Efficient Call Admission Control Methods in DiffServ Architecture

Angelos Michalas, Malamati Louta and Vassili Loumos
National Technical University of Athens, School of Electrical and Computer Engineering, Athens, GREECE

***Abstract*— In order to achieve absolute QoS guarantees in the DiffServ architecture, admission control procedures have been developed. Their role is to ensure that the admittance of a new flow into the network does not violate service commitments of already established flows and the network can satisfy the constraints of the new flow. In this paper we discuss related work of parameter and measurement based admission control techniques, while a set of indicative results of their performance is provided.**

I. INTRODUCTION

Service differentiation is considered to be of outmost importance for QoS provisioning in IP networks, due to the high variations of the connection requirements posed by Internet users and the statistical in general nature of the generated traffic, which the last years is presenting an exponential increase. The research community has concentrated on two different techniques to provide QoS differentiation to customers of packet switched networks. First, the Integrated Services (Int-Serv) [1] approach. Second, the Differentiated Services (DiffServ) [2] approach. The major difference between Int-Serv and Diffserv architecture is the granularity of service differentiation.

The IntServ concept lies on resource reservation concept, while it is based on connection admission control and packet scheduling [1]. Each application requests levels of service in terms of service rate or end-to-end delay. The network accepts or rejects requests according to its resources availability. In Intserv architecture, each connection is strictly controlled both by admission control at connection establishment time and packet scheduling during the lifetime of the connection. Specifically, at establishment time the necessary resources for the new connection are allocated, and during its lifetime, the connection is policed to ensure that potential abnormal behavior does not affect other connections.

However, the Int-Serv approach faces problems concerning scalability and manageability, since all routers must maintain per-flow state information. This lack of scalability is, to a large extent, being addressed within the DiffServ architecture [2]. The main strength of DiffServ is that it allows IP traffic to be classified into a finite number of service classes that receive different routing treatment. Routers at the network edges classify packets into predefined service classes based on the demand requirements and characteristics of the associated application. Core routers forward each packet according to a class based scheduling policy. This way, the model provides service differentiation on each node for large aggregates of network traffic. DiffServ achieves scalability and manageability by providing quality per traffic aggregate and not per application flow.

In DiffServ architecture, an admission control scheme is used to provide QoS guarantees as absolute bounds of specific parameters such as bandwidth, packet transfer delay, packet loss rate, or packet delay variation (jitter). A connection request is rejected if sufficient resources are not available in the network so as to provide the desirable assurances. There are two basic approaches to admission control [3]. The first, which is called *parameter-based approach*, computes the amount of network resources required to support a set of flows given *a priori* flow characteristics. The second, *measurement-based approach*, relies on measurement of actual traffic load in order to make admission decisions.

Parameter-based admission control algorithms can be analyzed by formal methods. Measurement-based admission control algorithms can only be analyzed through experiments on either real networks or a simulator. A key difficulty encountered in most parameter based approaches is their requirement for maintaining state information per traffic flow on each node (e.g., traffic parameters, QoS class). Consequently, due to the corresponding signaling and computational demands, there are fundamental limits to the scalability of such admission control algorithms, and hence limitations to their applicability over large-scale networks such as the Internet are posed. On the other hand, measurement-based admission control algorithms are based on source behavior, which is not static in general, thus service commitments made by such algorithms can never be absolutely accurate.

The aim of this paper is to further improve the scalability and manageability of an IP network for ensuring QoS service provisioning. Three admission control methods within a DiffServ architecture have been selected from relative research literature and applied to an extensive set of experiments in order to provide indicative evidence of their effectiveness. The rest of the paper is organised as follows. In section II, the admission control algorithms are briefly presented, while in Section III, a set of results, indicative of their performance is given. Finally, in Section IV conclusions are drawn.

II. ADMISSION CONTROL ALGORITMS

In this section the admission control schemes that have been adopted by the authors will be briefly described. The first one exploits the parameter based admission control approach of *sink trees* [4], while the second and the third are based on measurement based admission control. Specifically, the second one adopts the *arrival/service envelope* scheme [5], while the third one is based on the *out of bound dropping* notion [6]. All three methods are characterised by the following properties: *scalability* (since the overhead introduced is independent of the number of flows in the system), *effectiveness* (since the system with a high probability accepts a new flow if resources are available) and *compatibility* (since communication infrastructure modifications, such as the architecture of routers, signaling protocols, or packet formatting, are not required).

A. Parameter Based Admission Control

Following the DiffServ model, at the output link of each router, certain percentage of bandwidth is reserved

for individual traffic classes. Let a_i denote the percentage of bandwidth reserved for class i. Admission control ensures that the bandwidth usage of individual classes does not go beyond the pre-specified reserved portion. This is necessary so as to provide isolation among classes and hence to guarantee end-to-end flow delays in each class. For a new flow requesting to be served, the admission control algorithm should check whether the bandwidth allocation is or is not violated.

Since flows require resources on a sequence of nodes in the network, appropriate *signaling* must be in place so as to synchronise the admission control. Independently of whether the signaling is centralized (e.g., using a bandwidth-broker [2]) or distributed (such as in RSVP), the overhead in case of high flow establishment activity is enormous. A scalable resource management approach must thus be able to make admission decisions with high accuracy, while avoiding both numerous message counts and centralized decision entities. The deployment of sink trees [4] may minimise the signaling overhead at runtime.

Sink trees aggregate connections according to their egress nodes. The root of a sink tree is then the egress router, and the leaves are the ingress routers. By allocating resources so that for each ingress router it is known how many resources are available for each path towards each egress router, the admission control can be immediately performed at the entrance of the network. Since each egress node has its own sink tree, every possible pair of source and destination node has its own unique path in a sink tree.

The local delay suffered by packets belonging to a class k at an output link of router n may be formulated as following ([4]).

$$d_{k,n} = \frac{\sum_{l=1}^{k}(T_l + \rho_l Y_{l,n})\frac{a_l}{\rho_l} + (\sum_{l=1}^{k} a_l - 1)\frac{a_k(T_k + \rho_k Y_{k,n})}{\rho_k (N - a_k)}}{1 - \sum_{l=1}^{k-1} a_l} \quad (1)$$

$$Y_{l,n} = \max_{Path \in S_{l,n}} \sum_{j \in Path} d_{l,j} \quad (2)$$

where $S_{l,n}$ is the set of all paths traversed by class k packets before arriving at router n, T_k denotes the burst size of a class k traffic flow at the ingress routers, ρ_k is the average rate of a class k traffic flow, a_k denotes the percentage of bandwidth reserved for class k, and N is the number of input links contributing to the output link of router n. At this point it should be noted that the source traffic of a flow is controlled by a leaky bucket with parameters (T_k, ρ_k). Additionally, it is assumed that class i has been attributed with higher priority than class $i+1$.

Worst-case delay experienced by any flow of class k at a particular output link of a router may be computed by equation (1), considering the allocation of the reserved bandwidth portion for every individual class on each router's output link. The formulae depends only on values of T, ρ, a and N, while the number of flows that are admitted and pass through the output link is not taken into account. If T and ρ values are the same for all flows of a class, end-to-end delay that can be experienced by any flow of class k in the system can be computed off-line given $d_{k,n}$ and route information. This may be accomplished by summing up local delays $d_{k,n}$ corresponding to output links of routers along the path of that flow. Thus, it can be examined off-line whether the delay requirement of a class k flow is satisfied or not, given the bandwidth allocation of service classes on the links. In such a case, admission control during flow establishment is limited to examining if enough bandwidth is available on the links along the path of the flow.

B. Measurement Based Admission Control

A key difficulty encountered with parameter based admission control approaches is their requirement for coordination and maintenance of state information for all traffic flows on each network node. Measurement-based admission control techniques provide a solution to this problem via the management of *aggregate* traffic. Such algorithms allocate resources according to measured properties of the aggregate flow rather than user-specified properties of individual flows. Admission control decisions are made at edge routers (i.e., at a flow's ingress and/or egress router), without maintaining per-flow state. Thus, coordination of state among routers is not required. In this section two measurement based admission control systems ([7],[6]) will be highlighted.

1) Based on Arrival and Service Envelopes

This technique [7] exploits the notion of *envelopes* [5] to accurately characterize and control both arrivals and services in a general way. The network is regarded as a "black box", without particular knowledge of its service discipline, cross traffic, load, etc.

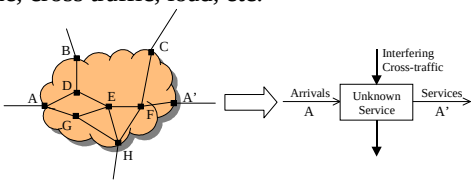

Figure 1. Blackbox system abstraction

The arrival/service envelope for a class is defined as the maximum arrival/minimum service rates of length τ measured at the path's ingress/egress nodes on successive windows of length t (where $t = \tau \cdot k$, $k = 1,2,...$). $\overline{R(t)}$ denotes the mean and $\sigma^2(t)$ the variance of the arrival peak rates over M timeslots of length t. Similarly, $\overline{S(t)}$ denotes the mean and $\psi^2(t)$ the variance of the minimum service rate over M timeslots of length t, when the class is backlogged (i.e., there is at least one packet of that class to be served). A new flow requesting admission to the class with peak-rate envelop $r(t)$ is accepted with delay bound D if for all interval lengths $0 \le t \le T$ the following inequality stands:

$$t\overline{R(t)} + tr(t) - \overline{S(t+D)} + \alpha\sqrt{t^2\sigma^2(t) + \psi^2(t+D)} < 0 \quad (3)$$

The proof of (3) can be found in [7].

2) Based on Probing

According to measurement based admission control techniques based on probing explored in [6], the traffic source or the ingress router probes the network by sending probe packets at the data rate it would like to reserve and recording the resulting level of packet losses or *Explicit Congestion Notification* (*ECN*) marks [8]. The flow is accepted only if the loss or marking percentage is below a predefined threshold value. Assuming that the queueing delays are likely to be quite small, the quality of service is measured strictly in terms of packet loss; the goal is to make this loss rate small but not to give any precise assurances of its level. Thus, to gain admission, a flow sends its probe packets for some period of time (usually many multiplies of e_i^{-1}, measured in packet transmissions) and measures the resulting loss fraction; the flow is admitted only if the probe loss fraction is below threshold value e_i. Small value of parameter e_i in essence means

extremely long probe times, resulting in a significant amount of wasted bandwidth and a substantial delay in data traffic transmission. Thus, a choice exists between long set-up times and small loss fractions, or short set-up times but somewhat higher loss fractions.

The main design options for the probing algorithms are whether to probe in-band or out-of-band (i.e., probe packets have the same or lower priority as the admitted controlled traffic, respectively) and whether to signal congestion with packet drops or congestion marks [6]. Thus, there are four basic design choices: dropping in-band, dropping out-of-band, marking in-band, and marking out-of-band. Dropping in-band is the simplest scheme, and requires only a rate-limited priority scheduler to separate admission-controlled traffic from best-effort traffic. The in-band marking scheme is very similar to that proposed in [9] and requires simulating a virtual queue and the use of ECN bits. The out-of-band dropping scheme is similar to that proposed in [10] and requires three levels of priority (one for admission controlled data, one for probes, and one for best-effort traffic). With out-of-band probing the data packet loss fraction is substantially lower than the probe packet loss fraction. Thus, one can have a reasonably sized e_i, with its corresponding reasonable set-up delays, and still achieve low data losses in contrast to the in-band dropping. The out-of-band marking scheme is a hybrid method consisting of the latter two approaches.

III. EXPERIMENTAL RESULTS

In this section, some indicative results are provided in order to assess the framework presented, which allows for efficient call admission control. Specifically, the results attained indicate the efficiency and the effectiveness of the three different admission control schemes.

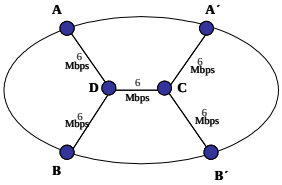

Figure 2. Simulation Topology

In order to evaluate the performance of the proposed framework of this paper we used NS2 network simulator [11] developed by National Berkley Labs as the simulation platform. Figure 2 shows the topology used in the simulations of this section. Specifically, the network consists of six nodes each with link capacity 6 Mbps. The packet length is taken equal to 1 KByte. Additionally, for all experiments conducted, at least two service classes and traffic types have been considered. *Class 1* packets are generated by Pareto sources with mean on and off time 360 ms and shape parameter alpha 1.8. *Class 2* packets are generated by *Constant Bit Rate (CBR)* sources giving aggregate traffic of 1 Mbps. Moreover, the network nodes employ *Class Based Queueing (CBQ) scheduling* [12] with *Class 1* having higher priority than *Class 2*, which is considered as the best effort (BE) class. Service rate allocations are taken equal to 0.83 and 0.17 for *Class 1* and *2*, respectively. Nodes A, B, A´, B´ are acting as edge nodes, while nodes C and D as core nodes.

Flows of *Class 1* traverse nodes A-D-C-A´, while *Class 2* flows have as ingress router node B and egress node B´ and are used as background traffic. For evaluating the admission control methods the following scenario is considered. A couple of Pareto sources of *Class 1* have already been admitted giving total peak rate 4 Mbps and average 2 Mbps. Four simulation experiments have been conducted. On each experiment a new Pareto source of *Class 1* requests admission with peak rates 1 Mbps, 1.5 Mbps, 1.75 Mbps and 2.5 Mbps, respectively. The packet delay requirement for this source is set equal to 100 msec. Table I presents the average network load, the average packet delay and the packet loss of *Class 1* traffic measured for all the experiments when the new flow is also admitted. The queueing delays per packet of *Class 1* for the four experiments are depicted in Figure 3 (a)-(d).

TABLE I. REQUESTING FLOW CHARACTERISTICS

Peak rate of new flow (Mbps)	Average rate of new flow (Mbps)	Average Network Utilization	Average packet delay (msec)	Packet loss
1	0,5	0,63	3,52843	2
1,5	0,75	0,705	28,0513	39
1,75	0,875	0,7425	99,6606	154
2,5	1,25	0,855	800,372	284

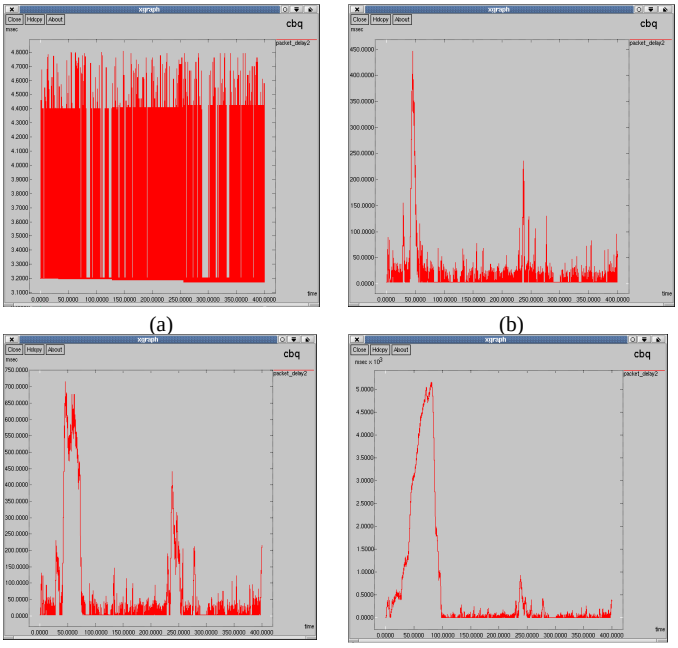

Figure 3. Individual packet delays when the flow with peak rate a)1Mbps, b)1.5 Mbps, c)1.75 Mbps, d)2.5 Mbps is admitted

Considering the parameter based approach, for the network topology depicted in Figure 2, the worst case delay for *Class 1* Pareto On-Off sources for path A-D-C-A´ may be estimated, by summing up the worst case local delays experienced by packets of *Class 1* flows along the path, which are computed using formulae (1)-(2). Considering *Class 1* Pareto flows with peak rate 4 Mbps and average rate ρ=2 Mbps, their burst size T may be computed in accordance with the methodology proposed in [13]. Specifically, the peak rates p of flows described by a token bucket filter (T, ρ) may be derived using equation: $p = \rho + \mathrm{T}/U$, where U is a user-defined average period. In the context of our experiments U is taken equal to 360 msec and the relative result is $T = 0.72$ Mb. As already mentioned, the portion of link bandwidth assign to *Class 1* for all routers is $a = 0.83$. The worst case path delay D is equal to $D = d_{1,A} + d_{1,D} + d_{1,C} + d_{1,A'} = 300\,ms$. Thus, according to the parameter based admission control scheme described in Section II, flows of *Class 1* can be admitted to the network as long as enough bandwidth is available on the links along the path and the packet delay requirement is not below 300msec. Additionally, from Figure 3 we may

observe that if the new admitted flow has peak rate 1 Mbps its average delay as well as its individual packet delay are far below 300ms. The second, third and fourth case (new flow's peak rate equals to 1.5 Mbps, 1.75 Mbps and 2.5 Mbps, respectively) give individual packet delays beyond 300 ms in cases where the incoming rate of *Class 1* flows is above the available bandwidth of the line.

TABLE II. TREATMENT OF FLOW ESTABLISHMENT REQUEST

Peak rate of new flow (Mbps)	Arrival envelope R1=4 Mbps	Arrival envelope R1=3.2 Mbps	Arrival envelope R1=2.4 Mbps
1	Accepted	Accepted	Accepted
1,5	Rejected	Accepted	Accepted
1,75	Rejected	Accepted	Accepted
2,5	Rejected	Rejected	Accepted

Considering the arrival/service envelope measurement based approach, for a measurement interval $t = 0.005$ sec the arrival envelope is $R_1 = 4$ Mbps, which approaches the aggregate peak rate of the accepted sources. For $t = 0.05$ sec the arrival envelope is $R_1 = 3.2$ Mbps, for $t = 0.1$ sec, $R_1 = 2.4$ Mbps and for longer measurement intervals the arrival envelope approaches 2 Mbps, which is the aggregate average rate of the admitted sources. Therefore, we may conclude that for small measurement intervals the arrival envelope approaches the peak rate of the sources, while for large measurement intervals the arrival envelope approximates the sources' average rate. Service envelope S_1 equals 5 Mbps for all measurement intervals due to the fact that the service rate portion allocated for *Class 1* to the CBQ scheduler over the 6 Mbps line is taken equal to 0.83. Equation (3) is used for admission control, with confidence level 99% and delay bound $D = 100$ msec. Because we set a large confidence level and small D the last term of (3) converges to 0. Table II presents for each experiment whether the new flow is accepted or not on the basis of (3) for the three distinct cases: $R_1 = 4$ Mbps, $R_1 = 3.2$ Mbps, $R_1 = 2.4$ Mbps. The average packet delays and the network utilization values suggest that peak arrival envelope $R_1 = 3.2$ Mbps is an adequate approximation for the arrival envelope to perform admission control. This is further justified by observing the individual packet delays depicted in Figures 3(a,b,c) where only few packets (less than 5%) experience packet delays of more than 100 msec when the new flow is accepted.

TABLE III. TREATMENT OF FLOW ESTABLISHMENT REQUEST

Probe rate = Peak rate of new flow(Mb)	Probe loss fraction	Accepted / Rejected flow
1	0	Accepted
1,5	1,33333E-05	Accepted
1,75	0,015885533	Accepted
2,5	0,073815409	Rejected

For the out-of-band dropping measurement based approach, the network nodes are modeled as a system with two priority queues for *Class 1* flows, one for the high priority accepted traffic and the other for the probes. The low priority queue can store a single probe packet and it is only served when the high priority queue is empty. On each simulation experiment the probe packet's rate is equal to the peak rate of the flow requesting admission and the probe duration is 1 sec. The target maximum loss fraction of probe packets is $2x10^{-2}$. Table III presents the loss fraction of probes measured, as well as whether the new flow is accepted or not for each simulation experiment. We observe that the same flows are accepted as in the admission control experiment based on arrival/service envelopes with arrival envelope $R_1 = 3.2$Mbps.

IV. CONCLUSIONS

Parameter based admission control approaches necessitate state information to be maintained on each node per traffic flow. This provides limitations to their scalability and applicability to large-scale networks. On the contrary, measurement based techniques rely on measurements of actual traffic in making admission decisions. They are able to make QoS statements without over provisioning, and without maintaining per flow state. However, due to the non-static in general behavior of the sources, they provide a statistical rather than a deterministic service.

In this paper one parameter based and two measurement based admission control algorithms were presented with characteristics their scalability with respect to the number of flows in the system, their effectiveness in network resources utilization and finally their compatibility to the network infrastructure of the DiffServ architecture. From the experiments performed we concluded that measurement based techniques represent a radical efficient solution to the limitations of the parameter based methods and offer more scalable and deployable approaches with slight deviations to absolute user requirements.

REFERENCES

[1] P. White, "RSVP and Integrated Services in the Internet: A Tutorial", *IEEE Communications Magazine*, May 1997.

[2] K. Nichols, V. Jacobson, and L. Zhang, "Two-bit differentiated services architecture for the Internet", IETF RFC2638, July 1999.

[3] S. Jamin, S. Shenker, Peter B. Danzig, "Comparison of Measurement-based Admission Control Algorithms for Controlled-Load Service", Proc. *INFOCOM '97*, April 1997.

[4] B. Choi, R. Bettati, "Efficient Resource Management for Hard Real-Time Communication over Differentiated Services Architecture", Proc. of the *7th IEEE RTCSA*, December 2000.

[5] J. Qiu and E. Knightly, "Measurement-based admission control with aggregate traffic envelopes", Proc. of the *10th IEEE ITWDC '98*, September 1998.

[6] L. Breslau, E. W. Knightly, S. Shenker, I. Stoica, and H. Zhang, "Endpoint admission control: Architectural issues and performance", Proc. of *ACM SIGCOMM'00*, pp. 57-69, September 2000

[7] C. Cetinkaya, V. Kanodia, and E. Knightly, "Scalable Services via Egress Admission Control", *IEEE TRANSACTIONS ON MULTIMEDIA*: Special Issue on Multimedia over IP, vol. 3, no. 1, March 2001.

[8] K. Ramakrishnan and S. Floyd, "A proposal to add explicit congestion notification (ECN) to IP", Internet RFC 2481, 1999.

[9] R. Gibbens and F. Kelly, "Distributed connection acceptance control for a connectionless network", Proc. of *ITC '99*, June 1999.

[10] V. Elek, G. Karlsson, and R. Ronngre, "Admission control based on end-to-end measurements", Proc. of the *IEEE INFOCOM*, March 2000.

[11] McCanne and S. Floyd, http://www-mash.cs.berkeley.edu/ns/ns.html Network Simulator, 1996.

[12] S. Floyd and V. Jacobson, "Link-sharing and resource management models for packet networks", *IEEE/ACM Transactions on Networking*, vol. 3, no. 4, pp. 365–386, August 1995.

[13] S. Floyd. "Comments on Measurement-based Admissions Control for Controlled-Load Service", *Computer Communication Review*, 1996.