http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 5 (3): 427-432, 2006
ISSN 1812-5638

Network Border Patrol, a Novel Congestion Avoidance Mechanism for Improving QOS in Wireless Networks

T. Sasipraba and S.K. Srivatsa
Sathyabama Deemed University,
Madras Institute of Technology, Chennai, India

Abstract: This study considers the potentially negative impacts of an increasing deployment of non-congestion-controlled best-effort traffic on the internet. These negative impacts range from extreme unfairness against competing TCP traffic to the potential for congestion collapse. To promote the inclusion of end-to-end congestion control in the design of future protocols using best-effort traffic, we argue that router mechanisms are needed to identify and restrict the bandwidth of selected high-bandwidth best-effort flows in times of congestion. The paper discusses several general approaches for identifying those flows suitable for bandwidth regulation. As a result of its strict adherence to end-to-end congestion control, the current Internet suffers from main maladies: congestion collapse from undelivered packets. This has the beneficial effect of preventing congestion collapse from undelivered packets; because an unresponsive flow's otherwise undeliverable packets never enter the network in the first place. The end-to-end nature of Internet congestion control is an important factor in its scalability and robustness. However, end-to-end congestion control algorithms alone are incapable of preventing the congestion collapse and unfair bandwidth allocations created by applications, which are unresponsive to network congestion. This study propose and investigate a new congestion avoidance mechanism called Network Border Patrol (NBP).

Key words: Admission control, TCP/IP patrolling, ingress router, egress router, round trip time, rate control, congestion collapse, congestion control

INTRODUCTION

TCP congestion control illustrates some of the shortcomings in the end-to-end argument. NBP overcomes these problems by the exchange of feedback between routers at the borders of a network in order to detect and restrict unresponsive traffic flows before they enter the network, there by preventing congestion collapse with in the network. The primary idea behind NBP's congestion control mechanism is to compare, at the borders of the network, the rates at which each flow's packets are entering and leaving the network. If packets are entering the network faster than they are able to leave the network, then this implies that either the packet are buffered or discarded by some core router (Albuquerque *et al*., 2000). In other words the network is congested. This can be prevented, by measuring the rate at which a flow's packets are leaving the network and ensuring that they don't enter the network at a greater rate. This guarantees that the network will not get congested, as an unresponsive flow's packets are not allowed to enter the network in the first place. Since only the routers at the edges of the network are modified and the core routers are left unchanged this subscribes to the Internet design philosophy of keeping the router implementations simple and pushing the complexity to the edges of the network (Floys and Fall, 1999). The main goal of NBP is to prevent congestion collapse from undelivered packets but when combined with fair queuing at core outers, NBP can achieve global max-min fairness.

Basic principle of NBP: The basic principle of NBP is to compare, at the borders of a network, the rates at which packets from each application flow are entering and leaving the network. If a flow's packets are entering the network faster than they are leaving it, then the network is likely buffering or, worse yet, discarding the flow's packets. In other words, the network is receiving more packets than it is capable of handling. NBP prevents this scenario by patrolling the network's borders, ensuring that each flow's packets do not enter the network at a rate greater than they are able to leave the network. This patrolling prevents congestion collapse from undelivered packets; because unresponsive flow's otherwise undeliverable packets never enter the network in the first place. Figure 1 shows the Internet architecture assumed by NBP.

Corresponding Author: T. Sasipraba, Sathyabama Deemed University, Madras Institute of Technology, Chennai, India

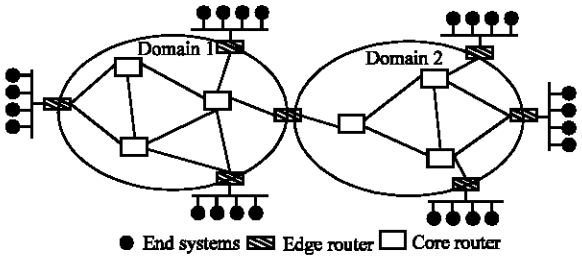

Fig. 1: Core-stateless internet architecture assumed by NBP

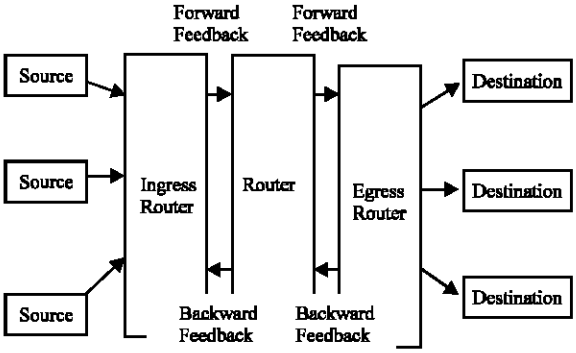

Fig. 2: System flow diagram

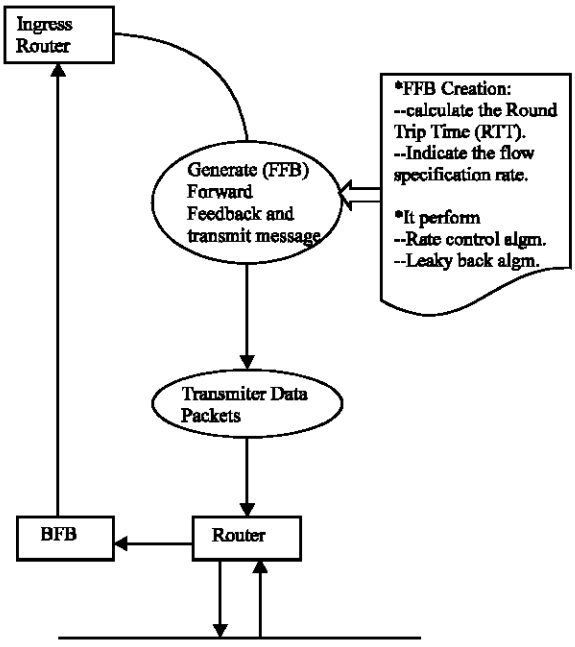

Fig. 3: Working of ingress router

Although NBP is capable of preventing congestion collapse and improving the fairness of bandwidth allocations, these improvements do not come for free. NBP solves these problems at the expense of some additional network complexity, since routers at the border of the network are expected to monitor and control the rates of individual flows in NBP. NBP also introduces added communication overhead, since in order for an edge outer to know the rate at which its packets are leaving the network, it must exchange feedback with other edge routers. Unlike some existing approaches trying to solve congestion collapse, however, NBP's added complexity is isolated to edge routers; routers within the core of the network do not participate in the prevention of congestion collapse (Liu and El-Zarki, 1994; Ho *et al*., 2001; Comaniciu and Poor, 2003). Moreover, end systems operate in total ignorance of the fact that NBP is implemented in the network, so no changes to transport protocols are necessary at end systems.

Congestion control: Congestion control means preventing (or trying to prevent) the source from sending data that will end up getting dropped by a router because its queue is full. This is more complicated, because packets from different sources traveling different paths can converge on the same queue.

Congestion collapse: When a packet is dropped in the network, all the resources that it used on the way from the source to the place where it got dropped are wasted, instead of being used to carry some other packet that actually would have reached its destination. As the number of packets entering the network increases, the number of packets reaching destinations increases at first, but then starts to fall toward zero, because nearly all the network resources are being used to carry packets partway before they get dropped (Jacobson, 2001; Nagel, 2000; Vazquez-Abad and Krishnamurthy, 2002). This is called congestion collapse. Because of this resource-wasting effect, the only way to prevent

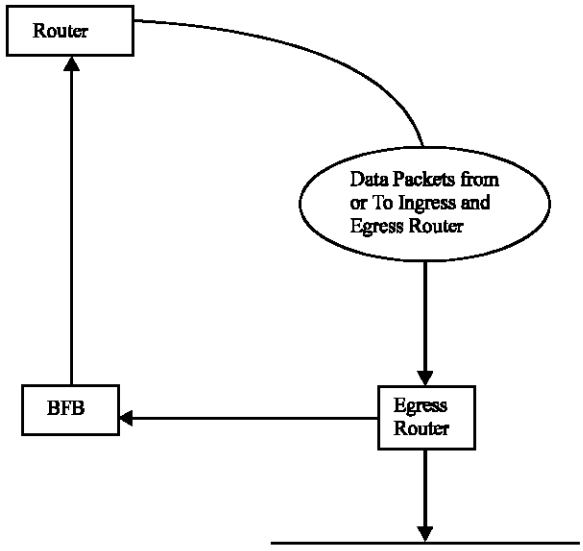

Fig. 4: Working of a egress router

congestion is to prevent too many packets from entering the network. Limiting the window limits the rate at which the source can send, because it can send at most one window per round-trip time (Singh *et al*., 2002; Comainiciu *et al*., 2000; Jeon and Jeong, 2002).

Proposed work: The main purpose of this study was to control congestion collapse in Network. By using rate control, Leaky bucket, Time sliding window, rate monitoring Algorithms traffic (congestion) in the network is reduced. The Internet's excellent scalability and robustness result in part from the end-to-end nature of internet congestion control. End-to-end congestion control algorithms alone, however, are unable to prevent the congestion collapse and unfairness created by applications that are unresponsive to network congestion. To address these maladies, we propose and investigate a novel congestion-avoidance mechanism called Network Border Patrol (NBP). Figure 2 shows the model of the system used for the study.

Source module: The task of the module is to get the input from user and send the input in the form of the packets to the ingress router.

Ingress router module: An edge router operating on a flow passing into a network is called an ingress router. NBP prevents congestion collapse through a combination of per flow rate monitoring at egress router and per flow rate control at ingress router. Rate control algorithm allows an ingress router to police the rate at which each packet enters the network. Ingress Router contains a flow classifier, per-flow traffic shapers (e.g., leaky buckets), a feedback controller and a rate controller. The working of the Ingress router is shown in the Fig. 3.

Router module: The task of this module is to accept the packet from the Ingress Router and send it to the Egress Router.

Egress router module: An edge router operating on a flow passing out of a network is called an Egress Router. NBP prevents congestion collapse through a combination of per flow rate monitoring at egress router and per flow rate control at ingress router. Rate Monitoring allows an egress router to determine how rapidly each flow's packets are leaving the network. Rate monitored using a rate estimation algorithm such as the Time Sliding Window (TSW). Egress Router contains a flow classifier, Rate monitor, a Feedback controller. Figure 4 gives the working of a Egress Router module.

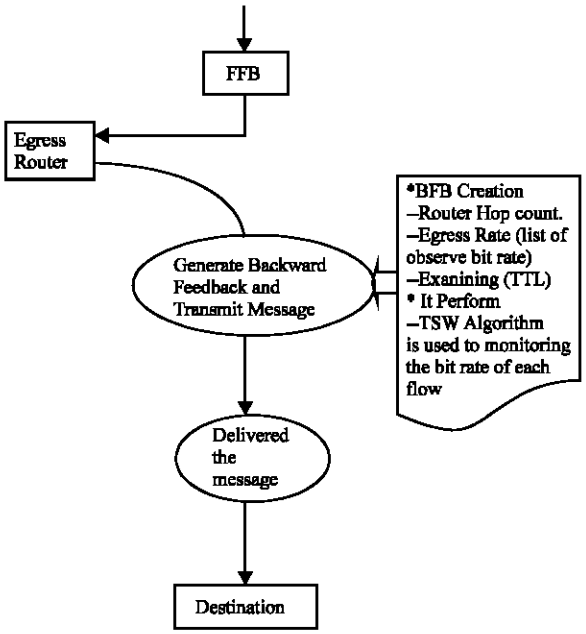

Fig. 5: Working of a destination router

Destination module: The task of this module is to accept the packet from the Egress router and stored in a file in the Destination machine. The working of the Destination Module is shown in Fig. 5.

Simultaneous process: Data and forward feedback are performing at the same time. The NBP feedback control algorithm determines how and when feedback packets are exchanged between edge routers. Feedback packets take the form of ICMP packets and are necessary in NBP for three reasons. First, they allow egress routers to discover which ingress routers are acting as sources for each of the flows they are monitoring. Second, they allow egress routers to communicate per-flow bit rates to ingress routers. Third, they allow ingress routers to detect network congestion and control their feedback generation intervals by estimating edge-to-edge round trip times.

IMPLEMENTATION

The feedback control algorithm: The NBP feedback control algorithm determines how and when feedback packets are exchanged between edge routers. Feedback packets take the form of ICMP packets and are necessary in NBP for three reasons. First, they allow egress routers to discover which ingress routers are acting as source for each of the flows they are monitoring. Second, they allow egress router to communicate per-flow bit rates to ingress routers. Third, they allow ingress router to detect network congestion control their feedback generation intervals by estimating edge-to-edge round trip times.

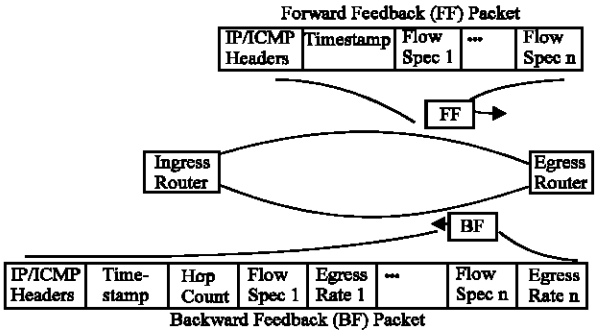

Fig. 6: Forward and backward feedback packets exchanged by edge routers

Forward feedback packet contains a Time stamp and a list of flow specifications for originating at the ingress router. The Time stamp is used to calculate the round trip time between two edge routers and the list of flow specifications indicates to an egress router the identifies of active flows originating at the ingress router. When an egress router receives a forward feedback packet, it immediately generates a backward feedback packet and returns it to the ingress router. Contained within the backward feedback packet are the forward feedback packet's original Time stamp, a router hop count and a list of observed bit rates, called egress rates, collected by the egress router for each flow listed in the forward feedback packet. The router Hop count, which is used by the ingress router's rate control algorithm, indicates how many routers are in the path between the ingress and the egress router. The egress router determines the hop count by examining the Time To Live (TTL) field of arriving forward feedback packets. When the backward feedback packet arrives at the ingress router, its contents are passed to the ingress router's rate controller, which uses them to adjust the parameters of each flow's traffic shaper. Figure 6 shows the forward and backward feedback packets echanged by edge routers.

In order to determine how often to generate forward feedback packets, an ingress router keeps, for each router, a timer which determines the frequency of forward feedback packet generation. To maintain an adequate and consistent feedback update interval, the timer repeatedly expires after an interval of timer known as the base round trip time. The base round trip time for egress router e, denoted e.base RTT, is defined as the shortest observed round trip time between the ingress router and egress router e and it generally reflects the round trip time between the two edge routers when the network is not congested. The value e.base RTT is calculated by estimating the current round trip time from each arriving backward feedback packet and updating e.base RTT whenever the current round trip time is less.

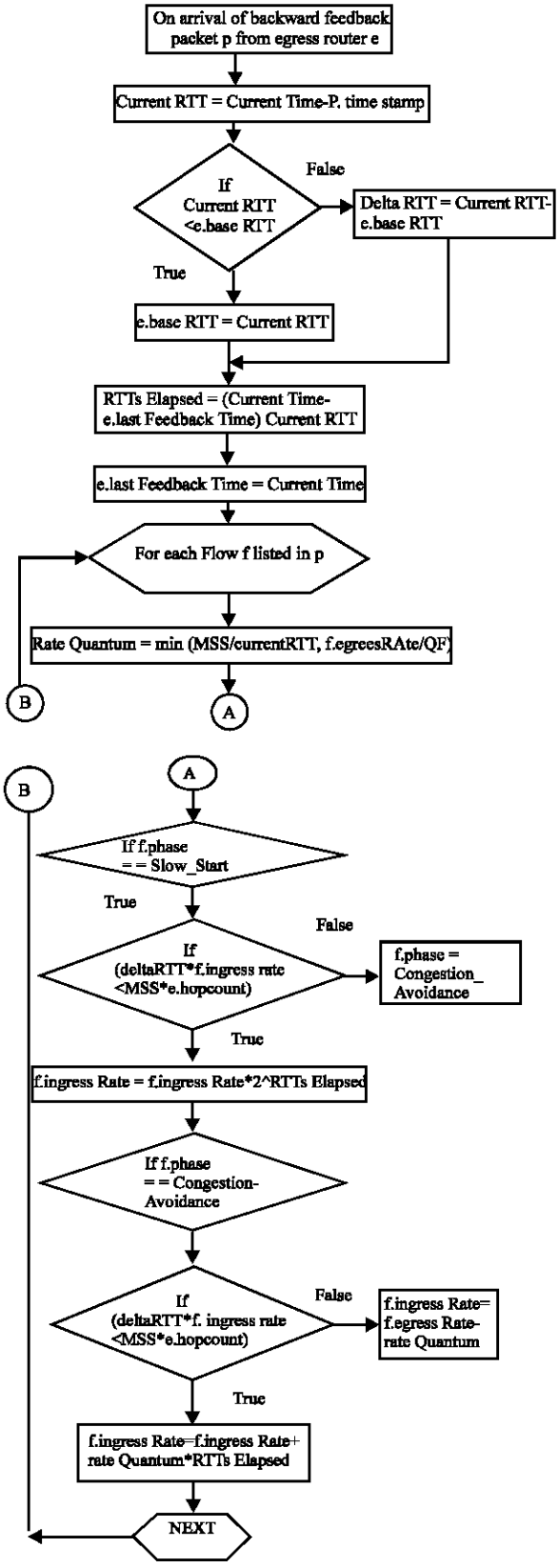

Fig. 7: Rate control algorithm

Egress routers may also generate backward feedback packets asynchronously. If an egress router does not receive a forward feedback packet from an ingress router within a fixed interval of time, it generates and transmits a backward feedback packet to the ingress router. The reason for asynchronous backward feedback packet generation is to prevent the squelching of congestion feedback when forward feedback packets are delayed or dropped by the network. It also ensures that ingress routers receive frequent rate feedback and are able to respond to congestion even when the distance between edge routers is very large. The Rate control algorithm is shown in Fig. 7.

However, when congestion occurs, NBP reacts first by reducing f.ingress Rate and, therefore, reducing the rate at which TCP packets are allowed to enter the network (Jeon and Jeong, 2002). TCP eventually detects the congestion (either by losing packets or due to longer round-trip times) and then promptly reduces its transmission rate.

SIMULATION RESULTS

When the rate-control algorithm determines that a flow is not experiencing congestion, it increases the flow's ingress rate. This is done to avoid the creation of congestion. The rate quantum is computed as the

Fig. 8: Modules showing before message transfer

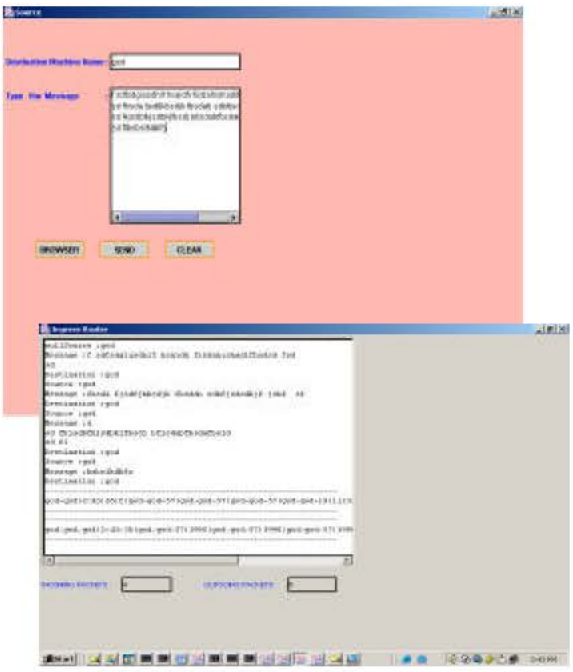

Fig. 9: Modules showing after message transfer

maximum segment size divided by the current round-trip time between the edges routers. This results in rate growth behavior that is similar to TCP in its congestion-avoidance phase. NBP's rate-control algorithm is designed to have minimum impact on TCP flows. Fig. 8 shows the output of experiment before message transfer and the status after message transfer is given in Fig. 9.

CONCLUSIONS

This result presented a novel congestion avoidance mechanism for the internet called Network Border Patrol. This paper implements only the ingress router. Unlike existing internet congestion control approaches, which rely solely on end-to-end control, NBP is able to prevent congestion collapse from undelivered packets. It does this by ensuring at the border of the network that each flow's packets do not enter the network faster than they are able to leave it. NBP requires no modifications to core routers or to end systems. Only edge routers are enhanced so that they can perform the requisite per-flow monitoring, per-flow rate control and feedback exchange operations. This work may be extended that ingress and Egress router are embedded inside a single edge router.

REFERENCES

Albuquerque, C., B. Vickers and T. Suda, 2000. Network border patrol. IEEE Transactions on Communications, 1: 158-167.

Comamciu, C. and H.V. Poor, 2003. Jointly optimal power and admission control for delay sensitive traffic in CDMA networks with LMMSE receivers. IEEE Trans. Signal Processing, 51: 2031-2003.

Comainciu, C., N.B. Mandayam, D.F. Amolari and P. Agarwal, 2000. Qos guarantees for 3G CDMA systems via admission and flow control. In Proc 52nd IEEE Vehicular Technology Conf., 1: 249-256.

Floyd, S. and K. Fall, 1999. Promoting the use of End-To-End Congestion control in the Internet. IEEE/ACM Transactions on Networking, 2: 234-243.

Ho, C.J., J.A. coprland, C.T. Lea and G.L. Stuber, 2001. On call admission control in DS/CDMA cellular networks. IEEE Trans. Veh. Technol., 50: 1328-1343.

Jacobson, V., 2001. Congestion avoidance and control. ACM Computer Communication, 1: 45-52.

Jeon W.S. and D.G. Jeong, 2002. Call Admission control for CDMA mobile communication systems supporting multimedia services. IEEE Trans. Wireless Commun., 1: 649-659.

Liu, Z. and M. ElZarki, 1994. SIR-based all call admission control for DS-CDMA cellular systems. IEEE J. Select. Areas Commun., 12: 638-644.

Nagle, J., 2002. Congestion control in IP/TCP Internet works Internet. Engineering Task Force, 2: 78-86.

Singh, S., V. Krishnamurthy and H.V. Poor, 2002. Integrated voice/data cell admission control for wireless DS-CDMA systems. IEEE Trans. Signal Processing, 50: 1483-1495.

Vazquez-Abad, F.J. and V. Krishnamurthy, 2002. Self learning call admission control for multimedia wireless DS_CDMA systems. In Proceding of Craction. 6th Intl. Workshop Discrete Event Systems, Zaragoza, Spain, pp: 399-404.