A novel Architecture and an algorithm for access control of real-time flows.

J.David Sukeerthi Kumar,
Asst.Prof, Dept of CSE,
Santhiram Engg.College, Nandyal, Kurnool(Dt), A.P.INDIA,

Dr.P.Prabhakaran
Prof,Dept of CSE,
Santhiram Engg.College, Nandyal, Kurnool(Dt), A.P.INDIA,

***Abstract* - It is very important to allocate and manage resources for multimedia type of data traffic flows with real-time performance requirements in order to guarantee quality-of-service (QoS). In this paper, we develop a scalable architecture and an algorithm for access control of real-time flows. Since individual management of each traffic flow on each transit router can cause a fundamental scalability problem in both data and control planes, we consider that each flow is classified at the ingress router and data flow is aggregated according to the class inside the core network as in a DiffServ framework. In our approach, access decision is made for each flow at the edge routers, but it is scalable because per-flow states are not maintained and the access algorithm is simple. In the proposed access control scheme, an admissible bandwidth, which is defined as the maximum rate of a flow that can be accommodated additionally while satisfying the delay performance requirements for both existing and new flows, is calculated based on the available bandwidth measured by edge routers. The admissible bandwidth is a entry for access control, and thus, it is very important to accurately estimate the acceptable bandwidth. The performance of the proposed algorithm is evaluated by taking a set of simulation experiments using bursty traffic flows.**

Keywords* - *bandwidth, Traffic, edge-routers, routers, decision, multimedia, Quality of Service, framework, algorithm, domain.

I. INTRODUCTION

Although the capacity of core networks has increased tremendously due to advanced optical transmission equipments and high-speed routers/ethernet switches, quality-of-service (QoS) is not well guaranteed in the current P networks. Integrated Services (IntServ) is one of the approaches proposed to address this problem. While IntServ is capable of providing QoS within a domain, it is not scalable since every router is required to manage per-flow information.

On the other hand, DiffServ scales well since core routers treat not per-flow information, but only class-level traffic aggregate. There are two types of approaches for supporting QoS under DiffServ framework: reactive and preventive approaches. In the reactive approaches, QoS is supported by adaptively changing the source traffic load based on the network status. Resource is usually not reserved, but this reactive approach may not be directly applicable to the applications which do not change the traffic rate adaptively. Access control is a typical preventive approach. The traffic rate does not need to be adjusted adaptively in this case and we focus on this preventive approach. There are two important goals of access control algorithms. The first one is to guarantee the contracted QoS for real-time flows, and the other one is to achieve high network utilization. We propose a new access control scheme to achieve these goals. We consider delay as a QoS target because real-time flows are more sensitive to delay than loss. In our proposed access control scheme, each ingress router manages admissible bandwidth, which is a threshold for access control, for each relevant egress router. Access decision is made for each flow by comparing the peak rate of the flow with the admissible bandwidth. We derive a simple equation for admissible bandwidth considering the delay QoS based on the available bandwidth, which is estimated by the egress router through monitoring probing packets. our scheme can perform access control even for the requests arriving at the rate of up to the link rate. In addition, both edge and core routers need not manage any per flow state. Thus, our scheme is scalable in terms of both the number of flow requests and the number of flows.

II. RELATED WORKS

Access control algorithms for internet flows can be assified into two categories. The first one is a traffic-model based approach and the second one is a measurement based approach. In the traffic-model-based approach input traffic is usually mathematically modeled and access is determined based on the model. The accuracy of model based approaches depends on the reliability of the assumed source models. If we calculate the effective bandwidth just based on the parameters of long-range dependent traffic considering some QoS such as loss probability, the utilization of the bandwidth can be very low due to huge rate fluctuation. However, if we monitor the network status periodically, we can increase the bandwidth utilization by capturing the dynamic network status and allocating the resource accordingly. Measurement-based access control algorithms (MBACs) can achieve a much higher utilization than traffic-model-based algorithms while providing somewhat relaxed QoS.

We can classify the MBAC schemes into two categories depending on the location of access decision. First, access decision is made at ingress end hosts. The end host probes the network by sending probe packets at the data rate it wants to reserve and recording the resulting level of packet losses. The host then admits a flow only if the loss percentage is below some threshold value. This kind of access control is called as *endpoint access control*. Here routers keep no per-flow states and do not process reservation requests, and routers drop or mark packets in a normal manner. Thus, the endpoint access control avoids the scalability problem of per-flow state management at each router. However, probing inherently

involves a rather long set-up delay, on the order of seconds. In addition, probing overhead can cause a non-negligible problem especially when the network utilization is high. Endpoint access control has a scalability problem in terms of the number of flow requests. Second, access decision is made at network nodes. Several measurement-based access control algorithms belonging to this type have been proposed and our scheme also belongs to this category. Since it is difficult to predict future behavior accurately with traffic measurements, MBAC can lead to occasional violation of the contracted QoS.

III. SYSTEM ARCHITECTURE

Consider an autonomous system as depicted in Fig. 1. Routers A, E, F, G, and I are edge routers, and B, C, D, and H are core routers. Routers which provide interface to access networks are edge routers, and core routers do not operate as an interface. In the proposed architectural solution, an ingress router manages admissible bandwidth for the path to each relevant egress router. For example, Edge Router A manages admissible bandwidths for Egress Nodes E, F, G, and I, individually. Traffic arrivals at ingress routers of DiffServ domain are differentiated by the given QoS requirements. All arriving traffic with the same QoS requirements is treated as the same class.

Admissible bandwidth is managed separately according to the classes. Admissible bandwidth between a specific ingress/egress node pair is defined considering the level of services that can be provided. In this paper, we consider only delay bound violation probability as a QoS requirement. Let R'_j denote the admissible bandwidth for the j-th class between Ingress Router A and Egress Router E. Let d_j and ε_j be the delay bound and the threshold for the delay violation probability, respectively. $D_j(0)$ is a random variable representing the current end-to-end delay, and $D_j(R)$ is a random variable representing the end-to-end delay which the total traffic of class j experiences after admitting a flow with a rate of R. Then, the admissible bandwidth R'_j is defined by:

$$R'_j = \max\{R : P(D_j(R) > d_j) \leq \varepsilon_j\}.$$

Thus, R'_j is the maximum available bandwidth that can be supported additionally satisfying the delay constraint.

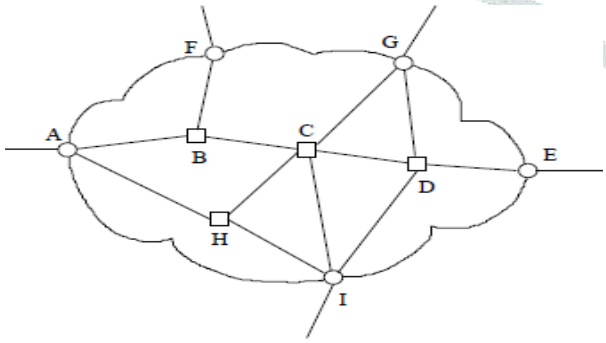

Fig. 1. Reference network model.

In order to support QoS for a new flow while guaranteeing the contracted QoS for the existing flows, a negotiation is needed between the network and a new end- point application.

The network determines whether to admit a new flow or not according to an access control policy/algorithm assuming that the user complies with the contract. The characteristics of the new flow should be included in the contract because the network cannot determine whether the required QoS will be satisfied or not if it does not know how much traffic will be offered by the new flow. Thus, we assume that the contract is made just based on the peak rate r_p of a flow. Peak rate r_p is the only traffic parameter used in our access algorithm, and we assume that each flow is policed so that the instantaneous traffic rate can be maintained less than or equal to the peak rate r_p. If the request from a new flow, which is destined to Router E and has a peak rate of r_p, arrives at Edge Router A, then Router A can accept the flow as the j-th class if the following condition is satisfied:

$$r_p < R'_j.$$

Then, the delay constraint can be satisfied for both the existing and the new traffic. Since the proposed access control algorithm is simple and ingress routers determine whether it accepts the new flow or not, access control can be performed very quickly for real-time flows. In this scheme, ingress routers need not calculate the admissible bandwidth whenever a new flow arrives. An ingress router sends probing packets to relevant egress routers to monitor the condition of each path, especially the available bandwidth for the path and calculates the admissible bandwidth $R'j$ for each ingress/egress node pair in advance.

IV. PRELIMINARIES

Before the access control scheme is proposed, we need to introduce an important concept of minimal backlogging, because this concept plays an important role in the proposed access control scheme. Calculation of the admissible bandwidth considering the delay QoS is the key problem in the proposed access control scheme. We need to distinguish available bandwidth from admissible bandwidth reflecting QoS. For example, we consider a queueing system with a First-Come-First-Served(FCFS) service policy. C and λ denote the service rate in bits per second and the arrival rate of data packets in packets per second, respectively. Let L'denote the average length of the packets. Then, for the queueing system, available bandwidth Ca is defined as $Ca = C(1 - \rho)$;where $\rho = \lambda L'/C$. This available bandwidth is the maximum spare service rate that the server can provide while maintaining stability of the system. In case of accepting a new flow with a rate of C_a, the desired QoS is usually not satisfied. Thus, the admissible bandwidth reflecting QoS is usually lower than the available bandwidth. However, we need to know the available bandwidth in order to obtain the admissible bandwidth. we proposed a probing scheme to estimate the available bandwidth of a single server. We briefly introduce the probing scheme and the available bandwidth estimation mechanism.

Definition 1: Suppose that we send probing packets into a queueing system so that there exists only one probing packet

in the system. This probing method is called a *minimal backlogging method*. If we send a new probing packet into a queueing system just at the departure time of the previous probing packet, then there exists only one probing packet in the system. In order to introduce an estimator for available bandwidth, we define available service as follows:

Definition 2: The available service $\tilde{Y}_{s,t}$ is the amount of probing packets served in a time interval $[s,t]$ when probing packets are sent to the queueing system according to the minimal-backlogging method. Suppose that the size of probing packets is fixed to L. Then, we obtain that for a $G/G/1$ queueing system,

$$\lim_{t\to\infty} E\left[\left| Y_{s,t}/(t-s) - C(1-\rho) \right|\right] = 0 \; ; \; 0 < q < \infty :$$

Thus, the service rate of probing traffic is equal to the available bandwidth of the queueing system probed by the minimal backlogging method for an infinite duration, which implies that the service rate of minimally backlogging probing traffic can be used as an estimator of the available bandwidth.

V. ACCESS CONTROL SCHEME

As described in the previous sections, calculation of the admissible bandwidth is a crucial part of the proposed access control scheme. If the calculated value is larger than the real available capacity, then delay QoS may not be guaranteed due to excessive amount of input traffic. On the other hand, if the calculated value is smaller than the real capacity, the utilization of the network resource decreases. In order to evaluate the admissible bandwidth between a specific ingress/egress router pair, we derive a relation that predicts the delay distribution if a new flow with rate R is accepted. If the new delay distribution can be predicted, then the admissible bandwidth can be calculated. We also investigate a method to estimate the available bandwidth for a path between a given ingress/egress node pair by sending probing packets. We state a simple access control scheme and discuss the complexity and scalability issues of the proposed scheme.

A. Model

We assume that there are only two classes of flows in the core network. The first is the premium class in which all flows abide by their peak rate constraints and have delay QoS requirements. This is the only class that is subject to access control. The second is the best-effort class. Intermediate routers are assumed to give a strict priority to the premium class in managing two classes so that the delay of the premium class traffic is not affected by the best-effort traffic. Traffic is served according to the first-come-first-service (FCFS) policy in the same class. We model a network path from a specific ingress router to an egress router as a simple path which is a concatenation of a fixed delay component (D_f) and a virtual server S. In this model, the end-to-end delay of a packet De is decomposed as $D_e = D_f + D;$ where D is the delay experienced by the packet at the virtual server. Suppose that a probing packet p arrives at the path at time a_p and departs from the path at time d_p. Then, the packet arrives at S at time $a^s_p = a_p + D_f$. When the packet arrives at the destination node, it departs from both the path and the virtual server

B. Evaluation of Admissible Bandwidth

In this subsection, we propose how to evaluate the admissible bandwidth when we know the available bandwidth. The amount of input traffic to a network path can be treated as being continuous in high speed communication networks. We assume $X_{u,v}(X^e_{u,v}, X^n_{u,v})$ and $Y_{u,v}(Y^e_{u,v}, Y^n_{u,v})$ to be continuous in this subsection. Let D^n_t be the virtual delay of the new flow at time t. Since there is no priority between the existing flow and the new flow, the server treats the two traffic streams from the existing and new flows as if they come from the same flow. This implies that there is no difference in virtual delay at a given time no matter whether the virtual bit is of new flow or not. Thus, it follows: *Proposition 1:* Suppose that a new flow starts at time $\tau > 0$.Then, $Dn\ t = Dt, \ t > \tau$: For the virtual server with the arriving traffic amounts of $X^e_{u,v}$ and $X^n_{u,v}$ and the service amounts of $Y^e_{u,v}$ and $Y^n_{u,v}$, if we focus only on the arrival and service traffic of the new flow, we can know that a virtual bit arriving at time t from the new flow can be served just after the traffic arriving from the new flow during the interval $[0,t]$, $X^n_{0,t}$, is served completely under the assumption that $X^n_{0,s}$ $(s>0)$ is increasing. Thus, D^n_t can be interchangeably expressed as $D^n_t = \min\{s : s \geq 0, X^n_{0,t} \leq Y^n_{0,t+s}\}$.

C. Estimation of Available Service

In this subsection, we describe how to estimate the parameters a and σ of the available service $\sim Y^n_{\tau,t}$ by using probing packets. We can obtain the value of $\sim Y^n_{\tau,t}$ if we can provide the minimally backlogging probing traffic exactly. However, this is not possible in real networks. Instead, we send the probing packets by the scheme, which enable the probing packets to be offered to the virtual server of the network path satisfying the minimal backlogging condition approximately.

D. Access Control Algorithm

Let's consider an access control algorithm for a specific ingress/egress router pair. The egress router calculates the lower bound of the admissible bandwidth R^*once every T seconds and sends it back to the ingress router. Then, the ingress router performs access control according to the algorithm described in Fig. 2. If the ingress router has not given access to any flow in the previous window, the ingress router admits the request of a new flow with a peak rate of rp if the following condition is satisfied:

$rp < R^* - rs;$ where rs is the sum of the peak rates of the flows admitted in the current window before the current request.

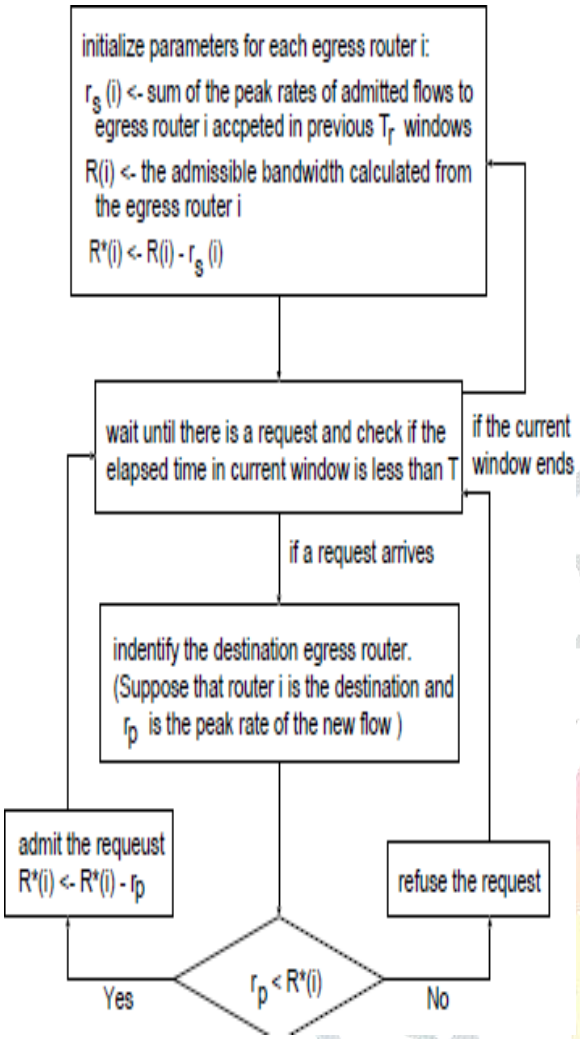

Fig. 2. Access control algorithm for an egress router *i*

E. Complexity and Scalability Issues

The admissible bandwidth is calculated and the access decision is made by just comparing the peak rate of the requesting flow with the admissible bandwidth. In addition, the admissible bandwidth is not calculated on demand, but it is calculated periodically in an interval of at least one second. Thus, the proposed scheme has a low complexity and can perform per-flow access control even at a high request arrival rate through high speed links. We now investigate scalability issues of the proposed access control scheme. Our scheme does not require per-flow state management or processing at the core routers except the class-level scheduling. The class-level scheduling, especially priority scheduling, can be implemented in the framework of DiffServ. Since even the edge routers do not manage per-flow states, our scheme is scalable in terms of the number of flows.

VI. CONCLUSION

In this paper, we proposed a new access control scheme. In the proposed scheme, access decision is made for each flow at the ingress routers, but it is scalable because per flow states are not managed and the access algorithm is simple. An ingress router manages the admissible bandwidth, which is a threshold for access control, for each relevant egress router. Since the admissible bandwidth is calculated considering the delay QoS, it is possible to guarantee the delay performance by the proposed access control scheme.

REFERENCES

[1] R. Branden, D. Clark, and S. Shenker, "Integrated services in the Internet architecture: an overview," IETF RFC 1633, June 1994.

[2] S. Blake, D. Black, M. Carlson, E. Davis, Z. Wang, and W. Weiss, "An architecture for differentiated services," IETF RFC 2475, Dec. 1998.

[3] A. Bose, M. E. Gendy, and K. G. Shin, "Sapphire: Statistical characterization and model-based adaptation of networked applications," *IEEE Trans. Parall. Distrib. Syst.*, vol. 17, no. 12, pp. 1512-1525, Dec. 2006.

[4] E. Lochin, L. Dairaine, and G. Jourjon, "gTFRC, a TCP friendly QoSaware rate control for DiffServ assured service," *Telecommunication Systems*, vol. 33, no. 1-3, pp. 3-21, Dec. 2006.

[5] S. Jamin, P. B. Danzig, S. J. Shenker, and L. Zhang, "A measurementbased access control algorithm for integrated services packet networks," *IEEE/ACM Trans. Netw.*, vol. 5, pp. 56-70, Feb. 1997.