12th POLISH TELETRAFFIC SYMPOSIUM PSRT2005

PSRT

RECOVERY, FAIRNESS AND CONGESTION CONTROL MECHANISMS IN RPR NETWORKS

Jerzy Domżał, Krzysztof Wajda
Department of Telecommunications, AGH University of Science and Technology,
al. Mickiewicza 30, 30-059 Cracow, Poland, e-mail: {jdomzal@kt.agh.edu.pl, wajda@kt.agh.edu.pl}
Salvatore Spadaro, Josep Sole-Pareta, Davide Careglio,
Universitat Politecnica de Catalunya,
Barcelona, 08034, Spain, e-mail: {sspadaro@ac.upc.edu}

Abstract

The paper describes fundamental features of RPR (Resilient Packet Ring - IEEE 802.17 standard). It focuses on proposals how to improve fairness mechanism and to increase network efficiency in state of congestion. Recovery mechanisms are also discussed, with presented analytical and simulation results. The goals of paper are threefold. At first, we show RPR main features and describe its current status. Secondly, we present main recovery and resilience features of RPR and propose solutions for improving both fairness and congestion control. Finally, a new concept, the enhanced hold-off timer (EHOT) is introduced improving recovery actions in multilayer networks. Some simulation results are presented in order to illustrate advantages of proposed solution.

Index terms -Resilient Packet Ring (RPR), OTN, congestion control, fairness, resilience

1. INTRODUCTION

At present most of MAN and WAN networks are built using ATM and SDH technologies. In the nearest future the multilayer IP/MPLS/OTN architectures will be more often used for improving recovery and resilience in networks. An alternative for such a proposition may be using IP/RPR/OTN or, what is more probable, IP/MPLS/RPR/OTN multilayer strategy. *Resilient Packet Ring* (RPR) is a new IEEE 802.17 standard, finished and approved in June 2004. Complex IP/MPLS/RPR/OTN architecture may improve network operation and its robustness against any single failure occurring in RPR ring.

In the following points main features of RPR will be presented. We will show methods for improving the fairness algorithm and the congestion control mechanisms (used in RPR). At the end the main aspects of RPR and OTN interworking will be introduced and illustrated by simulation results.

2. RESILIENT PACKET RING

RPR (Resilient Packet Ring) is a novel protocol for using at second layer in OSI/ISO model. RPR ensures improved resilience and efficient utilisation of resources.

RPR is based on DPT (Dynamic Packet Transport), the protocol proposed by Cisco [4]. The main aspects of RPR that decide of its functionality are:

- Protection mechanisms,
- Scalability in speeds and number of nodes,
- Spatial Reuse possibility,
- Support for a limited number of priorities (2 or 3).

RPR architecture is based on two symmetric, counter rotating rings. One of them is called *inner* and the second *outer*. Packets are transmitted in both rings simultaneously in opposite directions. When data packets are transmitted in outer ring, the control packets corresponding to them are transmitted in the second ring. Packets are destination stripped, which allows for providing spatial reuse.

A RPR ring composed of 8 nodes is presented in Fig. 1.

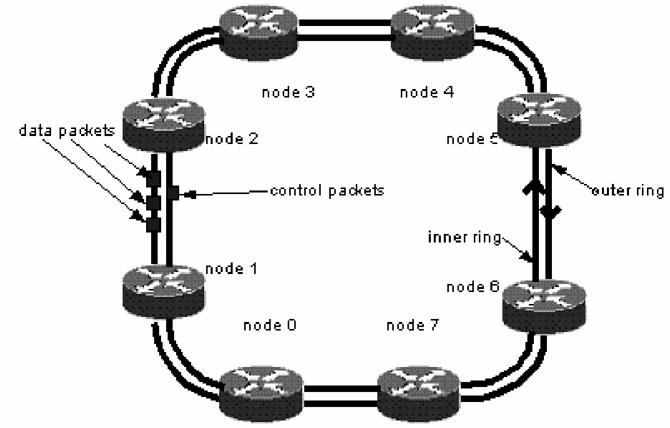

Fig. 1. RPR ring composed of 8 nodes

The protocol is designed to operate over a variety of physical layers, including SONET/SDH, Gigabit Ethernet (IEEE 802.3ab), DWDM and dark fibre. It is expected that the RPR will be able to work over higher-speeds physical layers. The minimum supported data rate is 155Mbit/s.

Main components of RPR will be briefly described below. They are:

- *Spatial Reuse*

In RPR architecture packets are destination stripped. It gives possibility to transmit more data at the same time (in opposite to the ring techniques proposed earlier). This situation is shown in Fig. 2. All source nodes can send their data at the same time (spatial reuse). The flows originated form node 1 and node 2 are transmitted through the link between node 2 and node 3, thus their traffic can’t be transmitted faster then *C/2*, where *C* is a link capacity. At the same time node 5 can transmit it’s traffic to node 6 with max rate (up to *C*). This is one of the most important advantage of RPR.

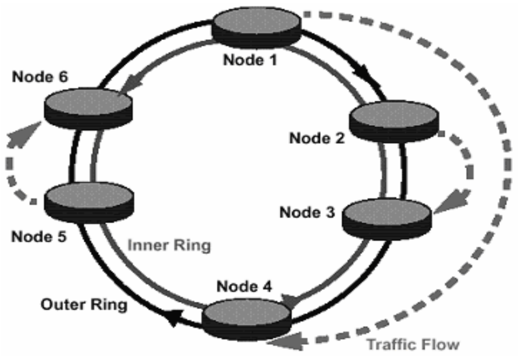

Fig. 2. Spatial reuse mechanism in RPR ring composed of 6 nodes

- *Topology discovery*

The main objective of topology discovery mechanism is fast reaction to topology change. The topology discovery packets are updated in every node. When the TD packet comes back to the source node, the map of topology is built in the node and the packet is stripped. This mechanism is activated at time of activation RPR rings, at time of any failure and at time of add new node to the ring or drop the node from the ring. Topology discovery packets are also sending periodically in the ring. Each topology discovery packet have to be stripped by source node. Data packets are allowed to send when each node in the ring has own topology map. In Fig. 3 transfer of topology discovery packet is shown. The MAC address of each station is added to the field in the packet to keep right order of nodes in the ring.

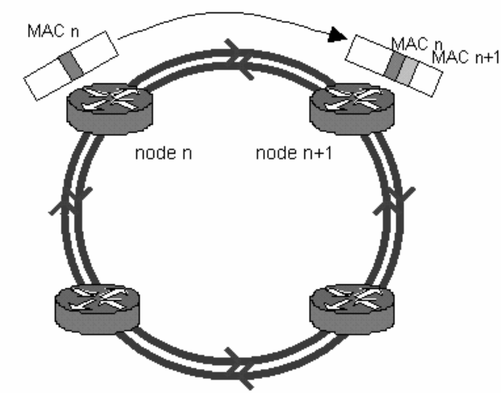

Fig. 3. Transfer of TD packet in RPR ring

- *Traffic classes*

There are three traffic classes in RPR:

class A – designed for high priority traffic, in particular for flows with low delays and guaranteed link bandwidth demands (e.g. VoD services)

class B – designed for medium priority traffic, in particular for packets for which the traffic contract isn’t possible to be filled (e.g. VoIP)

class C – designed for low priority traffic, in particular for all best effort traffic (e.g. data transfer)

Class A traffic has absolute priority over class B and C traffic. Priority possibilities for B class traffic aren’t fully described in standard 802.17. Medium class packets should be discarded or treated as best effort packets. If the second proposition is chosen, the thresholds in transit buffers should be properly placed to allow for elastic treating such packets (like best effort traffic), but with higher priority than class C packets. Class C packets have fair access to the resources not used by higher classes packets. Thus fairness algorithm is proposed. A few versions of this algorithm are proposed to improve fairness and reduce oscillations round the fair value. Moreover congestion control mechanisms are proposed for improving fairness after any single failure in the network.

3. CONGESTION CONTROL MECHANISM IN RPR

Well planned congestion control mechanism is crucial to any network architecture in case of single bottleneck. Congestion control in ring networks has several specific features. Every node in ring is responsible for congestion detection and proper reaction on it. In particular a RPR node needs to estimate fair rate of the flows contributing to the congestion and generate appropriate feedback to the upstream nodes to prevent buffer overflow.

Feedback messages in RPR are sent as Fairness Control Messages (FCM). These messages are sent very frequently (approx. each 100μs) which enables fast reaction for the congestion. The upstream nodes are able to fast adjust locally inserted traffic. The other goals of effective congestion control mechanism in RPR are:

- to improve utilization of ring resources,
- to allow fair transmission of downstream nodes (non-starvation),
- to enable coexistence of high and low classes traffic simultaneously with guarantees on delay and jitter for high priority traffic and fairness for low priority traffic.

Congestion control mechanism that addresses above issues for conservative mode is presented in [1]. The aggressive and conservative modes of fairness algorithm and DVSR and DBA algorithm presented in section 3 of this paper also play the role of congestion control mechanism. The mechanism presented here allows for earlier reaction to incipient congestion by introducing an intermediate threshold for the transit buffer occupancy that limits the computed fair rate and allows for more quickly computation of this parameter. The advantages of the algorithm are that it works properly in large rings and allows for fast start of newly active stations.

The described algorithm's name is enhanced conservative mode (ECM) for fairness algorithm. It ensures spatial reuse – the nodes placed out of the congestion domain aren't bounded by the fair rate.

The computation of *fair_rate* in ECM algorithm is very simple. When the node is a *head* of the congestion domain the *fair_rate* (F_{ECM}) is computed from formula (1)

$$F_{ECM}(t) = local\_fair\_rate(t) \quad (1)$$

When the downstream link isn't congested the *fair_rate* increases up to "unreserved rate" as in formula (2)

$$F_{ECM}(t+1) = F_{ECM}(t) + (R - F_{ECM}(t)) \quad (2)$$

where R is the "unreserved rate".

When the node isn't a *head* of the congestion domain, but the downstream link in congested, the *fair_rate* value is computed from formula (3)

$$F_{ECM} = \min(L, W_i \times A_i) \quad (3)$$

where L is the node's locally computed *fair_rate*, W_i is the weight associated to node i, and A_i is a *fair_rate* received by a node in fairness frame (FCM).

The main advantage of presented proposition is that when the transmission begins (and after topology change) the nodes starts sending the traffic with maximum allowed rates. The main disadvantage of this mechanism are rate oscillations in nodes after failure (when they tries to achieve *fair_rate*). The answer for this problem is modification of fairness algorithm.

4. FAIRNESS ALGORITHM

The fairness algorithm, used in RPR, ensures fair access to the resources for low priority traffic. This algorithm is very simple in it's basic assumption. But it needs some time to properly describe fairness messages and to ensure steady state. So it has some limitations. It is undesirable, especially in case of any network element failure. In this point of view the algorithm oscillations are most unfavourable. These oscillations are a barrier to achieving spatial reuse and high bandwidth utilization. Two versions of Fairness Algorithm are proposed in the standard 802.17:

- *Conservative mode* – message with new fair rate value is sending after all stations in the congestion domain have adjusted to the fair rate (by default used in architecture with single transit queue in the nodes),

- *Aggressive mode* – messages with new fair rate value are sending periodically with default interval of 100µs (by default used in architecture with two transit queues in the nodes).

In both modes two values are measured:

- *forward_rate* – byte count of all serviced transit traffic in the node,
- *my_rate* – byte count of all serviced local traffic in the node.

These measurements are taken to compute the *fair_rate* value in a fixed *aging_interval*, but are used differently in both modes.

There are many propositions for improving problems with stability of fairness algorithm. One of them is DVSR algorithm (Distributed Virtual-time Scheduling in Rings) proposed in [6].

4.1. DVSR (Distributed Virtual-time Scheduling in Rings) algorithm

The DVSR algorithm is proposed to use in architectures with one transit queue in nodes (conservative mode). No queuing operations on these queues are provided. The reference model for DVSR is RIAS (Ring Ingress Aggregated with Spatial Reuse), which ensures fair bandwidth allocation and spatial reuse in the ring. The fair rate of link *k* at time *t*, in RIAS concept, is computed form formula (4)

$$\mathrm{F_k}(t) = \frac{C - B(t)}{w(t)} \qquad (4)$$

where *B(t)* is the sum of the rates transmitted through to the last node before link *k*, bottlenecked elsewhere or at their ingress points and *w(t)* is the number of flows bottlenecked at link *k*.

The objective of DVSR algorithm is to ensure RIAS-fair rate at ingress point. The l_i value is measured as input to the algorithm and denote the number of arriving bytes from ingress node *i* in time *T*. The *b* value denotes the fraction of time during the previous interval *T* that the multiplexer is busy serving packets. Thus, if *b* is less than 1 (b<1) the fair rate is computed form formula (5)

$$\mathrm{F} = \mathrm{l_k} / CT + (1 - b) \qquad (5)$$

In the other case (if b>=1), the fair rate is computer using the pseudo code (6)

```
$\mathrm{i} = 1$
$\mathrm{F} = 1/k$
$Count = k$
$Rcapacity = 1$
$while((l_i / CT < F)\,\&\&(l_k CT \geq F))\{$          (6)
$Count--$
$Rcapacity-= l_i / CT$
$F = Rcapacity / Count$
$l_i = l_{i+1}\}$
```

Because the byte counters are ordered such that $l_1 \leq l_2 \leq ... \leq l_k$ (where *k* is the number of nodes transmitting packets), when b<1, the fair rate is equal to the largest ingress-aggregated flow transmission rate l_k / CT plus the unused capacity. If *b=1* the max-min fair allocation is computed. Thus $F = \max\_\min_k(1, l_1/CT, l_2/CT, ..., l_k/CT)$.

The DVSR algorithm ensures spatial reuse in the rings and low oscillations before achieving steady state when the topology changes (e.g. after failure). The main disadvantage of DVSR algorithm is its high computational complexity $O(k\log k)$.

4.2. DBA (Distributed Bandwidth Allocation) algorithm

The DBA algorithm doesn't need per-source information like in RPR fairness or DVSR algorithms. Spatial reuse, oscillations after topology change and fairness are on DVSR level, but, what is very important, computational complexity is low - $O(1)$.

The reference model for DBA is RIAS, like in DVSR. The fair rate of link *k* is computed form formula (7)

$$F_k(t+1) = F_k(t) + \frac{1}{\widetilde{M}}(C - \widetilde{A}(t)) \qquad (7)$$

where $\widetilde{M}$ is an effective number of flows traversing link *k* and is equal to $\frac{\widetilde{A}(t)}{F_k(t)}$ and $\widetilde{A}(t)$ is the arrival rate at link *k* expressed as : $\widetilde{A}(t) = F_k(t)\sum_{i=1}^{M}\rho_i$ and M is a number of flows traversing link *k* [2].

The main goal of DBA algorithm is that $\widetilde{A}(t)$ matches the available bandwidth (spatial reuse and high bandwidth utilization). Moreover $F_k(t)$ converges the optimal fair rate. The algorithm is scalable for a ring network with any number of nodes (computation complexity is low and independent form the number of nodes). The oscillations before achieving a steady state are low and on the same level as in DVSR algorithm.

4.3. FLC (Fuzzy Logic Control) algorithm

The FLC algorithm uses Membership Function (MF) to compute *fuzzy_add_rate* which approximates the *local_fair_rate* value.

The FLC algorithm uses two groups of inputs: *add_rate* and *?add_rate* in one group and *rcvd_rate* and *?rcvd_rate* in another group. The output of the algorithm is *fuzzy_add_rate.* FLC accelerates or decelerates the sending traffic intelligently in order to reduce oscillations and improving bandwidth efficiency. A triangle MF function was chosen for RPR. (because of its simplicity). The *fuzzy_add_rate* value is computed from formula (8)

$$fuzzy\_add\_rate = \frac{Wx\sum_{i=1}^{n}(Y_i xWEIGHT_i)}{\sum_{i=1}^{n}Y_i} \qquad (8)$$

where *n* is a number of If-Then rules which have to be taken to determine how FLC is defuzzified, *W* is the half of the range chosen for MF, Y_i is the output of MF for *I* rule, $WEIGHT_i$ is the weight assigned to the *i* rule.

The FLC algorithm is more stable and reliable than fairness algorithm proposed in 802.17.

5. RECOVERY MECHANISMS IN RPR

There are two recovery mechanisms in RPR architecture:

- steering protection – obligatory mechanism implemented in each node; after failure packets are redirected in source node in order to avoid sending them by failed links or nodes,
- wrapping protection – activated only in nodes which declared it during topology discovery process; after failure packets are redirected in node located next to failed link or node and sent in the other ring.

There are two RPR rings presented in Fig. 4 (before and after link failure). Wrapping mechanism is illustrated on the right.

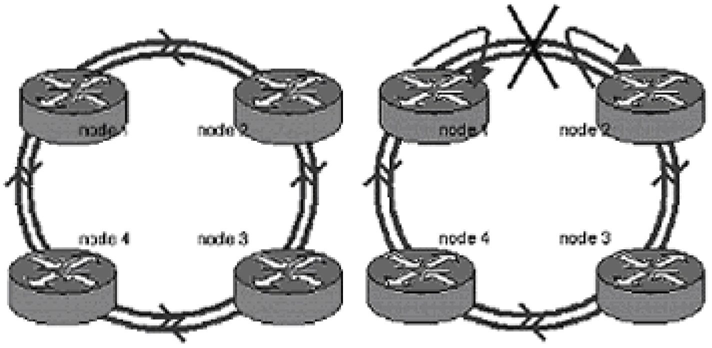

Fig. 4. RPR rings before and after link failure.

The mechanisms work under control of IPS (Intelligent Protocol Switching) protocol, which is similar to APS (Automatic Protection Switching), used in SONET/SDH rings. The protocol id designed in order to detect any failure in the RPR rings. In particular IPS detects loss of continuity of transmission in the medium, loss of signal power, increasing the level of errors in transmitted packets. The failure may be detected in RPR layer or in the other. So, the multi-layer interworking is possible. One of such interworking proposition is presented in section 7.

The IPS protocol is related to fairness algorithm. Any failure in the ring causes congestion and needs the *fair_rate* to decrease. The recovery mechanisms proposed in 802.17 standard ensures fast reaction to any failure (<50ms). It allows for fast transmissions in real time. The propositions of new versions of fairness algorithm, presented in section 5, may improve reaction to the failure. It can be faster and less noticeable for the users.

6. RECENTLY PROPOSED IMPROVEMENTS IN RPR STANDARD

Despite the fact that RPR standard was approved in 2004 after few years of significant efforts as IEEE 802.17, further works have begun towards resolving the raised objections, such as support for multiring architectures and multiservice traffic (i.e. clarification of A, B and C class usage).

802.17b is a new version of RPR standard that is currently prepared. It is proposed to improve bandwidth utilization for applications working over RPR that involve bridging clients. In this standard a new MAC sublayer is proposed, called Spatially Aware Sublayer (SAS). This solution enables to use multiring architectures in RPR, broadening functionality and size of RPR networks.

SAS ensures spatial reuse method to be used even if the destination address of station is remote address. The other goal of using SAS sublayer is to provide spatial reuse mechanism for multicast traffic. SAS proposition shouldn't change base assumptions of RPR 802.17 standard. The compatibility with 802.1 bridging specifications (e.g. 802.1D/Q) ought to be maintained and the overall cost of this solution should be minimized.

The main operation of the SAS is to associate a remote address (and optionally VLAN identifier) with RPR station MAC that provides an attachment interface to the client identified by the remote address. Nodes with SAS sublayer can use directional transmissions over the ring, which isn't considered in 802.17 standard. A learning process is proposed for associating remote addresses and VID (virtual identifiers) with local RPR addresses.

One of possible implementation assumes using a database (SAS DB), where all addresses of nodes with implemented SAS mechanism are written during teaching process (probably Topology Discovery process). When node with SAS implemented, sends a packet, it checks if the destination address is placed in SAS DB, and if yes the directed transmission is possible. In the other case, when the destination address is unknown, the broadcast transmission is necessary. Data in SAS DB should be updated after any topology change.

The presented proposition is still developed. Properly use of described concept may improve transmissions in multi-ring RPR network.

7. MULTILAYER RECOVERY STRATEGY IN RPR/OTN NETWORK

The simplest way to implement multi-layer recovery is to run the different mechanisms in parallel and independently from each other (uncoordinated approach).

If we consider that RPR runs over intelligent optical transport networks, both RPR and optical layer recovery mechanisms act independently from each other. However, due to the fact that they detect the failure in similar times, both layers will try to restore the connectivity at the same time. While RPR recovers from failure by ring wrapping around failed span or by packet steering, the optical layer relies, for example, on dedicated resources for recovery (i.e. 1+1 and/or 1:1 dedicated protection).

This can lead to significant performance degradation for the layer above RPR (i.e. IP) as well as leading to potential networks instability and unnecessary reduction of the network capacity. If both RPR and optical layer start recovery actions, independently of the failure scenario, once detected the failure, RPR will wrap its ring, thus reducing the available bandwidth. As a result, a failure at the optical level that is efficiently managed by the optical layer using the uncoordinated approach implies the reduction of the bandwidth at the client (IP/RPR) layer .

This section suggests a novel multi-layer resilience strategy, based on the interworking between RPR and the optical layer.

It consists on implementing the enhanced hold-off timer (hereafter EHOT). RPR can detect a failure in different ways, depending on the used sources of information about failures: some of them are independent from other layers and one is the information signalled from the underlying layer (i.e. optical layer). RPR, detecting a failure (through signal fail (SF) signalling), is able to distinguish between two cases:

- when the optical layer has also detected the failure (it has occurred at optical layer),
- when the optical layer has not detected the failure (and RPR is the only layer that is able to do a successful recovery).

In the latter case, the failure has occurred in the upper layers.

The suggested EHOT approach is based on dividing the entire hold-off timer into two parts: H1 (short) and H2 (long). The first one (H1) is activated after the RPR layer detects the failure. An RPR station determines whether a link is alive if it is receiving fairness messages from it. The number of ms that pass without receiving a fairness message from the neighboring stations is then measured and the default keepalive timer is set to 3 ms.

H1 timer serves to give to the optical layer some time to detect the failure and signal it to the RPR layer. It has to be underlined that the detection failure at the optical level is strongly influenced by the optical components themselves and their management. Anyway, according to our knowledge, it takes few ms. After the expiration of H1, if the optical layer has not detected the failure, RPR triggers its protection immediately (Fig. 5).

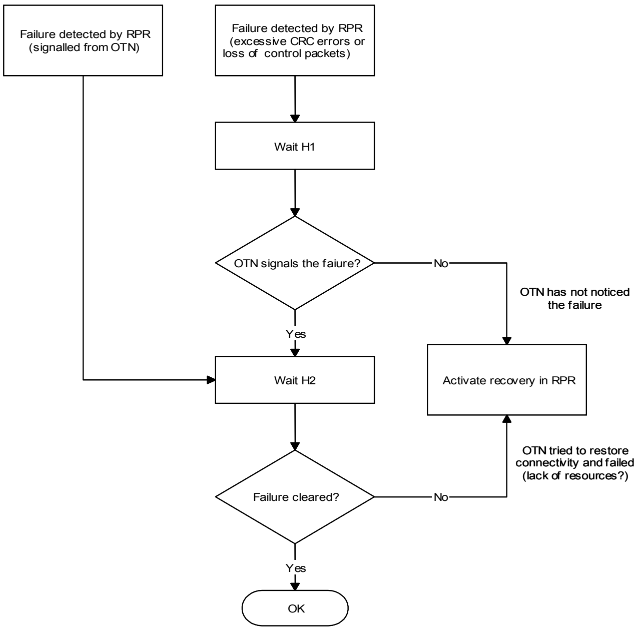
Failure detected by RPR (signalled from OTN)
Failure detected by RPR (excessive CRC errors or loss of control packets)
Wait H1
OTN signals the faiure?
No
OTN has not noticed the failure
Yes
Wait H2
Activate recovery in RPR
OTN tried to restore connectivity and failed (lack of resources?)
Failure cleared?
No
Yes
OK

Fig. 5. Enhanced Hold-Off Timer (EHOT) approach

On the other hand, if the failure is signaled to RPR layer by the optical layer, the RPR layer waits during the H2 timer to give time for recovery in the optical layer. The recovery procedure in the optical layer encompasses both fault localization and the recovery mechanisms (i.e. dedicated path protection or restoration). If the optical layer is unable to solve the failure (basically due to the unavailability of available resources in case of using restoration) during the H2 period, then RPR protection mechanism is launched.

The required functionalities for the EHOT implementation have already been incorporated both in optical transport layer and in RPR. In fact, OTN is required to signal to its client layer both signal degradation and signal failure [8] while RPR is able to accept such signals from the underlying layer [5]. The main advantage of this approach, when compared to the HOT (*Hold-Off Timer*) one is that the recovery time is much shorter when failure root is above the optical layer, allowing in this case minimizing the traffic lost due to the failure. If the failure occurs at the optical layer, the EHOT provides the same performance as HOT approach.

7.1. Performance Evaluation

To compare the HOT and the EHOT approaches for different failure scenarios, we carried out a simulation study. The simulated scenario consisted of 5 IP routers equipped with RPR cards logically connected through a meshed optical transport network composed by optical cross-connects (OXCs). The distance among the nodes was set to 3 km, whot results in the propagation time between nodes of 15 μs.

The optical nodes are connected through bi-directional optical paths (i.e. two physically disjoint optical fibers) and the 1:1 path protection was implemented. For the fault management in the optical layer, we implemented the GMPLS-based Link Management Protocol [9]. The fault detection is carried out through the implementation of the HELLO messages sent between the optical nodes controllers combined with the Loss of Light (LoL) alarms from the OXCs. Specifically, an in-fiber out-of-band signaling approach has been implemented. The offered load (ρ) was set to 0.45; Class A represented the 20% of the generated traffic, Class B another 20% and the rest represented Class C traffic. The traffic inserted in the ring by each node was uniformly distributed among the rest of nodes.

The simulated operation time was set to 120 ms and as stated above, the *bottom-up* approach was used. The failures occur at the instant t = 50 ms. Two case studies were carried out. The first one concerned a failure that occurs at the optical level (cut of the fiber connecting two OXCs breaking the logical connection between two IP/RPR routers) while the second referred to the case in which the failure occurs at RPR layer (e.g. failure of RPR card of one of the routers composing the ring).

Focusing on the first case study, according to the defined EHOT approach, RPR layer, once detected the failure instead of launch immediately the recovery action, waits for H1 in order to enable to take recovery action in optical layer. In this case, the failure root is in the optical level and it signals the failure detection to RPR layer. Once the optical level has recovered the network from the failure (e.g., through path protection recovery), the network comes back to the initial conditions. In this case study, both the EHOT and the HOT approaches provides the same behavior.

Focusing in the second case study, Fig. 6 shows the comparison between the HOT and the EHOT approach. The former foresees that the RPR layer waits for the entire hold-off timer (i.e. H1+H2). Once the timer has expired and the failure has not been recovered by the optical layer, then RPR starts to recovery from failure. By using the EHOT approach, the RPR layer just waits for the first short timer (i.e. H1). If H1 expires and the optical layer has not signaled the failure detection, then the RPR starts immediately the recovery action (in this case, we implemented the wrapping mechanism). In such a case, after H1, the network throughput comes back again to the value before the failure. In terms of recovery time, we can estimate that in case of HOT is about 45 ms while in case of using EHOT in the same conditions is about the half (Fig. 6).

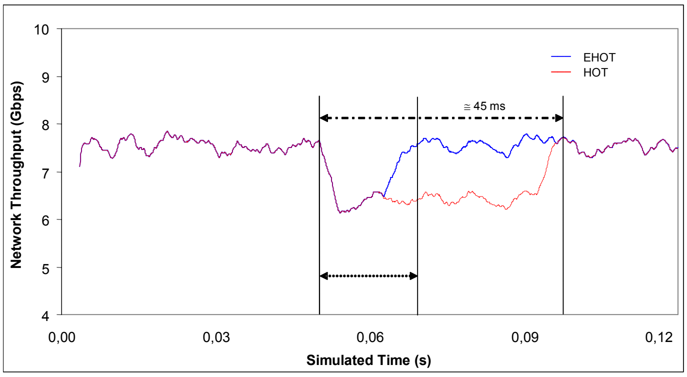

Fig. 6. SHOT vs. EHOT, failure at RPR level

As additional simulation case study, we obtained the relative traffic losses (i.e., $R=(\mathit{Packets\ Lost})_{EHOT}/(\mathit{Packets\ Lost})_{HOT}$, comparing the HOT and the EHOT approaches for different values of the H1 and H2 timers, when the failure occurs at RPR layer. Table 1 depicts the gain in terms of percentage of reduction of the traffic losses (i.e., 100*(1-*R*)) arising from the implementation of the EHOT approach with respect to the HOT. Both RPR protection mechanisms have been considered. Specifically, in the considered simulation scenario, the results indicate that the traffic losses reduction ranges from the 52% to 77%. It has to be underlined that the recovery time is slightly higher when packet steering is applied.

H1 = 10 ms	***EHOT vs. HOT:*** ***Traffic Lost reduction***	
H2 (ms)	*RPR wrapping*	*RPR steering*
20	62.5%	62.0%
30	71.5%	71.1%
35	74.5%	74.2%
40	77.0%	76.6%

H2 = 30 ms	***EHOT vs. HOT:*** ***Traffic Lost reduction***	
H1 (ms)	*RPR wrapping*	*RPR steering*
10	71.5%	71.1%
15	63.9%	63.6%
20	57.5%	57.2%
25	52.7%	52.5%

TABLE I.. EHOT vs. SHOT: Packets lost

It is worth noting that this percentage strongly depends on the actual traffic load, the failure scenario and the set of the H1 and H2 timers.

8. CONCLUSIONS AND FURTHER INVESTIGATIONS

The fairness and congestion control mechanisms proposed for use in RPR rings are presented in the paper. The main goal of them is to enable taking fast recovery action in case of failure. The algorithms need to ensure fair and efficient access to the resources. The low computation complexity and little oscillations near the fair rate value are the advantages of DBA algorithm.

The work on developing mechanisms use in RPR are still taken. The SAS concept will be probably the most popular solution for use in multi-rings architectures.

This paper suggests a multi-layer recovery strategy to be used in an IP/RPR over optical transport networks scenario. It is based on the interworking between the RPR and the optical layer and proposes a novel approach, the Enhanced Hold-Off Timer (EHOT) to coordinate their recovery actions. The EHOT provides benefits in terms of better recovery (lower recovery time and traffic losses) from higher layers failures, compared to the well-know HOT. In fact, the EHOT allows to faster react to different failure scenarios reducing the traffic losses. Specifically, the simulation results show that, when the failure occurs at the higher layers, the EHOT approach allows a traffic losses reduction of about the 70% with respect to the HOT approach.

The RPR protection mechanisms, although very efficient and fast, provoke the substantial reduction of the available bandwidth. As further study, we are currently investigating the use of the automatic switching capability provided by the ASON/GMPLS paradigm to face with such bandwidth reduction in order to carry out the logical reconfiguration of RPR networks in order to track the client traffic dynamic fluctuations.

REFERENCES

[1] D. Wang, K.K. Ramakrishnan, Ch. Kalmanek, “Congestion Control in Resilient Packet Rings”, Proceedings of 12^{th} IEEE International Conference on Network Protocols (ICNP’04).

[2] F. Alharbi, N. Asari, „Distributed Bandwidth Allocation for Resilient Packet Ring Networks”, Computer Networks, Manuscript Draft.

[3] S. Spadaro, J. Solé-Pareta, D. Careglio, K. Wajda, A. Szymański, “Positioning of RPR standard in contemporary operator’s environment”, IEEE Network, March 2004.

[4] Official IEEE 802.17 Web site: http://www.ieee802.org/17/.

[5] 802.17 IEEE Standard, June 2004.

[6] V. Gambiroza, P. Yuan, L. Balzano, Y.Liu, S. Sheafor, E. Knightly, “Design, Analysis, and Implementation of DVSR: A Fair, High Performance Protocol for Packet Rings”, IEEE/ACM Transactions o Networking, 2004.

[7] X. Zhang, H. Ghandehari, G. Yip, N-W Ma, K. Raahemifar, „Fuzzy Logic Control in RPR Network”, CCECE 2004 – CCGEI 2004 IEEE.

[8] ITU-T Rec. G.872, “Architecture of Optical Transport Networks”, February 1999.

[9] J. Lang, “Link Management Protocol (LMP)”, IETF draft draft-ietf-ccamp-lmp-10.txt, October 2003.