ISSN: 2321-7782 (Online)
Volume 2, Issue 1, January 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Paper
Available online at: www.ijarcsms.com

Novel Implementation of Enhancing Reliability of Transmission on High Performance Networks

KP. Vijay[1]
M.Tech (II Year)
Computer Science and Engineering
PRIST University, Kumbakonam campus.
India

S. V. Karthick[2]
Assistant Professor
Computer Science and Engineering
PRIST University, Kumbakonam campus.
India

Abstract: ***The end-to-end nature of Internet congestion control is an important factor in its scalability and robustness. However, end-to-end congestion control algorithms alone are incapable of preventing the congestion collapse and unfair bandwidth allocations created by applications, which are unresponsive to network congestion. In this, we propose and investigate a new congestion avoidance mechanism coupled with authenticated mode of data transfer. It is a core-stateless congestion avoidance mechanism, which relies on the exchange of feedback between routers at the borders of a network in order to detect and restrict unresponsive traffic flows before they enter the network and to transmit the data securely by employing the cryptographic technique. This mechanism is compliant with the Internet philosophy of pushing complexity toward the edges of the network whenever possible. It helps to audit packets that are received or sent in Local Area Network. It entails the exchange of feedback between routers at the borders of a network in order to detect and restrict unresponsive traffic flows before they enter the network, thereby ensuring that packets are transferred without loss in a network. It also ensures data security by applying cryptographic methods.***

Keywords: TCP, Congestion, Data transfer, acknowledgement.

I. INTRODUCTION

In the world of computers, networking is the practice of linking two or more computing devices together for the purpose of sharing data. Networks are built with a mix of computer hardware and computer software. Networks consist of the computers, wiring, and other devices, such as hubs, switches and routers that make up the network infrastructure. Some devices, such as network interface cards, serve as the computer's connection to the network. Devices such as switches and routers provide traffic- control strategies for the network. All sorts of different technologies can actually be employed to move data from one place to another, including wires, radio waves, and even microwave technology. A router is an internetworking device that forwards packets between networks by processing information found in the datagram or packet (Internet protocol information from Layer 3 of the OSI Model). In many situations, this information is processed in conjunction with the routing table (also known as forwarding table). Routers use routing tables to determine what interface to forward packets (this can include the "null" also known as the "black hole" interface because data can go into it, however, no further processing is done for said data).

While the loss of data has become a major problem that needs to be solved in all kinds of organizations, the routes along which data can be lost have become complicated and numerous, making data loss countermeasures all the more difficult. The fundamental philosophy behind the network is expressed by the scalability argument: no protocol, mechanism, or service should be introduced into the network if it does not scale well. A key corollary to the scalability argument is the end-to-end argument: to maintain scalability, algorithmic complexity should be pushed to the edges of the network whenever possible .Perhaps the best example of the network philosophy is TCP congestion control, which is implemented primarily through algorithms

operating at end systems. Unfortunately, TCP congestion control also illustrates some of the shortcomings the end-to-end argument. As a result of its strict adherence to end-to-end network traffic, the current Internet suffers from main malady: congestion collapse from undelivered packets. The Internet's excellent scalability and robustness result in part from the end-to-end nature of network congestion control. End-to-end congestion control algorithms alone, however, are unable to prevent the network traffic and unfairness created by applications that are unresponsive to network congestion.

This system entails the exchange of feedback between routers of a network in order to detect and restrict unresponsive traffic flows before they enter the network, thereby preventing congestion within the network. It also ensures safe transmission of data over the network by implementing the techniques used in cryptography.

Scope of Data Transmission in Network

A Network must prevent congestion from the undelivered packets in a network. It ensures that packets are delivered at the right destination. It also ensures that the data is hidden while transfer. The transfer of data at the edge routers and at the router designed is hidden using cryptographic standards and hence any unauthorized access or view of the data is prevented.

Designated Data Loss Prevention solutions

Designated Data Loss Prevention solutions detect and prevent unauthorized attempts to copy or send sensitive data, intentionally or unintentionally, without authorization, mainly by personnel who are authorized to access the sensitive information.

II. TCP CONGESTION CONTROL ALGORITHM

TCP is the most widely accepted reliable, connection-oriented, full-duplex, byte stream transport level protocol that is in use today. It is basically developed for the data communication over reliable network environments. There are millions of network applications that have already been built on top of TCP and will continue to be in the foreseeable future. With the invention of handheld devices and laptops, new environments such as mobile telephony and Wireless LANs are now becoming ubiquitous. As a result of these , there is a significant increase in the number of combined wired and wireless networks. We could expect significant usage of the commonly used TCP/IP protocol stack in these systems, considering massive amount of popular network applications deployed on the top of TCP. One considerable problem that has emerged and received attention in research is the performance of the TCP over a mobile, wireless link. Optimizing TCP performance over these networks would have a broad and major impact on the user perceived data application performance. However, it is important to improve its performance without any modification to the application interface provided by TCP on fixed hosts (FHs), as this is the only way by which mobile devices communicating on wireless links can seamlessly integrate with the rest of the wired Internet.

The TCP congestion control algorithm is the existing implementation which avoids end to end congestion in the network. This TCP congestion control algorithm suffers from congestion collapse from undelivered packets. The percentage of traffic carried by UDP is increasing as non-TCP applications like stream media grow in popularity. Unlike TCP, UDP does not perform any congestion control and instead leaves this responsibility to its applications. It is not possible to rely on all applications to incorporate congestion control mechanism and if the network does not control its resource utilization, it may lead to congestion collapse from undelivered packets. Congestion collapse from undelivered packets arises, when bandwidth is wasted by delivering packets through the network that are dropped before reaching their ultimate destination. Moreover the Internet protocols themselves are responsible for unfair allocations of bandwidth between competing traffic flows. For instance, each TCP flow receives a bandwidth that is inversely proportional to its round trip time. Hence, TCP connections with short round trip times may receive unfairly large allocations of network bandwidth when compared to connections with longer round trip times.

TCP Behaviour and Loss Recovery

One of the reasons for the widespread usage of TCP over the Internet (as well as intranets and extranets) is its inbuilt flow and congestion control algorithms and its end-to-end reliability. TCP assumes that packet losses are caused by congestion in a network and applies congestion control techniques in order to give the network a chance to recover. We briefly introduce them below for the sake of continuity.

TCP Congestion Control

The implementation of the congestion control scheme is intertwined with TCP‘s window based flow control scheme through the use of two sender-side state variables congestion window (cwnd) and the slow start threshold (thresh) both of which are measured in bytes. A TCP sender is never allowed to have more bytes outstanding than the minimum of the advertised window (by the receiver) and the congestion window. So, a TCP sender‘s load on the network is limited by flow control imposed by the receiver and implicitly by the congestion in the network . TCP uses the sliding window mechanism, as illustrated in fig.1 below; to accomplish reliable, in-order delivery and flow / congestion control. The basis of TCP congestion control lies in the following algorithms: slow start, congestion avoidance, fast-retransmit and fast recovery. TCP-Tahoe implements the slow-start, congestion avoidance and fast-retransmit algorithms. TCP-Reno implementation modified the TCP sender logic to include the fast recovery algorithm.

TCP’s Response to Packet Loss

A TCP packet, after transmission is determined to have been lost either if no acknowledgement (ACK) is received within the Retransmission Timeout (RTO) period or if multiple duplicate ACKs (Dup ACK) arrive for the packet prior to the one that was lost. TCP continually measures how long the acknowledgments take to return. It maintains a running average of this delay (Round Trip Time - RTT) and an estimate of the expected deviation in delay from the average (Delay Variation). These RTT measurements are collected and the RTO is set to the sum of the smoothed RTT (or approximate average) and four times its mean deviation. When a lost packet is determined by expiration of the RTO, TCP initiates an exponential back-off of the RTO and enters the slow start and congestion avoidance mode. The exponential back-off of the RTO involves doubling its value with successive failure of packet retransmissions. Then actions are taken so as to evade network congestion with the help of reduced transmission rate. It is important to note here that multiple lost packets will cause the slow start threshold to be repeatedly reduced, and thus the congestion avoidance mode will dominate and the packet transmission rate will grow very slowly. This can lead to degradations in throughput.

III. ANTICIPATED WORK

Achieving a Secured Data Transfer in an Network Environment

The use of conventional thin clients cannot adequately provide safe sharing of sensitive information across multiple organizations. Secured Network Packet Auditing System overcomes the problems by the exchange of feedback between routers at the borders of a network in order to detect and restrict unresponsive traffic flows before they enter the network, thereby preventing congestion collapse within the network. The primary idea behind congestion control mechanism is to compare, at the borders of the network, the rates at which each flow’s packets are entering and leaving the network. If packets are entering the network faster than they are able to leave the network, then this implies that either the packet are buffered or discarded by some core router. In other words the network is congested. This can be prevented, by measuring the rate at which a flow’s packets are leaving the network and ensuring that they don’t enter the network at a greater rate. This guarantees that the network will not get congested, as an unresponsive flow’s packets are not allowed to enter the network in the first place. Since only the routers at the edges of the network are modified and the core routers are left unchanged this subscribes to the Internet design philosophy of keeping the router implementations simple and pushing the complexity to the edges of the network. The Cryptographic Algorithm is used to encrypt and decrypt the data to be sent on the network, so the data transferred is secured.

The main goal of this mechanism is to transmit the data securely and to prevent congestion collapse from undelivered packets. But when combined with fair queuing at core routers, it can achieve global max-min fairness.

Application Layer Performance and Rate Control Algorithm

In this Section, we consider four different traffic classes for exploring the impact of the RCAs on application level throughput. Application layer performance is what ultimately affects the session quality of the mobile user. Similar to the ones proposed in universal mobile telecommunications service (UMTS), we use the following four traffic classes: (i) *Heterogeneous* (ii) *Streaming* (iii) *Interactive* and (iv) *Background* traffic. Examples of each traffic classes are *VoIP*, *video streaming*, *web browsing* and *file download* respectively.

System Implementation

In this system the data is sent from source to destination in an network such that the data is not being lost at the destination even in case of excessive network traffic.

An edge router operating on a flow passing into a network is called an ingress router. This mechanism prevents congestion collapse through a combination of per-flow rate monitoring at egress routers and per-flow rate control at ingress routers. Rate control allows an ingress router to police the rate at which each flow's packets enter the network. Ingress Router contains a flow classifier, per-flow traffic shapers (e.g., leaky buckets), a feedback controller, and a rate controller.

A Router accepts the packet from the Ingress router and send it to the Egress router. An edge router operating on a flow passing out of a network is called an egress router. It prevents congestion collapse through a combination of per-flow rate monitoring at egress routers and per-flow rate control at ingress routers. Rate monitoring allows an egress 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. Egress Router contains a flow classifier, Rate monitor, a feedback controller.

At the destination the packet from the Egress router and store in a file in the Destination machine. The message received from the Egress Router will be stored in the corresponding folder as a text file depending upon the source machine name.

ALGORITHMS USED

Three main algorithms are used in the proposed system namely

i) Leaky Bucket algorithm,

ii) Rate control algorithm and ,

iii) Time Sliding Window algorithm.

Leaky Bucket algorithm

- The Leaky Bucket Algorithm used to control rate in a network. It is implemented as a single-server queue with constant service time. If the bucket (buffer) overflows then packets are discarded.
- The leaky bucket enforces a constant output rate regardless of the burstiness of the input. Does nothing when input is idle.
- The host injects one packet per clock tick onto the network. This results in a uniform flow of packets, smoothing out bursts and reducing congestion.
- When packets are the same size (as in ATM cells), the one packet per tick is okay. For variable length packets though, it is better to allow a fixed number of bytes per tick.

- For traffic of packet, incoming data is larger.In interface ,the leaky bucket algorithm takes the packet size in the structure mentioned below.

VT = MAX(VT,CT)

IF (VT + (PS/AR) > CT + B)

DROP INCOMING PACKET

ELSE

DIVIDE THE PACKET INTO SEGMENTS

PUT THE SEGMENT IN THE BUCKET

VT = VT + (PS/AR)

Where VT is virtual time,CT is current time, B is burst, PS is packet size, AR is average rate.

Scheme of Rate control

Based on minimum distortion based QP estimation mode decision process and motion complexity measure, we propose a rate control scheme. This scheme includes two levels of rate control: frame-level rate control and MB-level rate control. At Frame-level rate control, we estimate the target bit of current frame according to motion complexity. At MB-level rate control, we estimate QP in the mode decision process, according to the minimum distortion after all-mode motion estimation. The target bit of current MB is estimated equally. The steps are as follows :

1. Estimate target bit and QP of frame.
2. Estimate target bit and QP of MB.
3. Update parameters of QP and MB model.
4. Finish the frame then update frame level bit model and QP model.

Time Sliding Window algorithm

TCP implements an algorithm for flow control called *Sliding Window*; the reader will surely be familiar with this kind of algorithms which are used for flow control at the data link control layer of some protocols as well, so only a short explanation is provided here.

The "window" is the maximum amount of data we can send without having to wait for ACKs. In summary, the operation of the algorithm is as follows:

1. Transmit all the new segments in the window.
2. Wait for acknowledgement/s to come (several packets can be acknowledged in the same ACK).
3. Slide the window to the indicated position and set the window size to the value advertised in the acknowledgement.

When we wait for an acknowledgement to a packet for some time and it has not arrived yet, the packet is retransmitted. When the acknowlegement arrives, it causes the window to be repositioned and the transmission continues from the packet following the one transmitted last.

IV. CONCLUSION

In this paper we have presented a novel congestion-avoidance mechanism describing the current activities towards the prevention of data loss in a multi-organization environment for the network and in network environments called Internet.

Unlike existing congestion control approaches, which rely solely on end-to-end control, this mechanism is able to prevent the network traffic from undelivered packets and enables secured data transfer. This provides fair bandwidth allocations in a core-stateless fashion. It ensures at the border of the network that each flow's packets do not enter the network faster than they are able to leave it, while at the core of the network that flows transmitting at a rate lower than their fair share experience no congestion, i.e., low network queuing delay. This allows the transmission rate of all flows to converge to the network fair share.

This mechanism requires no modifications to core routers or to end systems. Only edge routers are enhanced so that they can perform the requisite per-flow monitoring, per-flow rate-control and feedback exchange operations, while the existing system has a simple core-stateless modification to core routers. Simulation results show that it is successfully prevents network traffic from undelivered packets. They also show that, while this mechanism is unable to eliminate unfairness on its own, it is able to achieve approximate global max-min fairness for competing network flows. It approximates global max-min fairness in a completely core-stateless fashion.

References

1. Improving TCP performance in Network with frequent disconnections. Purvang Dalal, Nikhil Kothari and K. S. Dasgupta
2. S. Ryu, C. Rump, and C. Qiao, "Advances in Internet congestion control," IEEE Communications Surveys and Tutorials, vol. 3, pp. 28–39, 2003.
3. W. Stevens, TCP Illustrated, Volume 1. Reading, MA: Addison-Wesley, Professional Computing Series, 1984.
4. Y. Tian, K. Xu, and N. Ansari,"TCP in Wireless Environments: Problems and Solutions," IEEE Commun. Mag., vol. 43, no. 3 Mar. 2005, pp. S27–S32.
5. R. Roy, S. Das, A. Ghosh, and A. Mukherjee, "Modified TCP congestion control algorithm for throughput enhancement in wired-cum-wireless networks" In Proceedings of the 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), 2007.
6. C. Zhang and V. Tsaoussidis. TCP Real: Improving Real-Time Capabilities of TCP Over Heterogeneous Networks," Proc. 11th IEEE/ACM NOSSDAV 2001, New York, 2001, pp. 189–98.
7. Techniques for Eliminating Packet Loss in Congested TCP/IP Networks. Wu-Chang Feng, Dilip D. Kandlur, Debanjan saha, and Kang G. Shin.
8. Study of Proposed Internet Congestion control algorithms. http://www.nist.gov/itl/cxs/index.cfm
9. Characterizing Sources and Remedies for Packet Loss in Network Intrusion Detection Systems . Lambert Schaelicke, J. Curt Freeland
10. A Novel Approach to Reduce Packet Loss in OBS Networks. Amit Gupta, Harbhajan Singh, Jagdish Kumar.
11. Phua, C., Protecting organisations from personal data breaches, Computer Fraud and Security, 1:13-18, 2009.

