Pinpointing Delay and Forwarding Anomalies Using Large-Scale Traceroute Measurements

Romain Fontugne
IIJ Research Lab

Emile Aben
RIPE NCC

Cristel Pelsser
University of Strasbourg / CNRS

Randy Bush
IIJ Research Lab

ABSTRACT

Understanding data plane health is essential to improving Internet reliability and usability. For instance, detecting disruptions in distant networks can identify repairable connectivity problems. Currently this task is difficult and time consuming as operators have poor visibility beyond their network's border. In this paper we leverage the diversity of RIPE Atlas traceroute measurements to solve the classic problem of monitoring in-network delays and get credible delay change estimations to monitor network conditions in the wild. We demonstrate a set of complementary methods to detect network disruptions and report them in near real time. The first method detects delay changes for intermediate links in traceroutes. Second, a packet forwarding model predicts traffic paths and identifies faulty routers and links in cases of packet loss. In addition, we define an alarm score that aggregates changes into a single value per AS in order to easily monitor its sanity, reducing the effect of uninteresting alarms. Using only existing public data we monitor hundreds of thousands of link delays while adding no burden to the network. We present three cases demonstrating that the proposed methods detect real disruptions and provide valuable insights, as well as surprising findings, on the location and impact of the identified events.

ACM Reference Format:
Romain Fontugne, Emile Aben, Cristel Pelsser, and Randy Bush. 2017. Pinpointing Delay and Forwarding Anomalies Using Large-Scale Traceroute Measurements. In *Proceedings of IMC '17*. ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3131365.3131384

1 INTRODUCTION

The Internet's decentralized design allows disparate networks to cooperate and provides resilience to failure. However, significant network disruptions inevitably degrade users' connectivity. The first step to improve reliability is to understand the current health of the network. While network operators usually understand their own network's condition, understanding the state of the multi-provider Internet beyond their own network border remains a crucial but hard task. Monitoring multiple networks' health is difficult, and far too often requires many manual observations. For example, network operators' group mailing lists are a common way to signal and share knowledge about network disruptions [13]. Manual network measurements, such as ping and traceroute assist in diagnosing connectivity issues but they suffer from poor visibility.

We investigate the potential of existing data from a large-scale measurement platform, RIPE Atlas [7], to systematically detect and locate network disruptions. The widespread deployment of Atlas probes provides an extensive view of the Internet that has proved beneficial for postmortem reports [8, 9, 34]. Designing automated detection tools for such large-scale platforms is challenging. The high variability of network performance metrics, such as round trip time (RTT), is a key obstacle for reliable event detection [40]. Beyond detecting network disruptions, pinpointing their location is quite challenging due to traffic asymmetry and packet loss.

A key contribution of this paper is a method for estimating link delay changes on intermediate links in traceroute data. This method is robust to noisy RTTs and asymmetric paths. It infers very stable link delays and permits accurate predictions for anomaly detection. This is a significant contribution enabling us to leverage the numerous traceroute measurements continually generated by Atlas and monitor the health of the vast number of probed networks. As our method uses only pre-existing data, it adds no burden to the network. We also provide our tools [6] and report problems in near real time [4, 5] so that others can build upon our work.

In the rest of this paper, we examine the traffic asymmetry, RTT variability, and packet loss challenges faced when dealing with traceroute data (§ 3). Then, we devise a method to monitor RTT from traceroute results and report links with unusual delay changes (§ 4). This method takes advantage of the wide deployment of Atlas by monitoring links from numerous vantage points, accurately measuring delay changes. We also explore a packet forwarding model to learn and predict forwarding behavior and pinpoint faulty routers experiencing sudden packet loss (§ 5). Finally, we present a technique to aggregate these signals per network and detect interrelated events (§ 6). These methods are all based on nonparametric and robust statistics which cope with outliers commonly found in traceroute measurements. We found that measuring the accuracy of these methods is particularly hard because of the difficulty to obtain comprehensive ground truth data. In this paper we investigate three significant network events (§ 7), each demonstrating key benefits of our techniques. The first analyzes the impact of a DDoS infrastructure attack. The second shows congestion in a tier-1 ISP caused by inadvertent rerouting of significant traffic. And the last presents connectivity issues at an Internet Exchange due to a technical fault.

IMC '17, November 1–3, 2017, London, United Kingdom
© 2017 Association for Computing Machinery.
ACM ISBN 978-1-4503-5118-8/17/11…$15.00
https://doi.org/10.1145/3131365.3131384

2 DATASET

To monitor as many links in the meshy Internet as possible, we need a vast number of vantage points collecting network performance data. With its impressive spread across the globe and almost 10,000 probes constantly connected, RIPE Atlas is the best candidate. Atlas performs, among others, two classes of repetitive measurements providing an extensive collection of traceroute data publicly available in near real time. The first type, *builtin* measurements, consists of traceroutes from all Atlas probes to instances of the 13 DNS root servers every 30 minutes. Due to the wide distribution of probes and the anycast DNS root server deployment, this is actually to over 500 root server instances. The second type, *anchoring* measurements, are traceroutes to 189 collaborative servers (super probes) from about 400 normal probes every 15 minutes. All measurements employ Paris traceroute [12] to mitigate issues raised by load balancers and link aggregation [40]. Atlas sets the response timeout to 1 second for builtin measurements and 4 seconds for anchoring measurements. We filter out private IP addresses found in the traceroutes, consequently the proposed methods are not able to detect anomalies in private networks. The accuracy of the methods is however unaffected by this pre-process.

We have analyzed the builtin and anchoring measurements from May 1st to December 31st 2015, corresponding to a total of 2.8 billion IPv4 traceroutes (1.2 billion IPv6 traceroutes) from a total of 11,538 IPv4 probes (4,307 IPv6 probes) connected within the eight studied months.

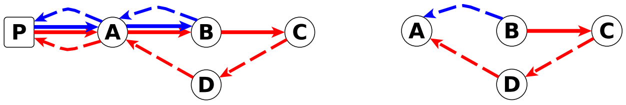
As our study relies solely on traceroute results the scope and terminology of this paper are constrained to the IP layer. That is, a link refers to a pair of IP addresses rather than a physical cable. Therefore, our methods suffer from common limitations faced by traceroute data [31, 32, 45]. Visibility is limited to the IP space, hence, changes at lower layers that are not visible at the IP layer can be misinterpreted. For example, the RIPE Atlas data report MPLS information if routers support RFC4950. But for routers not supporting RFC4950, the reconfiguration of an MPLS tunnel is not visible with traceroutes while being likely to impact observed delays. The RTT values reported by traceroute include both network delays and routers' slow path delay [31]. Therefore, the delay changes found using traceroute data are not to be taken as actual delay increases experienced by TCP/UDP traffic, though they are good for detecting network problems.

3 CHALLENGES AND RELATED WORK

Monitoring network performance with traceroute raises three key challenges. In this section, we present these challenges, discuss how they were tackled in previous work, and give hints of our approach to be discussed in detail in the next two sections.

3.1 Traffic asymmetry

Traceroutes are a rich source of information for monitoring Internet delay. They reveal the path to a destination and provide RTTs for every router on this path. Each RTT value is the sum of the time spent to reach a certain IP address and the travel time for the corresponding reply. Due to the asymmetry and diversity of routes [51, 60] the paths taken by the forwarding and returning packets often differ; also traceroute is unable to reveal IP addresses on the return path. Path asymmetry is very common; past studies report about 90% of AS-level routes as asymmetric [18, 47]. For these reasons one must take particular care when comparing RTT values for different hops.



(a) Round-trip to router B (blue) and C (red).

(b) Difference of the two round-trips (Δ_{PBC}).

Figure 1: Example of traceroute results with different return paths. P is the probe initiating the traceroute. A, B, and C are routers reported by traceroute. D is a router on the return path, unseen in the traceroute. Solid lines represent the forward paths, dashed the return paths.

For instance, quantifying the delay between two adjacent hops can be baffling. Figure 1 illustrates this by breaking down the RTT from the probe P to router B (blue in Fig. 1a) and the one to the following hop, router C (red in Fig. 1a). The solid lines represent the forward path exposed by traceroute, and the dotted the unrevealed return path. If we want to measure the delay between routers B and C using only the information provided by traceroute (i.e. solid lines in Fig. 1), one is tempted to compute the delay between B and C as the difference between the RTT to B and the one to C. But the resulting value is likely incorrect when forward and return paths are asymmetric. Packets returning from C are not going through B but D, a router not seen on the forward path. If one is monitoring the difference between the two RTTs over time and identifying an abnormality, then it is unclear if a change is due to abnormal delay on link *BC*, *CD*, *DA*, or *BA* (Fig. 1b).

Previous studies approach this using reverse traceroute techniques based on IP options to expose the return path [27, 35]. Using these techniques Luckie et al. [31] filter out routers with different forward and return paths and characterize congestion for the remaining routers. Due to the limitations of these reverse traceroute techniques [17] and the strong asymmetry of Internet traffic [18], they could study only 29.9% of the routers observed in their experiments.

Coordinated probing from both ends of the path is another way to reveal asymmetric paths and corresponding delays [15, 19]. However, coordinated probing requires synchronized control on hosts located at both ends of the path, which is difficult in practice and limits the probing surface.

Tulip [33] and cing [11] bypass the traffic asymmetry problem by measuring delays with ICMP options but require routers to implement these options.

In Section 4.1 we review the asymmetric paths problem and propose a new approach that takes advantage of multiple probes and path diversity to accurately monitor delay fluctuations for links visited from different vantage points.

3.2 RTT variability

As packets traverse multiple links, routers, queues, and middleboxes, they are exposed to multiple sources of delay that result in complex RTT dynamics. This phenomenon has been studied since the early days of the Internet and is still of interest, as comprehensive understanding of delay is a key step to understanding network conditions [21, 39, 43, 49]. Simply stated, monitoring delay is a delicate task because RTT samples are contaminated by various noise sources. In the literature, RTTs are monitored with different goals in mind. Minimum RTT values reveal propagation and transmission delays but filter out delays from transient congestion, so are commonly used to compute geographic distance in IP geolocation systems [26, 58]. Studies focusing on queuing delays usually rely on RTT percentiles [10, 36]; there is however no convention to choose specific quantiles. For instance, Chandrasekaran et al. [15] define the 10^{th} percentile as the *baseline* RTT and the 90^{th} percentile as *spikes* (i.e. sudden RTT increases), in the same study they also report results for the 5^{th} and 95^{th} percentiles.

We monitor the median RTT (i.e. 50^{th} percentile) which accounts for high delays only if they represent the majority of the RTT samples. Section 4.2 presents the other robust statistics we employ to analyze RTT measurements.

3.3 Packet loss

Delay is an important but insufficient indicator to identify connectivity issues. In worst-case scenarios networks fail to transmit packets, and the lack of samples clouds delay measurements. Increases in delay and packet loss are not necessarily correlated [36]. Congestion provides typical examples where both metrics are affected [50], but routers implementing active queue management (e.g. Random Early Detection [20]) can mitigate this [31], as the routers drop packets to avoid significant delay increase. Other examples include bursts of lost packets on routing failure [53]. We stress that a comprehensive analysis of network conditions must track both network delay and packet loss.

Packet loss is sometimes overlooked by congestion detection systems. For instance, Pong [19] and TSLP [31] probe routers to monitor queuing delays, but users are left with no guidance in the case of lost probes. Consequently, studies using these techniques tend to ignore incomplete data due to lost packets (e.g. 25% of the dataset is disregarded in ref. [15]), and potentially miss major events.

Detecting packet loss is of course an easy task; the key difficulty is to locate where the packets are dropped. Several approaches have been proposed to address this. The obvious technique is to continuously probe routers, or networks, and report packet loss or disconnections [33, 41]. This is, however, particularly greedy in terms of network resources, hence, difficult to deploy for long-term measurements. Another approach employs both passive and active monitoring techniques to build end-to-end reference paths, passively detect packet loss, and actively locate path changes [59]. Approaches using only passive measurements are also possible; although wide coverage requires collection of flow statistics from many routers [23].

In Section 5 we introduce a forwarding anomaly detection method that complements the proposed RTT analysis method (§ 4). It analyzes traceroute data and creates reference forwarding patterns for each router. These patterns are used to locate routers that drop packets in abnormal situations.

3.4 Qualitative comparison

As opposed to tulip [33], cing [11], Pong [19] and TSLP [31], the main benefits of our proposal are its compliance with current router functionalities, its robust statistical analysis and the recycling of existing data.

All techniques, including ours, require routers sending back ICMP packets for TTL-expired packets. In addition, TSLP requires routers to implement IP options (pre-specified timestamps or record route). Tulip and cing require routers to implement ICMP Timestamp and have strong assumptions for IP ID implementation.

In addition to these restrictions, some techniques have coverage limits. Pong can only monitor paths between probes, TSLP considers only inter-domain symmetric links adjacent to the probes' ASs, and our system is constrained to links monitored by probes from at least 3 different ASs.

Tulip and cing are also consuming significantly more network resources than other methods. These two methods rely on ICMP timestamps and require a large number of samples to correct routers' clocks artifacts. Consequently, the authors of tulip estimate delays on a path using 1000 measurements per router plus an extra 500 measurements per router for packet loss estimation [33]. In contrast, our system requires as little as nine packets per router and is designed to take advantage of existing traceroute data, thus really adding no extra load to the network.

Internet tomography algorithms [14, 16, 37] are also aimed at detecting and localizing network performance problems. The detection is based on specialized end-to-end measurements (e.g. one way delay or packet reordering) from a dedicated monitoring infrastructure [25, 42] and the localization is usually inferred using IP addresses found in traceroutes [57]. Consequently, network tomography may provide very detailed diagnoses but at the expense of a dedicated monitoring infrastructure and additional measurements.

4 IN-NETWORK DELAYS

We now describe our approach to detecting abnormal delay changes in wide-area traceroute measurements. To address the traffic asymmetry challenge we propose monitoring a link's delay using Atlas probes from multiple ASs (§ 4.1). We then use a robust detector to identify abnormal delay changes (§ 4.2).

4.1 Differential RTT

As stated in Section 3.1, locating delay changes from traceroute data is challenging because of traffic asymmetry. We address this challenge by taking advantage of the topographically-diverse deployment of Atlas probes.

Let's revisit the example of Figure 1 and introduce our notation. RTT_{PB} stands for the round-trip-time from the probe P to the router B. The difference between the RTT from P to the two adjacent routers, B and C, is called differential RTT and noted Δ_{PBC}. The

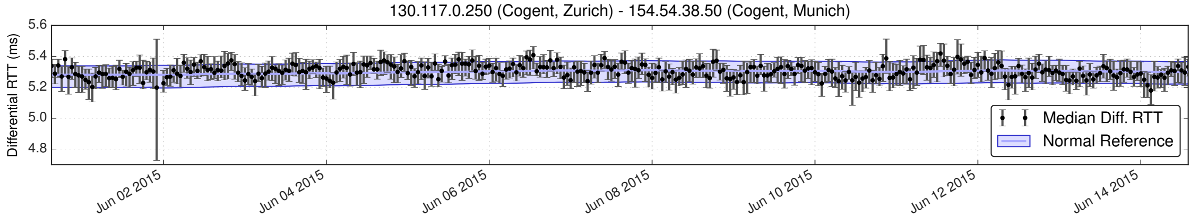


Figure 2: Example of median differential RTTs for a pair of IP addresses from Cogent Communications (AS174). Every median differential RTT is computed from a 1-hour time window, the error bars are the 95% confidence intervals obtained by the Wilson Score and the normal reference is derived from these intervals.

differential RTT of Figure 1b is decomposed as follows:

$$\begin{aligned}\Delta_{PBC} &= RTT_{PC} - RTT_{PB} &(1)\\ &= \delta_{BC} + \delta_{CD} + \delta_{DA} - \delta_{BA} &(2)\\ &= \delta_{BC} + \varepsilon_{PBC} &(3)\end{aligned}$$

where δ_{BC} is the delay for the link BC and ε_{PBC} is the time difference between the two return paths.

Δ_{PBC} alone gives a poor indication of the delay of link BC because the two components, δ_{BC} and ε_{PBC}, are not dissociable. Nonetheless, these two variables are independent and controlled by different factors. The value of δ_{BC} depends only on the states of routers B and C, and is unrelated to the monitoring probe P. In contrast, ε_{PBC} is intimately tied to P, the destination for the two return paths.

Assuming that we have a pool of n probes $P_i, i \in [1, n]$, all with different return paths from B and C; then, the differential RTTs for all probes, Δ_{P_iBC}, share the same δ_{BC} but have independent ε_{P_iBC} values. The independence of ε_{P_iBC} also means that the distribution of Δ_{P_iBC} is expected to be stable over time if δ_{BC} is constant. In contrast, significant changes in δ_{BC} influence all differential RTT values and the distribution of Δ_{P_iBC} shifts along with the δ_{BC} changes. Monitoring these shifts allows us to discard uncertainty from return paths (ε_{P_iBC}) and focus only on delay changes for the observed link (δ_{BC}).

Now let's assume the opposite scenario where B always pushes returning packets to A, the previous router on the forwarding path (see link AB in Fig. 1). In this case ε_P represents the delay between B and A; hence, Equation 3 simplifies as:

$$\Delta_{PAB} = \delta_{AB} + \delta_{BA}. \tag{4}$$

Meaning the differential RTT Δ_{PAB} stands for the delays between router A and B in both directions. This scenario is similar to the one handled by TSLP [31], and in the case of delay changes, determining which one of the two directions is affected requires extra measurements (see [31] Section 3.4).

In both scenarios, monitoring the distribution of differential RTTs detects delay changes between the adjacent routers. Note that we are looking exclusively at differential RTT fluctuations rather than their absolute values. The absolute values of differential RTTs can be misleading; as they include error from return paths, they cannot account for the actual link delay. In our experiments we observe negative differential RTTs, $\Delta_{PXY} < 0$, meaning that Y has a lower RTT than X due to traffic asymmetry (see Fig. 7c and 7d).

4.2 Delay change detection

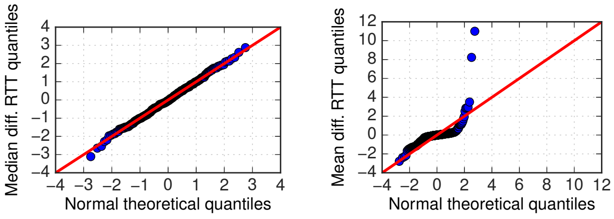
The theoretical observations of the previous section are the fundamental mechanisms of our delay change detection system. Namely, the system collects all traceroutes initiated in a 1-hour time bin and performs the following five steps:

(1) Compute the differential RTTs for each link (i.e. pair of adjacent IP addresses observed in traceroutes).
(2) Links that are observed from only a few ASs are discarded.
(3) The differential RTT distributions of the remaining links are characterized with nonparametric statistics,
(4) and compared to previously computed references in order to identify abnormal delay changes.
(5) The references are updated with the latest differential RTT values.

The same steps are repeated to analyze the subsequent time bins. The remainder of this section details steps for handling differential RTTs (i.e. steps 1, 3, 4, and 5). Step 2 is a filtering process to discard links with ambiguous differential RTTs and is discussed later in Section 4.3.

4.2.1 Differential RTT computation. The first step is calculating the difference between RTT values measured for adjacent routers. Let X and Y be two adjacent routers observed in a traceroute initiated by the probe P. The traceroute yields from one to three values for RTT_{PX} and RTT_{PY}. The differential RTT samples, Δ_{PXY} are computed for all possible combinations $RTT_{PY} - RTT_{PX}$; hence, we have from one to nine differential RTT samples per probe. In the following, all differential RTTs obtained with every probe are denoted Δ_{XY}, or Δ when confusion is not likely.

4.2.2 Differential RTTs characterization. This step characterizes the distributions of differential RTTs Δ_{XY} obtained in the previous step, in order to compute a normal reference and detect significant deviations from it. In practice, these anomalies are detected using a variant of the Central Limit Theorem (CLT). The original CLT states that, regardless the distribution of Δ_{XY}, its arithmetic mean is normally distributed if the number of samples is relatively large. If the underlying process changes, in our case the delays for X and Y, then the resulting mean values deviate from the normal distribution and are detected as anomalous.



(a) Median diff. RTT. **(b) Mean diff. RTT.**

Figure 3: Normality tests for the same data as Figure 2. Q-Q plots of the median and mean differential RTT versus a normal distribution.

Our preliminary experiments suggest that the frequent outlying values found in RTT measurements greatly affect the computed mean values; thus an impractical number of samples is required for the CLT to hold. To address this we replace the arithmetic mean by the median. This variant of the CLT is much more robust to outlying values and requires less samples to converge to the normal distribution [55]. Figure 2 depicts the hourly median differential RTTs (black dots) obtained for a link in Cogent networks (AS174) during two weeks in June 2015. This link is observed by 95 different probes between June 1st and June 15th. The raw differential RTT values exhibit large fluctuations; the standard deviation ($\sigma = 12.2$) is almost three times larger than the average value ($\mu = 4.8$). Despite this variability, the median differential RTT is remarkably steady, all values lie between 5.2 and 5.4 milliseconds (Fig. 2). Significant fluctuations of the median would strongly indicate delay changes on that link.

We confirm that the employed CLT variant holds very well with differential RTTs. Figure 3a compares the quantiles of the computed medians to those of a normal distribution. As all points are in line with the $x = y$ diagonal, the computed median differential RTTs fit a normal distribution quite well. In contrast, the mean differential RTT is not normally distributed (Fig. 3b). By manually inspecting the raw RTT values, we found 125 outlying values (i.e. greater than $\mu + 3\sigma$) that greatly alter the mean. These outliers are isolated events spread throughout the two weeks, and are attributed to measurement errors. Despite the large number of probing packets going through this link, the mean differential RTTs are greatly altered by these few outliers. These observations support our choice for the median CLT variant against the original CLT.

To account for uncertainty in the computed medians, we also calculate confidence intervals. In the case of the median, confidence intervals are usually formulated as a binomial calculation and are distribution free [22]. In this work we approximate this calculation with the Wilson score [56] since it has been reported to perform well even with a small number of samples [38]. The Wilson score is defined as follows:

$$w = \frac{1}{1 + \frac{1}{n}z^2}\left(p + \frac{1}{2n}z^2 \pm z\sqrt{\frac{1}{n}p(1-p) + \frac{1}{4n^2}z^2}\right) \qquad (5)$$

where n is the number of samples, the probability of success p is set to 0.5 in the case of the median, and z is set to 1.96 for a 95% confidence level. The Wilson score provides two values, hereafter called w_l and w_u, ranging in $[0, 1]$. Multiplying w_l and w_u by the number of samples gives the rank of the lower and upper bound of the confidence interval, namely $l = nw_l$ and $u = nw_u$.

For example, let $\Delta^{(1)}, ..., \Delta^{(n)}$ be the n differential RTT values obtained for a single link, and assume these values are ordered, i.e. $\Delta^{(1)} \leq \Delta^{(2)} \leq ... \leq \Delta^{(n)}$. Then, for these measures the lower and upper bound of the confidence interval are given by $\Delta^{(l)}$ and $\Delta^{(u)}$.

Based solely on order statistics, the Wilson score produces asymmetric confidence intervals in the case of skewed distributions, which are common for RTT distributions [21]. Further, unlike a simple confidence interval based on the standard deviation, this non-parametric technique takes advantage of order statistics to discard undesirable outliers.

The whiskers in Figure 2 depict the confidence intervals obtained for the Cogent link discussed above. These intervals are consistent over time and show that the median differential RTT for this link reliably falls between 5.2 and 5.4 milliseconds. The large confidence interval reported on June 1*st* illustrates an example where RTT measures are noisier than other days; yet we stress that the median value and confidence interval are compatible with those obtained by other time bins. The following section describes how we identify statistically deviating differential RTTs.

4.2.3 Anomalous delays detection. A delay change results in a differential RTT distribution shift; therefore a significant change in the corresponding median differential RTT value. Assume we have a reference median and its corresponding 95% confidence interval that represents the usual delay measured for a certain link (as calculated in § 4.2.4). To measure if the difference between an observed median and the reference is statistically significant we examine the overlap between their confidence intervals. If the two confidence intervals are not overlapping, we conclude that there is a statistically significant difference between the two medians [46] so we report the observed median as anomalous. As a rule of thumb we discard anomalies where the difference between the two medians is lower than 1ms (in our experiments these account for 3% of the reported links). Although statistically meaningful, these small anomalies are less relevant for the study of network disruption.

The deviation from the normal reference is given by the gap between the two confidence intervals. Let $\bar{\Delta}^{(l)}$ and $\bar{\Delta}^{(u)}$ be, respectively, the lower and upper bound of the reference confidence interval and $\bar{\Delta}^{(m)}$ the reference median. Then, the deviation from the normal reference of the observed differential RTTs, Δ, is defined as:

$$d(\Delta) = \begin{cases} \dfrac{\Delta^{(l)} - \bar{\Delta}^{(u)}}{\bar{\Delta}^{(u)} - \bar{\Delta}^{(m)}}, & \text{if } \bar{\Delta}^{(u)} < \Delta^{(l)} \\ \dfrac{\bar{\Delta}^{(l)} - \Delta^{(u)}}{\bar{\Delta}^{(m)} - \bar{\Delta}^{(l)}}, & \text{if } \bar{\Delta}^{(l)} > \Delta^{(u)} \\ 0, & \text{otherwise.} \end{cases} \qquad (6)$$

This deviation represents the gap separating the two confidence intervals and is relative to the usual uncertainty measured by the reference confidence interval. Values close to zero represent small delay changes while large values represent important changes.

Figure 2 exhibits confidence intervals along with the corresponding normal reference. As the reference intersects with all confidence intervals, no anomaly is reported for this link. The evaluation section presents several examples of anomalies. For example, Figure 7c depicts two confidence intervals deviating from the normal reference on November 30th.

4.2.4 Normal reference computation. In the previous section we assumed a reference differential RTT distribution for each link. We will now show how to compute this. The goal of the references is to characterize the usual delays of observed links. As median differential RTT values are normally distributed (§ 4.2.2), the expected median value for a link is simply obtained as the arithmetic mean of previously observed medians for that link. Because anomalies might impair mean values and make them irrelevant as references, we employ exponential smoothing to estimate the medians' mean value to reduce the impact of anomalies. Exponential smoothing also facilitates the online implementation of our delay change method for near real time analysis [4, 6]. Let $m_t = \Delta^{(m)}$ be the median differential RTT observed for a certain link in time bin t, and, $\bar{m}_{t-1} = \bar{\Delta}^{(m)}$ be the reference median computed with median differential RTTs observed in the previous time bin, $t - 1$. Then the next reference median, $\bar{m}_t$ is defined as:

$$\bar{m}_t = \alpha m_t + (1 - \alpha)\bar{m}_{t-1} \tag{7}$$

The only parameter for the exponential smoothing, $\alpha \in (0, 1)$, controls the importance of new measures as opposed to the previously observed ones. In our case a small α value is preferable as it lets us mitigate the impact of anomalous values. The initial value of the reference, $\bar{m}_0$, is quite important when α is small. We arbitrarily set this value using the first three time bins, namely, $\bar{m}_0 = \text{median}(m_1, m_2, m_3)$.

For the reference confidence interval, the lower and upper bounds (resp. $\bar{\Delta}^{(l)}$ and $\bar{\Delta}^{(u)}$) are computed in the same way as the reference median ($\bar{\Delta}^{(m)}$) but using the boundary values given by the Wilson score (i.e. $\Delta^{(l)}$ and $\Delta^{(u)}$).

4.3 Probe diversity

The above differential RTT analysis applies only under certain conditions. Section 4.1 shows that monitoring Δ_{XY} reveals delay changes between router X and Y only if the following hold true. (1) The link is monitored by several probes and the return paths to these probes are disparate. (2) All returning packets are also going through the link XY but in the opposite direction. Therefore, if we have differential RTT values Δ_{XY} from ten probes which share the same asymmetric return path, we cannot distinguish delay changes on XY from delay changes in the return path, so these differential RTT values cannot be used.

To filter out ambiguous differential RTTs we avoid links monitored only by probes from the same AS (thus more likely to share the same return path due to common inter-domain routing policies); but instead, take advantage of the wide deployment of Atlas probes and focus on links monitored from a variety of ASs. We devise two criteria to control the diversity of probes monitoring a link.

The first criterion filters out links that are monitored by probes from less than 3 different ASs. The value 3 is empirically set to provide conservative results and can be lowered to increase the number of monitored links but at the cost of result accuracy. To determine this value we make the following hypothesis. Links where the error added by return paths is not mitigated by probe diversity are reported more frequently as their differential RTTs also account for links on the return path. For links visited by probes from at least 3 different ASs we observe a weak positive correlation (0.24) between the average number of reported alarms and the number of probes monitoring a link. Meaning that links observed by a small number of diverse probes are not reported more than those monitored by a large number of probes, thus a small diversity of return paths is enough to mitigate the error added by return paths.

This simple criterion allows us to avoid ambiguous results when links are monitored from only a few ASs, but is insufficient to control probe diversity. For instance, a link XY is monitored by 100 probes located in 5 different ASs but 90 of these probes are in the same AS. Then, the corresponding differential RTT distribution is governed by the return path shared by these 90 probes, meaning that delay changes on this return path are indistinguishable from delay changes on XY.

The second criterion finds links with an unbalanced number of probes per AS. Measuring such information dispersion is commonly addressed using normalized entropy. Let $A = \{a_i | i \in [1, n]\}$ be the number of probes for each of the n ASs monitoring a certain link, then the entropy $H(A)$ is defined as:

$$H(A) = -\frac{1}{\ln n} \sum_{i=1}^{n} P(a_i) \ln P(a_i). \tag{8}$$

Low entropy values, $H(A) \simeq 0$, mean that most of the probes are concentrated in one AS, and, high entropy values, $H(A) \simeq 1$, indicate that probes are evenly dispersed among ASs. This second criterion ensures that analyzed links feature an entropy $H(A) > 0.5$.

If the second criterion is not met (i.e. $H(A) \leq 0.5$) the link is not discarded. Instead, a probe from the most represented AS (namely AS i such as $a_i = \max(A)$) is randomly selected and discarded, thus increasing the value of $H(A)$. This process is repeated until $H(A) > 0.5$, hence the corresponding differential RTTs are relevant for our analysis.

4.4 Theoretical limitations

The sensitivity of our approach in detecting abnormal delay changes depends mainly on the size of the time bin which in turn is based on probes deployment and probing rate. A link is monitored only if it is traversed from vantage points within at least three different ASs (Section 4.3). As traceroute sends three packets per hop, for a link we expect at least $m = 3 * 3$ packets per time bin. Consequently, the number of vantage points monitoring a link and their probing rate r (i.e. number of traceroutes per hour) determine the minimum usable time bin $T_{min} = \frac{m}{3rn}$. Intuitively experiments with many probes or a high probing rate would permit the use of short time bin.

Let $T \geq T_{min}$ be the selected time bin, then $3rnT$ is the expected number of packets obtained for a link per time bin. Because our approach relies on the median, 50% of these packets should be impacted by an event to be detected. In other words, an event is detected if it affects more than $1 + \frac{3rnT}{2}$ packets within a time bin.

Consequently, the smallest detectable event in hour is:

$$\frac{1}{3rn}(1 + \frac{3rnT}{2}) = \frac{1}{3rn} + \frac{T}{2}. \tag{9}$$

In Section 7 we analyze builtin measurements which initiate traceroute every 30 minutes ($r = 2$ traceroutes per hour) thus the minimum usable time bin is $T_{min} = 0.5$ hour. In our experiments we conservatively set the time bin $T = 1$ hour, hence, according to Equation 9, the shortest event we can detect for a link monitored by three vantage points ($n = 3$) is 33 minutes. Because of the higher probing rate of anchoring measurements ($r = 4$), one could detect events lasting only nine minutes with this dataset.

Low frequency traceroute measurements originally designed for topology discovery are not suitable for our approach. For example, the *IPv4 Routed /24 Topology Dataset* from CAIDA [3] has a 48 hour cycle which is not appropriate to monitor transient delay changes.

5 FORWARDING ANOMALIES

Latency is a good indicator of network health, but deficient in certain cases. For example, if traffic is rerouted or probing packets are lost then the lack of RTT samples impedes delay analysis. We refer to these cases as forwarding anomalies. In this section we introduce a method to detect forwarding anomalies, complementing the delay analysis method presented in Section 4.

A forwarding anomaly can be legitimate, for example rerouted traffic, but it can also highlight compelling events such as link failures or routers dropping packets. Using traceroute data, such events appear as router hops vanishing from our dataset. So our approach monitors where packets are forwarded and constructs a simple packet forwarding model (§ 5.1). This model allows us to predict next hop IP addresses in traceroutes, thus detecting and identifying disappearing routers (§ 5.2).

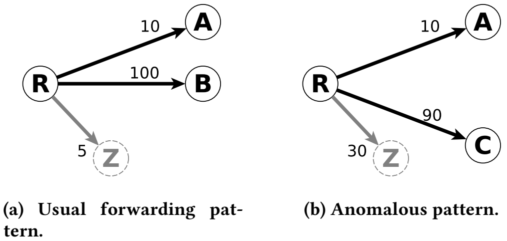
5.1 Packet forwarding model

The proposed packet forwarding model learns the next hops usually observed after each router from past traceroute data. Because routers determine next hops based on the packet destination IP address, we compute a different model for each traceroute target.

Let us consider traceroutes from all probes to a single destination in the same time bin. For each router in these traceroutes we record the adjacent nodes to which packets have been forwarded. We distinguish two types of next hop, responsive and unresponsive ones. The responsive next hops are visible in traceroutes as they send back ICMP messages when a packet TTL expires. Next hops that do not send back ICMP packets to the probes or drop packets are said to be unresponsive and are indissociable in traceroutes.

Figure 4a illustrates the example of a router R with two responsive hops, A and B, and unresponsive hop, Z. The packet forwarding pattern of this router is formally defined as a vector where each element represents a next hop and the value of the element is the number of packets transmitted to that hop. For Figure 4a the forwarding pattern of R is $F^R = [10, 100, 5]$.

To summarize router R's usual patterns and to update this reference with new patterns, we again employ exponential smoothing. Let $F^R_t = \{p_i | i \in [1, n]\}$ be the forwarding pattern for router R at time t and $\bar{F}^R_{t-1} = \{\bar{p}_i | i \in [1, n]\}$ be the reference computed at time $t - 1$. These two vectors are sorted such as p_i and $\bar{p}_i$ correspond to the same next hop i. If the hop i is unseen at time t then $p_i = 0$, similarly, if the hop i is observed for the first time at time t then $\bar{p}_i = 0$. The reference $\bar{F}^R_{t-1}$ is updated with the new pattern F^R_t as follows:



(a) Usual forwarding pattern.

(b) Anomalous pattern.

Figure 4: Two forwarding patterns for router R. A, B, and C are next hops identified in traceroutes. Z shows packet loss and next hops that are unresponsive to traceroute.

$$\bar{F}^R_t = \alpha F^R_t + (1 - \alpha)\bar{F}^R_{t-1}. \tag{10}$$

As in Section 4.2.4, a small α value allows us to mitigate the impact of anomalous values. The reference $\bar{F}^R_t$ represents the usual forwarding pattern for router R and is the normal reference used for the anomaly detection method discussed in the next section. A reference $\bar{F}^R_t$ is valid only for a certain destination IP address. In practice we compute a different reference for each traceroute target; thus, several references are maintained for a single router.

5.2 Forwarding anomaly detection

5.2.1 Correlation analysis. Detecting anomalous forwarding patterns consists of identifying patterns F that deviate from the computed normal reference $\bar{F}$. In normal conditions we expect a router to forward packets as they did in past observations. In other words, we expect F and $\bar{F}$ to be linearly correlated. This linear dependence is easily measurable as the Pearson product-moment correlation coefficient of F and $\bar{F}$, hereafter denoted as $\rho_{F,\bar{F}}$. The values of $\rho_{F,\bar{F}}$ range in $[-1, 1]$. Positive values mean that the forwarding patterns expressed by F and $\bar{F}$ are compatible, while negative values indicate opposite patterns hence forwarding anomalies. Therefore, all patterns F with a correlation coefficient $\rho_{F,\bar{F}} < \tau$ are reported as anomalous. In our experiments we arbitrarily set $\tau = -0.25$, as the empirical distribution of $\rho_{F,\bar{F}}$ features a knee around that value. Conservative results can be obtained with lower τ values, but higher values are best avoided as $\rho > -0.25$ represents very weak anti-correlation.

5.2.2 Anomalous next hop identification. When a forwarding pattern F is reported as anomalous, it means that the proportions of packets sent to next hops are different from those observed in the past. Further, an anomalous pattern can be caused by just a few aberrant next hops. We devise a metric to identify hops that are responsible for forwarding pattern changes. Let $F = \{p_i | i \in [1, n]\}$ be an anomalous pattern and $\bar{F} = \{\bar{p}_i | i \in [1, n]\}$ the computed normal reference. Then we quantify the responsibility of the next hop i to the pattern change as:

$$r_i = -\rho_{F,\bar{F}} \frac{p_i - \bar{p}_i}{\sum_{j=1}^{n} |p_j - \bar{p}_j|}. \quad (11)$$

The responsibility r_i ranges in $[-1, 1]$. Values close to 0 mean that the next hop i received a usual number of packets thus it is likely not responsible for the pattern change. On the other hand, values deviating from 0 indicate anomalous next hops. Positive values stand for hops that are newly observed, and negative values represent hops with an unusually low number of packets.

For example, assume Figure 4a depicts $\bar{F}^R$, the computed normal reference for router R, and Figure 4b illustrates F^R, the latest forwarding pattern observed. The correlation coefficient for these patterns, $\rho_{F^R,\bar{F}^R} = -0.6$, is lower than the threshold τ, thus F^R is reported as anomalous. The responsibility scores for A, B, C, and Z are, respectively, $0, -0.28, 0.25$, and 0.07; suggesting that packets are ordinarily transmitted to A and Z, but, the number of packets to B is abnormally low while the count to C is exceptionally high. In other words traffic usually forwarded to B is now going through C. In the case of a next hop dropping a significant number of packets, the responsibility score of this hop will be negative while the score of Z will be large.

6 DETECTION OF MAJOR EVENTS

The proposed delay analysis method (§ 4) and packet forwarding model (§ 5) are both designed to report anomalies found in large-scale traceroute measurements. With RIPE Atlas these methods allow us to monitor hundreds of thousands links and potentially obtain a large number of alarms (i.e. either delay changes or forwarding anomalies). Investigating each alarm can be very tedious and time consuming. In this section we introduce a simple technique to aggregate alarms and report only significant network disruptions.

6.1 Alarm aggregation

Major network disruptions are characterized by either a large-scale alteration of numerous links or exceptional connectivity issues at a one or more locations. We wish to emphasize both by aggregating alarms based on their temporal and spatial characteristics. The temporal grouping of alarms allows us to highlight large-scale events impacting many routers at the same time. Similarly, collecting alarms that are topologically close allows us to emphasize network disruptions bound to a particular entity. In early experiments we have tried several spatial aggregations, including geographical ones, and found that grouping alarms per AS is relevant because most significant events are contained within one or a few ASs.

Consequently, we group delay change alarms by the reported IP pair and forwarding anomalies by the next hops' IP addresses. The IP to AS mapping is done using longest prefix match, and alarms with IP addresses from different ASs are assigned to multiple groups.

Alarms from each AS are then processed to compute two time series representing the severity of reported anomalies, thus the AS's condition. The severity of anomalies is measured differently for delay change and packet forwarding alarms. For delay changes the severity is measured by the deviation from the normal reference, $d(\Delta)$ (Equation 6). Severity of forwarding anomalies is given by r_i, the responsibility score of the reported next hop i (Equation 11). Thereby, AS network conditions are represented by two time series, one is the sum of $d(\Delta)$ over time and the other the sum of r_i over time. In the case of forwarding anomalies, r_i values are negative if a hop from the AS is devalued and positive otherwise. Consequently, if traffic usually goes through a router i but is suddenly rerouted to router j, and both i and j are assigned to the same AS, then the negative r_i and positive r_j values cancel out, thus the anomaly was mitigated at the AS level.

6.2 Event detection

Finding major network disruptions in an AS is done by identifying peaks in either of the two time series described above. We implement a simple outlier detection mechanism to identify these peaks.

Let $X = \{x_t | t \in \mathbb{N}\}$ be a time series representing delay changes or forwarding anomalies for a certain AS and $mag(X)$ be the magnitude of the AS network alteration defined as:

$$mag(X) = \frac{X - \text{median}(X)}{1 + 1.4826\,\text{MAD}(X)} \quad (12)$$

where median and MAD are the one-week sliding median and median absolute deviation [55]. The scale factor 1.4826 is used to estimate the standard deviation of X from MAD(X). The magnitude scores allow us to rank events, so an operator can prioritize its investigations. In the following sections we report large magnitude scores found with our dataset and investigate corresponding network disruptions.

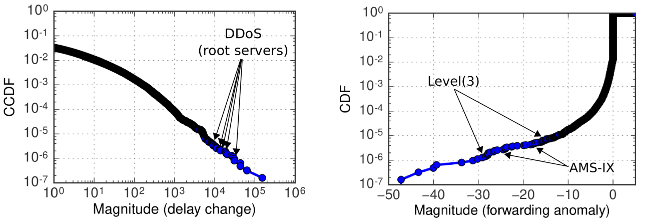
7 RESULTS

Using the Internet-wide traceroutes from RIPE Atlas (§ 2), we report delay changes and forwarding anomalies from eight months in 2015 and 1060 ASs. In the following we present aggregate results of the identified delay changes and forwarding anomalies. Then, we dive into case studies showing the relevance of the proposed methods to detect and locate network disruptions of different types (§ 7.1, 7.2, and 7.3).

Delay changes. In our experiments we monitored delays for 262k IPv4 links (42k IPv6 links). On average links are observed by 147 IPv4 probes (133 IPv6 probes) and 33% of the links were reported to have at least one abnormal delay change.

We computed the hourly delay change magnitude for each monitored ASs, Figure 5a depicts the distribution of all these values. 97% of the time we observe a magnitude lower than 1, meaning that ASs are usually free of large transient delay changes. The heavy tail of the distribution, however, indicates that delay changes can have a very detrimental impact on Internet delays. We manually inspected the most prominent delay changes but found that validating such results is particularly hard as public reports are rarely available and Internet service providers are reluctant to disclose troubles that occurred in their networks. In Section 7.1, we detail a DDoS attack that generated congestion in several ASs and accounts for 5 of the top 23 delay changes reported in our dataset (Fig. 5a).

Furthermore, in accordance with the central limit theorem, we observe a narrower confidence interval for links visited by numerous probes; hence a better differential RTT estimation and the ability to detect smaller delay changes.



(a) Complementary cumulative distribution function for the delay change magnitude. Prominent changes are on the right hand side.

(b) Cumulative distribution function of the forwarding anomaly magnitude. Prominent anomalies are on the left hand side.

Figure 5: Distribution of hourly magnitude for all ASs. Arrows point to prominent anomalies presented in the three study cases.

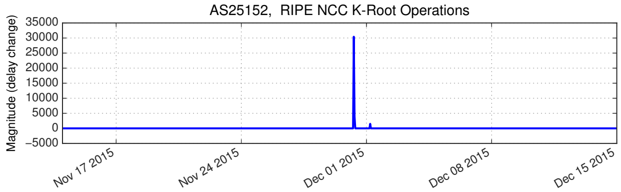


Figure 6: Delay change magnitude for AS25152 reveals the two DDoS against the K-root server.

Forwarding anomalies. Using RIPE Atlas traceroutes, we also computed packet forwarding models for 170k IPv4 router IPs (87k IPv6 router IPs). These are the number of router IP addresses found in traceroutes; to resolve these to routers IP alias resolution techniques should be deployed [29]. On average forwarding models contain four different next hops over the eight months of data.

We computed the hourly forwarding anomaly magnitude for each AS, Figure 5b illustrates the distribution of these values. This distribution features a heavy left tail representing a few significant forwarding anomalies due to important packet loss or traffic redirection. Namely, forwarding anomaly magnitude is lower than −10 for only 0.001% of the time. Similarly to the delay changes, validating these results is challenging. In Section 7.2 and 7.3 we investigate two significant events from the top 20 forwarding anomalies found in our dataset (Fig. 5b). These events are already publicly documented but the proposed method provides further insights on their location and impact.

7.1 DDoS attack on DNS root servers

Our first case-study shows the impact of a large distributed denial-of-service (DDoS) attack on network infrastructure. The simplest form of DDoS attack consists of sending a huge number of requests to a targeted service, overwhelming the service and leaving little or no resources for legitimate use. The extremely large amount of traffic generated by this type of attack is not only detrimental to the victim but also routers in its proximity.

We investigate network disruptions caused by two DDoS attacks against DNS root servers. These attacks have been briefly documented by root server operators [44, 54]. The first attack was on November 30th from 06:50 to 09:30 UTC, the second on December 1st from 05:10 until 06:10 UTC. As the source IP addresses for both attacks were spoofed, it is unclear from reports [54] where the traffic originated.

Thanks to the K-root operators, we were able to carefully validate our results for the attack toward the K name server and the corresponding AS (AS25152).

Event detection. Monitoring the delay change magnitude for AS25152 clearly shows the two attacks against the K-root infrastructure (Fig. 6). The two peaks on November 30th and December 1st highlight important disruptions of an unprecedented level. The first peak spans from 07:00 to 09:00 UTC and the second from 05:00 to 06:00 UTC, which correspond to the intervals reported by many server operators.

The highest forwarding anomaly magnitude for AS25152 is recorded on November 30th at 08:00 and is negative ($mag(X) = -0.5$), meaning that only a few packets have been dropped in ASs hosting root servers. These observations match the server operators' reports and emphasize the strength of anycast in mitigating such attacks.

In-depth analysis: K-root. A key advantage of our method is reporting delay changes per link, allowing us to precisely locate the effects of the two attacks in the network. Reported delay changes contain one IP address for each end of the link. Delay changes detected on the last hop to the K-root server are identified by the server IP address (193.0.14.129) and the router in front of it. Since K-root is anycast, the actual location of a reported server instance must be revealed by locating the adjacent router. For example, Figure 7a depicts the differential RTT for an IP pair composed of the K-root IP address and a router located in Kansas City; hence this link represents the last hop to the K-root instance in Kansas City.

During the two attacks we saw alarms from 23 unique IP pairs containing the K-root server address. Different instances were impacted differently by the attacks. First, we found instances affected by both attacks, for example the one in Kansas City (Fig. 7a) is reported during the entire period of time documented by server operators. Second, we also observed instances impacted by only one attack, see Figure 7c. The most reported instance during that period is the one deployed in St. Petersburg (Fig. 7d). For this instance abnormal delays are observed for 14 consecutive hours. A possible explanation for this is that hosts topologically close to this instance caused anomalous network conditions for a longer period of time than other reported DDoS intervals. Finally, thanks to anycast, for some instances we did not record anomalous network conditions. Figure 7b illustrates the differential RTT for an instance in Poland that exhibits very stable delays. The corresponding normal reference is exceptionally narrow and constant even during the attacks.

Not only are the last hops to K-root instances detected by our method; we also observe other links with important delay changes.

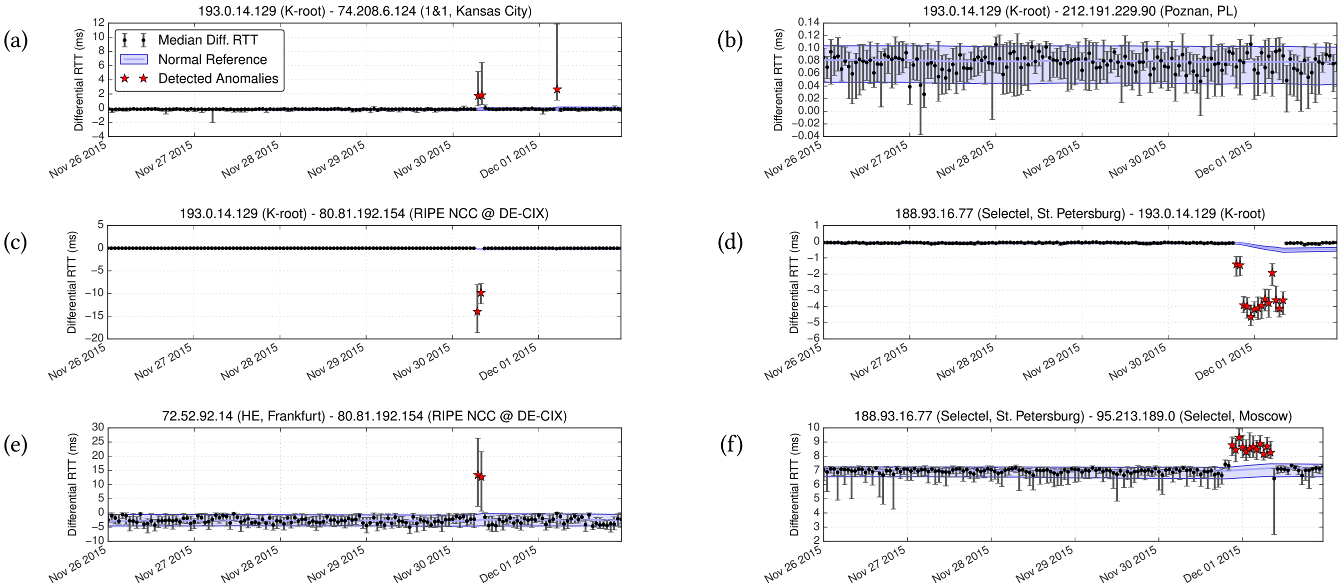


Figure 7: Examples of delay change alarms reported during the DDoS attacks against DNS root servers. The attacks have differently impacted the connectivity of K-root server instances.

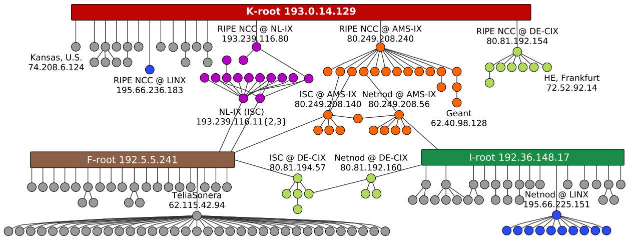


Figure 8: Alarms reported on November 30th at 08:00 UTC and related to the K-root server. Each node represent an IPv4 address, edges stand for reported alarms. Rectangular nodes represent anycast addresses, hence distributed infrastructure. Circular node colors represent IP addresses related to certain IXPs.

Figure 7e depicts a link in the Deutscher Commercial Internet Exchange (DE-CIX) which is upstream of the K-root instance in Frankfurt (Fig. 7c). This link between Hurricane-Electric (AS6939) and the K-root AS exhibits a 15ms delay change (difference between the median differential RTT and the reference median) during the first attack. The upstream link of the instance in St.Petersburg (Fig. 7f) is also significantly altered during the attack and is consistent with the peculiar changes observed for this instance (Fig. 7d). In certain cases, we observed effects of the attack even further upstream. For example, we observe 7.5ms delay change on a link in the Geant network three hops away from the K-root server (see *Geant 62.40.98.128* in Fig. 8).

To assess the extent of the attacks on the network, we create a graph, where nodes are IP addresses and links are alarms generated from differential RTTs between these IP addresses. Starting from the K-root server, we see alarms with common IP addresses, and obtain a connected component of all alarms connected to the K-root server. Figure 8 depicts the connected component involving K-root for delay changes detected on November 30th at 08:00 UTC. An anycast address is illustrated by a large rectangular node, because it represents several physical systems. Figure 8 does not show the physical topology of the network but a logical IP view of reported alarms. Each edge to an anycast address usually represents a different instance of a root server. There are rare cases where two edges may represent the same instance, for example, the K-root instance available at AMS-IX and NL-IX is actually the same physical cluster. Some of the alarms mentioned above and illustrated in Figure 7a, 7c, and 7e are also displayed in Figure 8. The shape of the graph reveals the wide impact of the attack on network infrastructure. It also shows that alarms reported for the K-root servers are adjacent to the ones reported for the F and I-root servers. This is due to the presence of all three servers at the same exchange points; hence some network devices are affected by malicious traffic targeting multiple root servers. The concentration of root servers is of course delicate in this situation. Although packet loss at root servers has been negligible, we found significant forwarding anomalies at their upstream providers. For example, AMS-IX (AS1200) shows a forwarding anomaly magnitude of −24 during that incident.

Additional root servers are represented by different connected components. During the three hours of attack there were 129 alarms involving root servers for IPv4 (49 for IPv6). In agreement with

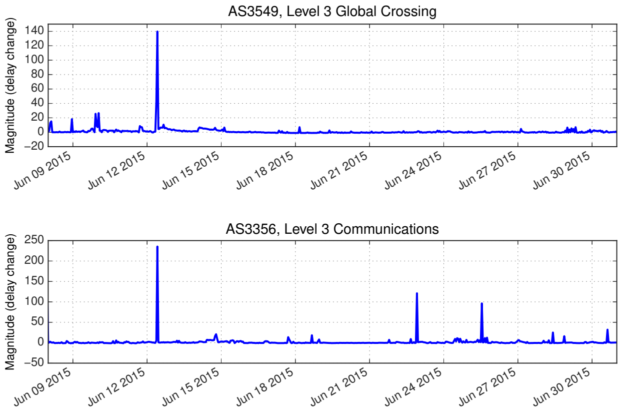


Figure 9: Delay change magnitude for all monitored IP addresses in two Level(3) ASs.

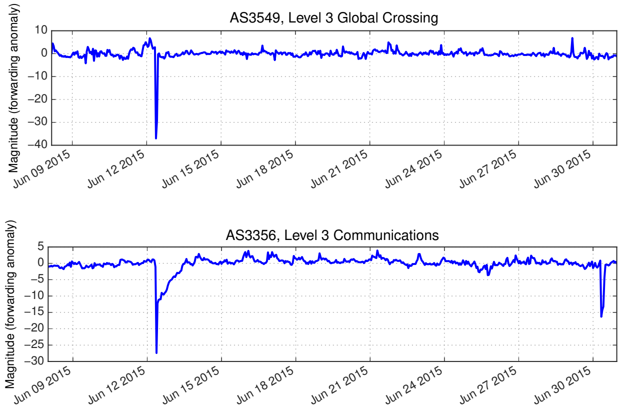


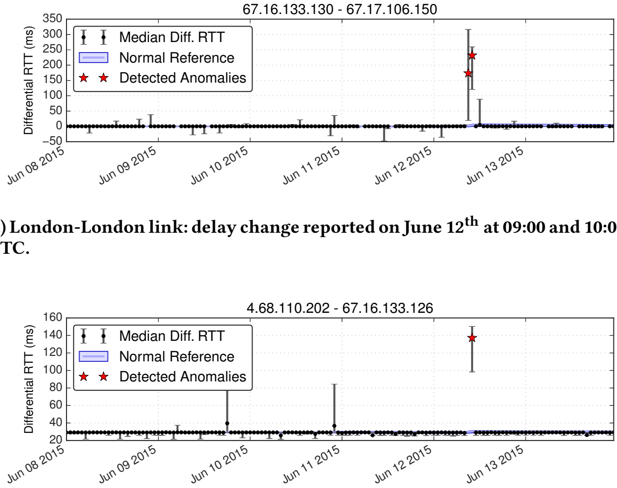
Figure 10: Forwarding anomaly magnitude for all monitored IP addresses in two Level(3)ASs.

the observations made by servers operators [54], we observed no significant delay change for root servers A, D, G, L, and M.

7.2 Telekom Malaysia BGP route leak

The above example of the K-root servers illustrates the benefits of our delay change detection method in detecting anomalies near a small AS at the edge. In this section we investigate network disruptions for a tier 1 ISP showing that the methods also enable us to monitor large ASs containing numerous links. This case study also exposes a different type of network disruption; here the detected anomalies are caused by abnormal traffic rerouting.

On June 12th 2015, 08:43 UTC, Telekom Malaysia (AS4788) unintentionally sent BGP announcements for numerous IP prefixes to its provider Level(3) Global Crossing (AS3549) which accepted them. The resulting traffic attraction to Telekom Malaysia caused latency increases for Internet users all over the globe. The event was acknowledged by Telekom Malaysia [2], and independently reported by BGP monitoring projects [28, 52]. Connectivity issues have been mainly attributed to congested peering links between Telekom Malaysia and Level(3) Global Crossing. In the remainder of this section we investigate the impact of rerouted traffic on Level(3) Global Crossing (AS3549) and its parent company, Level(3) Communications (AS3356), showing worldwide disruption.



(a) London-London link: delay change reported on June 12th at 09:00 and 10:00 UTC.

(b) New York-London link: delay change reported at 10:00 UTC. RTT samples for June 12th at 09:00 UTC are missing due to forwarding anomaly (packet loss).

Figure 11: Example of delay change alarms reported during the Telekom Malaysia BGP route leak for two links from Level3 networks.

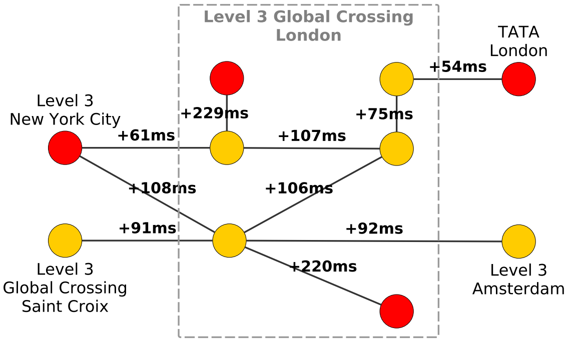


Figure 12: Congestion at Level(3) Global Crossing (AS3549) in London on June 12th 2015. Each node represents an IPv4 address, edges represent delay changes for an IP pair. Red nodes depict IP addresses involved in forwarding anomalies.

Network disruptions in Level(3). Monitoring delay changes and forwarding anomalies for the numerous links that constitute the two Level(3) ASs is made easy with the magnitude metric. Figure 9 and 10 depict the magnitude in terms of, respectively, delay change and forwarding anomaly for the two Level(3) ASs in June 2015. The two positive peaks in Fig. 9 and the two negative peaks in Fig. 10 are all reported on June 12th from 09:00 to 11:00 UTC, exposing the impact of rerouting on both ASs. The overall delay increased for both ASs, but AS3549 was most affected. The negative forwarding anomaly magnitudes (Fig. 10) show that routers from both ASs were disappearing abnormally from the forwarding model obtained by traceroute. At the same time packet loss increased, implying that numerous routers from both ASs dropped a lot of packets. These are the most significant forwarding anomalies monitored for Level(3) in our 8-month dataset.

In-depth analysis. Reverse DNS lookups of reported IP addresses suggests congestion was seen in numerous cities, including, Amsterdam, Berlin, Dublin, Frankfurt, London, Los Angeles, Miami, New York, Paris, Vienna, and Washington, for both Level(3) ASs. Figure 11 shows the differential RTT obtained for two links located in New York and London. Both links exhibit significant delay increases synchronous with the Telekom Malaysia route leak. The London-London link (Fig. 11a) is reported from 09:00 to 11:00 UTC, while the New York-London link (Fig. 11b) is reported from 10:00 to 11:00 UTC. The IP address identified in New York is found in forwarding anomalies, and is suspected of dropping probing packets from 09:00 to 10:00 UTC; hence preventing the collection of RTT samples for this link. This example illustrates the complementarity of the delay change and forwarding anomaly detection methods.

As in the case of the K-root servers, several adjacent links are reported at the same time. Figure 12 shows related components of alarms reported on June 12th at 10:00 UTC in London. The label on each edge is the absolute difference between the observed median differential RTT and the median of the normal reference. The links in Fig. 11a and 11b are marked by delay changes of, respectively, *+229ms* and *+108ms*. Similar observations are made for the two Level(3) ASs and numerous cities mainly in U.S. and Europe. Consequently, even non-rerouted traffic going through Level(3) at that time could also incur significant latency increase and packet loss.

7.3 Amsterdam Internet Exchange Outage

The first two study cases presented network disruptions with significant delay changes. Here we introduce an example of network disruption visible only through forwarding anomalies; showing the need for both delay change and forwarding anomaly detection methods. In this example the disruption is caused by a technical fault in an Internet exchange resulting in extensive connectivity issues.

On May 13th 2015 around 10:20 UTC, the Amsterdam Internet Exchange (AMS-IX) encountered substantial connectivity problems due to a technical issue during maintenance activities. Consequently, several connected networks could not exchange traffic through the AMS-IX platform; hence a number of Internet services were unavailable [1]. AMS-IX reported that the problem was solved at 10:30 UTC; but traffic statistics indicate that the level of transmitted traffic did not return to normal until 12:00 UTC [9, 30].

Event detection. The delay change method did not conclusively detect this outage, due to lack of RTT samples during the outage. Indeed, the packet loss rate showed significant disturbances at AMS-IX. These changes were captured by our packet forwarding model as a sudden disappearance of the AMS-IX peering LAN for many neighboring routers. Consequently, forwarding anomalies with negative responsibility scores (Equation 11) were synchronously reported for IP addresses in the AMS-IX peering LAN. Monitoring the magnitude for the corresponding AS (Fig. 13) reveals these changes as a significant negative peak on May 13th 11:00 UTC. Further, the coincidental surge of unresponsive hops reported by forwarding anomalies supports the fact that traffic was not rerouted but dropped. The packet forwarding model allows us to precisely determine peers that could not exchange traffic during the outage. In total 770 IP pairs related to the AMS-IX peering LAN became unresponsive. Therefore, the proposed method to learn packet forwarding patterns and systematically identify unresponsive IP addresses greatly eases the understanding of such an outage.

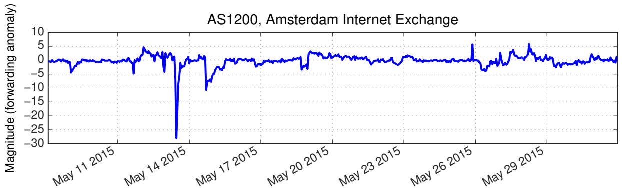


Figure 13: Forwarding anomaly magnitude for the Amsterdam Internet Exchange peering LAN (AS1200).

8 INTERNET HEALTH REPORT

The key contribution of our method is to allow operators to troubleshoot connectivity issues outside their own network, normally a very difficult task. Typical circumstances include distant users of other ISPs complaining that an ISP's web service is unavailable, or local customers complaining to their ISP about connectivity issues, though their ISP's network is not the cause of the issues. In these cases being able to pinpoint the exact location of the problem allows operators to contact the appropriate NOC, or to consider routing decisions to avoid unreliable networks.

In order to provide a practical tool to network operators, we have integrated the proposed methods with the RIPE Atlas streaming API. This gives us near-real time traceroutes for all long-lived Atlas measurements (including built-in and anchoring measurements) and enables us to detect events in a timely manner. Our results are publicly available through an interactive website [4] and an API [5] (along with results from the outage detector Disco [48]) such that researchers and operators can access computed results in an easy and systematic way. Of course, an operator can take our code and run it against the Atlas streaming API themselves, focusing on only the part(s) of the topology which interests them [6]. Thanks to an increasing number of Atlas measurements and probes, the number of monitored ASs is constantly increasing. As of May 2017, we were monitoring a total of 5,465 ASs, a significant fraction of the 7,800 transit ASs in the Internet [24].

We encourage operators interested in using our system to deploy Atlas anchors in their network so that probes will automatically initiate traceroutes towards their network, and visited transit links will be monitored by our system. The results enable operators to easily monitor the diverse transit networks between their infrastructure and the thousands of Atlas probes deployed world-wide.

Providing this service also assists us in understanding the deployment and runtime overhead of our methods in practice. The

Atlas measurement platform provides us with around 500k traceroutes hourly, which are fed to two applications; one implementing the method detecting delay changes and the other implementing the method detecting forwarding anomalies. Each application is multi-threaded (one main thread and 12 workers) and consumes around 12GB of RAM memory. To analyze and report results for an hour of data the applications take less than ten minutes on a 1U server with two Intel(R) Xeon(R) CPU E5-2670 v3 @ 2.30GHz. Meaning that the low complexity of our methods permits to cope with the abundant flow of data produced by the Atlas platform using only commodity hardware.

9 CONCLUSIONS

In this paper we investigated the challenges to monitoring network conditions using traceroute results. We then tackled these challenges with a statistical approach that took advantage of large-scale traceroute measurements to accurately pinpoint delay changes and forwarding anomalies. Because of the lack of ground truth data we were not able to fully quantify the accuracy of our system, but our experiments with the RIPE Atlas platform emphasized the benefits of our approach to characterize topological impacts.

The methods proposed in this paper complement the literature by circumventing common problems found in past work. With the help of the packet forwarding model, we take advantage of all collected traceroutes including even those that are incomplete due to packet loss. Also, as we do not rely on any IP or ICMP options, the number of monitored routers is superior to previous work. In fact, our statistical approach allows us to study any link with routers responding to traceroute and that can be seen by probes hosted in at least three different ASs. Therefore, the number of monitored links mainly depends on the placement of probes and the selected traceroute destinations. In other words, using our techniques the number of monitored links is given by the measurement setup rather than the router's implementation. Stub ASs hosting probes but no traceroute targets were not monitored as they were observed only by probes from the same AS. In the case of symmetric links we could release the probe diversity constraint. However, due to the current lack of efficient technique to assert an arbitrary link symmetry we leave this task for future work .

We make our tools and results publicly available [4–6] in order to share our findings and contribute to a better understanding of Internet reliability.

ACKNOWLEDGMENTS

We thank Kenjiro Cho, Kensuke Fukuda, Johan Mazel and Anant Shah for their valuable comments on an earlier version of the paper. Many thanks also to Massimo Candela for his help with the RIPE Atlas streaming API and data visualisation tools. We are also grateful to the IMC reviewers and our shepherd, Partha Kanuparthy, for their suggestions to improve the quality of the paper.

REFERENCES

[1] 2015. Follow-up on previous incident at AMS-IX platform. https://ams-ix.net/newsitems/195. (May 2015).

[2] 2015. Telekom Malaysia: Internet services disruption. https://www.tm.com.my/OnlineHelp/Announcement/Pages/internet-services-disruption-12-June-2015.aspx. (June 2015).

[3] 2017. CAIDA, The IPv4 Routed /24 Topology Dataset. https://www.caida.org/data/active/ipv4_routed_24_topology_dataset.xml. (2017).

[4] 2017. Internet Health Report. http://ihr.iijlab.net. (2017).

[5] 2017. Internet Health Report API. http://ihr.iijlab.net/ihr/api/. (2017).

[6] 2017. Internet Health Report source code. https://github.com/romain-fontugne/tartiflette. (2017).

[7] 2017. RIPE NCC, Atlas. https://atlas.ripe.net. (2017).

[8] Emile Aben. 2013. Hurricane Sandy as seen by RIPE Atlas. *NANOG 57* (February 2013).

[9] Emile Aben. 2015. Does the Internet Route Around Damage? A Case Study Using RIPE Atlas. https://labs.ripe.net/Members/emileaben/does-the-internet-route-around-damage. (November 2015).

[10] Jay Aikat, Jasleen Kaur, F Donelson Smith, and Kevin Jeffay. 2003. Variability in TCP round-trip times. In *Proceedings of IMC'03*. ACM, 279–284.

[11] Kostas G Anagnostakis, Michael Greenwald, and Raphael S Ryger. 2003. cing: Measuring network-internal delays using only existing infrastructure. In *INFOCOM 2003*, Vol. 3. IEEE, 2112–2121.

[12] Brice Augustin, Xavier Cuvellier, Benjamin Orgogozo, Fabien Viger, Timur Friedman, Matthieu Latapy, Clémence Magnien, and Renata Teixeira. 2006. Avoiding traceroute anomalies with Paris traceroute. In *IMC*. ACM, 153–158.

[13] Ritwik Banerjee, Abbas Razaghpanah, Luis Chiang, Akassh Mishra, Vyas Sekar, Yejin Choi, and Phillipa Gill. 2015. Internet Outages, the Eyewitness Accounts: Analysis of the Outages Mailing List. In *Passive and Active Measurement*. Springer, 206–219.

[14] Tian Bu, Nick Duffield, Francesco Lo Presti, and Don Towsley. 2002. Network tomography on general topologies. In *ACM SIGMETRICS Performance Evaluation Review*, Vol. 30. ACM, 21–30.

[15] Balakrishnan Chandrasekaran, Georgios Smaragdakis, Arthur Berger, Matthew Luckie, and Keung-Chi Ng. 2015. A Server-to-Server View of the Internet. In *CoNEXT*. ACM.

[16] Mark Coates, Alfred Hero, Robert Nowak, and Bin Yu. 2002. Internet tomography. *IEEE Signal processing magazine* 19, 3 (2002), 47–65.

[17] Walter de Donato, Pietro Marchetta, and Antonio Pescapé. 2012. A hands-on look at active probing using the IP prespecified timestamp option. In *Passive and Active Measurement*. Springer, 189–199.

[18] Wouter de Vries, José Jair Santanna, Anna Sperotto, and Aiko Pras. 2015. How asymmetric is the Internet? A study to support the use of traceroute. In *Intelligent mechanisms for network configuration and security (LNCS)*, Vol. 9122. Springer, 113–125.

[19] Leiwen Deng and Aleksandar Kuzmanovic. 2008. Monitoring persistently congested Internet links. In *Network Protocols, 2008. ICNP 2008. IEEE International Conference on*. IEEE, 167–176.

[20] Sally Floyd and Van Jacobson. 1993. Random early detection gateways for congestion avoidance. *Networking, IEEE/ACM Transactions on* 1, 4 (1993), 397–413.

[21] Romain Fontugne, Johan Mazel, and Kensuke Fukuda. 2015. An empirical mixture model for large-scale RTT measurements. In *INFOCOM'15*. IEEE, 2470–2478.

[22] Jean Dickinson Gibbons and Subhabrata Chakraborti. 2011. Nonparametric statistical inference. (2011).

[23] Yu Gu, Lee Breslau, Nick Duffield, and Subhabrata Sen. 2009. On passive one-way loss measurements using sampled flow statistics. In *INFOCOM 2009, IEEE*. IEEE, 2946–2950.

[24] Geoff Huston. 2017. BGP in 2016. https://labs.ripe.net/Members/gih/bgp-in-2016. (2017).

[25] Partha Kanuparthy, Danny H Lee, Warren Matthews, Constantine Dovrolis, and Sajjad Zarifzadeh. 2013. Pythia: Detection, Localization, and Diagnosis of Performance Problems. *IEEE Communications Magazine* (2013), 56.

[26] Ethan Katz-Bassett, John P John, Arvind Krishnamurthy, David Wetherall, Thomas Anderson, and Yatin Chawathe. 2006. Towards IP geolocation using delay and topology measurements. In *Proceedings of IMC'06*. ACM, 71–84.

[27] Ethan Katz-Bassett, Harsha V Madhyastha, Vijay Kumar Adhikari, Colin Scott, Justine Sherry, Peter Van Wesep, Thomas E Anderson, and Arvind Krishnamurthy. 2010. Reverse traceroute.. In *NSDI*, Vol. 10. 219–234.

[28] Nick Kephart. 2015. Route Leak Causes Global Outage in Level 3 Network. https://blog.thousandeyes.com/route-leak-causes-global-outage-level-3-network/. (June 2015).

[29] Ken Keys, Young Hyun, Matthew Luckie, and Kim Claffy. 2013. Internet-scale IPv4 alias resolution with MIDAR. *IEEE/ACM Transactions on Networking (TON)* 21, 2 (2013), 383–399.

[30] Robert Kisteleki. 2015. The AMS-IX Outage as Seen with RIPE Atlas. https://labs.ripe.net/Members/kistel/the-ams-ix-outage-as-seen-with-ripe-atlas. (May 2015).

[31] Matthew Luckie, Amogh Dhamdhere, David Clark, Bradley Huffaker, and kc claffy. 2014. Challenges in Inferring Internet Interdomain Congestion. In *IMC*. ACM, 15–22.

[32] Matthew Luckie, Young Hyun, and Bradley Huffaker. 2008. Traceroute probe method and forward IP path inference. In *IMC*. ACM, 311–324.

[33] Ratul Mahajan, Neil Spring, David Wetherall, and Thomas Anderson. 2003. User-level Internet path diagnosis. *SOSP'03* 37, 5 (2003), 106–119.

[34] Vesna Manojlovic. 2016. Using RIPE Atlas and RIPEstat to detect network outage events. *SANOG 27* (January 2016).

[35] Pietro Marchetta, Alessio Botta, Ethan Katz-Bassett, and Antonio Pescapé. 2014. Dissecting round trip time on the slow path with a single packet. In *PAM*. Springer, 88–97.

[36] Athina Markopoulou, Fouad Tobagi, and Mansour Karam. 2006. Loss and delay measurements of internet backbones. *Computer Communications* 29, 10 (2006), 1590–1604.

[37] Abia Moloisane, Ivan Ganchev, and Máirtín OâĂŹDroma. 2014. *Internet Tomography: An Introduction to Concepts, Techniques, Tools and Applications.* Cambridge Scholars Publishing.

[38] Robert G Newcombe. 1998. Two-sided confidence intervals for the single proportion: comparison of seven methods. *Statistics in medicine* 17, 8 (1998), 857–872.

[39] Ramakrishna Padmanabhan, Patrick Owen, Aaron Schulman, and Neil Spring. 2015. Timeouts: Beware Surprisingly High Delay. In *Proceedings of the 2015 Internet Measurement Conference (IMC '15)*. ACM, New York, NY, USA, 303–316. https://doi.org/10.1145/2815675.2815704

[40] Cristel Pelsser, Luca Cittadini, Stefano Vissicchio, and Randy Bush. 2013. From Paris to Tokyo: on the suitability of ping to measure latency. In *Proceedings of IMC'13*. ACM, 427–432.

[41] Lin Quan, John Heidemann, and Yuri Pradkin. 2013. Trinocular: Understanding Internet Reliability Through Adaptive Probing. In *Proceedings of the ACM SIGCOMM Conference*. ACM, Hong Kong, China, 255–266.

[42] Michael Rabbat, Robert Nowak, and Mark Coates. 2004. Multiple source, multiple destination network tomography. In *INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies*, Vol. 3. IEEE, 1628–1639.

[43] L. Rizo-Dominguez, D. Munoz-Rodriguez, C. Vargas-Rosales, D. Torres-Roman, and J. Ramirez-Pacheco. 2014. RTT Prediction in Heavy Tailed Networks. *IEEE Communications Letters* 18, 4 (April 2014), 700–703. https://doi.org/10.1109/LCOMM.2014.013114.132668

[44] Root Server Operators. 2015. Events of 2015-11-30. http://www.root-servers.org/news/events-of-20151130.txt. (December 2015).

[45] Matthew Roughan, Walter Willinger, Olaf Maennel, Debbie Perouli, and Randy Bush. 2011. 10 lessons from 10 years of measuring and modeling the internet's autonomous systems. *Selected Areas in Communications, IEEE Journal on* 29, 9 (2011), 1810–1821.

[46] Nathaniel Schenker and Jane F Gentleman. 2001. On judging the significance of differences by examining the overlap between confidence intervals. *The American Statistician* 55, 3 (2001), 182–186.

[47] Yaron Schwartz, Yuval Shavitt, and Udi Weinsberg. 2010. On the diversity, stability and symmetry of end-to-end Internet routes. In *INFOCOM IEEE Conference on Computer Communications Workshops, 2010*. IEEE, 1–6.

[48] A. Shah, R. Fontugne, E. Aben, C. Pelsser, and R. Bush. 2017. Disco: Fast, good, and cheap outage detection. In *2017 Network Traffic Measurement and Analysis Conference (TMA)*. 1–9. https://doi.org/10.23919/TMA.2017.8002902

[49] Ankit Singla, Balakrishnan Chandrasekaran, P Godfrey, and Bruce Maggs. 2014. The internet at the speed of light. In *Proceedings of the 13th ACM Workshop on Hot Topics in Networks*. ACM, 1.

[50] Joel Sommers, Paul Barford, Nick Duffield, and Amos Ron. 2005. Improving accuracy in end-to-end packet loss measurement. *ACM SIGCOMM Computer Communication Review* 35, 4 (2005), 157–168.

[51] Renata Teixeira, Keith Marzullo, Stefan Savage, and Geoffrey M Voelker. 2003. In search of path diversity in ISP networks. In *Proceedings of the 3rd ACM SIGCOMM conference on Internet measurement*. ACM, 313–318.

[52] Andree Toonk. 2015. Massive route leak causes Internet slowdown. http://www.bgpmon.net/massive-route-leak-cause-internet-slowdown/. (June 2015).

[53] Feng Wang, Zhuoqing Morley Mao, Jia Wang, Lixin Gao, and Randy Bush. 2006. A measurement study on the impact of routing events on end-to-end internet path performance. *ACM SIGCOMM Computer Communication Review* 36, 4 (2006), 375–386.

[54] Matt Weinberg and Duane Wessels. 2016. Review and analysis of attack traffic against A-root and J-root on November 30 and December 1, 2015. *OARC 24* (April 2016).

[55] Rand R Wilcox. 2010. *Fundamentals of Modern Statistical Methods: Substantially Improving Power and Accuracy.* Springer Science & Business Media.

[56] Edwin B Wilson. 1927. Probable inference, the law of succession, and statistical inference. *J. Amer. Statist. Assoc.* 22, 158 (1927), 209–212.

[57] Sajjad Zarifzadeh, Madhwaraj Gowdagere, and Constantine Dovrolis. 2012. Range tomography: combining the practicality of boolean tomography with the resolution of analog tomography. In *Proceedings of the 2012 ACM conference on Internet measurement conference*. ACM, 385–398.

[58] Bo Zhang, T.S.E. Ng, A. Nandi, Rudolf H. Riedi, P. Druschel, and Guohui Wang. 2010. Measurement-Based Analysis, Modeling, and Synthesis of the Internet Delay Space. *IEEE/ACM Transactions on Networking* 18, 1 (Feb 2010), 229–242. https://doi.org/10.1109/TNET.2009.2024083

[59] Ming Zhang, Chi Zhang, Vivek S Pai, Larry L Peterson, and Randolph Y Wang. 2004. PlanetSeer: Internet Path Failure Monitoring and Characterization in Wide-Area Services.. In *OSDI*, Vol. 4. 12–12.

[60] Han Zheng, Eng Keong Lua, Marcelo Pias, and Timothy G Griffin. 2005. Internet routing policies and round-trip-times. In *Passive and Active Network Measurement*. Springer, 236–250.