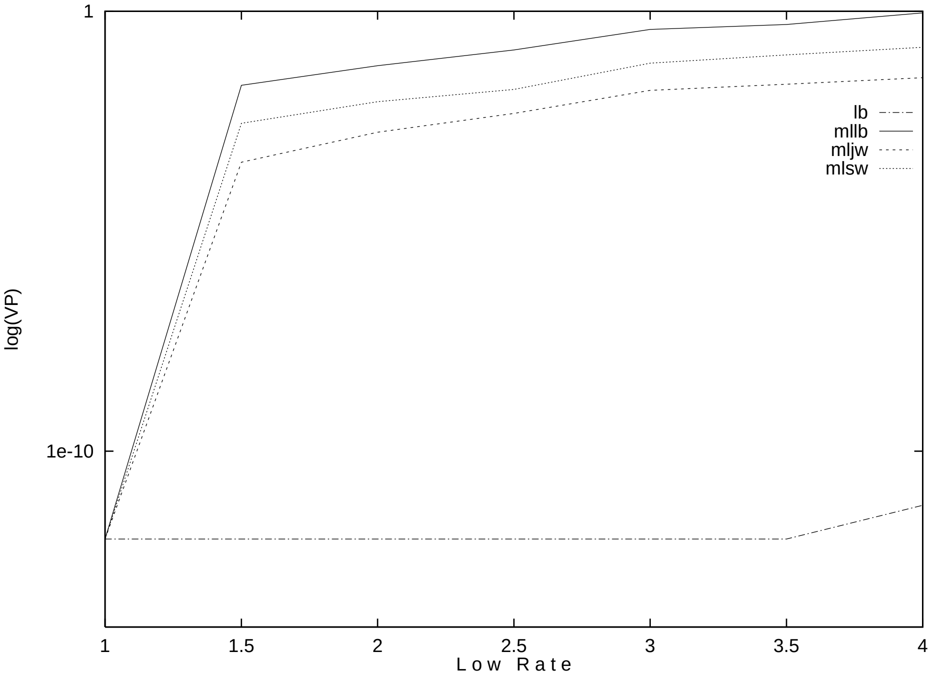

Figure 6: Violation probability x low bit rate

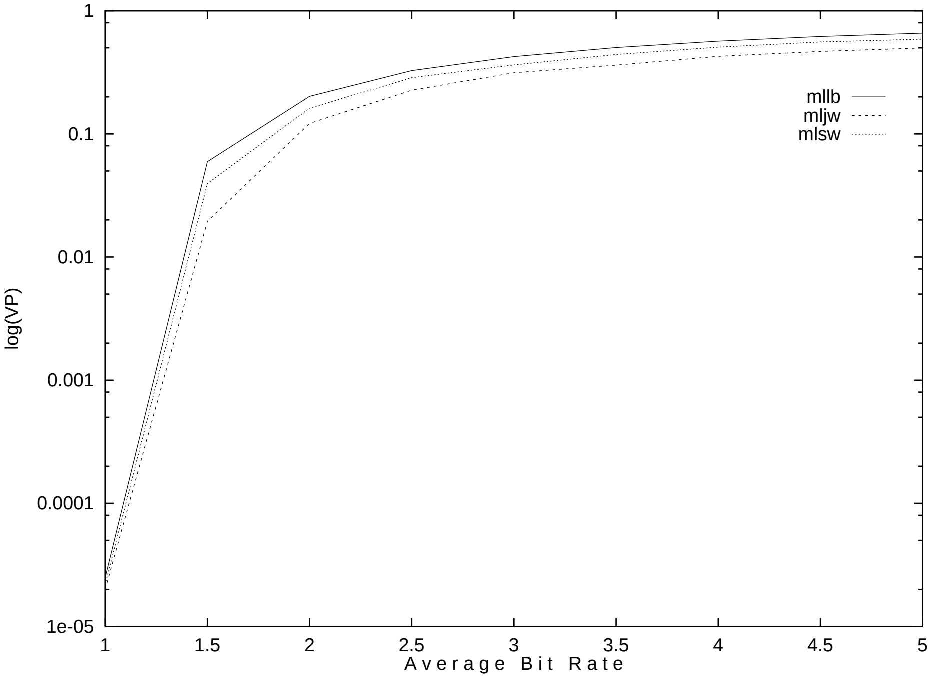

Figure 7: AR source

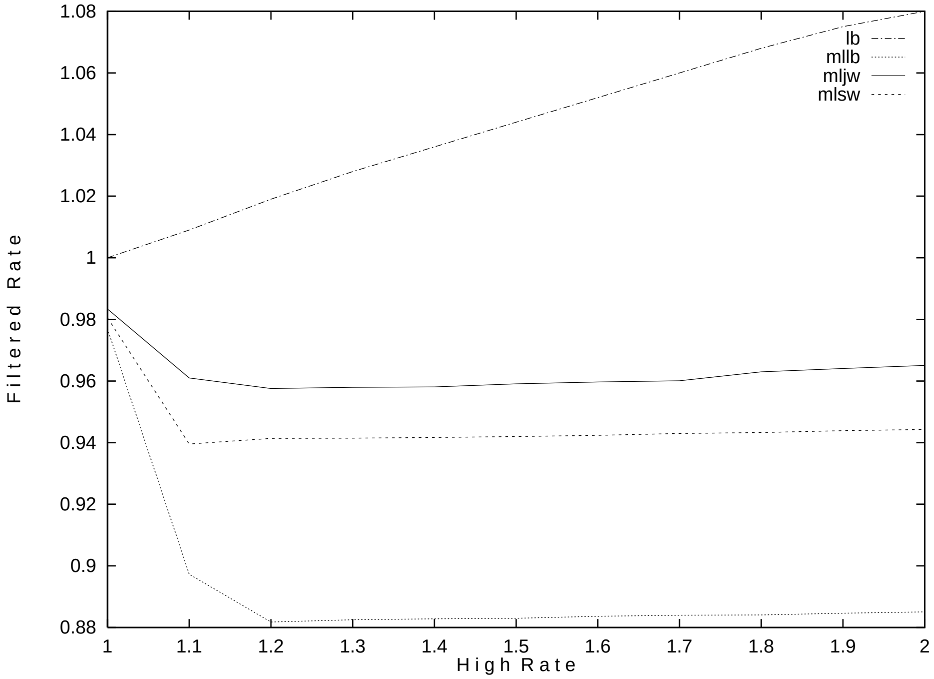

Figure 4: Filtered rate x Peak bit rate

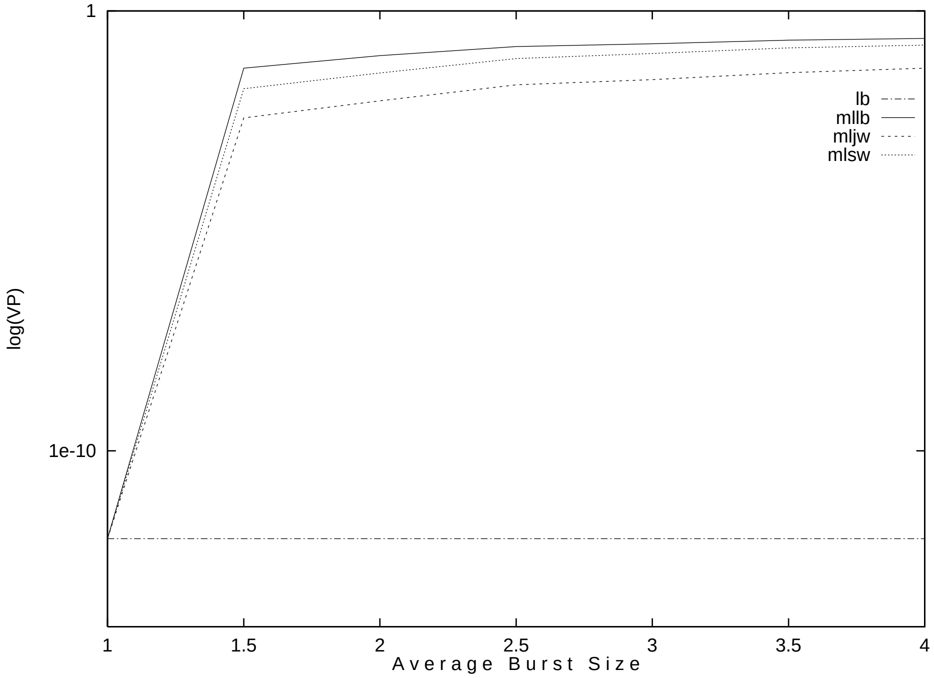

Figure 5: Violation probability x average burst size

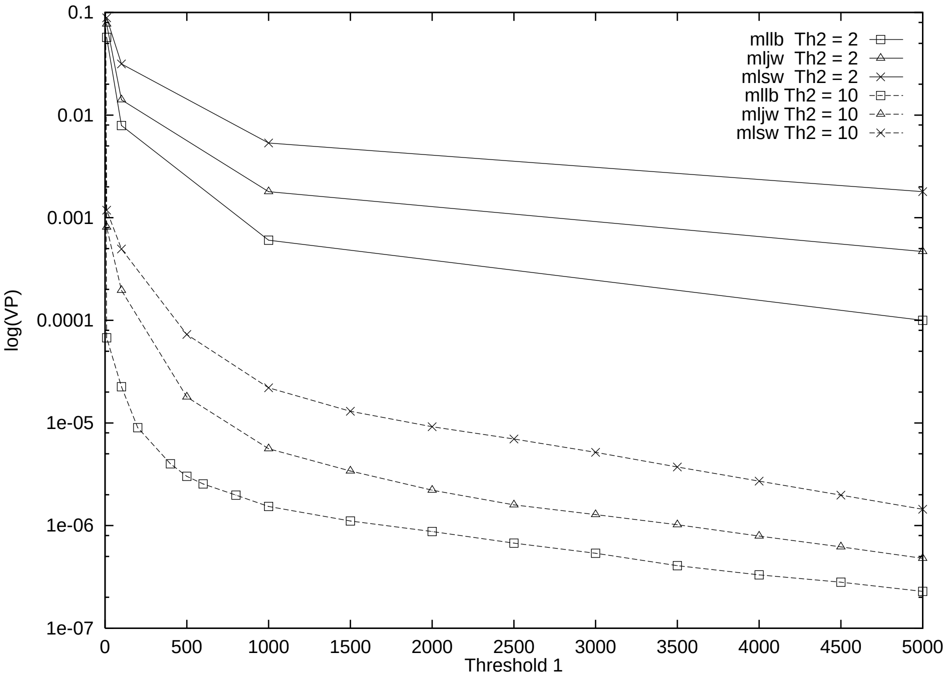

Figure 2:Violation Probability x Th1 for different Th2

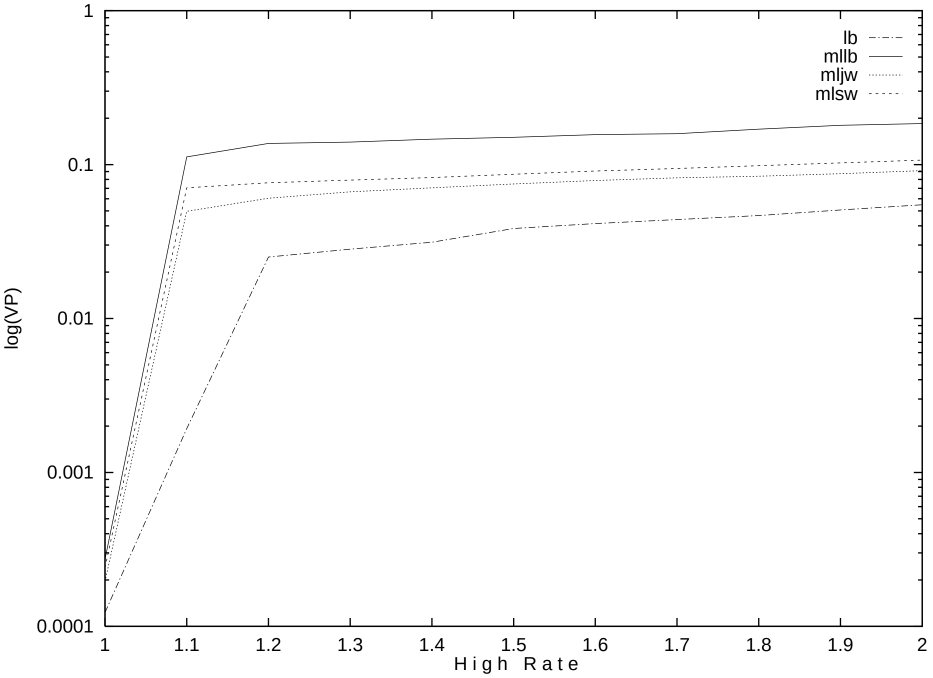

Figure 3: Violation Probability x Peak bit rate

[2] E. Rathgeb, “Modeling and Performance Comparison of Policing Mechanisms for ATM Networks”, *IEEE JSAC*, Apr,1991.

[3] V. Anantharam and T. Konstantopoulos, ``Burst Reduction Properties of the Leaky Bucket Flow Control Scheme in ATM Networks’’, *IEEE Trans. Commun*, Dec.,1994.

[4] J. Boudec,”An Efficient Solution Method for Markov Models of ATM Links with Loss Priorities”, *IEEE JSAC*, April 1991.

[5] K.Sohraby and M.Sidi, ``On the Performance of Bursty Modulated Sources Subject to Leaky Bucket Rate-Based Access Control Schemes’’, *IEEE T.C*., Feb/Mar/Apr, 1994.

Acknowledgements

The authors would like to thank CNPq, FAPESP, CAPES and Intel Corp. for their financial support.

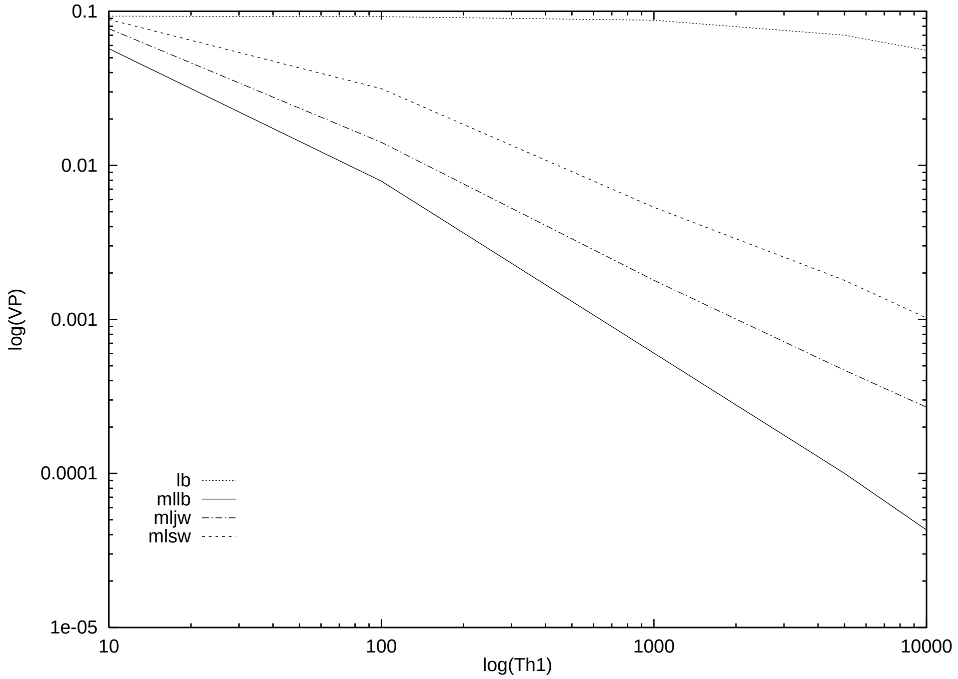

Figure 1: Violation Probability x Threshold 1

period. The high state bit rate has a very high bit rate, in fact we model it equal to the channel capacity, since cells are transmitted at each time slot during the busy period. The sojourn time in the high bit rate state is 2.27ms, the period required to transmit the information generated by the source at its highest bit rate. The sojourn time at the low bit rate state will be the remaining time of the frame, i.e. 31ms. The cycle will be the interarrival frame interval, i.e. 1/30s. And the ABR is equal to 10.6 Mbps. In other words, we allocate the channel bandwidth only during the amount of time that is required to transmit a frame.

In our experiment we changed the expected value of the Gaussian r.v. in order to increase the source's average bit rate. We can see in Figure 7 that the MLLB presents a very low violation probability for the source at nominal rates and is very efficient in detecting any large variation of the average bit rate of the source. It is clearly a better mechanism than the LB for policing this type of source since we do not need to allocate the peak bandwidth during the entire connection.

V) Conclusion

Multi-level mechanisms are simple to implement and give useful information about the current bit rate of a multi-rate source. They are also able to enforce the behavior of a variable-bit-rate source by allowing the source to transmit at different rates for certain periods of time. Our results show that multi-level mechanisms are much more effective than single-state mechanisms in detecting the misbehavior of variable-bit-rate sources. In general, the MLLB is more sensitive to the source's rate fluctuation than the window mechanisms. The novelty of the multi-level approach lies in the fact that we are able to mimic and to enforce the behavior of a multi-rate source.

VI) References

[1] J.A.S.Monteiro, M. Gerla and L.Fratta,``Leaky Bucket Analysis for ATM Networks'', *Proc. of IEEE SBT ITS*, 1990.

each time the system goes to state 2 and comes back in a period of time less than a minimum amount, called the minimum period, we decrease the value of Th_1 by *k* units. In our simulation we found out that *k* equal to 10 and the minimum period equal to 75 time slots for the MLLB give us a low violation probability at nominal rates and is still able to detect variations in the bit rate. This new adaptive algorithm is able to account for fluctuations of the low bit rate, and it is still able to detect violation of the peak rate very efficiently. Moreover, if the MLLB moves back and forth very frequently between two states it means that we chose the wrong rates for our states. In fact, this type of problem should not occur if the rates of the first and second state are chosen carefully. In other words, the rate of the first state should not be lower than the source's low bit rate state. A trivial solution is to turn on an alarm that indicates that the MLLB parameters were chosen incorrectly whenever the mechanism fluctuates very fast between two states.

V) Results for the AR Source

The AR source behaves similarly to an On-Off source. During the transmission of each frame we have a busy period where cells arrive at each time slot until all the data is sent, followed by an idle period where no cell is transmitted. The amount of data that needs to be transmitted is given by the AR formula. There is no time interval between the transmission of two consecutive cells therefore the instantaneous bit rate is equal to the channel capacity.

This type of traffic results in a very high violation probability for the LB mechanism even if the source does not violate its agreement. For this type of source the leaky rate must be close to the channel capacity otherwise the value of violation probability is extremely high even for large thresholds, e.g greater than 100,000. The LB cannot guarantee that the source will use the entire channel bandwidth for only a limited amount of time. On the contrary, the multi-level mechanisms are able to enforce the behavior of the source.

In order to handle the bursty behavior of this source, we model our mechanism with two states. The first state has a very low bit rate about 10kbps, since it is usually an idle

Case 2

The leaky rate and threshold of the LB are increased to 140 Mbps and 100 so that it can achieve a 10^{-11} violation probability for well-behaved sources. The MLLB's Th_2 is also increased to 100 so that it achieves the same violation probability; all others parameters are kept the same. We increase the average burst size in order to check if both mechanisms are able to detect the source misbehavior. As we can see in Figure 5, the LB is completely insensitive to the size of the burst. In fact the source can transmit at the leaky rate, i.e. close to the peak bit rate, for the entire duration of the connection without being ever detected. On the contrary, the multi-level mechanisms are able to detect the increase of the burst size. No significant difference among the multi-level mechanisms were observed. Moreover, since the mechanism knows how long the source has been transmitting at the peak bit rate, we can easily implement a policy that limits the duration of a burst.

Case 3

The rate of the low bit rate state is increased up to four times its value. The MLLB parameters are the same as in case 2. The leaky rate and the LB's threshold are 135Mbps and 20 respectively. (we can't chose a leaky rate close to the source's average rate because we would need to chose a threshold extremely large so that congestion could occur before we detect overload). Figure 6 shows that the LB is also completely insensitive to variations of the low bit rate. In fact, unless the low bit rate surpasses the leaky rate, the LB does not flag any cell. Although the multi-level mechanisms are sensitive to the variations on the low bit rate, it is not able to flag all violating cells. The violation probability is still low, on the order of 10^{-2}, when the low bit rate is twice its nominal value. This is due to the fact that C_1 is reset to zero each time it moves to the second state. Since the rate of the source is still lower than the second state rate, the system goes back to the first state and no cell is marked. The system keeps moving back and forth from the first to the second state and no cell is marked unless $MaxTime_2$ expires. In order to prevent this from happening we modified the control algorithm so that Th_1 gets smaller if the system moves from one state to another very frequently. In other words, *ABR* is very close to the source's average bit rate. The leaky rate, the maximum residence time and threshold for *State*$_1$ and *State*$_2$ are (50 Mbs, 2.0 s and 20), and (140 Mbs, 0.1 s, 10), respectively. The leaky rate and the LB's threshold are 135 Mbps and 20 respectively. We chose our settings so that both LB and the multi-level mechanisms present similar violation probability for well-behaved sources.

As we can see in Figure 3, the multi-level mechanism is very sensitive to variations of the peak bit rate, a small increase of the peak bit rate produces a sharp increase in the violation probability. In fact, even if we increase *Max_time*$_2$ to a larger value, the multi-level mechanisms are still capable of detecting the increase of the peak bit rate very quickly. The Leaky Bucket is also able to police the peak bit rate of the source but it does not detect the overload as fast as the multi-level mechanisms. No significant difference among the three multi-level mechanisms was observed.

In Figure 4 we present the filtered rate when the source exceeds the peak rate. The filtered rate is normalized by the average bit rate of the source. For the LB, the filtered rate is a function of the leaky rate. We can see that the filtered rate increases slightly when the peak bit rate is increased. In the multi-level case, the filtered rate drops fast whenever the source exceeds its peak bit rate. After a certain point, it remains almost constant, i.e. it does not depend on the source's peak bit rate. The filtered rate depends on the rates of each state. The MLLB penalizes the non-conforming sources more effectively than the window mechanisms. In this specific example the MLLB penalizes non-conforming sources by allowing the transmission of only 88% of its average bit rate. The MLSW was not much sensitive to the high rate variation allowing 98% of the average bit rate. We are able to tune the multi-level mechanism parameters to achieve any given filtered rate. In this way, we can implement different types of policies by choosing to penalize or not a non-conforming source. Moreover, since we have the knowledge of the source's state at any given time, we can dynamically adjust the filtered rate or the violation probability by changing the multi-level mechanism's rates. For example, we can increase the filtered rate of a source if we detect that more bandwidth is available.

old, so that it achieves a very high violation probability even if we choose high values for the threshold. In fact, in our experiments we increased the threshold as much as 50,000 and the violation probability was still large. In order to police the peak bit rate of a bursty source and to obtain a low violation probability, the leaky rate must be close to the source’s peak bit rate. Our results are in close agreement with [6]. On the other hand, the multi-level mechanisms presents lower violation probability than the LB even for a small threshold. The violation probability decreases linearly with the increase of the first threshold. Moreover, we notice that the MLLB is more sensitive to the variations of Th_1 than the window mechanism. The MLSW reacts slower than the other two mechanisms due to the memory of the last *m* cells.

Case 2

In the second experiment we looked at the violation probability as a function of the second threshold, Th_2. All other parameters for the multi-level mechanisms are kept the same as before.

A slight increase in the size of the second threshold from 2 to 10 provides a large reduction in the violation probability for the three mechanisms. The MLLB can provide a violation probability in the order of 10^{-6} for an *ABR* close to the mean bit rate of the source. Although the window mechanisms are also sensitive to the variation of Th_2, the MLSW present a significant higher (one order of magnitude) violation probability than the MLLB.

Scenario II - Non-Conforming Sources

In this case, the source violates its agreement in three different ways: i) it exceeds its peak bit rate, ii) it exceeds its average burst duration and iii) it exceeds its low bit rate. For each experiment we compute the violation probability and the filtered rate.

Case 1

In the first experiment the peak bit rate is increased from its nominal value 135 Mbps, up to twice its value, i.e. 270 Mbps. We model the multi-level mechanisms so that the

The second source is an autoregressive Markovian model. It is based on a measured data of a videophone scene and has a mean output bit rate of 3.9 Mb/s. The peak bit rate is about 10.575 Mb/s. The actual bit rate during the nth frame, λ_n, is calculated as follows:

$$\lambda(n)=0.8781 \times \lambda(n\text{-}1)+(0.1108 \times w(n) \times 7.5)$$

where *w(n)* is a Gaussian random variable with mean 0.572 and variance 1. There are 30 frames per second. The cells can be sent sequentially according to the maximum bit rate of the codec during a single frame. It implies a pattern with one burst and one silence period during each frame. This traffic stream yields a highly variable output stream with a coefficient of variation of about 10.6 for the cell interarrival times.

In the first scenario, the source behaves according to its connection agreement, so that the control mechanism should present a low violation probability. In the second scenario, we change the source's parameters so that it violates its agreement.

Scenario I - Well Behaving Source

Case 1

In this experiment, we chose the MLLB rates to be slightly higher than the source's nominal rates. $State_1$ and $State_2$ have bit rates of 40 Mbps and 140 Mbps respectively. $MaxTime_2$ is 0.3 s and the cycle time is 2.1 s. Therefore, the *ABR* is 54.28 Mbps. In other words, each 2.1 seconds the MLLB mechanism can spend at most 0.3 seconds in the high bit rate state. The *ABR* is closely related to the filtered rate. If we increase it we can increase the filtered rate. The maximum burst that a source can send is limited to 2 x $MaxTime_2$ if two bursts occur back to back at the end of the cycle. For this reason we did not choose a very large cycle in order to limit the value of the maximum burst size. The value of Th_2 is equal to 2 so that if a source exceeds its peak bit rate the MLLB (MLSW, MLJW) can detect it very fast. The violation probability is calculated for different values of Th_1, ranging from 20 to 5000. For the LB, we choose the leaky rate equal to the *ABR* and the threshold equal to Th_1

As we can see in Figure 1, the LB has a high violation probability for a leaky rate close to the average bit rate. Moreover, the LB is not sensitive to the size of the thresh-

IV) Numerical Examples

We are interested in calculating the violation probability and the filtered rate for well behaved and non-conforming sources. We define filtered rate as the average rate composed only of the cells that are not marked. It is the average bit rate that the source transmits if we assume that marked cells are discarded.

Ideally a flow control mechanism should work as a filtering device that allows the transmission of well behaved cells and marks the non-conforming cells. The violation probability must be low, in the range of the channel error probability, for well behaved sources and must increase if a source is exceeding its pre-defined parameters. Moreover, the filtered rate should be kept close to the source's average bit rate even if the source is exceeding its contract. The flow control mechanism needs to detect the misbehavior of a source and start flagging its cells in a short period of time. It should respond very fast, especially in the presence of non-conforming high speed bursty sources.

We illustrate the novel mechanism by showing the results for a two-level mechanism given that the wide-used criteria for admission control takes into consideration the average and the peak rate only. We compare multi-level mechanisms with the Leaky Bucket (single-level), since the LB is the single-level mechanism which better approaches the ideal policing mechanism.

In our numerical examples, we assume ATM traffic carried on SONET links with rates of 155.52 Mbps. Two traffic source models were used in our simulations to show the sensitivity of the results to the assumptions about the traffic models. The first source is a Markov Modulated Binomial Process (MMBP) with parameters set according to an HDTV model [4]. A source oscillates between two states (high and low). When in the low state it generates cells according to a low bit rate, 35 Mbps. When in the high state it generates cells according to a peak bit rate, 135 Mbps. The sojourn time in the low state corresponds to the time between scene changes and ranges from 1 to 3 s. The burst duration corresponds to the time to transmit one scene change and its average length is assumed to be 100 ms. The MMBP source can be characterized by the following set of parameters: i) the low bit rate, 35 Mbps, ii) the peak bit rate,135 Mbps; iii) the average burst duration, 0.1s; iv) the average low bit rate state duration, 2.0 s.

The threshold values can be made small, especially for high bit rates states, so that the mechanism can detect fluctuations in the current bit rate very quickly. The rates of each state depend on the characteristics of the contract and can be easily defined for an assumed multi-state, e.g. a MMBP source. In this way, we can keep track of the current bit rate of the source. We can increase the granularity of the mechanism by adding states, although this increases the complexity. Since many traffic models have only two bit rate levels, we can police many interesting sources with a two state policing mechanism.

We are also interested in policing the source behavior. If we limit the amount of time that the source can spend in each state we are able not only to monitor the source's behavior but also to enforce it. Therefore each state has another counter that measures the number of time slots that the system spends in it. We call these timers (*Timer*$_i$), to distinguish them from the cell counters. At the connection setup it is specified the maximum amount of time that a source can spend in each state (*Max_time*$_i$), i.e. transmitting at a given bit rate, within a given window of time interval. This interval window is called cycle. For example, an HDTV source transmits on average at 135 Mbps during 0.1 s out of a 2.1s interval. Therefore 2.1 s is the cycle.

If the system reaches the threshold in a state and cannot move to the next state because of the limited amount of time it can spend in any state, then incoming cells are marked. There is no limit to the amount of time that a source can spend in the lowest rate state.

We can define the Allowable Bit Rate (*ABR*) as:

$$ABR = \sum_{i=1}^{n} Rate_i \times Maxtime_i \big/ (Cycle)$$

which is the average bit rate that would be generated by a *n*-state MMBP process with the same rates and average sojourn times of the multi-level mechanism. It gives us a measure of the bit rate that the mechanism allows to enter the network without marking any cell.

remembered by a time interval of a window. For comparison purpose, the ratio between the maximum number of accepted cells in an window and the window width for these window mechanisms should be equal to the leaky rate.

These mechanism lack flexibility. For bursty sources, if we choose a small threshold, well behaving cells may be marked and the violation probability may be high. On the contrary, if a high threshold is chosen, the reaction time, the time interval until overload is detected, is large and congestion may occur. Moreover, the burstiness of the output flow of the queueing system increases with the threshold [3]. Another option is to choose a higher leaky rate, but then it is not possible to police the average bit rate of the source. The usual solution is to chose a leaky rate close to the source's peak bit rate, but this may waste bandwidth since the source usually does not transmit at full speed all the time.

The problem with these mechanisms is that we can change only two parameters: the leaky rate and the threshold when trying to police multi rate sources. In a multi-level policing mechanism, we have a larger number of parameters to be tuned, and consequently gain more flexibility to better monitor the source transmission rate with little additional complexity.

III) Multi-Level Policing Mechanism

Multi-level policing mechanisms can be used either to estimate a variable-bit-rate source's state or to enforce a source behavior. A multi-level policing mechanism consists of n states where each state i has an associated single-state mechanism. In the Multi Level Leaky Bucket (MLLB) for each state i there is an associated rate $Rate_i$ and a threshold Th_i, where $Rate_{i+1} > Rate_i$. In the window mechanisms, each state has its own threshold and window size. When the source increases its bit rate, the counter of the current state reaches a threshold and the system moves to the next state, a higher bit rate state than the previous one. If the counter of the state, C_i, reaches zero, the system moves to the previous state, a lower bit rate state. Therefore at any given time, the current state of the multi-level mechanism reflects the approximate bit rate of the source.

In this paper, we investigate multi-state mechanisms based on the traditional leaky bucket, jumping window and sliding window mechanisms [2]. We show the benefits of adopting the multi-state approach and compare the ability of different multi-state mechanisms to support variable-bit-rate sources. Our numerical examples show the impact of several of the mechanism's control parameters, such as the counter threshold, window size, etc., on the violation probability and on the filtered rate. We also show the mechanism's properties when the admission contract is violated by increasing the average and/ or peak rates of the source. In our analysis, we use two different arrival processes: a Markov Modulated Bernoulli Process and an auto-regressive process. We found that our results were insensitive to the arrival process. We conclude that multi-level policing mechanisms are much more effective for ATM traffic control than their traditional counterparts. We also found that among those compared, the multi-level leaky bucket is most accurate in monitoring a variable-bit rate source.

II) Policing Mechanism

A policing mechanism keeps track of a source in order to enforce that its behavior is in accordance with the parameters negotiated at the call setup time. For example, if a source transmits faster than its agreed peak bit rate a policing mechanism either discards or marks the excessive cells as violating (in this paper, we consider that cells are marked). Several policing mechanisms have been proposed. Among them, we consider the leaky bucket, the jumping window and the sliding window and their multi-state counterparts

The Leaky Bucket (LB) consists of a counter, a (leaky) rate and a threshold. Each time a cell arrives, the counter is incremented provided it has not reached the threshold. The counter is decremented at a constant rate, the leaky rate, if its value is greater than zero. If the counter reaches a predefined threshold, the corresponding cell is marked. The Jumping Window (JW) mechanism limits the number of accepted cells within a fixed time interval. A new interval starts immediately at the end of the proceeding interval and the associated counter is restarted at every new window. Similarly, in the Sliding Window (SW) mechanism the number of cells in a window is also limited. However, each cell is

I) Introduction

Statistical multiplexing was adopted in the ATM standard due to its potential for effective use of bandwidth. Coping with diverse Quality-of-Service requirements and with the variable-bit rate nature of multimedia applications makes traffic control a challenging task, so it is no surprise that traffic control mechanisms are a topic of intense research. A key function is that of policing, a mechanism to keep track of a source in order to enforce that its behavior is in accordance with the parameters negotiated at call setup time. In this paper, we show the advantages of adopting multi-level policing mechanism for ATM traffic control and compare several different mechanisms.

Traditional policing mechanisms lack flexibility in policing variable bit rate sources due to the small number of variables used to keep track of the source behavior. For instance, a leaky bucket mechanism is implemented by a counter, a (leaky) rate and a threshold. The counter is incremented at every arrival and decremented at the leaky rate. All arriving cells which find the counter at its threshold value are considered to be violating cells. For bursty sources if we choose a small threshold, well behaving cells may be marked as violating cells. If a high threshold is chosen the reaction time may be too large and congestion may occur. On the other hand, if we set a leaky rate close to the average arrival rate we do not allow bursty periods. Moreover, if we choose the leaky rate close to the peak arrival rate, we might waste bandwidth [1].

In a multi-state (multi-level) policing mechanism, we have a set of variables for each state. In addition to the traditional set of parameters (leaky rate, threshold, and counter), we also have a maximum residence time which is used to monitor the time that a source may transmit at a certain rate. Whenever the counter associated with a state reaches its threshold, the controller changes state and moves to a state with a higher leaky rate. If the counter reaches its threshold and the controller is prevented from moving to the next higher state due to expiration of the residence timer, then arriving cells are considered to be in violation. There is also a low threshold (usually zero). When the low threshold is reached the controller moves to a lower level state. In this way, we are able to better estimate or track the current bit rate of a source. Moreover, this new flow control mechanism is able to police sources with widely fluctuating transmission rate.

The Effectiveness of Multi-Level Policing Mechanisms in ATM Traffic Control

J.A. Silvester[1], N. L. S. Fonseca[2], G. S. Mayor[1] e S. P. S. Sobral[2]

University of Southern California[1]
Department of Electrical Engineering - Systems
Los Angeles, CA 90089-2562
U.S.A.

State University of Campinas[2]
Institute of Computing
P.O. Box 6176
13081-970 Campinas SP
Brazil
{nfonseca, ssobral}@dcc.unicamp.br

Abstract

Statistical multiplexing was adopted in the ATM standard due to its potential for effective use of bandwidth. Coping with diverse Quality-of-Service requirements and with the variable-bit rate nature of multimedia applications makes traffic control a challenging task. In this paper, we show the advantages of adopting multi-level policing mechanism for ATM traffic control and compare different multi-level mechanisms based on the Leaky Bucket, on the Sliding Window and on the Jumping Window mechanism

O conteúdo do presente relatório é de única responsabilidade do(s) autor(es)
(The content of this paper are the sole responsability of the author(s))

The Effectiveness of Multi-Level Policing

Mechanisms in ATM Traffic Control

J.A. Silvester, N.L.S. Fonseca

G.S. Mayor, S.P.S. Sobral

Relatório Técnico IC 96-08

Agosto de 1996