EFFICIENT ALLOCATION OF BANDWIDTH & CONGESTION AVOIDANCE DURING DATA

[1]Yogendra. N Prajapati, [2]Pronob K Adhikari

[1,2]Assistant Professor, Ajay Kumar Garg Engineering College, Ghaziabad, UP, India

[1] prajapatiyogendra@akgec.ac.in, [2] adhikaripronab@akgec.ac.in

Abstract—**Today's internet sender-to-receiver congestion control is crucial for scalability and robustness, but it's important to note that the end-to-end algorithms are plagued by two distinct types of issues. The first is the potential for congestion collapse, and the second is the inequitable distribution of bandwidth among various applications. Network Border Patrol is a brand-new congestion avoidance method that we suggest and research. The main feature in this case is the feedback exchange between the routers that are situated at the start and end of the data exchange. Here, the starting point router's buffer scheme is also being used effectively. Simulated data is used to study effective bandwidth allocation and congestion avoidance during data flow. The effective transfer of preventing them from loss and discarding will be made possible by this method. By exchanging feedback with edge routers, it will monitor the packet flow rate**

Keywords— **Component, formatting, Style, Styling, Insert, Control of congestion, Congestion crumble, Ailments, Bandwidth allocation, Feedback**

I. INTRODUCTION

The word "scalability" is a good way to describe the functionality of the internet. All the protocols, algorithms, and services are useless if there is a scaling problem with the internet. Algorithms are moved as far out into the network's edges as they can go in order to solve this problem. TCP congestion control, which is accomplished at the beginning algorithms applied at one side systems, is one of the key instances of the Internet. However, if TCP congestion restrictions are used in the sender end to receiverend debate[1] there may be some problems. Due to its tight devotion to server end to receiver end, the current Internet suffers from two ailments.

Congestion control: congestion buildup from undelivered packets and unequal bandwidth allotment between two or more data packet flows. The issue is that undelivered packages cause congestion crumble because they continuously use up bandwidth even though they never get to their destination. Deliverable packets mostly use bandwidth because of their unresponsive flow[2]. This sort of congestion collapse is primarily caused by unresponsive flows, which are growing more common on the Internet as multimedia usage grows. However, there is currently no effective means to control these flows on the Internet. fair bandwidth allocation is the second issue with TCP congestion control. Malicious packet flow is the main cause of this. When they detect network congestion, responsive flow (TCP flow) slows its rate of transmission and, as a result, receives less bandwidth while competing withmalicious flow. Internet protocol design inherently introduces inequality. For instance, the TCP algorithm logically ensures that each TCP flow receives bandwidth that is more than its round-trip time. Giving significant weight to TCP connections with a short journey time may thus be irrational. Network bandwidth allotment in the case of extended travel periods.

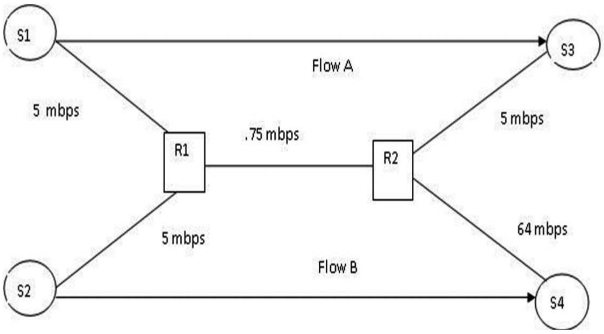

Fig 1.An illustration of a network with congestionproblems is a collapse

Consider Figure 1i set threshold value for available bandwidth as 400 (kilobyte per second) and using this threshold value finding all for an example of this fact. In thisinstance, a fair queuing mechanism acts as the arbitrator between two unconnected flows competing for bandwidth over two bottleneck connections in a network. To ensure that each flow obtains one-third of the link's available bandwidth at the initial bottleneck connection (R1 to R2), fair queuing is used (-25 kilobyte per second). Due to the lower capacity of the link, a large portion of the traffic from flow B is unneeded on R2 to S4 (64 kilobyte per second)[3].

As a result, whereas flow B can only handle 64 kilobyte per second, flow A can handle (-25) kilobyte per second. Flow B packets mistakenly decreased the throughput of flow A via the first bottleneck link before being rejected on the second bottleneck connection, which resulted in congestion collapse. On the initial bottleneck link, equal bandwidth is allocated to flows A and B, but their worldwide distribution is not max-min fair[4]. A maximum-minimum fair bandwidth allocation for flows A and B would have been 64 kbps and 6572 Mbps, respectively.

Finally, under TCP congestion control, connections may obtain disproportionately high allocations during short round trip periods compared to longer round trip times[5].

Many individuals have lately suggested that these types of issues may be resolved by adopting packet scheduling techniques such weighted fair queuing, core stateless fair queuing, etc.In this study, we suggest employing the Network Border Patrol technique to control congestion. We can monitor the rate of data transfer across a network using network border patrol[6]. Additionally, it would assist in resolving problems like uneven bandwidth distribution and congestion collapse. By preventing packet loss during the transfer process, it would assist in establishing a dependable data transfer path from source to destination.

Working aspects of CFR:
Mechanism:
The networks required architectural elements, specifically the upgraded edge routers,
The feedback control algorithm regulates the time andfrequency of data transfer between edge routes.

- There is no period after the “et” in the Latinabbreviation “et al.”.
- The abbreviation “i.e.” means “that is”, and theabbreviation “e.g.” means “for example”.
- An excellent style manual for science writers is [7].

II. IMPLEMENTATION

Network border patrol is an effective strategy for effective bandwidth distribution and for preventing congestion collapse, as we showed in the previous section. However, there are a number of substantial practical issues that must be overcome before NBP can be effectively deployed on the internet. A few of these issues are listed below.

Flow Scalability Classification: Its reliance on flow classification at edge routers may be the main barrier to NBP’s scalability. In a network with many flows, it may alsobecome expensive to maintain each flow’s state, communicate each flow’s feedback, and carry out each flow’s rate control and rate monitoring [10].Scalable Inter Domain Deployment: Creating connections across domains that use NBP is another strategy for enhancing its scalability. If trust connections cannot be formed to prevent congestion collapse both inside and across multiple domains, conventional border routers between the two domains may communicate congestion data[8]. Multicast routing, which permits copies of flow packets to exit the network, can be utilized with several egress routers. When this occurs, the backward feedback pack sent by each multicast flow’s egress router must be examined by the NBP ingress router[9]. The ingress router must run its rate control algorithm in order to detect whether the multicast traffic is congested.

III CONCLUSION

In this paper, we present network border patrol, an end-to- end control-free congestion avoidance method for the internet. To reduce congestion collapse brought on by undelivered packets, NBP employs a method. It tries to prevent packets from entering the network at the edge quicker than they can depart it.. In our upcoming work, we intend to conduct an analytical evaluation of NBP’s stability and convergence towards max-min fairness using the methodologies outlined above.

REFERENCES

[1]. 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. 2008.

[2]. V. Jacobson, “Congestion avoidance and control,” ACM Comput. Commun. Rev., vol. 18, no. 4, pp. 314– 329, Aug. 2009.

[3]. 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. 279–282.

[4]. IEEE Paper,2009 Network Border Patrol: PreventingCongestion Collapse

[5]. Shigang Chen and Na Yang. Congestion avoidancebased on lightweight buffer managementin sensor networks. IEEETrans. Parallel Distrib. Syst., 17(9):934–946, Septembe r2006.

[6]. Van Jacobson. Congestion avoidance and control. In SIGCOMM, pages 314–329, August 1988.

[7]. Chieh-Yih Wan, Shane B. Eisenman, and Andrew T. Campbell. Coda: congestion detection and avoidance in

[8]. M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.

[9]. MKS Y. N. Prajapati, International Journal of Roboticsand Automation (IJRA) 8 (3), 184-188

[10]. Sensor networks. In SenSys, pages 266–279,November 2003.

ABOUT THE AUTHORS

Yogendra Narayan Prajapati (B.Tech, M.Tech, PhD* (Assistant Professor at AKGEC, India, publish 12 paper in international journal and alsomember of IEEE, IET, IFERP, IEANG And research area in machine learning.

Pronab Kumr Adhikari B.Tech, M.Tech, (Assistant Professor at AKGEC, India, publish 4 paper in international journal and alsomember of IEEE, IET, IFERP and research area in computer network.