International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 21 Issue 2 – APRIL 2016.

IMPROVING THE PERFORMANCE OF NETWORK USING LEAKY-BUCKET ALGORITHM

D. Keerthana, V. Ajitha

PG Scholar, Computer Science and Engineering, Saveetha Engineering College, Chennai, Tamil Nadu, India
Assistant Professor, Computer Science and Engineering, Saveetha Engineering College, Chennai, Tamil Nadu, India

keerthanadeva16@gmail.com
ajithanice@gmail.com

***Abstract*— Network congestion is occurred due to the number of packets reaching a network is more than a number of packets leaving the network. Scalability and robustness are the two important factors in network congestion control. The congestion collapse, network traffic and unfair bandwidth allocation cannot be fully prevented by end-to-end congestion control algorithm alone. To solve these problems, propose a congestion-avoidance algorithm called Network Border Patrol (NBP). NBP performs the function of exchanging the feedback information between routers of the network. NBP is used to preventing congestion within a network. Leaky-Bucket algorithm is used to regulate the traffic flows and increase the efficiency and reduce the congestion control.**

***Keywords*—Leaky-bucket algorithm, Rate monitor algorithm, feedback controller algorithm, Network border patrol, congestion control.**

I. INTRODUCTION

A network is a group of two or more system or nodes linked together. Network basically performs the packet transfer from source to destination. A network is a series of nodes interconnected by communication path. Network can interconnect with other network and contain sub network. The purpose of a network is to enable the sharing of files and information between multiple subsystems. Network is responsible for moving data from source to destination without any loss.

The concept behind the Internet is explained through using scalability argument for moving data from source to destination. The best example of the Internet is TCP Congestion Control, which is implemented through algorithm operating at end systems. Congestion can be increased due to the growth and maximum usage of multimedia application. This causes unresponsive and misbehaving traffic flows. Networks basically perform the packet transfer from source to destination. To maintain scalability, complexity should be forced to the edges of the network to avoid congestion whenever possible. The current internet suffers from two problems. The two problems are congestion collapse can be occurred due to undelivered packets and unfair bandwidth allocation. The congestion collapse from undelivered packets can be caused due to insufficient bandwidth. The packets are dropped before reaching their destination due to insufficient bandwidth. The congestion collapse can be caused due to retransmission of packets. The unfair bandwidth allocation can be caused due to unresponsive flows. To solve these problems, a novel based protocol called network border protocol. NBP exchange the feedback information between routers. NBP uses patrolling. Patrolling prevent the congestion collapse from undelivered packets, because undelivered packets never enter the network. NBP is used to restrict from congestion collapse and improving the usage of bandwidth allocation**.** NBP added a algorithmic complexity to the edge routers of a network in order to increase performance.

The leaky bucket is used to avoid traffic in a network. It can be used for data transmissions, in the form of packets, conform bandwidth limits. It can be used to regulate the data flow. Error control coding performs two operations; they are error detection and error correction. Error detection is the detection of error origin by noise or other damage during transmission from the transmitter to the receiver. Detection of errors, removing the error data and reconstruction of the original data packets is called error correction. The Sliding window algorithm is used to serves several purposes: It guarantees the reliable delivery of data; it ensures that data is delivered in order, and it enforces flow control between the sender and the receiver. Sliding window is a method by which multiple packets data can be affirmed with a single acknowledgement. A sliding window protocol is a feature of packet-based data transmission protocols. Sliding window protocols are used where reliable in-order delivery of packets is required, such as the data link layer. Sliding window technique is used by an internet transmission control protocol. The basic of TCP congestion control is for each source to determine how much capacity is available in the network, so that it knows how many packets it can safely have in transmit. Once a given source has this many packets in transmit, it uses the arrival of an ACK as a signal that one of its packets has left the network, and that it is safe to insert a new packet into the network without adding to the level of congestion. TCP is also known as self-clocking**.**

II. Related Work

Network is the process of transferring a packet from a source to destination. Network congestion is occurred while transferring packets from source to destination. The two problems occurred are congestion collapse and unfair bandwidth allocation. The problem of congestion collapse in the existing system is the retransmission of loss packets and slow data transmission causes delay in a network.

In existing system, using the Alpha fair congestion control and back-pressure for scheduling algorithm are used to analyses the route. It can be used only for analyzing the edge router capacity of a network using CSMA algorithm to schedule the packets.

The proposed system focuses on the network congestion control problem. In previous paper author describes a redesign framework for fluid-flow models of congestion control algorithms. Motivated by the augmented Lagrangian method, introduce a extra dynamics to algorithms resulting from traditional primal-dual methods to improve their performance while guaranteeing stability. Redesign framework provides stability, robustness to a network and causes the problem retransmission of lost packets, and slow data transmission. Redesign framework are used to improve efficiency and avoid congestion problem in [1]. Redesign framework of distributed Proportional-Integral-Derivative (PID) control is used. The modified dynamics contain PID control action, and the implementation of the scheme remains distributed. PID controller is a control loop feedback mechanism commonly used in industrial control system. A PID controller continuously calculates an error value as a difference between a measured process variable and a desired set point. The controller is used to minimize the error over time by adjustment of a control variable. PID is used for network congestion control problems at the level of fluid-flow models in [2]. E. Wei, A. Ozdaglar, & A. Jadbabaie proposed a distributed Newton-type fast converging algorithm for solving network utility maximization problems using self-concordant utility functions. By using novel matrix splitting technique, both primal and dual updates for the Newton step can be computed using iterative schemes in a decentralized manner with limited information exchange. This algorithm is a iterative scheme to compute the stepsize and the Newton direction. These methods are based on subgradient and dual decomposition. This can be used to improving the rate performance and solving network utility maximization problem. This algorithm provides an iterative scheme to compute the stepsize and the Newton direction [3][4]. The author proposed a algorithm based on Alternating Direction of Multipliers (ADMM). Apply ADMM to distributed model predictive control (MPC) and TCP/IP congestion problem. This method is used to solve the optimization problem that is occurred over a network of nodes. This method provides a accuracy solution. ADMM solves the optimization problem and suitable for bipartite network. The author proposed a algorithm to solve the congestion control problems and optimization problem. ADMM is used to divide the problem into small piece of problems. So that it is easier to handle the problem [5]. Other design methodology uses subgradient methods are used to design of node or link dynamics to guarantees nominal functionality based on arbitrary system sizes. This method is used to solve bandwidth allocation problem and optimization problem in a centralized manner [6].The available resource allocation controllers are used to derive the state of the system to a desired equilibrium point. This design is used to solve real network problem, optimal control problem on which some practical constraints, such as a real-time link capacity constraints. This design is used to improve the real-time performance and steady-state performance. The congestion control problem should be solved by maximizing a proper utility functional as utility function [7]. The author demonstrate a dynamic laws that s saddle point of a function of two variables, by moving each in the direction of the corresponding partial gradient. These methods are used to obtain scalability proofs of these primal-dual laws in different scenarios, and applications to cross-layer network optimization are exhibited [8]. P.Wan&M.D, Lemmon proposed dual decomposition. Dual decomposition is used distributed algorithm that solves the network utility maximization (NUM) problem. This approach uses a stepsize that is inversely proportional to measures of network size. The author proposed an event-triggered distributed NUM algorithm based on the augmented lagrangian methods. This algorithm establishes state-dependent event-triggering thresholds. The proposed algorithm reduces the number of message exchanges is virtually scale-free [9]. The author develops a distributed algorithm that converges to the globally and jointly optimal rate allocation and persistence probabilities. This algorithm uses a network utility maximization formulation, in which by adjusting the types of utility function. NUM framework has found applications in network rate allocation through congestion control protocol .In NUM framework, each end-user has its utility function and link bandwidths are allocated so that network utility is maximized. Utility functions can be interpreted to control the tradeoff between efficiency and fairness. NUM framework designs a contention-based MAC protocol. It is a deterministic approximation approach to solve congestion problem and provides a accurate performance [10]. Several approaches are used to avoid congestion collapse. Floyd and Fall solves the problem of congestion collapse by proposing low-complexity router mechanisms. These approaches can be used to identify high-bandwidth flows and can't identify the flow rates and unresponsiveness flows [11].

A. Network congestion control for high performance

F. Paganini, Z. Wand, J.C. Doyle & S.H Low made survey on "Congestion control for high performance, stability and fairness in general networks". The author design a congestion control system that scales gracefully with network capacity, providing high utilization, low queuing delay, dynamic stability, and fairness among users. This focus is on developing decentralized control laws at end-systems and routers at the level of fluid-flow models that can satisfy such properties in arbitrary networks and packet-level implementation. Two families of control laws are developed. The first dual control law is able to achieve the first three objectives for arbitrary network, delays and resource allocation.

B. *Internet congestion control*

S.H. Low, J.C. Doyle & F. Paganini made survey on "Internet congestion control". The author describes an optimization-based framework that provides an interpretation of various flow control mechanism, review a transmission control protocol and congestion control protocol. TCP uses "window" flow control, where a destination sends acknowledgments for packets that are correctly received. A source keeps a variable called window size that determines the maximum number of outstanding packets that have been transmitted but not yet acknowledged. When the window size is exhausted, the source must wait for an acknowledgment before sending a new packet. Two features are important. The first is the "self-clocking" feature that automatically slows down the source when a network becomes congested and acknowledgments are delayed. TCP Congestion Control was introduced into the network. The idea of TCP congestion control is for each source to determine how much capacity is available in the network, so that it knows how many packets it can safely have in transmit. Once a given source has this many packets in transmit, it uses the arrival of an ACK as a signal that one of its packets has left the network, and that it is therefore safe to insert a new packet into the network without adding to the level of congestion. The second is that the window size controls the source rate: roughly one window of packets is sent every round-trip time. TCP also provides other end-to-end services such as error recovery and round-trip time estimation. A connection starts cautiously with a small window size of one packet and the source increments its window by one every time it receives an acknowledgment. This doubles the window every round-trip time and is called slow-start.

III. PROPOSED SYSTEM

The proposed system defines an algorithm network border patrol (NBP) to prevent the congestion and traffic flows. The proposed system uses a fixed size window scheme to limit the number of packets to prevent loss of data packets. The data packets are sent into the network based on the capacity of the network and hence there is no possibility of any undelivered packets in a network. Buffering of packets is carried only at the core router not in the edge router. So, it can be used to increase the transient performance and ensure fair bandwidth allocation.

NBP monitor and control the rates of individual flows at the border of the network. NBP can be used to exchange the feedback between routers. NBP is also called as core-stateless congestion avoidance mechanism. This section explains 1) Architectural component, which describes overall performance of an network; 2) Leaky-bucket algorithm is needed to regulate the data flow. It is used to improve the lifetime of network and prevent from traffic flows increases performance of our network; 3) the network border patrol, which exchange the information between routers; 4) the rate control algorithm, which monitor the rate of flow; and 5) the feedback control algorithm, which exchange a FF and BF feedback between routers.

A. *Architectural component*

The architecture component describes the packet sending from source to destination through routers. The leaky-bucket algorithm is used to avoid traffic and regulate flow of data. The feedback can be exchanged between source and destination to avoid packet loss.

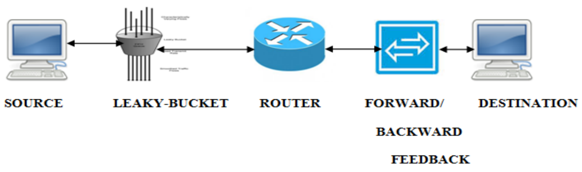

Fig.1. Architecture component

The input data packets received by the egress router are collected and performs a flow classification. The ingress router performs the flow classification by receiving packets based on their flow classification policy. This policy is used to determine the source and destination network address and send to the egress router. The output of the ingress router data packet contains flow classifier and per-flow traffic data. The flow classifier divides packets into flows and the traffic shaper limits the rate of data packets which enter into the network. The feedback controller send a backward feedback packets to ingress router that are send by egress router; contains contents that are passes into rate controller.

B. *Leaky-Bucket Algorithm*

The leaky-bucket algorithm stores a irregular number of requests and organizing them into a set-rate output of packets in an asynchronous transfer mode (ATM) network. The leaky bucket is used to implement traffic policing and traffic shaping in Ethernet and cellular data network. It can be used for data transmissions, in the form of packets, define bandwidth limits. It can be used to regulate the traffic data flow. Assume that Leaky bucket as a bucket which has a small hole at the bottom. If a packet reaches at the queue when it is full, packet is discarded. Leaky-Bucket algorithm is used to increase the efficiency and reduce the congestion control. The packets arrives in a queue, if the queue is already full then, the new packets are discarded.

C. *Network Border Patrol*

NBP is also called as core-stateless congestion avoidance mechanism. Network Border Patrol (NBP) is used to compare, the rate of packets in each application determines the flow entering and leaving the network. Flow packets are entering the network is faster than they are leaving it, then the network is buffering or discarding the flow's packet. NBP prevent this scenario by patrolling. Patrolling prevent the congestion collapse from undelivered packets, because undelivered packets never enter the network. NBP is having ability to prevent congestion collapse and improve the fairness of bandwidth allocation. NBP monitor and control the rates of individual flows at the border of the network. NBP entails the exchange of feedback between routers. NBP doing flow classification and maintain per-flow state in a network.

D. *Rate controller algorithm*

The rate-controller algorithm monitors the rate at which each flow is permitted to enter the network. A set of per-flow transmission rates are evaluated to prevent congestion collapse from undelivered packets. Rate control algorithm flow contains two phases; they are slow start and congestion avoidance. Whenever the backward feedback returns to an ingress router at the time rate-control algorithm is performed. The backward feedback contains timestamp and list of flows reaches the egress router. There are two types of backward feedback sends to ingress router. They are normal backward feedback and asynchronous backward feedback. When the egress router receives forward feedback, then it generates normal backward feedback packets. An egress router produces asynchronous backward feedback without any prompting from an ingress router.

Rate controller algorithm used to calculate the current round trip time and base round trip time. The algorithm calculates the difference between the current round trip time and base round trip time is called delta round trip time. To compute the ingress rate performs the product of ingress rate and delta round trip time.

E. *Feedback controller algorithm*

The feedback controller algorithm determines how and when feedback is exchanged between routers. Feedback can be sending in the form of ICMP packets. Feedback controller performs two main functions. They are 1) the egress router finds which ingress router acts as a source by using forward feedback. 2) The egress router provides a communication by using feedback. The Forward feedback is used to monitor each flow and acting as source node. The forward feedback contains timestamp and flow specification. Backward feedback provides a communication between ingress and egress router. The backward feedback contains timestamp, hop count, egress rate and flow specification. The forward and backward feedback used to detect network congestion in a network. After receives forward feedback packets, an egress router immediately produces backward feedback packets to ingress router. Egress rate is a collection of observed bit rates. The hop count defines to determine how many routers are present in between ingress and egress router.

F. *Time sliding window algorithm*

The time sliding window algorithm is used for rate monitoring. TSW evaluate the sending rate for each flow of packet arrival time. TSW contains three data: window, average rate and time front.

IV. IMPLEMENTATION

A. *Source*

Source is mainly responsible for data transfer to destination. The task of source is to get input from user and send the input in the form of packets to router. Source performs the operation of converting a message into packets. The source is used to send the packets to next router levels. The source sends a packet with destination machine name and IP address. The input parameter is user typed message and its output parameter is data packets. This also includes destination IP address.

B. *Ingress router*

Flow passing into a network that is operated by an edge router is called an Ingress router. NBP restrict congestion collapse through a combination of egress router per flow rate monitor and ingress router per flow rate control. Rate control allows an ingress router to monitor the rate at which each flows packet enters into the network. NBP are used in ingress router to exchange a feedback between routers at the border of the network. NBP is a congestion-avoidance mechanism. Ingress router uses ingress filter to filter IP packets with trusted source address. Each data flow contains a flow classifier, per-flow traffic shapers, a feedback controller, and a rate controller. The flow classifier classifies packets into flows, and the traffic shapers limit the rates at which packets from individual flows enter the network. The feedback controller receives backward feedback packets returning from egress routers and passes their contents to the rate controller. It also generates forward feedback packets, which it periodically transmits to the network's egress routers. The rate controller regulates traffic shaper parameters according to a TCP-like rate control algorithm. Ingress router uses ingress filtering method to filter IP packets with trusted source address before they enter and affect our network.

C. *Router*

The router is used to accept the packet from the ingress router and send it to the egress router. Leaky-bucket algorithm is used to regulate the data flow.

D. *Egress router*

Flow passing out of a network that is operating at edge router is called an egress router. NBP detect congestion collapse through a combination of per flow monitoring at egress router and per flow rate at ingress router. Rate can be monitored using a rate estimation algorithm such as the time windowing algorithm (TSW). The modified input ports of egress router perform per-flow monitoring of bit rates, and the modified output ports of ingress routers perform per-flow rate control. In addition to that, ingress and the egress routers are used to exchange and handle feedback information. Ingress routers send packets to the input port of the egress router and the packets are classified by flow classification. In the case of IPv6, examining the packet header’s flow label does this, whereas in the case of IPv4, examining the packet’s source and destination addresses and port numbers does it. Each flow's bit rate is monitored using a rate estimation algorithm such as the Time Sliding Window (TSW). This rate is collected by a feedback controller and sends backward feedback packets to an ingress router whenever a forward feedback packet attain from that ingress router. Backward feedback packets are also generated asynchronously; that is, an egress router sends them to an ingress router without first waiting for a forward feedback packet. Egress router is needed to use egress filtering method to filter outbound traffic flows and can be used to prevent from modification that are occurred in outgoing packets.

E. *Destination*

Destination module perform the task is to take the packet from the egress router and reserved in the Destination machine as a file. Message will be stored in the corresponding folder as a text file depends upon the source machine name that is received from egress router.

V. RESULT ANALYSIS

The graph shows the relation between the performances of the network and the traffic or congestion occurred in a network. The performance can be increased by using leaky-bucket algorithm. This graph shows the comparison graph of existing algorithm (using FIFO) and proposed algorithm (using NBP).

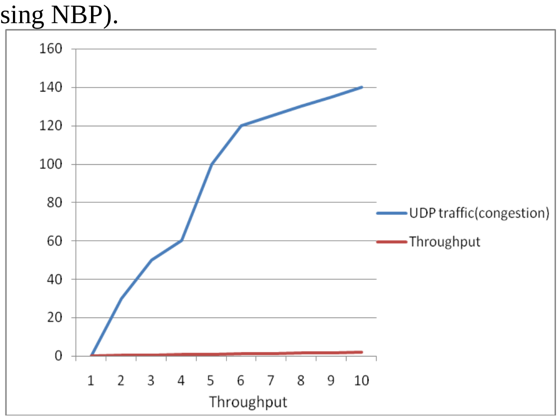

Fig.2. a) Heavy congestion using FIFO

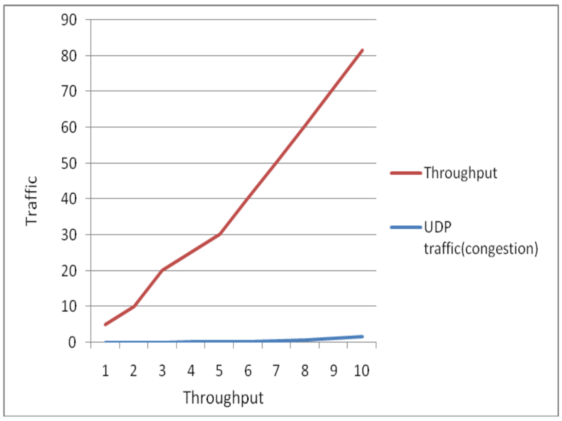

Fig.2. b) No congestion using NBP

VI. CONCLUSION

Improving performance is an important aspect of network. The proposed model with leaky-bucket algorithm provides accuracy, secure and lower delay. The algorithm is used to solve congestion control problem. Overall system could achieve robustness and reduce delays. Compared to standard algorithms, these algorithms provide a better performance and added scalability for the overall system. This provides a guaranteed towards overall performance increment, reduces the time and energy consumption. It will increase the network lifetime by reducing the delay.

REFRENCES

[1] X. Zhang and A. Papachristodoulou, “Improving the performance of network using congestion control algorithm,” IEEE transaction on automatic control,vol. 60, no. 2, feburary 2015.

[2] X. Zhang and A. Papachristodoulou, “A distributed PID controller for network congestion control problems,” in *Proc. of American Control Conference*, 2014, pp. 5453.

[3] E. Wei, A. Ozdaglar, and A. Jadbabaie, “A distributed Newton method for network utility maximization, Part I: Algorithm,” *IEEE Transactions on Automatic Control*, vol. 58, no. 9, pp. 2162–2175, 2013.

[4] E.Wei, A. Ozdaglar, and A. Jadbabaie, “A distributed Newton method for network utility maximization, Part I: Convergence,” *IEEE Transactions on Automatic Control*, vol. 58, no. 9, pp. 2162–2175, 2013

[5] J. Mota, J. Xavier, P. Aguiar, and M. Puschel, “Distributed ADMM for model predictive control and congestion control,” in *Proc. of 51th IEEE Conference on Decision and Control*, 2012, pp. 5110–5115.

[6] A. Papachristodoulou and A. Jadbabaie, “Delay robustness of nonlinear internet congestion control schemes,” *IEEE Transactions on Automatic Control*, vol. 55, pp. 1421–1428, 2010.

[7] J. Lavaei, J. C. Doyle, and S. H. Low, “Utility functionals associated with available congestion control algorithms,” in *Proc. of IEEE INFOCOM*, 2010.

[8] D. Feijer and F. Paganini, “Stability of primal-dual gradient dynamics and applications to network optimization,” *Automatica*, vol. 46, no. 12, pp. 1974–1981, 2010.

[9] P. Wan and M. D. Lemmon, “Distributed network utility maximization using event-triggered augmented lagrangian methods,” in *Proc. of American Control Conference*, 2009, pp. 3298–3303.

[10] E. Wei, A. Ozdaglar, and A. Jadbabaie, “A distributed newton method for network utility maximization,” LIDS Report 2832, 2010.

[11] S. Floyd and K. Fall,”Promoting the use of end-to-end congestion control in the internet,”IEEE/ACM Trans. Networking, vol.7, pp. 458-472, Aug. 1999.

[12] E. Camponogara and H. Scherer, “Distributed optimization for model predictive control of linear dynamic networks with control-input and output constraints,” *IEEE Trans. Aut. Sc. Engin.*, vol. 8, no. 1, 2011.

[13] J. Mota, J. Xavier, P. Aguiar, and M. Püschel, “D-ADMM: A communication-efficient distributed algorithm for separable optimization,” 2012.

[14] S.Boyd, N. Parikh, E. Chu, B. Peleato, and J. Eckstein, “Distributed optimization and statistical learning via the alternating method of multipliers,” *Found. Trends Mach. Learning*, vol. 3, no. 1, 2011

[15] S. Boyd, N. Parikh, E. Chu, B. Peleato, and J. Eckstein, “Distributed optimization and statistical learning via the alternating method of multipliers,” *Found. Trends Mach. Learning*, vol. 3, no. 1, 2011.

[16] E. Camponogara and H. Scherer, “Distributed optimization for model predictive control of linear dynamic networks with control-input and output constraints,” *IEEE Trans. Aut. Sc. Engin.*, vol. 8, no. 1, 2011.

[17] S. Boyd, N. Parikh, E. Chu, B. Peleato, and J. Eckstein, “Distributed optimization and statistical learning via the alternating method of multipliers,” *Found. Trends Mach. Learning*, vol. 3, no. 1, 2011

[18] D. Papadimitriou, M. Welzl, M. Scharf and B. Briscoe, “Open research issues in Internet congestion control,” RFC 6077, Internet Research Task Force (IRTF), 2011.

[19] A. Papachristodoulou and A. Jadbabaie, “Delay robustness of nonlinear internet congestion control schemes,” IEEE Transactions on Automatic Control, vol. 55, pp. 1421–1428, 2010.

[20] D. Feijer and F. Paganini, “Stability of primal-dual gradient dynamics and applications to network optimization,” Automatica, vol. 46, no. 12, pp. 1974-1981, 2010.

[21] A. Jadbabaie, A. Ozdaglar and M. Zargham,“A Distributed Newton method for network optimization,” Proc. of CDC, 2009.

[22] A. Olshevsky and J. Tsitsiklis, “Convergence speed in distributed consensus and averaging. SIAM Journal on Control and Optimization,” 48(1):33–35,2009.

[23] A. Zyrnnis, D. Bickson, Y. Tock, S. Boyd and D. Dolev, “Distributed large scale network utility maximization,” Proceedings of the 2009 IEEE international conference on Symposium on Information Theory,2009.

[24] M. Chiang, S.H. Low, A.R. Calderbank and J.C.Doyle,“layering as optimization decomposition: A mathematical theory of network architectures,” Proc. Of IEEE, vol. 95, no. 1, pp. 255-312,2007.

[25] A. Mustafa and M.Hassan,”End to end IP rate control,” in Recent Advances in computing and communications. New York: McGraw-Hill, Dec.2000, pp. 278-282.