Quality of Service Analysis of Internet Links with Minimal Information

Felipe Mata and Javier Aracil
High Performance Computing and Networking Group
Escuela Politécnica Superior
Universidad Autónoma de Madrid, Spain
Email: felipe.mata@gmail.com, javier.aracil@uam.es

***Abstract*—Monitoring the Quality of Service (QoS) of Internet links is of paramount importance for network managers, and consequently has received great attention from the research community. To monitor QoS, practitioners leverage on network traffic measurements and, by means of practical models and statistical techniques, make predictions and detect outliers that allow the planning of telecommunication networks and detection of abnormal behavior, respectively.**

However, obtaining detailed measurements from Internet links at current network speeds is very challenging. Moreover, the amount of resources required to properly storage detailed network measurements make unfeasible to perform long measurement campaigns. These facts have motivated the application of techniques to reduce the information gathered from the network, such as sampling or the use of summarized statistics, making network traffic monitoring less demanding and allowing longer measurement campaigns.

Accordingly, this thesis proposes two novel methodologies to perform QoS analysis of Internet links leveraging on summarized statistics of network traffic. Each methodology relies on a network traffic model, on which sound statistical methodologies are used on attempts of detecting relevant events that either require action from the network managers or are related with degradations of the provided QoS.

I. Introduction

A. Overview and Motivation

Quality of Service (QoS) refers to the delivery of data over communication networks attending to special requirements. Particularly in computer networks, QoS refers to the guarantee of certain levels of performance to data delivery by means of Traffic Engineering (TE) tasks. Such levels of performance are commonly agreed in a contractual document signed by both the provider and the consumer—the Service Level Agreement (SLA). A SLA defines the performance of the service being offered in terms of some measurable network indicators, such as throughput, latency or jitter. As a result, network managers monitor the network with the aim of timely detecting QoS degradations. The TE tasks they make use for QoS control can be divided into two main classes: system based and measurement based approaches. The former class is basically formed by two architectures that provide frameworks for ensuring QoS, namely Integrated Services (IntServ) and Differentiated Services (DiffServ). IntServ implements a parametrized approach where applications use the Resource Reservation Protocol (RSVP) to request and reserve resources through a network, whereas DiffServ implements a prioritized model by marking packets according to the type of service they desire and applying different queueing strategies to tailor performance to expectations.

On the other hand, measurement based approaches leverage on network traffic measurements and, by means of practical models and statistical techniques, make predictions to plan telecommunication networks and detect abnormal behavior. This second alternative for QoS provisioning is commonly used in practice, as there are studies pointing out that improving QoS by investing in capacity is more profitable than investing in provision of multiple service classes [1]. Consequently, this thesis focuses on this latter class, and provides useful network traffic models, and algorithms leveraging on them, to facilitate the decision making process of TE tasks of large-scale networks.

In order to accurately perform TE tasks, it is of paramount importance to have detailed descriptions about what is happening in the network. For this reason, there are many measurement techniques existing in the literature (active and passive), most of them being implemented nowadays in large-scale networks, allowing the network managers to tackle incidences. This increasing interest in network traffic measurements has been reflected in the research community: there have been many contributions involving network traffic measurements to characterize the Internet traffic [2], [3], [4], and even to characterize specific applications [5].

These studies demonstrate the importance of network measurements for network research and operation; however, collecting accurate network traffic measurements has become an arduous task because links' speeds have increased at a larger pace than memory accesses' speeds [6], making it unfeasible to monitor all the network traffic. This has motivated the use of different techniques, such as the application of sampling to network traffic measurement [7], [8] or aggregation of statistics in time bins [9]. These techniques allow longer measurement campaigns; however, they entail a reduction of the available information. Therefore, the application of statistical inference and digital signal processing techniques have gained importance, allowing to obtain further information from the measured data. One of the most common ways for extracting this information is by identifying patterns or footprints that are easily detectable, and then characterize in an accurate manner the measured traffic [10], even measuring these footprints at different time resolutions [11]. Once the footprints are detected, statistical methodologies are applied to corroborate whether the conclusions obtained from them

978-3-901882-50-0

can be extrapolated, or they are just a particular case of the study [12].

This constraint in the amount of information possible to gather and analyze from the network has fostered the development of techniques able to identify abnormal behavior [13] or pattern shifts [24] with minimal information. The ability to infer different network status with minimal information makes these techniques also useful for real-time monitoring. As a consequence, network managers are still capable of control their networks and take action timely to resolve security breaks and capacity shortages, even though the information they measure from the network is a subsample of what really is being transmitted in the network.

B. Objectives and Hypothesis

This thesis presents the analysis of different measurement datasets of Internet links, with the aim of detecting degradations of the QoS in the network. The analyzed datasets contain minimal information, in the sense that they are formed by summarized statistics instead of having detailed records of each event in the network.

We make two common assumptions for developing models of the analyzed traffic. First, we assume that *network traffic is short-term stationary*—i.e., the statistics of the traffic distribution, and consequently their corresponding parameters, slowly vary with time. Second, we assume that *network traffic exhibits a normal baseline under benign and without problems usage*, and deviations from such baseline may evidence the presence of attacks or pattern shifts, which we term as anomalous events. These anomalies, which may pose QoS degradations to the network customers, may be detected as deviations from the proposed models.

Consequently, our objective is *to provide the necessary machinery to detect such anomalous events in a timely fashion, with statistical foundation of their relevance*—which is of paramount interest for Internet Service Providers (ISPs). This machinery should place alerts of the detected events to the network managers, allowing them to take appropriate responses on attempts of diminishing the impact of these events in the level of QoS offered by the network. To this end, we build network traffic models that are useful for tracking the network traffic behavior at the timescales of interest—which are given by the relevant events we aim to detect with the corresponding model. These models constitute the normal baseline from which deviations are flagged as anomalous, which are detected using sound statistical techniques.

II. Our Contributions

This thesis contributes with two novel methodologies for automated network traffic QoS analysis leveraging on minimal information—average network traffic at equidistant time instants obtained from the Multi Router Traffic Grapher (MRTG) tool [9].

The first methodology is designed to detect shifts in users' behavior, and therefore the detected events may entail capacity planning decisions. It builds on modeling the network traffic during a day using a multivariate fairly Gaussian distribution, from which changes in the parameters are detected at timescales of weeks. The change point instants are detected using clustering techniques and validated through the application of the Multivariate Behrens-Fisher Problem (MBFP). The proposed methodology is applied to real network measurements obtained from the Spanish academic network RedIRIS, showing satisfactory performance and entailing large Operational Expenditures (OPEX) reduction to ISPs in the management process of large-scale networks. This contribution is presented in Section III.

The second methodology performs anomaly detection through trend removal of network traffic measurements. It is tailored for Voice over Internet Protocol (VoIP) traffic data, which is one of the most popular services provided through Internet nowadays. The methodology takes as input call count measurements of a VoIP service exhibiting seasonal trends, and outputs stationary residuals, which are used to detect anomalies by means of the application of unsophisticated statistical assumptions. Moreover, we propose a measurement alternative for monitoring VoIP systems; this alternative yields smaller correlations between the obtained measurements when some assumptions are met, which we showed to be satisfied in the actual measurements we analyzed. This contribution is presented in Section IV.

III. Detection of Traffic Changes in Large-Scale Backbone Networks

A. Introduction

As the amount of information provided by management systems in large-scale networks is humongous, network managers face with visual inspection of too many graphs, which calls for automated procedures. Consequently, we proposed a traffic load model for network links that is capable of efficiently tracking sustained load changes, which may call for links capacity upgrades to maintain the level of QoS. Our model facilitates network-wide monitoring of large-scale networks by identifying network links with varying behavior. As a result, network managers can devote their time to different TE tasks, instead of having to visually inspect network traffic load graphs; they can leverage in the proposed tool to highlight the relevant events, and take response after receiving an alert of their detection, which entails a large OPEX reduction.

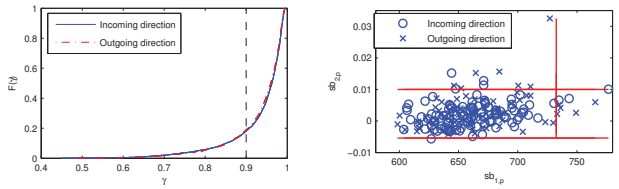
B. Multivariate Normal Model for Daily Traffic

We designed a model for daily traffic based on the short-term stationary assumption introduced before, which is validated using actual network traffic measurements. We take this model as the normal baseline, from which deviations in the parameters are monitored to detect shifts in the user population behavior. The model is based on the following assumptions and considerations:

- Measurements of the same interval during different days come from the same probability distribution.
- The parameters of the distribution vary along the day, thus calling for a multivariate distribution.
- We group measurements in 16 disjoint intervals of 90 minutes to reduce the model dimension.
- The Gaussian distribution is appropriate for modeling the average load in such intervals.

C. Model Validation

To validate the applicability of the model for network traffic inference, we have performed several verifications of the fairly Gaussian assumption. Particularly, we check the univariate and multivariate fairly Gaussianity: we use the linear correlation coefficient γ [14] for univariate normality; we use Mardia's multivariate skewness ($b_{1,p}$) and kurtosis ($b_{2,p}$) coefficients [15] to measure deviations from multinormality. The first step is important, because a multivariate distribution cannot be assumed to be multivariate Gaussian in case any of its marginal distributions violates the Gaussian assumption. The second validation is necessary, since the fact that several variables have univariate normal distributions does not imply that they jointly have a normal distribution [16]. Furthermore, Mardia has shown that the significance of the normal theory tests of mean vectors and covariance matrices is adversely affected by skewness [17] and kurtosis [18], respectively—i.e., having a large skewness (kurtosis) deviation from multinormality adversely affects the false positive rate of normal theory tests applied to the mean vector (covariance matrix).



(a) (b)

Fig. 1. Normality test results: (a) Univariate normality results; (b) Multivariate normality results. Samples are separated by traffic direction: incoming direction (from the Internet to our network); outgoing direction (from our network to the Internet).

The results of the validation are presented in Fig. 1. The univariate normality assumption is verified for more than 80% of the samples ($\gamma > 0.9$ in Fig. 1(a)), which allows us to assume *fairly* Gaussianity—the test was performed at the 5% significance level, and the results are in concordance with previous studies [14]. Regarding the multivariate normality (Fig. 1(b)), we observe that only a few samples lie within the rejection region (to the right of the vertical line, and above and below the upper and bottom horizontal lines, respectively), thus confirming the fairly multivariate Gaussianity assumption—10% of the samples lie in the rejection region at the 1% significance level, but indeed we are only interested in the skewness test, since we will only apply inference to the mean vector, and the result is even better: 4% of the samples are in the rejection region.

D. On-line Load Change Detection Algorithm

We have designed an on-line algorithm to track changes in the model parameters. We look for sustained and statistically significant change points: we use clustering techniques (k-means) to locate the change points; to determine the statistical significance of the change points we face the multivariate version of the Behrens-Fisher problem (MBFP)—whose null hypothesis is that there is no change between the analyzed populations. This algorithm is presented in the work-flow chart of Fig. 2. We have a restriction on the number of instances in each cluster to apply the MBPF methodology, as it has to estimate the inverses of the covariance matrices; this fact is controlled at several points in the algorithm to avoid useless computations.

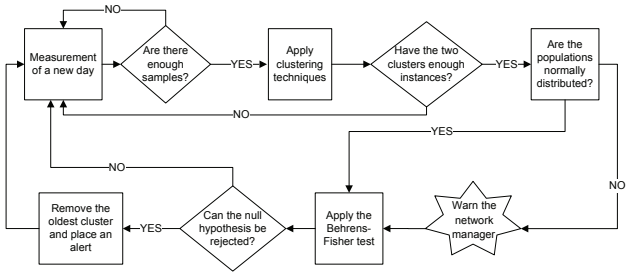


Fig. 2. Work-flow of the on-line algorithm. The starting point is defined in the "Measurement of a new day" box.

The advantage of our on-line algorithm for load change detection is that it decreases the OPEX by reducing the human supervision. We remark that our algorithm produces an alert only in case a stationary change in the load happens. The rest of the time the link is considered normal and no intervention from the network manager is required. We applied our algorithm to actual network traffic measurements from the Spanish academic RedIRIS network: our algorithm placed in average less than 12 network load change alerts requiring human supervision per link in a period of more than 750 days (including holidays), which means a load change nearly every two months in average. We show in Table I the average values for both the number of tests and the number of alerts in both directions, when grouped by link type, and the total average of such quantities.

TABLE I. AVERAGE OF THE ON-LINE ALGORITHM RESULTS (INCOMING/OUTGOING).

Link type	Number of tests	Number of alerts
University	80.20/79.50	11.00/11.09
Backbone	84.20/79.00	10.40/10.60
eXchange	78.33/81.33	10.33/11.66
Total	80.94/79.67	10.72/11.06

E. Network Management Based on Relevant Events

We developed a network management system based on the change point detection algorithm. However, the algorithm only reports the change point location, but not any measure of the relevance of the change points. To differentiate changes, we applied univariate normality tests once our algorithm has detected a change point, identifying which vector component is responsible for the change. We developed an alert color code to differentiate the importance of the detected changes, which allows us to create weather maps of the operators network. An example of how the weather map looks like is shown in Fig. 3, where we show the topology of the RedIRIS backbone with the legend for the different colors used to mark the relevance of the detected changes. In this way, the network manager is able to prioritize the most important detected changes, and once an action has been taken, the link can be marked as normal again—green color.

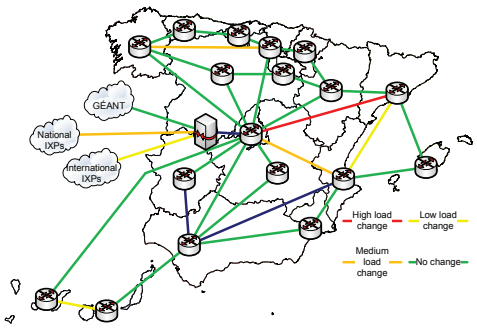


Fig. 3. Sample weather map of the RedIRIS network, with some links needing the network manager attention.

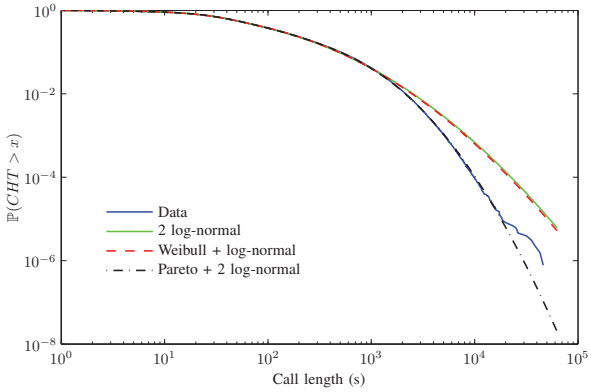


Fig. 4. *Log-log* plot of the CCDF of the data and the best fitting models according to the Kolmogorov-Smirnov statistic value.

IV. Weekly Pattern Time Series Trend Removal: The Case of VoIP

A. Introduction

QoS is very important in the VoIP service, for which low values of latency, packet loss and jitter are crucial. Packet losses have the largest impact, and they are mainly due to overload periods; however, abnormal underload periods are also interesting, since they may signal shortages of the service. Timely detection of these periods is vital for the management of VoIP services. Typically, timely detection relies on statistical analysis of network traffic measurements, which are not stationary. As most of the sound statistical techniques relies on stationary data, we proposed an unsophisticated methodology to remove the trend from network traffic measurements, tailored for VoIP services.

B. Measurement Dataset

Experiments in this section use actual traffic traces collected from an operational network in Italy. A total of 22,000 customers were continuously monitored for more than 4 months. The resulting dataset contains the log of the call arrival epochs and the corresponding durations, and the number of calls at equidistant time instants. In order to develop our methodology, we first inspect the main characteristics of our dataset.

1) Arrival Process: Classical theoretical models for voice traffic posit that the call arrival process is Poisson distributed. In practice, the process rate is assumed to remain constant for blocks of time. We conjecture that the arrival process in our dataset is time-varying Poisson in this sense, and thus the intensity remains constant for time-blocks of length L. From the results of testing this hypothesis we can conclude that it is fairly true when $L \leq 10$ minutes.

2) Call Holding Time Distribution: Regarding the Call Holding Time (CHT) distribution, classically it has been modeled with the exponential distribution. A lot of studies point out that this model is not longer appropriate, and instead remark that heavy tailed distributions should be used. In Fig. 4 we show the analysis of the CHT in our dataset, and the fitting to different heavy tailed models—in some cases we use mixtures of heavy tailed distributions. Our results show that in the case of using a single distribution, the best fitting is obtained with a Log-normal distribution; however, a better fit is obtained using mixtures, particularly a mixture of a Pareto and two Log-normal distributions.

C. Trend Removal Methodology

In what follows, we introduce the notation and assumptions of our trend removal methodology. We denote x_i^n to the network traffic measurements: $i = 0, 1, 2, \ldots, 2015$ refers to the 5-minute time interval within the week; n is the week number, out of a total of $N = 12$ weeks that we analyzed. Our objective is to find a good estimate $\mathbf{y}^n$ for the measurement vector of week n, $\mathbf{x}^n$, using history data, $\mathbf{x}^j$, $j < n$. We assume that the differences from week to week in the weekly pattern are due to random deviations from an average network usage pattern: $\mathbf{x}^n = \boldsymbol{\alpha} + \boldsymbol{\varepsilon}^n$.

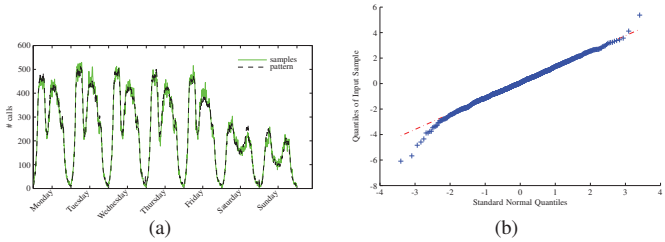
The simpler approach for estimating the average pattern is to set the prediction vector to a windowed average of the data: we used the arithmetic average in a window of size $w = 5$, because it represents a trade-off between model accuracy and robustness to pattern shifts—we used the arithmetic mean because it minimizes the Mean Squared Error of the estimator.

$$\mathbf{y}^n = \hat{\boldsymbol{\alpha}}^n = \bar{\mathbf{x}}^n(w) = \sum_{j=1}^{w} \frac{1}{w} \mathbf{x}^{n-j}. \tag{1}$$

The output of the methodology are standardized normal residuals. To standardize the residuals, we have used the property of Poisson processes relating the mean and variance:

$$\boldsymbol{r}^n = \frac{\boldsymbol{x}^n - \boldsymbol{y}^n}{\sqrt{\boldsymbol{y}^n}}. \tag{2}$$

The performance of the algorithm is illustrated in Fig. 5. In Fig. 5(a) we depict the week pattern of a representative week (green line) and the predicted pattern (black dashed line) for that week. It can be observed that the fit obtained by the prediction is remarkable. On the other hand, we show in Fig. 5(b) the Gaussian QQ-plot of the residuals, where the fit to a straight line is evident except on the tails, and consequently fairly Gaussianity can be assumed. In these results we have filtered out the night periods, a condition that we realized to be necessary given the low amount of calls during the night.



(a) (b)

Fig. 5. (a) Data samples for the week under study and estimated pattern based on previous weeks data samples—nights removed; (b) Gaussian Quantile-Quantile plots of the residuals—nights removed.

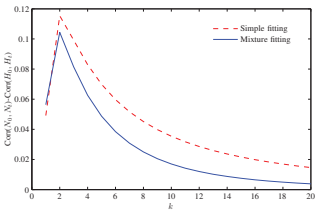
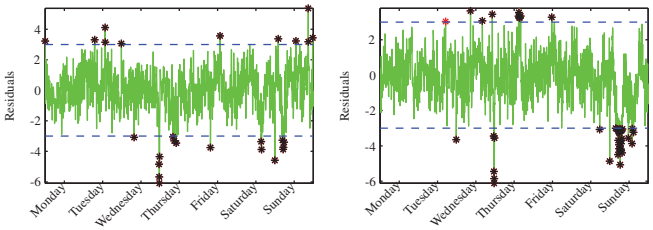


Fig. 6. Correlation comparison of both measurement alternatives assuming the call holding time is distributed accordingly to the two best fitting models presented before.



(a) (b)

Fig. 7. Results of applying the anomaly detection algorithm to the residuals obtained from the model (the ticks refer to the middle of each day): (a) all the samples outside the 3σ confidence band are reported as anomalies; (b) one sample outside the 3σ confidence band is not reported as anomalous.

D. Measurement Alternative

The methodology proposed so far yields fairly standard-normal residuals. However, the correlation is non-negligible in these residuals. This is a problem because most of the sound statistical techniques relies on independence. We believe such correlations are due, among others facts, to the way the measurements were obtained. As a consequence, we proposed an alternative measurement process for call counts, and compared the correlations in both approaches. Traditionally, these systems are measured counting the number of calls N present in the system at regular time instants (e.g., $N_0, N_t, N_{2t}, \ldots$).

We proposed to measure instead the number of calls that have been present in the system during an interval of length t, instead of using the traditional point process $\{N_{kt}\}_{\{k\geq 0\}}$. More precisely, we define:

$$H_a = \{\#\text{calls that have been present in the system during the interval } [a, a+t]\}.$$

Using this alternative process, we found that the correlation between H_0 and H_{kt} is as follows:

$$Corr(H_0, H_{kt}) = \frac{\mathbb{P}(S_e > (k-1)t)}{1 + \frac{t}{\mathbb{E}[S]}}, \qquad (3)$$

where S is the CHT distribution, $\mathbb{E}[S]$ denotes its mean and S_e is its excess lifetime. We want to compare such correlation with $Corr(N_0, N_{kt}) = \mathbb{P}(S_e > kt)$, which is a well-known result from classic queueing systems theory. To do show, we select different CHT distributions, as the only assumption to compute (3) was that the arrival process is Poisson distributed. The results of this comparison are shown in Fig. 6 for the best simple and mixture fitting models, where we show the difference between the correlations in the traditional point process and our proposed alternative as a function of the separation between samples. As can be seen, these differences are always positive, which means that our proposed alternative yields smaller correlations for any time lag, thus being preferable.

E. Anomaly Detection Algorithm

Based on this trend removal methodology, we developed an outlier-friendly algorithm to detect anomalies. We consider as anomalies residuals deviating more than s_{lower} times σ from the mean. However, we consider some anomalies as outliers if they are isolated in the history interval. We flag as anomalous all the residuals deviating more than s_{upper} times σ, irrespectively of whether they are isolated or not. The length of the history interval is set to $m(t) = round\left(\frac{1}{2\phi(-|t|)}\right)$, where $\phi(\cdot)$ is the standard normal Cumulative Distribution Function, and consequently $2\phi(-|t|)$ is the likeliness of observing a residual sample t. The proposed algorithm is as follows:

1) Draw the next sample under test t and compute the length of the interval $m(t)$: proceed to step 2.
2) If $m(t) \geq m_{max}$, place an alert and proceed to step 1, else, proceed to step 3.
3) If $m(t) < m_{min}$, the sample is normal: do not place an alert and proceed to step 1. Else, proceed to step 4.
4) Inspect the $q \cdot m(t)$ samples previous to t. If there is at least one sample r such that $|r| \geq |t|$ within such interval, then place an alert. On the contrary, if the sample is not anomalous, it is just an outlier. In any case, proceed back to step 1.

m_{max} and m_{min} are given by s_{upper} and s_{lower}, respectively, and q is the fraction of samples we inspect backwards in our algorithm to determine whether a sample is isolated or not, given a free $(1-q)\cdot m(t)$ in the future direction to compensate for the unavailability of such data. We illustrate the application of this algorithm to our data for two consecutive weeks in Fig. 7, where the used parameters in the algorithm are shown in Table II. In this figure, the residuals are depicted with a green straight line, whereas the confidence bands given by s_{lower} use blue dashed lines. Flagged anomalies are shown with a black asterisk symbol, whereas isolated anomalies (outliers) use red ones. One example of an outlier may be found in Fig. 7(b), between Tuesday and Wednesday. It is reasonable to consider it an outlier as there was no other sample outside the confidence band since Sunday of the previous week.

TABLE II. PARAMETERS OF THE ON-LINE ALGORITHM FOR DETECTING ANOMALIES IN THE RESIDUALS.

Parameter	Value
s_{lower}	3
s_{upper}	4
q	0.75
m_{min}	370
m_{max}	15,787

V. CONCLUSION

As a conclusion, we summarize the main contributions of this thesis work. Regarding the first main contribution, which detected sustained changes related to user behavior, we have shown that:

- Sustained load changes are detectable in large-scale networks with statistical foundation by leveraging on coarse grained network link measurements.
- A multivariate fairly-Gaussian distribution models the day-night traffic pattern of sufficiently large aggregated measurements.
- An on-line algorithm works with the model to detect potential change points assessing their statistical significance.
- Finally, we contributed with a visualization framework for the relevant discovered events using a network weather map.

Regarding the second main contribution, which detected anomalies in time series with trends, we have shown that:

- Mid-term volume-based anomalies are detectable using prediction in time series with trends using history data.
- The call arrival process is a time-inhomogeneous Poisson process, whereas the call holding time distribution is best modeled in terms of a mixture model of heavy tailed distributions.
- The nature of the call arrival process allows removing the trend of call count data yielding standard normal residuals.
- There exist alternatives for measuring call counts that may outperform the traditionally used one for specific objectives. In particular, we have proposed an alternative measurement technique that outperforms the traditional one in terms of correlations.
- Finally, we contributed with a outlier-friendly anomaly detection algorithm.

VI. THESIS MATERIAL

The thesis can be downloaded from http://www.ii.uam.es/~fmata/research.htm. A full list of publications from the author may be found in http://www.ii.uam.es/~fmata/publications.htm.

ACKNOWLEDGMENT

The authors would like to thank the Spanish Ministery for the F.P.U. scholarship program that funded the development of this thesis.

REFERENCES

[1] A. M. Odlyzko, "The economics of the internet: Utility, utilization, pricing and quality of service," University of Minnesota, Tech. Rep., 1999.

[2] N. Brownlee and K. C. Claffy, "Understanding Internet traffic streams: dragonflies and tortoises," *IEEE Communications Magazine*, vol. 40, no. 10, pp. 110–117, oct 2002.

[3] H. T. M. Neto, J. M. Almeida, L. C. D. Rocha, W. Meira, P. H. C. Guerra, and V. A. F. Almeida, "A characterization of broadband user behavior and their e-business activities," *ACM SIGMETRICS Performance Evaluation Review*, vol. 32, no. 3, pp. 3–13, 2004.

[4] F. Mata, J. L. García-Dorado, J. E. López de Vergara, and J. Aracil, "Factor analysis of Internet traffic destinations from similar source networks," *Internet Research*, vol. 22, no. 1, pp. 29–56, 2012.

[5] S. A. Baset and H. Schulzrinne, "An Analysis of the Skype Peer-to-Peer Internel Telephony Protocol," in *IEEE Infocom*, 2006.

[6] L. G. Roberts, "Beyond Moore's Law: Internet Growth Trends," *Computer*, vol. 33, no. 1, pp. 117–119, 2000.

[7] K. C. Claffy, G. C. Polyzos, and H.-W. Braun, "Application of sampling methodologies to network traffic characterization," *SIGCOMM Comput. Commun. Rev.*, vol. 23, no. 4, pp. 194–203, Oct. 1993.

[8] W. J. Liu and J. Gong, "Double sampling for flow measurement on high speed links," *Computer Networks*, vol. 52, no. 11, pp. 2221–2226, 2008.

[9] T. Oetiker and D. Rand, "MRTG: The Multi Router Traffic Grapher," in *Proceedings of USENIX Conference on System Administration*, Boston, USA, 1998, pp. 141–148.

[10] S. McCreary and K. C. Claffy, "Trends in Wide Area IP Traffic Patterns," The Cooperative Association for Internet Data Analysis (CAIDA), Tech. Rep., 2000.

[11] K. Papagiannaki, N. Taft, Z.-L. Zhang, and C. Diot, "Long-term forecasting of Internet backbone traffic," *IEEE Transactions on Neural Networks*, vol. 16, no. 5, pp. 1110–1124, Sept. 2005.

[12] J. Kilpi and I. Norros, "Testing the Gaussian approximation of aggregate traffic," in *Proceedings of ACM SIGCOMM Workshop on Internet Measurement*, Marseille, France, 2002, pp. 49–61.

[13] G. Androulidakis, V. Chatzigiannakis, and S. Papavassiliou, "Network anomaly detection and classification via opportunistic sampling," *IEEE Network.*, vol. 23, no. 1, pp. 6–12, 2009.

[14] R. van de Meent, M. Mandjes, and A. Pras, "Gaussian traffic everywhere?" in *Proceedings of IEEE International Conference on Communications*, vol. 2, Instanbul, Turkey, June 2006, pp. 573–578.

[15] K. V. Mardia, "Measures of multivariate skewness and kurtosis with applications," *Biometrika*, vol. 57, no. 3, p. 519, 1970.

[16] C. J. Kowalski, "Non-normal bivariate distributions with normal marginals," *The American Statistician*, vol. 27, no. 3, pp. pp. 103–106, 1973.

[17] K. V. Mardia, "Assessment of multinormality and the robustness of Hotelling's T 2 test," *Applied Statistics*, pp. 163–171, 1975.

[18] ——, "Applications of some measures of multivariate skewness and kurtosis in testing normality and robustness studies," *Sankhyā: The Indian Journal of Statistics, Series B*, vol. 36, no. 2, pp. 115–128, 1974.

PUBLICATION RELATED TO THIS THESIS

[19] F. Mata, J. Aracil, and J. García-Dorado, "Automated detection of load changes in large-scale networks," in *Proceedings of International Workshop on Traffic Monitoring and Analysis*, 2009, pp. 34–41.

[20] F. Mata and J. Aracil, "Performance Evaluation of an Online Load Change Detection Algorithm," in *Second International Conference on Computer and Automation Engineering*, vol. 1, 2010, pp. 261–266.

[21] F. Mata, J. García-Dorado, and J. Aracil, "Multivariate fairly normal traffic model for aggregate load in large-scale data networks," in *Wired/Wireless Internet Communications*, ser. Lecture Notes in Computer Science. Springer Berlin / Heidelberg, 2010, vol. 6074, pp. 278–289.

[22] ——, "On the suitability of multivariate normal models for statistical inference based on traffic measurements," in *Passive and Active Measurement conference, Poster Session*, 2010, p. 1.

[23] ——, "Caracterización temporal de las demandas de ancho de banda en enlaces con alta agregación mediante un modelo normal multivariante *(*in spanish)," in *IX Jornadas de Ingeniería Telemática*, 2010, pp. 1–8.

[24] ——, "Detection of traffic changes in large-scale backbone networks: The case of the spanish academic network," *Comput. Netw.*, vol. 56, no. 2, pp. 686 – 702, 2012.

[25] F. Mata, P. Żuraniewsky, M. Mandjes, and M. Mellia, "Anomaly detection in VoIP traffic with trends," in *24th International Teletraffic Congress (ITC)* ***(Best Student Paper Award)***, Krakow, Poland, Sep. 2012, pp. 1–8.

[26] ——, "Anomaly detection in diurnal data," *Computer Networks (under review)*.

[27] F. Mata and J. Aracil, "A survey on anomaly detection taxonomies and techniques in networked environments," *IEEE Communications Surveys and Tutorials (under minor revision)*.