Admission Control Policies in Flow-Aware Networks

Jerzy Domżał[1], Robert Wójcik[1], Andrzej Jajszczyk[3]
AGH University of Science and Technology, al. Mickiewicza 30, 30-059 Krakow, Poland
Tel: (4812) 6173937, Fax: (4812) 6342372, e-mail: {jdomzal, robert.wojcik, jajszczyk}@kt.agh.edu.pl
Víctor López[1], José Alberto Hernández, Javier Aracil[2]
Universidad Autónoma de Madrid, Calle Francisco Tomas y Valiente, 11 - Madrid, Spain
Tel: +34914972268, Fax: +34914972235, e-mail: {victor.lopez, jose.hernandez, javier.aracil}@uam.es
[1]Student Member, IEEE, [2]Senior Member, IEEE, [3]Fellow, IEEE

ABSTRACT
In this paper, the admission control policies proposed for Cross-Protect routers in Flow-Aware Networks (FAN) are compared. A Multilayer FAN (MFAN) architecture defines policies to decide which flows are more suitable to be transmitted through the optical layer in case of congestion. In this work, we evaluate how to include the information of such policies in the admission control process. As a result of the analysis, a new admission control strategy is proposed. This solution inherits the advantages from already established admission control proposals while ensuring fast acceptance times of new streaming flows.
Keywords: Flow-Aware Networks, admission control, congestion control, quality of service, traffic engineering.

1. INTRODUCTION

Flow-Aware Networking (FAN) is a novel approach to assure QoS in current IP networks [1]. Up to now, admission control policies [2][3] as well as multi-layer interoperability methods [4] have been proposed for FAN. Multi-layer FAN proposes a new flow classification algorithm to detect which flows are sent using the optical layer, when the IP layer cannot accept any more incoming flows. In this paper, we analyze and compare the proposed admission control policies for the Cross-Protect routers under the ordinary FAN architecture and we include the policies defined in MFAN into the admission control mechanisms proposed in the literature.

The remainder of the article is organized as follows. Section 2 provides the background for the FAN architecture, it presents MFAN solution and the admission control strategies proposed for FAN, which are, consequently analyzed, evaluated and compared in Section 3. Finally, Section 4 concludes the paper.

2. FLOW-AWARE NETWORKING

FAN seeks two main objectives: to minimize the delay and losses of streaming flows and to assure some minimum bandwidth to the elastic flows. FAN implicitly classifies the incoming flows as elastic or streaming flows, thus, it does not require any packet marking. A flow, whose rate is under the minimum bandwidth assured, is considered as a streaming flow. On the other hand, the flows which are transmitting at a higher bit rate than this minimum bandwidth are considered as elastic flows.

To assure a minimum rate to the flows, it is mandatory to add an admission control mechanism in order to avoid congestion. The tag of each flow that is accepted by the router is stored in the Protected Flow List (PFL). When a packet arrives, FAN checks if this packet belongs to one of the flows already signed on the PFL. If the flow is found, the packet is served. Otherwise, the flow is new and the admission control mechanism checks if the Priority Load (PL) is lower than Th_{PL} and if the Fair Rate (FR) is greater than Th_{FR}. PL computes the load at the FAN queue due to the streaming flows and FR is an estimation of the available bandwidth. If the load of the streaming flows is small ($PL < Th_{PL}$) and there is enough available bandwidth ($FR > Th_{PL}$), FAN can accept the new incoming flow. Otherwise, the temporal congestion is observed and the packet is dropped.

Finally, in order to give priority to the streaming flows, rather than the elastic flows, FAN has defined two queuing algorithms: Priority Fair Queuing (PFQ) [5] and Priority Deficit Round Robin (PDRR) [6]. The behaviour of both algorithms is similar, but they have differences in the algorithm complexity [6]. In this work, the PFQ algorithm is used. PFQ has a PIFO queue with a priority and a non-priority area. The packets of the streaming flows are located at the priority area of the queue, while the elastic flows use the non-priority area. Thanks to this queuing algorithm, FAN gives priority to the streaming flows.

2.1 Multilayer FAN

Flow-Aware Networking (FAN) is defined to provide QoS at the IP layer, but it was not defined to operate over Intelligent Optical Networks (ION). This is the reason why Multi-layer Flow-Aware Networking (MFAN) is defined to extend FAN to IP over WDM architectures [4]. MFAN assumes that the QoS at the IP layer is provided solely by FAN. However, when the FAN queue is congested, MFAN can use the additional resources of the underlying optical layer. An MFAN node is defined as a router which is able to transmit the traffic at the IP layer using FAN, but it can also send traffic using these optical resources.

978-1-4244-4826-5/09/$25.00 ©2009 IEEE

MFAN defines three policies to select which flows are the most suitable ones to be transmitted using the optical layer. The first policy is called the “Newest-flow” policy. Once a packet is rejected at the FAN system in the IP layer, MFAN tests if the optical resources can accept more traffic demands and, if so, it transmits the new packet using the optical queue. To check if there are resources at the optical queue MFAN checks if the queue occupation level is over a threshold called *OTh*. This policy does not use any information about the flows from the original IP-layer FAN. On the other hand, the “Most-active-flow” policy selects the flow that is transmitting at the highest bit rate and it is switched over the optical queue, while the new flow is accepted at the primary FAN queue. The “Oldest-flow” policy works similarly to “Most-active-flow” policy, but the flow which has been active for a longer period of time is selected for optical switching.

2.2 Admission control policies for FAN

There are three congestion control mechanisms proposed for FAN [2][3]: Enhanced Flushing Mechanism (EFM), Remove Active Elastic Flows (RAEF) and Remove and Block Active Elastic Flows (RBAEF). These mechanisms work based on total or partial cleaning of the PFL content when the congestion state is observed. It removes congestion in a link for a short period of time and gives the possibility for new flows to be accepted in a router.

The EFM algorithm identifies all elastic flows to be removed from the PFL, when there is congestion. An example of the operation of EFM algorithm is shown in *Figure 1*. EFM has a parameter denoted *pfl_flushing_timer* that defines the minimum period between two PFL flushing actions. This parameter allows detecting if the congestion has been reduced, thanks to the flushing process.

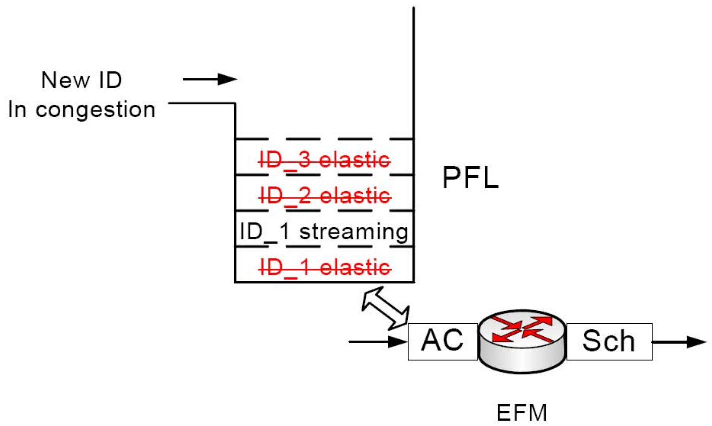


Figure 1. The operation principle of EFM.

For instance, the dialling time for international calls should not be greater than 11 seconds for the 95% of the calls, while for local calls this should not exceed 6 seconds [7]. In light of the previous results [2][3], these mechanisms ensure fast acceptance times of new streaming flows.

The congestion control mechanisms have one important drawback. The number of accepted flows in the PFL right after a flushing procedure can be too high. However, the number of elastic flows, whose identifiers (IDs) are removed from the PFL during the flushing action may be reduced by using the MFAN-based policies as we will see in the next section.

3. SIMULATION ANALYSIS

The scenario to carry out the simulations is a simple network with one source node, one FAN link and one destination node simulated using ns-2. In such a topology, it is possible to observe the acceptance times of new flows and the number of elastic flows accepted in a link. The arrival process distribution for the elastic and streaming flows is exponential. We decided to provide the traffic pattern with Pareto distribution for calculating the volume of traffic to be sent by each of 200 elastic flows in the FAN link with capacity equal to 100 Mbps. This rate overloads the FAN’s queue, thus triggering the admission control mechanisms. The duration of each simulation run is set to 250 s. The fair rate threshold (Th_{FR}) is set to 5% and Th_{PL} equals to 70%.

Firstly, we simulate the performance of the system when EFM mechanism is used at the FAN queue (*Table 1*). In this case, the streaming flows are accepted very quickly (1.43 s), but the number of elastic flows accepted after a flushing is too high. As a lot of elastic flows are accepted in a short period, the fair rate computation is not stable. Consequently, this high amount of elastic flows competes for the bandwidth and the minimum bandwidth (Th_{FR}) cannot be assured.

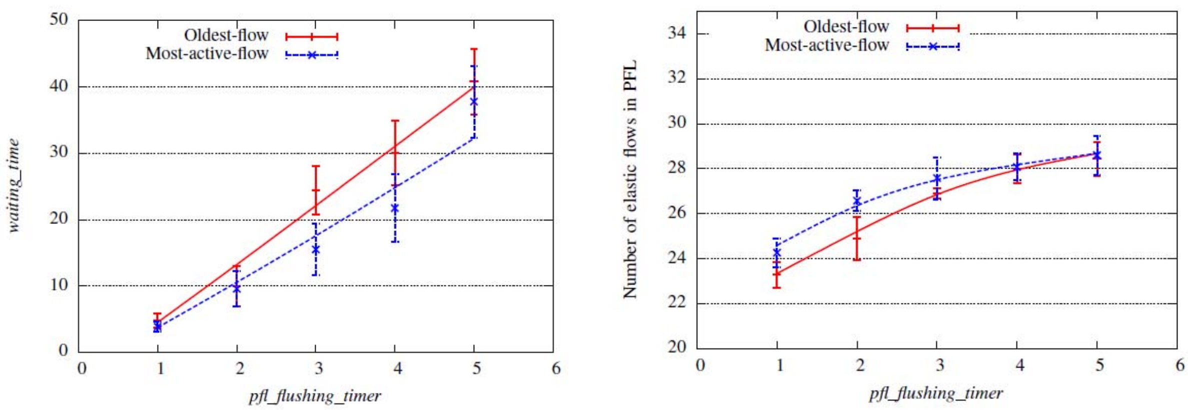
The second and third rows of *Table 1* present the results of a new solution. Instead of removing all elastic flows from the PFL during the flushing (like it was in the EFM, see *Figure 1*), the oldest flow is removed from the PFL in congestion. The *pfl_flushing_timer* is set to 1 s, which means that the minimum time period between two consecutive flushing actions was 1 s. The second solution (third row of *Table 1*) deletes the identifier of the Most-active flow from the PFL. The results show very good properties of both solutions. However, there is a problem when using the described algorithms. The removed flow is not accepted again in the PFL in a short time which may increase the mean transmission time of elastic flows.

We propose to use the EFMP (EFM with Priority) to ensure quick acceptance of removed flows from the PFL while ensuring all advantages of the mechanism described previously. In this solution, the identifier of the removed flow is written into a Priority Access Flow List (PAFL) for a short period of time (in our analysis it is set to 1 s). If there is any identifier in the PAFL, the flows whose IDs are not in the PAFL are accepted with small probability (experimentally calculated as 0.03). On the other hand, the flows whose IDs are in the PAFL are accepted without limitations. The results in the last two rows of *Table 1* show that EFMP solution gives acceptable values of all analyzed aspects in both admission control policies. It ensures fast acceptance of new streaming flows, good transmission properties of elastic flows and it is scalable.

Table 1. The properties of admission control policies.

Architecture or mechanism	***waiting time* [s]**	**No. of admitted flows**	**Advantages**	**Drawbacks**
EFM (5s)	1.43±0.91	160.43±10.91	• quick acceptance of streaming flows • low cost	• instability of fair rate • high number of accepted flows
EFM (1s, oldest flow)	3.55±0.53	23.55±0.62	• quick acceptance of streaming flows • low cost • fair rate assurance • low number of accepted flows	• removed flow may not be accepted again
EFM (1s, most active flow)	3.68±0.45	23.13±0.45		
EFMP (1s, oldest flow)	4.73±1.06	23.48±0.56	• quick acceptance of streaming flows • low cost • fair rate assurance • low number of accepted flows • quick acceptance of removed flows	• none
EFMP (1s, most active flow)	**3.86±0.80**	**24.26±0.64**		

Fig. 2 shows the mean waiting time and the number of admitted flows after a flushing procedure with respect to the *pfl_flushing_timer* parameter. The 95% confidence intervals are calculated using the Student's t-distribution. Satisfactory results can be obtained when the parameter is set to 1 s (mean waiting time less than 6 s). If the parameter value is decreased, the waiting time can be reduced even more, but it is not required and it increases the computational power required for the router.



(a) Waiting time. *(b) Number of elastic flows in the PFL.*

Figure 2. Acceptance times of streaming flows and the number of accepted elastic flows in FAN with EFMP.

4. CONCLUSIONS

There are numerous admission control policy proposals for the FAN routers. This paper surveys and assesses them with regards to the mean waiting time for streaming flows that is achieved by each, and to the number of flows that are admitted on a link after the accepting procedure for the streaming flows occurs. The outcome shows that the EFMP method produces short waiting times (less than 5 s) while being scalable and allowing a fast acceptance of the removed flows from the PFL.

As future work we will evaluate the performance of admission control mechanisms not only in single-layer scenarios, but also in multi-layer architectures. In this situation, we will study how it is possible to coordinate the mechanisms proposed in the MFAN solution and the admission control mechanisms.

ACKNOWLEDGEMENTS

The work described in this paper was carried out with the support of the BONE-project ("Building the Future Optical Network in Europe"), a Network of Excellence funded by the European Commission through the 7th ICT-Framework Programme.

REFERENCES

[1] J. Roberts, S. Oueslati: Quality of service by flow aware networking, in *Philosophical transactions of the Royal Society,* vol. 358, no. 1773, pp. 2197-2207, 2000.

[2] J. Domzal, A. Jajszczyk.: New congestion control mechanisms for flow-aware networks, in *Proc. ICC 2008*, Beijing, China, May 2008.

[3] J. Domzal, A. Jajszczyk.: The flushing mechanism for MBAC in flow-aware networks, in *Proc. NGI 2008*, Krakow, Poland, April 2008.

[4] V. Lopez, C. Cardenas, J. A. Hernandez, J. Aracil, M. Gagnaire: Extension of the flow-aware networking (FAN) architecture to the IP over WDM environment, in *Telecommunication Networking Workshop on QoS in Multiservice IP Networks, 2008. IT-NEWS 2008. 4th International*, Venice,, Feb. 2008, pp. 101-106.

[5] A. Kortebi, S. Oueslati, J. Roberts: Cross-protect: implicit service differentiation and admission control, in *IEEE HPSR 2004*, Phoenix, USA, April 2004.

[6] A. Kortebi, S. Oueslati, J. Roberts: Implicit service differentiation using deficit round-robin," in *ITC19*, Beijing, China, August/September 2005.

[7] ITU-T Recommendation E.721. Network grade of service parameters and target values for circuit-switched services in the evolving ISDN, May 1999.

ICTON 2009

11th International Conference on Transparent Optical Networks

Home Page ICTON 2009 Agenda ICTON 2009 Committees Venue Conference and Hotel Registration Author Index

June 28 – July 2, 2009

Island of São Miguel, Azores, Portugal, http://www.itl.waw.pl/icton

8th European Symposium on Photonic Crystals, ESPC*

8th Workshop on All-Optical Routing, WAOR

6th Global Optical & Wireless Networking Seminar, GOWN

5th Reliability Issues in Next Generation Optical Networks Workshop, RONEXT

5th Photonic Integrated Components & Applications Workshop, PICAW*

4th Nanophotonics for All-Optical Networking Workshop, NAON*

4th Special Session on Microresonators and Photonic Molecules: trapping, harnessing and releasing light, MPM*

4th Special Industrial Session

3rd Special Session on Novel glasses for photonic devices*

2nd Special Session on Market in Telecommunications, MARS

Euro-FOS NoE and SARDANA project Worshops

** denotes section of 1st Annual Conference of COST Action MP0702: Towards Functional Sub-Wavelength Photonic Structures*

IEEE Catalog Number: CFP09485-CDR

ISBN: 978-1-4244-4826-5

Library of Congress: 2009905508

Formal publisher: National Institute of Telecommunications, Department of Transmission and Optical Technologies, 1 Szachowa Street, Warsaw, Poland.

This publication is supported by COST.

Editors: Marek Jaworski, Marian Marciniak

Insti

Plati

Gold

Silve

Bron

Endo