CONGESTION CONTROL IN AN ATM NETWORK

D.A. HUGHES, H.S. BRADLOW

Switched Networks Research Centre, The University of Wollongong,
P.O. Box 1144, Wollongong, NSW, Australia 2500.

G. ANIDO

Network Research & Development, O.T.C. (Australia) Ltd.

Broadband ISDN resource allocation and congestion control present a major challenge. A preventative control scheme based on a call admission procedure and source policing is favoured by a number of groups. This paper investigates the behaviour of the leaky bucket policing mechanism. Simulation studies of a simple ATM multiplexer model in which a number of policed sources feed a deterministically served buffer indicate that under overload conditions the leaky bucket can introduce correlations into the policed stream. These correlations result in lower than expected long term cell loss within the network accompanied by a rise in the conditional probability of successive cell losses for a particular user.

1. INTRODUCTION

The availability of wide bandwidth optical data links capable of carrying hundreds of megabits per second and a growing demand for high performance integrated networks are pushing forward research and standardisation efforts aimed at implementing a broadband integrated services network. Despite the wide acceptance of the potential of Asynchronous Transfer Mode (ATM) has been standardised as the switching technique for the BISDN [1] there are nevertheless significant outstanding problems which require attention. In particular there is a need to define methods by means of which network providers can control the traffic load and guarantee to give customers the quality of service for which they have paid. This issue is complicated by the wide range of traffic characteristics which may be offered to the network.

One attractive possibility is a three level resource management architecture [2] based on a preventative congestion control strategy. At the highest level resources are allocated to virtual paths. The next level is connection admission control which allocates path capacity to calls based on traffic parameters, quality of service requirements and available network resources. The lowest level, connection usage control, is concerned with policing traffic streams to ensure their statistics remain within the agreed bounds. These ideas are expanded in section 2 which describes preventative congestion control and examines the possibility of using policed virtual paths in an implementation of the three level scheme suggested.

In this layered scheme policing plays two important roles: first monitoring the users traffic streams and secondly eliminating interference between paths. In section 3 we describe a simple model which allows us to investigate the characteristics of policing mechanisms in both contexts. The model is essentially a deterministically served multiplexer fed by a number of policed streams. Section 4 presents the results of simulation studies investigating the leaky bucket policing mechanism. It is found that correlations introduced into the traffic stream by the policer have unexpected effects on the multiplexer performance.

2. PREVENTATIVE CONGESTION CONTROL

Congestion in packet switched networks is traditionally controlled by means of buffers which temporarily store packets until the transmission channels become available. However in all networks there is a practical limit on the size of the buffers, and in ATM networks this is particularly true since buffer sizes are not only bounded by economic considerations but also by a desire to ensure that the overall delay and delay variance experienced by a cell is minimized. Since the buffer sizes are small there is a probability of buffer overflow which will result in cell loss within the network. Therefore some mechanism (in addition to buffering) is required to avoid, or at least control, congestion. The reactive flow control schemes used in existing packet networks are unsuitable for use in a broadband environment since they are fundamentally limited by the ratio of link speed to propagation delay. Consequently it is widely agreed that preventative control will be the most simple and effective approach to controlling congestion in an ATM network [2][3][4][5].

2.1 Connection Admission Control

A preventative congestion control strategy governs access to the network resources with a connection admission procedure which blocks calls likely to drive the network into congestion. This concept is familiar to all circuit switched network users, where unless the channel is available from source to destination, the user’s call is blocked. In the case of an ATM network, the situation is complicated by the fact that the
user may not want continuous use of the full bandwidth of a channel. The network may exploit this to achieve better utilisation of resources through statistical multiplexing. In order to do this it must examine the traffic statistics proposed by the user and determine whether links and nodes between the source and destination have the capacity to handle the extra load.

2.2 Connection Usage Control

Having allowed the user to vary the use of the network resources during a call, it is necessary for each virtual circuit to be policed to ensure the negotiated characteristics are not ignored. Excessive traffic may be discarded by a policing unit (or enforcer) before entering the network. Alternatively it may be tagged as low loss priority and allowed to enter the network [4][5] in which case it is preferentially discarded by the network nodes during periods of congestion. In some applications where cell loss must be avoided the user may employ a shaper. A shaper is identical to the enforcing unit, only instead of discarding cells it buffers them and throttles the source in order to prevent cell loss. In effect it shapes the traffic to have the desired characteristics, so that the cell loss imposed by the enforcer within the network can be avoided.

2.3 Leaky Bucket Algorithm

Enforcers will be required for every virtual circuit so the policing algorithm must be simple and economic to implement in high speed hardware. The leaky bucket (shown in figure 2) has been proposed as a suitable mechanism which can be used to limit the rate and burstiness of a connection [5][6]. It is essentially an up-down counter, which saturates at a maximum count of K and a minimum of zero. The counter is incremented by each cell "passing into the bucket". When the counter reaches K, the bucket is "full" and the cell must be discarded. Meanwhile the counter is decremented (the bucket is "leaking") at a constant rate R. The leaky bucket limits the cell arrival rate to R. The timescale over which the policing applies is determined by the depth K and the maximum continuous burst length permitted is K/(1-R). Shallow buckets are suitable for policing peak rate; deeper buckets can be used to police average rate.

![Figure 2: Leaky bucket policing mechanism](image)

2.4 Policed Virtual Paths

Virtual paths are pre-established routes through the network into which virtual circuits may be grouped [1]. Although the virtual path was initially seen as a means of reducing routing overheads, other advantages have since been realised. In particular there is potential to use different virtual paths for disparate services on the same route, allowing the cell loss rate to be tailored for each individual service [2]. In order to prevent interference between the calls on different virtual paths and achieve the virtual separation depicted in figure 3 each path could be peak rate policed. In a layered management scheme the call acceptance procedures for each path could be implemented independently. Services for which high statistical gain was desired (at the expense of a higher cell loss) could coexist on the same links with other services for which it was required to minimize the cell loss (at the expense of less efficient use of bandwidth). Furthermore by opening a virtual path for each homogeneous traffic type, not only could the characteristics of each path be tailored to the requirements of the specific service it carries, but it also may make the calculation of the traffic statistics more tractable.

At first sight, the virtual separation of traffic may appear as moving a step away from integration. Note however, that a system using virtual separation is far more flexible than one with physical separation. The network operator may change the bandwidth allocation and indeed the route of any virtual path in response to demand. The boundaries between paths are hard but not immovable. Partitioning transmission capacity into peak policed virtual paths may appear to sacrifice the gains available by statistically multiplexing the virtual paths themselves. However, often an overall increase in efficiency will be
achieved since the virtual separation implies there is no need for a uniformly high grade of service for all the paths on a given link.

3. POLICED SOURCE MULTIPLEXER MODEL

The complex interaction between nodes makes it extremely difficult to analyse or simulate an ATM network as a whole. Our approach is to reduce the ATM network into decoupled policed source multiplexer performance models as in figure 4. The inherent assumption when making such a simplification is that the switches have a negligible effect on the parameters of the virtual circuits they carry. Because the switch buffers are small there is little opportunity for them to cause cell jitter large enough to change the call parameters (e.g. the peak or average rate) and because ideally the probability of loss within the network is small this assumption would appear to be intuitively acceptable. By comparing the results using single multiplexer models with simulation results for two or more cascaded stages it is possible to examine the implications of decomposing the problem into smaller parts. This approach has been followed by Woodruff et al [3] and their findings indicate that the resulting loss and delay estimates for the decoupled system tend to be conservative.

By extending our scope to consider policed virtual paths we can identify two fortunate isomorphisms. The sources depicted could represent virtual paths, each being peak policed and multiplexed into a switch buffer. Furthermore by realising that a leaky bucket peak policing mechanism is very similar to a deterministically served queue we can identify this same basic subsystem at a lower level where policed virtual circuits are grouped into a virtual path.

The authors have limited their investigation to consider only the discard-at-the-edge enforcement policy. In this case the cell loss probability for a call can be divided into two components:

(i) discard by the source policing mechanisms, and

(ii) cell loss within the network due to buffer overflows.

The first component is a function of the source characteristics and the policing parameters and can be avoided by not exceeding the negotiated statistics or by using a shaper. The user must be able to estimate the likely component of loss due to policing in order to specify a suitable call policing parameters.

The second component is a sum of the loss due to overflow in all the intervening nodes. Looking at each node in isolation this is a complicated function of the source characteristics and policing parameters of every call sharing the multiplexer buffer. When overflow occurs the cells are dropped arbitrarily. This component characterises the degree of interference between policed streams, and assuming no malicious correlations, is shared evenly amongst all the users.

Of most interest is the maximum value of this cell loss probability as a function of the policing parameters, independent of the offered traffic load and statistics. It is this quantity which determines the quality of service that the network provider can guarantee. An estimate of the maximum probability of cell loss within the network could provide the basis of a very robust call acceptance procedure: when a request for a connection is received the new maximum loss probability is calculated and if this expected loss exceeds some acceptable level, the call is blocked.

The aim of the authors work has been to characterise these two loss components and to examine the effects of correlations, which have been found to be non negligible.

4. RESULTS

The investigation concentrated on understanding the behaviour of shallow leaky buckets. Such devices may be suitable for peak policing virtual circuits or for the separation of virtual paths. Using the single multiplexer model the effects of the following have been studied:
A selection of the most significant results are reported here.

Figure 5: Multiplexer queue distribution against normalised offered traffic intensity.

An unexpected relationship was observed between the offered traffic intensity and the multiplexer queue distribution and hence loss due to buffer overflow. Figure 5 shows simulation results for a typical configuration (three Bernoulli sources, each policed with a leaky bucket mechanism of depth 15 such that the total traffic into the multiplexer (dimensioned load) does not exceed 99% of the outgoing link capacity. The buffer size was chosen large enough that no cell loss was experienced.)

Figure 6: Cell interarrival distribution of a policed stream against normalised offered traffic intensity.

The tail of the queue distribution extends dramatically as the offered traffic (normalised with respect to outgoing link capacity) approaches one. This is fairly intuitive: the policers discard few cells when the system is underutilised and hence the queue length increases with the offered traffic level. The decrease in queue length as the offered traffic intensity exceeds one requires a more complicated explanation. When the offered traffic exceeds the policed rate cells are discarded by the policer in such a manner that correlations are introduced. When the bucket is full only the first cell following a decrement is permitted past the policer. As the load increases the bucket is more likely to be full and hence the effect becomes more prominent. This is reflected in figures 6 and 7 which show the cell interarrival distribution and serial autocorrelation for the policed stream for various loadings. As the offered traffic increases the cell interarrival distribution shifts from geometric to deterministic. This in turn reduces the multiplexer buffer occupancy since the policed stream has less variance in, and some correlation between, interarrival times.

Although these figures (5, 6 and 7) correspond to a specific system this phenomenon was observed for all the parameter sets which were investigated. This effect is significant since it implies that as the load offered to the network increases above the dimensioned capacity the cell loss within the network will in fact drop. If some sources attempt to overutilise the network, the remaining users may experience a reduction in cell loss rate although the network throughput is higher. However while the periodicity introduced by the policer may cause a drop in the absolute probability of cell loss this may be accompanied by a rise in the conditional probability of losing successive cells from the same source. The effects of such correlations are of current interest [7][9]. It may be possible to eliminate the correlations and these negative effects by using modified leaky buckets with a non-deterministic decrement signals.

Figure 7: Autocorrelation of a policed stream for normalised offered traffic intensities between 0.6 (flattest line) and 1.5 (most spiky line).
The following figures (8, 9 and 10) seek to illustrate the effects of bucket depth, policed rate and source burstiness on the multiplexer performance and in particular to clarify the generality of the observations made above. The plots show loss due to overflow in a finite buffer multiplexer, with twenty waiting places and ten homogeneous sources.

The maximum loss probability increases with bucket depth. Also note that the position of the peak loss appears to be independent of bucket depth.

The effect of dimensioned load, that is the sum of the policed rates as a fraction of the outgoing link capacity, is seen in figure 9. If the network is dimensioned such that the utilisation can approach one, the expected queue length and hence the probability of buffer overflow rise dramatically. The offered traffic intensity at which cell loss probability is maximum is slightly affected by the dimensioned load.

Figure 8: Cell loss probability due to overflow versus offered traffic intensity for bucket depths varying from 1 (bottom curve) to 20 (top curve), dimensioned load constant at 95%.

Figure 9: Cell loss probability due to overflow versus offered traffic intensity with dimensioned loads varying from 90% (bottom curve) to 99% (top curve), bucket depth constant at 10.

Figure 10: Cell loss probability due to overflow versus offered traffic intensity for a bursty source model (average burst length, B noted on plot), dimensioned load constant at 95%, bucket depth constant at 5.

Increasing the bucket depth of the policer extends the time scale over which the rate is measured, tending to permit more bursty sequences of cells to enter the network. This obviously results in a lower loss due to discard by the policing units and hence the possibility of achieving greater multiplexing gain, but is offset by higher loss within the network and hence interference between users. Figure 8 confirms that the maximum loss probability increases with bucket depth.

5. CONCLUSIONS

It is clear the BISDN will be based on an ATM network. The basic details of the switching technique have been finalised but the issue of congestion
control still requires attention. The most suitable scheme likely to be a preventative control strategy which governs access to the network resources. A three level resource management architecture could be adopted. By using policed virtual paths different qualities of service could be guaranteed in a network with no need for any priority scheme.

The behaviour of policing mechanisms is relevant to both source policing and virtual path separation. It is central to the issue of connection admission and the choice of parameters to describe a call. The ability to guarantee quality of service and yet maintain network efficiency will depend crucially on the ability to estimate cell loss within the network. A simple multiplexer model has been chosen to study the impact of policers on a traffic stream and the relationship between the policing algorithm and loss due to multiplexer (or switch) overflow.

Using this model some of the characteristics of the leaky bucket policing mechanism have been investigated. Simulations have shown that the periodic nature of the decrement signal applied to the leaky bucket can under overload conditions induce correlations in the policed stream. This observation is of significance since it implies the maximum cell loss within the network reaches a peak and then becomes less with further increases in load. It is this maximum cell loss probability which determines the quality of service which can be guaranteed to the users.

ACKNOWLEDGEMENT

The authors gratefully acknowledge the support of O.T.C. (Australia) Ltd. for this research work.

REFERENCES


