Reactive Management of Quality of Service in Multimedia OBS Networks Based on GMPLS

Fernando N.N. Farias[1], Rafael P. Esteves[1], Waldir A. Moreira[2], Antonio J.G. Abelém[1], and Michael A. Stanton[3]

[1] Research Group on Computer Networks and Multimedia Communications, Federal University of Pará, Belém, Pará, Brazil
[2] Institute for System and Computer Engineering of Porto, Porto, Portugal
[3] Computing Institute, Federal Fluminense University, Niterói, Rio de Janeiro, Brazil
{fernnf,esteves,abelem}@ufpa.br, wjunior@inescporto.pt, michael@ic.uff.br

Abstract. This paper presents a proposal for dynamic control of Quality of Service (QoS) in optical networks based on optical burst switching (OBS) using a GMPLS control plane. In this proposal, monitoring agents are used to verify the QoS experienced by the burst classes and to deploy reactive mechanisms in order to guarantee absolute performance levels. Using GMPLS traffic engineering, these agents also offer idle resources to traffic flows whose service level is not being achieved. Simulation results show that the proposal can minimize the blocking probability when there are violations of burst flow parameters.

Keywords: Quality of Service, Optical Burst Switching, Generalized Multiprotocol Label Switching, Traffic Engineering.

1 Introduction

The consolidation of optical networking and wavelength division multiplexing (WDM) provides optical links with transmission capacity of tens of gigabits per second. However, with the aim of extending the benefits of optical communication and minimizing the disadvantages of electronic switching, all-optical switching was proposed. Basically, there are three approaches to all-optical switching: optical circuit switching (OCS) [1], optical packet switching (OPS) [2], and optical burst switching (OBS) [3].

Of these paradigms, OBS is notable since it is a hybrid proposal between OCS and OPS, capable of solving problems encountered in these two paradigms, such as lack of scalability, or the need for optical buffers or for sending control information along with the data.

The extension of the MultiProtocol Label Switching (MPLS)the control plane the Generalized MultiProtocol Label Switching (GMPLS) [4] has provided the best way for integrating the IP protocol with WDM, because with generalized labels an end-to-end label-switched path (LSP) can be established regardless of the multiplexing technology used, whether it be by wavelength, cell/packet

R. Mehmood et al. (Eds.): EuropeComm 2009, LNICST 16, pp. 13–22, 2009.

or time division, thus providing a simpler architecture, with intelligence and guarantees.

Quality of service (QoS) is important in all-optical networks and multimedia applications because of the increasing performance requirements of network applications, and also of the existing restrictions on optical technologies for temporary information storage. In [3], there are two basic models of QoS in OBS networks multimedia application: absolute QoS and relative QoS. In absolute QoS, quantitive performance limits are of great importance, such as in requirements of guarantees of maximum delay, minimum blocking, or minimum bandwidth. In relative QoS, the QoS parameters are not defined in absolute terms, but based on criteria that allow, for example, a high priority burst class to have a lower blocking probability than that of a low priority class, but there is no imposition on how small this probability must be.

However, in scenarios with a very high traffic load, the traditional QoS mechanisms cannot guarantee the desired performance, even if there are available resources in other routes of the network. GMPLS traffic engineering can be used for offering quality of service for OBS networks with a dynamic decision-making scheme to help in the choice of alternative routes. Reactive QoS management could monitor blocking probability levels of burst classes and offer idle network resources to these bursts, in order to reduce blocking in all classes.

The goal of this paper is to propose an architecture for dynamic control of QoS in OBS networks which uses the GMPLS control plane. Each class has its QoS context, which are metric values (e.g., delay, jitter or blocking probability) defined for a given class of service that must be satisfied. Dynamic QoS-control agents located at nodes in the OBS core monitor QoS measurements for each burst flow and, in the case of a parameter violation, they generate alarms and adjust the flow dynamically, using GMPLS traffic engineering, diverting affected flows to alternative routes that have idle resources. To validate this proposal, extensions were built for the Network Simulator 2, such as modules for QoS management and for OBS networks with GMPLS control plane and monitoring agents.

This paper is organized as follows. In Section 2, we describe related work. In Section 3, we provide an overview of OBS network architecture and of the detailed functioning of dynamic control agents. In Section 4, the proposal is analyzed in order to evaluate its impact on QoS in the OBS network. Finally, Section 5 concludes the paper and lists intended future works.

2 Related Work

In [5], a proposal for dynamic QoS is presented, using admission control at each OBS network node. A new model of admission protocol for bursts is proposed, using an OBS network architecture where each node is composed of a switching unit, a wait unit formed by fiber delay lines, a switching control unit (responsible for resource reservation and contention resolution), and entry and exit processing units. When it needs to send a burst, the entry edge node sends a burst control packet (BCP) with QoS information and delay statistics. Intermediate nodes receive the BCP, check the QoS values and estimate delay and blocking metrics. In the case of blocking, the control unit routes the incoming burst to a fiber delay line (FDL). If no FDL is available, the burst is discarded. On exit of the burst from the FDL, if blocking is still taking place, the burst is discarded. If the delay estimate exceeds the value defined in the QoS metric, the burst is also discarded.

In [6], it is proposed to use the differentiated services (Diffserv) architecture to offer QoS in OBS networks. Burst control packets are electronically processed to provide differentiated treatment to the corresponding bursts through different per hop behaviors (PHBs) for the services supported: Expedited Forwarding (EF), Assured Forwarding (AF) and Best Effort (BE). The definition of these PHBs has an impact on the process of burst assembly that varies according with the service class.

Both static and dynamic burst admission control mechanisms are proposed in [7]. The two mechanisms are similar, reserving a certain number of wavelengths in a link for each service class. Both are based on link usage for admitting bursts of each service class and, in this way, to differentiate the blocking probabilities experienced by different classes. The two mechanisms use the JET protocol and are used at those OBS network nodes where each burst occupies an entire wavelength during transmission and the node has complete capability for wavelength conversion.

The main problem of these previous approaches is that, in high traffic scenarios, none of them takes into account the availability of alternative network resources that could be used, even when the proposed techniques are incapable of guaranteeing the fulfillment of absolute restrictions on performance. The intention of this paper is to get around the limitations identified in the work mentioned here, through dynamic adaptations in the paths used by the burst flows, so that their QoS parameters are satisfied in an absolute way.

3 Dynamic Control of QoS in OBS Networks

3.1 Dynamic QoS Management Architecture (DQM)

In order to provide QoS in OBS networks, we propose an architecture for dynamic QoS management (DQM) that offers tools to provide improved control and monitoring of the service classes supported by the OBS network. In Figure 1, we present a general view of the DQM architecture.

In the proposed architecture, aspects related to the metrics, policies, decision making and agent are highlighted. The metrics are QoS measurements collected by the agent in the node where it is present. For this paper, we just observed the blocking probability.

The policies are restrictions on the QoS context that should be obeyed for the service classes of the OBS network. The context of each class contains thresholds with the maximum or minimum values of metrics that should be guaranteed.

Decision making defines the actions that are to be carried out as a result of possible policy violations (QoS context violation), and these actions can include the sending of an alarm to the network edge or the rerouting of flows using GMPLS traffic engineering. The agents are responsible for monitoring the network and to carry out QoS management actions.

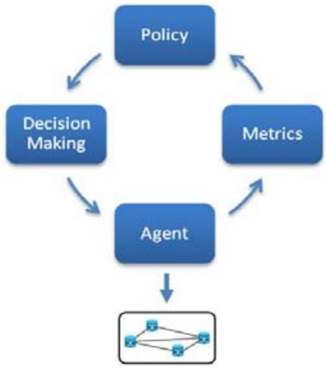

Fig. 1. View of the DQM architecture

3.2 DQM Agent

A Dynamic QoS Management Agent (DQMA) is incorporated into each node of the OBS network, as shown in Figure 2. A DQMA can be classified as a core DQMA or an edge DQMA.

A core DQMA has as function updating the metric tables while traffic goes through the node, and of sending an alarm to the edge DQMA in the case of a QoS context violation for a given service class. The metric stored in this table is the blocking probability that is calculated for each burst flow which is classified in one of the classes.

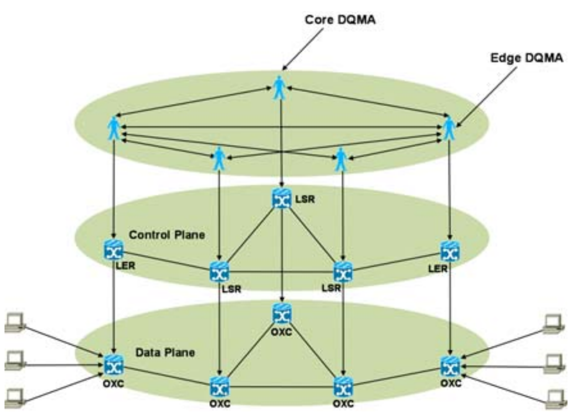

Fig. 2. DQM Agents

A core DQMA receives the context of each class, containing information on QoS measurements (for example: maximum value of blocking probability supported by the class) that should be obeyed in an absolute way. This information is stored in a policy table such as: High Class has 10% of blocking; Average Class has 20% of blocking; and Low Class has 30% of blocking. During network operation, comparisons are made between the metric values and the defined limits in the policy table. In case of detection of a QoS context violation, the core DQMA sends an alarm to the edge DQMA reporting which classes suffered as a result of policy violations, and which flows of those classes were the most affected.

An edge DQMA has the same functions as a core DQMA, with the difference of being capable of receiving and processing alarm signals sent by core agents and interacting with the GMPLS control plane to divert flows that are experiencing QoS context violations. An edge DQMA stores alternative routes that can be used in case of a QoS context violation. The number of alternative routes varies for each class, and is also in accordance with the available resources in the network. A high priority class will have a larger amount of additional routes to their flows. Figures 3a and 3b illustrate the agents' operation.

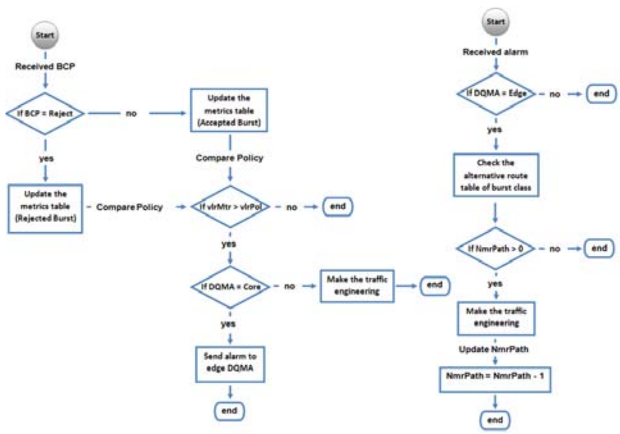

Fig. 3. DQMA operation for receiving: BCP (a) and alarm (b)

When a network node receives a BCP, the availability of wavelengths is verified for its outgoing link. If resources are available for the burst corresponding to the BCP being processed, the accepted burst counter for the DQMA of the node is updated. If there is no wavelength available for the burst at the moment of the request, the blocked burst counter is updated. In both cases, a comparison is made between the value of the blocking probability metric based on the collecte/stored values in the DQMA and the limits established in the policy table (if vlrMtr > vlrPol). In the case of a QoS context violation, the core DQMA sends an alarm to the ingress edge DQMA that makes a traffic engineering decision based on the existence of alternative routes for the service class (if NmrPath > 0). If an alternative route is available for the flow, then the flow is rerouted. An edge DQMA does not send an alarm to itself; in this case, traffic engineering is carried out automatically.

In order to incorporate DQMA into OBS networks, modifications to OBS signaling were needed to minimize the amount of control information exchanged by DQMAs and to take advantage of the OBS signaling, represented by BCP, to store the QoS context of each burst. This allows a burst class to change its context characteristics dynamically, as well as to offer the possibility of an individual flow altering its service class in a way that is transparent to the OBS network.

Three fields are added to the BCP structure: the flow identification (ID Flow), the identification of the class to which the burst belongs (ID Class) and the maximum blocking probability allowed for the class.

4 Analysis of the Proposal

This section evaluates the impact of the use of QoS monitoring and of a managing architecture based on the blocking probability of the burst classes in an OBS network using the GMPLS control plane. To this end, simulations were carried out using the NS-2 platform [8].

Several extensions to the simulator were developed to make it possible to analyze this proposal. Among the main contributions, we can enumerate: a component to simulate an edge OBS node that is capable of gathering packets into bursts and implementing JET signaling, a DQMA responsible for monitoring the burst flows, calculating the statistics of each flow and sending alarms to the network edge in the case of a QoS context violation.

The chosen topology for the simulations is based on a hypothetical extension to the backbone of the Brazilian National Research and Education Network (RNP) [9], with the addition of nodes and links that allowed the creation of alternative routes for the bursts. These links have a capacity of 10 Gb/s and a propagation delay of 1 millisecond. Each link has eight wavelengths and the high priority class (gold) can use up to four, the intermediate priority class (silver) has three reserved channels and the low priority class (bronze) can use up to two wavelengths. Figure 4 shows the network topology.

Fifteen traffic generators are used and are distributed according to four scenarios that differ in the amount of traffic attributed to each of the three service classes. In the first traffic scenario, the load was split in one third of the amount of burst traffic for each of the considered classes, namely class, silver, bronze. For the second traffic scenario, the load was divided in 46% for gold class, 27% for silver class and 27% for bronze class. As for the third traffic scenario, the distribution was of 27% for gold class, 46% for silver class and 27% for bronze class. Finally, in the fourth traffic scenario, the amount remained the same but with 27% for gold class, 27% for silver class and 46% for bronze class. Individual packets have size of 500 bytes [10]. The process of burst assembly is based on the fixed size, in other words, it will only be sent when it reaches a given size.

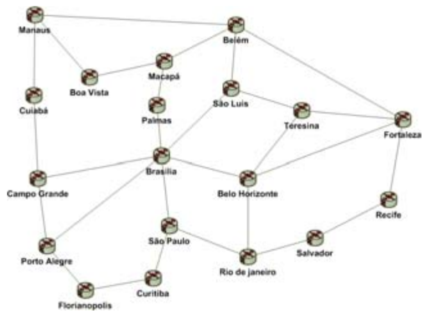

Fig. 4. Topology used in the simulations

In this paper, bursts are of 125KB on average [6]. The arrival of bursts follows a Poisson distribution.

The source of the flows of the gold class is the Brasília node and the destination is the Belém node. For the silver class, the source is the Recife node and the destination is the São Paulo node. Finally, the bronze class flows are sent from the Porto Alegre node to the Manaus node.

The alternative routes are known by the edge DQMAs and were defined according with the burst service class. There is a set of alternative routes for the bursts of a class. It was determined that the gold class bursts have three options of alternative routes, the silver class has two alternatives and the bronze class has only an additional route. Below, we have the original routes of each class and their respective alternative routes:

- *Gold:*
  Real route: São Luis, Brasília, Belém
  Alternative Route 1: Brasília,Palmas, Macapá, Belém
  Alternative Route 2: Brasília, Campo Grande, Cuibá, Belém
  Alternative Route 3: Brasília, Belo Horizonte, Fortaleza, Belém
- *Silver:*
  Real route: Recife, Salvador, Rio de Janeiro, São Paulo
  Alternative Route 1: Recife, Fortaleza, Belo Horizonte, Rio de Janeiro, São Paulo
  Alternative Route 2: Recife, Fortaleza, Teresina, São Luís,Brasília, São Paulo
- *Bronze:*
  Real route: Porto Alegre, Campo Grande, Cuiabá, Manaus.
  Alternative Route 1: Porto Alegre, Brasília, São Luís, Belém, Macapá, Boa Vista, Manaus.

A specific context was defined for each of the service classes. The maximum blocking probability allowed is of 5%, 15%, and 25% for the gold, silver and bronze classes, respectively.

Results regarding DQMA usage in the proposed scenarios are presented below. The goal is to analyze the impact of using agents for dynamic QoS control in an OBS network.

Each of the traffic generators produces a load that varies from 0.1 to 0.5 erlangs, and in the high load scenario the information generated in the network arrives at about 2000 bursts per second ($\simeq$ 2 Gbps). Fifty simulations were run for each point, with a confidence interval of 95% regarding the average of the samples.

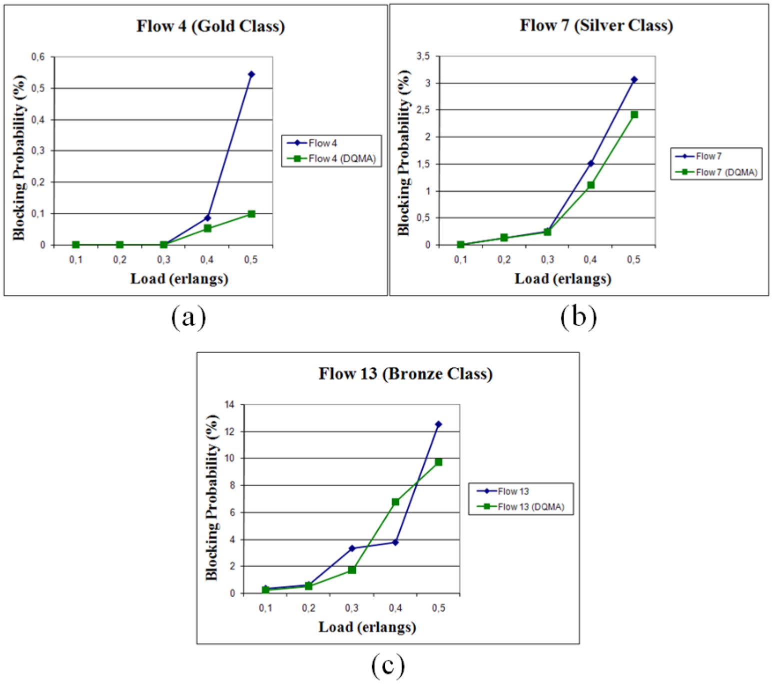

Fig. 5. Blocking probability in flow class: gold (a), silver (b) and bronze (c)

The blocking probability of each flow is calculated based on the average of the blocking probability registered in each node of the determined route. The blocking probability of each class is determined by the average of the blocking probabilities of each flow belonging to the class.

Figures 5a, 5b, and 5c show the blocking probability as a function of the load for a flow of each of the three service classes. Figures 6a, 6b, 6c, and 6d show the blocking probability for the whole class as a function of the defined traffic scenarios.

Figures 5a, 5b, and 5c show that there is a decrease of the blocking probability in the flows of all of the classes when DQMAs are used to perform dynamic QoS management. It is worth pointing out that not all of the flows will be served using explicit routing, since the number of alternative routes for each class is finite. A problem that can occur is when a given route explicitly shares links and wavelengths with other flows. In this case, the contention level can increase instead of decreasing, as can be seen in Fig. 5c for the load of 0.4 erlangs.

It can be observed from Figure 6 that there was a reduction in blocking probability for all of the classes with the use of DQMAs. It can be noticed that with an increase in the amount of traffic in each class, dynamic QoS control becomes even more necessary, so that absolute levels of performance for the bursts can be offered.

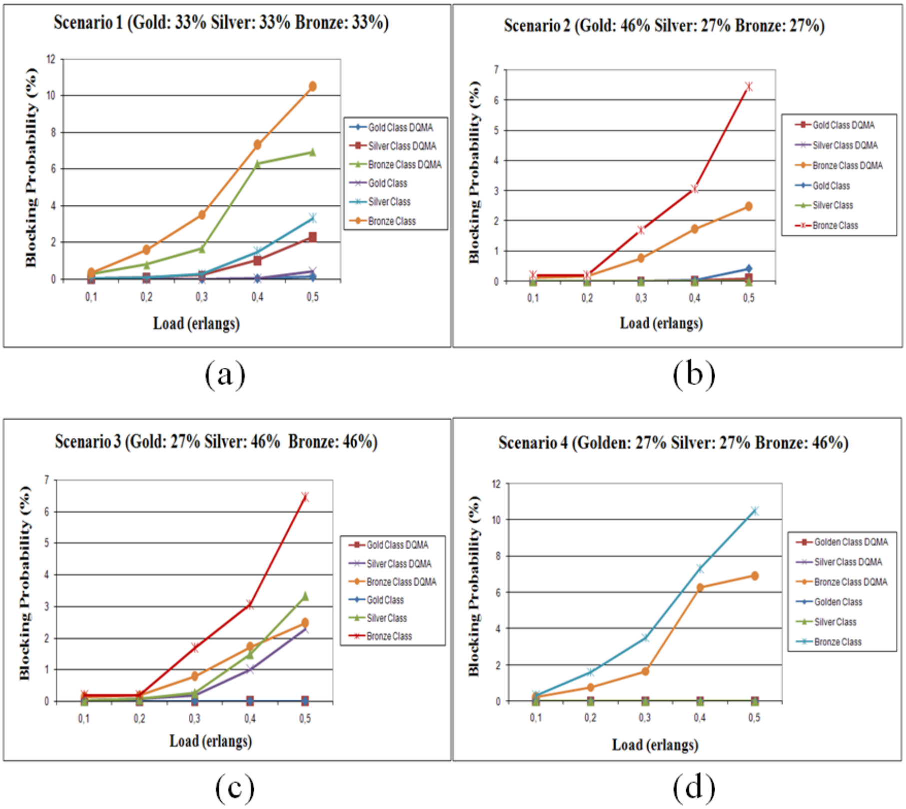

Fig. 6. Blocking probability for load class, In: Scenario 1 (a), Scenario 2 (b), Scenario 3 (c) and Scenario 4 (d)

5 Final Considerations and Future Work

This paper proposes an architecture for dynamic QoS control in OBS networks, based on traffic monitoring and automatic rerouting of bursts belonging to flows that suffer from high levels of blocking, according to the restrictions defined for each class. Thus, it is possible to define absolute levels of QoS for the applications that have strict performance requirements.

The proposal improved the performance of the service classes in a general way, besides guaranteeing the fulfillment of the given requirements. The results also show that, depending on the amount of traffic originating from each class, the demand for additional resources can really increase. For that reason, the main limiting factor of this proposal is the availability of additional network resources to meet the demands of the service classes. In case these are unavailable, there are no warranties that the proposal will provide the desired performance.

Another important aspect is related to the definition of the alternative routes that will be used. If these routes conflict with other existing ones, the level of contention experienced by the diverted bursts can be influenced by the existence of other flows.

In future studies, we intend to investigate the possibility of using a mechanism of automatic resource discovery to determine alternative routes for the bursts. In addition to performance requirements, resource discovery should also take into account the level of usage of candidate routes. Some means of admission control is also needed, as a more efficient means of avoiding disturbance of high priority flows by those of low priority. In addition, the metrics evaluated should include, besides the blocking probability, the delay and jitter relative to the thresholds defined in the QoS context, taking into account the synchronization between the agents.

References

1. Chlamtac, I., Ganz, A., Karmi, G.: Ligthpaths Communications: An Approach to High Bandwidth Optical WANs. IEEE Transactions on Communications 40(7), 1171–1182 (1992)
2. O' Mahony, M.J., et al.: The Application of Optical Packet Switching in Future Communication networks. IEEE Communications Magazine 39(3), 128–135 (2001)
3. Jue, J.P., Vokkaranne, V.M.: Optical Burst Switched Networks. Optical Networks Series, pp. 1–3. Springer, Heidelberg (2005)
4. Mannie, E.: Generalized Multi-Protocol Label Switching (GMPLS) Architecture, RFC 3945 (October 2004)
5. Lazzez, A., El Fatmi, S.G., Boudriga, N., Obiadat, M.S.A.: Dynamic QoS-based Scheme for Admission Control in OBS Network. In: IEEE Communication Society, ICC 2007, vol. 1, pp. 449–454 (2007)
6. Long, K., Tucker, R., Wang, C.: A New Framework and Burst Assembly for IP Diffserv over Optical Burst Switching Networks. In: IEEE Global Telecommunications Conference, GLOBECOM 2003, vol. 22(1), pp. 3159–3164 (2003)
7. Zhang, Q., Vokkarane, V.M., Jue, J.P., Chen, B.: Absolute QoS Differentiation in Optical Burst-Switched Networks. IEEE Journal on Selected Areas in Communications 22, 2062–2071 (2004)
8. VINT Project (2007, jul 07), The Virtual InterNetwork Testbed, `http://www.isi.edu/nsnam/vint/index.html`
9. RNP (2007, jul 07). Rede Nacional de Ensino e Pesquisa, `http://www.rnp.br/backbone`
10. Zhang, F., Macnicol, J., Pickering, M.R., Frater, M.R., Arnold, J.F.: Efficient Streaming Packet Video Over Differentiated Services Networks. IEEE Transactions on Multimedia 8(5), 1005–1010 (2006)