ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Packet Damage Handle Utilizing Tokens with the Network Border Utilizing WRED

Singampalli Ramu
MTech Student
Department of CSE
Sanketika Vidya Parishad Engineering College
P.M Palem, Visakhapatnam,AP.

V. Samuel Susan, M.Tech
Assistant Professor
Department of CSE
Sanketika Vidya Parishad Engineering College
P.M Palem, Visakhapatnam,AP.

Abstract:
Packet loss is taboo; to an Internet architect, it immediately signifies an inefficient design likely to exhibit instability and poor performance. In this paper, we argue that such an implication is not fundamental. In particular, there exist design points that provide many desirable properties including near optimal performance while suffering high loss rates. We focus specifically on congestion control, where researchers have long clung to the belief that loss avoidance is central to high throughput. A protocol that supports the sharing of resources that exist in different packet switching networks is presented. The protocol provides for variation in individual network packet sizes, transmission failures, sequencing, flow control, end-to-end error checking, and the creation and destruction of logical process-to-process connections. Some implementation issues are considered, and problems such as internetwork routing, accounting, and timeouts are exposed. initial TCP congestion control algorithm, the entire tradition of end-to-end congestion control has attempted to optimize network performance by tempering transmission rates in response to loss. We argue that by removing the unnecessary yoke of loss avoidance from congestion control protocols, by using Random Early Detection (RED)Detect incipient congestion. They can become less complex yet simultaneously more efficient, stable, and robust.

Keywords: ***TCP, Tokens, Network, Congestion Control Algorithm, Addressing, Formatting, Buffering, Sequencing, Flow Control, Error Control, Qos, Random Early Detection (RED).***

INTRODUCTION

There are a number of very good reasons to avoid loss in today's networks. Many of these stem from the fact that loss is often a symptom of overflowing router buffers in the network, which can also lead to high latency, jitter, and poor fairness. In the last few years considerable effort has been expended on the design and implementation of packet switching networks [1,2]A principle reason for developing such networks has been to facilitate the sharing of computer resources.

In this paper, we study whether the benefits of a network architecture that embraces rather than avoids widespread packet loss outweigh the potential loss in efficiency. We propose an alternative approach to Internet congestion control called decongestion control.

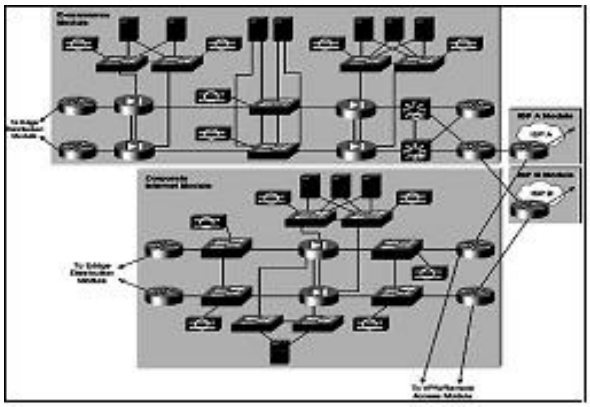

Fig1: packet switching communications at network Edge

In a departure from traditional approaches, end hosts strive to transmit packets faster than the network can deliver them, leveraging end-to-end erasure coding and

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

in-network fairness enforcement. In this paper we present a protocol design and philosophy that supports the sharing of resources that exist in different packet switching networks. After a brief introduction to internetwork protocol issues, we describe the function of a GATEWAY as an interface between networks and discuss its role in the protocol. [2,3,4]We then consider the various details of the protocol, including addressing, formatting, buffering, sequencing, flow control, error control, and so forth. A typical packet switching network is composed of a set of computer resources called HOSTS, a set of one or more packet switches, and a collection of communication media that interconnect the packet switches.The ensemble of packet switches and communication media is called the packet switching subnet as shown in Fig. 1. In a typical packet switching subnet, data of a fixed maximum size are accepted from a source HOST, together with a formatted destination address which is used to route the data in a store and forward fashion.

Literature Survey:

Improve TCP and Stay with end-point only architecture Enhance routers to help TCP and Random Early Discard with Enhance routers to control traffic and Rate limiting and Fair Queuing and Provide QoS by limiting congestion. We have discussed some fundamental Issues related to the interconnection of packet switching networks. In particular, we have described a simple but very powerful and flexible protocol which provides for variation in individual network packet sizes, transmission failures, sequencing, flow control, and the creation and destruction of process to process associations. We have considered some of the implementation issues that arise and found that the proposed protocol is implementable by HOST'S of widely varying capacity. The next important step is to produce a detailed specification of the protocol so that some initial experiments with it can be performed. These experiments are needed to determine some of the operational parameters of the proposed protocol.

Status of Analysis

Normally, we would expect the sender to abide by the window limitation. Expansion of the window by the receiver merely allows more data to be accepted. For the receiving HOST with a small amount of buffer space, a strategy of discarding all packets whose sequence numbers do not coincide with the current left edge of the window is probably necessary, but it will incur the expense of extra delay and overhead for retransmission. Every segment that arrives at the destination TCP is ultimately acknowledged by returning the sequence number of the next segment which must be passed to the process (it may not yet have arrived). Earlier we described the use of a sequence number space and window to aid in duplicate detection. Acknowledgments are carried in the process header and along with them there is provision for a "suggested window" which the receiver can use to control the flow of data from the sender. This is intended to be the main component of the process flow control mechanism.

Computer Networks

A network is nothing more than two or more computers connected by a cable or by a wireless connection so that they can communicate and exchange information or data.

In other words " Network Means a collection of interconnected computer network of stand-alone computer. Commenting on the computer for the exchange of information. The connection can be over copper, fiber optic, microwave and satellite communications".

Obviously, computers can exchange information in other ways called the sneakernet or FloppyNet. Means that copy a file to a diskette and then walk the disk over to some other computer.

You can create a computer network by hooking all the computers in your office together with cables and installing a special network interface card (NIC) in each computer so you have a place to plug in the cable.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Then you set up your computer's operating-system software to make the network work. If you don't want to mess with cables, you can create a wireless network instead. In a wireless network, each computer is equipped with a special wireless network adapter.

WIRELESS NETWORKS

Wireless networks use some sort of radio frequencies in air to transmit and receive data instead of using some physical cables. The most admiring fact in these networks is that it eliminates the need for laying out expensive cables and maintenance costs

EXISTING SYSTEM

In the existing system, the sender sends the packets without the intermediate station.

The data packets has been losses many and time is wasted. Retransmission of data packets is difficulty.

PROPOSED SYSTEM

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.

MODULES:

Network Congestion:
Stable Token Limit Congestion Control (STLCC)
Token
Core Router
Edge Router

Module Description:

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

STABLE TOKEN LIMIT CONGESTION CONTROL (STLCC):

STLCC is able to shape output and input traffic at theinter-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.

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

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

number the edge router at the source, thus reducing the congestion on the path.

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.

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.

Aim of the Work:

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.

An application may also decide to retry an operation that is taking a long time, in which case another set of To avoid all of these problems, the Internet Protocol allows for routers to simply drop packets if the router or a network segment is too busy to deliver the data in a timely fashion, or if the IPv4 header checksum indicates the packet has been corrupted. Obviously this is not ideal for speedy and efficient transmission of data, and is not expected to happen in an uncongested network. Dropping of packets acts as an implicit signal that the network is congested, and may cause senders to reduce the amount of bandwidth consumed, or attempt to find another path. For example, the TCP protocol is designed with a slow-start connection strategy so that excessive packet loss will cause the sender to throttle back and stop flooding the bottleneck point with data (using perceived packet loss as feedback to discover congestion). The data packets will be transmitted over a longer duration.

Problem Statement:

In the existing system, the sender sends the packets without the intermediate station.

The data packets has been losses many and time is wasted. Retransmission of data packets is difficulty.

- Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination.
- Packets will be added to the burden of delivering the original set. Such a network might also need a command and control protocol for congestion management, adding even more complexity.
- If the network made reliable guarantees on its own, that would require store and forward infrastructure, where each router devoted a significant amount of storage space to packets while it waited to verify that the next node properly received it. A reliable network would not be able to maintain its delivery guarantees in the event of a router failure.

Methodology

Existing congestion control protocols are susceptible to a variety of sender misbehaviors, many of which cannot be mitigated by router fairness enforcement. Because end points are already forced to cope with high levels of loss and reordering in steady state, decongestion is inherently more tolerant. The transmit time for this data is usually dependent upon internal network parameters such ascommunication media data

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

rates, buffering and signalling strategies, routeing, propagation delays, etc.

Senders always attempt to over-drive network links.Should available capacity increase at any router due to, for example, the completion of a flow, the remaining flows instantaneously take advantage of the freed link resources. To translate increased throughput into increased goodput, senders encode flows using an erasure coding scheme appropriate for the path loss rate experienced by the receiver.

Normally, we would expect the sender to abide by the window limitation. Expansion of the window by the receiver merely allows more data to be accepted. For the receiving HOST with a small amount of buffer space, a strategy of discarding all packets whose sequence numbers do not coincide with the current left edge of the window is probably necessary, but it will incur the expense of extra delay and overhead for retransmission. Every segment that arrives at the destination TCP is ultimately acknowlegded by returning the sequence number of the next segment which must be passed to the process (it may not yet have arrived). Earlier we described the use of a sequence number space and window to aid in duplicate detection. Acknowledgments are carried in the process header and along with them there is provision for a "suggested window" which the receiver can use to control the flow of data from the sender. This is intended to be the main component of the process flow control mechanism.

CONCLUSION:

Improve TCP and Stay with end-point only architecture Enhance routers to help TCP and Random Early Discard with Enhance routers to control traffic and Rate limiting and Fair Queueing and Provide QoS by limiting congestion.We have discussed some fundamental issues related to the interconnection of packet switching networks. In particular, we have described a simple but very powerful and flexible protocol which provides for variation in individual network packet sizes, transmission failures, sequencing, flow control, and the creation and destruction of processto- process associations. We have considered some of the implementation issues that arise and found that the proposed protocol is implementable by HOST'S of widely varying capacity. The next important step is to produce a detailed specification of the protocol so that some initial experiments with it can be performed. These experiments are needed to determine some of the operational parameters of the proposed protocol.

References:

1.G. Appenzeller, N. McKeown, J. Sommers, and P. Barford, "Recent Results on Sizing Router Buffers," in Proceedings of the Network Systems Design Conference, Oct. 2004.

2.M. Enachescu, Y. Ganjali, A. Goel, N. McKeown, and T. Roughgarden, "Part III: Routers with very small buffers," ACM/SIGCOMM Computer Communication Review, vol. 35, pp. 83- 90, July 2005.

[3] G. Appenzeller, N. McKeown, J. Sommers, and P. Barford, "Recent Results on Sizing Router Buffers," in Proceedings of the Network Systems Design Conference, Oct. 2004

[4] M. Enachescu, Y. Ganjali, A. Goel, N. McKeown, and T. Roughgarden, "Part III: Routers with very small buffers," ACM/SIGCOMM Computer Communication Review, vol. 35, pp. 83- 90, July 2005.

[5] L. Zhang, S. Shenker, and D. Clark, "Observations on the dynamics of a congestion control algorithm: The effects of two-way traffic," in Proceeedings of ACM SIGCOMM, pp. 133–147, Sept. 1991.

[6] F. R. E. Dell, "Features of a proposed synchronous data network," in Proc. 2nd Symp. Problems in the Optimization of Data Communications Systems, 1971, pp. 50—57.

[7] R. A. Scantlebury and P. T. Wilkinson, "The design of a switching system to allow remote access to computer services by other computers and terminal

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

devices," in Proc. 2nd Symp. Problems in the Optimization of Data Communications Systems, 1971, pp. 160-167.

[8] D. L. A. Barber, "The European computer network project," in Computer Communications: Impacts and Implications, S. Winkler, Ed. Washington , D.C., 1972, pp. 192-200.

[9] R. Despres, "A packet switching network with graceful saturated operation," in Computer rkshop on Quality of Service (IWQoS), June 2005. Communications: Impacts and Implications, S. Winkler, Ed. Washington, D.C., 1972, pp. 345-351.

[10] R. E. Kahn and W. R. Crowther, "Flow control in a resource-shaping computer network," IEEE Trans. Commun., vol. COM-20, pp. 539-546, June 1972.

[11] J. F. Chambon, M. Elie, J. Le Bihan, G. LeLann, and H. Zimmerman, "Functional specification of transmission station in the CYCLADES network. STST protocol" (in French), I.R.I.A. Tech. Rep. SCH502.3, May 1973.

[12] S. Carr, S. Crocker, and V. Cerf, "HOST-HOST Communication Protocol In the ARPA Network," in Spring Joint Computer Conf., AFIPS Conf. Proc., vol. 36. Montvale, N.J.: AFIPS Press, 1970, pp. 589-597.

[103] A. McKenzie, "HOST/HOST protocol for the ARPA network," in Current Network Protocols, Network Information Cen., Menlo Park, Calif., NIC 8246, Jan. 1972.

[14] L. Pouzin, "Address format in Mitranet," NIC 14497, INWG 20, Jan. 1973.

[15] D. Walden, "A system for interprocess communication in a resource sharing computer network," Commun. Ass. Comput. Mach., vol. 15, pp. 221-230, Apr. 1972.

[16] D. Katabi, M. Handley, and C. Rohrs, "Internet congestion control for future high bandwidth-delay product environments," in Proceedings of ACM SIGCOMM, Aug. 2002.

[17] S. Kandula, D. Katabi, B. Davie and A. Charny, "Walking the tightrope: Responsive yet stable traffic engineering," in Proceedings of ACM SIGCOMM 2005, Aug. 2005.