with an independently-derived approach (published slightly earlier). However, it's weather-triggered architecture means it is unlikely to cover non-weather-triggered outages.

Disco: Active, from the Inside: Trinocular and Thunderping employ active probing from a few, central sites to the edge of the Internet. Disco reverses this trend, observing connectivity from thousands of distributed devices (RIPE Atlas probes) to a few central sites [30].

Because Disco is measured from the field, it provides a uniquely strong source of ground truth. While centralized systems like Trinocular and Thunderping may be confused by dynamically-assigned addresses (since address renumbering may appear to be an outage), Disco is robust to such changes and presents what an end-user will see. However, coverage of Disco is limited to locations where physical devices are deployed. As of 2018-08-12, there are 10,292 active measurement sites distributed around the world, although most are in Europe and North America.

CAIDA: Passive, from a Network Telescope: Researches at CAIDA have shown that observations of drops in traffic from a network telescope indicate network outages [4], and they are reporting this data in their IODA website [3]. Their network telescope is a large block of unused addresses, and it receives different kinds of "background radiation", the random traffic sent to any public IPv4 address [22] (for example, worms scanning all of IPv4, or replies to traffic sent with a randomly spoofed source address).

This kind of passive observations are an important complement to active probes, because active probes may be firewalled, background radiation originates from external networks and so is often let out of otherwise firewalled networks.

The limitation of telescopes as a source of passive data is that they receive only a small fraction of background radiation, and that it can be hard to tell real background radiation from traffic with a spoofed source address. Together, these factors reduce the sensitivity of telescopes to detect outages that are small in space or short in duration.

(The IODA website reports three data sources: passive data from a network telescope, routing outages, and active probing inspired by Trinocular.)

Passive, from a CDN: Recently researchers from MIT, U. Maryland, and Akamai suggested CDN data can serve as an alternative source of passive traffic [28]. They look for drops in CDN traffic to indicate network disruption or outages. Unlike background radiation, traffic to CDNs is interactive and so cannot be spoofed (in one sense, it is active traffic between the user and the CDN, although it is a passive source for outage detection). Major CDNs receive a great deal of traffic from human-driven and automated processes running on end-user devices.

Use of CDN traffic as a passive source of outage data may provide much greater sensitivity than network telescope data. Since it is based on two-way traffic exchange, it can also be a strong alternative method to compare active measurement systems like Trinocular. Its main limitation is that it is only available to operators of large, widely used network services such as a major CDN.

Overall Conclusions: Each of these methods have different trade-offs, with some providing more or less precise measurements, greater or less coverage. These methods have all been developed in the last five years and the field continues to evolve rapidly. However, multiple methods with different approaches suggest that we will continue to gain confidence in our ability to observe network reliability.

Current approaches are all specific to the IPv4 portion of Internet. Internet Protocol, version 6 (IPv6) was designed in the late 1990s and today is seeing increasing deployment, particularly on mobile phones. Extending current network measurement systems to IPv6 is an active area of research.

2.3 Coming Approaches: Near Real-Time

In principle, any of the methods described in §2.2 could operate in near real-time.

We have been developing a near-real-time version of Trinocular, called Trinocular-NRT. Trinocular was first implemented based on batch analysis of data in three month chunks. Some Trinocular algorithms explicitly require evaluation of large blocks of times (for example, gone-dark detection requires three weeks of data). However, many of the current implementation choices assume batch processing, and the algorithms are not written to run incrementally. In principle, though, the core Trinocular algorithms can run as quickly as data comes in.

We are currently prototyping Trinocular-NRT, a near-real-time version of the algorithms. We will stream data as it is collected and integrate results from multiple sensors as data arrives. By default, Trinocular probes all blocks every round of 11 minutes (a different base period could be selected if desired), and outage conclusions require fusing results from all sites. This implies the fastest possible response is two rounds or 22 minutes. We have added data compression, and need to account for processing time and potential queueing delay. We expect to report outages within one hour or so of their occurrence.

As of August 2018, Trinocular-NRT is in early alpha testing. We expect it to be operational in fall 2018.

2.4 Case Study: A Large U.S. Internet Service Provider

As an example of outages we can observe with Trinocular, we examined one large U.S. Internet Service Provider (ISP) in 2017q4. Our goal here is to show that it is possible to observe real-world network outages.

Data Analysis: We extract data from Trinocular outage dataset A30 for 2017q4 [32] (outage software version 3). We then identify all network blocks (/24 IPv4 prefixes) for one AS (Autonomous System, the identifier used in wide-area Internet routing) of a large U.S. ISP based on WHOIS data from ARIN taken on 2017-10-06. Many ISPs operate multiple ASes—this ISP has about 120, and we examined its second largest AS which handles about 10% of the address space of the entire ISP. Trinocular measures 2962 blocks in this AS.

Individual Trinocular observers report the status of each block as up, down, or indeterminate. A block is indeterminate if belief about block status is not clearly up or down after 15 probes. (We send at most 15 probes per 11 minutes to limit traffic to any given block.) Indeterminate blocks often have sparse and dynamic address use and so may falsely appear to be down. Manual inspection found about 314 blocks to frequently report indeterminate; we removed these from analysis, leaving 2648 blocks in our results. (We are working to automate detection detection of indeterminate blocks.)

Marginal Distribution of Outages over Time: Figure 1 shows the fraction of blocks of that AS that are out, grouped into 15-minute bins, over this quarter. We see a number of features in this marginal distribution, and label them (a) through (g) for reference.

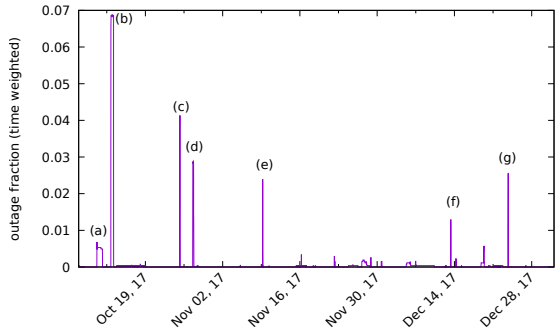

Figure 1: Fraction of blocks that are out over time for a large U.S. ISP in 2017q4.

Examining public outage data made available by this network operator, we found events that correspond to the first three events. The short but wide bump at (a) indicates 15 blocks, all in Alabama, that are out for 25 hours. This period corresponds to when Hurricane Nate was passing through that state. The largest spike, (b) is the loss of 182 blocks for 11 hours. Most of these blocks are in Missouri (161), with 20 in Kansas and one in Alabama. The start of this outage matches an emergency maintenance performed by the operator to one of their networks, but a network in Europe. It is possible that this outage in the US was collateral damage.

We were not able to find external information about the remaining spikes, (c) through (g). All correspond to relatively specific geographic regions (based on IP geolocation). Outage (c) corresponds a short 30-minute outage affecting mainly Alabama (131 blocks), and Florida and Georgia (1 block each). Outage (d) lasted 5 hours, mostly in Montana (69 blocks), with a few others in the west (Kansas, 4; Idaho, 1; Wyoming, 1; Colorado, 1). Outage (e) lasted two hours, in Alabama (60 blocks) and Tennessee (10). Outage (f) also lasted two hours, mostly in Colorado (33 blocks), but also Kansas and Missouri (1 each). Finally, outage (g) lasted 3 hours, mostly in Wisconsin (72 blocks), but also 1 each in Missouri and Michigan.

The marginal distribution can mix results from different events that happen concurrently. For example, event (a) overlaps with two blocks that are flickering up and down, and event (g) overlaps with a number of blocks that become unavailable at the end of the trace. (We filter blocks that are unavailable for more than 25% of the time in a 3 weeks window.)

Clustered events: To disambiguate overlapping events, we next clustered events in time using the Back-Out clustering algorithm [14], which identifies groups of blocks that have common failure and recovery times. Figure 2 shows all clusters where more than one block from this AS has a common outage. Each row of the figure is a block, each gray and white strip is a cluster of blocks, sorted by size. Colored rectangles show outage events.

In Figure 1 each outage is a peak, but here we see that each of those peaks are different parts of the ISP, since each cluster (gray or white band) has only one outage. This visualization of clusters suggests it is likely that these events share a common cause because these events generally share a common start and end time. Three of the larger events, (a), (b), and (d), are split into two or three clusters. Our clustering algorithm is imperfect and sometimes splits some blocks into two clusters due to assignment outage times (measured in seconds, but only with 11 minute precision) to cluster bins (4096 s periods).

3 APPLICATIONS TO POLICY QUESTIONS

One goal of Trinocular outage detection is that public information about outages will allow researchers and policy makers to evaluate questions about Internet policy, reliability, and how they relate. We see *public* data as a key enabler to discussion about these questions, on the principle that such data can be reproduced by independent parties and will serve as a basis for dialog about policy options. We list possible policy questions below, but *our overall goal is add reliability as an explicit design goal*, much as "fast" is a goal today. We also list open challenges to answering these questions.

3.1 Long-term Policy Questions

We see two broad sets of long-term policy questions: understand the technology, and understanding how evenly used it is.

Questions About Technology: Internet outage data can be used to answer important questions about the reliability of different types of "last mile" technologies. For example, are cable modems, DSL, or fiber-to-the-curb or fiber-to-the-home more reliable? The Thunderping researchers have early results exploring these questions [21]. While outage information may be public, details about specific last mile technology is not readily available. Partial evaluation can use inferences from public reverse domain names (DNS), using clues like "dsl" or "cable" to infer link type. However, such information is likely incomplete, since reverse DNS names may not identify technology or may be out-of-date, and it is certainly imprecise, providing no information about specific models of home router or modem.

Public Access: With nation-wide and global outage data, it becomes possible to study questions about consistency of service by location. For example, are urban and rural access equally reliable? U.S. states differ in their local telecommunications policies. Can we see the effects of those differences?

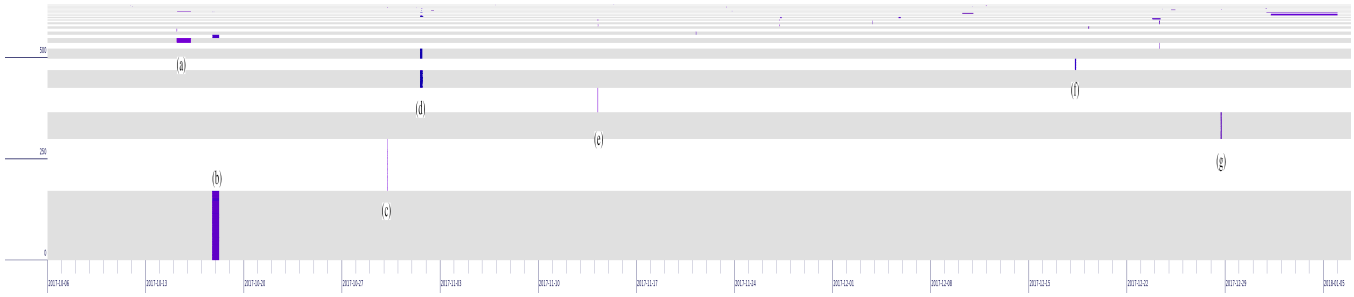

Figure 2: Clusters of outages for a large U.S. ISP in 2017q4. Each row indicates a block over time. Colored regions indicate outages, with colors corresponding to geolocation.

One can also observe effects of global policy differences. We used data from outage detection to evaluate address activity in prior work [26]. We found that the number of active IP addresses in the U.S. and western Europe are roughly constant over the course of a day, but South America, Russia, India and China see large swings in the number of active IP addresses over the course of a day. These swings correspond to the diurnal cycle, addresses least active in the early morning hours, and most active in the late afternoon and evening. Figure 3 shows the fraction of diurnal blocks in each geographic grid cell (grid cells are 2 degree latitude and longitude, and diurnal means that address activity shows a 24-hour periodicity, as defined in Quan et al. [26]).

Long-term Trends and Changes: Observations about network outages can help establish trends in Internet reliability. Important questions include: how do technology changes affect reliability? Does the transition from dial-up and leased lines, to ISDN, to DSL and DOCSIS, and now to fiber-to-the-home, fixed wireless, and newer technologies come with changes in reliability? Long-term, longitudinal studies are possible provided data is collected with a consistent methodology. We plan to study trends using our two years of data.

Planning and Design Studies: Finally, a complement of analysis of trends in the past is planning for the future. Design studies pose "what if" questions, like how reliability may change with greater redundancy, or how many people would be affected by specific damage to infrastructure. Recent reports on the physical infrastructure of the U.S. Internet has suggested that there is sometimes surprisingly limited redundancy at the physical layer in some locations [6]. Edge information such as Trinocular provides may help anticipate the implications of physical outages. Alternatively, measured outage data could be used to *test* such models and evaluate their predictive accuracy.

A particular concern of capacity planning is the risk of cascading problems, where shifts in traffic from one outage trigger overload and failure at another point. Outage observations may help model or test models of cascading failures.

3.2 Short-Term Policy: Detecting and Reacting to Events

Network outage data can also be useful in the very short term to detect, observe, and perhaps react to events like natural disasters and government intervention.

Disasters: Internet outages can occur because of the results of natural disasters. Our early data showed the effects of Hurricane Sandy (2012) on the New York/New Jersey area [15], and we have also reported data about 2011 Tohoku earthquake [25], and and the 2017 Hurricanes Harvey, Irma, and Maria [13].

One use of near-real-time outage reporting (§2.3) is to provide information on disasters as the situation evolves. The extent of a disaster can be difficult to judge, with many parties holding part of the picture. Utility companies have information of the location of problems with their infrastructure (downed power lines, flooded telecommunications facilities, etc.), but public versions of this information are often slow to emerge and obscured. For example, after-action analysis indicated that information about power outages and restoration times were slow to emerge, constraining allocation of resources for recovery and making it difficult for the public to decide when they could return from evacuations [20].

We are working to provide near-real-time outage information to improve *situational awareness* of first responders and the public during disasters. An early version can be seen at our website at https://ant.isi.edu/outage/world/. We have used this website to visualize the 2017 Hurricane Irma's effects on Florida in Figure 4. Here we show outages on a 0.5 degree latitude/longitude grid. In each grid cell, circles indicate the number of network blocks that are out (each block represents 256 adjacent IPv4 addresses, a /24 IPv4 prefix). The color of the circles shows what fraction of blocks are down in that grid cell, with red showing high percentages

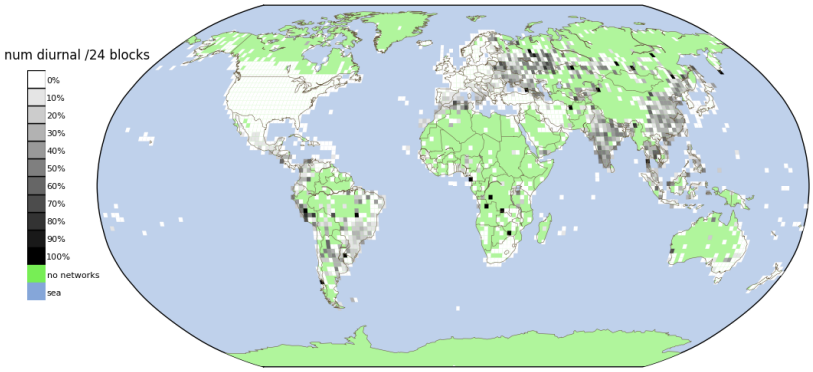

Figure 3: Percent of blocks in each geographic region (a two degree latitude/longitude square) that are diurnal (Figure 13 from [25]).

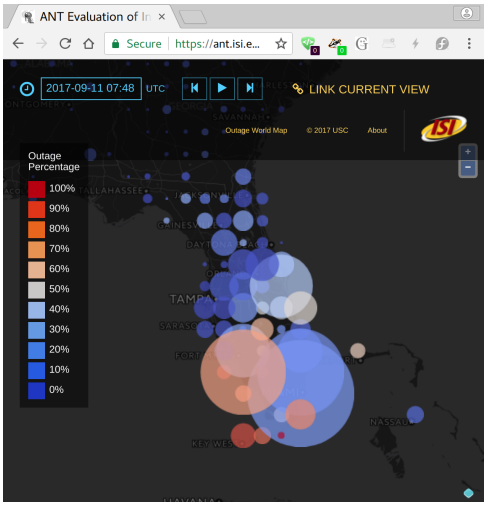

Figure 4: Hurricane Irma affecting Florida. This represents Internet outages observed at 2017-09-11t07:48Z, around 18 hours after landfall in the Florida Keys. Circle sizes show the number of network outages, colors are the percentage.

and blue low. This figure shows many networks are out in the Miami area (the largest circles), and half or more of the network blocks out in the Florida keys and on the gulf coast of the peninsula (the red circles).

This visualization was made with data computed days after the event, but we are expecting to be able to provide near-real-time data by the end of 2018. This visualization shows the potential to provide information about disasters as they occur, with much greater detail about the extent, location, and timing of outages quite soon after problems occur. We hope this information can support first responders and the general public.

Government Intervention: In some countries, government intervention in network connectivity is common. Sometimes this is done to control communications during times of crisis, such as during the velvet revolution in Egypt in 2011 [4, 12], or recently in Ethiopia [2]. Other countries regularly turn off the Internet to prevent cheating on national exams, including Iraq [11, 19] and Bangladesh [5]. Outage detection measurements can help document these events.

4 CONCLUSIONS

We have suggested that we should begin considering the policy implications of *network reliability*. We have described ongoing research by multiple groups to collect data on Internet outages using multiple methods including active measurement and passive observations. Using data from Trinocular, an outage detection system using active measurements operated by the University of Southern California, we showed that we can see specific network events in a large U.S. ISP. We also showed we can provide detailed information about network outages that result from natural disasters, identifying both the time and the location of problems shortly after they occur. We are currently working to deploy this kind of near-real-time reporting, and hope that our long-term data can inform policy studies, and our near-real-time data can assist immediate response.

We make our data available at no cost to researchers, with both on-line visualization (https://ant.isi.edu/outage/world/) and downloadable datasets for analysis (https://ant.isi.edu/datasets/outage/).

ACKNOWLEDGMENTS

This research is partially supported by the Department of Homeland Security (DHS) Science and Technology Directorate, HSARPA, Cyber Security Division, as sponsored by Air Force Research Laboratory under agreement number

FA8750-17-2-0280, and by DHS S&T/CSD via contract number 70RSAT18CB0000014. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon.

REFERENCES

[1] Randy Bush, Olaf Maennel, Matthew Roughan, and Steve Uhlig. Internet optometry: assessing the broken glasses in Internet reachability. In *Proceedings of the ACM Internet Measurement Conference*, pages 242–253. ACM, November 2009.

[2] Abdi Latif Dahir. Ethiopia has resorted to its old habit of blocking the internet to quell internal unrest. News website Quartz Africa, Aug. 8 2018.

[3] Alberto Dainotti, kc claffy, Alistair King, Vasco Asturiano, Karyn Benson, Marina Fomenkov, Brad Huffaker, Young Hyun, Ken Keys, Ryan Koga, Alex Ma, Chiara Orsini, and Josh Polterock. IODA: Internet outage detection & analysis. Talk at Active Internet Measurement Workshop, March 2017.

[4] Alberto Dainotti, Claudio Squarcella, Emile Aben, Marco Chiesa, Kimberly C. Claffy, Michele Russo, and Antonio Pescapé. Analysis of country-wide Internet outages caused by censorship. In *Proceedings of the ACM Internet Measurement Conference*, pages 1–18, Berlin, Germany, November 2011. ACM.

[5] Dhaka Tribune Desk. Internet services to be suspended across the country. *Dhaka Tribune*, Feb. 11 2018.

[6] Ramakrishnan Durairajan, Paul Barford, Joel Sommers, and Walter Willinger. InterTubes: A study of the US long-haul fiber-optic infrastructure. In *Proceedings of the ACM SIGCOMM Conference*, pages 565–578, London, United Kingdom, August 2015. ACM.

[7] Federal Communication Commission. *Code of Federal Regulations, Tile 47 (Telecommunications), Part 4 (Disruptions To Communications)*, December 2004. Ammended 2016.

[8] Federal Communication Commission. Disaster Information Reporting System (DIRS). FCC Service https://www.fcc.gov/general/disaster-information-reporting-system-dirs-0, 2007.

[9] Federal Communication Commission. Collecting America: the national broadband plan. Technical report, FCC, March 2010.

[10] Federal Communication Commission. 2016 measuring broadband America fixed broadband report. Technical report, FCC, December 2016.

[11] Samuel Gibbs. Iraq shuts down the Internet to stop pupils cheating in exams. *The Guardian*, 18 May 1996.

[12] James Glanz and John Markoff. Egypt's autocracy found Internet's 'off' switch. *New York Times*, page A1, Feb. 16 2011.

[13] John Heidemann. Internet reliability, from addresses to outages. Talk at the UCLA Computer Science Department, February 2017.

[14] John Heidemann, Yuri Pradkin, and Aqib Nisar. Back out: End-to-end inference of common points-of-failure in the Internet (extended). Technical Report ISI-TR-724, USC/Information Sciences Institute, February 2018.

[15] John Heidemann, Lin Quan, and Yuri Pradkin. A preliminary analysis of network outages during Hurricane Sandy. Technical Report ISI-TR-2008-685b, USC/Information Sciences Institute, November 2012. (correction Feb. 2013).

[16] Ethan Katz-Bassett, Harsha V. Madhyastha, John P. John, Arvind Krishnamurthy, David Wetherall, and Thomas Anderson. Studying black holes in the Internet with Hubble. In *Proceedings of the 5th USENIX Symposium on Network Systems Design and Implementation*, pages 247–262, San Franciso, CA, USA, April 2008. USENIX.

[17] Ethan Katz-Bassett, Colin Scott, David R. Choffnes, Ítalo Cunha, Vytautas Valancius, Nick Feamster, Harsha V. Madhyastha, Tom Anderson, and Arvind Krishnamurthy. LIFEGUARD: Practical repair of persistent route failures. In *Proceedings of the ACM SIGCOMM Conference*, pages 395–406, Helsinki, Finland, August 2012. ACM.

[18] Harsha V. Madhyastha, Tomas Isdal, Michael Piatek, Colin Dixon, Thomas Anderson, Arvind Krishnamurthy, and Arun Venkataramani. iPlane: An information plane for distributed services. In *Proceedings of the 7th USENIX Symposium on Operating Systems Design and Implementation*, pages 367–380, Seattle, WA, USA, November 2006. USENIX.

[19] Doug Madory. Iraq downs internet to combat cheating...again! Dyn Blog https://dyn.com/blog/iraq-downs-internet-to-combat-cheating-again/, February 2017.

[20] Department of Energy (Office of Electricity Delivery and Energy Reliability). Overview of response to Hurricane Sandy-nor'easter and recommendations for improvement. Technical report, DOE-OEDER, February 2013.

[21] Ramakrishna Padmanabhan, Aaron Schulman, Ramakrishnan, Sundara Raman, Reethika Ramesh, Dave Levin, and Neil Spring. Measuring and inferring weather's effect on residential Internet infrastructure. Presentation at Active Internet Measurement Workshop, March 2018.

[22] Ruoming Pang, Vinod Yegneswaran, Paul Barford, Vern Paxson, and Larry Peterson. Characteristics of Internet background radiation. In *Proceedings of the ACM Internet Measurement Workshop*, pages 27–40, Taormina, Sicily, Italy, October 2004. ACM.

[23] Larry Peterson and Timothy Roscoe. The design principles of PlanetLab. *ACM Operating Systems Review*, 40(1):11–16, January 2006. (Also PDN-04-021, June 2004).

[24] ANT Project. Ant project outage datasets. https://ant.isi.edu/datasets/outage/, April 2013. Outage datasets are updated quarterly since Nov. 2013.

[25] Lin Quan, John Heidemann, and Yuri Pradkin. Trinocular: Understanding Internet reliability through adaptive probing. In *Proceedings of the ACM SIGCOMM Conference*, pages 255–266, Hong Kong, China, August 2013. ACM.

[26] Lin Quan, John Heidemann, and Yuri Pradkin. When the Internet sleeps: Correlating diurnal networks with external factors. In *Proceedings of the ACM Internet Measurement Conference*, pages 87–100, Vancouver, BC, Canada, November 2014. ACM.

[27] Y. Rekhter and T. Li. A border gateway protocol 4 (bgp-4). RFC 1654, Internet Request For Comments, July 1994.

[28] Philipp Richter, Ramakrishna Padmanabhan, Neil Spring, Arthur Berger, and David Clark. Advancing the art of internet edge outage detection. In *Proceedings of the ACM Internet Measurement Conference*, page to appear, Boston, Massachusetts, USA, October 2018. ACM.

[29] Aaron Schulman and Neil Spring. Pingin' in the rain. In *Proceedings of the ACM Internet Measurement Conference*, pages 19–25, Berlin, Germany, November 2011. ACM.

[30] Anant Shah, Romain Fontugne, Emile Aben, Cristel Pelsser, and Randy Bush. Disco: Fast, good, and cheap outage detection. In *Proceedings of the IEEE International Workshop on Traffic Monitoring and Analysis*, pages 1–9, Dublin, Ireland, June 2017. Springer.

[31] Srikanth Sundaresan, Walter de Donato, Nick Feamster, Renata Teixeira, Sam Crawford, and Antonio Pescapè. Broadband Internet performance: A view from the gateway. In *Proceedings of the ACM SIGCOMM Conference*, pages 134–145, Toronto, Ontario, Canada, August 2011. ACM.

[32] USC/LANDER Project. Internet outage measurements. IMPACT ID USC-LANDER/LANDER:internet_outage_adaptive_a30all-20171006 at https://ant.isi.edu/datasets/internet_outages/, October 2017.

[33] Route Views. University of Oregon Route Views Project. web site http://www.routeviews.org, 2000.

[34] Lisa Yan and Nick McKeown. Learning networking by reproducing research results. *ACM Computer Communication Review*, 47(2):19–26,

April 2017.