A Demonstration of the FN Packet Marking Probability

Mohammed M. Kadhum
MIEEE
InterNetWorks Research Group
College of Arts and Sciences
Universiti Utara Malaysia
06010 UUM Sintok, MALAYSIA
kadhum@uum.edu.my

Suhaidi Hassan
SMIEEE
InterNetWorks Research Group
College of Arts and Sciences
Universiti Utara Malaysia
06010 UUM Sintok, MALAYSIA
suhaidi@uum.edu.my

***Abstract*— The effectiveness of queue management mechanisms relies on how good their control decisions will help in satisfying their goals regarding congestion avoidance and control. These decisions are implemented and compelled during the design of the packet mark probability and the mark activation functions. The design of Fast Congestion Notification (FN) drop/mark probability function enables the two control decisions, packet admissions and congestion control directing, to be made along with each other. This permits sending congestion avoidance notification as early as required even if the queue is almost empty, and preventing congestion notification even if the queue is almost full but the arrival rate is controllable. This leads to good buffer utilization and proper congestion detection. This paper demonstrates the drop/mark probability functions that the fast FN policy would exercise for different values of optimal queue size, and also for a specific optimal queue size value.**

Keywords- Packet drop probability; Random Early Detection (RED) gateway; Fast congestion Notification (FN) gateway

I. INTRODUCTION

Queue management algorithms manage the length of the packet queues by dropping packets when necessary or appropriate [1]. The efficiency of queue management mechanisms depends on how well their control decisions, on packet admission to the queue and congestion control directing, will help in satisfying their objectives regarding congestion avoidance and control. These decisions are implemented and compelled during the design of the packet mark probability and the mark activation functions. Packet admission and congestion control directing control decisions are dependent on each other. Based on the drop activation characteristic, the queue management policies can be classified into two categories. The first category is *reactive (passive) queue management policies*, which do not employ any preventive packet drop before the gateway buffer is flooded. The second category is *proactive* (*active*) *queue management policies*(*AQM*) which employ preventive packet drop before the gateway buffer gets full [2]. Drop-Tail, which is one of reactive queue management policies, is currently widely developed in the Internet routers. It introduces several problems, such as global synchronization, on the Internet. Active queue management policies, such as Random Early Detection (RED), are expected to eliminate global synchronization and improve Quality of Service (QoS) of the networks. The promised advantages of AQM are increase in throughput, reduce the delay, and avoid lock-out.

Preventive packet drop provides implicit feedback method to notify the traffic senders of the congestion onset [3]. As a reaction, senders reduce their transmission rate to moderate the congestion level. Arriving packets from the senders are dropped randomly, which prevents senders from backing off at the same time and thereby eliminate global synchronization [3].

RED is the default AQM mechanism that is recommended by IETF for the Internet routers [1], which was proposed by Floyd and Jacobson [4] in 1993. A router implementing RED detects early by computing the average buffer length (*avg*) and sets the two queue thresholds (Max_{th} and Min_{th}) for packet drop. The average buffer length at time *t*, is defined as *avg* (*t*) = (1-*w*) *avg* (*t*-1) + *wq* (*t*), is used as a control variable to perform active packet drop. The *avg* (*t*) is the new value of the average buffer length at time *t*, *q* (*t*) is instantaneous buffer length at time *t*, and *w*, which is normally less than one, is a weight parameter in calculating *avg*. Figure 1 shows the RED gateway buffer.

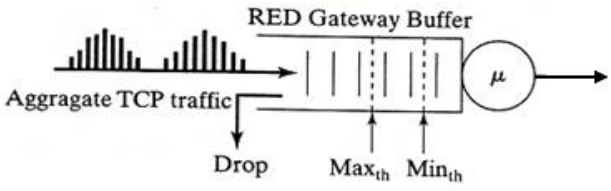

Figure 1. RED Gateway Buffer

The FN [5] queue management algorithm randomly marks (if ECN) / drops (if non-ECN) the arriving packets before the buffer overflows, to effectively control the:

- instantaneous queue length below a the optimal queue length to reduce the queuing delay and avoid the buffer overflows

- average traffic arrival rate of the queue in the proximity of the departing link capacity to enable the congestion and queue length control

FN integrates the instantaneous queue length and the average arriva1 rate of queue to compute the drop probability of the packet upon each arriving packet, as described in the following sections.

The use of the instantaneous queue length in conjunction with the average queue speed (average arrival rate) can provide superior control decision criteria for an active queue management scheme [6]. Figure 2 shows the FN gateway buffer.

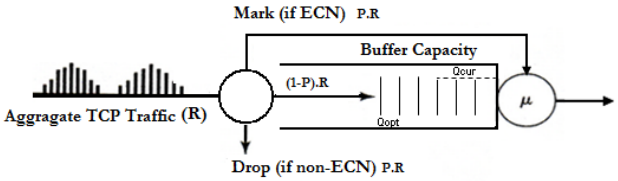

Figure 2. FN Gateway Buffer

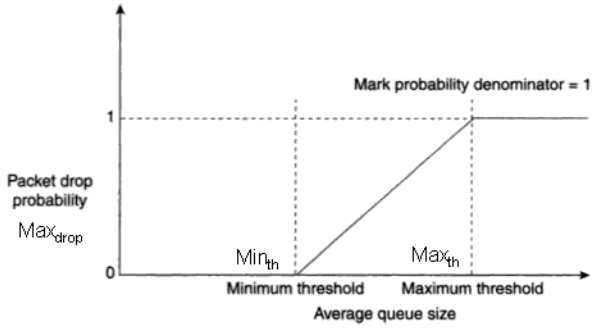

Figure 3. RED Packet Drop Function

II. PACKET DROP PROBABILITY

Packet drop probability function determines the probability that the packet is dropped when the drop activation function imposes drop procedure initiation and the drop position function selects the specific packet to be dropped. For example in drop-tail, the chosen packet which is the packet at the tail of the queue is dropped with probability one.

A. RED Packet Drop Probability

RED packet drop probability is a linear function of the average queue size. It also based on the minimum threshold Min_{th}, maximum threshold Max_{th}, and mark probability denominator, which is the fraction of packets dropped when the average queue depth is at the maximum threshold Max_{th} [7], see figure 3. In RED, the probability of dropping packet, P, is calculated by $P = Max_{drop}\left((avg - Min_{th}) / (Max_{th} - Min_{th})\right)$

The RED algorithm includes two computational parts: computation of the *average buffer length* and calculation of the *drop probability*.

The RED algorithm involves four parameters to regulate its performance. Min_{th} and Max_{th} are the queue thresholds to perform packet drop, Max_{drop} is the packet drop probability at Max_{th}, and w is the weight parameter to calculate the average buffer size from the instantaneous queue length. The average buffer length follows the instantaneous buffer length. However, because w is much less than one, avg changes much slower than q. Therefore, avg follows the long-term changes of q, reflecting persistent congestion in networks. By making the packet drop probability a function of the level of congestion, RED gateway has a low racket-drop probability during low congestion, while the drop probability increases the congestion level increases [3].

The packet drop probability of RED is small in the interval Min_{th} and Max_{th}. Furthermore, the packets to be dropped are chosen randomly from the arriving packets from different hosts. As a result, packets coming from different hosts are not dropped simultaneously. RED gateways, therefore, avoid global synchronization by randomly dropping packets.

The performance of RED significantly depends on the values of its four parameters [8], Max_{drop}, Min_{th}, Max_{th}, and w.

B. FN Packet Drop/Mark Probability Function

The FN linear drop/mark probability function [9] is derived based on the assumption that the arrival traffic process remains unchanged over the control time constant period of length (T) seconds. In other words, it is supposed that immediately following the packet's arrival, the traffic continues to arrive at the fixed rate of (R) bits/sec, the estimated average arrival rate to the buffer computed upon the packet's arrival, for the period of the control time constant. The buffer has a capacity of (C) bits and is served by an outgoing link at a fixed rate of (μ) bits/sec. The packet drop/mark probability (P), is computed for, and applied to, every incoming packet, based on the above assumptions, with the goal of driving the instantaneous (current) queue length (Q_{cur}) to some desired optimal level (Q_{opt}) over the control time constant period (T). These are shown in figure 2. The FN drop/mark probability, P, is calculated by

$$P^{(i)} = \frac{((R_i - \mu).T) - (Q_{opt} - Q_{cur})}{R_i.T} = \frac{\Delta Q_u - \Delta Q_d}{Q^+}$$

III. FN DROP/MARK PROBABILITY FUNCTION DEMOSTRATION

It is assumed for the sake of illustration that the physical buffer size is (C) 105000 bytes, the control time constant is 64 msec, and the outgoing link of 10 Mbps. Since the optimal and the instantaneous queue sizes can differ from 0 to 150,000 bytes , their difference, (Q_{opt} - Q_{cur}), varies between -150,000 and 150,000. Positive values indicate the allowed growth in the queue while negative values indicate the desired drain. Figure 4 shows the FN drop/mark probability function as a

function of the range of desired drain in the queue (allowed growth) (Q_{opt} - Q_{cur}) and the average arrival rate (R).

The graph in figure 4 assumes that the average arrival rate varies between 0 and 20 Mbps which is twice the outgoing link capacity related to when the gateway buffer is operating at 200% load.

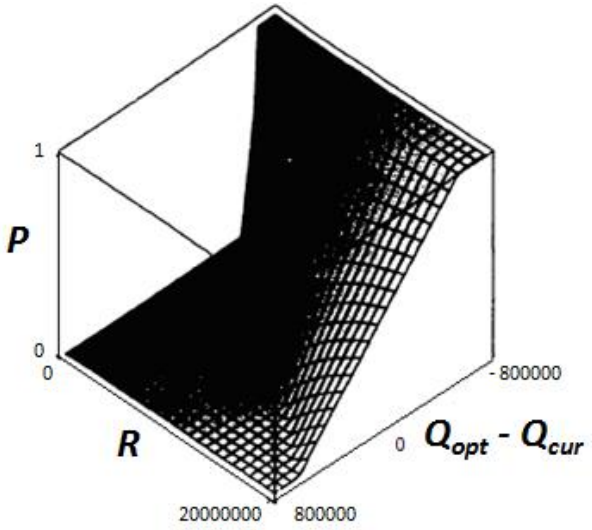

Figure 4. Family of FN packet marking probability functions - C =105,000 bytes, T = 64 msec, μ= 10 Mbps

The graph in figure 4 includes the drop probability functions family that the FN mechanism would exercise for different values of optimum queue size. In actuality, the queue management mechanism is configured to work with a specific optimum queue size. The resulting drop probability function would be a slice from the drop probability function graph in figure 4 along the rate axis with the lower and upper bounds of the slice being specified by the optimum queue size.

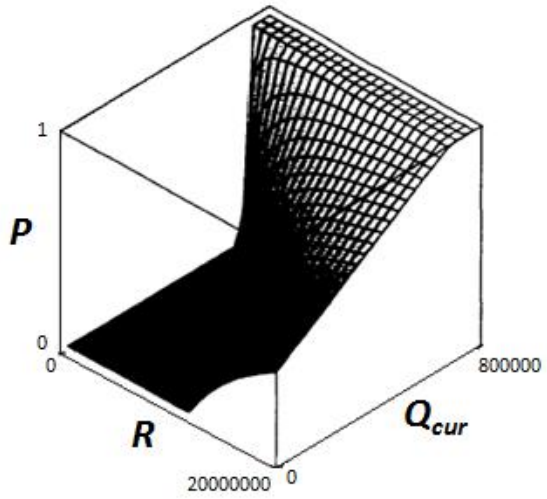

Figure 1. FN Packet Marking Probability Function - Q_{opt}=13,125 bytes, C=105,000 bytes, T=64 msec, μ=10 Mbps

The graph figure 5 shows the FN drop probability function as a function of rate (R) and instantaneous queue size (Q_{cur}) for an optimum queue size (Q_{opt}) of (13,125) bytes. Since the instantaneous queue size can vary between (0) and (13,125) bytes, the difference ($Q_{opt} - Q_{cur}$) would vary between (-91,875) and (13,125). Hence, the plot of the drop probability function for when the optimum queue size is (13,125) bits (figure 5) is the slice of the drop probability functions family presented in figure 4 cut out by two vertical planes along the rate axis which would pass through the points ($Q_{opt} - Q_{cur}$) = 13,125 bits on the left side and ($Q_{opt} - Q_{cur}$) = -91,875 bytes on the right side. This can be easily confirmed by visually comparing the two graphs in Figures 4 and 5.

IV. Discussion

To show how the designed drop probability function allows the two decisions regarding average arrival rate control and queue length control interact with each other, the drop probability function can be written as a sum of two components :

$$P^{(i)} = \frac{((R_i - \mu).T\ ) - (Q_{opt} - Q_{cur})}{R_i.T} =$$

$$P^{(i)} = \frac{((R_i - \mu).T\ )}{R_i.T} + \frac{(Q_{cur} - Q_{opt})}{R_i.T}$$

$$P^{(i)} = P_R^{(i)} + P_Q^{(i)}$$

The (P_R) component expresses the average arrival rate effects and the (P_Q) component form the instantaneous queue length effects. The relative influence of each decision control on the other is specified by the relative sizes of the two components of the drop probability function, (P_R) and (P_Q). This depends on the degree to which the arrival rate differs from the outgoing link capacity and the instantaneous queue length from the optimal desired queue length.

V. Conclusion

In this paper, we have demonstrated the linear version of the FN drop probability function based on the assumptions of constant rate. We also showed how the designed drop probability function allows the two decisions regarding average arrival rate control and queue length control interact with each other.

References

[1] B. Braden, D. Clark, J. Crowcroft, B. Davie, S. Deering, D. Estrin, S. Floyd, V. Jacobson, G. Minshall, C. Partridge, L. Peterson, K. Ramakrishnan, S. Shenker, J. Wroclawski, and L. Zhang, *Recommendations on Queue Management and Congestion Avoidance in the Internet*: RFC Editor, 1998.

[2] S. Leonardo, P. Adriano, and M. Wagner, Jr., "Reactivity-based Scheduling Approaches For

Internet Services," in *Proceedings of the Fourth Latin American Web Congress*: IEEE Computer Society, 2006.

[3] M. Hassan and R. Jain, *High Performance TCP/IP Networking: Concepts, Issues, and Solutions*: Pearson Prentice Hall, 2004.

[4] S. Floyd and V. Jacobson, "Random early detection gateways for congestion avoidance," *Networking, IEEE/ACM Transactions on,* vol. 1, pp. 397-413, 1993.

[5] M. M. Kadhum and S. Hassan, "Fast Congestion Notification mechanism for ECN-capable routers," in *Information Technology, 2008. ITSim 2008. International Symposium on*, 2008, pp. 1-6.

[6] M. M. Kadhum and S. Hassan, "The Design Motivations and Objectives for Fast Congestion Notification (FN)," in *Proceedings of the APAN Network Research Workshop* Malaysia, 2009.

[7] S. Vegesna, *IP Quality of Service*: Cisco Press, 2001.

[8] F. Wu-Chang and D. K. Dilip, "Adaptive packet marking for maintaining end-to-end throughput in a differentiated-services internet," *IEEE/ACM Trans. Netw.,* vol. 7, pp. 685-697, 1999.

[9] M. M. Kadhum and S. Hassan, "A Linear Packet Marking Probability Function for Fast Congestion Notification," in *Proceedings of the 4th IEEE LCN Workshop on Network Measurements* Zürich, Switzerland, October 20-23, 2009.