TRANSACTIONS ON EMERGING TELECOMMUNICATIONS TECHNOLOGIES
Trans. Emerging Tel. Tech. 2014; **25**:1137–1148
Published online 28 June 2013 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/ett.10.1002/ett.2671

RESEARCH ARTICLE

EFMP – a new congestion control mechanism for flow-aware networks

Jerzy Domżał[1]*, Robert Wójcik[1], Victor López[2], Javier Aracil[2] and Andrzej Jajszczyk[1]

[1] AGH University of Science and Technology, Department of Telecommunications, Al. Mickiewicza 30, 30-059 Krakow, Poland
[2] Universidad Autónoma de Madrid, Dept. Ingeniería Informática, Calle Francisco Tomás y Valiente, 11 - Madrid, Spain

ABSTRACT

In this paper, a new congestion control mechanism for flow-aware networks, that is, enhanced flushing mechanism with priority (EFMP) is introduced. Proposed by J. Roberts and S. Oueslati in 2004, flow-aware networking is a concept that ensures quality of service in networks based on flows. EFMP improves the efficiency of transmission in FAN by introducing new policies in the admission control block of a cross-protect router. The mechanism is thoroughly described, analysed, and validated through simulations. The proposed mechanism inherits the advantages of previously known admission control schemes while ensuring fast acceptance times of new streaming flows and proper transmission of the remaining traffic. Moreover, the comparison with the multilayer flow-aware networks architecture shows that EFMP ensures better performance and lower cost of transmission in a network with limited resources. Copyright © 2013 John Wiley & Sons, Ltd.

KEY WORDS

flow-aware networks; FAN; admission control; congestion control; quality of service; traffic engineering

***Correspondence**

Jerzy Domżał, AGH University of Science and Technology, Department of Telecommunications, Al. Mickiewicza 30, 30-059 Krakow, Poland.

E-mail: jdomzal@kt.agh.edu.pl

Received 15 February 2013; Revised 24 April 2013; Accepted 3 May 2013

1. INTRODUCTION

Since the early days of the Internet over two decades ago, traffic carried in the global networks has been increasing constantly. Lawrence Roberts, one of the originators of the Internet, noted that the volume of Internet traffic doubled every year until 2008, and he anticipates it will continue to grow annually [1]. Similar observations are presented in [2] by K. G. Coffman and A. M. Odlyzko. Other analyses, originating from studies conducted by Minnesota Internet Traffic Studies [3], Cisco, Swanson, and Gilder [4], predict that such traffic will grow by approximately 40–60 per cent per year. On this basis, it is unlikely that this trend will change in the coming years. Since 1994, when IntServ appeared, many quality of service architectures have emerged, with the concept of flow-aware networking [5] among the most promising. It eliminates the need of signalling that has proved unscalable. Despite its simple approach to quality of service assurance, the service differentiation in FAN works sufficiently well. However, the architecture is not flawless. Some disadvantages are mitigated by several additional mechanisms proposed with the development of FAN: the limitation mechanism [6], support for emergency calls [7], congestion control mechanisms [8], [9], and the multilayered architecture [10].

There are various proposals that improve data transmission in FAN when congestion occurs. Firstly, the mentioned congestion control mechanisms are based on partial or total cleaning of the protected flow list (PFL) in the FAN routers. Secondly, there is multilayer FAN (MFAN) that supports the internet protocol (IP) level FAN with lower layers. Although these proposals are valid and bring certain improvements, this paper presents a new mechanism called enhanced flushing mechanism with priority (EFMP). It combines the enhanced flushing mechanism (EFM) congestion control mechanism with admission control policies proposed for MFAN. The EFMP allows for fast acceptance of streaming flows and improves transmission performance in MFAN. Implementing EFMP may result in network resources being used more effectively. As a result, it is possible to accept and serve more streaming flows, minimising operational costs. The new solution is presented in detail and compared with EFM and MFAN in terms of performance and cost. Finally, an analysis of which

congestion control mechanism is suitable for a particular case is provided.

The rest of the paper is organised as follows. Section 2 introduces the concept of flow-aware networking. Section 3 presents the congestion control mechanisms for FAN and MFAN networks. The concept and the pseudo-code for realising the EFMP functionality are shown in Section 4. Section 5 contains extensive simulation results showing the performance of selected congestion control mechanisms designed for FAN. Finally, Section 6 concludes the paper.

2. FLOW-AWARE NETWORKS

The concept of FAN as an approach to ensure quality of service (QoS) in packet networks was originally introduced in [11], and presented as a complete system in 2004 [5]. Additionally, in [12], it was shown that despite being a QoS architecture, FAN fits into the network neutrality restrictions perfectly. The goal of FAN is to enhance the current IP network by improving its performance under heavy congestion. In FAN, traffic is sent as flows with a guaranteed quality. Although basic FAN is an IP level architecture, it can also work with the physical layer of optical networks. Several researchers, including Lawrence Roberts and James Roberts, believe that in the Future Internet, traffic will be served and managed as flows [13, 14]. Currently, many concepts that assume flow-aware transmission are analysed and deployed.

A survey of established QoS flow-aware architectures, including FAN, is presented in [15]. The authors also propose a new solution. The QoS management architecture, flow-aggregate-based services, has two new blocks: inter-domain flow aggregation and endpoint implicit admission control. The option of aggregating flows across the network domain in this proposal is provided by the inter-domain flow aggregation mechanism. The endpoint implicit admission control scheme eliminates inefficiency resulting from discarding packets in the middle of the path of a flow by congestion notification to the edge nodes.

The authors of [16] present an overview of FAN and propose a new method for classifying flows in the admission control block. It performs traffic control on the flow level and improves traffic performance in overload situations. Simulation analysis in the ns-2 environment shows that the proposed solution works efficiently.

The paper [17] reviews the QoS control architectures defined by standardisation bodies such as cable-lab, DSL forum, multiservice switching forum), European Telecommunications Standards Institute and International Telecommunication Union Telecommunication Standard Sector. The flow-aware networking concept is presented as an example of flow level control architectures. Another flow-aware technology referred to as flow state aware, described in [18], divides Internet services into several types according to the associated requirements and control procedures.

Flow-aware concept is promising when considering multi-path transmission in a network. The authors of [19] propose a new model for multi-path allocation based on traffic sent by flows in DiffServ enabled MPLS networks.

The flow-aware concept in IP networks is well recognised. However, there are still many problems that need to be solved. Some have been analysed in literature, including fairness [20], reliability [9, 21] and performance in a wireless environment [22]. However, they and many other issues require further research. This paper focuses on FAN as an example of flow-aware architectures. In our opinion, it is the most promising solution.

To provide service differentiation and QoS assurance to IP networks, certain traffic management mechanisms controlling link sharing are proposed in FAN, including measurement-based admission control [14] and fair scheduling with priorities [5], [23]. The former keeps flow transmission rates high in case of overload to ensure that at least a basic level of service is provided. The latter maintains fair link bandwidth sharing while ensuring negligible packet latency for flows emitting at lower rates.

Figure 1 is a schematic illustration of the operation of FAN. All incoming packets are first classified into flows. The flow identification process is implicit and its goal is to create an instance on which service differentiation can be performed. To begin with, the packet header is analysed to find the flow ID (FID), which is determined on the basis of incoming and outgoing interfaces, port numbers, and the name of the transport protocol. All the flows that are currently in progress, that is, their FIDs have been written to the PFL, are allowed to be served on the link, whereas all new flows are subject to admission control. The admission control in FAN is measurement based admission control (MBAC), which means that the accept/reject decisions are based on the current link congestion status only. If a new flow is accepted, its FID is put onto the PFL list, and all the following packets of this flow are forwarded without checking the status of the outgoing link by MBAC.

The main goal of FAN is to improve the perceivability of current IP networks by using a new type of router – the cross-protect router (XP router). This device is responsible for providing admission control and fair queuing. FAN adds the admission control and scheduling blocks to the standard IP router. The former is placed in the incoming line cards of the router, whereas the latter is situated in the

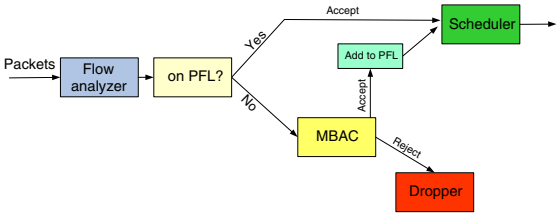

Figure 1. Packet service in flow-aware networks. MBAC, measurement based admission control; PFL, protected flow list.

Trans. Emerging Tel. Tech. **25**:1137–1148 (2014)
DOI: 10.1002/ett

outgoing line cards. Admission control is responsible for accepting or rejecting the incoming packets, based on the current congestion status of the destination outgoing link. The purpose of scheduling is twofold: it provides prioritised forwarding of streaming flows and ensures a fair share of the residual bandwidth by all remaining flows.

Three well-known scheduling algorithms have been proposed for FAN so far: priority fair queuing (PFQ) [5], priority deficit round robin [23] and approximate flow-aware networking) [24].

Naming FAN devices as cross-protect routers results from the mutual cooperation and protection that exist between both the introduced blocks. The admission control block limits the number of active flows in a router, which improves the functionality of the queuing algorithm and reduces its required performance. It is important that queuing mechanisms operate quickly. Conversely, the scheduling block provides admission control including information on the congestion status on the outgoing interfaces. The information is obtained based on the current occupancy of the queues. The cross-protection contributes to a smaller protected flow list and active flow list sizes, which significantly improves FAN's scalability.

To provide congestion information, each XP router constantly monitors two link indicators: fair rate (*FR*) and priority load (*PL*). The fair rate is the rate available to each flow at a given moment. The priority load represents the sum of the lengths of priority packets transmitted in a certain time interval, divided by the duration of that interval, and normalised with respect to the link capacity. A more detailed definitions of *FR* and *PL* can be found in [5].

Congestion is observed if the current value of the *FR* is lower than the minimum acceptable value of this parameter (Th_{FR}), or the current value of the *PL* is greater than the maximum accepted value of this parameter (Th_{PL}). Although the link is considered to be congested, new flows are not accepted. Unfortunately, such a situation can endure for a long time. This is extremely important for the streaming flows, which in most cases should begin to send their packets immediately. There are a few solutions to mitigate the problem. This paper describes congestion control mechanisms proposed for both FAN and MFAN architectures.

3. CONGESTION CONTROL IN FLOW-AWARE NETWORKS

There are four congestion control mechanisms proposed for FAN so far. The principles of enhanced flushing mechanism (EFM) [8], remove active elastic flows, remove and block active elastic flows [25], [26], [27], and remove and prioritize in access active elastic flows [9] mechanisms are based on total or partial cleaning of the PFL content when the congestion state is observed. It eliminates congestion in a link for a short time and gives the possibility for new flows to be accepted in a router. The packet service controlled by EFM is presented in Figure 2. In the congestionless state, all packets are accepted in the MBAC block. In

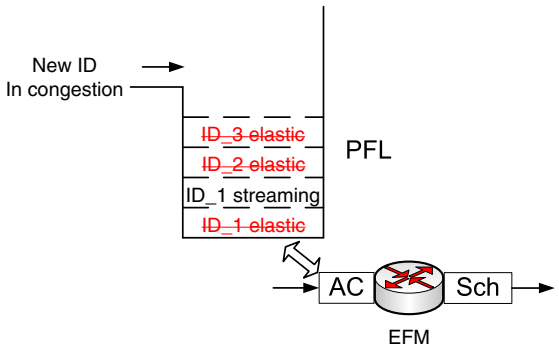

Figure 2. Packet service in flow-aware networks controlled by enhanced flushing mechanism (EFM).

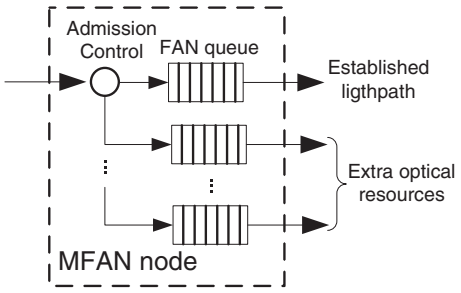

Figure 3. Multilayer flow-aware networking (MFAN) node architecture.

the congestion state we remove the identifiers of all elastic flows from the PFL. As a result, for a short period of time, congestion is eliminated and new flows may be accepted. PFL can be flushed at most once every *pfl_flushing_timer* seconds, as flushing too frequently may result in an unstable transmission in a FAN link. As the EFM is the simplest congestion control mechanism proposed for FAN so far, we consider and develop this mechanism in this paper. In Section 5, we present the results of simulation analysis of the EFM.

The other option for dealing with congestions in FAN is to use the MFAN concept, which assumes the use of additional resources at the optical layer for traffic that cannot be accepted in FAN links at the IP layer.

MFAN is an evolutionary solution enhancing FAN performance in multilayer environments. It assumes that the QoS provided by FAN at the IP layer is good enough for the network performance. However, if the IP layer FAN queue is congested, MFAN can use the underlying optical layer where an optical lightpath is set up. Therefore, an MFAN node is a router which is able to transmit traffic at the IP layer using FAN, as well as sending traffic using optical resources as illustrated in Figure 3.

As explained in Section 2, FAN can reject new flows when the link performance decreases. MFAN nodes know whether the optical network has free resources. Consequently, they can ask for extra optical connections to accept

the flows that have been rejected by the IP-layer in FAN. Once the new optical connection is set up, the flows transmitted through it are stored in the PFLλ list. The PFLλ list has exactly the same functionality as the standard PFL list for IP-layer FAN routers. Therefore, each MFAN node maintains more than one PFL list. Several lambdas may be used at the optical layer to transmit redirected traffic. When we have more than one lambda, the proper multiwavelength optical buffer scheduling discipline has to be implemented to ensure fair transmission of queued packets [28].

MFAN defines three policies to select which flows are the most suitable for transmission by using the optical layer [10]. The first policy is the 'newest-flow' policy. Once a packet is rejected at the FAN system in the IP layer, MFAN tests whether the optical resources can accept more traffic and, if so, the new packet is transmitted through the optical layer. To determine whether there are resources at the optical layer, MFAN checks if the queue occupation is lower or greater than the threshold known as *OQTh*. The second policy is the 'most-active-flow' policy. It selects the flow that is transmitting at the highest bit rate at a given moment; this flow is redirected to the optical layer, whereas the new flow is accepted at the primary FAN queue. The third approach, the 'oldest-flow' policy, works similarly to the most-active-flow policy; however, the flow which has been active the longest is selected for redirecting. Figure 4 summarises the complete admission control in MFAN nodes, including the policies.

The concept of MFAN is similar to the idea of optimised routing mechanism where traffic form overloaded links is redirected to uncongested ones. Such mechanism for FAN was proposed in [29]. The results presented in this paper and also in [30], where several similar proposals were analysed for meshed topologies, show that a network with optimised routing algorithm can carry up to two or even three times more traffic than a network with fixed paths.

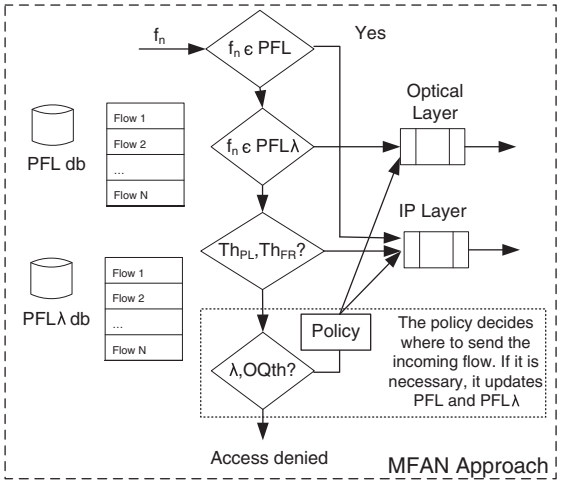

Figure 4. Packet service in multilayer flow-aware networks.

4. ENHANCED FLUSHING MECHANISM WITH PRIORITY

This section presents a new congestion control mechanism known as EFMP (EFM with priority). It is a combination of the EFM with admission control policies proposed for MFAN and the priority access flow list (PAFL). The packet service in EFMP with the oldest-flow policy is presented in Figure 5.

The pseudocode for realising the EFMP functionality with the oldest-flow policy is presented in Table I.

When a packet of a new flow arrives at the admission control block in congestion, it starts the EFMP procedure. The *For* loop is executed for each flow from the PFL (line 7). It is necessary to find the flow's active time (line 9) and check whether it is elastic (line 10). The procedure to find the oldest flow (lines 11–17) is run next. The FID of the oldest flow is removed from the PFL (line 19) and added to the PAFL (line 20). Moreover, the parameter *PAFL_occup* is set to 1, which means that the PAFL is not empty (line 21). The procedure is repeated until the outgoing link is not congested (lines 2 and 24).

If there are any identifiers in the PAFL in a congestion-less state (*PAFL_occup=1*), the flows whose FIDs are not in the PAFL are accepted with a small P_{EFMP} probability (experimentally calculated as 0.03) (line 40). On the other hand, the flows that FIDs are in the PAFL are accepted without limitations, with the highest possible priority (lines 38 and 39). If the PAFL is empty, the packets of flows whose FIDs are in the PFL are always accepted, and the other packets are served if there is no congestion in the outgoing link (line 42).

The PAFL content is cleaned in a congestion-less state after the time given by the *priority_access* parameter (in our analysis, this value was set to 1 s – twice the *FR* measurement interval) since the last cleaning action on the PFL (lines 27–35). On the basis of our observations, it can be assumed that the value of twice the *FR* measurement interval guarantees that the majority of streaming flows are accepted by the admission control block. On the other hand, during this period almost no new elastic flows are accepted.

The implementation of the EFMP in the cross-protect router is more complex than the EFM. In EFM, we have to find all elastic flows (one loop) and remove their identifiers from PFL. In EFMP, we have to find the oldest or the most active flow (one loop), remove its ID from PFL and write it to PAFL. Such operations are repeated until the link becomes uncongested. This increases complexity because loops may be executed many times. Moreover, we have to check if *priority_access* time ends and according to this make acceptance decisions in congestion-less state in different ways. We can see that the cross-protect router with EFMP has to execute more operations in comparison with EFM; however, it should not be a problem for currently used devices, which usually have enough memory and efficient processors.

Trans. Emerging Tel. Tech. **25**:1137–1148 (2014)
DOI: 10.1002/ett

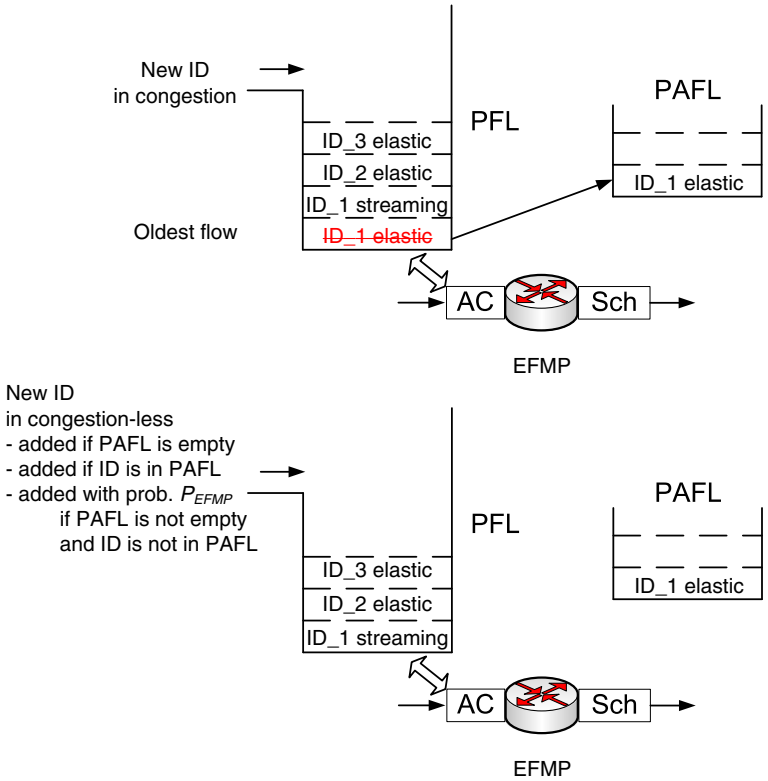

Figure 5. Packet service in flow-aware networks with enhanced flushing mechanism with priority with the 'oldest-flow' policy.

5. SIMULATION ANALYSIS

5.1. Enhanced flushing mechanism

This section presents the results of carefully selected simulation experiments on the EFM. The simulations were performed in the ns-2 simulator [31] and provided for a single FAN link with many source and destination nodes (the examined topology is presented in Figure 6). The simulated topology is very simple while being sufficient for analysing the mechanisms in FAN networks. The reason is that all the nodes in FAN operate independently and all the decisions are taken without any information from the network. Therefore, the topology is sufficient for demonstrating the operation of the analysed congestion control mechanism.

The nodes S_{E1}–S_{En} are the sources of elastic traffic, whereas the nodes S_{S1}–S_{Sm} are the sources of streaming traffic. The nodes D_{E1}–D_{En} and D_{S1}–D_{Sm} represent the destination nodes of elastic and streaming traffic, respectively.

Over 400 simulation runs were made under various conditions to show the acceptance times of new streaming flows (*waiting_time*) in the AC block in a FAN link. The duration of each simulation run was set to 250 s, which made it possible to observe flow acceptance time. The number of sources generating background elastic flows ranged between 200 and 600. The volume of elastic traffic was modelled with the Pareto distribution (shape factor = 1.5, mean size = 150 Mbit). The packet size for elastic flows was set to 1000 bytes and the interarrival times of flows were modelled with the exponential distribution (mean interarrival time: 0.1 s). As a result, the observed link was congested almost from the beginning of the simulation experiment. The exponential distribution was also used to generate the time intervals between the starting points of the streaming flows (mean interarrival time was set to 1 s). Twenty streaming flows were sent by the source nodes. We analysed the VoIP connections running the Skype service. The packet size was set to 100 bytes and the transmission rate was set to 80 kbit/s for each streaming flow. The elastic traffic was treated as the background traffic and used to saturate the analysed FAN link. It was assumed that the capacity of link between routers was set to 100 Mbit/s and the PFQ algorithm was implemented. The capacity of access links (with FIFO queues) was set to 1 Gbit/s. The buffer in router R1 wa sized at 1000 packets, which is a reasonable value for FAN link, and the *MTU* was set at 1500 bytes. The measurement interval for the *PL* parameter was set as 50 ms, whereas the *FR* values were estimated every 500 ms. Th_{PL} was set at 70%, and Th_{FR} was set at 5%. The flow time out parameter was set at 20 s, which is the time after which an FID of an inactive flow is removed from the PFL.

Table I. Pseudocode for realising the enhanced flushing mechanism with priority (EFMP) functionality in FAN.

```
1.  on a new flow packet arrival in congestion state
2.   While link is congested do
3.   begin
4.     current_time = Scheduler :: instance().clock()
5.     If current_time − last_EFMP_action > priority_access then
6.     begin
7.        For (i = 1; i ≤ pfl_size; i++) do
8.         begin
9.              active_time(i) = current_time − first_operation_time(i)
10.             If flow_bytes(i) ≥ MTU then
11.            begin
12.                If oldest_flow_time < active_time(i) then
13.                begin
14.                  oldest_flow_time = active_time(i)
15.                  oldest_flow_id = i
16.               end
17.            end
18.        end
19.        remove FID(oldest_flow_id) from PFL
20.        add FID(oldest_flow_id) to PAFL
21.        PAFL_occup = 1
22.        last_EFMP_action = Scheduler :: instance().clock()
23.    end
24.  end
*****************************************************************
25.   ******************admission decision*********************
26.   on arriving packet p of flow i in congestion-less state after EFMP run
27.      current_time = Scheduler :: instance().clock()
28.      If current_time − last_EFMP_action > priority_access then
29.      begin
30.          If PAFL_occup = 1 then
31.          begin
32.              clean PAFL content
33.              PAFL_occup = 0
34.          end
35.      end
36.      If PAFL is not empty then
37.      begin
38.          If i is in PAFL then
39.              proceed with packet p
40.          Else proceed with p with acceptance probability P_EFMP
41.      end
42.      Else proceed with p
43.   *************************end*****************************
*****************************************************************
```

Each simulation experiment was repeated at least 10 times. 95% confidence intervals were calculated by using the student's t-distribution. We assumed that the safe warm-up time in the simulation experiments was 20 s. In most cases, the link became congested after 3–4 s. Having a sufficiently long warm-up time ensured that the results of each simulation run were always analysed in a steady-state.

The values of simulation parameters are summarised in Table II.

The mean values of *waiting_time* as a function of the number of elastic flows active in the background for the FAN with PFQ are presented in Figure 7.

Four values of the *pfl_flushing_timer* parameter were examined. The results show that regardless of the number of elastic flows in the background, the acceptance time of streaming flows is constant for each *pfl_flushing_timer* value. This means that a new streaming flow is accepted in the AC block at the same time independently of the

Trans. Emerging Tel. Tech. **25**:1137–1148 (2014)
DOI: 10.1002/ett

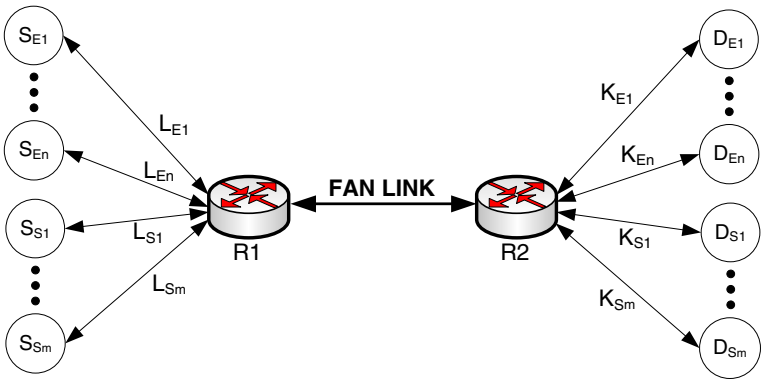

Figure 6. Basic simulation topology.

Table II. Values of simulation parameters.

Parameter	Value
No. of simulation runs	400
Duration of a simulation run	250 s
No. of elastic flows Transmission Control Protocol (TCP)	200–600
Size of elastic flows	Pareto distribution (shape factor = 1.5, mean size = 150 Mbit)
Packet size of elastic flows	1000 B
Interarrival of elastic flows	exponential distribution (mean interarrival time: 0.1 s)
No. of streaming flows User Datagram Protocol (UDP)	20
Rate of streaming flows	80 kbit/s
Packet size of streaming flows	100 B
Interarrival of streaming flows	exponential distribution (mean interarrival time: 1 s)
Capacity of FAN link	100 Mbit/s
Capacity of access links	1 Gbit/s
Size of buffer in R1	1000 packets
Measurement interval for the *PL*	50 ms
Measurement interval for the *FR*	500 ms
Th_{PL}	70%
Th_{FR}	5%
Flow time out	20 s
Warm-up time	20 s

FAN, flow-aware networks.

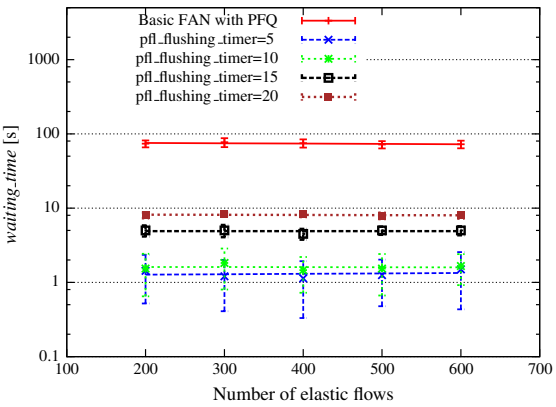

Figure 7. Acceptance times of streaming flows in flow-aware networks (FAN) with the enhanced flushing mechanism.

load of the FAN link. Without using the congestion control mechanism, *waiting_time* values are significantly higher than when the flushing mechanism (EFM) is implemented. The *waiting_time* values increase with increasing values of the *pfl_flushing_timer* parameter in the examined range. The best results were obtained when the *pfl_flushing_timer* was set to 5 s. The simulation results show that in this case a new flow was always accepted within 2 s, starting from the time when it began to send the traffic. When the *pfl_flushing_timer* was set to 10 or 15 s, a new flow was accepted a few seconds later; however, the results are still acceptable for local voice calls. It should be noted that according to [32], the setup time (post-selection delay) of local calls should be less than 6 s, whereas for international calls, it should not exceed 11 s. When the *pfl_flushing_timer* was set to 20 s, the results show that

a new streaming flow was accepted after approximately 8 s; this is not acceptable for local calls, although it is sufficiently low for international calls.

All the congestion control mechanisms proposed for FAN so far have one important drawback. The number of accepted flows in the PFL immediately after a flushing procedure is too high, and significantly greater than in the basic FAN. In the simulation experiment described in the later text, the mean number of elastic flows in FAN with PFQ was analysed. The simulation duration was set to 500 s. It is a reasonable value, making it possible to calculate the values of the analysed parameter in the steady state for a sufficiently long time. The rest of the simulation parameters were set as in the previous case.

The values of the mean number of elastic flows as a function of the number of elastic flows active in the background for FAN with PFQ are presented in Figure 8.

The mean number of elastic flows (ftp connections) added to the PFL in the router following any flushing action increases with the number of elastic flows being active in the background. The observed values for FAN with the EFM are significantly higher than for the basic FAN. Moreover, in the basic FAN, the mean number of accepted elastic flows is almost independent of the number of all active flows which want to transmit their packets. This is a major drawback of the EFM and shows that this solution may not be scalable, especially for low values of the *pfl_flushing_timer* parameter.

The following sections present the simulation results for MFAN and EFM with admission control policies proposed for MFAN and for EFMP. Simulation analyses were provided in the topology presented in Fig. 6. When MFAN was considered, an extra optical link was provided between routers R1 and R2. We analysed a case with 200 elastic flows active in the background. We made our simulation runs under various conditions and for different admission control policies and changed the values of the congestion control parameter. The duration of each simulation run was set to 250 s. The remainder of the simulation parameters was set as in the previous cases.

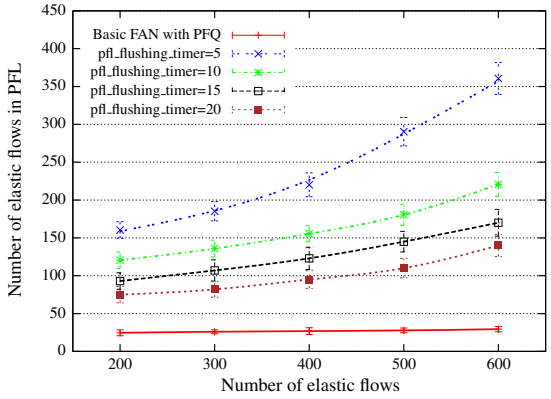

Figure 8. Mean number of elastic flows in protected flow list (PFL) in flow-aware networks (FAN) with priority fair queuing (PFQ) and enhanced flushing mechanism.

5.2. Multilayer flow-aware networks with policies

The results of simulating MFAN with the two most promising admission control policies (oldest-flow and most-active-flow) are presented in the first two rows of Table III. In the analysed case, the transmission in the optical link was implemented as a best effort service (with FIFO queue). Flows were rerouted in congestion if the buffer occupancy of the optical link did not exceed 80%. Otherwise, new flows were rejected. The new streaming flows were accepted after a short, acceptable time and the number of elastic flows accepted in the first FAN router on the primary route was sufficiently low, providing the fair rate assurance in the primary link. Unfortunately, it was impossible to assure a fair rate on the 5-Mbit/s level in the backup optical link. The results of the MFAN with both strategies and the timer between any flushing action set to 1 s are presented in the first and second rows of Table III. In this solution, the redirected traffic is accepted immediately in the backup link. This solution ensures quality of service for both traffic types. However, it must be noted that it requires additional resources in the physical layer, which increases the cost of transmission.

5.3. Enhanced flush mechanism with policies

The results of the EFM with the *pfl_flushing_timer* set to 5 s are presented in the third row of Table III. In this solution, the backup resources are not needed, which reduces the cost. The streaming flows are accepted quickly, although the number of elastic flows accepted after a flushing is too high. The fair rate varies widely, and it is usually a long way from the Th_{FR} value. In EFM, the PFL may be flushed less frequently than in the other cases presented in Table III. This is because in this case, we removed the identifiers of all elastic flows and congestion was eliminated quickly.

The fourth and fifth rows of Table III present the results of the new solution. We did not remove all elastic flows from the PFL during the flushing (as it was in the EFM), and used the policies proposed for the MFAN instead. First, we simulated the scenario where the identifier of the oldest flow was removed from the PFL under congestion. The *pfl_flushing_timer* was set to 1 s, which means that the minimum time period between two flushing actions was 1 s. Second, the identifier of elastic flows was selected according to the most-active-flow policy. The results show very good properties of both solutions. There is one problem when using the described algorithms. In some cases, the removed flow is not accepted again in the PFL for an excessively long time. This increases the mean transmission time of elastic flows.

Trans. Emerging Tel. Tech. **25**:1137–1148 (2014) © 2013 John Wiley & Sons, Ltd.
DOI: 10.1002/ett

Table III. The properties of admission control policies.

Architecture or mechanism	*waiting_time* [s]	Admitted flows	Advantages	Drawbacks
MFAN (1 s oldest-flow)	3.36±0.76	26.05±0.48	Short acceptance times of all flows, low number of accepted flows	High cost, lack of fair rate assurance
MFAN (1 s most-active-flow)	2.93±0.90	25.35±0.76		
EFM (5 s)	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 (1 s 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	
EFM (1 s most-active-flow)	3.68±0.45	23.13±0.45		Removed flows may not be accepted again Transmission of elastic flows is not continuous
EFMP (1 s 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	
EFMP (1 s most-active-flow)	3.68±0.80	24.26±0.64		

MFAN, multilayer flow-aware networks; EFMP, enhanced flush mechanism with priority; EFM, enhanced flush mechanism.

5.4. Enhanced flush mechanism with priority

The results of the simulation analysis of the EFMP are presented in the sixth and seventh rows of Tablw III. They show that our solution gives acceptable values of all analysed aspects in both admission control policies. The EFMP ensures fast acceptance of new streaming flows and good transmission properties of elastic flows, and it is scalable.

The results shown in Figures 9 and 10 (also presented in part in [33]) explain why we set the value of *pfl_flushing_timer* to 1 s. We also have to note that in this mechanism the *pfl_flushing_timer* means difference between end of *priority_access* and beginning of next EFMP run. The higher values of this parameter do not generate satisfactory results. The acceptance time of streaming flows and the number of elastic flows accepted again in the PFL increase significantly with the increasing value of the *pfl_flushing_timer* parameter. On the other hand, when

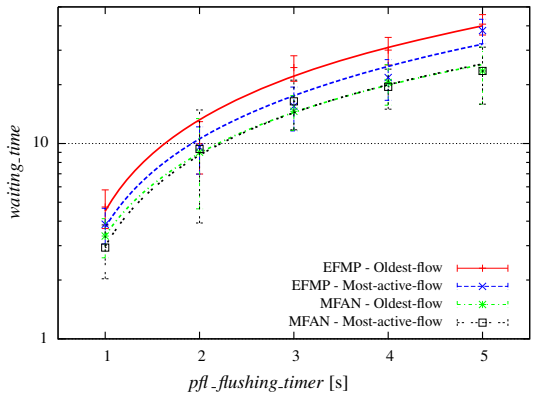

Figure 9. Acceptance times of streaming flows in flow-aware networks (FAN) with enhanced flush mechanism with priority (EFMP) or in multilayer FAN.

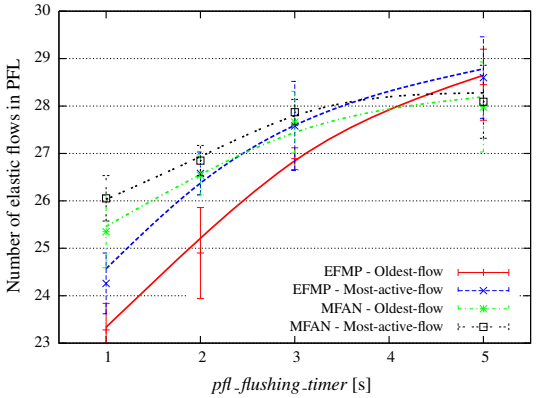

Figure 10. Number of elastic flows accepted in protected flow list (PFL) after flushing in flow-aware networks (FAN) with enhanced flush mechanism with priority (EFMP) or in multilayer FAN.

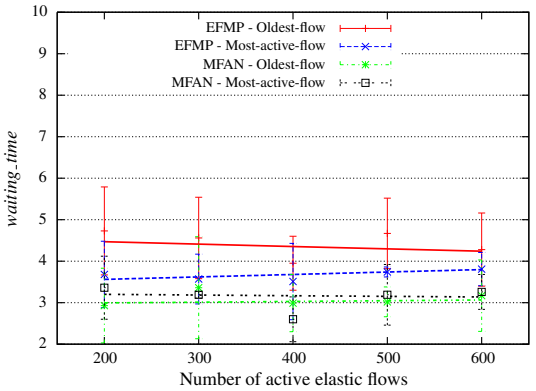

Figure 11. Acceptance times of streaming flows in flow-aware networks (FAN) with enhanced flush mechanism with priority (EFMP) or in multilayer FAN.

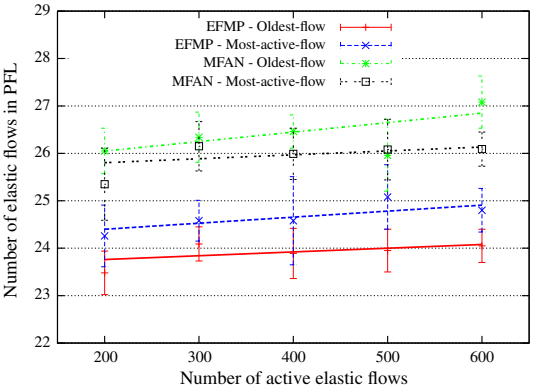

Figure 12. Number of elastic flows accepted in protected flow list (PFL) after flushing in flow-aware networks (FAN) with enhanced flush mechanism with priority (EFMP) or in multilayer FAN.

the value of this parameter is lower than 1 s, the EFMP mechanism is unstable. The same situation is observed for the MFAN with any strategy.

In the last simulation experiment, we checked how the values of *waiting_time* and number of elastic flows admitted to the PFL change as a function of the active elastic flows in the background. The simulations were provided for MFAN and for EFMP mechanisms with two admission control strategies, that is, the oldest-flow and the most-active-flow strategies. The simulation analysis was provided in the topology presented in Figure 6 and the number of active elastic flows varied from 200 to 600. The congestion control parameter (minimum time between any flushing action) was set to 1 s. The duration of each simulation run was set to 250 s. The other simulation parameters were set as in the previous cases. The results are presented in Figures 11 and 12.

Acceptance time values of streaming flows and the number of accepted elastic flows on the PFL are almost constant in each case. It is consistent with our predictions and confirms that MFAN and EFMP are scalable and ensure quality of service for both traffic types in FAN independently of traffic load in the network.

6. CONCLUSIONS

The flow-aware networking concept is a new proposal for the Future Internet; it appears to be very promising, although some improvements are required. Some problems are observed when congestion occurs in a network. In such a case, the new flows cannot be accepted, which causes significant transmission delays. This is highly important for voice connections or other real time applications.

In FAN, there are four congestion control mechanisms – EFM, remove active elastic flows, remove and block active elastic flows and remove and prioritize in access active elastic flows – which are based on total or partial cleaning of the PFL content in congestion. They make it possible for new flows to be accepted quickly in the admission control block. The mechanisms improve the transmission of the streaming flows, although they deteriorate the transfer of elastic ones. The other approach is implemented in MFAN. In this proposal, the excessive traffic is transmitted through an additional link placed in the optical layer. Three policies are used to select the excessive traffic: the newest-flow, the most-active-flow and the oldest-flow. The presented proposals have some drawbacks, including high cost and no guarantees for the traffic sent in the optical layer.

This paper proposes a new congestion control mechanism, EFMP. It is an extended version of EFM and assumes that elastic flows are removed from PFL according to the admission control policies proposed for MFAN. Such a solution allows for fast acceptance of streaming flows and ensures stable (without long breaks) transmission of elastic flows.

Both MFAN and EFMP are valid and have certain advantages. The paper presents their functionalities and compares them in terms of performance and cost. Because it provides additional capacity, the MFAN approach is better in terms of overall performance. It is an expensive solution, although if resources are available, it is the preferred choice. If cost is an issue, or the cooperation between layers is not allowed, the best alternative solution is the EFMP congestion control mechanism. The presented simulation results show that EFMP meets the expectations related to the scalable network with the guaranteed quality of service for both streaming and elastic traffic.

ACKNOWLEDGEMENT

The research was carried out with the support of the project ‘High quality, reliable transmission in multilayer optical networks based on the Flow-Aware Networking concept’ founded by the Polish National Science Centre under the project no. DEC-2011/01/D/ST7/03131.

Trans. Emerging Tel. Tech. **25**:1137–1148 (2014) © 2013 John Wiley & Sons, Ltd.
DOI: 10.1002/ett

REFERENCES

1. Roberts L. Beyond Moore's law: Internet growth trends. *Computer* 2000; **33**(1): 117 –119.
2. Coffman KG, Odlyzko AM. Growth of the Internet, 2002. Optical fiber telecommunications IV B: systems and impairments.
3. Minnesota internet traffic studies, 2009. Available at http://www.dtc.umn.edu/mints/.
4. Swanson B, Gilder G. The impact of video and rich media on the Internet – A zettabyte by 2015?, 2008. Available at http://www.discovery.org/a/4428.
5. Kortebi A, Oueslati S, Roberts J. Cross-protect: implicit service differentiation and admission control, In *Proceedings of High Performance Switching and Routing, HPSR 2004*, Phoenix, USA, 2004; 56–60.
6. Wojcik R, Domzal J, Jajszczyk A. Fair rate degradation in flow-aware networks, In *Proceedings of IEEE Intenational Conference on Communications, ICC 2010*, Cape Town, South Africa, 2010; 1 –5.
7. Jajszczyk A, Wojcik R. Emergency calls in flow-aware networks. *Communications Letters, IEEE* 2007; **11**: 753–755.
8. Domzal J, Jajszczyk A. The flushing mechanism for MBAC in flow-aware networks, In *Proceedings of 4th EURO-NGI Conference on Next Generation Internet Networks, NGI 2008*, Krakow, Poland, 2008; 77–83.
9. Domzal J, Wojcik R, Jajszczyk A. Reliable transmission in flow-aware networks, In *Proceedings of IEEE Global Telecommunications Conference, GLOBECOM 2009*, Honolulu, USA, 2009; 1 –6.
10. Lopez V, Cardenas C, Hernandez JA, Aracil J, Gagnaire M. Extension of the flow-aware networking (FAN) architecture to the IP over WDM environment, In *Proceedings of 4th Int. Tel. Net. Workshop on QoS in Multiservice IP Networks 2008*, Venice, Italy, 2008; 101–106.
11. Roberts J, Oueslati-Boulahia S. Quality of service by flow aware networking. *Philosophical Transactions of Royal Society* 2000; **358**(1773): 2197–2207.
12. Domzal J, Wojcik R, Jajszczyk A. Qos-aware net neutrality, In *Proceedings of First International Conference on Evolving Internet'09*, Cannes, France, 2009; 147 –152.
13. Roberts LG. Flow rate management, September 2008. Anagram Whitepaper.
14. Oueslati S, Roberts J. A new direction for quality of service: flow-aware networking, In *Proceedings of 1st Conference on Next Generation Internet Networks - Traffic Engineering, NGI 2005*, Rome, Italy, 2005; 226–232.
15. Joung J, Song J, Lee SS. Flow-based QoS management architectures for the next generation network. *ETRI Journal* 2008; **30**: 238–248.
16. Kaczmarek S, Landowski M. Performance of FAN conception of traffic control in IP QoS networks, In *Proceedings of the 1st International Conference on Information Technology, IT 2008*, Gdansk, Poland, 2008; 1–4.
17. Song J, Chang MY, Lee SS. Overview of ITU-T NGN QoS control. *IEEE Communications Magazine* 2007; **45**: 116–123.
18. ITU-T Recommendation Y.2121. Requirements for the support of stateful flow-aware transport technology in an NGN, September 2007.
19. Alparslan O, Akar N, Karasan E. TCP flow aware adaptive path switching in diffserv enabled MPLS networks. *European Transactions on Telecommunications* 2011; **22**(5): 185–199. DOI: 10.1002/ett.1468. http://dx.doi.org/10.1002/ett.1468.
20. Domzal J, Wojcik R, Jajszczyk A. Per user fairness in flow-aware networks, In *Proceedings of IEEE Intenational Conference on Communications, ICC 2012*, Ottawa, Canada, 2012; 1361–1346.
21. Domzal J. Flow-aware resilient ring new proposal for metropolitan area networks. *Telecommunication Systems* 2013. paper accepted for publishing.
22. Domzal J, Ansari N, Jajszczyk A. Congestion control in wireless flow-aware networks, In *Proceedings of IEEE Intenational Conference on Communications, ICC 2011*, Kyoto, Japan, 2011; 1–6.
23. Kortebi A, Oueslati S, Roberts J. Implicit service differentiation using deficit round robin, Proceedings of 19th International Teletraffic Congress, ITC19, Beijing, China, 2005.
24. Domzal J, Jajszczyk A. Approximate flow-aware networking, In *Proceedings of IEEE Intenational Conference on Communications, ICC 2009*, Dresden, Germany, 2009; 1–6.
25. Domzal J, Jajszczyk A. New congestion control mechanisms for flow-aware networks, In *Proceedings of International Conference on Communications, ICC 2008*, Beijing, China, 2008; 12–16.
26. Domzal J, Jajszczyk A. The impact of congestion control mechanisms for flow-aware networks on traffic assignment in two router architectures, In *Proceedings of International Conference on the Latest Advances in Networks, ICLAN 2008*, Toulouse, France, 2008; 133–138.
27. Domzal J, Wojcik R, Jajszczyk A. The impact of congestion control mechanisms on network performance after failure in flow-aware networks, In *Proceedings of International Workshop on Traffic Management and Traffic Engineering for the Future Internet, FITraMEn 2008*, Porto, Portugal, 2008; 1–7.
28. Morozov E, Rogiest W, De Turck K, Fiems D, Bruneel H. Stability of multiwavelength optical buffers with delay-oriented scheduling. *Transactions*

on Emerging Telecommunications Technologies 2012; **23**(3): 217–226. DOI: 10.1002/ett.1524. http://dx.doi.org/10.1002/ett.1524.

29. Domzal J. Intelligent routing in congested approximate flow-aware networks, In *Proceedings of IEEE Global Telecommunications Conference, Globecom 2012*, Anaheim, USA, 2012; 1751–1756.
30. Menth M, Martin R, Hartmann M, Sprlein U. Efficiency of routing and resilience mechanisms in packet-switched communication networks. *European Transactions on Telecommunications* 2010; **21**(2): 108–120. DOI: 10.1002/ett.1379. http://dx.doi.org/10.1002/ett.1379.
31. Network simulator ns-2, 2011. Available at http://nsnam.isi.edu/nsnam.
32. ITU-T Recommendation E.721. Network grade of service parameters and target values for circuit-switched services in the evolving ISDN, May 1999.
33. Domzal J, Wojcik R, Jajszczyk A, Lopez V, Hernandez JA, Aracil J. Admission control policies in flow-aware networks, Proceedings of 11th International Conference on Transparent Optical Networks, ICTON 2009, Azores, Portugal, 2009; 1–4.

Trans. Emerging Tel. Tech. **25**:1137–1148 (2014)
DOI: 10.1002/ett