Measurement-based Admission Control for Real-time Traffic in IP Differentiated Services Networks

Stylianos Georgoulas, Panos Trimintzios, George Pavlou and Kin-Hon Ho

Abstract—**The primary role of admission control in Quality of Service enabled networks is to control the amount of traffic injected into the network so that congestion is avoided. We consider IP Differentiated services networks able to support real-time traffic and we present a Measurement-based Admission Control (MBAC) scheme that uses only measurements of aggregate bandwidth without keeping track of any per-flow information. Through simulations we show that the admission control scheme is relatively robust to traffic heterogeneity and measurement errors and that it compares favorably against other MBAC proposals found in the literature.**

Index terms— **QoS, Differentiated services, Admission control, Real-time traffic, Effective bandwidth**

I. Introduction

Real-time services have stringent delay, jitter and loss requirements. Differentiated services (Diffserv) is seen as the emerging technology to support IP Quality of Service (QoS) in a scalable fashion, without the inherent problems of Integrated services (Intserv), which require per-flow state information in the core network. In Diffserv, per-flow state is only kept at ingress routers, while in the core network, traffic with similar QoS requirements is grouped in one of the engineered traffic classes and forwarded in an aggregate fashion.

In order to provide QoS guarantees, a Diffserv network must exercise admission control [1] to control the amount of traffic injected into the network. Admission control comprises a set of actions required at the service instance establishment phase to check whether a service request is to be admitted or rejected. A new service instance should be admitted when the requested QoS can be satisfied without causing any QoS violation to the already established service instances.

The various admission control approaches can be divided into three categories: (a) Endpoint admission control (EAC), (b) Admission control using *a priori* traffic descriptors, and (c) Measurement-based admission control (MBAC).

Endpoint admission control is based on some metric applied on probing packets sent by the end host/application along the transmission path [2]. The end-to-end route should be the same for probing packets and flows. Setup delays may be high and, furthermore, simultaneous probing by many sources can lead to a situation known as *thrashing* [2]. That is, even though the number of admitted flows is small, the cumulative level of probe packets prevents further admissions.

In admission control using *a priori* traffic descriptors, it is assumed that a traffic descriptor is provided by the user or application for each flow. This approach achieves high network utilization when traffic descriptors used by the admission control scheme are tight [3]. Nevertheless, in practice, it suffers from several problems [1]. One of them is the inability of the user or application to come up with tight traffic descriptors. Another problem is that this traffic descriptor and the associated QoS guarantee define a contract between the application and the network. Therefore, the need to police based on this traffic specification arises, which is difficult for statistical traffic descriptors [1].

Measurement-based admission control tries to avoid the aforementioned problems by shifting the task of traffic characterization from the user to the network [4]. Instead of users explicitly specifying their traffic descriptors, the network attempts to "learn" the characteristics of existing flows through real-time measurements. This approach has a number of advantages. First, the user-specified traffic descriptors can be very simple, e.g. peak rate. Second, an overly conservative specification does not result in over-allocation of resources for the entire duration of the service session. Third, when traffic from different flows is multiplexed, the QoS experienced depends often on their aggregate behavior, the statistics of which are easier to estimate than those of an individual flow. However, relying on measured only quantities for admission control raises a number of issues that need to be considered, such as the estimation errors, flow level dynamics and memory related issues [4].

In order for an MBAC scheme to be successful in practice, it has to fulfill several requirements [1, 3].

Robustness: An MBAC scheme must ensure that the requested QoS is provided. This is not trivial, since measurement inevitably has some uncertainty, leading to admission errors. The QoS should also be robust to flow heterogeneity, time-scale fluctuations, as well as to heavy offered loads.

Resource utilization: The secondary goal for MBAC is to maximize resource utilization, subject to the QoS constraints for the admitted flows.

Implementation: The cost of deploying an MBAC scheme must be smaller than its benefits. In addition, the traffic characteristics required by the MBAC scheme should be easily obtained from the traffic sources and the network.

In this work we present a measurement-based admission control scheme for real-time traffic. We define as real-time traffic, sources that have a strict *delay* and *jitter* requirement and a bounded *packet loss rate* (PLR) requirement.

This work was undertaken in the context of the IST MESCAL research project, which is partially funded by the Commission of the European Union.

S.Georgoulas, P.Trimintzios,G.Pavlou and K.Ho are with the Centre for Communication Systems Research, University of Surrey, Guildford, Surrey, GU2 7XH, UK (email: {S.Georgoulas, P.Trimintzios, G.Pavlou, K.Ho}@eim.surrey.ac.uk).

P.Trimintzios is also with ICS-FORTH, PO Box 1385, GR-71110, Heraklion, Crete, Greece (email: ptrim@ics.forth.gr).

In our scheme, we assume that the *delay* requirement of the traffic aggregate has been taken into account in the provisioning stage. This means that the network provisioning processes configure appropriately small packet queues for the real-time traffic aggregate in order to keep the per-hop delay small. In addition, by manipulating the routing processes to choose paths with constrained number of hops, we can keep the overall edge-to-edge delay under given bounds.

According to [5], *jitter* can remain controlled in successive multiplexing queues as long as the flows are shaped to their nominal peak rate at the network ingress. Therefore, we assume that real-time traffic is conditioned and shaped based on the contracted peak rate.

Our assumption related to *packet loss*, is that packets are expected to be lost *only* at the first point of aggregation (ingress link), where the serialization of the various traffic sources takes place and which, according to [6], is currently considered as the most probable congestion point of a domain. We assume that further downstream inside the domain, real-time traffic aggregates are provisioned in a peak rate manner. This is feasible since, as stated in [7], in a common network configuration, backbone links are over-provisioned.

As a result of this provisioning process, and taking into account the routing behavior, at each ingress node we can have an estimate of the minimum bandwidth available for the real-time traffic aggregate from that ingress to each of the corresponding egress nodes. This available bandwidth is the *basis* for our admission control approach, which is employed at the edge (ingress) node of the first Diffserv aggregation point, for accepting real-time traffic sources on behalf of the entire Diffserv domain.

This paper is organized as follows: Section 2 presents our admission control scheme. In Section 3 we evaluate the performance of our scheme against other approaches found in the literature. Finally, in Section 4 we conclude, summarizing our findings and giving directions for further research work.

II. MBAC SCHEME

In this section we will present our Measurement-based Admission Control scheme, which relies *only* on a single traffic descriptor, the source's peak rate.

Given the diversity of Internet applications that might use real-time services, the use of more complex traffic descriptors in admission control, as stated in [8], to accurately characterize source traffic, is neither necessary nor plausible. Therefore, we assume that the only available traffic descriptor for use in admission control is the source's peak rate. This traffic descriptor is easy to police and even if not available, for sources described by a token bucket filter (r, b) an estimate $\hat{p}$ of it can be derived [8] using the equation:

$$\hat{p} = r + b / U \qquad (1)$$

where U is a user-defined averaging period.

In our MBAC scheme we adopt the bufferless statistical multiplexing approach. Bufferless multiplexing ensures that the traffic experiences minimal delay. In addition, the dynamics leading to an overload event in a bufferless system are much simpler than those of a buffered system [9]. The main disadvantage of using a buffer is that overflow probability depends on flow characteristics [10] and can only be controlled if these characteristics are known. We need to stress here that bufferless multiplexing is just a model abstraction [10]. For packetized traffic, as in IP networks, a small buffer for packet scale queuing is needed to take into account coincident packet arrivals from distinct flows [5].

For bandwidth manipulation we adopt the equivalent capacity approach. According to [11], when the effect of statistical multiplexing is significant, the distribution of the stationary bit rate can be accurately approximated by a Gaussian distribution. In [12] it is strongly suggested that the aggregation of even a fairly small number of traffic streams is usually sufficient for the Gaussian characterization of the input process. In that case, the effective bandwidth of the multiplexed sources is given by:

$$C \simeq m + a'\sigma \text{ with } a' = \sqrt{-2\ln(\varepsilon) - \ln(2\pi)} \qquad (2)$$

where m is the mean aggregate bit rate, σ is the standard deviation of the aggregate bit rate and ε is the upper bound on allowed loss probability.

A. Admission Control Logic

We assume that through provisioning and traffic engineering, at minimum C_{total} bandwidth is available edge-to-edge for the real-time traffic aggregate.

In our scheme, we assume that every time a source wants to establish a service instance, it signals this to the ingress node through a resource reservation protocol. A similar assumption can be made for the service termination. If the latter is not explicitly signaled, an alternative option could be to employ a time-out period as an indication of the service termination. In any case, at each point in time, the MBAC process at a single ingress point knows the number of active sources.

When a new service request arrives, we need to decide whether to allow the source to send traffic using the real-time traffic aggregate resources until the known egress point.

Initially, we need to calculate an appropriate time period, the measurement window, in which we need to take and use measurements for bandwidth estimations. The measured parameters are the mean rate of the offered load, $M_{measured}$, and the variance of the offered load, $\sigma^2_{measured}$, at the output queue of the ingress node. Having the measurements and the peak rate p_{new} of the new source, and by making the worst case assumption that the new source will be transmitting at its peak rate, we compute the estimated bandwidth C_{est} as follows:

$$C_{est} = M_{measured} + p_{new} + a'_{PLR}\sqrt{\sigma^2_{measured}} \qquad (3)$$

where a'_{PLR} is computed as in (2), based on the target PLR bound of the real-time traffic aggregate. This value C_{est} is the estimated bandwidth used in the admission control criterion of our scheme.

B. The Measurement Window

We define the measurement window w, as the time interval within which the offered load is taken into account for deriving the required measurements. In a similar fashion to [13], we use the following expression for the measurement window:

$$w = \max(DTS, w') \quad (4)$$

In (4), DTS represents the Dominant Time Scale. DTS is the most probable time scale over which overflow occurs. In [12], the authors describe a systematic way to derive DTS using real-time measurements, with the assumption that the input process to the multiplexing point in the network is Gaussian. This is by definition our assumption when employing (2), therefore we use this method in order to estimate the DTS. DTS, as computed in [12], is a function of the mean rate, the variance of the offered load and the output buffer size. The reader should recall at this point that even though we employ the bufferless multiplexing approach, a small output buffer is still required for packet scale queuing, as explained in the previous section. This value for the output buffer is involved in the estimation of the DTS.

Let w' represent the mean inter-departure delay [4], defined as follows (Little's formula):

$$w' = \frac{h_{avg}}{N_{active}} \quad (5)$$

where N_{active} is the number of simultaneously active sources and h_{avg} is their average duration.

Since we assume in our scheme, that the service establishment and termination is signaled to the ingress nodes, the average duration of the sources can be easily obtained.

We select as measurement window the mean inter-departure delay, i.e. the time interval within which the system can be considered stationary -no flow departures-, unless this time interval is not long enough to capture the time-scale fluctuations of the aggregate traffic stream. This can happen in case of long-range dependent traffic. In this case and in order to enable the network to react to these traffic fluctuations, we use DTS as the value of the measurement window.

C. The Admission Control Criterion

Given the allocated bandwidth for the real-time traffic aggregate from edge-to-edge is C_{total}, and having computed the estimated bandwidth C_{est}, the admission control criterion in our scheme becomes:

$$\begin{aligned} &\mathit{If} \quad (C_{est} \times APF) \le C_{total,} \quad \mathit{admit} \\ &\mathit{If} \quad (C_{est} \times APF) > C_{total,} \quad \mathit{reject} \end{aligned} \quad (6)$$

where *APF* is an Admission Policy Factor we involve in the admission control criterion.

The use of *APF* reflects how strict the admission control should be. Setting the *APF* can be based on simple heuristics or ad hoc engineering methods. In the following section we describe an example heuristic approach for setting *APF*. In our heuristic, we take into account two issues: (a) the traffic source heterogeneity, and (b) the effect of measurement errors.

D. The Admission Policy Factor (APF)

The reason for introducing *APF* is to reflect the provider's policies. This means that appropriately tuning the *APF* can lead to a more conservative or a more relaxed admission control criterion. In our case we give a heuristic formula for *APF* with which we address two important issues that need to be taken into account in the admission control decision.

The first issue is that the aggregate traffic stream might have characteristics that do not suit the effective bandwidth formula (2). This, for instance, can happen if the stream is composed of a small number of very bursty connections with high peak rates and low utilizations [11].

To account for this, we use an exponential ON/OFF source, with mean and standard deviation (m_{ref}, σ_{ref}) as a model source for engineering reasons (*reference source*). The reason for the specific selection is that exponential ON/OFF sources are representative models for VoIP traffic, which is likely to be a big part of the traffic carried by real-time traffic aggregates and their traffic characteristics suit the effective bandwidth formula (2). Furthermore, exponential ON/OFF sources are short-range dependent, which means that their traffic characteristics are more easily captured within the given measurement window. We define as *reference trunks* (T_{ref}) the number of simultaneously established reference sources that can fit in C_{total}, according to (2), for a given bound on packet loss rate.

When a new request arrives, having measured the mean rate $M_{measured}$ and the variance $\sigma^2_{measured}$ of the offered load, we calculate the number N_m of the reference sources, whose aggregate mean rate is equal to or greater than $M_{measured}$. We also calculate the number N_σ of the reference sources, whose aggregate variance is equal to or greater than $\sigma^2_{measured}$. That is, N_m and N_σ satisfy the following relationships:

$$N_m = \left\lceil \frac{M_{measured}}{m_{ref}} \right\rceil \text{ and } N_\sigma = \left\lceil \frac{\sigma^2_{measured}}{\sigma^2_{ref}} \right\rceil \quad (7)$$

Having estimated N_m and N_σ, we compute their mean value N_{ref}:

$$N_{ref} = (N_m + N_\sigma)/2 \quad (8)$$

This value represents a rough estimate of the number of reference sources that produce load with characteristics (mean rate and variance) similar to the ones measured.

To compensate for the above, we set *APF* to be proportional to the quantity (N_{ref} / T_{ref}).

The second issue that needs to be taken into account with the policy factor is the effect of measurement errors. As shown in [4], the *certainty equivalence* assumption, i.e. that the measured parameters represent the real traffic, can heavily compromise the performance of an MBAC scheme. The stringent the PLR requirement, the easier it is to violate it due to measurement errors. In the case where only aggregate bandwidth information is available through measurements, as in our scheme, the degradation in performance can be mainly attributed to errors in the estimation of the variance [1]. With non-negligible probability the variance can be underestimated. To compensate for the measurement uncertainty, we proceed as follows: given (2), for a specific target PLR, we set *APF* to be proportional to the quantity $\dfrac{\sqrt{-2\ln(PLR) - \ln(2\pi)}}{\sqrt{-2\ln(PLR_{ref}) - \ln(2\pi)}}$.

That is, we inflate the part of equation (2) that relates to the variance estimation, based on a reference PLR level. By setting PLR_{ref} to be higher as a value than PLR, we ensure that the more stringent the PLR requirement, the greater the value of this quantity. This reference PLR can be set by policy to adjust the conservativeness of the MBAC scheme.

Combining the two aforementioned quantities, the final expression for the admission policy factor that is adopted is:

$$APF = (N_{ref} \,/\, T_{ref}) * \frac{\sqrt{-2\ln(PLR) - \ln(2\pi)}}{\sqrt{-2\ln(PLR_{ref}) - \ln(2\pi)}}\} \quad (9)$$

We also set $APF = 1$ when its computed value is less than 1. That is, we employ *APF* in a conservative way.

APF can be considered as a tuning parameter. Although we derive *APF* somehow heuristically, based on intuition rather than mathematical analysis, one should take into account that all MBACs employ additional tuning parameters [1].

III. Performance Evaluation

In order to evaluate the performance of our admission control scheme, we run simulations using the network simulator *ns* [14] using the dumbbell topology of Fig. 1.

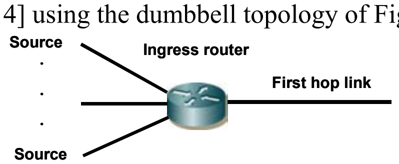

Fig. 1. Simulation topology.

We configure the output queue to hold a maximum of 5 packets and we set the reference PLR equal to 0.01. We use scenarios with the target packet loss rate for the aggregate real-time traffic being equal to 0.01 and 0.001.These bounds represent typically acceptable PLR values for the VoIP service and for real-time applications in general, according to [15, 16].

We set the output link capacity to correspond to T_{ref} equal to 100. That means that the output link capacity is 3.33Mbps for the target PLR 0.01 case and 3.56Mbps for the target PLR 0.001 case. All the results are based on averages of simulations for 20 random seeds, each for a total of 4100 seconds, using the first 500 seconds as a warm-up period.

In order to test the *robustness* of the scheme with respect to traffic heterogeneity and long-range dependency, we use both VoIP and Videoconference traffic. For VoIP traffic we use an ON/OFF source model with exponentially distributed ON and OFF times, having a peak rate of 64kbps. The mean durations for the ON and OFF periods are 1.004sec and 1.587sec respectively [17]. This model is also used as the *reference source* model. The active time of the VoIP sources is exponentially distributed with an average of 300sec. For Videoconference traffic we use an H.263 coded trace from [18] with peak rate 332.8kbps. The H.263 format has been widely employed to model videoconference traffic, e.g. see [19]. The active time of the Videoconference sources is exponentially distributed with an average of 180sec. For both VoIP and Videoconference sources, the activation processes are Poisson arrival processes. For the cases where both VoIP and Videoconference sources are employed (mixed traffic), the averages of their activation rates follow a ratio of 2:1.

In order to test the *robustness* of the scheme with respect to offered load, we test varying load conditions ranging from 0.5 to 5, where 1 (*reference load)* corresponds to the load incurred by a source activation rate equal to 1000 VoIP sources/hour.

In order to compare the performance of our scheme against existing MBAC proposals, we implement a representative algorithm from the literature. This algorithm is an implementation of the scheme described in [20] as Rate Envelope Multiplexing (REM), with adaptive weight factor and no histogram update. The reasons for the selection of the specific scheme for comparison are that: (a) REM also makes the zero buffer approximation with respect to statistical multiplexing and (b) implementation-wise, similar to our scheme, it requires only aggregate bandwidth measurements and the peak rate of the source requesting admission in order to derive the admission control decision.

As stated in [21], any admission control scheme must address the trade-off between packet loss and utilization, and these are the metrics we use for the evaluation of our algorithm (we call it GEO) and the scheme in [20] (we call it ZUK).

We consider two different cases for the sources that request permission to use the real-time traffic aggregate resources. The cases we examine are: (a) Videoconference sources only and (b) Mixed VoIP and Videoconference sources.

A. Videoconference Sources

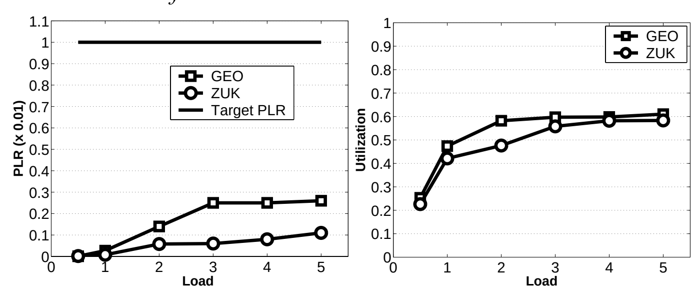

Fig. 2. Achieved PLR and utilization for target PLR 0.01.

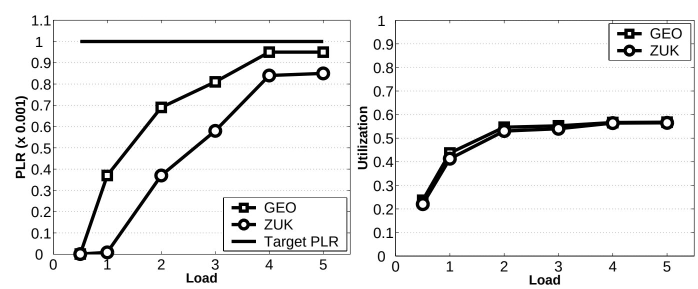

Fig. 3. Achieved PLR and utilization for target PLR 0.001.

For Videoconference traffic, both GEO and ZUK achieve the target PLR for all load conditions with GEO being slightly less conservative than ZUK. For target PLR 0.01, both schemes are unnecessarily conservative, which can be partly attributed to the stringent admission control criterion (both schemes make the worst case assumption that the new source will be transmitting at its peak rate) and the high peak rate of the Videoconference sources. Regarding utilization, the performance of GEO is slightly better than that of ZUK, as a result of the less conservative admission control criterion.

The reader should recall at this point that the objective is not to achieve the lowest PLR possible (if that was the case, a simple peak rate admission control scheme would suffice), but to keep the achieved PLR below the target PLR value and maximize the utilization at the same time.

B. Mixed VoIP and Videoconference Sources

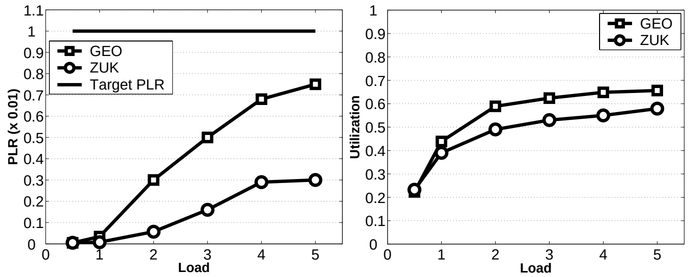

Fig. 4. Achieved PLR and utilization for target PLR 0.01.

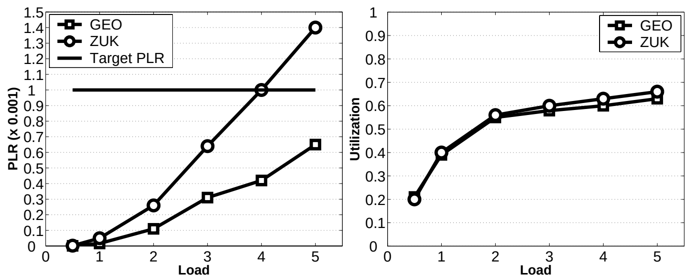

Fig. 5. Achieved PLR and utilization for target PLR 0.001.

For mixed traffic, both GEO and ZUK achieve the target PLR 0.01 with GEO being less conservative, achieving, therefore, a higher utilization. For target PLR 0.001, GEO achieves this PLR for all load conditions. ZUK violates this PLR for load conditions more than 4 times the *reference load*.

Compared to the previous case, where we have Videoconference sources, both schemes are less conservative. This can be attributed to the low peak rate and high activation rate of the VoIP sources compared to the respective peak rate and activation rate values of the Videoconference sources.

In all cases, for both GEO and ZUK we observe an increase in the achieved PLR for higher load conditions. This is anticipated [4] because since they both rely on measurements, every new admission request carries the potential of making a wrong decision. This means that a high source activation rate is expected to have a negative effect on performance.

IV. Conclusions

In this paper we propose a measurement-based admission control scheme for real-time traffic in IP Differentiated services networks. We assume that an instance of our MBAC scheme runs at every ingress node, serving real-time traffic, entering the Diffserv domain through that ingress node, towards any of the domain's egress nodes.

We show through simulations that the scheme is relatively *robust* to flow heterogeneity, time-scale fluctuations, as well as to heavy offered loads.

Furthermore, the scheme achieves satisfactory *utilization* and compares well against existing measurement-based approaches for the same simulation setup.

Finally, we have to mention that our scheme is also easy to *implement*. It only relies on aggregate bandwidth information and does not require any per-flow information state. In addition, the scheme requires the use of signaling only from the sources to the ingress nodes, but not further downstream, since it is based on provisioned Diffserv information.

In our current research efforts, we are focusing on extending our MBAC scheme for inter-domain traffic; that is traffic that crosses more than one domains. For the inter-domain traffic case, since peering links at the border routers between neighboring domains are often bottlenecks [6], they cannot be considered over-provisioned. Therefore, MBAC should also take into account the state of these links before deriving the admission control decision. We are investigating what type of information needs to be measured in this case to depict the state of the peering links and how this information can be incorporated in our MBAC scheme.

References

[1] M. Grossglauser and D. Tse "A Time-Scale Decomposition Approach to Measurement-Based Admission Control", IEEE/ACM Transactions on Networking, August 2003.

[2] L. Breslau, E. Knightly, S. Shenker, I. Stoica and Z. Zhang "Endpoint Admission Control: Architectural Issues and Performance", SIGCOMM 2000.

[3] G. Mao and D. Habibi "Loss Performance Analysis for Heterogeneous ON-OFF Sources with Application to Connection Admission Control", IEEE/ACM Transactions on Networking, February 2002.

[4] M. Grossglauser and D. Tse "A Framework for Robust Measurement-Based Admission Control", IEEE/ACM Transactions on Networking, June 1999.

[5] T. Bonald, A. Proutiere and J. Roberts "Statistical Performance Guarantees for Streaming Flows using Expedited Forwarding", IEEE INFOCOM 2001.

[6] A. Akella, S. Seshan and A. Shaikh "An Empirical Evaluation of Wide-Area Internet Bottlenecks", ACM Internet Measurement Conference 2003.

[7] G. Iannaccone, M. May, and C. Diot "Aggregate Traffic Performance with Active Queue Management and Drop from Tail", Computer Communications Review, July 2001.

[8] S. Floyd "Comments on Measurement-based Admission Control for Controlled-Load Services", July 1996, Lawrence Berkeley Laboratory Technical Report.

[9] D. Tse and M. Grossglauser "Measurement-based Call Admission Control: Analysis and Simulation", IEEE INFOCOM 1997.

[10] T. Bonald, S. Oueslati-Boulahia and J. Roberts "IP traffic and QoS control: the need for a flow-aware architecture", World Telecommunications Congress, September 2002, Paris, France

[11] R. Guerin, H. Ahmadi, and M. Naghshieh "Equivalent Capacity and its Application to Bandwidth Allocation in High-Speed Networks", IEEE Journal on Selected Areas in Communications, September 1991.

[12] D. Eun and N. Shroff "A Measurement-Analytic Approach for QoS Estimation in a Network Based on the Dominant Time Scale", IEEE/ACM Transactions on Networking, April 2003.

[13] S. Belenki "An Enforced Inter-Admission Delay Performance-Driven Connection Admission Control Algorithm", ACM SIGCOMM 2000.

[14] K. Fall and K. Varadhan "The *ns* manual" (www.isi.edu/nsnam/ns/ns_doc.pdf).

[15] I. Frigui "Services and Performance Requirements for Broadband Fixed Wireless Access", IEEE P802.16 Broadband Wireless Access Working Group.

[16] T. Chaded, "IP QoS Parameters", TF-NGN, November 2000.

[17] C. Chuah, L. Subramarian, and R. Katz "Furies: A Scalable Framework for Traffic Policing and Admission Control", May 2001, U.C Berkeley Technical Report No. UCB/CSD-01-1144.

[18] http://www-tkn.ee.tu-berlin.de/research/trace/trace.html

[19] M. Diaz, D. Garduno, T. Gayraud and S. Owezarski "Multimedia Multicast Protocols Based on Multimedia Models", MMM 2001.

[20] T. Lee and M. Zukerman "Admission Control for Bursty Multimedia Traffic", IEEE INFOCOM 2001.

[21] R. Gibbens and F. Kelly "Measurement-based connection admission control", 15th International Teletraffic Congress, June 1997.