Simulation Study on the Effect of the trTCM Parameters

Hakyong Kim, Changmo Yoo, and Woo-Young Jung
Research and Development Center
Corecess Inc., Seoul, Korea
hykim@ieee.org, {cmyoo and wyjung}@corecess.com

Abstract—**In this paper, we study the effect of the trTCM parameters on policing accuracy via computer simulation. The trTCM (two-rate three-color marker) is a traffic conditioner and can be used as a policing/limiting mechanism in Differentiated Services networks. The trTCM algorithm described in RFC 2698 [7] is configured using 4 traffic parameters: CBS (committed burst size), PBS (peak burst size), CIR (committeed information rate), and PIR (peak information rate). With these parameters, it marks incoming packets either green, yellow, or red. Packets marked green is always queued and delivered to the output side, but packets marked yellow or red are either queued or dropped depending on the policing policy of the network. Among them, green packets are related to the policing rate and, therefore, policing accuracy. The policing rate of the trTCM algorithm is determined by CIR. By contrast, policing accuracy is influenced by other trTCM parameters. Our findings in this study is that the policing accuracy of the trTCM is maximized when we use PIR, which is equal to CIR, and CBS, which is larger than twice the maximum packet length. PBS has no influence on the policing accuracy.**

Keywords—**two-rate three-color marker (trTCM), quality of service, policing, limiting**

I. Introduction

As different kinds of applications are being intergated into a single network based on IP protocol, it becomes crucial to guarantee the characteristics of each application traffic in the best-effort network. To the end, many protocols are being developed or have been developed. They are Differentiated Service (DiffServ) [1], [2], Integrated Service (IntServ) [3], Resource Reservation Protocol (RSVP) [4] Multi-Protocol Label Switching (MPLS) [5], Virtual LAN (VLAN), and so on. Among them, the DiffServ is regarded as a dominent protocol for its flexibility, scalability, and capability of QoS guarantee. In order to provide the (end-to-end) QoS guarantee in DiffServ networks, each routing/switching node should perform different types of functions related to QoS metrics such as bandwidth, delay, and packet loss. Among them, traffic policing or rate limiting is a fundamental but indispensible function.

Traditionally, policing or limiting function was implemented by using single-stage token bucket or leaky bucket. In DiffServ networks, it is implemented by using two-stage token bucket algorithms such as srTCM (single-rate three-color marker) [6] and trTCM (two-rate three-color marker) [7]. Major differences between srTCM and trTCM are as follows: i) The srTCM uses only CIR (comitted information rate) to update two token counters, T_c and T_e, while the trTCM uses CIR and PIR (peak information rate) to update token counters T_c and T_p. ii) The srTCM limits the rate of incoming traffic based on the burst length, while the trTCM limits the rate of incoming traffic based on the peak rate as well as the burst length.

In reality, traffic is usually limited or policed by the traffic rate rather than only by the burst length. Therefore, many state-of-the-art network equipments use the trTCM algorithm preferably rather than the srTCM or single-stage token bucket to police or limit the incoming traffic.

In this paper, we study the trTCM algorithm. We focus our concern on the trTCM parameters which are not discussed in RFC 2698. Through diverse computer simulation, we investigate the effect of the trTCM parameters on policing accuracy. This study will be useful to those who develop the policing function using the trTCM and those who have to manage and configure policing parameters of trTCM in order to provide policing services precisely. It will provide them with the ability to optimize the trTCM parameters.

This paper is organized as follows: In Section 2, we review the policing/limiting function and the trTCM algorithm. We try to understand the physical meaning of the trTCM parameters by analyzing the trTCM algorithm and expect the effect of each parameter on policing accuracy. In Section 3, we present diverse results of this study based on computer simulation. Finally, we conclude this paper with a brief summary.

II. Policing and trTCM

In this section, we review the concept, function, and necessity of traffic policing. After that, we investigate the trTCM algorithm and its traffic parameters.

A. Policing Algorithms

QoS should be guaranteed end-to-end. Considering the fact that a packet has to pass through many interim nodes in order to get to its destination, guaranteeing end-to-end QoS is not a easy work. However, reminding the fact that most QoS issues stems from network congestion, we could prevent or circumvent many potential QoS problems from occuring by limiting the amount of traffic entering the network.

Limiting the rate or amount of incoming traffic is called *rate limiting* or *traffic limiting*. It is also referred to as *policing* since this function is similar to that of police officers who control or regulate the traffic on the road. In this paper, we will use these three expressions interchangeably. As mentioned previously, policing has its significance in that it can prevent many possible QoS problem from occuring by reducing the chance of network congestion.

The policing or limiting fucntion is usually implemented in edge nodes of a network. Edge nodes limit the incoming user traffic based on TCA (traffic conditioning agreement) or more generally on SLA (service level agreement). Traditionally, the policing/limiting function was implemented by using single-stage token bucket or leaky bucket. In ATM, dual leaky buckets called GCRA (generic cell rate algorithm) was used. In DiffServ networks, it is implemented by using two-stage token bucket algorithms such as srTCM (single-rate three-color marker) [6] and trTCM (two-rate three-color marker) [7].

A major difference between leaky bucket or single-stage token bucket and two-stage token bucket is the number of packet groups with different priority or drop precedence. In leaky bucket or single-stage token bucket, packets are divided into two groups of conforming packet group and non-conforming packet group according to the existence of available tokens in token bucket. In two-stage token bucket, packets are divided into three groups of conforming packet group, exceeding packet group, and violating packet group. Three packet groups correspond to three drop precedences or colors in DiffServ protocol, respectively.

Major differences between srTCM and trTCM are as follows: i) The srTCM uses only CIR (comitted information rate) to update two token counters, T_c and T_e, while the trTCM uses CIR and PIR (peak information rate) to update token counters T_c and T_p. ii) The srTCM limits the rate of incoming traffic based on the burst length, while the trTCM limits the rate of incoming traffic based on the peak rate as well as the burst length.

In reality, the traffic rate is usually limited/policed by the traffic rate and burst length rather than simply by the burst length. Therefore, many state-of-the-art network equipments, especially supporting DiffServ protocol, use the trTCM algorithm preferably rather than srTCM, single-stage token bucket or leaky bucket to police or limit the incoming traffic.

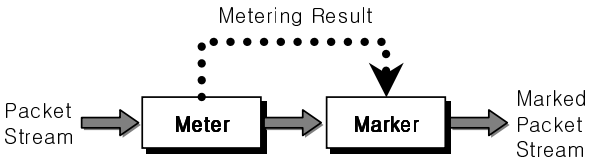

Fig. 1. Traffic conditioner.

The trTCM algorithm, which will be discussed in the following subsection, is configured using 4 parameters. The definition and conditions for these parameters are mentioned in RFC 2698. However, the effect of these parameters is not stated in the RFC and is not found in any other studies. We will derive the physical meaning of each parameter in the following subsection and compare our analogy with the simulation result of the next section.

B. Two-Rate Three-Color Marker (trTCM)

The basic idea of the trTCM algorithm is very simple. It marks the incoming packets either green, yellow, or red according to the metering result as shown in Figure 1. If a packet exceeds the peak information rate (PIR), it is marked red. Otherwise, it is marked either yellow or green depending on whether it exceed or doesn't exceed the comitted information rate (CIR).

The meter operates in one of two modes: color-blind mode and color-aware mode. In the color-blind mode, the meter assumes that the incoming packet stream is uncolored. Therefore, the traffic conditioner does not check or reflect the color of the incoming packets in metering and marking process. In the color-aware mode, on the contrary, the meter assumes that the incoming packet stream has been pre-colored by some proceeding entity. Therefore, the traffic conditioner has to check and reflect the color of the incoming packets in metering and marking process. In this paper, we limit our concern only to the color-blind mode.

The trTCM is configured by setting its mode and by assigning values to its four traffic parameters. Here, we assume that the trTCM is set to the color-blind mode. The four parameters of trTCM are CIR (committed information rate), PIR (peak information rate), CBS (committed burst size), and PBS (peak burst size). As their name implies, the first two are related to the traffic rate and the other two are related to the packet burst size.

The CIR and PIR are measured in bytes of IP packets

per second. Therefore, IP header is included in byte count while link specific headers such as MAC address are not included in byte count. This fact implies that the policing result might differ from the target rate that we want since test equipments usually measures the link layer frame. The other condition for CIR and PIR is that PIR must be equal to or greater than CIR.

As to CBS and PBS, they are also measured in byte. Basically, these parameters must be configured to be greater than 0. However, it is recommended that they should be configured to be equal to or greater than the maximum possible packet length in the incoming traffic stream. It implies that CBS and PBS are set to be equal to or greater than 1500 since the maximum IP packet size, namely maximum transmission unit (MTU), is 1500 bytes in Ethernet. PBS should be equal to or greater than CBS.

The trTCM uses two token buckets P and C, with rates PIR and CIR, respectively. The maximum size of the token bucket P is PBS and the maximum size of the token bucket C is CBS. The token buckets are initially (at time 0) full. That is, the token counter $T_p(0) = PBS$ and the token counter $T_c(0) = CBS$. Thereafter, the token count T_p is incremented by one PIR times per second up to PBS and the token count T_c is incremented by one CIR times per second up to CBS. In network equipments, 1 second is divided into several million time durations and above operation is performed once every time duration. (In our study, we divide 1 second into 6×10^6 time durations.) Thus, the token counters T_p and T_c are updated by the fraction of time duration during every time duration.

When a packet of size B bytes arrives at time t, the trTCM in the color-blind mode determines the packet color according to the following rules:

- If $B > T_p(t)$, the packet is red, else
- if $B > T_c(t)$, the packet is yellow and T_p is decremented by B, else
- the packet is green and both T_p and T_c are decremented by B.

Above rule is straightforward in that if a token bucket has token counts less than the length of an incoming packet, it can not serve a packet. The marker following the meter marks the packet based on the metering result by the above rule. Figure 2 shows the flow chart of the trTCM algorithm in color-blind mode.

The acutal policing/limiting function is occurred using the marking result. Usually, green packets are permitted to be passed, yellow packets are dropped or passed with lower drop precedence depending on the policing policy of the network, and red packets are dropped promptly in most cases.

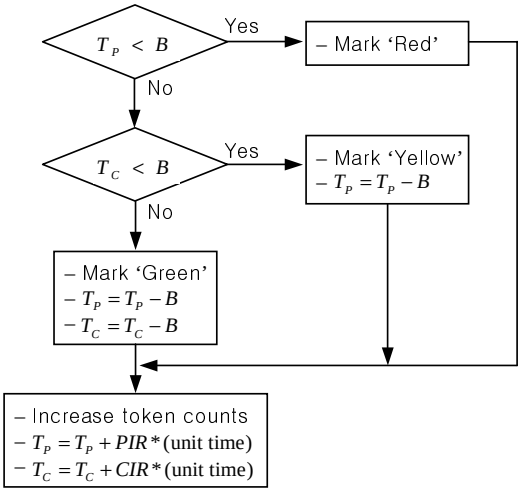

Fig. 2. Flow chart of the trTCM algorithm.

As we know from above description of the trTCM, PBS seperates packets marked red from packets marked yellow or green. Therefore, the larger the PBS, the smaller the fraction of packets marked red. But, PBS does not affect the ratio of packets marked yellow to packets marked green. That is, we can guess that PBS does not have any influence on policing accuracy. Considering the role of PBS, it is straigtforward to say CBS separates packets marked yellow from packets marked green. Similarly, larger CBS leads to smaller fraction of packets marked yellow. Namely, larger CBS leads to larger fraction of green packets. Considering the fact that the fraction of green packet is limited by the CIR, we can expect that larger CBS makes policing result more accurate.

As mentioned previously, CIR determines the policing rate that we are targetting. Therefore, CIR is not the component incluencing on policing accuracy but the criteria for the policing accuracy. On the contrary, PIR affects the policing accuracy. If PIR is larger than CIR, the token counter T_p is updated faster than T_c. It means that the fraction of packets marked yellow or green becomes larger. However, since the portion of green packets is determined by CIR, we can infer that a larger PIR increases the portion of yellow packets.

If PBS is equal to CBS and PIR is equal to CIR, the incoming packets are divided into only red and green packets, since in this case the trTCM becomes a single-stage token bucket.

III. Simulation

In the previous section, we reviewed the concept of policing/limiting and the trTCM algorithm. We also in-

ferred the effect of four traffic parameter of the trTCM on the policing accuracy. In this section, we validate that our inference is correct through diverse computer simulation.

A. Simulation Environments

In order to confirm our guess on the influence of trTCM parameters on the policing accuracy, we performed extensive computer simulation. The simulation results will be introduced in the following subsection one by one. In this subsection, we describe the simulation environments used commonly to all simulation and assumptions made.

In the simulation, we generated a single traffic flow of a specific traffic rate. We generated the traffic flow at the rate of 50 Mbps or 100 Mbps. A traffic flow can be composed of either fixed-length packet or randomized-length packet. In the traffic flow with fixed-length packets, the packet length is fixed to a specific length, such as 64, 300, 600, 782, 900, 1200, or 1500. In the traffic flow with randomized-length packets, the packet length can be determinded in two ways:

- The packet length is selected randomly or with uniform probability between the minimum packet length and the maximum packet length. For example, it can be selected between 64 and 1500, making the average packet length 782 bytes.
- The packet length is selected randomly or with uniform probability among a set of possible packet lengths. For example, it can be selected among 600, 900, and 1200, making the average packet length 900 bytes.

In the simulation, we assumed that the time duration of the network equipment is $1.67 \times 10^{-}7$ sec. That is, the trTCM operation described in Subsection II-B are performed 6×10^6 times per second. We assumed that only one packet can arrive at the equipment during a time duration. Packets can arrive successively in adjacent time durations. We ran the simulation coded by using BC++ 6.0 for 20 seconds, corresponding to 1.2×10^8 time durations, to get a point in the figures 3 through 10.

B. Simulation Results

Under the simulation environments and assumptions described in the previous subsection, we performed diverse simulation. In each simulation, we changed values of one or two parameters. In some cases we used traffic of fixed packet length, while in other cases we used traffic of randomized packet length. These changes will be mentioned additionly for each simulation.

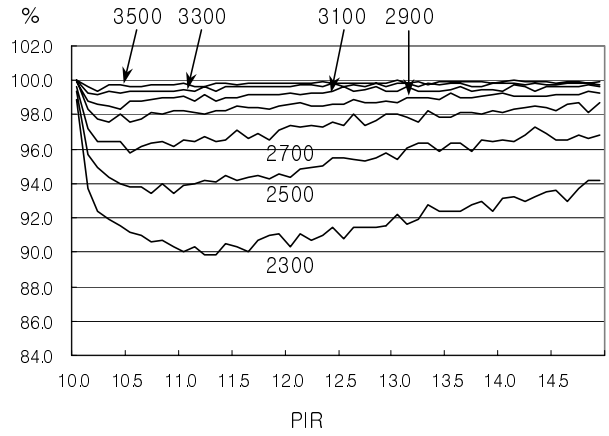

Fig. 3. The effect of CBS to the policing accuracy. The ordinate designates the policing accuracy.

Figure 3 shows the effect of CBS on the policing accuracy when the incoming traffic is composed of fixed-length packets. The packet length was fixed to 1500 bytes. We generated the incoming traffic of 50 Mbps and limited it to 10 Mbps. That is, CIR was set to 10 Mbps. PIR was increased by 0.1 Mbps from 10 Mbps to 14.9 Mbps. CBS was increased by 200 bytes from 2300 bytes to 3500 bytes. PBS was set to equal to CBS for three reasons. The first reason is that PBS should be greater than or equal to CBS according to RFC 2698. The second reason is from our inference in Subsection II-B. That is, the policing accuracy may not be affected by PBS. The third reason is from other simulation results. That is, the policing accuracy was maximized when PBS is equal to CBS. Anyhow, the figure shows that the policing accuracy is improved as increasing CBS values. This result coincides with our expection in Subsection II-B. As shown in the figure, when CBS is greater than twice the packet size, it guarantees 98% or more policing accuracy. Furthermore, it shows that the maximum policing accuracy is acquired when PIR is equal to CIR.

Figure 4 shows the CBS required for accurate policing. In this simulation, we assumed that traffic was generated at 100 Mbps and limited to the target policing rate from 10 Mbps to 90 Mbps by 10 Mbps. We generated two types of traffic, with fixed-length packets and with randomized-length packets. For the traffic with randomized-length packets, packet length is selected randomly between 64 and 1500 bytes. For the traffic with fixed-length packets, packet length is fixed to 782 bytes. 782 bytes is the same as the average packet length of the traffic with randomized-length packets. The solid lines plot the minimum CBS value which is required for policing accuracy of 97%. (97% or 95% policing accuracy is required in

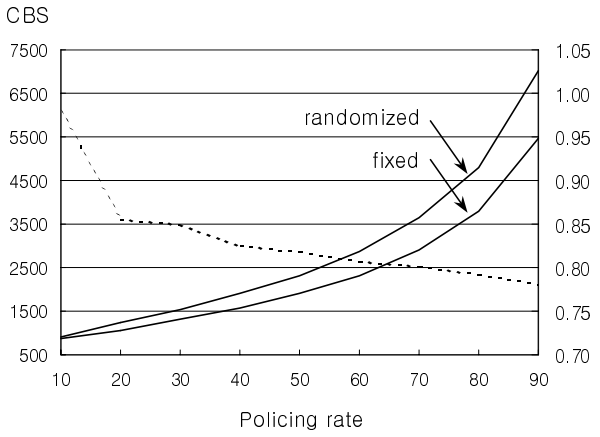

Fig. 4. Comparision of CBS required for traffic with randomized packet length and traffic with fixed packet length.

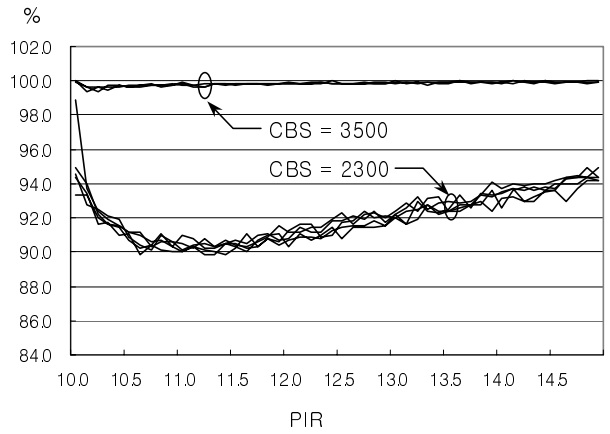

Fig. 5. The effect of PBS for the traffic with fixed packet length.

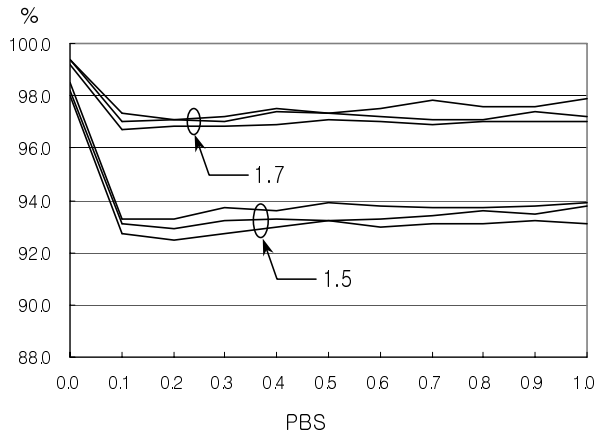

Fig. 6. The effect of PBS for the traffic with randomized packet length.

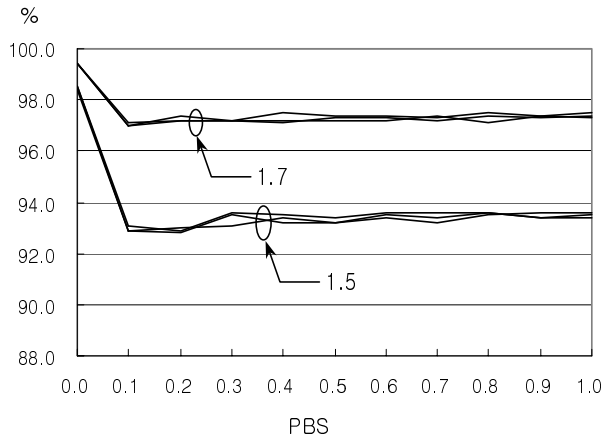

Fig. 7. The effect of PBS for the traffic with fixed packet length.

the network industry.) As shown in the figure, the traffic with fixed-length packets requires less CBS than the traffic with randomized-length packets. For both types of traffic, CBS values increase exponentially over target policing rate. The dashed line plots the ratio of CBS required for the fixed-packet-length traffic to CBS required for the randomied-packet-length traffic. The ratio is alwasy less than 1.0 and decreases over target policing rate. For the policing rate larger than 20 Mbps, the fixed-length traffic requires CBS less than 85% of CBS required for randomized-length traffic.

Figure 5 shows the effect of CBS and PBS to the policing accuracy when the incoming traffic is composed of fixed-length packets. The packet length was fixed to 1500 bytes. We generated the incoming traffic of 50 Mbps and limited it to 10 Mbps. That is, CIR was equal to 10 Mbps. PIR was increased by 0.1 Mbps from 10 Mbps to 14.9 Mbps. CBS was set to 2300 bytes or 3500 bytes. PBS was set to either 2300, 2500, 2700, 2900, or 3100 bytes for CBS of 2300 and set to either 3500, 4000, or 4500 bytes for CBS of 3500. As shown in the figure, the large CBS provides better policing accuracy, which has been verified in Figure 3. For both values of CBS, it shows that PBS has no influence on the policing accuracy. However, when PIR is equal to CIR, PBS which is equal to CBS yields the best policing accuracy.

Figure 6 shows the effect of PBS to the policing accuracy. In this simulation, we generated the incoming traffic at the rate of 50 Mbps and limited it to the rate of 10 Mbps. The incoming traffic is composed of randomized-length packets. The average packet length used was 600, 900, and 1200 bytes and the maximum and minimum packet length was $\pm$ 300 bytes from the average packet length. For CBS, we selected 1.5 times and 1.7 times average packet length. That is, when we used packets whose average is 600 bytes, CBS was set to 900 and 1020, respectively. PBS was set to CBS at first and increased by 10% of packet length continuously. In this figure, we can derive four results. The first result is that the policing accuracy was better for larger

CBS value, which is already verified. The second result is that the policing accuracy was made worse by using PBS value different from CBS. The third result is that policing accuracy did not affected by different PBS values when PBS is greater than CBS. The fourth result is that policing accuracy did not affected by packet size when we use CBS value with a consistent ratio to the packet size. Whenever we increase the average packet size by 300 bytes, the policing accuracy was improved by only 0.3%. It is a negligible and meaningless value.

Figure 7 shows the effect of PBS to the policing accuracy when the incoming traffic is composed of fixed-length packets. The other simulation configuration, except the packet length type, is same as those of Figure 6. Comparing the results in Figure 7 with those in Figure 6 for the traffic of randomized packet length confirms that PBS does not affect the policing accuracy irrespective of the packet length distribution. It is interesting that the policing accuracy for the traffic of fixed-length packets is almost same as that for the traffic of randomized-length packets.

Figure 8 shows the effect of PIR to the policing accuracy when the incoming traffic is composed of fixed-length packets. The packet length was fixed to 900 bytes. We generated 50 Mbps incoming traffic and limited it to 10 Mbps. That is, CIR was 10 Mbps. PIR was increased by 0.1 Mbps from 10 Mbsp to 14.9 Mbps CBS was set to 1200 and PBS was set to 1200, 1400, 1600, 1800, and 2000. Each curve corresponds to different PBS values, respectively. As shown in the figure, however, the policing accuracy is not affected by PBS. When PBS is greater than CBS, that is, PBS=1400, 1600, 1800, and 2000, curves shows the same movement and the accuracy is very similar. When PBS is equal to CBS, the maximum accuracy is obatined when PIR is equal to CIR. The policing accuracy was minimum near PIR of 11.5 (115% of CIR).

Figure 9 shows the effect of PIR to the policing accuracy when the incoming traffic is composed of randomized-length packets. The packet length was selected from 300, 600, 900, 1200, and 1500 bytes in random manner, maintaining the arrival rate of 50 Mbps. The incoming traffic was limited to 10 Mbps. That is, CIR is 10 Mbps. PIR was increased by 0.1 Mbps from 10 Mbps to 14.9 Mbps. CBS was set to 1200 and PBS was set to 1200, 1400, 1600, 1800, and 2000. Each curve corresponds to different PBS values, respectively. Except when CBS and PBS are equal to 1200, the curves show the almost consistent policing accuracy near 86%. The maximum policing accuracy was acquired when CBS and PBS are equal to 1200 and PIR is equal to CIR as in the fixed-length-packet case. Except for the case where CBS and PBS are equal to 1200, PIR does not affect on the policing accuracy.

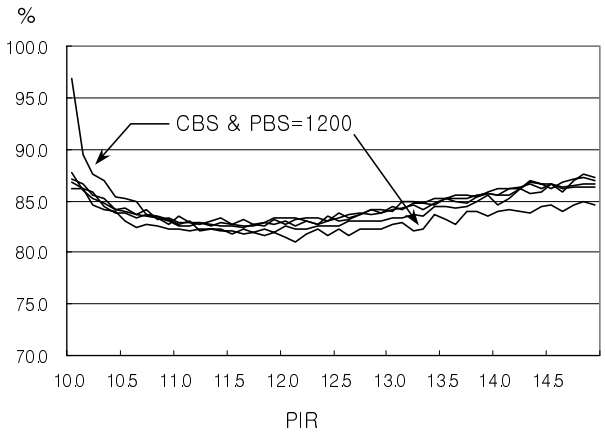

Fig. 8. The effect of PIR and PBS for the traffic with fixed packet length.

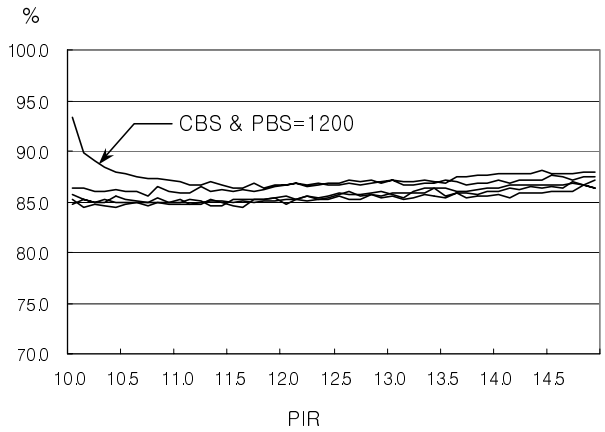

Fig. 9. The effect of PIR and PBS for the traffic with randomized packet length.

IV. Conclusions

In this paper, we studied the effect of trTCM parameters on the policing accuracy via computer simulation. The trTCM is useful when we perform the policing/limiting function based on the peak rate of the incoming traffic as well as the burst length. The trTCM algorithm, described in RFC 2698, uses 4 traffic parameters of CBS, PBS, CIR, and PIR. By RFC 2698, CBS and PBS should have values larger than or equal to the maximum packet size and PBS should be larger than or equal to CBS. According to our study, the policing accuracy was improved as CBS was increased. When CBS is greater than twice the maximum packet length, we could acquire more than 98% policing accuracy. The trTCM algorithm requires less CBS value for the traffic of fixed packet length than for the traffic with

randomized packet length distribution. The polcing accuracy was not affected by PBS. This fact was proved in diverse simulation results. As to PIR, we can not affirm that PIR has a definite effect on the policing accuracy. However, when PIR becomes unequal to or larger than CIR, the policing accuracy falls off depending on the CBS value. When CBS is big enough, e.g., three times the maximum packet size, we can acquire almost 100% policing accuracy irrespective of PIR. When CBS is not big enough, that is, less than twice the maximum packet size, the policing accuracy becomes deteriorated. The maximum policing accuracy of the trTCM is acquired when PIR is set to CIR and PBS is set to CBS, where CBS is larger than twice the maximum packet length.

REFERENCES

[1] K. Nichols, S. Blake, F. Baker and D. Black, "RFC 2474 - Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers," Dec. 1998.

[2] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss, "RFC 2475 - An Architecture for Differentiated Services," Dec. 1998.

[3] R. Braden, D. Clark, and S. Shenker, "RFC 1633 - Integrated Services in the Internet Architecture: an Overview," June 1994.

[4] R. Braden, Ed., L. Zhang, S. Berson, S. Herzog, and S. Jamin, "RFC 2205 - Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification," Sep. 1997.

[5] E. Rosen, A. Viswanathan, and R. Callon, "RFC 3031 - Multiprotocol Label Switching Architecture," Jan. 2001.

[6] J. Heinanen and R. Guerin, "RFC 2697 - A Single Rate Three Color Marker," Sep. 1999.

[7] J. Heinanen and R. Guerin, "RFC 2698 - A Two Rate Three Color Marker," Sep. 1999.