FLoadAutoRED: An Active Queue Management Scheme to Prevent Congestion in a Dynamically Varying Traffic in IP Networks

CHAPTER 1

INTRODUCTION

INTRODUCTION

Internet has grown as the most powerful knowledge and information repository, as an extremely popular communication and entertainment media, and a platform on which various networking applications could be developed. The flourish of the Internet is mainly due to the great success achieved by the TCP/IP protocol stack in providing a robust yet simple network platform. TCP is designed to provide a reliable service over packet-switched IP networks. With the increasing variety of the Internet users in the current heterogeneous IP network, the end systems can behave aggressively during congestion to enjoy better service in the TCP/IP networks. Therefore the intermediate routers in IP networks should be enhanced to prevent end systems from misbehaving to reach its full potential.

1.1 IP NETWORKS

Internet is no longer a small, closely knit user community but an expanded large community network resulting in increased network traffic. It is a packet-switched network with nodes in the network passing data to other nodes along links. Packets are routed from one link to the next via nodes, more commonly, routers. Routers usually buffer incoming packets before they are transmitted on an outgoing link.

All requested connections are admitted, and the available capacity is shared between the connections as shown in Figure 1.1. As a result, no explicit guarantees can be given about the bandwidth availability to each connection. However, the simplicity of the network infrastructure is compelling, since there is no concept of connection within the network, only the ability to forward packets is required of the network. This simplicity is the key reason for the success of IP networks. IP networks are so active and growing worldwide that they are dominating and influencing the global market in various vital applications.

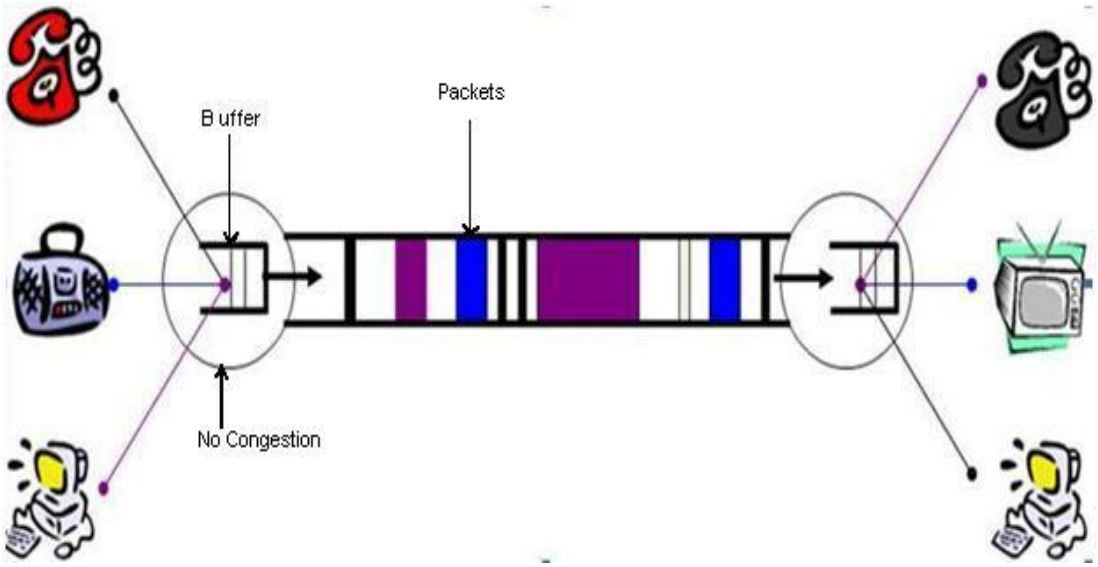

Figure 1.1 Simple IP Network

1.1.1 APPLICATIONS OF IP NETWORKS

At present, the development and need of distributed data and multimedia applications are growing rapidly in the IP networks. Some common examples [1] are Video conferencing, Internet telephony, On-line games, File transfer; Internet banking, Email distributions, News updates, Stock updates and E-business. Introduction of these applications has opened a series of exciting opportunities in business, leisure, education and many other areas. Therefore, significant developments have been made to design networks with the ability to guarantee the QoS for the dynamically varying traffic across the IP network for these application-oriented operations.

Further, the deployment of these applications increases the percentage of dynamic varying traffic in the Internet resulting in congestion and starvation of TCP traffic. Such an effect in Internet results in multiple packet losses, low throughput and low delay leading to a congestion collapse. Internet multimedia and data applications cannot tolerate such performance degradation due to congestion. Therefore, IP networks face various research challenges to be overcome to promote the capabilities of these applications.

1.1.2 RESEARCH CHALLENGES IN IP NETWORKS

The history of the Internet reflects the problem of controlling congestion in networks. Congestion collapse occurs when the load of packets placed onto the network exceeds the networks' capacity to carry the packets. An approach is required to ensure that the load of packets placed onto the network is within the capacity of the network.

When the capacity available is less than the demand for capacity, congestion mechanism [1] is the critical element which determines how many packets are allowed onto each link of the network, which user gets to send them and when. This controls the Quality of Service (QoS) metrics such as bandwidth, delay and jitter experienced by users.

Packet loss is also possible in IP networks because the packets from many sources are temporarily stored in a queue prior to transmission over an outgoing link in a router. Since the queue is finite, an arriving packet is lost (or dropped) in the network if there is no space left in the queue when the network is congested. Packet loss can cause severe damage to QoS of the applications.

A congestion mechanism should ensure that hosts do not send packets onto the network at a rate that exceeds the networks' capacity. However, if this rate is greater than the rate at which the network can serve the packets, backlog will inevitably be built inside the routers in the network. Congestion mechanism has their place in ensuring that this backlog stored is minimum in the routers to control the Quality of Service metrics for all applications.

The need to meet the requirements of increasingly more bandwidth hungry applications and a growing user population puts pressure on the amount of capacity that needs to be provisioned on the Internet. It is worth considering the future and what impact the continuing increase in capacity and user population creates on the nature of congestion, and the QoS experienced. The next section briefs about the important factors for the congestion to occur.

1.1.3 CONGESTION IN IP NETWORKS

A network is congested when one or more network components discard packets due to lack of buffer space [3]. Congestion is caused by a shortage of buffer space, and can be solved by increasing the size of buffers. Congestion is also caused by slow links. Congestion is caused by slow processors. There are solutions to handle congestion due to anyone or all the three types. Practically speaking, congestion cannot be solved with a large buffer**:** this only postpones the inevitable packet loss when network load is larger than network capacity. Slow links by themselves do not cause congestion, but the mismatch of network link speed cause congestion. Similarly, slow processors do not cause congestion, however the introduction of a high-speed processor in an existing network may actually increase the mismatch of processing speeds and the chances of congestion. In fact, congestion may also occur even if all links and processors are of the same speed.

Figure 1.2 demonstrates the problem of congestion. Congestion occurs when network components are unable to determine the rate of data flow that can be sustained between the source and the destination as discussed in [2]. Incase of a source transmitting data at a rate too high to be sustained between it and the destination, one or more routers will begin to queue the packets in their buffers [1].

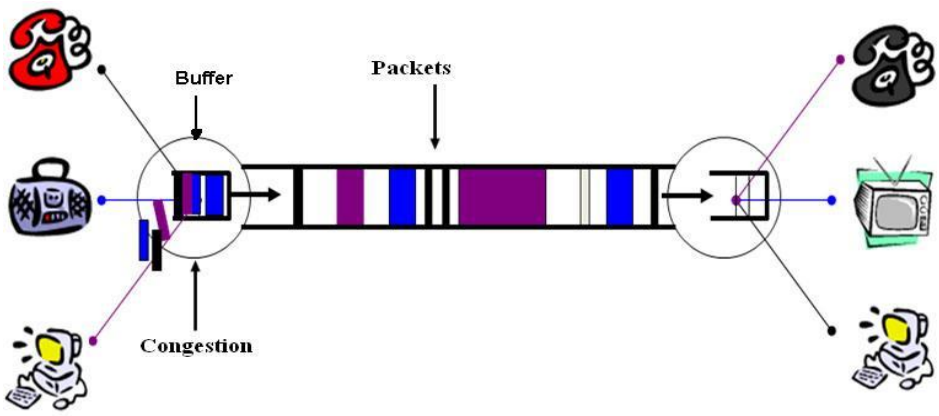

Figure 1.2 Congestion in Simple IP Network

If the queuing continues, the buffers will become full and packets from the source will be discarded, causing data loss. If the source is attempting to guarantee transmission reliability, the result is retransmission of data and increased transmission time between the source and the destination.

As the rate of data or load transmitted through the network increases, the rate of data reaching the destination also increases linearly. However, as the load reaches the networks' capacity, the buffers in the routers begin to fill. This increases the response time or time for data to traverse the network between source and destination and lowers the throughput. Increase in response time also increases the queuing delay of the network.

Once the buffers in routers begin to overflow, packet loss occurs. Increase in load at this point increases the probability of packet loss. In a network under extreme load conditions, response time approaches infinity and the throughput approaches zero and hence the network reaches the point of congestion collapse. However, the special characteristics of the multimedia and data applications increase the percentage of dynamic varying traffic in the Internet resulting in congestion and starvation of TCP traffic. Such an effect in Internet results in multiple packet losses, low throughput and high delay leading to a congestion collapse. The performance of the network is affected thereby. Internet multimedia and data applications cannot tolerate such performance degradation due to congestion.

According to Stevens W. et al [7], lack of attention to the dynamics of packet forwarding can result in "severe service degradation" or "Internet meltdown" or "congestion collapse". This phenomenon was first observed during the early growth phase in Internet in mid 1980s. Van Jacobson [4] fixed originally the Internet meltdown. Thereafter, many congestion handling mechanisms are adopted to solve the problem of congestion in Internet.

1.2 CONGESTION HANDLING MECHANISMS

Two approaches are generally adopted to solve the problem of congestion. As shown in Figure 1.3, first is **Congestion Control**, which comes into play after the congestion at a network has occurred and the network is overloaded. Second is **Congestion Prevention** technique, which comes into play before network is congested by overloading.

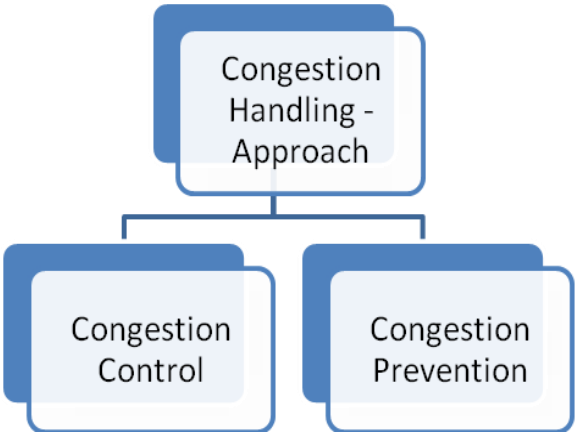

Figure 1.3 Congestion Handling Approach

A congestion preventive scheme is a proactive one that maintains the network in a state of low delay and high throughput by keeping the average queue size moderate to accommodate bursty traffic and transient congestion. However, the first one is a reactive scheme that reacts after the congestion occurs. A Proactive approach would be beneficial or suitable for a dynamically varying traffic in IP networks as the congestion can be detected, regulated and prevented at the earliest.

Congestion as shown in Figure 1.4 can be regulated and taken care either by **End hosts** or by the network itself i.e. in the network component – **Router.** In a router-centric mechanism [2], each router takes the responsibility for deciding when packets are forwarded and which packets are to be dropped and how many packets are allowed to send. In a host-centric design, the end hosts observe the network conditions and adjust their behavior accordingly. These two are not mutually exclusive.

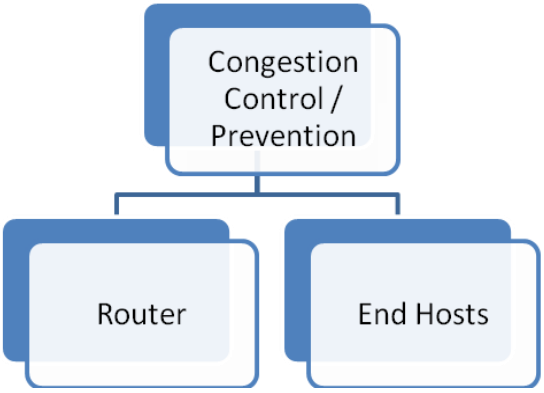

Figure 1.4 Level of Congestion Handling

A network that places the primary burden for managing congestion on routers still expects the end host to adhere to any advisory messages the routers send. Therefore, the router in network that uses end-to-end congestion control has some policy for deciding which packets to drop when their queues do overflow.

Stevens. W. et. al [7] developed the congestion avoidance mechanisms that are required in TCP implementations. These mechanisms operate in the hosts to cause TCP connections to "back off" during congestion. TCP flows are "responsive" to congestion signals (i.e., dropped packets) from the network. It is primarily these TCP congestion avoidance algorithms that prevent the congestion collapse of earlier days of Internet. However, it was not the end and considerable research continued on Internet dynamics, and the Internet has grown to a very large extent today. It is clear that the TCP congestion avoidance mechanisms [7] that are necessary and powerful are not sufficient to provide good service in all circumstances. Basically, there is a limit to how much control can be accomplished from the edges of the network. Some mechanisms are needed in the routers to complement the endpoint congestion avoidance mechanisms.

The congestion is generally produced at the buffers that routers use for queuing packets in an IP network. As a result, in case of heavy traffic, router

gets congested and further due to unresponsive and non TCP-compatible flow, the danger of congestion collapse is likely to occur. Therefore buffer space in routers is a key resource in IP networks and resource allocation must be done efficiently in routers of IP networks.

In a router-centric design, indication of congestion to end sources can be **Implicit** or **Explicit** as shown in Figure 1.5.

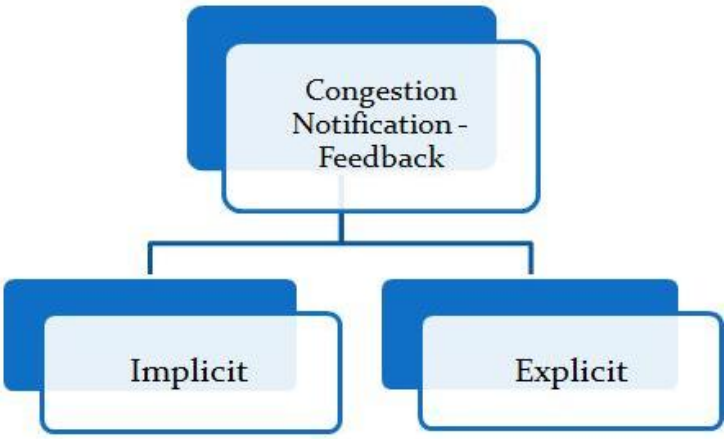

Figure 1.5 Congestion Notification - Feedback

In an explicit congestion notification [2], a bit is set by routers in the packet when congestion is encountered. It requires two bits; one is set by the source to indicate that it is Explicit Congestion Notification (ECN) capable, (i.e), its ability to react to a congestion notification. The other is set by routers along the end-to-end path when congestion is encountered. The latter bit is also echoed back to the source by the destination host. The end host responds to the ECN bit set in exactly the same way it responds to a dropped packet. However, in an implicit packet drops at the routers, congestion is indicated to the end sources in the network. Then the end host adjusts its sending rate or window size according to the congestion indication by the routers. In a host-centric, the feedback approach is such that the end hosts begin sending data rate and then adjust their sending rate according to the feedback they receive. This feedback can be explicit i.e a congested router sends a “slow down” message to the host

or it can be implicit, i.e the end host adjusts its sending rate according to the externally observable behavior of the network such as packet losses.

Therefore, to regulate the dynamic flows in IP networks, buffer space in routers must be properly managed to achieve good performance which would otherwise cause performance degradation. Each router implements queuing discipline that governs how packets are buffered while waiting to be transmitted. Hence, an efficient **Queue management** [5] [6] is required to handle the Internet applications with dynamically varying load flooding the Internet routers with data.

1.2.1 QUEUE MANAGEMENT

In IP networks, the overall goal of congestion prevention mechanism is to optimize the performance during communication. Optimization implies, sending rates at the data sources should be as high as possible, without overloading the network. The primary measure of network overload is packet loss; when the arrival rate at a link exceeds capacity, the corresponding queue starts to build up, and when the queue is full, packets are discarded. The bottleneck links in the network should be fully utilized. The requirement of a small loss rate implies that the average arrival rate at each bottleneck link should either match the link capacity exactly, or be very slightly larger. When the network is shared with dynamic traffic, it becomes important not only to maintain a small packet loss rate, but also to maintain reasonably moderate queues, since large queues imply large delays.

Congestion mechanism has been a very active area of research during the last decade. Therefore in IP networks, resource allocation is the process by which network elements try to meet the competing demands that the applications have for network resources like link bandwidth and buffer space in routers. The congestion prevention mechanism determines how resources are shared between users. The network load is constantly varying, links have

varying capacity and delay. The congestion mechanism must react to these changes and adjust the sending rates so as to reduce the probability of packet loss due to congestion.

In case of dynamically varying traffic in IP networks, large queues and large queue fluctuations can harm applications using the network and moreover all bottleneck links should be fully utilized. Therefore to fully utilize the links in Internet, buffer space in routers must be properly allocated and managed to achieve high performance otherwise the performance of the Internet would deteriorate. Hence an efficient Queue management is required to handle the Internet applications flooding the routers with the intention to maximize their utilisation. These mechanisms should improve the situation in IP networks to all the users rather than causing great pain to a few and finally resulting in congested routers.

Queue management in routers plays an important role in congestion handling. The two main objectives of queue management is high link utilization with low packet loss and low packet queuing delay. Hence the queue management at router level of an IP network becomes a challenge. Queue management is strongly associated with packet drop that is when to drop a packet and which packet to drop. Queue management is associated with how a network effectively and fairly allocates its resources.

In recent years, research activities have come out with various queue management mechanisms in IP networks to completely handle Internet traffic. Each of these mechanisms has certain limitations especially in heavy network traffic and therefore research has become a continuous process in identifying the best Queue Management algorithm. These mechanisms can be classified as passive queue management i.e traditional queue management and active queue management as shown in Figure 1.6. Congestion in routers results in high packet loss leading to high cost that can be reduced by A**ctive Queue Management** scheme [5] [6].

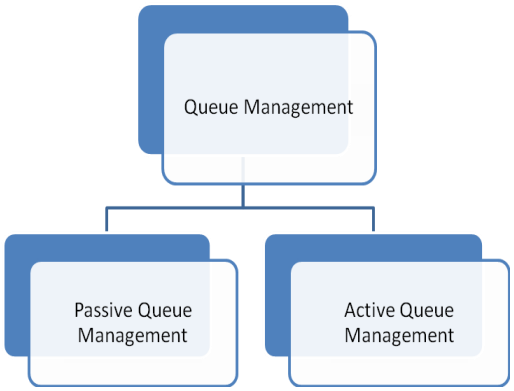

Figure 1.6 Classification of Queue Management

1.2.2 ACTIVE QUEUE MANAGEMENT (AQM)

Active Queue Management techniques come into play to prevent or avoid the chance of severe congestion, to achieve unbiased packet dropping in queues shared by multiple flows. It is a congestion preventive mechanism. AQM is a proactive approach that early drops packets when congestion arises. It gives sources enough time to react to congestion before queues fill up and do not keep queues full. It also drops packets selectively to avoid global synchronization.

The goal of AQM is to provide efficient resource allocation by reducing the average queue length and packet loss with increased link utilization. It uses congestion indicators as queue length, input rate to detect incipient congestion. The first AQM algorithm is RED that detects congestion by observing the queue length. As queue length does not act as a complete congestion indicator, the input rate is also included as a congestion indicator. Some of the AQM methods use both these congestion indicators to detect congestion at the earliest. AQMs perform better compared to the traditional scheme as they detect incipient congestion to prevent congestion occurring in future.

In a system of different applications, where the user demand has some flexibility, it is necessary to achieve a better solution for sharing the available capacity ensuring the QoS of the whole community of users. IP networks

ensure that the available capacity of network is utilised, and the QoS perceived by the users is maximised. To achieve these objectives, the machinery behind the IP network needs just two fundamental elements, a source algorithm and a link active queue management (AQM) algorithm.

As shown in Figure 1.7, a source algorithm resides in the host transmitting information, and decides how much information to transmit based on the congestion level of the network. The link AQM algorithm lives inside a router/switch, and monitors the queues that buffer packets awaiting transmission on the outgoing links connecting the router/switch to the next router/switch in the network. The AQM algorithm estimates the level of congestion the link is experiencing and generates a congestion signal, which communicates the congestion level to the source. Each AQM, on the source-to-destination path of the connection (e.g. TCP connection), contributes to the total congestion signal received by the source. Therefore an AQM ensures the QoS of the whole community of users in an IP network.

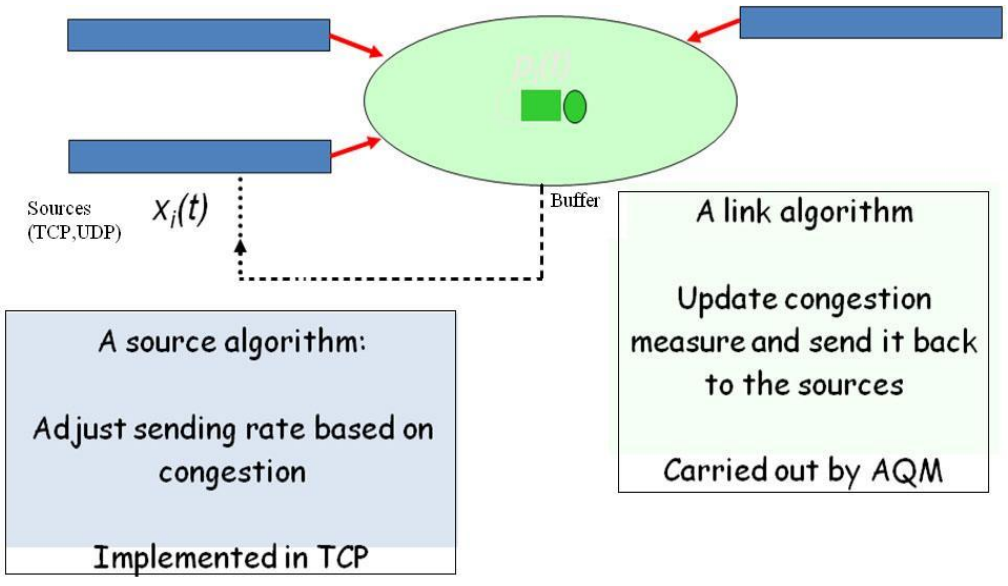

Figure 1.7 AQM and the source algorithm

Various AQMs are noted in the literature review. The significant contributions in AQMs are discussed in chapter 2. Based on the elaborate

discussions on the IP networks, their challenges, the increasing number of significant applications and the various active queue management schemes, the problem statement of the thesis is formulated and objectives are presented.

1.3 PROBLEM STATEMENT

Based on the background study, the problem statement is formulated as follows:

To present an Active Queue Management policy as a Router based mechanism for early detection and Prevention of Congestion inside the Network to steer the Overall Performance of the dynamically varying traffic in IP Networks.

1.4 OBJECTIVES OF THE THESIS

Based on the problem statement, the main objectives of the thesis are presented as follows:

To identify an Active Queue management scheme that

- Restricts disproportionate bandwidth usage
- Minimises packet drop rate
- Stabilizes and moderates network queues
- Increases link utilization
- Minimises queuing delay
- While providing better QoS by preventing congestion in a dynamically varying traffic in IP networks.

This thesis presents an Active Queue Management policy as a Router based mechanism for early detection and prevention of congestion inside the network

to steer the overall performance of the dynamically varying traffic in IP Networks.

1.5 SIGNIFICANT CONTRIBUTIONS OF THE THESIS

An AQM called FLoadAutoRED is proposed that achieves good QoS requirements for the dynamically varying traffic in IP networks. Simulations indicate that the proposed FLoadAutoRED benefits traffic under congestion by greatly improving the delay and effective loss performance, thus providing a good solution to quality degradation of traffic under congested network conditions. For this the performance efficient existing AQM AutoREDwithRED is improved in terms of fairness, minimum packet loss, stabilized network queues, high link utilization and minimum queuing delay in a dynamically varying traffic in IP networks. Therefore, it achieves the objectives of

- Obtaining better fairness in a varying traffic
- Achieving moderate and stable queue size with minimum packet loss in a dynamic traffic
- Attaining high link utilization with minimum queuing delay.

1.6 ORGANISATION OF THE THESIS

Chapter 1 has elaborately discussed the problem area and the objectives of the thesis. Chapter 2 reviews the current methods employed to deal with congestion. The Chapters 3 to 6 outline the methodology and its implementation. Finally, the methodology is tested in several network conditions where it is compared against existing methods and summarised in Chapter 7 and Chapter 8. The conclusion and future scope of the thesis is discussed after that.

CHAPTER REFERENCES

1. Andrew S Tanenbaum, "Computer Networks", Fourth Edition, Pearson Education.

2. Behrouz. A. Forouza, "Data communications and Networking", Third Edition, Tata McGraw Hill.

3. W. Feng, D. Kandlur, D. Saha et al. "Blue: A New Class of Active Queue Management Algorithms", UMichigan CSE-TR-387-99, 1999.

4. V. Jacobson, B. Braden, D. Clark, J. Crowcroft et al., "Recommendations on Queue Management and Congestion Avoidance in the Internet", RFC 2309, April 1998.

5. N. Hu, L. Ren, J. Chang, "Evaluation of Queue Management Algorithms", Course Project Report for 15-744 Computer Networks.

6. B. Sikdar, K. Chandrayana et al., "Queue Management Algorithms and Network Traffic Self-Similarity", Supported in parts by DARPA contract, DoD MURI contract and NSF grant ANI.

7. W. Stevens et al., "TCP Slow Start, Congestion Avoidance, Fast Retransmit, and Fast Recovery Algorithms", RFC 2001, January 1997.