Packet Drop Prevention Using Network Border Protocol
Sonali Bhapkar, Pratik Awari, Poonam Borse, Hasib Shaikh
Department of Computer Engineering,
K.C. College of Engineering & Management studies & Research,
Kopri, Thane(E)-400 603, India.

Abstract- Network Congestion is basically a situation where the number of packets arriving is more than the number of packets leaving the network. It results from applications sending more data than the network devices can accommodate in its buffer as a result of which it fills up and possibly overflow. 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. But End-to-end congestion control algorithms alone are incapable of preventing the congestion collapse and unfair bandwidth allocations created by applications that are unresponsive to network congestion. To address this flaw, we propose and investigate a novel congestion avoidance mechanism called Packet Drop Prevention (PDP) Using NBP (Network Border Protocol).

Keywords: Network Border Protocol, Leaky Bucket Algorithm, Feedback Control Algorithm, Rate Control Algorithm, Time Sliding Window Algorithm, Inrouter, router, Outrouter.

I. INTRODUCTION
The basic principle of PDP Using NBP is to compare the rates of packets at which packets are entering and leaving the network by sitting at the borders of a network. PDP ensures that each packet do not enter the network at a rate greater than they are able to leave the network. PDP Using NBP is a combination of standard congestion control algorithms like Leaky Bucket Algorithm, Feedback Algorithm, Rate Control Algorithm, Time Sliding Window Algorithm to avoid congestion of packets at the time of packets transfer. PDP uses new concept of Edge Routers i.e. Ingress Router and Egress Router. PDP relies on the exchange of feedback between edge routers of a network in order to detect and restrict unresponsive traffic flows before they enter the network. An enhanced core bred ronidesoporpsimsinahcemgniueuqriaslesetasp rovide fair bandwidth allocations among competing flows.

II. PROBLEM DEFINITION
A. Existing system:
As a result of network’s strict adherence to end-to-end Congestion control, the current internet suffers from two maladies: Congestion Collapse from undelivered packets and Unfair Bandwidth Allocation between competing traffic flows. Congestion collapse from undelivered packets arises when packets that are dropped before reaching their destination continually consume bandwidth. Unfair bandwidth allocation arises due to the existence of the applications that do not respond properly to congestion. To overcome the problems of congestion collapse the existing algorithms uses following concepts
- Retransmission of lost or dropped packets
- Increment in size of queue
- Slow data transmission

But these techniques are not advisable beyond certain limit.

B. Proposed system:
To address the maladies i.e. congestion collapse and unfair bandwidth allocation, in our proposed system we are also introducing a Congestion Free Router (CFR). The basic principle of CFR is to compare the rates at which packets from each application flow are entering and leaving the network. CFR prevents this scenario by “patrolling” the network’s borders, ensuring that each flow of packets do not enter the network at a rate greater than they are able to leave the network. For that it uses the exchange of feedback between edge routers of a network in order to detect and restrict unresponsive traffic flows before they enter the network. This patrolling prevents congestion collapse from undelivered packets.
III. BACKGROUND WORK

A. Leaky Bucket Algorithm:
The Leaky Bucket Algorithm is used to regulate the traffic flow from the input port to the output port. We assume that leaky bucket as a bucket which has a small hole at the bottom. Hence due to hole any packet that enters the bucket at any rate must go out of the bucket at a controlled rate. And we also assume that the limit of the bucket is infinity. Hence there is no case of bucket getting overflow, so packets do not get lost.

B. Time Sliding Window Algorithm (TSW):
The Time Sliding Window Algorithm is used for rate monitoring. TSW estimates the sending rate upon each packet arrival time. TSW maintains three state variables in the hash structure: window, average rate and time front. Window Length: It is predetermined which is measured in units Average Rate: Average rate is estimated upon each packet arrival. Time Front: Time front is the time of last packet arrival. TSW estimate the rate upon each packet arrival, so state variables average rate time front are updated each time a packet arrives

C. Feedback Control Algorithm:
The Feedback Control Algorithm in NBP 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 two reasons. First, forward feedback packets allow egress routers to discover which ingress routers are acting as sources for each of the flows they are monitoring. Second backward feedback packets allows egress router to send the information to ingress router about a timestamp and a list of flows arriving at the egress router from the ingress router as well as the monitored egress rates for each flow.

D. Rate Control Algorithm:
The NBP rate-control algorithm regulates the rate of packets at which they are entering and leaving the network. The ratecontrol algorithm is invoked whenever a backward feedback packet arrives at an ingress router. Rate control algorithm calculates the Current Round-Trip Time (current RTT) between the edge routers and updates the base round-trip time (e.base RTT), if necessary. However the base round-trip time (e.base RTT) reflects the best-observed round-trip time between the two edge routers.

IV. IMPLEMENTATION

The various modules in the protocol are as follows:

A. Source Module:
First of all sending message is converted into packets and then these packets are forwarded to InRouter. The task of this Module is to send the packet to the InRouter router for further transfer of packets to destination.

B. InRouter Router Module:
An edge router operating a flow of packets from source router and passing it into a network through main router is called an In Router router. In other words the InRouter router is the one which is nearer to input port. InRouter router contains a flow classifier, per-flow traffic controller (e.g. leaky buckets), a feedback controller and rate controller.

C. Router Module:
The task of this Module is to accept the packet from the InRouter router and send it to the OutRouter router. It basically works as core router without any congestion occurrence problem.

D. OutRouter Router Module:
An edge router operating a flow of packets from main router to destination is called an OutRouter router. In other words the OutRouter router is the one which is nearer to output port. Rate monitoring allows an OutRouter 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) algorithm. OutRouter router contains a flow classifier, Rate monitor, and a feedback controller.

E. Destination Module:
The task of this Module is to accept the packet from the OutRouter router and stored in a file in the Destination machine.

V. WORKING

1. Sender sends a message to receiver.
2. The sender messages are received in the form of packets, then these packets are forwarded to InRouter using Leaky bucket algorithm.
3. At InRouter feedback control and rate control algorithm get invoked to prevent the Congestion collapse. And then router comes into picture.
4. Router accepts the packets from InRouter and forwards to OutRouter.
5. From the OutRouter the messages are transmitted to destination.
VI. CONCLUSION

To prevent Congestion, Retransmission of lost or dropped packets and increment in size of queue is not advisable. Also, there is a need of faster data transfer without the loss of packet while transmission. NBP is able to prevent congestion collapse by satisfying all the user’s demand. NBP provides proper utilization of bandwidth available to the systems. Hence based on our study Packet Drop Prevention Using NBP is a better technique for prevention of packets loss in the network.

ACKNOWLEDGEMENT

we would like to take this opportunity to thank all those individuals who have helped us in this project. We thank the management staff for providing the necessary resources and helping us out whenever required. We express our deep gratitude to our internal project guide Prof. Hasib Shaikh for providing timely assistance to our queries and the guidance that he gave us owning to his experience in their field for many years.

REFERENCES


Fig.1. Working of Network Border Protocol