Congestion Control in Flow-Aware Resilient Multi-ring Networks

Jerzy Domżał, *Member, IEEE*

***Abstract*—A complete congestion control system for Flow-Aware Resilient Multi-ring Networks (FARMN) is presented and analyzed in the paper. The FARMN combines the Flow-Aware Networks and the Resilient Packet Ring in one resilient QoS architecture in a multi-ring topology. The Simple Congestion Control Mechanism along with the Global Protected Flow List and the Intelligent Routing in FARMN ensure fast acceptance of streaming traffic (sent with priority) and protection of it when a link in a network fails. Moreover, it allows for more efficient transmission in a network. The advantages and weaknesses of the solutions presented in the paper are described and analyzed theoretically and by simulation experiments.**

***Index Terms*—Flow-Aware Resilient Ring; Flow-Aware Networks; Resilient Packet Ring; Quality of Service; congestion control**

I. Introduction

The new concepts for Metropolitan Area Networks (MANs) have been proposed for many years and still the development of MANs is an interesting topic for researchers and scientists. MANs have to ensure Quality of Service (QoS) properties and should be fast, resilient and consistent with the net neutrality concept [1], [2]. Many MAN architectures have been proposed and implemented during last years, e.g., SONET/SDH or Gigabit Ethernet and other proposals designed and developed in the framework of the European Union projects, like WONDER, SWRON, or OPSRN [3], [4]. Of course, the mentioned solutions have advantages and disadvantages. For example, the most popular SONET/SDH networks were designed many years ago for carrier-class performance and reliability, and for circuit-switched operation. As a result, network elements are quite complex and expensive and the implementation of a SONET/SDH network becomes sometimes inefficient, because the operational costs may be unacceptable. On the other hand, new proposals developed under research projects are in many cases at a very initial stage and a lot of research and implementation effort is still needed.

In this paper, the concept of a complete congestion control system for Flow-Aware Resilient Multi-ring Networks (FARMN) is presented and analyzed. The Flow-Aware Resilient Ring (FARR) concept was first proposed in [5]. The extended analysis of FARR networks was presented in [6] where multi-ring topologies have been theoretically analyzed. The congestion control system for FARMN consists of the Simple Congestion Control Mechanism which ensures fast acceptance of streaming flows in congestion, the Global Protected Flow List which guarantees immediate acceptance of streaming flows on a backup path when a link in a network fails and the Intelligent Routing which allows for more efficient transmission in a congested network.

This paper is organized as follows. Section II describes the architecture of FARMN. Section III shows the assumptions of the SCCM, the GPFL and the Intelligent Routing for FARMN. In Section IV, the results of carefully selected simulation experiments for FARMN with and without the congestion control system proposed in the paper are presented. Section V concludes the paper.

J. Domżał is with the Faculty of Computer Science, Electronics and Telecommunications, Department of Telecommunications, AGH University of Science and Technology, Al. Mickiewicza 30, 30-059 Kraków, Poland (e-mail: domzal@kt.agh.edu.pl).

II. Flow-Aware Resilient Multi-ring Networks

The Flow-Aware Resilient Multi-ring Networks are built based on the FARR architecture. That is why this section begins with description of the FARR concept.

A. Flow-Aware Resilient Ring

FARR combines advantages of two architectures: Resilient Packet Ring (RPR) and Flow-Aware Networks (FAN).

RPR is a well known architecture standardized as IEEE 802.17 in 2004 [7]. RPR assumes that traffic is sent in a network composed of two counter-rotating ringlets. Traffic in outer ringlet is sent in a counterclockwise direction, while in a inner ringlet traffic is transmitted in a clockwise direction. According to the routing protocol, the shortest path is chosen. When paths have the same number of hops, the outer ring is preferred. The example of traffic service in an RPR network is presented in Fig. 1.

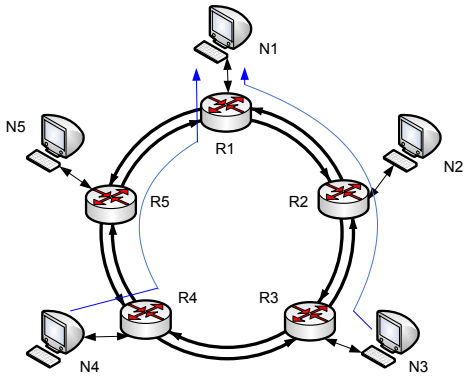

Fig. 1. Traffic service in RPR

RPR networks have many advantages, including reliability, QoS guarantees, fast transmission and others. Reliability is ensured by using one of two mechanisms: steering (mandatory) or wrapping (optional). In the first one, traffic is redirected to the opposite ringlet in a source node when a failure occurs. In the second one, traffic is wrapped in a node which corresponds to a failed link. It is also possible to combine both the mechanisms in one – wrapping-then-steering. The proper QoS for transmitted traffic is ensured by using traffic classes: A (with the highest priority), B or C. However, it is still not decided how to differentiate traffic and how to assign it to the proper class. Operators decide on it by themselves, usually by using the DS field in the header of IP packet. In IPv4 it is the ToS (*Type of Service*) byte while in the IPv6 it is the TC (*Traffic Class*) byte. Such a solution is susceptible to undesirable operations made by malicious users who may try to change the values of the DS field to speed up their transmission. Moreover, such a method of packet marking may not be consistent with the network neutrality assumptions. Another problem with RPR is that after failure, the redirected high priority traffic is not protected.

In 2007 the new version of the RPR standard (802.17b) was published [8]. It defines how RPR should work in multi-ring topologies. The SAS layer was specified to be used in nodes which belong to more than one ring.

FAN were proposed by S. Oueslati and J. Roberts in 2004 [9]. Traffic in FAN is sent by flows which are identified by source and destination addresses, source and destination ports and the identifier of transmission protocol. The incoming packets are implicitly classified to one of two flow types:

- elastic – flows which transmit with rate higher than minimum acceptable fair rate (min_FR),
- streaming – flows which transmit with rate lower than (min_FR).

Thanks to this assumption, FAN conform to the net neutrality paradigm. In FAN, the cross-protect routers (XP routers) are used. Apart from the traditional functionality, XP routers are additionally equipped with the admission control block (AC block) and the scheduler block. The first one decides which flows may be accepted in a router, while the second one puts packets into the proper queues and decides which packets should be sent first. Moreover, two parameters are periodically estimated in the scheduler block:

- *FR* — the maximum rate that is or might be realized by a flow,
- *PL* — the ratio, which represents the rate of incoming priority packets with reference to the link capacity.

When the FR in a link is lower than min_FR or the PL is higher than max_PL (maximum acceptable value of PL) the link is considered as congested. In congestion, new flows cannot be accepted in the AC block. Only flows already accepted (with IDs written to the Protected Flow List (PFL)) may be served in congestion.

FARR networks are based on both described above architectures. It is assumed that XP routers are used and traffic is sent as flows. Moreover, traffic classes are not used. Instead of it, packets are classified to one of two flow types: streaming or elastic. No signalling or packet marking is needed in FARR, which ensures lower complexity in comparison to RPR. On the other hand, in FARR the values of *PL* and *FR* must be periodically computed and the PFL has to be maintained. In FARR the ring topology is assumed. The neighbor nodes are connected by two single one-way links (in opposite directions). As packets are destination stripped, the spatial reuse is allowed (as in RPR). The topology discovery protocol (originally proposed for RPR) is implemented to ensure proper behavior of protection mechanisms (steering or wrapping). The streaming flows are sent with priority and the fairness among elastic flows is guaranteed by implementing the scheduling algorithm.

FARMN are composed of at least two Flow-Aware Resilient Rings. The key point in such architecture is a node which belongs to more than one ring. An example of FARMN is presented in Fig. 2, which is a reference topology for simulation experiments presented in this paper.

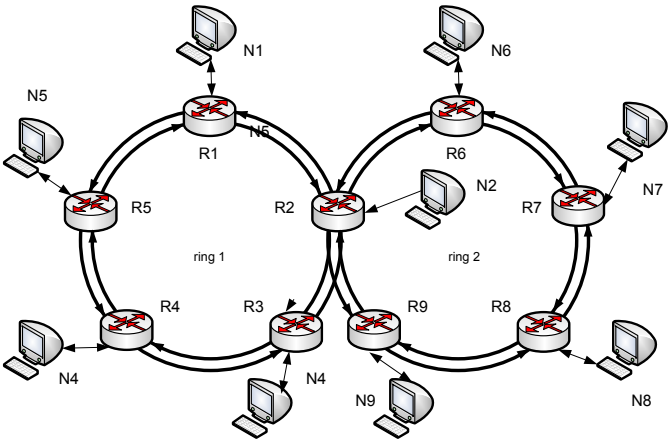

Fig. 2. Traffic service in FARMN

Node N2 belongs to both rings and has to serve traffic inside each ring and also traffic sent form one ring to another. Therefore it has to maintain four PFLs (each for an outgoing link).

III. Congestion control system for FARMN

The congestion control system for FARMN proposed in this paper is composed of the SCCM, GPFL and Intelligent Routing. The original proposals presented in the literature have been adapted to the needs of FARMN. The whole congestion control system ensures fast acceptance of streaming (high priority) flows, protection of streaming flows in case of a failure and efficient transmission of traffic in congested FARMN.

A. Simple Congestion Control Mechanism

The SCCM was originally proposed in [10] to minimize an acceptance delay ($waiting\_time$) of streaming flows in congested FAN. It assumes that the value of the min_FR is periodically reduced to 0 for a time equal to half of

the measurement period of the FR parameter. It allows for acceptance of new flows waiting for transmission. Of course, as a result of such operation, also new elastic flows are accepted (which is undesirable). However, after the time period given by the $clean\_el\_time$ parameter from the last reducing of the min_FR, the identifiers of all elastic flows accepted during this interval are deleted from PFL. It is recommended to set the value of the $clean\_el\_time$ parameter to 2 s, as it was done in the simulation experiments, results of which are presented in this paper. This value ensures that the IDs of all new elastic flows accepted in congestion are deleted from the PFL. Each congestion control mechanism, originally proposed for FAN, may be used in FARMN. However, the SCCM is less complex than its predecessors analyzed e.g. in [6], [11]. In this case, there is no need to maintain the additional flow list and to remove and add identifiers of active flows. While the results are similar to e.g. the Remove and Prioritize in access Active Elastic Flows mechanism, the SCCM works more intuitively and less operations have to be performed in congestion.

According to [12], the acceptance delay of international streams (e.g. intercontinental voice calls) should not exceed 11 s, while the acceptance delay for local streams ought to be less than 6 seconds. The results presented in [10] show that the SCCM gives satisfactory results. However, in this paper it is proposed to slightly change the operation of the SCCM. While the values of the FR are written to memory with fast reading and writing (min_FR is written in memory with short reading time but with long writing time) it is suggested to periodically set FR to min_FR instead of setting the min_FR to 0.

B. Global Protected Flow List

GPFL was first proposed in [13]. The goal of the GPFL is to ensure immediate redirection of streaming flows when a failure occurs in a network. Each router in a network maintains one Global Protected Flow List. When a flow is accepted for transmission in any outgoing link connected to the router, its ID is also added to the GPFL. The router periodically checks the status of all flows which IDs are on the GPFL and marks streaming flows. When a failure in a network is indicated the routers which need to redirect traffic to the backup paths first accept streaming flows from GPFL, even if the backup paths are congested. If they are not congested all redirected traffic is accepted.

The modification of the GPFL is proposed in this paper. The original solution ensures that redirected streaming flows are accepted in the first router. However, they may wait for acceptance in further routers on the backup path. To solve this problem it is proposed to mark first packets of redirected streaming flows, e.g. by using the DS field in the header of IP packet and accept them on the whole path. While the marking process is made in the core routers and without interference from network administrators or users it conforms to the net neutrality rules.

Each node has to maintain one GPFL for all outgoing interfaces. It means that in FARMN routers will keep the GPFL for two links. However, the router which belongs to two rings needs to maintain the GPFL for four outgoing links.

C. Intelligent Routing for FAN

The new method for packet routing in FAN was proposed in [10] and called Intelligent Routing. It also may be used in FARMN. The goal of the mechanism is to make possible to choose a different path for flows when the path appointed by the routing protocol is congested. It is assumed that the congested links in a network are reported to the routing protocol as failed. In such a case the routing protocol calculates new paths without considering the congested links. Once an outgoing interface is selected for a flow, its identifier is added to the PFL and further packets of such a flow are sent based on the outgoing ID written to the PFL (without looking at the routing table). In this way, the network is able to deliver more traffic to destination nodes. The results presented in [10] confirm that it is possible to significantly increase the total amount of traffic transmitted in a network.

In this paper, it is proposed to slightly change the Intelligent Routing mechanism. Instead of reporting the failure of congested links, it is suggested to increase the cost of congested links to the highest possible value. As a result, when all paths are congested the routing protocol chooses the path with minimum cost (the path which was computed first by the routing protocol). Even if it is congested, new streaming flows may be accepted thanks to implementation of the SCCM.

The pseudo-code for the complete congestion control system for FARMN is presented in Tab. 3.

```
 1  on a new flow packet p arrival in the congestion−less state
 2  choose the outgoing interface based on the routing table
 3  add ID of a flow and ID of the outgoing interface to PFL
 4  add ID of a flow to GPFL
 5  send p
 6  If a cost of a link changes in a network then
 7     begin
 8     compute new routing table
 9     do not change interface IDs in PFL
10     end
11  If an outgoing link is congested then
12     run the SCCM
13  If a link fails in a network then
14     begin
15     compute new routing table
16     change int. IDs of redirected flows based on the routing table
17     mark first packets of redirected stream. flows based on GPFL
18     accept redirected streaming flows
19     end
```

Fig. 3. Pseudo-code for the complete congestion control system for FARMN

When a new packet of a new flow (which does not have ID in PFL) arrives at the router, its ID is added to the PFL and to the GPFL. Moreover, the ID of the outgoing interface (selected based on the current routing table) is also added to the PFL (lines 1 - 4 in Tab. 3). If a link in a network becomes congested its cost is changed to the maximum value and new routing table is computed. However, the IDs of the outgoing interfaces currently added to the PFL do not change (lines 6 -

9). If all outgoing links are congested the SCCP is run to allow for acceptance of streaming flows (lines 11 - 12). When a link in a network fails, new routing table is computed and IDs of outgoing interfaces of redirected flows are changed according to the current routing table (lines 15 - 16). Moreover, the first packets of redirected streaming flows are marked and accepted immediately (lines 17 - 18).

IV. Simulation analysis of FARMN

In this section the results of carefully selected simulation experiments for FARMN carried out in the ns-2 simulator are presented.

In the first experiment it was decided to observe the acceptance delays ($waiting\_time$) of streaming flows before and after failure and total amount of traffic transmitted in a FARMN without the congestion control system.

10 simulation runs were made to observe the above mentioned parameters in topology presented in Fig. 2. The duration of each simulation run was set to 500 s. The number of background elastic flows activated by each node was set to 600 to saturate the network during the whole simulation experiments. The elastic flows were sent as follows: from N1 to N4, from N2 to N5, from N3 to N1, from N4 to N2, from N5 to N3, from N2 to N8, from N6 to N9, from N7 to N2, from N8 to N6 and from N9 to N7. Such an assignment caused that all elastic traffic was sent through the outer ringlets and each link in these ringlets was congested from the beginning of the simulation experiment. It was decided to provide the traffic pattern with Pareto distribution for calculating the volume of traffic to be sent by the elastic flows (ftp connections). The mean size of each elastic flow was set to 150 Mbit and the shape parameter was set to 1.5. The packet size was set to 1000 bytes. The exponential distribution for generating the time intervals between beginnings of transmissions of the elastic flows as well as for generating the start times of streaming flows was used. The elastic flows were sent from the beginning of the simulation run with the mean interval equal to 0.1 s. 20 streaming flows were sent by node N5 to N8. Streaming traffic before failure was sent through the inner ringlet in ring 1 and through the outer ringlet in ring 2 based on the information from the topology discovery protocol. It was assumed to analyze the VoIP connections realizing the Skype service. The packet size was set to 100 bytes and the transmission rate was set to 80 kbit/s for each of the streaming flows. Streaming flows were generated from 50 s with mean interval equal to 1 s. The capacity of links between routers was set to 100 Mbit/s. The capacity of access links (with FIFO queues) was set to 1 Gbit/s. The buffers in XP routers were sized to 1000 packets which is a reasonable value for FARMN links and the *MTU* was set to 1500 bytes. The measurement interval for the *PL* parameter was set to 50 ms while the *FR* values were estimated every 500 ms. The *max_PL* and the *min_FR* were set to 70% and 5% of the link capacity, respectively, and the *pfl_flow_timeout* parameter was set to 20 s, which is the time after which an ID of an inactive flow is removed from the PFL. At 200 s time instant links between R1 and R2 got failed and traffic was redirected according to the wrapping-then-steering mechanism. The warm-up time was 50 s. 95% confidence intervals were calculated by using the Student's t-distribution.

10 additional simulation runs were made in the second experiment when the Intelligent Routing was implemented. The simulation results are presented in Tab. I and in Tab. II. We may see that in basic FARMN streaming flows are immediately accepted in R5 and R1 because they are sent through the inner ringlet in ring 1 (which was empty). However the *waiting_time* in R2 exceeds 60 s because the outgoing ringlet in ring 2 was congested and new flows had to wait for acceptance. The same situation was observed in R9. As a result, the streaming flows had to wait over 100 s to begin transmission which was completely unacceptable. The worse results were observed for FARMN with the Intelligent Routing. In this case the streaming flows had to wait for acceptance for dozen of seconds in each router on their path. It was caused by the fact that inner ringlet in ring 1 was congested from the beginning of the simulation runs.

After failure of links between R1 and R2, streaming flows were redirected in R1 and had to be accepted in this router but in the outer ringlet. While this ringlet was congested at that time, the redirected streaming flows had to wait for dozen of seconds before they were accepted (see Tab. II). The same situation was observed in each router on the backup path. Of course the obtained results were unacceptable.

TABLE I
Mean *waiting_time* of streaming flows in basic FARMN (without SCCM and GPFL)

Routing type	*waiting_time* [s]		
	N5	**N1**	**N2**
Basic routing	0	0	60.12±6.01
Intelligent Routing	59.73±4.35	98.22±16.68	124.56±10.23

TABLE II
Mean *waiting_time* of streaming flows in N1 after a link between R1 and R2 failure in basic FARMN (without SCCM and GPFL)

Routing type	***waiting_time* [s]**
Basic routing	44.60±9.46
Intelligent Routing	35.54±14.33

20 further simulation runs were made in FARMN with SCCM and GPFL implemented (10 for basic FARMN and 10 for FARMN with the Intelligent Routing). The results are presented in Tab. III. We may see that mean values of the $waiting\_time$ parameter decreased significantly to the acceptable level (less than 6 s) in both cases (for basic FARMN and for FARMN with the Intelligent Routing). The values of the observed parameter after a failure of the link between R1 and R2 are not shown because the redirected streaming flows were immediately accepted in each router on the backup path.

We may conclude that the SCCM allows for fast acceptance of streaming flows and the GPFL ensures redirection of streaming flows in a case of a link failure without breaks in transmission.

TABLE III
MEAN *waiting_time* OF STREAMING FLOWS IN FARMN WITH SCCM AND GPFL

Routing type	***waiting_time* [s]**			
	N5	**N1**	**N2**	**N9**
Basic routing	0	0	1.55±0.18	2.31±0.33
Intelligent Routing	1.52±0.21	2.44±0.30	3.88±0.29	4.65±0.30

Tab. IV shows how much traffic was transmitted (delivered to destination nodes) in a network. Four cases have been compared. We may see that in basic FARMN (without Intelligent Routing, SCCM and GPFL) the amount of transmitted traffic is similar to the value obtained when the SCCM and GPFL were implemented. It proves that both the mechanisms do not deteriorate transmission of elastic flows in a network, regardless of a case when a failure occurs or not.

When we look at the values obtained for FARMN with the Intelligent Routing, we may see that the amount of transmitted traffic in a network increased significantly. In such a case the spare resources were utilized. The values are similar for both cases, with SCCM and GPFL and without them.

TABLE IV
TRANSMITTED TRAFFIC IN A NETWORK

Routing type	***transmitted traffic* [Gb]**
*basic network (**with** link between R1 and R2 failure, but **without** SCCM and GPFL)*	
Basic routing	219.93±1.17
Intelligent Routing	314.05±0.90
*basic network (**with** link between R1 and R2 failure, SCCM and GPFL)*	
Basic routing	218.76±1.13
Intelligent Routing	315.88±0.49

The results presented in this section show that the complete congestion control system for FARMN ensures fast acceptance of streaming flows in congestion without deteriorating of transmission of other traffic in a network. Moreover, the redirected streaming flows are immediately accepted on the backup path. The implementation of the Intelligent Routing ensures better utilization of resources available in a network.

V. CONCLUSION

The Flow-Aware Resilient Ring concept is a relatively new proposal for Metropolitan Area Networks. It combines the advantages of Flow-Aware Networks and Resilient Packet Ring. In this solution, traffic is served as flows and implicitly classified to one of two types: streaming or elastic. The streaming flows are served with a higher priority over elastic ones. The bandwidth not used by streaming flows is fairly divided among elastic flows. As a result, traffic is served with QoS guarantees and transmission conforms to the net neutrality paradigm. Moreover, the network is fast and reliable. The FARR architecture may be extended into the multi-ring topologies in an easy way. The Flow-Aware Resilient Multi-ring Networks eliminate the limitation of the maximum number of nodes in a ring and, as a result, they may transmit more traffic.

The congestion control system for FARMN, presented in this paper, is composed of three mechanisms: the Simple Congestion Control Mechanism which ensures short acceptance delay for streaming flows, the Global Protected Flow List which is used when a failure occurs in a network and ensures redirection of streaming flows without breaks in transmission and the Intelligent Routing which allows for more effective usage of network resources. The simulation results presented in the paper prove that the proposed congestion control system is efficient and significantly improves transmission in FARMN.

The new proposal of the congestion control system for FARMN meets the requirements of modern networks and may be used in the Future Internet based on optical rings.

ACKNOWLEDGEMENTS

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.

REFERENCES

[1] P. Cochrane, "Net Neutrality or Suicide?" *Proceedings of the IEEE*, vol. 94, pp. 1779–1780, October 2006.
[2] J. Domzal, R. Wojcik, and A. Jajszczyk, "QoS-Aware Net Neutrality," in *First International Conference on Evolving Internet, 2009. INTERNET '09.*, Cannes, France, August 2009.
[3] A. Bianciotto and R. Gaudino, "WONDER: overview of a packet-switched MAN architecture," in *Proceedings of the OpNeTec*, Pisa, Italy, October 2004.
[4] J. M. Finochietto, F. Neri, K. Wajda, R. Watza, J. Domzal, and M. N. E. Zouganeli, "Towards Optical Packet Switched MANs: Design Issues and Tradeoffs," *Optical Switching and Networking (OSN)*, vol. 5, pp. 253–267, October 2008.
[5] J. Domzal, K. Wajda, and A. Jajszczyk, "Flow-Aware Resilient Ring," in *IEEE ICC 2010*, Cape Town, South Africa, June 2010.
[6] J. Domzal, "Flow-Aware Resilient Ring – new proposal for Metropolitan Area Networks," *Telecommunication Systems*, 2013 - to be published.
[7] *802.17 IEEE Standard*, 2004.
[8] "SAS — spatially aware bridging over RPR," *802.17b IEEE Standard*, 2007.
[9] S. Oueslati and J. Roberts, "A new direction for quality of service: Flow-aware networking," in *NGI 2005*, Rome, Italy, April 2005.
[10] J. Domzal, "Intelligent Routing in Congested Approximate Flow-Aware Networks," in *IEEE Globecom 2012*, Anaheim, USA, December 2012.
[11] J. Domzal, N. Ansari, and A. Jajszczyk, "Congestion Control in Wireless Flow-Aware Networks," in *IEEE ICC 2011*, Kyoto, Japan, June 2011.
[12] ITU-T, "Network grade of service parameters and target values for circuit-switched services in the evolving ISDN," Recommendation ITU-T E.721, May 1999.
[13] J. Domzal, R. Wojcik, and A. Jajszczyk, "Reliable Transmission in Flow-Aware Networks," in *IEEE Globecom 2009*, Honolulu, USA, November-December 2009.