RESEARCH ARTICLE OPEN ACCESS

# Network Border Patrol: Preventing Congestion Collapse and Promoting Fairness in the Network

Jasmeet Singh[1], Muhib A. Lambay[2]

PTU/RIMT Institute of Engineering and Technology Mandi Gobindgarh Punjab – India

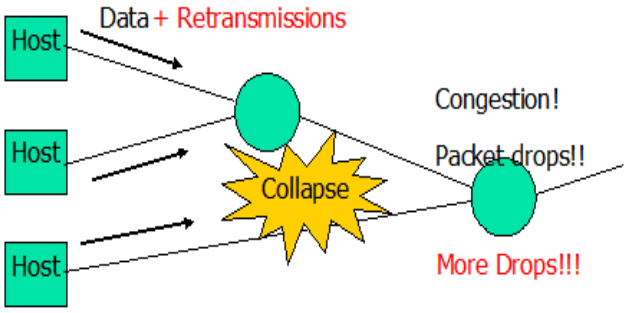
## Abstract:

The Internet's outstanding scalability and robustness result in part from the end-to-end nature of Internet blocking control. End-to-end congestion control algorithm however, congestion fall down and unfairness created by applications were unable to prevent the system which is indifferent to network congestion. A novel congestion-avoidance mechanism called network border patrol (NBP) were planned and investigated to address these maladies. In order to detect and restrict unresponsive traffic flows before they enter the network, thereby preventing congestion within the network, NBP entails the exchange of feedback between routers at the borders of a network. In order to provide fair bandwidth allocations to opposing flows, NBP is complemented with the proposed enhanced core-stateless fair queuing (ECSFQ) mechanism. Both NBP and ECSFQ are compliant with the Internet philosophy of pushing difficulty toward the edges of the network whenever possible. Simulation results show that NBP effectively eliminates congestion collapse and that, when combined with ECSFQ, about max-min fair bandwidth allocations can be achieved for competing flows

*Keywords :-* **Sybil attacks ,Message Authentication ,Networks Using Message.**

## 1. INTRODUCTION

Network margin Patrol is a core-stateless congestion prevention mechanism. That is, it is united with the core-stateless approach which allows routers on the limits (or edges) of a network to perform flow organization and maintain per-flow shape but does not allow routers at the core of the association to do so. Figure one illustrate this architecture. In this paper, we draw a further difference between two types of edge routers. Depending on which flow it is operating on, an edge router may be viewed as entrance or an *egress* router. An edge router in service on a flow passing into a network is called an entrance router, whereas an edge router operating on a flow passing out of a network is called an egress router. Note that a current may pass during more than one egress (or ingress) router if the end-to-end path crosses various networks.



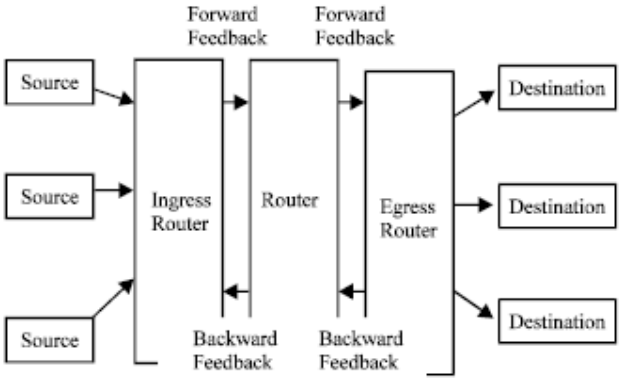

**Internet congestion collapse**

TCP jamming control illustrates some of the shortcomings in the end-to-end argument. NBP overcomes these problems by the swap of feedback between routers at the limits of a network in order to detect and restrict impassive traffic flows before they enter the system, thereby preventing congestion collapse with in the network. The primary idea at the back NBP's congestion control mechanism is to compare, at the borders of the network, the rates at which each flow's packets are inflowing and leaving the network. If packets are incoming the network faster than they are able to leave the network, then this imply that either the

packet are buffered or redundant by some core router (Albuquerque *et al*., 2000). In other words the set of connections is congested. This can be prevented, by measuring the rate at which a flow's packets are leaving the set of connections and ensuring that they don't enter the network at a better rate. This guarantees that the network will not get overcrowded, as an unresponsive flow's packets are not allowed to enter the network in the primary place. Since only the routers at the edges of the network are adapted and the core routers are left unmoved this subscribes to the Internet design thinking of keeping the router implementations simple and pushing the complexity to the edges of the set-up (Floys and Fall, 1999). The main goal of NBP is to prevent congestion collapse from undelivered packets but when shared with fair queuing at core routers, NBP can achieve global max-min fairness.

## BASIC PRINCIPLE OF NBP

The basic rule of NBP is to compare, at the limits of a network, the rates at which packets from each application flow are toward the inside and leaving the network. If a flow's packets are entering the network earlier than they are parting it, then the network is likely buffering or, worse yet, disposal the flow's packets. In other words, the network is receiving more packets than it is able of handling. NBP prevents this scenario by patrolling the network's margins, ensuring that each flow's packets do not enter the association at a rate better than they are able to leave the set-up. This patrolling prevents congestion collapse from undelivered packets; because unresponsive flow's otherwise undeliverable packets not at all enter the network in the first place.




***System flow Diagram***

## CONGESTION COLLAPSE

Congestive collapse (or congestion collapse) is the situation in which congestion prevents or limits useful announcement. Congestion collapse generally occurs at "choke points" in the network, where incoming traffic exceed outgoing bandwidth. association points between a LAN and a WAN are common choke points.

When a network is in this situation, it settles into a stable state where traffic command is high but little useful throughput is available, packet wait and defeat and QOS is very poor.

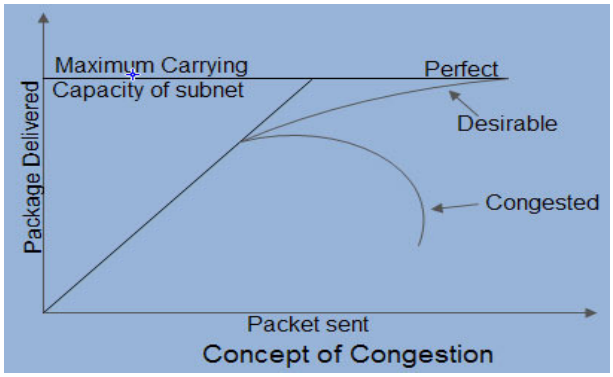
Congestion collapse was known as a possible problem by 1984, It was first experimental on the early Internet in October 1986, when the NSFnet phase-I moral fiber dropped three orders of magnitude from its capacity of 32 Kbit/s to 40 bit/s, which nonstop until end nodes started implementing Van Jacobson's congestion control between 1987 and 1988.

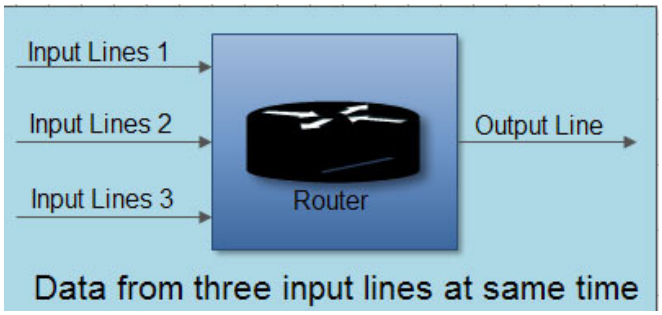
When more packets were sent than could be handled by in-between routers, the in-between routers discarded several packets, expecting the end points of the network to retransmit the information. However, early TCP implementations had poor retransmission behaviour. When this packet loss occurred, the endpoints sent extra packets that repetitive the information lost, doubling the incoming rate.

## CONGESTION CONTROL

Congestion is an significant issue that can arise in packet switched network.

Congestion is a situation in announcement Networks in which too many packets are present in a part of the subnet, recital degrades. Congestion in a network may occur when the load on the network *(i.e.* the number of packets sent to the network) is better than the capacity of the network *(i.e.* the number of packets a network can handle.)




In other words when too much traffic is presented, congestion sets in and performance degrades stridently

***Effects of Congestion***

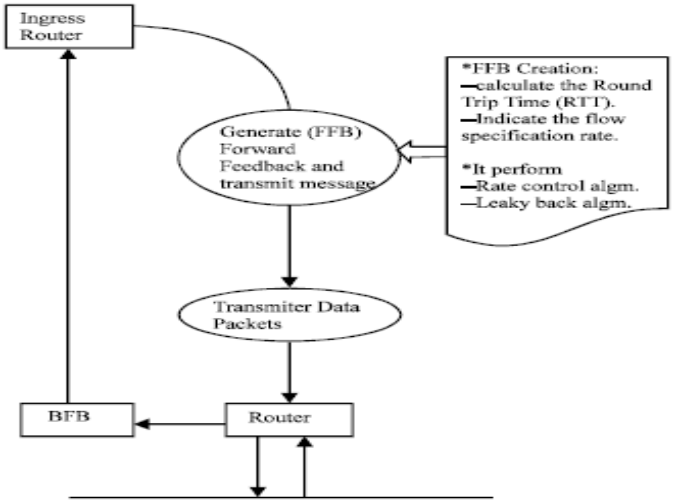
- Packets arriving are stored at input buffers
- Routing resolution made
- Packet moves to yield buffer
- Packets queued for yield transmitted as quick as possible
  *numerical time division multiplexing
- if packets arrive to fast to be routed, or to be output, buffers will fill
- can throw away packets
- can use flow manage

The main principle of this study was to control blockage collapse in Network. By using rate control, Leaky bucket, Time downhill window, rate monitor Algorithms traffic (congestion) in the network is condensed. The Internet's excellent scalability and toughness result in part from the end-to-end nature of internet congestion control. End-to-end congestion control algorithms alone, however, are powerless to prevent the obstruction collapse and grievance created by applications that are indifferent to network congestion. To address these maladies, we propose and inspect a novel congestion-avoidance machinery called set of connections Border Patrol (NBP).

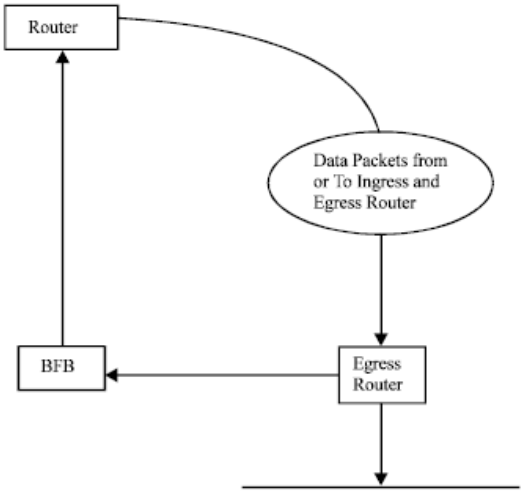
***Source module:*** The task of the unit is to get the input from customer and send the contribution in the form of the packets to the entrance router.

***Ingress router module:***

An edge router in commission on a flow passing into a network is called an entrance router. NBP prevents congestion collapse through a mixture of per flow rate monitoring at egress router and per flow rate control at way in router. Rate control algorithm allows an way in router to police the rate at which each packet enters the network. Ingress Router contains a flow classifier, per-flow interchange shapers (e.g., leaky buckets), a advice controller and a rate controller. The working of the way in router is shown below




*Working of ingress router*



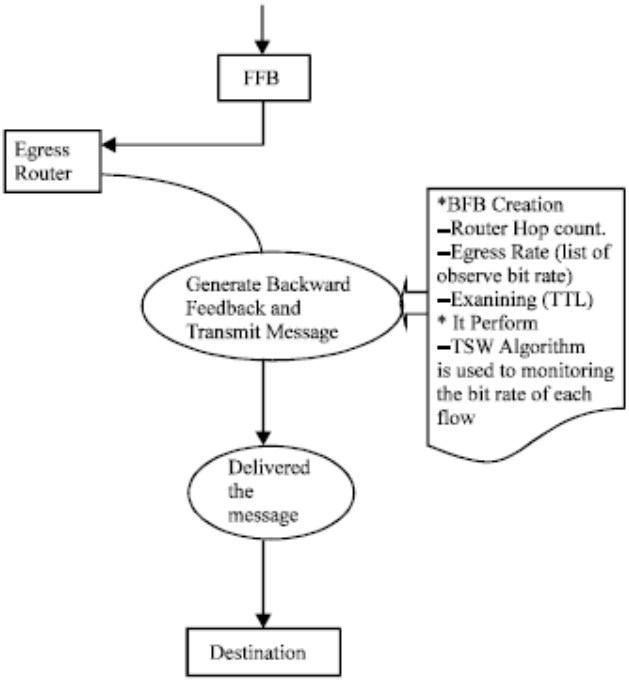

*Working of a egress router*

**Router module:** The task of this unit is to accept the packet from the way in Router and send it to the way out Router.

***Egress router module:***

An edge router operating on a flow fleeting out of a network is called an way out Router. NBP prevents obstruction collapse through a mixture of per flow rate monitoring at way out router and per flow rate control at way in router. Rate Monitoring allows an way out router to determine how rapidly each flow's packets are leaving the network. Rate monitored using a rate evaluation algorithm such as the Time Sliding Window (TSW). way out Router contains a flow classifier, Rate examine, a Feedback controller.

***Destination module:*** The task of this unit is to accept the packet from the way out router and stored in a file in the Destination machine. The working of the Destination unit is shown below



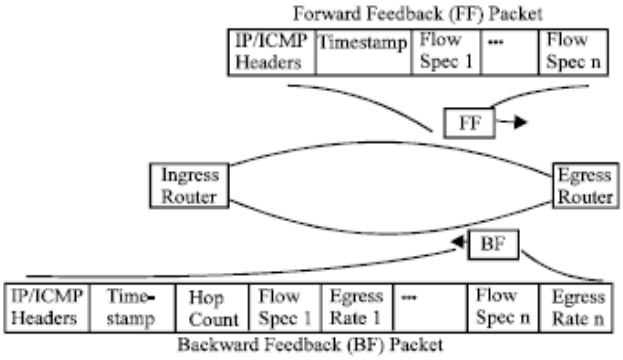
***Simultaneous process:***

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

## *ALGORITHM DESCRIPTION*

***The feedback control algorithm:***

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




***Forward and backward feedback packets exchanged by edge routers***

Onward feedback packet contains a Time stamp and a list of flow condition for originating at the way in router. The Time stamp is used to calculate the round trip time among two edge routers and the list of flow condition indicates to an way out router the identifies of active flows originating at the way in router.

When an egress router receives a onward opinion packet, it immediately generates a rearward opinion packet and returns it to the way in router. Contained within the back opinion packet are the forward feedback packet's original Time stamp, a router hop count and a list of experiential bit rates, called egress rates, collected by the way out router for each flow listed in the onward opinion 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 way in and the way out router. The way out router determines the hop count by examining the Time To Live (TTL) field of arriving onward feedback packets. When the toward the back opinion packet arrives at the ingress router, its contents are passed to the way in router's rate controller, which uses them to adjust the parameters of each flow's transfer shaper.

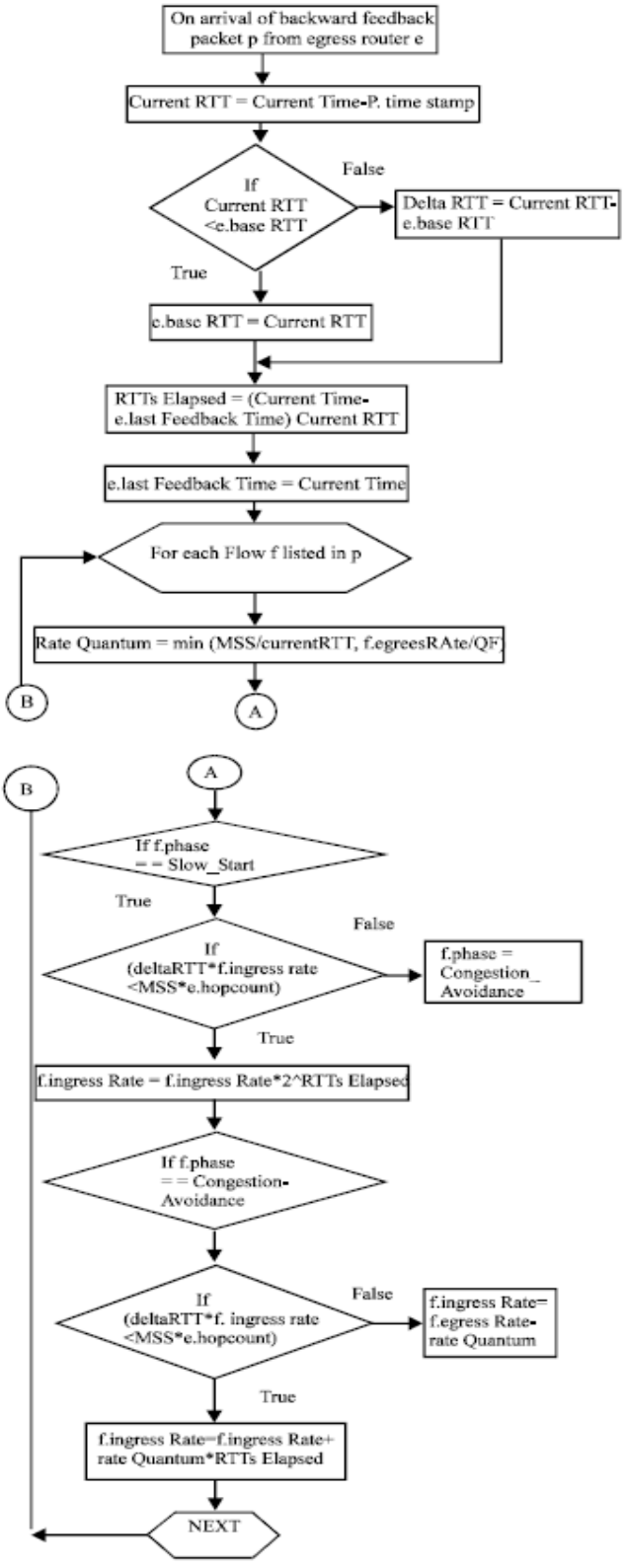
In regulate to determine how often to generate onward opinion packets, an way in router keeps, for each router, a timer which determines the frequency of onward feedback packet generation. To maintain an adequate and consistent opinion update interval, the timer repeatedly expires after an distance of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

## *RATE CONTROL ALGORITHM:*

NBP rate control Algorithm regulates the rate at which each flow is permitted to go into the network.

*NBP rate control algorithm may be in two phases:*

1. Slow Start Phase
2. Congestion Avoidance Phase



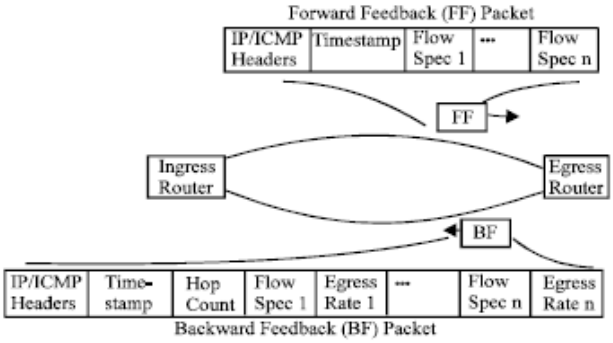

**Rate control algorithm**

## *CONGESTION CONTROL ALGORITHMS*

### *1. Leaky bucket algorithm:*

Each host is associated to the network by an interface containing absorbent bucket i.e., a finite internal queue. If a packet arrives at the queue when it is full packet is unnecessary. In other words, if one or more processes within the host try to send a packet when the maximum number is already queued, the new packet is unceremoniously unnecessary. The host is allowed to put one packet per clock tick onto the network. This mechanism turns an not smooth flow of packets from the user processes inside the host into an even flow of packets onto the network, smoothing out bursts and greatly reducing the probability of congestion.

**Flow chart representation of Leaky Bucket Algorithm**

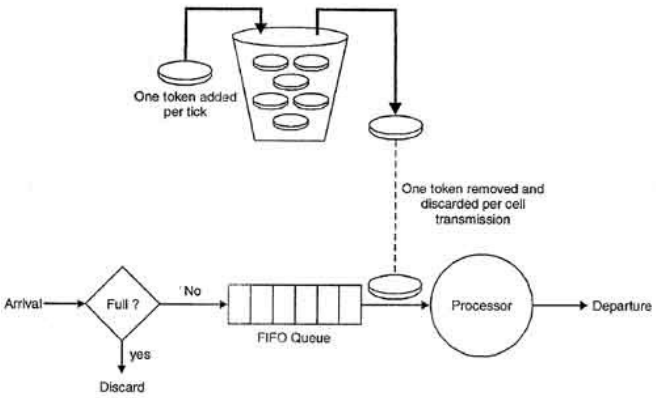



### *2. Token bucket Algorithm*

The leaky bucket algorithm allows only an average (constant) rate of data flow. Its main problem is that it cannot contract with bursty data. A leaky bucket algorithm does not believe the idle time of the host. For example, if the host was idle for 10 seconds and now it is willing to send data at a very high speed for another 10 seconds, the total data show will be divided into 20 seconds and average data rate will be maintained. The host is having no benefit of sitting idle for 10 seconds. To overcome this difficulty, a token bucket algorithm is used. A token bucket algorithm allows bursty data transfers. A token bucket algorithm is a alteration of leaky bucket in which leaky bucket contains tokens. In this algorithm, a token(s) are generate at every clock tick. For a packet to be transmit, system must remove token(s) from the bucket. Thus, a token container algorithm allows idle hosts to gather credit for the future in form of tokens. For example, if a method generates 100 tokens in one clock tick and the host is inactive for 100 ticks. The bucket will contain 10,000 tokens.

Now, if the host wants to send bursty data, it can put away all 10,000 tokens at once for sending 10,000 cells or bytes.

Thus a host can launch bursty data as long as bucket is not empty

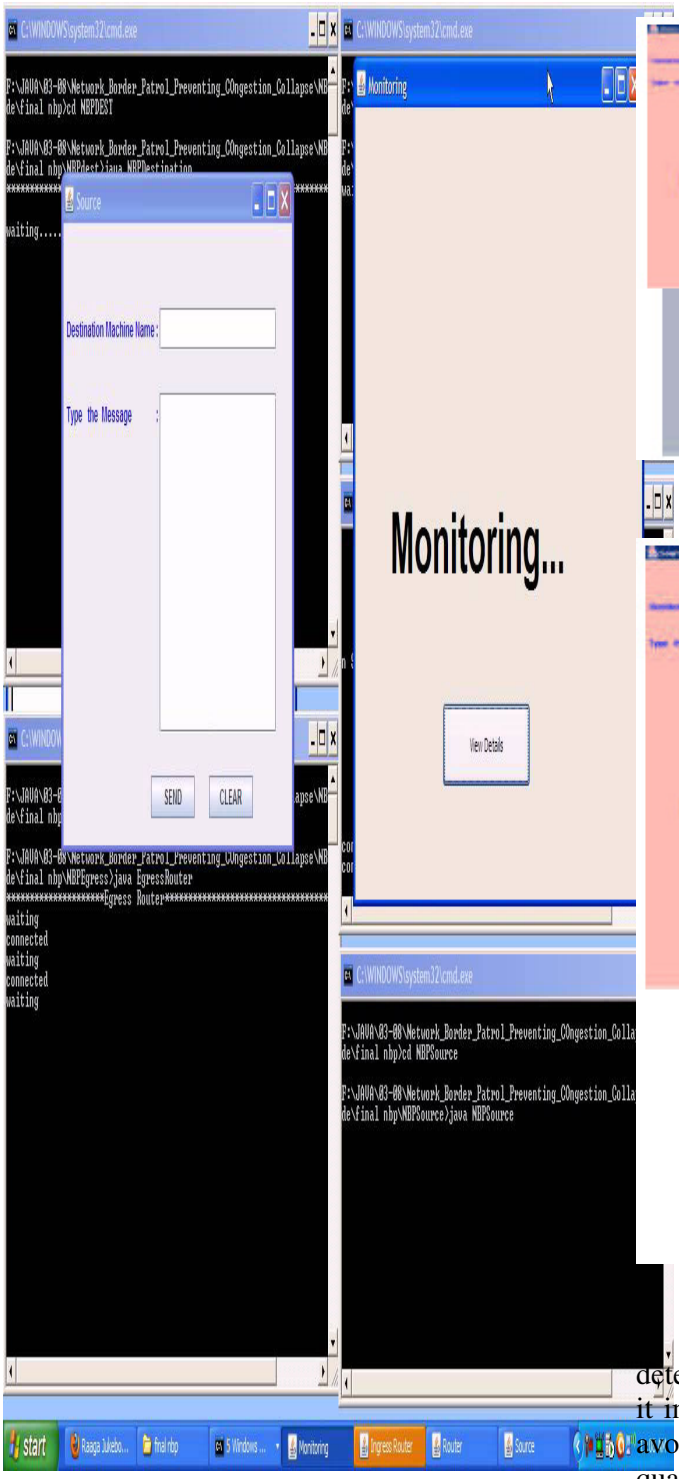



Token bucket algorithm

way out routers may also generate backward feedback packets asynchronously. If an egress router does not receive a onward opinion packet from an ingress router within a fixed gap of time, it generates and transmits a backward opinion packet to the ingress router. The reason for asynchronous back opinion packet generation is to prevent the squelching of congestion feedback when onward opinion packets are delayed or dropped by the network. It also ensures that ingress routers receive normal rate feedback and are able to respond to congestion even when the distance between edge routers is extremely large.

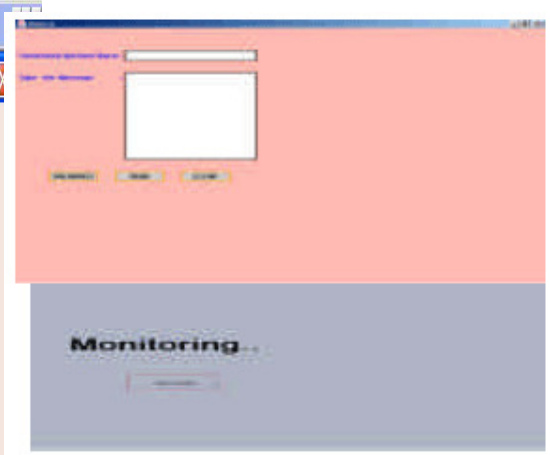
However, when congestion occurs, NBP reacts first by reducing way in Rate and, therefore, reducing the rate at which TCP packets are allowed to enter the network .TCP finally detects the congestion (either by losing packets or due to longer round-trip times) and then promptly reduce its transmission rate.

## *RESULTS*




*Modules showing before message transfer & Modules showing after message transfer*

***Eg.2 RESULT WINDOWS***




***Modules showing before message transfer***

***Modules showing after message transfer***

When the rate-control algorithm determine that a flow is not experience congestion, it increases the flow's way in rate. This is done to avoid the formation of congestion. The rate quantum is computed as the greatest segment size separated by the current round-trip time between the limits routers.

This results in rate expansion behaviour that is parallel to TCP in its congestion-avoidance phase. NBP's rate-control algorithm is designed to have smallest amount crash on TCP flows. Above figure shows the output of experiment before message transfer and the position after message relocate is given in same window image

## CONCLUSION

Unlike accessible internet congestion control approaches, which rely on end-to-end control, NBP is able to prevent the congestion collapse from undelivered packets. NBP requires no modification to core routers or to end systems. Buffering of packets in passed out in the edge routers rather than in the core routers. The packets are sent into the network based on the capacity of the network and hence there is no option of any undelivered packets present in the network. Only edge routers are improved so that they can perform the requisite per-flow monitoring, per-flow rate control and opinion exchange operations. The feedback-based traffic control mechanism, stability is an important presentation concern in NBP. Fair allocation of bandwidth is ensure using the Network Border Patrol and this avoiding the jamming in the network.

As in any feedback-based traffic control mechanism, constancy is an important presentation concern in NBP. Using technique were described we plan as part of our future work to perform an methodical study of NBP's stability and convergence toward max min fairness. Introduction results already suggest that NBP benefits greatly from its use of explicit rate opinion, which prevents rate over-corrections in reply to indication of network congestion.

## REFERENCES

[1] Sally Floyd, Van Jacobson. Random Early Detection Gateways for Congestion Avoidance (1993). IEEE/ACM Transactions on Networking, vol.1 (4): pp.397–413. Invented Random Early Detection (RED) gateways.

[2] Computer networking notes/communication-networks by Dinesh Thakur [author of the hugely popular Computer Notes blog]

[3] Congestion Avoidance Mechanism article by T. Sasipraba and S.K. Srivatsa.

[4] Network Border Patrol by Celio Albuquerque, Brett J. Vickers, Tatsuya Suda.

[5] B.Brsden et al, "Recommendations on queue management and Congestion Avoidance in the Internet, "RFC 2309, IETF, April 1998.

[6] B. Vandalore, S. Fahmy, R. Jain, R. Goyal, and M. Goyal, "A Definition of Generalized Fairness and its Support in Switch Algorithms," ATM Forum Document 98-0151, Traffic ManagementWG, February 1998.

[6] Images courtesy www. Google.com