

Advancing the Art of Internet Edge Outage Detection

Abhishek Shrestha
(abhishek.shrestha@campus.tu-berlin.de)

Seminar "Network Architectures: Internet Measurement",
Technische Universität Berlin

SS 2019

1 Introduction

Internet connectivity has become ubiquitous in the modern society. Not only individual users but a multitude of critical services and business enterprises depend on a reliable network connection. This is also reflected by various studies and projects undertaken by government and research bodies for measuring and monitoring internet connectivity [4 - 7]. Thus, reliability is an important characteristic for any network. Nevertheless, reliability in terms of network connection is very hard to measure, particularly because of the sheer size of networks spanning over millions of connections, heterogeneity of these networks as well as due to lack of available data provided from the service providers to study the internet outage events [1]. There are already measures like replicated services and content delivery networks that can suppress outages, however, understanding cause, duration and timings of failures across a network is one of the important steps towards providing a more robust connection.

The authors in this paper present a prediction model to analyze and breakdown causes of internet disruptions and outages by studying the data from a large CDN and thereby try to provide a fine grain understanding of when and why these disruptions occur.

Their study is based on the CDN access logs which contain entries of per hour requests sent by the connected devices and address blocks. A sudden absence of entry in the log indicates a loss of internet connectivity in the specific IP address blocks, this is called a disruption. A service outage on the other hand means loss of internet access service in the address blocks. Therefore, although a disruption might be caused due to an actual service outage, every disruption does not necessarily mean that there was a service outage but instead a disruption might mean that the public IP of the host has changed or has been reassigned. The authors present a detailed study featuring disruption size, timing and frequency of occurrences based on the CDN logs and connectivity log from individual devices to argue that large share of detected disruption or service outage might be due to planned human activities such as server maintenance, prefix migration and user movement and thus might not always indicate network failures or issues. Another important aspect of the paper is that the

authors, through the data, make a distinction between which disruptions represent an actual service outage and which are anti-disruptive events and not an actual service unavailability. Further, they compare their findings with Trinocular [2], an established tool to measure internet outage to validate their results.

The rest of the paper is organized as follows: We discuss the related works in Section 2. Section 3 details the implemented methodology. Section 4 analyses and interprets the results and also presents a comparison of results with Trinocular and finally in Section 5 provides an overview and discuss the implications of the work.

2 Related Work

There are a lot of research works in internet outage detection and reliability. Turner et al. [3] use router configuration files, syslog archives and operational mailing list to recreate failure events in a network. They then perform an extensive analysis of five years of such data from a network consisting of over two hundred routers. Basically, they extract the failure events from the syslog and router configuration files over the defined period and deduce cause of failure by referring to the administration email logs. The data is then analyzed for failure duration, cause and impact. The data sources used is easily available and is not restricted to a research group or require any special permission. Similarly, Banerjee [1] et al. use the outage mailing list [18] to investigate outages. The outage mailing list contains outage reports and discussion, impacts and troubleshooting information relating to major outages. This information is parsed using NLP and are then clustered into labeled categories using machine learning techniques and are then analyzed to derive probable cause, impact and type of disruption. The experiment was performed on outage data accumulated over seven years.

Benson et al. [8] use IBR traffic analysis to detect disruptions. Their methodology is rather interesting. Their system is based on observing IBR traffic from passive darknet [9]. IBR basically constitutes of TCP SYNs trying to connect to hosts but since darknet does not respond, these signals have to be retransmitted. These retransmissions follow a consistent pattern and thus the absence of these retransmission signals can be considered as packet loss and thus can be used to detect disruptions.

Trinocular [2] an outage detection system, uses active probing to detect disruptions. It sends multiple ICMP probes per hour to over 3 million /24 address blocks. If it detects any unresponsive prefixes, it flags it as a disruption. The authors compare their system against the disruptions detected by Trinocular.

3 Methodology

This section describes in detail the dataset and the analysis methodology implemented by the authors.

3.1 Dataset

Each request from the client to access web object from CDN is logged. The authors used these CDN logs as the data set for analysis. The data set consists of number of hits or requests from each IP address for a period of 54 weeks (March 2017 - March 2018). The dataset is quite large (about 1.2 billion active IPv4 addresses over the course of one year), considering they used logs from one of the world's largest CDNs which contained over 240,000 servers in over 13 countries and containing about 1,700 networks and serving about 3 trillion HTTP requests daily.

Due to hourly binning of datasets, for disruptions to be detected, they must last over a full calendar hour. CDN servers are generally in the same network as end user and also if there are any problems in connection to a server, as long as client has internet connection, user can be connected to another server and this usually takes less than a minute. So absence of hits from a particular IP address for about an hour indicates that either the device is disconnected by the client, loss of connection due to maintenance or could be due to other external events.

3.2 Baseline activity as reference

Always-on devices like mobile phones which are constantly connected to the network and make regular CDN requests provide us with a steady number of requests to CDN. This effect is called the baseline activity. The sudden absence of the requests from these devices can be recognized as a disruption.

The authors selected a subset of prefixes which demonstrated this base line activity and limited their observation to only those prefixes which have a constant high enough baseline i.e. prefixes with sufficient number of addresses which show the base line activity.

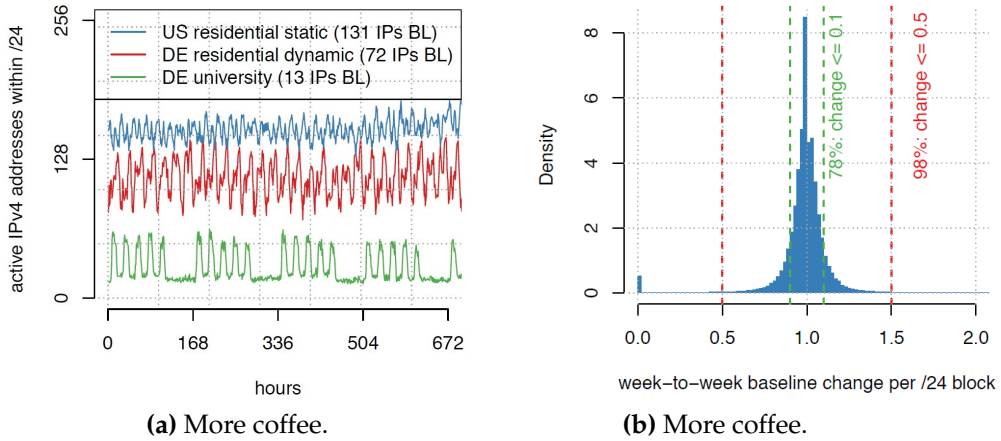


Figure 1: More coffee.

Fig 1.a. shows an example of baseline activity. The fig illustrates the number of active addresses per hour for three /24 address blocks. As we can see all of these address blocks show a baseline activity i.e. over the duration of a month, each address block has a steady minimum number of devices connected for any given hour. The drop to minimum value

during the end of the week for university address blocks is understandable since there are less number of students in the University during the weekends, and hence less number of connected devices

For the purpose of evaluation throughout the year the baseline activity should show a continuity i.e. the baseline should be maintained throughout the months over a whole year. Fig 1.b. shows that over 80% of address block show only about 10% change in baseline activity and only 2% address blocks have baseline varying more than 50%. To get the plot, for each /24 first, only those weeks which have minimum baseline of 40 were selected. Then the baseline of the week was divided by the baseline activity of the subsequent week where the subsequent week might have a baseline value greater or less than 40. Thus, we can see from the figure that the baseline activity is quite continuous.

3.3 Detecting the disruptions

For detecting the disruption a sliding window is used. For each /24, a minimum number of active addresses in each hour is calculated over the last 168 hours, this is denoted by b_0 . Then the window is slid over an hour, updating the value of b_0 . As soon as b_0 falls below a threshold $\alpha \times b_0$ where $0 < \alpha < 1$, the current window is left and a new window is created beginning at this hour and this hour is marked as the beginning of a non-steady-state period. The new window is slid and minimum value of b_0 is computed until it reaches a new threshold $\beta \times b_0$ where $\beta \times b_0$ is close to b_0 and this hour is then marked as the end of non-steady-state period. The non-steady-state period marks a disruption. This is illustrated in fig. 2. for a single /24 address block.

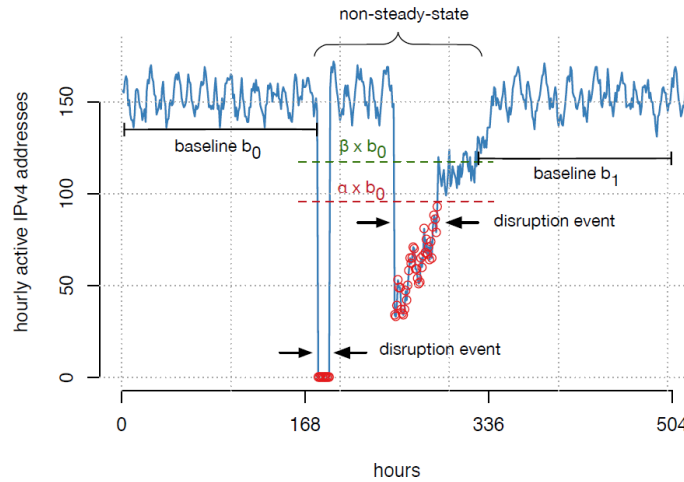


Figure 2: A boat.

However, there is a possibility that after entering a non steady state period, the new base line $\beta \times b_0$ is never reached. The window is slid regardless searching for the new baseline for 2 weeks. And if after 2 weeks the base line is not met then the non-steady-state is not regarded as disruption and the window is continued to slide.

3.4 Parameter selection

Authors state in the paper that they performed several experimentations for the minimum value of b_0 and found that for a prefix to be traceable, the minimum number of active addresses should be at least 40.

A proper calibration of the values of α and β is required for the algorithm to give accurate measurement. α being very low means that the algorithm will be less responsive while a high value of α would mean that the algorithm will be very sensitive to even slightest change in the baseline. Similarly, a high value of β would mean that for a non-steady-state to be classified as disruption, baseline has to be restored to values closer to b_0 while low value of b_0 would mean that it will take less addresses to be active again for a non-steady-state to be classified as a disruption, and hence there is possibility that long term baseline changes might be considered as a disruption.

For determining proper values of α and β , disruptions detected against various values of α and β are compared against ICMP probing responsiveness. We can see from figure 3.a. that a disruption i.e. loss of activity in CDN is also accompanied by a distinct drop in ICMP responsiveness. We can use this metric to calibrate proper values for α and β . Now since

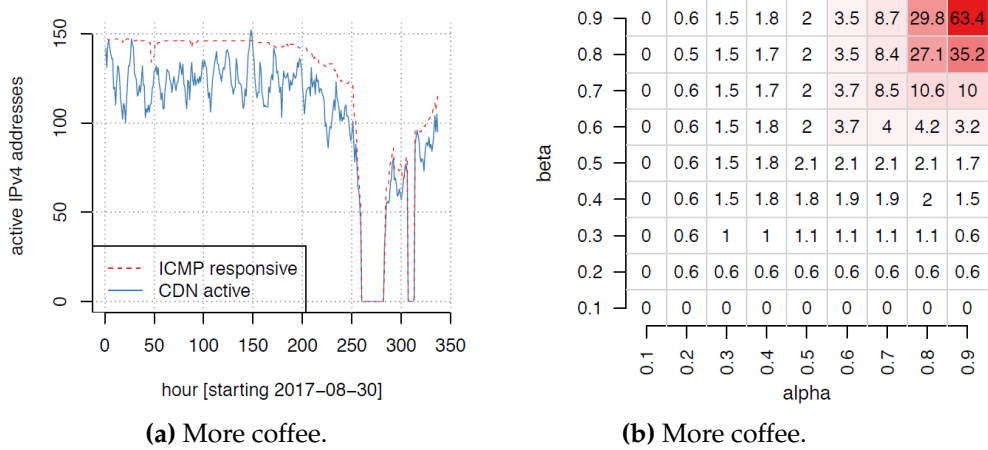


Figure 3: More coffee.

actively probing a large address space requires substantial bandwidth and also according to authors, measurements show that about 40% of addresses contacting CDN do not respond to ICMP probes. Therefore, they use already available ICMP data from ISI [10 -14]. The data is from four surveys between June and September 2017. Since, we are comparing against CDN data, the addresses in the survey data must also overlap with CDN. So, all addresses that are not in CDN are removed and also the address blocks that have less than 40 responsive addresses are removed which resulted in about 15K ISI data for comparison.

Authors then selected various combinations of values of α and β . Then the non-steady-states detected by each combination are compared against the ISI dataset. And as mentioned earlier the disruptions much also show a drop in ICMP responsiveness and for those which are not classified as disruptions, the ICMP responsiveness should not drop below 40. If the maximum value of ICMP responsive address during the disruption is less than the minimum

value outside the disruption, then the disruption is classified as “agree” otherwise it is classified as “disagree”.

Fig. 3.b. shows percentage of disagreement of CDN detection with the ISI data for different values of α and β . As we can see, for very low values of α and β the disagreement is also very low. This makes sense since low values of α and β means that the algorithm is more restrictive, for instance, if we consider α as 0.1 then this would require the active addresses to drop significantly (near 0) to be classified as disruption. This would definitely also be accompanied by drop in ICMP responsiveness because of drastic drop in active addresses. In contrast, for high values of α and β the disagreement is also higher. This is also obvious since high values of α and β would make the algorithm more sensitive. Authors end up selecting β as 0.8, since a higher value of β means that the system would want more addresses to be active to consider a period to be classified as a disruption which makes the system more restrictive and removes possibility of considering slight increase in active addresses to be end of a non-steady-state period. Moreover, for smaller values of α , β does not increase considerably for any value. Higher value of β is therefore more appropriate. Considering β as 0.8, from fig. 3.b. we can see that the value of α increases with largely after 0.5. Thus, from this observation, α is then fixed at 0.5 to keep the disruption under 3%.

4 Results and evaluation

4.1 Outcomes and experiments

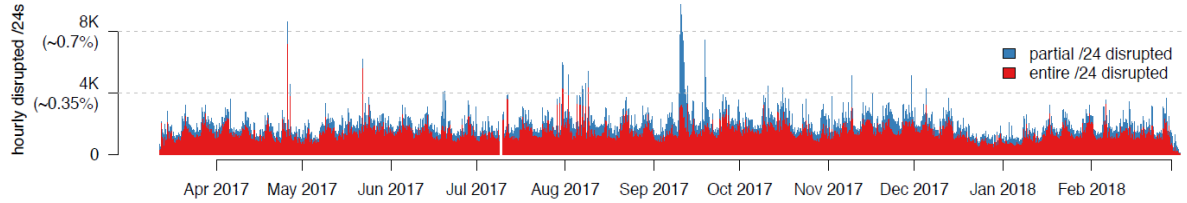


Figure 4: A boat.

Once the parameters are established, the authors applied the algorithm over the entire study period. Fig.4.a. shows the number of disrupted /24 address blocks in each hour from March 2017 to March 2018. The red bars in the figure show that for the duration the active addresses for the /24 block went down to 0 while blue indicates that some addresses were still active during the disruption.

We can observe from the figure that during September there was a huge disruption where more than 8k addresses went down. This coincides with the hurricane Irma. So the sudden spike is due to a natural disaster.

From the figure we can see somewhat uniform disruption pattern over the weeks. Fig.4.b. shows more clearly disruptions per day for an isolated week. We can see that the disruptions are higher during Tuesday, Wednesday and Thursday, which is typical server maintenance window. This becomes clearer when referring to fig.4.c. As shown in the figure the disruptions usually happen 1 A.M. and 3 A.M which is the maintenance time for most of the

servers. This emphasizes that most of the disruption events during the week can be credited to planned maintenances.

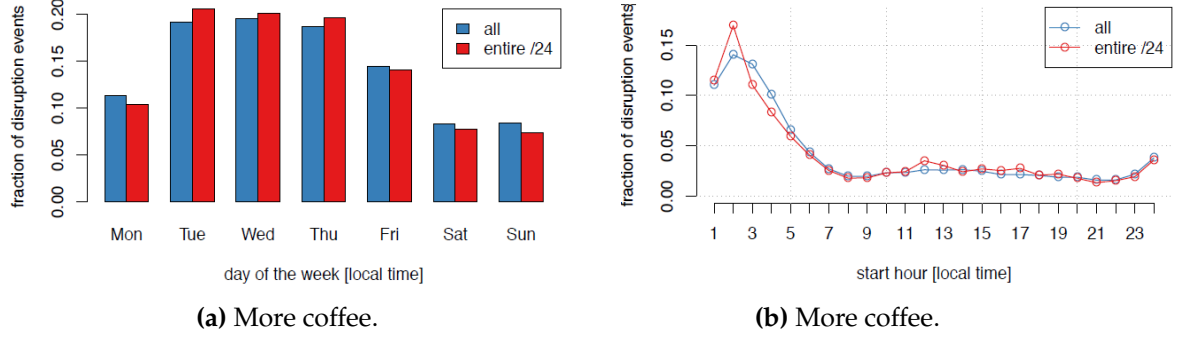


Figure 5: More coffee.

For further analysis of the disruption events and to actually understand whether or not these were actual service outages, the connectivity of individual devices to CDN during the disruptions can be analyzed. For this individual device activity before, during and after the disruptions had to be tracked. Tracking the activity of individual device was made possible by a software which clients can voluntarily install in their devices. The software supported both Windows and Mac OS X but could only run on desktops and laptops but not on smart phones.

This software makes repeated pings to CDN. Each software installation associates the device with a unique software ID and every time the device contacts the CDN, the time stamp along with this ID and the device IP at the time is logged. This log is different from the CDN log as this log only includes those devices that installed the software and contains an ID which identifies a unique device. Now, this log can be cross referenced with the CDN log to see whether the device was actually active or not during the disruption.

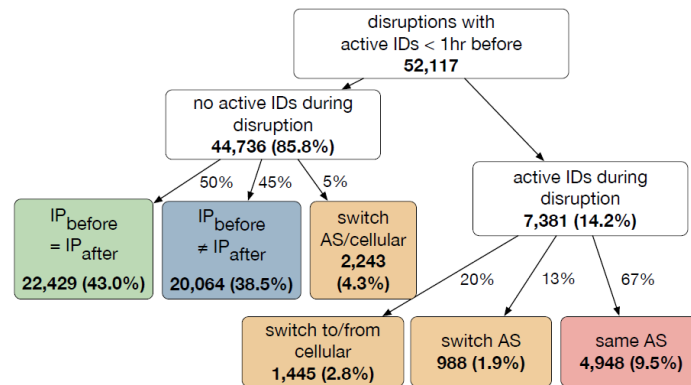


Figure 6: A boat.

For the purpose of this study, authors consider only those /24 address blocks which were entirely affected by disruption (active addresses went 0). These addresses can then be checked using the log obtained from devices to see if the device was active during the disruption in different address block. Fig 5 shows the result of these comparisons. In the figure, IP_{before}

means the IP of the device before the disruption, IPafter means the IP of the device after the disruption and IPduring means the IP of the address during the disruption.

About 14% of the devices showed activity even during the disruptions (in different address block). Authors assume that this could be attributed to various reasons like the user could have moved to some different location or connected their device to a different network. Another reason, they explain, could be that the IP address with which the user is connected was changed, thus causing sudden absence of activity in the initial address block and abrupt increase of activity in alternate address block in the same AS. This phenomenon is termed as "anti-disruption". These anti-disruptive events account for about 10% of the disruptions. After contacting several ISPs authors were able to confirm that majority of ISPs do indeed reassign prefixes and some do so more frequently. If one were to assume all disruptions are service outages then these anti-disruptive events can cause a network to seem to have bad reliability. Now, considering those devices that did not show activity during the disruption (about 86%), 43% of these devices had the same IP before and after the disruption. Authors believe that it is unlikely that the devices were assigned a new IP temporarily and again were reverted back to the original IP so this indicates an actual service outage. However, for the cases when the IP before the disruption is different that the IP after the disruption, there is an ambiguity about the cause as this could be due to actual outage, address reassignment or device movement.

4.2 Evaluation against Trinocular

The authors compared the disruptions detected by their algorithm against those detected by Trinocular, which is another disruption detection system. They used a three month (April 2017 – July 2017) ISI dataset [14] to implement Trinocular. They then evaluated the visibility of disruptions detected by their algorithm in Trinocular detected disruptions and vice versa.

For comparing the disruption detected by Trinocular with the CDN detected disruptions, only those disruptions in the Trinocular dataset that last more than an hour were filtered. About 29.9% of the disruptions in the Trinocular dataset lasted more than an hour. The authors found out that Trinocular detected significantly more disruptions than the disruptions detected from the CDN logs. Only about 27% of the disruptions detected by Trinocular agreed with the disruptions detected by the CDN logs. About 13% of the disruptions detected by Trinocular were reflected in terms of reduced CDN activity in the CDN logs but these were not below the threshold to be detected as disruptions. For about 60% of the disruptions in Trinocular, the CDN activity was normal, indicating that Trinocular was detecting more disruptions than actual occurrences.

To find the cause this discrepancy, the authors communicated with the authors of Trinocular and confirmed that Trinocular does detect false positives and it is a known issue with their methodology. Therefore, authors further narrowed down the data set by considering only address blocks with less than 5 disruptions decreasing the number of disruptions for comparison to 110K. After filtering 74% percent of the disruptions detected by Trinocular agreed with the CDN detected disruptions.

Next, authors compared the CDN detected disruptions with the Trinocular detected disruptions. For this only the disruptions in CDN that affected the whole /24 blocks were

considered since Trinocular detects disruptions in block-level. About 94% of the disruptions detected by Trinocular agreed with the CDN detected disruptions in this case. The authors then applied the same filter as before and found out that after filtering only 74% of the disruptions were agreeable. Thus, although filtering increased the visibility of Trinocular detected disruption in CDN detected disruptions by 47%, it also decreased the visibility of CDN detected disruption in Trinocular by 20%.

5 Discussion and conclusion

The authors, in their paper offer a passive approach in detecting internet outages and disruptions. Their detailed analysis of the results and experiments offer a clearer picture of probable causes and interpretation of disruptions. Their findings suggest that in majority of cases, the outages can be attributed to planned human activities. And disruption does not necessary mean loss of network connectivity or an outage but can be due to service providers re-assigning IP addresses.

The authors, while cross validating the device IDs and IP addresses obtained from the device activity log with the CDN logs found that that there were less than 0.01% devices which were seen to be active and have IP addresses during the disruption in the disrupted blocks. This is a very low error margin and implies that their algorithm is accurate enough. Using the device activity log, they also found out that about 10% of the disruptions were caused due to anti-disruption events. These anti-disruptions can potentially cause a network to seem to have less reliability.

Although the methodology and the findings are significant, it is not without its flaws. One of the flaws with their approach is that they use proprietary data which is not universally available. This severely imposes limits on anyone or any groups trying to extend or build on in their work. Another flaw is that the device ID log does not include smart phones whereas smart phones may have contributed heavily to the baseline activity in the CDN logs. So it seems that the results obtained from cross referencing these logs to confirm whether the devices were actually online during disruptions seems to be quite unreliable.

Future Work: From small business using the internet connectivity for growth [15] to large cities implementing ideas like IOT for better sustainability, efficiency and citizen welfare [16-17], the number of applications and services which need internet for functionality are growing. Internet is becoming a requirement rather than a luxury and thus proper understanding and interpretation of internet outages is important and will become more crucial in the coming days. Thus, there are bound to be more studies and research work in this area. However, since the devices and services that connect to internet are growing, they are also providing more data and this provides more opportunities to perform more detailed and accurate studies on outages.

References

- [1] R. Banerjee, A. Razaghpanah, L. Chiang, A. Mishra, V. Sekar, Y. Choi, and P. Gill: *Internet Outages, the Eyewitness Accounts: Analysis of the Outages Mailing List*. Passive and Active Measurement (PAM), Mar 2015, S. 206-219.

- [2] L. Quan, J. Heidemann, and Y. Pradkin: *Trinocular: Understanding Internet Reliability Through Adaptive Probing*. ACM SIGCOMM, Aug 2013, S. 255-266.
- [3] D. Turner, K. Levchenko, A. C. Snoeren, and S. Savage: *California Fault Lines: Understanding the Causes and Impact of Network Failures*. ACM SIGCOMM, 2010, S 315-326.
- [4] Broadband in the U.K.: data and research. <https://www.ofcom.org.uk/research-and-data/telecoms-research/broadband-research>
- [5] Broadband Measurement Project, Canada. <https://crtc.gc.ca/eng/internet/proj.htm>
- [6] Measuring Broadband America. <https://www.fcc.gov/general/measuring-broadband-america>
- [7] Measuring Broadband Australia. <https://www.accc.gov.au/consumers/internet-phone/monitoring-broadband-performance>
- [8] K. Benson, A. Dainotti, KC Claffy, E. Aben: *Gaining Insight into AS-level Outages through Analysis of Internet Background Radiation*. ACM SIGCOMM Conference on emerging Networking EXperiments and Technologies (CoNEXT) Student Workshop, Dec 2012, S. 63-64.
- [9] R. Pang, V. Yegneswaran, P. Barford, V. Paxson, and L. Peterson: *Characteristics of Internet Background Radiation*. Internet Measurement Conference (IMC 2004), Oct 2004, S. 27-40.
- [10] Internet Addresses Survey dataset. *PREDICT ID: USC-LANDER/internet-addresssurvey-reprobing-it76c-20170723/rev7956*. Traces taken 2017-07-23 to 2017-08-06. Provided by the USC/LANDER project. <http://www.isi.edu/ant/lander>
- [11] Internet Addresses Survey dataset. *PREDICT ID: USC-LANDER/internet-addresssurvey-reprobing-it76w-20170628/rev7942*. Traces taken 2017-06-28 to 2017-07-13. Provided by the USC/LANDER project. <http://www.isi.edu/ant/lander>
- [12] Internet Addresses Survey dataset. *PREDICT ID: USC-LANDER/internet-addresssurvey-reprobing-it77c-20170914/rev8018*. Traces taken 2017-09-14 to 2017-09-29. Provided by the USC/LANDER project. <http://www.isi.edu/ant/lander>
- [13] Internet Addresses Survey dataset. *PREDICT ID: USC-LANDER/internet-addresssurvey-reprobing-it77w-20170830/rev8013*. Traces taken 2017-08-30 to 2017-09-14. Provided by the USC/LANDER project. <http://www.isi.edu/ant/lander>
- [14] Internet Outage Dataset. *PREDICT ID: USC-LANDER/internet-outage-adaptivea28all-20170403*. Provided by the USC/LANDER project. <http://www.isi.edu/ant/lander>
- [15] B. M. Sadowski, C. F. Maitland, J. V. Dongen: *Strategic use of the Internet by small- and medium-sized companies: an exploratory study*. Information Economics and Policy, 14(1), Mar 2002, S. 75-93.
- [16] A.M Townsend: *Network Cities and the Global Structure of the Internet*. American Behavioral Scientist, 44(10), Jun 2001, S. 1697-1716.

- [17] S. Alawadhi, A. Aldama-Nalda, H. Chourabi, J. Ramon Gil-Garcia, S. L. Mellouli, T. Nam, T. A. Pardo, H. J. Scholl, S. Walker: *Building Understanding of Smart City Initiatives*. Electronic Government (EGOV), 7443, 2012. S. 40-53.
- [18] V. Rode: *Outages - outages (planned & unplanned) reporting*.
<https://puck.nether.net/mailman/listinfo/outages>