

Congestion Avoidance and Control Using Tokens at the Network Edge

Sameera Fatima¹

Nawab Shah College Of Engineering & Technology (Affiliated to JNTUH),

Waseema Masood²

Nawab Shah College Of Engineering & Technology (Affiliated to JNTUH),

ABSTRACT: Presently the Internet accommodates simultaneous audio, video, and data traffic. This requires the Internet to guarantee the packet loss which at its turn depends very much on congestion control. A series of protocols have been introduced to supplement the insufficient TCP mechanism controlling the network congestion. CSFQ was designed as an open-loop controller to provide the fair best effort service for supervising the per-flow bandwidth consumption and has become helpless when the P2P flows started to dominate the traffic of the Internet. Token-Based Congestion Control (TBCC) is based on a closed-loop congestion control principle, which restricts token resources consumed by an end-user and provides the fair best effort service with $O(1)$ complexity. As Self-Verifying CSFQ and Re-feedback, it experiences a heavy load by policing inter-domain traffic for lack of trust. In this paper, Stable Token-Limited Congestion Control (STLCC) is introduced as new protocols which appends inter-domain congestion control to TBCC and make the congestion control system to be stable. STLCC is able to shape output and input traffic at the inter-domain link with $O(1)$ complexity. STLCC produces a congestion index, pushes the packet loss to the network edge and improves the network performance. Finally, the simple version of STLCC is introduced. This version is deployable in the Internet without any IP protocols modifications and preserves also the packet datagram.

KEYWORDS: IP Protocols, Token Based Congestion Control(TBCC), P2P, Stable Token Limited Congestion Control(STLCC), Network Congestion, Inter Domain Link.

INTRODUCTION

Modern IP network services provide for the simultaneous digital transmission of voice, video, and data. These services require congestion control protocols and algorithms which can solve the packet loss parameter can be kept under control. Congestion control is therefore, the cornerstone of packet switching networks. It should prevent congestion collapse, provide fairness to competing flows and optimize transport performance indexes such as throughput, delay and loss. The literature abounds in papers on this subject; there are papers on high-level models of the flow of packets through the network, and on specific network architecture. Despite this vast literature, congestion control in telecommunication networks struggles with two major problems that are not completely solved. The first one is the time-varying delay between the control point and the traffic sources. The second one is related to the possibility that the traffic sources do not follow the feedback signal. This latter may happen because some sources are silent as they have nothing to transmit. originally designed for a cooperative environment. It is still mainly dependent on the TCP congestion control algorithm at terminals, supplemented with load shedding [1] at congestion links. This model is called the Terminal Dependent Congestion Control case Core-Stateless Fair Queuing (CSFQ) [3] set up an open-loop control system at the network layer, which inserts the label of the flow arrival rate onto the packet header at edge routers and drops the packet at core routers based on the rate label if congestion happens. CSFQ is the first to achieve approximate fair bandwidth allocation among flows with $O(1)$ complexity at core routers. According to CacheLogic report, P2P traffic was 60% of all the Internet traffic in 2004, of which Bit-Torrent [4] was responsible for

about 30% of the above, although the report generated quite a lot of discussions around the real numbers. In networks with P2P traffic, CSFQ can provide fairness to competing flows, but unfortunately it is not what end-users and operators really want. Token-Based Congestion Control (TBCC) [5] restricts the total token resource consumed by an end-user. So, no matter how many connections the end-user has set up, it cannot obtain extra bandwidth resources when TBCC is used. In this paper a new and better mechanism for congestion control with application to Packet Loss in networks with P2P traffic is proposed. In this new method the edge and the core routers will write a measure of the quality of service guaranteed by the router by writing a digital number in the Option Field of the datagram of the packet. This is called a token. The token is read by the path routers and interpreted as its value will give a measure of the congestion especially at the edge routers. Based on the token number the edge router at the source, thus reducing the congestion on the path. In Token-Limited Congestion Control (TLCC) [9], the inter-domain router restricts the total output token rate to peer domains. When the output token rate exceeds the threshold, TLCC will decrease the Token-Level of output packets, and then the output token rate will decrease.

LITERATURE SURVEY

Modern IP network services provide for the simultaneous digital transmission of voice, video, and data. These services require congestion control protocols and algorithms which can solve the packet loss parameter can be kept under control. Congestion control is therefore, the cornerstone of packet switching networks. It should prevent congestion collapse, provide fairness to competing flows and optimize transport performance indexes such as throughput, delay and loss. The literature abounds in papers on this subject; there are papers on high-level models of the flow of packets through the network, and on specific network architecture. Despite this vast literature, congestion control in telecommunication networks struggles with two major problems that are not completely solved. The first one is the time-varying delay between the control point and the traffic sources. The second one is related to the possibility that the traffic sources do not follow the feedback signal. This latter may happen because some sources are silent as they have nothing to transmit. Congestion control of the best-effort service in the Internet was originally designed for a cooperative environment. It is still mainly dependent on the TCP congestion control algorithm at terminals, supplemented with load shedding [1] at congestion links. This model is called the Terminal Dependent Congestion Control case. Although routers equipped with Active Queue Management such as RED [2] can improve transport performance, they are neither able to prevent congestion collapse nor provide fairness to competing flows. In order to enhance fairness in high speed networks, Core-Stateless Fair Queuing (CSFQ) [3] set up an open-loop control system at the network layer, which inserts the label of the flow arrival rate onto the packet header at edge routers and drops the packet at core routers based on the rate label if congestion happens. CSFQ is the first to achieve approximate fair bandwidth allocation among flows with $O(1)$ complexity at core routers. According to CacheLogic report, P2P traffic was 60% of all the Internet traffic in 2004, of which Bit-Torrent [4] was responsible for about 30% of the above, although the report generated quite a lot of discussions around the real numbers. In networks with P2P traffic, CSFQ can provide fairness to competing flows, but unfortunately it is not what end-users and operators really want. Token-Based Congestion Control (TBCC) [5] restricts the total token resource consumed by an end-user. So, no matter how many connections the end-user has set up, it cannot obtain extra bandwidth resources when TBCC is used.

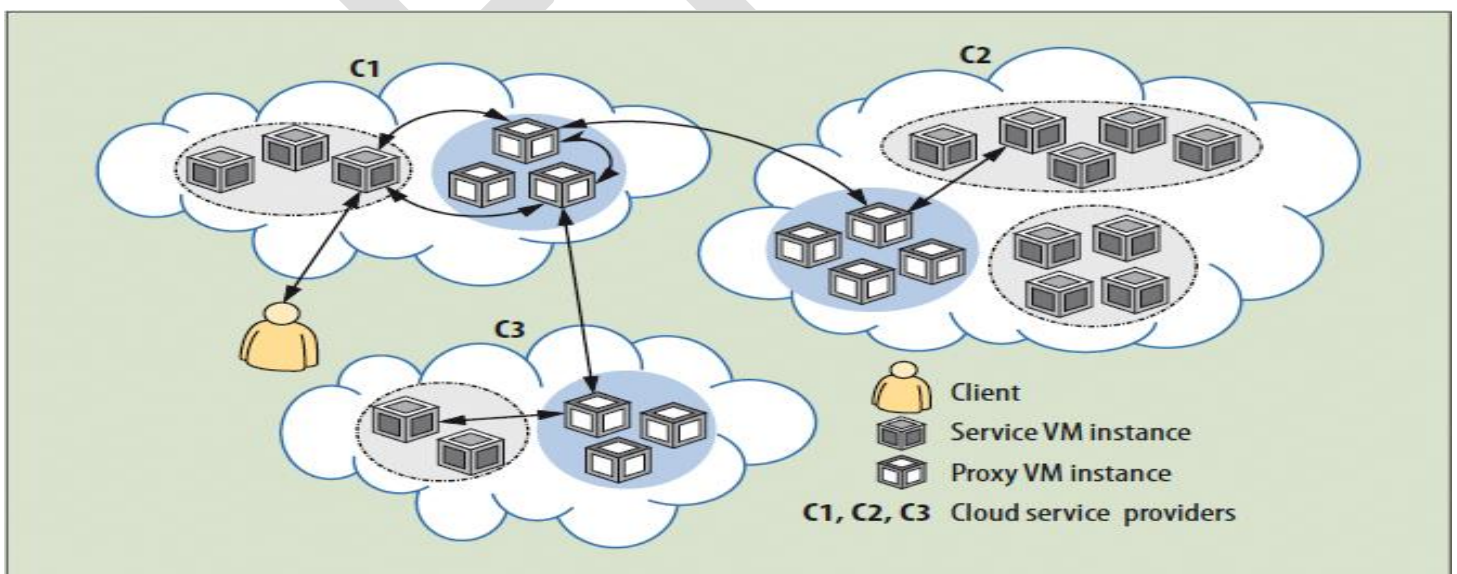
The Self-Verifying CSFQ [6] tries to expand CSFQ across the domain border. It randomly selects a flow, re-estimates the flow's rate, and checks whether the re-estimated rate is consistent with the label on the flow's packet. Consequently Self-Verifying CSFQ will put a heavy load on the border router and makes the weighted CSFQ null and void. In [7][8], the authors present a congestion control architecture Re-feedback, which aims to provide the fixed cost to end-users and bulk inter-domain congestion charging to network operators. Re-feedback not only demands very high level complexity to identify the malignant end-user, but also is difficult to provide

the fixed congestion charging to the inter-domain interconnection with low complexity. There are three types of inter-domain interconnection polices, the Internet Exchange Points, the private peering and the transit. In the private peering polices, the Sender Keep All (SKA) peering arrangements are those in which traffic is exchanged between two domains without mutual charge. As Re-feedback is based on congestion charges to the peer domain, it is difficult for Re-feedback to support the requirements of SKA. In this paper a new and better mechanism for congestion control with application to Packet Loss in networks with P2P traffic is proposed. In this new method the edge and the core routers will write a measure of the quality of service guaranteed by the router by writing a digital number in the Option Field of the datagram of the packet. This is called a token. The token is read by the path routers and interpreted as its value will give a measure of the congestion especially at the edge routers. Based on the token number the edge router at the edge routers. Based on the token number the edge router at the source's edge point will shape the traffic generated by the source, thus reducing the congestion on the path. In Token-Limited Congestion Control (TLCC) [9], the inter-domain router restricts the total output token rate to peer domains. When the output token rate exceeds the threshold, TLCC will decrease the Token-Level of output packets, and then the output token rate will decrease.

PROBLEM DEFINITION

The data packets has been losses many and time is wasted. Retransmission of data packets is difficulty. Modern IP network services provide for the simultaneous digital transmission of voice, video, and data. These services require congestion control protocols and algorithms which can solve the packet loss parameter can be kept under control. Congestion control is therefore, the cornerstone of packet switching networks . It should prevent congestion collapse, provide fairness to competing flows and optimize transport performance indexes such as throughput, delay and loss. The literature abounds in papers on this subject; there are papers on high-level models of the flow of packets through the network, and on specific network architecture.

SYSTEM ARCHITECTURE



METHODOLOGIES

1. NETWORK CONGESTION:

- Congestion occurs when the number of packets being transmitted through the network approaches the packet handling capacity of the network
- Congestion control aims to keep number of packets below level at which performance falls off dramatically

2. STABLE TOKEN LIMIT CONGESTION CONTROL (STLCC):

STLCC is able to shape output and input traffic at the inter-domain link with $O(1)$ complexity. STLCC produces a congestion index, pushes the packet loss to the network edge and improves the network performance. To solve the oscillation problem, the Stable Token-Limited Congestion Control (STLCC) is introduced. It integrates the algorithms of TLCC and XCP [10] altogether. In STLCC, the output rate of the sender is controlled according to the algorithm of XCP, so there is almost no packet lost at the congested link. At the same time, the edge router allocates all the access token resource to the incoming flows equally. When congestion happens, the incoming token rate increases at the core router, and then the congestion level of the congested link will also increase. Thus STLCC can measure the congestion level analytically, allocate network resources according to the access link, and further keep the congestion control system stable.

3. TOKEN

In this paper a new and better mechanism for congestion control with application to Packet Loss in networks with P2P traffic is proposed. In this new method the edge and the core routers will write a measure of the quality of service guaranteed by the router by writing a digital number in the Option Field of the datagram of the packet. This is called a token. The token is read by the path routers and interpreted as its value will give a measure of the congestion especially at the edge routers. Based on the token number the edge router at the source, thus reducing the congestion on the path.

4. CORE ROUTER

A core router is a router designed to operate in the Internet Backbone or core. To fulfill this role, a router must be able to support multiple telecommunications interfaces of the highest speed in use in the core Internet and must be able to forward IP packets at full speed on all of them. It must also support the routing protocols being used in the core. A core router is distinct from an edge routers.

5. EDGE ROUTER

Edge routers sit at the edge of a backbone network and connect to core routers. The token is read by the path routers and interpreted as its value will give a measure of the congestion especially at the edge routers. Based on the token number the edge router at the source, thus reducing the congestion on the path.

CONCLUSION AND FUTURE WORK

This paper is organized as follows. In section II, the architecture of Token-Based Congestion Control (TBCC), which provides fair bandwidth allocation to end-users in the same domain will be introduced. Section III evaluates two congestion control algorithms CSFQ and TBCC. In section IV, STLCC is presented and the simulation is designed to demonstrate its validity. Section V presents the

Unified Congestion Control Model which is the abstract model of CSFQ, Re-feedback and STLCC. In section VI, the simple version of STLCC is proposed, which can be deployed on the current Internet. Finally, conclusions will be given. To inter-connect two TBCC domains, the inter-domain router is added to the TBCC system as in Figure 8. To support the SKA arrangement, the inter-domain router should limit its output token rate to the rate of the other domains and police the incoming token rate from peer domains.

REFERENCES:

- [1] S. Floyd and V. Jacobson. Random Early Detection Gateways for Congestion Avoidance, ACM/IEEE Transactions on Networking, August 1993.
- [2] Ion Stoica, Scott Shenker, Hui Zhang, "Core-Stateless Fair Queueing: A Scalable Architecture to Approximate Fair Bandwidth Allocations in High Speed Networks", In Proc. of SIGCOMM, 1998.
- [3] D. Qiu and R. Srikant. Modeling and performance analysis of BitTorrent-like peer-to-peer networks. In Proc. of SIGCOMM, 2004.
- [4] Zhiqiang Shi, Token-based congestion control: Achieving fair resource allocations in P2P networks, Innovations in NGN: Future Network and Services, 2008. K-INGN 2008. First ITU-T Kaleidoscope Academic Conference.
- [5] I. Stoica, H. Zhang, S. Shenker, Self-Verifying CSFQ, in Proceedings of INFOCOM, 2002.
- [6] Bob Briscoe, Policing Congestion Response in an Internetwork using Refeedback, In Proc. ACM SIGCOMM05, 2005,