Adaptive Ingress Admission Control for Differentiated Services

Hannan XIAO and K. C. CHUA
Dept of Electrical & Computer Engineering
National University of Singapore
4 Engineering Drive 3, Singapore 119260
{elexh, eleckc}@nus.edu.sg

Abstract - **Admission control is a critical element for supporting Quality-of-Service in networks. We propose and evaluate the performance of an adaptive ingress admission control scheme that is suitable for use in a Differentiated Services Internet backbone. The proposed scheme improves upon the egress admission control scheme by measuring the maximal arrival rate envelope at an ingress node and adding an adaptive adjustment scheme that dynamically adjusts the perceived network capacity in correlation with the rate at which a specified end-to-end delay bound is violated. Simulation results are presented to show that the proposed adaptive ingress admission control scheme is more effective than the egress admission control scheme.**

Index terms- admission control; arrival envelope; differentiated services; service envelope

I. Introduction

Admission control is a critical element for supporting Quality of Service (QoS) in communication networks. Its function is to decide whether or not to accept a new flow given the available network resources and the requirements of existing flows. The Differentiated Services (DiffServ) [1] architecture is a scalable QoS framework that has been proposed for the global Internet backbone, where core routers have little capacity to perform admission control related functions such as resource reservations and management on a per-flow basis. As such, any admission control algorithm that is proposed for a DiffServ backbone must be readily scalable.

DiffServ admission control proposals that have been reported in the literature can be classified into four categories: per-domain agent [2]; end-point probing [3], [4], [5], [6], [7]; hop-by-hop message exchange [8], [9]; and measurement of arrival/service envelopes at edge routers [10], [11]. Among these proposals, the egress admission control scheme [10] appears most promising in that it imposes little processing on core routers. Instead, information necessary to estimate available network resources to make admission control decisions is obtained by measuring the arrival and service envelopes at an egress router. The admission control algorithm is built on extreme value theory to characterize the distribution of the maximal arrival rate and minimum service envelopes. In addition, the scheme, unlike probing schemes, has low flow setup delays.

However, by measuring the packet arrival statistics at an egress node, the egress admission control scheme is not able to capture the full packet arrival statistics when packets are dropped in the core network. As a result, we have observed in our simulations, the scheme over-admitting flows which then leads to a significant number of packets violating their specified end-to-end delay bounds (i.e., QoS targets). To address this shortcoming of the egress admission control scheme, we propose a modification which measures the maximal packet arrival envelope at an ingress node. In addition, we introduce an adaptive adjustment scheme that dynamically adjusts the network capacity (as perceived by the ingress node when making the admission control decision) in correlation with the rate at which the specified end-to-end delay bound is violated. In this paper, we show using simulation results that our proposed adaptive ingress admission control scheme is more effective than the egress admission control scheme. Delay and delay violation are the main metrics studied.

We organize the rest of the paper as follows. We first briefly describe the egress admission control scheme in Section 2. Then in Section 3, we present the proposed adaptive ingress admission control scheme. Next, we present simulation results comparing the performance of the two schemes in Section 4. Finally, we conclude the paper in Section 5.

II. Egress Admission Control

Fig. 1 shows a simplified model of the egress admission control scheme [10]. A typical ingress-to-egress path in a DiffServ domain, shown in the upper part of the figure, is modeled as a "black box" with an unknown service discipline and cross-traffic that cannot be directly measured as shown in the lower part of the figure. The egress admission control model estimates the workload and service properties of the ingress-to-egress path via a general traffic and service *envelope* abstraction. Not only the egress node of this path estimates the available service by measuring service envelope, but also it obtains the arrival envelope by stamping the arrival time in packet head at the ingress node and assuming they have synchronized clocks. Only letting the egress router process the reservation request, this approach thus simplifies the admission control architecture.

Consider a traffic class between an ingress-egress pair. The measured maximum arrival envelope has mean $\overline{R}(t)$ and variance $\sigma^2(t)$, i.e., over successive measurement periods the average maximum number of arrivals is given by $t\overline{R}(t)$ and its variance is given by $t^2\sigma^2(t)$. Moreover, the measured minimum service envelope has mean $\overline{S}(t)$ and variance $\psi^2(t)$. Consider a new flow requesting admission to the class with peak-rate envelope $r(t)$. The flow is admissible with delay bound D and confidence level $\phi(\alpha)$ if

$$t\overline{R}(t)+tr(t)-\overline{S}(t+D)+\alpha\sqrt{t^2\sigma^2(t)+\psi^2(t+D)} < 0 \quad (1)$$

0-7803-7788-5/03/$17.00 ©2003 IEEE.

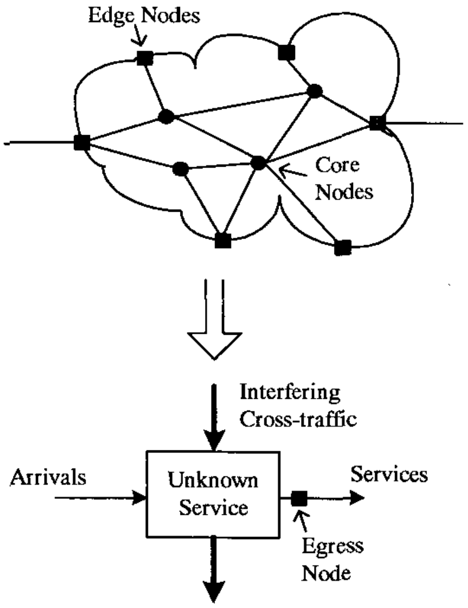

Fig. 1. Model of egress admission control system.

and

$$\lim_{t\to\infty} \overline{R}(t) + r(t) \leq \lim_{t\to\infty} \frac{\overline{S}(t)}{t} \tag{2}$$

where $\phi(\alpha) = exp(-exp(-(\alpha - \lambda)/\delta)$ is Gumbel distributed with mean $\mu = \lambda + 0.57772\delta$, and $\sigma^2 = \pi^2\delta^2/6$. Thus, α is set according to the required delay bound violation probability.

Intuitively, (1) is the admission requirements on available buffer, and (2) is the admission requirements on available bandwidth.

III. Adaptive Ingress Admission Control

Fig. 2 shows the system model of the proposed adaptive ingress admission control scheme. The "black box" with an unknown service and interfering crossing traffic is the abstraction of a typical ingress-egress path in a DiffServ domain; this is the same as in the system model of the egress admission control scheme in Fig. 1. Traffic arrives from the left side of the "box" where the ingress node at the border measures the aggregate traffic arrival envelope. Traffic departs out of the right side of the "box" where the egress node at the border measures the aggregate traffic service envelope. The egress node sends back periodically the service envelope information along with the measured values of QoS violation to the ingress node, which then uses this information to make the decision whether to accept or reject a new flow.

There are two major differences between the system models of the egress admission control (Fig. 1) and the adaptive ingress admission control (Fig. 2) schemes. First, the ingress node measures the traffic arrival envelope because only the ingress node sees all traffic arrivals to this path, including those that may be dropped along the path later on. Second, the egress node feeds back measured values of the service quality, viz., the delay violation probability, to the ingress node, which then adjusts the admission control conditions adaptively in order to meet the target QoS bounds.

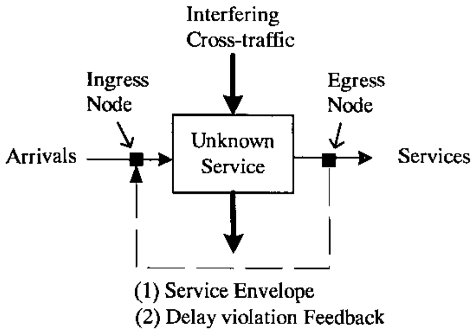

Fig. 2. Model of ingress admission control system.

It is aware that the ingress admission control scheme introduces extra traffic by sending the measured service envelopes and service quality violation values from the egress node to the ingress node. Each service envelope can be efficiently represented by 20 data type of "double", and the measured service quality violation can be efficiently represented by 4 data type of "double". Since each "double" data type takes up 8 bytes, the data length is $(20 + 4) * 8 = 192$ bytes. Assume that the measurement period is 1 second and the measurement results are sent from the egress node to ingress node per second, the bandwidth occupied by such extra traffic will be less than 2kbps, which is durable for each ingress-egress pair.

Consider a traffic class between an ingress-egress pair. The measured maximum arrival envelope has mean $\overline{V}(t)$ and variance $\tau^2(t)$ measured at the ingress node. The measured minimum service envelope at the egress node has mean $\overline{S}(t)$ and variance $\psi^2(t)$. Consider a new flow requesting admission to the class with peak-rate envelope $r(t)$. The flow is admissible with delay bound D if

$$t\overline{V}(t) + tr(t) - \overline{S}(t+D) + \alpha(t)\sqrt{t^2\tau^2(t) + \psi^2(t+D)} < 0 \tag{3}$$

and

$$\lim_{t\to\infty} \overline{V}(t) + r(t) \leq \lim_{t\to\infty} \frac{\overline{S}(t)}{t} \tag{4}$$

where $\alpha(t)$ is adjusted adaptively according to the required delay violation probability and the measured delay violation probability as elaborated below.

A. Delay Violation Control

$\alpha(t)$ is set to control the delay violation. However, this is very difficult to control due to factors including the quantization of the measured arrival and service envelopes, the discrete nature of the flows and their extreme burstiness. These factors are hard to predict or quantify, therefore, $\alpha(t)$ is set not only to the required violation probability but also the measured violation probability over time.

The adjustment of $\alpha(t)$ is as follows:

- When the measured violation probability is higher than the target violation probability, $\alpha(t)$ should be increased. The admission control conditions in (3) is then less likely to hold, resulting in fewer flows being admitted and the delay violation probability reduced.
- When the measured violation probability is lower than the target violation probability, $\alpha(t)$ should be decreased. The admission control conditions in (3) is then more likely to be satisfied, resulting in more flows being admitted and the delay violation probability increased.

Denote β_{target} as the targeted delay violation probability, and $\beta(t)$ as the measured delay violation probability. Then we have:

$$\begin{array}{llll} \alpha(t) & \uparrow & , \text{ if } & \beta(t) > \beta_{target} \\ \alpha(t) & \downarrow & , \text{ if } & \beta(t) < \beta_{target} \\ \alpha(t) & \rightarrow & , \text{ if } & \beta(t) = \beta_{target} \end{array} \tag{5}$$

Here, we calculate $\beta(t)$ as the running average of the delay violation probabilities over a series of measurements intervals (i.e., we discretize time to intervals). We use the exponential averaging method which can be expressed as follows:

$$\overline{\beta}_{N+1} = w \times \overline{\beta}_N + (1-w) \times \beta_{N+1} \tag{6}$$

In (6), β_N is the delay violation measured at the N^{th} time interval, $\overline{\beta}_N$ is the exponential average of β_N up to the N^{th} time interval. By using a constant value of w ($0 < w < 1$), independent of the number of past observations, we consider all past values of delay violations, but the more distant ones have less weightage.

B. Adaptive Control Algorithm

To satisfy the requirement of relationship between $\alpha(t)$ and $\beta(t)$ described in (5), we use the following to adjust the rates at which $\alpha(t)$ increases or decreases with $\beta(t)$:

$$\alpha_{N+1} = \begin{cases} \alpha_{initial} \times e^{\beta_N - \beta_{target}} & \text{if } \beta_N \leq \beta_{target} \\ \alpha_{initial} \times (\frac{\beta_N}{\beta_{target}})^2 \times e^{\beta_N - \beta_{target}} & \\ & \text{if } \beta_N > \beta_{target} \end{cases} \tag{7}$$

where $\alpha_{initial}$ is a constant. (7) is deliberately conservative in that it increases $\alpha(t)$ more rapidly than it decreases it, and it has an upper bound of α_{max}.

Fig. 3 shows an example of α_{N+1} changing with respect to β_N, where $\alpha_{initial} = 1$, $\beta_{target} = 0.04$ and $\alpha_{max} = 6$, respectively. The figure demonstrates that the function in (7) meets the requirements of (5).

IV. Performance Evaluation

The proposed adaptive ingress admission control scheme is evaluated by simulation using network simulator (*ns*). To facilitate performance compassion, the simulation setup is based on those used in the evaluation of the egress admission control algorithm in [12], [13] except that a total simulation period of 5000 seconds is used in our simulations.

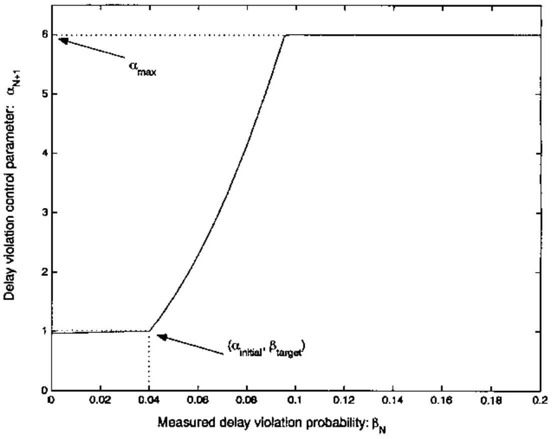

Fig. 3. Violation control algorithm.

A. Experiment 1: One Node

The first experiment consists of a single router, one traffic class, and no cross traffic. The topology is shown in Fig. 4. Traffic is sent from the main source hosts to the router, and then to the destination host. The single router functions as both ingress and egress router. The router is connected to the sources via faster links than that connected to the destination so that no queueing occurs in the hosts.

Table I lists the configurations of the network topology, traffic, and admission control schemes in experiment 1. Pareto on-off traffic flows are used because, with proper parameter settings, this traffic generator produces highly bursty traffic which, when aggregated, forms a traffic flow that exhibits self-similarity. Using the configuration in Table I, under a peak rate allocation scheme, 11 flows would be admitted, and to ensure stability, no more than 22 flows can be admitted.

In the adaptive ingress admission control scheme, $\alpha(t)$ adapts using (7). At every second, the router measures the arrival envelope, service envelope, and delay violation probability (also called delay outside bound). α in the egress admission control algorithm is set to 1.

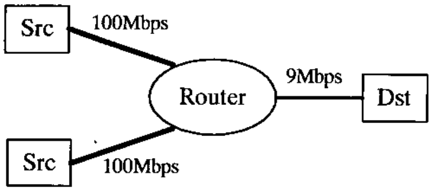

Fig. 4. One node experiment.

TABLE I

SIMULATION CONFIGURATIONS FOR EXPERIMENT 1.

Categories	Parameters	Values
Network	Topology	Fig. 4
	Link propagation delay	0.01ms for all links
Traffic	Type	Pareto on-off
	Packet size	1000 bytes
	Mean burst time	250 mseconds
	Mean idle time	250 mseconds
	Peak rate	800 kbps
	Mean rate	400 kbps
	Pareto shape parameter	1.9
	Flow life time	300 seconds
	Target delay requirements	5-60 mseconds
Adaptive ingress admission control	Delay violation control function	Equation (7)
	Target delay violation (β_{target})	0.04
	$\alpha_{initial}$	.1
	Parameter in running average algorithm (w)	0.5
	Period of measurement	1 second
Egress admission control	α	1
	Period of measurement	1 second
Simulations	Run time	5000 seconds

TABLE II

ADAPTIVE INGRESS ADMISSION CONTROL WITH EXPERIMENT 1.

Delay request (msec)	Average # of admitted flows	Utilization (%)	Mean delay (msec)	Maximum delay (msec)	Outside bound (%)
5	15.044	66.862	1.145	174.524	3.8587
10	15.931	70.803	1.817	174.524	3.9789
20	17.009	75.593	3.545	231.647	4.1486
30	17.683	78.591	6.848	373.432	5.0088
40	18.086	80.389	10.143	465.704	5.8456
50	18.068	80.303	16.480	872.415	6.4075
60	18.613	82.725	23.504	887.920	8.6375

TABLE III

EGRESS ADMISSION CONTROL WITH EXPERIMENT 1.

Delay request (msec)	Average # of admitted flows	Utilization (%)	Mean delay (msec)	Maximum delay (msec)	Outside bound (%)
5	15.317	68.077	1.326	174.524	4.9254
10	16.121	71.650	2.066	177.588	4.5591
20	17.478	77.680	6.656	500.781	7.7796
30	18.348	81.548	22.337	888.000	11.4401
40	19.243	85.526	36.695	887.988	18.3952
50	19.735	87.712	75.634	888.774	24.5778
60	20.174	89.660	118.081	888.114	32.9544

A.1 Simulation Results

Table II shows results for the adaptive ingress admission control scheme. Note that the algorithm shows statistical multiplexing gains even in this scenario of a moderate number of traffic flows by admitting up to an average of 18.61 flows. The average link utilization is in the range of 66.86% and 82.72%. Also, assigning different delay targets has the desired impact on measured performance, allowing mean delays in the range of 1.14ms and 23.50ms, and maximum delays in the range of 174.52ms and 887.92ms. Hence, the algorithm provides the basic mechanisms for performance differentiation in a multi-traffic classes network.

Delay violations occur due to over-estimation of available resources. The delay outside bounds range from 3.85% to 4.14% when the delay requests are from 5ms to 20ms; these are close to the target outside bound (4%). When the delay request are from 30ms to 60ms, the delay outside bounds range from 5.00% to 8.63%, and these are greater than the target outside bound. Therefore, the adaptive algorithm achieves the target delay violation probability in some cases but is not very acurate in other cases. This shows that the delay violation control function needs further investigation.

However, compared to the results of the egress admission control scheme shown in Table III, the adaptive ingress admission control scheme demonstrates improvements in controlling the delay outside bound. Table III shows that it is hard to control the delay violation in the egress admission control by setting a fix value for α. The different delay requests result in a wide range of outside bounds from 4.92% to 32.05%. In addition, note that the mean dealys in the last 2 delay request settings are excessive.

The maximum delay value reaches 888ms in some cases. This value is the delay of the last packet in the router buffer when the buffer is full. The value is $\frac{packetsize \times buffersize \times 8}{bandwidth} = \frac{1000 \times 1000 \times 8bits}{9Mbps} = 888.888ms$. Packets that arrive after the buffer is full are dropped. These dropped packets are ignored in the egress admission control scheme, resulting high delay outside bound in the last four rows of Table III.

B. Experiment 2: Ingress-Egress Pair

The topology of interest is shown in Fig. 5. Here, the ingress-egress path crosses an ingress router (Router A), a core router (Router B) and an egress router (Router C). There are five hosts connected to these routers. Traffic is generated among the hosts. Routers are connected via 9Mbps links (router A to B, router B to C); traffic sources are connected to routers via 100Mbps links (src and src1 to router A, src2 to router C) and traffic destinations are connected to the routers via 9Mbps links (router B to dst1, router C to dst and dst2). The configuration results in no queueing occurring in the source hosts. Each host generates multiple Pareto on-off

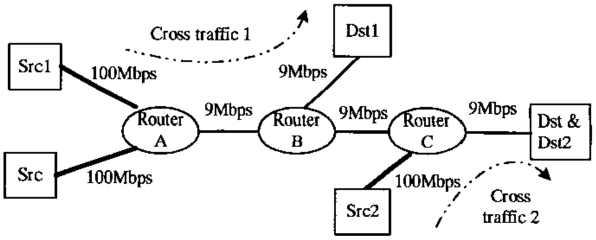

Fig. 5. Ingress-egress pair experiments.

traffic with parameters as listed in Table I except that the peak rate of each flow is 400 kbps and the mean rate is 200 kbps.

Three cases of interest are:

- Case 1: No cross traffic. Traffic is transmitted between hosts "Src" which is attached to the ingress router A, and "Dst" which is attached to the egress router C. No cross traffic is introduced to the ingress-egress pair. Thus, under a peak rate allocation scheme, 22 flows can be admitted, but to ensure stability, no more than 44 flows are admitted.
- Case 2: Cross traffic with congested ingress router. Cross traffic 1 is introduced from host "Src1 " to "Dst1". Cross traffic 1 is composed of 10 Pareto on-off flows. When one flow leaves the network after its life time, a new flow will be generated immediately. Cross traffic is accepted into the network without admission control. Admission control is only executed on the main traffic transmitted from host "Src" to "Dst". With the cross traffic in the network, no more than 34 flows can be admitted.
- Case 3: Cross traffic with congested egress router. Cross traffic 2 containing 10 Pareto on-off flows is introduced from host "Src2" to "Dst2". Main traffic is transmitted from host "Src" to "Dst". Similar to Case 2, with the cross traffic in the network, no more than 34 flows can be admitted.

The delay request of the main traffic is always 60 mseconds. The adaptive admission control and egress admission control schemes have parameters as listed in Table I.

B.1 Simulation Results

Table IV lists the results of the adaptive ingress admission control scheme with the three cases. For Case 1 without cross traffic, on average 38.64 flows are admitted which gives an average link utilization of 85.884%. In Case 2, cross traffic of 10 flows is introduced to induce congestion at the ingress node. As a result, only 28.69 flows of the main traffic are admitted on average, consuming 63.73% of the link bandwidth. For Case 3 with the same amount of cross traffic causing congestion at the egress node, similar results are obtained. This shows that the adaptive ingress admission control scheme can effectively measure the available bandwidth in the presence of cross traffic, regardless whether congestion occurs at the ingress or the egress node. In addition, the adaptive delay control algorithm achieves delay outside bounds in Cases 2 and 3 (4.47% and 4.48%) close to the target value (4.0%).

TABLE IV

ADAPTIVE INGRESS ADMISSION CONTROL WITH INGRESS-EGRESS PAIR.

Case	Average # of admitted flows	Utilization (%)	Mean delay (msec)	Maximum delay (msec)	Outside bound (%)
Case 1	38.648	85.884	24.064	889.899	7.0135
Case 2	28.692	63.759	14.497	736.006	4.4794
Case 3	28.664	63.698	16.435	669.532	4.4828

TABLE V

EGRESS ADMISSION CONTROL WITH INGRESS-EGRESS PAIR.

Case	Average # of admitted flows	Utilization (%)	Mean delay (msec)	Maximum delay (msec)	Outside bound (%)
Case 1	41.877	93.061	161.819	890.540	38.7985
Case 2	30.329	67.398	23.984	888.663	9.6233
Case 3	30.282	67.294	24.166	561.209	10.0225

Table V lists the results of the egress admission control scheme with the three cases. For Case 1 without cross traffic, the delay outside bound is very big (38.79%) and much higher than that of the adaptive ingress admission control scheme (7.01%). For Cases 2 and 3 with cross traffic, the delay outside bounds are reduced significantly to 9.62% and 10.02%, but these are still higher than those of the adaptive ingress admission control scheme. Therefore, the adaptive ingress admission control scheme is able to controll the delay violation probability better than the egress admission control scheme.

Fig. 6 shows an example of the arrival and service envelopes with the adaptive admission control scheme at a particular time instant during the simulation experiments for Case 1 without cross traffic. Observe that the arrival and service envelopes cross between interval length of 0.6 and 0.7 second. Prior to the crossing point, the arrival envelope is above the service envelope; this means that more packets arrive than depart. The extra packets are held in the buffers of the routers along the path. After the crossing point, the service envelope is above the arrival envelope; this means that admission control is successful at limiting further arrival of data and allow the system to clear the backlog of packets in the buffers. That is, the stability condition in the network is satisfied. Note however, that there is no such crossing point in the example of the arrival and service envelopes with the egress admission control scheme shown in Fig. 7. The service curve is always below the arrival envelope. This proves that at that moment, the scheme is not stable as it over-admits flows. This leads

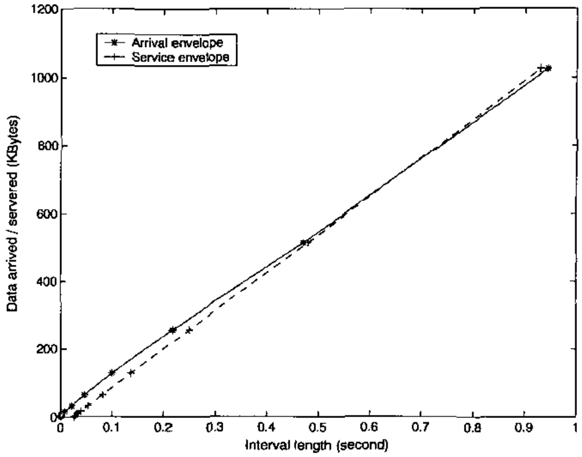

Fig. 6. Sample of arrival and service envelope for the adaptive ingress admission control scheme in Case 1 without cross traffic.

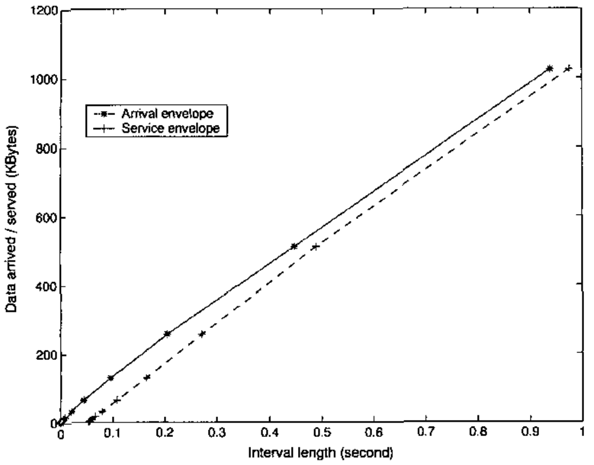

Fig. 7. Sample of arrival and service envelope for the egress admission control scheme in Case 1 without cross traffic.

finally to the large delay outside bound (38.79% as in Table V).

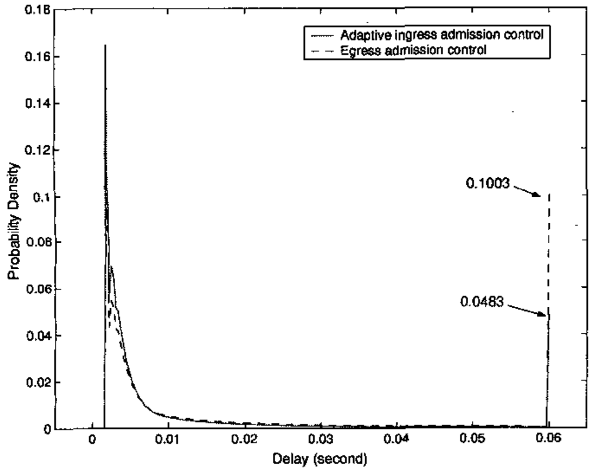

Fig. 8. Delay histogram for adaptive ingress admission control scheme and egress admission control scheme in Case 3 with egress router congested.

Finally, Fig. 8 shows the delay histogram for all the received packets for the two schemes in Case 3 with egress router congested. The X axis shows the delay of packets and the Y axis shows the probability density of packets that have such delays. The delay histogram is calculated up to 60ms, i.e., the delay request of traffic. Thus the value of the probability density at 60ms (mark) is the value of the delay outside bound. Fig. 8 shows that the adaptive ingress admission control scheme allows more packets to have delays within the delay request target than the egress admission control scheme.

V. Conclusions

An adaptive ingress admission control scheme has been proposed to provide scalable services for DiffServ networks. Given an ingress-egress path in a DiffServ domain, the scheme makes an admission control decision based on the aggregate arrival envelope measured at the ingress node and service envelope measured at the egress node. Furthermore, an adaptive adjustment scheme is introduced to the admission control algorithm in trying to achieve the targeted QoS (delay) violation probability. Simulation results indicate that the proposed scheme works effectively in providing scalable services and controlling the delay violation probability.

Acknowledgment

The authors would like to thank the networks group in the Rice University for their simulation codes of the egress admission control algorithm, and the anonimous reviewers for their comments which help improve the quality of this paper.

References

[1] S. Blake. An architecture for Differentiated Services. *Internet IETF RFC2475*, December 1998.

[2] K. Nichols, V. Jacobson, and L. Zhang. A two-bit Differentiated Services architecture for the Internet. *Internet IETF RFC2638*, July 1999.

[3] F. Kelly, D. Estrin, S. Shenker, and L. Zhang. Distributed admission control. *IEEE Journal on Selected Areas in Communications*, 18(2):2617–2628, December 2000.

[4] T. Kelly. An ECN probe-based connection acceptance control. *ACM Computer Communication Review*, 31(3):14–25, July 2001.

[5] G. Bianchi, A. Capone, and C. Petrioli. Throughput analysis of end-to-end measurement-based admission control in IP. In *Proceedings of IEEE INFOCOM 2000*, pages 1461–1470, Tel Aviv, Israel, March 2000.

[6] G. Bianchi, F. Borgonovo, A. Capone, L. Fratta, and C. Petrioli. PCP: An end-to-end measurement-based call admission control for real-time services over IP networks. In *QoS-IP 2001*, pages 391–406. Springer-Verlag Berlin Heidelberg, 2001.

[7] V. Elek, G. Karlsson, and R. Ronngren. Admission control based on end-to-end measurements. In *Proceedings of IEEE INFOCOM 2000*, pages 623–630, Tel Aviv, Israel, March 2000.

[8] J. G. Lim, B. Bensaou, and K. C. Chua. A resource updating protocol for the Differentiated Services environment. In *Proceedings of Quality of Future Internet Services*, Berlin, Germany, September 2000.

[9] M. Gerla, C. Casetti, S. S. Lee, and G. Reali. Resource allocation and admission control styles in QoS DiffServ networks. In *QoS-IP 2001*, pages 113–128. Springer-Verlag Berlin Heidelberg, 2001.

[10] C. Cetinkaya and Edward W. Knightly. Egress admission control. In *Proceedings of IEEE INFOCOM 2000*, pages 1471–1480, Tel Aviv, Israel, March 2000.

[11] C. Oottamakorn and D. Bushmitch. A Diffserv measurement-based admission control utilizing effective envelopes and service curves. In *Proceeding of IEEE ICC 2001*, pages 1765–1771, Helsinki, Finland, June 2001.

[12] A. Krishna. Performance analysis of egress admission control algorithm. *Master Thesis, Department of Computer Science, University of Houston*, August 2002.

[13] J. Schlembach, A. Skoe, P. Yuan, and Edward W. Knightly. Design and implementation of scalable admission control. In *QoS-IP 2001*, pages 1–15. Springer-Verlag Berlin Heidelberg, 2001.