Computer Networks xxx (2014) xxx–xxx

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Assessing the service quality of an Internet path through end-to-end measurement

Atef Abdelkefi, Yuming Jiang *, Bjarne Emil Helvik, Gergely Biczók, Alexandru Calu

Department of Telematics, Norwegian University of Science and Technology (NTNU), Norway

ARTICLE INFO

Article history:
Received 14 November 2012
Received in revised form 9 March 2014
Accepted 25 April 2014
Available online xxxx

Keywords:
Service quality assessment
End-to-end measurement
Internet path

ABSTRACT

Understanding the service quality of Internet paths is of great importance for both the service provider and the user. *Motivated by this and particularly the aim of extracting such information from a given dataset collected through end-to-end measurement*, this paper presents a novel approach, called SCI (Service-quality Characterization of Internet-path). Specifically, SCI utilizes delay and loss measurements collected from vantage points at the two ends of an Internet path. It transforms collected probes into performance signals, namely aggregate delay, average delay and aggregate loss signals. On the aggregate delay and average delay signals, abrupt changes are detected using Principal Component Pursuit (PCP). The detected abrupt changes in aggregate delay and average delay, together with the loss information, are further mapped as different types of events causing degradations and failures in the service within the path. Predicated on the set of identified such service-level events, SCI characterizes the service quality of the measured Internet path using three metrics, namely *availability*, *stability* and *fatigue*. The proposed approach has been systematically evaluated on the dataset collected from a real operational environment. The results show that SCI achieves good accuracy in detecting abrupt changes in aggregate delay and average delay and identifying service-level events, boosting the feasibility of service quality assessment of an Internet path based exclusively on end-to-end measurement.

1. Introduction

The Internet has become the mainstay platform for various networked services including content distribution, VoIP, IPTV and cloud computing. Given the popularity and the increasing reliance on these services, service failures and service quality degradations become ever costly in terms of reputation and revenue for service providers as well as for consumers. Thus, maintaining high *service quality* in the Internet has become increasingly important. However, the Internet is a packet-switched, best-effort service based network. Unlike circuit-switched networks where on each path, dedicated resources are reserved end-to-end to guarantee service quality, there is no dedicated (virtual) circuit in the Internet for *network level "direct link"* between two end systems, which is called a *virtual path* or simply *path* throughout this paper as termed in [32]. Because of this, the service quality of an Internet path highly depends on the underlying networking mechanisms, such as routing, buffer management and scheduling, plus the traffic condition on each hop along the path making service quality assessment highly challenging.

In this paper, we characterize service quality by the duration and frequency of service failures and degradations of the considered Internet path. Service failures

* Corresponding author. Address: Department of Telematics, Norwegian University of Science and Technology (NTNU), N-7491 Trondheim, Norway. Tel.: +47 73 59 27 24; fax: +47 73 59 69 73.

E-mail addresses: abdelkefi.atef@gmail.com (A. Abdelkefi), jiang@item.ntnu.no (Y. Jiang), bjarne@item.ntnu.no (B.E. Helvik), gbiczok@item.ntnu.no (G. Biczók), calu@ntnu.no (A. Calu).

http://dx.doi.org/10.1016/j.comnet.2014.04.016
1389-1286/

may be generated by failures in network elements, such as router errors, fiber cuts or routing anomalies; while service quality degradations can be caused by congestion, queues building up or re-routing. There is an emerging need for service providers as well as for their customers to understand and quantify the service quality of Internet paths. Not surprisingly, a great deal of academic and commercial work has been conducted on this issue from end-user [16,27], ISP [40] and backbone network [25] angles. Subsequently, these efforts have revealed various ambiguities and resulted in a better overall understanding of Internet behavior. However, quantifying the service quality of an Internet path is still a poorly understood problem.

A large body of related work has focused on detecting and flagging events, and characterizing failures in network elements, e.g., [37,9,41], and distinguishing unwanted behaviors caused by malicious activities, e.g., [36,7]. However, sophisticated measurement infrastructures are usually required; this limits wide adoption of the proposed approaches due to inadequate scalability, low effectiveness and/or high cost and complexity of deployment. In addition, there remains a class of events, e.g., congestion, re-routing, etc., which accounts for a large fraction of service degradation; still its impact is poorly quantifiable. Finally, the critical need to maintain the highest service quality over the Internet with the lowest possible cost, has transformed the customers' requirements towards a stronger obligation for service providers to meet their service level agreements (SLA). For these reasons, the objective of this paper is to propose a simple approach, based on which, the service quality of an Internet path can be assessed quantifiably. The work was particularly motivated by the aim of extracting service quality information about several Internet paths from a given dataset collected from a real operational environment through end-to-end measurement on these paths.

Specifically, a novel approach, called ***S**ervice-quality **C**haracterization of **I**nternet-path* (SCI), is proposed. For an Internet path, SCI only relies on delay and loss measurements collected from vantage points at the two ends of the path. Based on the end-to-end delay and loss measurements, performance signals are first constructed, namely *aggregate delay*, *average delay* and *aggregate loss* signals. Using Principal Component Pursuit (PCP) [12], abrupt changes on aggregate delay and average delay time series are first detected. They, together with loss information, are then mapped to service-level events causing service quality degradations. After that, predicated on the set of identified service-level events, SCI quantifies the service quality of the Internet path using three metrics, namely *availability*, *fatigue*, and *stability* corresponding to different levels of service quality of the path. The SCI approach is evaluated on the given dataset collected from a real operational environment. The results show that the proposed approach achieves good performance for service quality assessment, confirming the feasibility of assessing the service quality of an Internet path through end-to-end measurement.

The remainder is organized as follows. Section 2 introduces the dataset that motivated SCI. Section 3 introduces the design of SCI. Section 4 presents the validation and performance evaluation of SCI with regard to abrupt change detection and service-level event identification accuracy. Section 5 focuses on characterizing the service quality of the involved Internet paths in the dataset. Section 6 discusses issues in need of further investigation, and gives an overview on related work. Finally, Section 7 concludes the paper.

2. The dataset

The SCI work was initially motivated by the aim of extracting information about the service quality of Internet paths from a measurement dataset. The dataset consists of four traces and was provided by UNINETT that operates the Norwegian national research and education network. Specifically, this dataset was collected from a measurement infrastructure, called DragonLab [1], between three measurement end-systems located in three ISP networks in Norway, China and New Zealand as shown in Fig. 1. Each trace records active measurements between the measurement end-systems, conducted by *continuously* sending 64-byte UDP probe packets every 10 ms in both directions of each path. More specifically, the four measured paths are Norway to China (N–C), China to Norway (C–N), Norway to New Zealand (N–NZ), and New Zealand to Norway (NZ–N) via the Internet backbone. Recall that in this paper, we adopt the same notion of *path* as termed in [32]. We focus on the end-to-end behaviors of Internet paths. In other words, we treat the network as a blackbox, and each path is defined by its sender and its receiver at the two ends of the path.

In the measurement setup, each measurement end-system was directly connected via the border gateway router of the ISP facing the Internet core. This ensured that performance anomalies in the measurement probes stem, with a high probability, from events in the backbone network. Throughout this paper, a performance anomaly (in terms of a performance metric) is meant to be an abnormal/abrupt change in performance (on that performance metric).

Measurement end-systems were NTP-synchronized [4], generating probe packets using a tool called Rude/Crude [5]. Each probe packet is identified with a sequence number and timestamped on both the sender and receiver sides. From these, delay and loss behavior statistics for each path are obtained.

For our study, we have been provided with three-month measurement data in the period of July–September 2010 for the four measured Internet paths. During the three

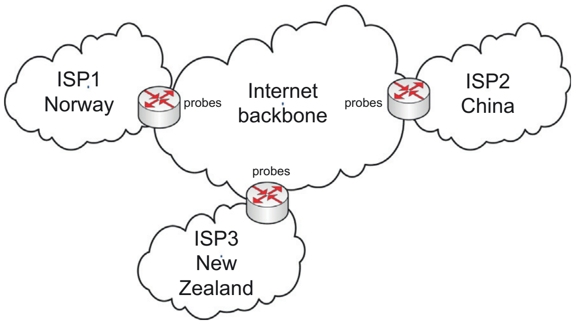


Fig. 1. Topology overview.

months, the measurement setup daily generated four traces of probes sent for each path. Each per-day trace contains information of about 86.4×10^5 probes. The information is a record per probe received: the probe sequence number and two timestamps (i.e. the sending time (tx) and the receiving time (rx)). A probe is lost if its sequence number does not appear among those in the records.

Note that the measurement was conducted on the two-ends of operational commercial Internet paths whose performance metrics and characteristics are unknown a priori and with no additional information collected by intermediate nodes. This motivated us to develop a method to help assess the service quality of such Internet paths, given only end-to-end delay and loss measurements available. We call the developed approach SCI and introduce it in the next section.

3. The SCI approach

In this section, we describe the design of SCI, our proposed approach for service quality assessment of an Internet path. Ultimately, SCI maps active probes sent along the path into a set of events which characterizes the service quality of the Internet path. Particularly, predicated on end-to-end delay and loss measurements fed into the SCI engine, our approach first constructs a set of performance signals potentially conserving performance anomaly signatures (Section 3.1). SCI then proceeds with the constructed performance signals to detect abrupt changes in the aggregate delay and average delay time series through a novel technique using low-rank and sparse matrix decomposition called Principal Component Pursuit (PCP) (Section 3.2). Alarms flagged by PCP are further mapped into service-level events pinpointing degradations and failures in the service over the Internet path (Section 3.3). While identified, service-level events are finally transformed into three metrics, *availability*, *fatigue* and *stability*, in order to characterize the service quality of the Internet path (Section 3.4). Fig. 2 provides an overview of the SCI design, where the right part is a zoom of the left part.

3.1. Constructing performance signals

As depicted in Fig. 2, end-to-end measurements of the investigated Internet path form the input to SCI. Particularly, packet probes are periodically injected and collected from vantage points at the two ends of the path. It is noted that there are issues surrounding the deployment of end-to-end network probes. For example, there is an inherent tension in designing optimal deployment algorithms by minimizing probing overhead. While there may be efficient mechanisms in the literature which tend to minimize probing overhead to monitor network performance [22,37], this is out of the scope of this paper, as our goal is to propose an approach for service quality assessment of Internet paths. We thus in this paper, ignore the possible effect due to probing overhead.

By leveraging the received packet probes, SCI extracts important path performance information, specifically delay and loss characteristics. The intuition behind this is that many performance anomalies on Internet paths leave their signatures on the delay and/or loss behavior. In some cases, a simultaneous increase in delay and loss is noticed when the path experiences congestion. In other cases, a simultaneous increase in loss and decrease in delay indicates a failure. However, only an increase in delay without a significant loss might indicate a queue building up in some routers on the path.

Predicated on the collected delay and loss measurements on the Internet path, SCI detects long-lasting, *persistent* performance anomalies in terms of delay and loss, which are *in the order of minutes*. There are a number of reasons for this. First, transient performance changes or anomalies, i.e., in the order of seconds or less, are quickly resolved and/or can be easily accommodated by Internet applications with application layer adaptation techniques. Second, transient performance anomalies have been shown to be much more frequent than persistent ones [31], and are indeed expected during BGP convergence or rerouting [20]. Finally, authors of [31] show that while less frequent, long-lasting performance anomalies have the most significant effect on availability. For this purpose, we divide time into intervals of equal length that is in the order of minutes and longer than the probing interval.

In SCI, the delay and loss behavior of probes over a time interval are conserved through a set of *performance signals*, which statistically summarizes the probe behavior. Certainly, various statistics might be used to construct the performance signals. For example, the minimum one-way delay time series may capture a variation in the minimum

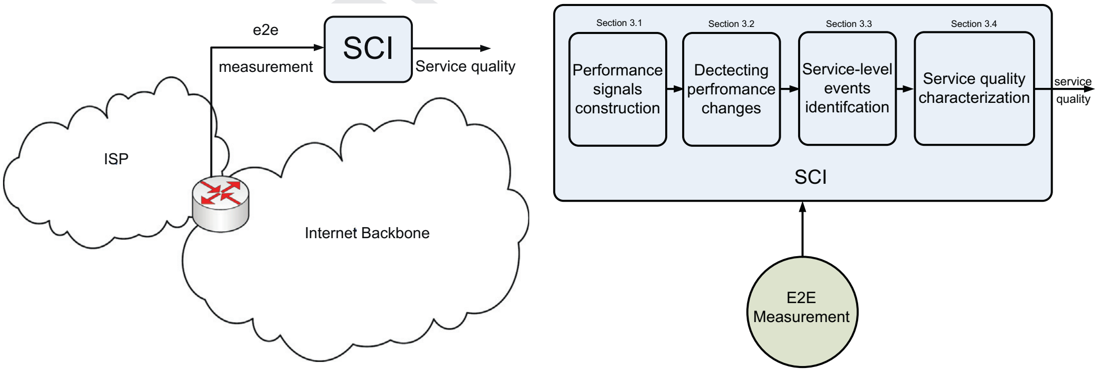


Fig. 2. SCI overview.

queuing delay on the measured Internet path. Since only service-level degradations and failures are targeted in our approach, we propose to construct performance signals using the sum and the average of one way delays in addition to aggregate loss, which is the sum of losses, for each time interval t, also called *time bin* throughout the rest of this paper. Our intuition behind this is that during a time interval when a path experiences failure, the average per packet delay might not change, unlike the sum of packet delays (aggregate delay) over that particular time bin: aggregate delay may dramatically decrease due to the high number of losses. On the other hand, a congestion event during a time bin might increase both the aggregate and average delays. Based on this intuition, Table 1 summarizes the performance signals chosen for our analysis.

In Table 1, d_i and l_i refer to per packet delay and per packet loss, respectively. Here, $l_i = 1$ means probe packet i is lost or otherwise $l_i = 0$ means the packet is received, while N is the number of packets received within the time bin.

3.2. Detecting abrupt changes: Principal Component Pursuit (PCP)

Given the time series of performance signals constructed according to Table 1, SCI proceeds with detecting abrupt changes in the delay signals which, together with losses, can be considered as indications of performance anomalies on the Internet path. This is motivated with the observation that while losses have been a well known indicator of performance anomalies in Internet paths [9,21], it has been recently shown that delay signals should be further decomposed to infer performance anomalies. Indeed, delay signals might fall down into two parts: "normal", having a smooth periodic behavior and "anomalous", exhibiting abrupt short-lived behavior [6].

3.2.1. Motivation of using PCP

There are a wide range of anomaly detection techniques in the literature, ranging from time series forecasting techniques, e.g., EWMA, ARIMA, to frequency and wavelet domain analysis techniques. However, it has been observed that 24-h (24-hour) delay signals exhibit high correlation and periodicity (e.g. [6]). Structural analysis methods, such as principal component analysis (PCA) are thus better suited for decomposing such matrices [19,30].

In brief, PCA constructs the baseline behavior by projecting the time series under analysis into a normal subspace, while flagging the deviation from the baseline into anomalous behavior. Let D be a matrix representation of the delay signals, where each column corresponds to a 24-h part of the time series, and each row represents the signal values for a time bin in the corresponding 24-h part. Essentially, PCA seeks the best rank-k estimate N of the delay signal matrix D by solving the following optimization problem:

$$\min \; \|D - N\|_2, \quad \text{subject to } rank(N) \leqslant k,$$

where $\| \|_i$, $(i = 0, 1, 2)$ denotes the ℓ_i-norm.

Solving this equation can be accomplished by singular value decomposition (SVD) of D [11]. Indeed, SVD decomposes D into three matrices $D = U\Sigma V^T$ such that the columns of U are the singular vectors of DD^T, the columns of V are the singular vectors of $D^T D$, while Σ is a rectangular diagonal matrix of singular values of D. Conventionally, the singular values of Σ are arranged in a descending order.

The singular values are of important significance as they capture the energy of the matrix D. The maximum energy component N captured by the first singular values k represents normal delay subspace, while the residual subspace ($A = D - N$) containing the remaining singular values captures the anomalous components [6].

Unfortunately, as a ℓ_2 norm decomposition of delay signals, PCA-based decomposition exhibits the so-called perturbation phenomenon due to the large outliers in delay signals [6,7,34].

Exploiting additionally the observation that abnormal delay variations occupy only with short duration within the total observation window (e.g., a day of measurement), thus temporally localized or sparse in time, we use a more robust technique called Principal Component Pursuit (PCP) [12].

PCP is a variation of PCA, but more robust to the outliers [12]. In this work, we adopt PCP to analyze the time series of the constructed signals, particularly aggregate delay and average delay.

3.2.2. PCP basics

To decompose delay matrix D into a normal low rank matrix N and a sparse anomalous matrix A, we attempt to find the matrix A such that the matrix $N = D - A$ has the lowest possible rank k. More formally we want to solve the following optimization problem:

$$\min_{N,A} \; \|A\|_0, \quad \text{subject to } D = N + A, \quad \text{rank}(N) \leqslant k \tag{1}$$

where $rank()$ denotes the rank of a matrix, and $\| \|_0$ denotes the ℓ_0-norm, i.e., the cardinality of the non-zero elements.

The optimization problem (1) is generally NP-hard [12]. However, based on recent advances in optimization theory, it has been proven that the nuclear norm, i.e., the sum of singular values, recovers the low rank component [13] while the ℓ_1 norm, i.e., the sum of absolute values, recovers the sparse component in terms of sign and support *with remarkable robustness to the outliers in comparison to the ℓ_2 norm* [18]. Accordingly, Eq. (1) (low-rank and sparse recovery) can be solved using a convex optimization problem called *Principal Component Pursuit* [12] defined as:

$$\min_{N,A} \; \|N\|_* + \lambda\|A\|_1, \quad \text{subject to } D = N + A, \tag{2}$$

where $D \in \mathbb{R}^{n_1 \times n_2}$, $\| \|_*$ denotes the nuclear norm, i.e., the sum of the singular values of the normal delay matrix N

Table 1
Performance signals.

Raw data	Metric	Definition
Per packet delay (d_i)	Aggregate delay	$\sum_i d_i$
	Average delay	$\frac{\sum_i d_i}{N}$
Per-packet loss (l_i)	Aggregate loss	$\sum_i l_i$

Q1 Please cite this article in press as: A. Abdelkefi et al., Assessing the service quality of an Internet path through end-to-end measurement, Comput. Netw. (2014), http://dx.doi.org/10.1016/j.comnet.2014.04.016

or $\|N\|_* = \sum_{i=1}^{\min(n_1,n_2)} \eta_i = \sum_{i=1} Diag\left(\sqrt{N^T N}\right)_i$, $\|\ \|_1$ denotes the ℓ_1-norm of the anomalous event matrix A, i.e., $\|A\|_1 = \sum_{i=1}^{n_1 \times n_2} |A_i|$, and $\lambda > 0$ is a weighting parameter.

The weight parameter λ can be linked to n_1 and n_2 as follows [12]:

$$\lambda = \frac{C}{\sqrt{\max(n_1, n_2)}}, \quad C \in \mathbb{R} \tag{3}$$

Note that for PCP to minimize the weighted combination of the nuclear norm and the ℓ_1-norm, one has to identify the appropriate value of the weighting parameter λ or indeed C such that the matrix A is sparse, while capturing the maximum number of abrupt changes in the delay time series with the lowest false positive rate. A detailed empirical investigation on the value of C is presented in Section 4.2.

To solve a convex problem such as Eq. (2), different solvers have been proposed, ranging from the Alternate Direction Method (ADM) [15] to Singular Value Thresholding (SVT) and the Dual Method [11]. We opt for the one which scales for large matrices using the inexact version of the Augmented Lagrange Multiplier (IALM) solver [24].

The key idea of IALM [24] is to transform Eq. (2) into the so-called augmented Lagrangian function of the form:

$$L(N, A, Y, \mu) = \|N\|_* + \lambda\|A\|_1 + \langle Y, D - N - A\rangle + \mu\|D - N - A\|_F^2, \tag{4}$$

where $Y \in \mathbb{R}^{n_1 \times n_2}$ is the Lagrangian multiplier, $\mu > 0$ is a penalty parameter, $\langle U, V\rangle$ denotes the usual inner product between matrices U and V of equal sizes, i.e., $\langle U, V\rangle = \sum_{i,j} U_{i,j} Y_{i,j}$ and $\|\ \|_F$ is Frobenius norm.

Eq. (4) would solve PCP by iteratively minimizing the Lagrangian function with respect to each one of the variables N and A while fixing the other variables at their latest values and then update the Lagrangian multiplier and the penalty parameter. Specifically, the algorithm progresses as follows [24]:

$$N_{k+1} = \arg\min_N L(N, A_k, Y_k, \mu_k) \tag{5a}$$
$$A_{k+1} = \arg\min_A L(N_{k+1}, A, Y_k, \mu_k) \tag{5b}$$
$$Y_{k+1} = Y_k + \mu_k(D - N_{k+1} - A_{k+1}) \tag{5c}$$
$$\mu_{k+1} = \rho\mu_k \tag{5d}$$

This procedure stops when the relative error $Rerr$ is below a threshold tol, i.e. $Rerr = \frac{\|D-N-A\|_F}{\|D\|_F} < tol$.

It has been shown [24] that IALM converges quickly to the optimal solution which makes it efficient for large scale data. This property motivates the adoption of IALM as the solver of PCP algorithm in SCI.

3.2.3. Using PCP in SCI

As introduced earlier, in SCI, for each delay signal (aggregate or average) series, we construct a matrix $D \in \mathbb{R}^{n_1 \times n_2}$, where n_1 (=720) is the number of 2-min time bins (see Section 6.1 for discussion about the choice of 2-min as the time bin duration) in a 24-h time series, and n_2 (=92) is the number of days in the 3-month measurement period. Specifically, $D(i,j)$ is the value of the delay signal in time bin i on day j. Our goal is to detect abrupt changes and identify their duration (i to $i + n$ time interval) in delay signals on each of the measurement days j in matrix D.

Applying PCP to D, we obtain a normal matrix N and a sparse anomalous matrix A. Each non-zero element (i,j) in the obtained matrix A is an alarm which flags an alarm in the corresponding (aggregate or average) delay signals. Particularly, the alarm pinpoints the time bin, where delay signals experience abrupt variations, and the sign of deviations. In addition, the located time information further allows to find from the loss signal the corresponding number of losses at the same time interval. Fig. 3 shows an example alarm flagged by SCI.

3.3. Service-level event identification

Here we introduce the targeted set of *service-level events* that have close relation to degradations in the end-to-end service quality on the path [16].

In essence, we base our analysis on the intuition that the detected abrupt variations in delay signals correlated with the loss signals form together potential signatures of quality degradations and failures in the end-to-end service. Particularly, *inter-* and *intra-domain routing anomalies* are potential reasons for an abrupt increase in delay and/or loss [39]; a simultaneous increase in aggregate and average delay with no loss is more likely due to some *queues persistently building up and emptying* on the Internet path; an increase in both aggregate and average delay coupled with losses may capture *long duration congestion*. In addition, *persistent failures* cause a high number of losses but with a decrease in aggregate delay.

Thus, the identification of service-level events including service degradations (SDs) and service failures (SFs) is predicated on the correlation between the detected delay abrupt variations and the corresponding losses. For this reason, we define a three dimensional subspace of basis as follows:

$$\Gamma = [\text{Agg.loss}, \text{Agg.delay}, \text{Ave.delay}]$$

where Agg.loss, Agg.delay and Ave.delay represent aggregate loss, aggregate delay, and average delay, respectively.

Alarms flagged using PCP as introduced in the previous subsection are projected into the Γ space and mapped to three service-level events defined as follows:

- SD1 is a set of events causing service degradation and defined as the subspace

$$\Sigma_1 = \{(x, y, z);\ x = 0,\ y > 0,\ z > 0\}.$$

Alarm:
Day: Thursday July 20th,
Time: 10:20 AM,
Aggregate delay sign : (-),
Average delay sign: (-),
Losses: 4025

Fig. 3. An alarm flagged by SCI.

- SD2 is a set of events corresponding to a different level of service degradation and defined as the subspace

$$\Sigma_2 = \{(x, y, z);\ x > 0,\ y > 0,\ z > 0\}.$$

- SF is the set of events causing service failure and defined as

$$\Sigma_3 = \{(x, y, z);\ x > 0,\ y \leqslant 0\},$$

where x, y and z are respectively the coordinate of loss, aggregate delay and average delay in the Γ space, extracted from the flagged alarms. We call the set $\Delta = \{\bigcup \Sigma_i,\ i = 1, 2, 3\}$, the *set of service-level events*. Accordingly, data points that do not belong to Δ, due to the algorithm artifact, are filtered out.

Table 2 summarizes the defined service-level events and their potential root causes.

Note that in Table 2, $(+)$ and $(-)$ respectively denote events inducing positive and negative changes in the performance signal, with (0) for loss denoting no loss. Also, $(*)$ denotes that the related metric might not have an impact on the corresponding service level.

To gain a better insight into SCI service-level event identification, we expose in Fig. 4 how service-level events are identified over a 24-h measurement period of an Internet path in the dataset based on the chosen performance signals. The time interval for aggregating/averaging is 2 min, or in other words, each time bin is 2 min long, and there are 720 time bins. We draw vertical boxes to locate variations in delay signals and their corresponding packet losses. The figure shows how PCP-detected delay abrupt variation events and their corresponding losses are correlated, and how they help identify the various service level events. Particularly, out of the measured 24-h, 5 service failures (SF) are identified at different time bins, while 4 service degradation episodes of level SD2 are recorded. In the figure, from left to right, the first two boxes are SD2 events, the next two boxes contain successive SF and SD2 events each, and the last three are all SF events. The alert reader may have noticed that, from the figure, it is visually not obvious to say the last box contains an SF event. In other words, SCI is not perfect or may indeed be conservative. Concerning this, we shall discuss the detection accuracy of SCI in Section 4.

3.4. Service quality assessment

Now that we have identified service-level events, we turn our attention to the assessment of service quality of the given Internet path. Particularly, we base our analysis on three *service quality metrics* (SQMs): *availability*, *fatigue* and *stability*.

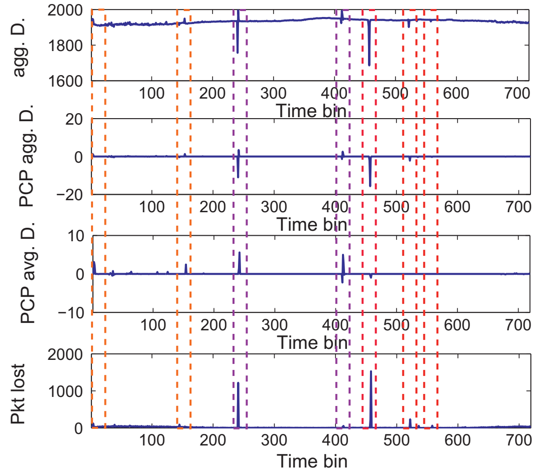


Fig. 4. Service level detection and identification.

Availability is a well-known metric for service assessment (e.g. [17,31]). In the context of an Internet path, the service is said to be available when the user of the path can communicate from one end to the other end of the path, and unavailable otherwise. *Fatigue* is a metric we introduce in this paper to quantify the service degradation while the service is still available on the path. Specifically, the service may experience performance degradation of level SD1 or SD2 due to persistent congestion, queues building up or re-routing/route changes. For such cases, we say the service is under *fatigue*. *Stability* is also a commonly used service assessment metric (e.g. [32]). In our context, it measures the fraction of time where the service is available, and does not experience degradations.

Quantifiably, let n_{Tot} denote the total number of time bins within a chosen reference time interval (e.g., an hour), n_{SD1}, n_{SD2} and n_{SF} the number of time bins within the chosen reference time interval where SD1, SD2 and SF events are encountered, respectively. Then the *service quality metrics* are computed as follows:

$$\text{Availability} = \frac{n_{Tot} - n_{SF}}{n_{Tot}}, \tag{6}$$

$$\text{Fatigue} = \frac{n_{SD1} + n_{SD2}}{n_{Tot} - n_{SF}}, \tag{7}$$

$$\text{Stability} = \frac{n_{Tot} - n_{SD1} - n_{SD2} - n_{SF}}{n_{Tot}}, \tag{8}$$

Table 2
Service-level events and potential root causes.

SL event	Performance signals			Root causes
	Agg. loss	Agg. delay	Ave. delay	
SD1	(0)	(+)	(+)	Queues filling up, intra/inter-domain routing anomalies
SD2	(+)	(+)	(+)	Congestion, intra/inter-domain routing anomalies
SF	(+)	(−)	(∗)	Failures

By definition, the SQMs are relative over the chosen time interval. The whole measurement period is divided into a number of such intervals n_{Tot}, based on which, the distributions of the computed service quality metrics can be drawn for the measured path (see Section 5.3).

We summarize the operation of SCI in Algorithm 1, where L_{Agg}, D_{Agg} and D_{Ave} respectively denote the aggregate loss matrix, the aggregate delay matrix, and the average delay matrix for the measurement period. In each of them, element (i,j) is the corresponding aggregate loss, aggregate delay or average delay value in time bin i on day j.

Algorithm 1. SCI

Input: Per-packet delay d and loss l
Output: SQMs
1: **while** *not converged* **do**
2: $D_{Agg}, D_{Ave}, L_{Agg} \leftarrow performance\_signals(d, l)$
3: $A_{Agg} \leftarrow PCP(D_{Agg})$
4: $A_{Ave} \leftarrow PCP(D_{Ave})$
5: $S \leftarrow service\_level\_event(L_{Agg}, A_{Agg}, A_{Ave})$
6: $SQM \leftarrow service\_quality\_assessment\ (S)$
7: **end while**

4. Validation

The previous section has described the proposed SCI approach for assessing the service quality of an Internet path. Central to SCI are detection of abrupt delay changes and service-level event identification. In this section, we validate SCI using the dataset introduced in Section 2. Based on this dataset, our validation is aimed at answering the following question: how well can SCI detect abrupt delay changes and identify service-level events?

4.1. Ground-truth

Evaluating the effectiveness of SCI requires a set of events that SCI results can be compared to, i.e., the ground-truth. Unfortunately, the construction of such a ground-truth is notoriously difficult. A common approach in anomaly detection is to inject synthetic anomalies into the network [35]. This approach has shown significant efficiency in the validation of traffic anomaly detection algorithms. However, in our context, it was not recommended to inject synthetic performance anomalies in the measured Internet paths, essentially due to concerns about negatively affecting the service quality of the measured paths in the real operational environment. To overcome such limitations, we adopted the approach proposed in [29,31], which has been shown to be advantageous for the end-to-end analysis of Internet paths, although requiring a great deal of effort. Specifically, to construct the ground-truth, we manually inspected delay and loss patterns in the measurement probes: we visually detected abrupt variations in delay signals and examined per-packet delay and loss patterns for the visually identified variations. One has to notice that there is no ideal scheme for isolating and quantifying abrupt variations in a delay time series due to the set of configuration parameters and/or modeling assumptions. We employed a manual inspection approach [29,31] to get a hopefully "correct" isolation of the "true" variations in the constructed performance signals.

In the manual inspection, three main patterns are associated to the three service level events in the dataset as follows:

- Per packet delay exhibiting a persistent increase and decrease during a time bin, which includes about 12,000 probe packets, or more, as shown in Fig. 5(a). This is likely induced by some queues on the path continuously building up and emptying. We associate, thereby, such a behavior with SD1.
- Per packet delay exhibiting the same behavior, while a cluster of losses is additionally observed in comparison to more dispersed losses during "normal" time bins. This is likely induced by congestion along the path [14], causing a level 2 service degradation (SD2). Fig. 5(b) illustrates per packet loss pattern.
- A very high number of losses is experienced (Fig. 5(c) shows 4800 packets lost successively at a particular time bin). Such a behavior eventuates a service failure (SF) for the corresponding time bin.

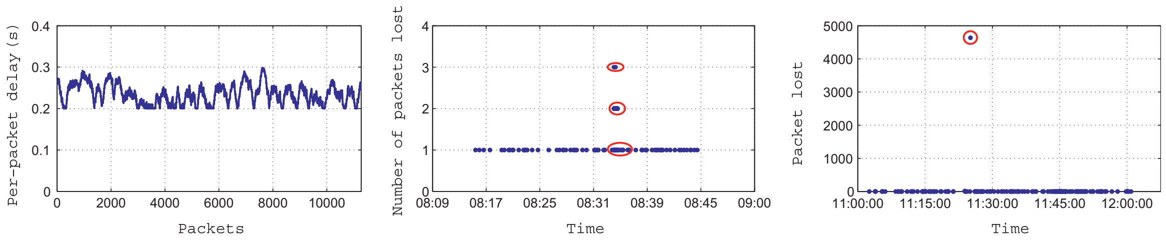
Note that the ground-truth constructed through the collected and processed data set is only approximate. There can be performance anomalies that are short or transient in a way that they do not affect the probes' behavior during a bin time interval. We recall that such performance anomalies of short duration, i.e., non-persistent, are out of scope for this paper.

Once constructed, the ground-truth serves to compute both the false positive and true positive rates. Particularly, given each of the visually inspected service level events, we compare the results of SCI to such a baseline. If SCI identifies a service level event correctly, then we label it a *true positive* or simply detected. On the other hand, if SCI identifies a service level event that is not visually observed and validated, then we label it as a *false positive*.

4.2. Detection accuracy

SCI's detection accuracy is predicated on PCP's capability in detecting abrupt changes in delay signals, which is highly affected by the choice of the weighting parameter λ in Eq. (2). In this subsection, we conduct an empirical study of both detection and false alarm probabilities as a function of λ for the four Internet paths in our dataset.

Fig. 6 shows SCI performance in terms of anomaly detection and false positive rates as a function of the weighting parameter λ. Note that it has been suggested for λ to take the form of Eq. (3). It is worth highlighting that each measured path has a specific overall performance. Particularly, while SCI experiences a detection rate in the order of 88% for the path from China to Norway at the value of $\lambda = \frac{3}{\sqrt{\max(n_1,n_2)}}$, it experiences only a detection rate of 64% at the same value of λ in the reverse direction. This is very likely due to the asymmetry of the associated Internet paths. Additionally, one might notice that for a suitable



(a) Baseline: SD1 (b) Baseline: SD2 (c) Baseline: SF

Fig. 5. SCI baseline construction.

value of $\lambda = \frac{2.5}{\sqrt{\max(n_1,n_2)}}$, SCI shows high detection rate in the order of 80% and 94% at a relatively low false alarm rate in the order of 6% and 14%, respectively, for the path from Norway to China and its reverse direction. Similarly SCI shows a good overall performance for the paths between Norway and New Zealand at the same value of λ. Note that as the value of λ increases, both detection and false alarm rates decrease. This is mainly due to the decrease of sensitivity of PCP to low intensity variations in delay signals, posing a tradeoff.

Fig. 7 shows ROC curves (Receiver Operator Characteristics) obtained for the four measured paths. The comparison of ROC curves shows a similar performance of SCI on each of the measured paths. In essence, SCI can achieve a high detection rate, in the order of 90% at a low false alarm rate, approximately in the order of 10%, for the four paths. Unfortunately, one has to adjust the value of λ for each of the four paths, to achieve such "good" performance. Expectedly, this adds more complexity to SCI deployment as it requires a tuning of the parameter λ. To overcome this issue, we propose the value of $\lambda = \frac{2.5}{\sqrt{\max(n_1,n_2)}}$ as a rule of thumb, which is shown to achieve, based on Fig. 6, the best sensitivity-correctness tradeoff.

In the following we fix the parameter λ to the proposed value. Nevertheless, we note that for a different path, the parameter λ may be adjusted to obtain the best possible results.

To get a better insight why our proposed technique with the chosen value of λ yields such a high detection rate combined with a low false alarm rate, we have illustrated a set of detected service-level events on the path from Norway to New Zealand in Fig. 4. We have marked with rectangles the time units where delay abrupt variations are found based on visual inspection. The figure illustrates how sharply PCP is able to separate abrupt variations (lower 3 plots) from the mass of the measured delay (upper plot). Particularly small intensity delay variations and outliers in the delay time series are readily detected by PCP, and the detection process does not need any additional thresholding.

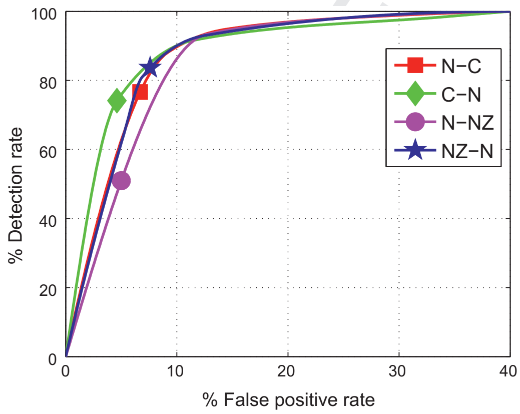


Fig. 7. ROC curves of SCI for all paths.

4.2.1. Detection accuracy: SCI-PCP vs. SCI-PCA

In this section we compare the detection accuracy of SCI using PCP (SCI-PCP) to that using PCA (SCI-PCA). We recall that PCA-based change detection requires two tuning

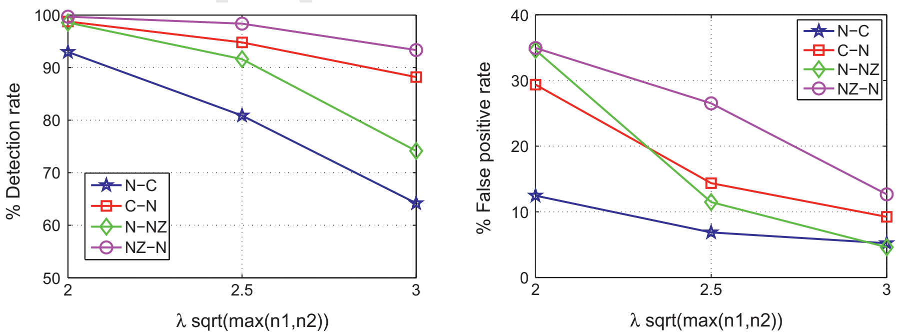


Fig. 6. Overall SCI performances in function of λ.

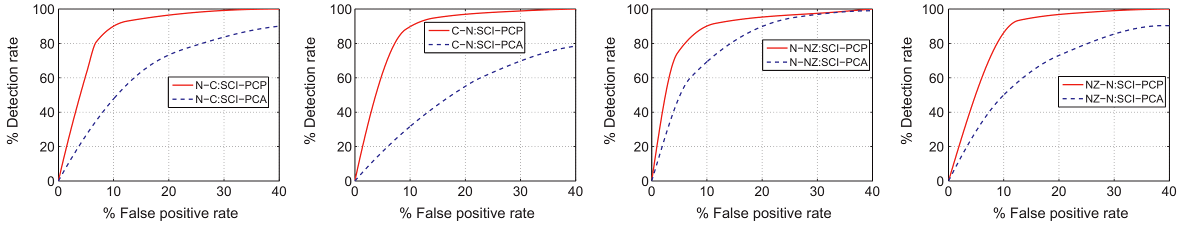


Fig. 8. Comparison of SCI-PCP and SCI-PCA.

parameters. They are the rank k of the matrix that estimates the normal subspace and the threshold value α that extracts anomalies from the residual subspace. In contrast, PCP only requires one tuning parameter λ that controls the sparsity of the anomalous matrix A. For the sake of comparison, we, for SCI-PCA, fix k such that the estimate matrices conserve 90% total energy of the matrices D_{agg} and D_{avg}, and vary the threshold value $\alpha = \mu + \tau\sigma$ in the interval $[\mu + \sigma, \mu + 3\sigma]$, where μ and σ are respectively the mean and standard deviation of the residual signal $(A(j))$. For SCI-PCP, we vary the threshold λ in the interval $\left[\frac{1}{\sqrt{\max(n_1,n_2)}}, \frac{3}{\sqrt{\max(n_1,n_2)}}\right]$, where n_1 and n_2 are the dimension of the delay matrix D.

Fig. 8 illustrates the result of the comparison for each of the measured paths. The ROC curves show a clear difference between SCI-PCP and SCI-PCA. Specifically, the detection performance by SCI-PCP is (much) better than by SCI-PCA. For example, SCI-PCA is only able to achieve a detection rate of 80% at a false positive rate of 40% for the path between China and Norway (C–N), while for the same path and the same detection rate, SCI-PCP achieves a false positive rate lower than 10%. The same observation also holds for other paths.

4.3. Identification accuracy

In order to investigate SCI's identification accuracy, we draw the ROC curves per service level in Fig. 9. It can be seen that SCI experiences the best identification performance for SD1 and SD2 on both paths between Norway and China. For example, SCI achieves 90% detection rate with only 5% false positive for SD2 identification on the path from China to Norway, while only a 2% false positive rate is recorded at a 97% detection rate for SD1 on the path from Norway to China. On the other hand, SCI experiences slightly better performance for SF identification on the path from Norway to New Zealand with a 3% false positive rate at a very high detection rate in the order of 99%.

The variation in SCI identification capabilities seems to be more likely due to the intensity of the changes in the delay signals which directly impact the detection capabilities of PCP. In fact, we observe that most of the SD1 and SD2 events induce small intensity variations in the delay time series for both paths between Norway and New Zealand, while higher intensity variations for the paths between Norway and China. SF events, on the other hand, normally induce significant outliers in delay signals, which can be more effectively detected and identified.

5. Assessing the service quality

In this section, we assess the service quality of the four paths involved in the dataset, after removing the identified false positives. The study discussed here not only shows that SCI assists in obtaining performance statistics of the various service-level (degradation) events, but also demonstrates that it is a potentially effective tool for service providers to evaluate the service quality of an Internet path.

5.1. Performance overview

Fig. 10 summarizes the distribution of service-level events identified for each of the measured paths during the three months of measurement. The figure shows that the service for the paths between Norway and China experiences different quality levels than between Norway and New Zealand. Indeed, while most of the service-level events for the paths between Norway and New Zealand

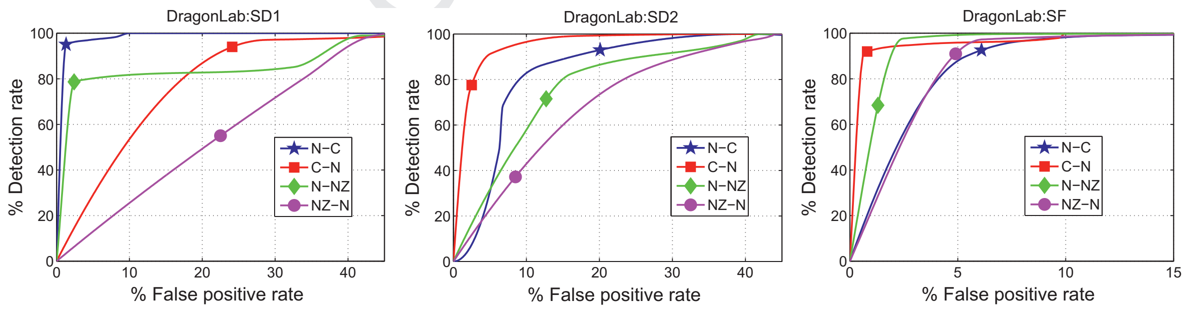


Fig. 9. ROC curves of SCI identification accuracy per service-level event.

Q1 Please cite this article in press as: A. Abdelkefi et al., Assessing the service quality of an Internet path through end-to-end measurement, Comput. Netw. (2014), http://dx.doi.org/10.1016/j.comnet.2014.04.016

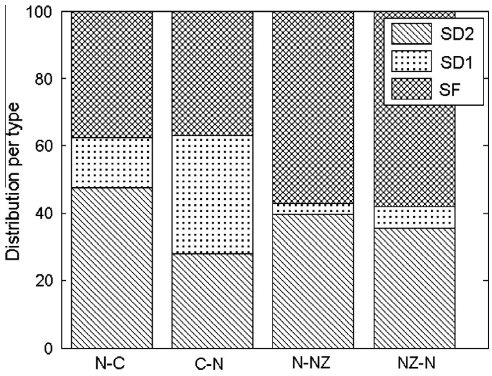


Fig. 10. Summary of service-level degradation events: SD1, SD2 and SF.

are failures, the paths between Norway and China appear to be relatively more robust with a smaller ratio of service failure events. In addition, it is shown that even the two directions of one Internet connection may experience different service quality levels. For example, the path from China to Norway seems to suffer from more service degradations of level SD1, which is in the order of 30%, unlike the reverse direction where SD1 events are three times less, only in the order of 10%. This enforces the hypothesis of asymmetry of Internet paths. If the two paths were the same, one would expect similar service level events experienced. Nevertheless, the proposed approach does not depend on whether measured paths between two entities are asymmetric or not: SCI works on a network level path independently of its "direction" (see Section 1 for the definition of a path adopted from [32]).

5.2. Service-level event analysis

In this subsection, we present a statistical analysis on the three service-level events: SD1, SD2 and SF, focusing on event duration and inter-event time.

Q2 5.2.1. SD1 events

Fig. 11 shows the cumulative distribution function (CDF) of SD1 event duration and the distribution of SD1 inter-event time for the four measured paths. The figure shows that on all paths, most of the SD1s have a short duration up to 2 min (single time bin). In addition, the CDF of SD1 inter-event time shows that they are mostly dispersed for all measured paths: more than 70% occur at least 1 h apart.

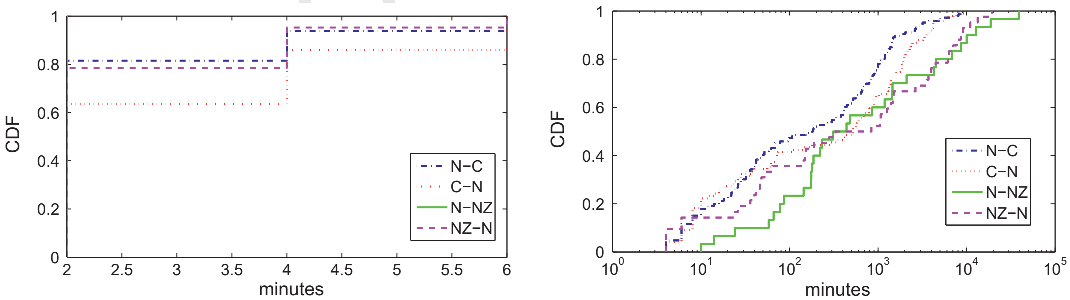
5.2.2. SD2 events

Fig. 12 illustrates the CDF of SD2 event duration. Perhaps surprisingly, the figure shows that SD2 evens may vary from 2 min to 60 min on the path from China to Norway and to 90 min from New Zealand to Norway. Fortunately, most of the SD2 events (more than 50%) are relatively short, up to 2 min. We have noticed that while short SD2 events seem to occur unpredictably, longer SD2 events seem to appear in "rush hours" due to traffic overflow when the network is highly utilized. To get a better insight into SD2 frequency within the measurement period, we also draw the CDF of the inter-event between SD2 episodes. The figure shows that most of the SD2 events are dispersed more than 1 h apart. The paths from New Zealand to Norway and China to Norway exhibit the largest inter-event times with 9 and 5 days, respectively.

5.2.3. SF events

So far we have considered service degradation levels SD1 and SD2. In this part, we show how long and how frequent service failures are. We recall that service failures are more likely induced by component failures along Internet paths, which is critical to understand in order to maintain smooth service delivery over the Internet. Fig. 13 plots the CDF of SF event duration. It can be seen that while most of the SF events are short (up to 2 min) forming a common body of about 70% for all paths, the maximum duration is in the order of 6 min. Whereas the path from New Zealand to Norway (NZ–N) is the one having the highest ratio of short duration SF events, the path from China to Norway (C–N) experiences the longest SF episodes. The measured paths seem to be more reliable in comparison to some previous studies in the literature, which claim that 60% of failures in the Sprint backbone [28] and 70% in the Cenic backbone are up to a duration of 6 min [38], while the maximum failure duration is much longer.

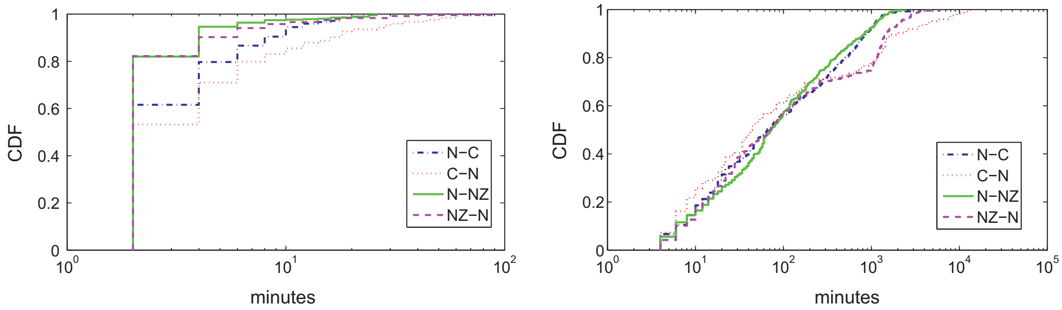
Fig. 13 also provides a deeper breakdown showing the time between SF episodes, i.e., time between failures. We draw a vertical line at 1 h, which serves as our definition of "flapping": two or more consecutive SF events, generally of short duration, occurring on the same Internet path separated by less than 1 h. The figure shows that half of the SF events (50.7%), on the path from Norway to New Zealand



(a) CDF of SD1 duration

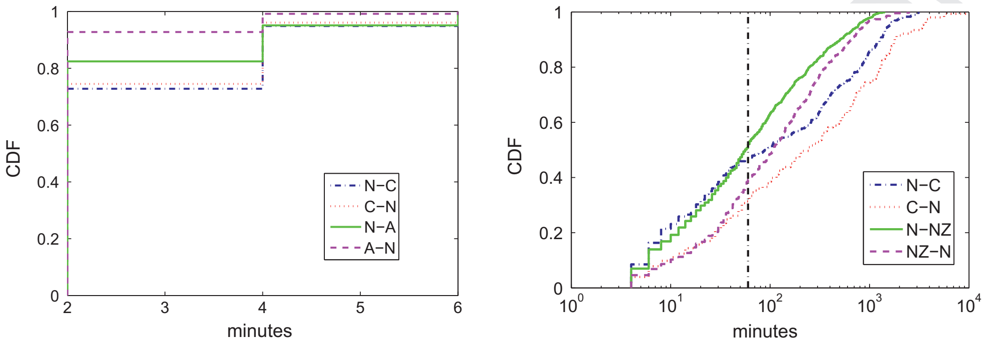
(b) CDF of SD1 inter-event time

Fig. 11. CDFs for SD1 events.



(a) CDF of SD2 duration (b) CDF of time between SD2 events

Fig. 12. CDFs for SD2 events.



(a) CDF of SF duration (b) CDF of time between SF events

Fig. 13. CDF for SF events.

(N–NZ), occur during flapping periods, while on the other paths, flapping episodes seem to be less frequent, e.g. 32% for the path from China to Norway (C–N) and 46% on the reverse path.

5.3. Service quality assessment

Finally, we assess the service quality of the four measured paths using performance metrics *availability*, *fatigue*, and *stability* introduced in Section 3.4. In the calculation, we divide the total 3-month measurement period into time slots with 1 h length each, which means there are a bit more than 2000 such time slots. Note that, within each one-hour time slot, there are 30 time bins of 2 min. We then calculate *availability*, *fatigue*, and *stability* for each time slot with regard to (6)–(8), and we draw the CDFs of each SQM.

5.3.1. Availability

Fig. 14 provides the CDF of per-hour service availability for each of the four measured paths. The figure shows that the path from China to Norway (C–N) experiences the highest per-hour service availability: around 94% of all 1 h time slots are 100% available. On the other hand, the path from Norway to New Zealand (N–NZ) experiences the lowest availability with only 75% of time slots being 100% available.

Interestingly, the figure additionally shows that while rare, per-hour service availability can drop to 70% in some paths. This is likely due to the flapping failures, although previously considered infrequent on the measured Internet paths. This implies that, although less frequent, service flapping episodes appear to be more disruptive than long SF events in affecting service availability. This finding indeed reinforces those of prior studies, e.g., Markopoulou et al. [28] and Turner et al. [38], which found that flapping failure is a predominant source of unavailability in Internet paths.

5.3.2. Fatigue

We investigate the CDF of the service fatigue experienced in the four measured paths. Particularly in Fig. 15, we draw the CDF of service that is *fatigue-free*, which is equal to 100% − (7), for visibility purposes. The figure shows that while the path from Norway to New Zealand (N–NZ) does not experience service fatigue for only 82% of all the 1 h time slots, the path from China to Norway (C–N) has the best performance with around 92% of the time slots that are “fatigue-free”. Not surprising, the service *fatigue* appears to be long-tailed with a maximum per-hour fatigue rate, which is the point where each curve in Fig. 15 starts, varying from 52% for the path from Norway to China (N–C) to 100% for the path from New Zealand to Norway (NZ–N). This is likely due to the long duration SD2 events experienced, as the SD1 events are shown to

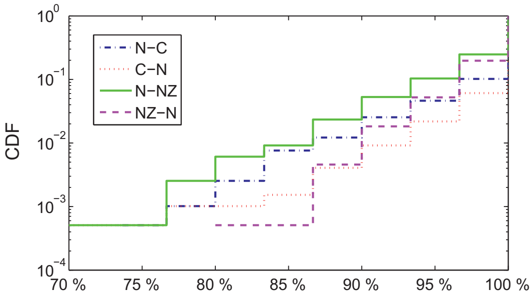


Fig. 14. Availability per path.

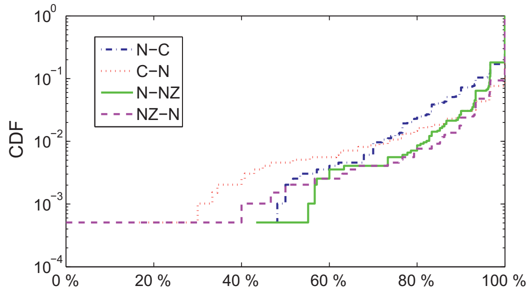


Fig. 15. Fatigue-free per path.

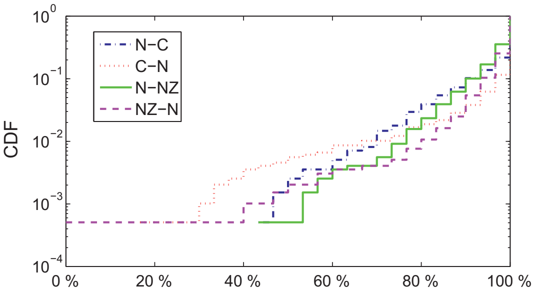


Fig. 16. Stability per path.

be mostly of short durations in the previous sub-section. On the whole, the fatigue in the service quality seems to be highly induced by long duration congestion epochs in the measured Internet paths.

5.3.3. Stability

The stability metric measures the impact of the detected service-level events including degradations and failures on the overall performance of the measured Internet paths. It provides a measure of the ratio of time slots which experience neither service degradation nor failure. The CDF of service stability for each of the four measured paths is presented in Fig. 16. The figure shows that while the path from Norway to New Zealand (N–NZ) experiences the highest service instability, indicated by the lowest jump at 100%, the service from China to Norway (C–N) experiences the highest stability. Particularly, while the path from Norway to New Zealand suffers from more frequent level SD2 service degradations and service failures than the one from China to Norway, the former bears only 64% of the 1 h time slots that are 100% stable, in comparison to 88% for the latter. This observation emphasizes that service degradations to level SD2 likely due to congestion and service failures have a high impact on the overall service stability in Internet paths. SD1 events, on the other hand, seem to have lower impact, even though they may affect the smoothness of service delivery.

6. Discussion and related work

6.1. Discussion

Though the design of SCI was initially motivated by the aim of extracting related Internet path service quality information from the given dataset, we believe SCI can also be used in other scenarios where similar end-to-end delay and loss measurements are available or possible. Here we highlight an application scenario, where SCI has a natural fit.

Network service level agreements (SLAs) define contractual commitment between a service provider and its costumers. While meeting SLA creates revenue and improves the service provider's reputation, failing to meet SLA might result in losses in terms of customers and revenue. Here, it is crucial to implement *SLA compliance monitoring*, which assesses whether the service level is within the agreement for a service provided. As a specific example, consider a company that has two data centers (DCs) distributed in two regions. This company, as a customer, establishes SLA with an ISP that provides Internet connection between the two DCs. It is natural that the service quality of the Internet connection or path between the two DCs is part of the SLA. Note that, as long as the contracted SLA is satisfied, the customer very likely will not care about how the path is constructed (e.g. which routers is on the path) and maintained (e.g. if re-routing is done). Nevertheless, in this case, in order to be sure if the contracted SLA on the service quality of the path is met, measurement is necessary, which should tell quantitatively the service quality (e.g. in terms of availability, fatigue and stability) of the path over time. We believe, for this scenario, SCI is a competitive candidate to use. One reason is that SCI may be implemented by the customer independent of the ISP,[1] or by the ISP, or by both. The competitiveness of SCI also lies in that it only requires measurement points sitting at the two ends of the path.

In this paper, availability, fatigue and stability have been used as the service quality metrics. They are intuitive metrics. Particularly, availability and stability are two commonly used service assessment metrics. (See discussion in Section 3.4.) If any or more among them are adopted in the SLA between the service provider and the customer, the information provided by SCI will be highly relevant and helpful. Up to this point, we stress that under an SLA

[1] In scenarios where the customer cannot set up measurement points at both ends of a path solely by itself, involvement of the ISP may be necessary, and in this case, the service provider and the costumer may collaborate to perform path-oriented SLA compliance monitoring.

violation, how the customer and/or the provide will re-act is out of the scope of this paper.

In the remaining of this subsection, we discuss factors that may affect the accuracy of SCI, and the intuition behind our choice of the delay and loss statistics.

Recall that, in this work, we have focused on three service-level events, namely SD1, SD2 and SF. We have shown that these service levels, which can be identified based only on end-to-end measurements, are highly useful for assessing the service quality of an Internet path. Nevertheless, due to lack of complete knowledge of the path (though Table 2 gives some potential root causes of such events), what exactly has happened (on the path) causing a service degradation or failure event is unlikely to be known, and hence, SCI is a compromise between accuracy and feasibility. The accuracy of SCI in service quality assessment may be influenced by several factors that we discuss in the following.

First, SCI requires measurement points at both ends of the monitored path, each regularly sending probe packets to the other end. In the provided dataset, probe packets were sent every 10 ms, causing an overhead of probing traffic at about 50 kbps. For different scenarios and requirements, different probing rates may be used. In general, the more frequently the probing packets are sent, the more accurate the assessment is. How to achieve balance between overhead and accuracy requires further study.

Second, SCI makes use of packet delay information, which implicitly requires synchronization of the two measurement points. For the dataset introduced in Section 2, measurement points were synchronized using NTP. Using other synchronization techniques such as Global Positioning System (GPS) might help improving the assessment accuracy.

Third, SCI aggregates per-packet measurement data into a series of time bins. In our validation and case study, we used 2 min as the length of each time bin. In the literature, the authors of [21,20] proposed mechanisms for detecting and localizing black holes in the Internet within time intervals of 15 min. Shorter duration was chosen by the authors of [16], where service level event detection was based on passive measurement within 5- or 10-min intervals. Tangentially related, the authors of [40] proposed time intervals of 1 h for service anomaly detection and localization based on passive measurement. Although there is no clear reason behind a particular choice of the time bin duration in these previous studies, we base our choice on the observation that persistent performance anomalies on Internet paths likely have a duration in the order of a few hundred seconds [31], and long outages have a duration ranging from seconds to 2 min [29]. In general, choosing a longer time bin will smooth the signals and reduce the accuracy, while using a smaller time bin duration may lead to better accuracy but increased dimensionality of the aggregated data and, consequently, increased processing overhead. In the extreme case when the time bin is too short, the signal fluctuation can be so strong that many (if not most) changes are only transient, which may lead to an increased false positive ratio and reduced assessment accuracy. Obtaining a more thorough understanding of the optimal time bin length surely needs more work.

Finally, we remark that from the dataset, many types of statistics may be constructed from the loss and delay measurements (e.g. see [10]). In our work, we have chosen aggregate/average delay and loss for each time bin. This choice is rather intuitive, and the intuition is reflected by Table 2, where, specifically, the considered service-level events, namely SD1, SD2 and SF, and their root causes can be easily mapped to and explained by the chosen statistics. As for other types of statistics, it may be interesting to consider, but we leave this for future investigation. In addition, we have focused on three intuitive service-level events, i.e. SD1, SD2 and SF, implying different levels of service level degradation. While other similar events may be introduced, how to easily identify them from end-to-end loss and delay measurements needs further investigation and we leave this as future work.

6.2. Related work

In SCI, active probes are used. In the literature, probing techniques have been widely adopted [2,3]. Probing has been frequently deployed in dedicated vantage points in various ISPs/networks to detect per-packet pathologies [33], failures [9,37] and silent failures [20]. Other researchers have proposed using probing to diagnose Internet path performance focusing on per-packet loss rate, reordering and replication per link [27], or available bandwidth (see [8,23] and references therein). In the same vein, several techniques have focused on the effect of routing on the overall performance in the Internet [33,9,37] and thus proposed probing at dedicated end-systems to identify routing disruptions. In addition, several authors have made use of both active and passive measurement in order to diagnose network performance. The basic motivation comes from the need of getting a more complete view instead of focusing on specific aspects of network behavior. Hubble [20] focuses on detecting reachability problems within the Internet using a distributed platform collecting a set of active and passive measurements. Iplane and a lightweight version Inano [25,26] leverage such a monitoring infrastructure to predict the path to the destination and its properties, e.g., delay, loss rate and bandwidth. PlanetSeer [41] uses passive measurement to detect network performance events and relies on active probes to cover the scope of the detected events.

In comparison to previous work, SCI is unique in the following ways.

1. SCI focuses on assessing the service quality of the Internet path of interest. Specifically, it utilizes delay and loss measurements from vantage points at both ends of the path. SCI's lightweight probing infrastructure is easy to implement and scales well with the targeted paths to be measured. In this sense, SCI is different from all those approaches requiring sophisticated distributed measurement infrastructures, and is indeed most related to, e.g., [8,23,27].
2. However, the performance metrics of interest in SCI are different. While SCI focuses on service degradation and failure events SD1, SD2 and SF, mechanisms described

in [8,23,27] are dedicated to available bandwidth or packet-level behavior like loss, reordering and replication.

3. In addition, SCI detects persistent performance changes on a relatively fine-grained time scale, i.e., in the order of a minute, unlike most of the related techniques, which operate with a coarser resolution: 5–10 min for CEM [16] and 1 h for Argus [40].
4. SCI not only identifies service-level events based on detection of abrupt delay changes together with loss information, but also assesses the service quality of Internet paths in terms of availability, fatigue and stability.

7. Conclusion

Understanding the service quality of Internet paths is of great importance for both the service provider and the user. In this paper we presented SCI, a novel approach for detecting abrupt changes in aggregate delay and average delay time series, identifying the corresponding service-level events, and eventually assessing the service quality of the measured path. SCI achieves these by leveraging lightweight packet probes between measurement systems which can be easily deployed at the two ends of the measured path. The work was initially motivated by the aim of extracting Internet path service quality information from a given dataset, which was collected through end-to-end measurement on four intercontinental Internet paths under the DragonLab project [1]. The performance of SCI was evaluated on this given dataset. The evaluation results are encouraging. Specifically, we found that, even though relying exclusively on end-to-end measurement data, SCI exhibits more than 90% accuracy for abrupt delay change detection and 80% accuracy for service-level event identification. These results not only justify the design of SCI, but also shed new light on service quality assessment of Internet paths through end-to-end measurement.

Acknowledgements

The authors would like to thank the anonymous reviewers for their comments that have helped us improve the quality of the paper. In addition, we are grateful to Renata Cruz Teixeira for her valuable comments. We also thank Nevil Brownlee from University of Auckland, Amund Kvalbein from Simula Research Laboratory, Qianli Zhang and Jilong Wang from CERNET, Christian Jenssen from NTE and the R&I department at UNINETT for the dataset they provided and for their helpful comments. Much of the work was conducted at "The Centre for Quantifiable Quality of Service in Communication Systems (Q2S), Centre of Excellence" (http://www.q2s.ntnu.no), appointed by The Research Council of Norway and funded by the Research Council, NTNU, UNINETT and Telenor.

References

[1] Dragonlab Project. <https://openwiki.uninett.no/dragonlab:start>.
[2] Gomez Inc. <http://www.gomez.com/>.
[3] Keynote Systems. <http://www.keynote.com/>.
[4] Rfc 1305 – Network Time Protocol (version 3) Specification, impl. <http://www.ietf.org/rfc/rfc5905.html>.
[5] Rude/crude. <http://rude.sourceforge.net/>.
[6] A. Abdelkefi, Y. Jiang, A structural analysis of network delay, in: Proc. Conference on Communication Networks and Services Research (CNSR), 2011.
[7] A. Abdelkefi, Y. Jiang, A. Oslebo, O. Kvittem, Robust traffic anomaly detection with principal component pursuit, in: Proc. ACM CONEXT, Student Workshop, 2010.
[8] G. Aceto, A. Botta, A. Pescapé, M. D'Arienzo, Unified architecture for network measurement: the case of available bandwidth, J. Network Comput. Appl. 35 (5) (2012) 1402–1414.
[9] P. Barford, N. Duffield, A. Ron, J. Sommers, Network performance anomaly detection and localization, in: Proc. IEEE INFOCOM, 2009.
[10] A. Botta, A. Pescapé, G. Ventre, An approach to the identification of network elements composing heterogeneous end-to-end paths, Comput. Networks 52 (15) (2008) 2975–2987.
[11] J.-F. Cai, E.J. Candes, Z. Shenx, A singular value thresholding algorithm for matrix completion, SIAM J. Optim. (2010).
[12] E.J. Candès, X. Li, Y. Ma, J. Wright, Robust principal component analysis?, J ACM 58 (3) (2011) 11:1–11:37.
[13] E. Candés, B. Recht, Exact matrix completion via convex optimization, Found. Comput. Math. 9 (2009) 717–772.
[14] Z. Cataltepe, P. Moghe, Characterizing nature and location of congestion on the public internet, in: Proc. IEEE Symposium Computers and Communication, (ISCC), 2003.
[15] C. Chen, B. He, X. Yuan, Matrix completion via an alternating direction method, IMA J. Numer. Anal. 32 (1) (2012) 227–245.
[16] D.R. Choffnes, F.E. Bustamante, Z. Ge, Crowdsourcing service-level network event monitoring, in: Proc. ACM SIGCOMM, 2010.
[17] M. Dahlin, B. Chandra, L. Gao, A. Nayate, End-to-end wan service availability, IEEE/ACM Trans. Network. 11 (2) (2003) 300–313.
[18] D.L. Donoho, Compressed sensing, IEEE Trans. Inform. Theory 52 (2006) 1289–1306.
[19] H. Hassani, S. Heravi, A. Zhigljavsky, Forecasting European industrial production with singular spectrum analysis, Int. J. Forecast. 25 (1) (2009) 103–118.
[20] E. Katz-Bassett, H.V. Madhyastha, J.P. John, A. Krishnamurthy, T. Anderson, Studying black holes in the internet with hubble, in: Proc. USENIX NSDI, 2008.
[21] R. Kompella, J. Yates, A. Greenberg, A. Snoeren, Detection and localization of network black holes, in: Proc. IEEE INFOCOM, 2007.
[22] F. Li, M. Thottan, End-to-end service quality measurement using source-routed probes, in: Proc. IEEE INFOCOM, 2006.
[23] J. Liebeherr, M. Fidler, S. Valaee, A system-theoretic approach to bandwidth estimation, IEEE/ACM Trans. Network. 18 (4) (2010) 1040–1053.
[24] Z. Lin, M. Chen, Y. Ma, The Augmented Lagrange Multiplier Method for Exact Recovery of Corrupted Low-rank Matrices, Technical Report, 2011. 1009.5055v2.
[25] H.V. Madhyastha, T. Isdal, M. Piatek, C. Dixon, T. Anderson, A. Krishnamurthy, A. Venkataramani, iplane: an information plane for distributed services, in: Proc. USENIX OSDI, 2006.
[26] H.V. Madhyastha, E. Katz-Bassett, T. Anderson, A. Krishnamurthy, A. Venkataramani, iplane nano: path prediction for peer-to-peer applications, in: Proc. USENIX NSDI, 2009.
[27] R. Mahajan, N. Spring, D. Wetherall, T. Anderson, User-level internet path diagnosis, in: Proc. of the Nineteenth ACM Symposium on Operating Systems Principles, 2003.
[28] A. Markopoulou, G. Iannaccone, S. Bhattacharyya, C.-N. Chuah, Y. Ganjali, C. Diot, Characterization of failures in an operational ip backbone network, IEEE/ACM Trans. Network. 16 (4) (2008) 749–762.
[29] A. Markopoulou, F. Tobagi, M. Karam, Loss and delay measurements of internet backbones, Comput. Commun. 29 (10) (2006) 1590–1604.
[30] V. Moskvina, A. Zhigljavsky, Commun. Stat.: Simul. Comput. (2003).
[31] E. Myakotnykh, O. Wittner, B. Helvik, A. Abdelkefi, J. Hellan, O. Kvittem, T. Skjesol, A. Øslebø, An analysis of interdomain availability and causes of failures based on active measurements, Telecommun. Syst. (2011).
[32] V. Paxson, End-to-end routing behavior in the internet, SIGCOMM Comput. Commun. Rev. 26 (4) (1996) 25–38.
[33] V. Paxson, End-to-end internet packet dynamics, IEEE/ACM Trans. Network. 7 (3) (1999) 277–292.
[34] H. Ringberg, A. Soule, J. Rexford, C. Diot, Sensitivity of pca for traffic anomaly detection, in: Proc. ACM SIGMETRICS, SIGMETRICS '07, ACM, New York, NY, USA, 2007, pp. 109–120.

[35] F. Silveira, C. Diot, Urca: pulling out anomalies by their root causes, in: Proc. IEEE INFOCOM, 2010.
[36] F. Silveira, C. Diot, N. Taft, R. Govindan, Astute: detecting a different class of traffic anomalies, in: Proc. ACM SIGCOMM, 2010.
[37] R.C. Teixeira, Network Troubleshooting from End Hosts, Technical Report, Universite Pierre et Marie Curie Paris6, 2010.
[38] D. Turner, K. Levchenko, A.C. Snoeren, S. Savage, California fault lines: understanding the causes and impact of network failures, in: Proc. ACM SIGCOMM, 2010.
[39] F. Wang, Z.M. Mao, J. Wang, L. Gao, R. Bush, A measurement study on the impact of routing events on end-to-end internet path performance, in: Proc. ACM SIGCOMM, 2006.
[40] H. Yan, A. Flavel, Z. Ge, A. Gerber, D. Massey, C. Papadopoulos, H. Shah, J. Yates. Argus end to-end service anomaly detection and localization from an isp point of view, in: Proc. IEEE INFOCOM, 2012.
[41] M. Zhang, C. Zhang, V. Pai, L. Peterson, R. Wang, Planetseer internet path failure monitoring and characterization in wide area services, in: Proc. USENIX NSDI, 2004.

Atef Abdelkefi is a PhD student in the Norwegian university of science and technology since August 2009. He got a computer engineering degree from the National school of computer science (ENSI, Tunisia) and a master degree from the Laboratory of analysis of system architecture at the French National research center (LAAS-CNRS) in respectively 2008 and 2009. His research interest includes network measurement and performance analysis.

Yuming Jiang received his BSc from Peking University, China, in 1988, MEng from Beijing Institute of Technology, China, in 1991, and PhD from National University of Singapore, Singapore, in 2001. He worked with Motorola from 1996 to 1997. From 2001 to 2003, he was a Member of Technical Staff and Research Scientist with the Institute for Infocomm Research, Singapore. From 2003 to 2004, he was an Adjunct Assistant Professor with the Electrical and Computer Engineering Department, National University of Singapore. From 2004 to 2005, he was with the Centre for Quantifiable Quality of Service in Communication Systems (Q2S), Norwegian University of Science and Technology (NTNU), Norway, supported in part by the Fellowship Programme of European Research Consortium for Informatics and Mathematics (ERCIM). He was a visiting scholar with Northwestern University, USA from 2009 to 2010. Since 2005, he has been with the Department of Telematics, NTNU, as a Professor.

He was Co-Chair of IEEE Globecom2005 – General Conference Symposium, TPC Co-Chair of 67th IEEE Vehicular Technology Conference (VTC) 2008, General/TPC Co-Chair of International Symposium on Wireless Communication Systems (ISWCS) 2007–2010, and General Chair of IFIP Networking 2014 Conference. He is first author of the book "Stochastic Network Calculus". His research interests are the provision, analysis and management of quality of service guarantees in communication networks. In the area of network calculus, his focus has been on developing models and investigating their basic properties for stochastic network calculus (snetcal), and recently also on applying snetcal to performance analysis of wireless networks.

Bjarne E. Helvik (1952) received his Siv.ing. degree (MSc in technology) from the Norwegian Institute of Technology (NTH), Trondheim, Norway in 1975. He was awarded the degree Dr. Techn. from NTH in 1982. He has since 1997 been Professor at the Norwegian University of Science and Technology (NTNU), the Department of Telematics. He is principal academic at the Norwegian Centre of Excellence (CoE) for Quantifiable Quality of service in Communication systems (Q2S). Since August 2009, he has been Vice Dean with responsibility for research at the Faculty of Information Technology, Mathematics and Electrical Engineering at NTNU. He has previously held various positions at ELAB and SINTEF Telecom and Informatics. In the period 1988–1997 he was appointed as Adjunct Professor at the Department of Computer Engineering and Telematics at NTH.

His field of interests includes QoS, dependability modeling, measurements, analysis and simulation, fault-tolerant computing systems and survivable networks as well as related communication system architectural issues. His current research focus is on distributed, autonomous and adaptive fault-management in telecommunication systems, networks and services. He has authored/co-authored a number of research papers.

Gergely Biczók is a postdoctoral fellow at the Norwegian University of Science and Technology. He earned his PhD at the Budapest University of Technology and Economics in 2010. He spent one year at Northwestern University as a Fulbright visiting researcher from 2007 to 2008. He was also a research fellow at Ericsson Research from 2003 to 2007. His research interests are in the broad area of network algorithms, measurements and economics.

Alexandru Calu is an IT infrastructure consultant in a Microsoft-products focused consultancy company, Avanade. He received his B. Eng. in Electronics, Telecommunications and Information Technology from "Politehnica" University of Bucharest in 2009, and his Master degree in Electrical Engineering – Telecommunications track from Delft University of Technology in 2011. He prepared his master thesis at the Norwegian University of Science and Technology (NTNU), Norway.