RESEARCH

Applying p-cycle Protection Approach for a Reliable IPTV Service in IP-over-DWDM Networks

Ahmed Frikha*, Bernard Cousin and Samer Lahoud

Abstract

Today, IPTV service has become very popular and service providers must deal with the rapid growth of IPTV customers. Service providers must also ensure the IPTV reliability to satisfy the customer's needs, as one network failure could disrupt the IPTV transmission. In addition, a reliable IPTV service requires service providers to ensure link and router failure recovery within a fast restoration time.

One important key issue for providing a reliable IPTV service, is survivable multicast routing. Generally, most of the carriers route the multicast traffic using the multicast protocol PIM-SSM based on the routing information provided by the Interior Gateway Protocol (IGP). Restoration using IGP reconfiguration at the IP layer requires IGP to be aware of the failure. After that, PIM-SSM can use the new IGP shortest paths to rebuild a new multicast tree using the prune and join process. This operation is slow, and typically takes from 10 to 60 seconds. To avoid the multicast tree rebuilding and ensure a fast restoration, we consider node and link failure recovery in the DWDM layer. The backup path is provided in this layer. Thus, the multicast tree does not change at the IP layer (logical links do not change) and restoration time is faster.

The *p*-cycle protection approach enables node and link failure recovery in the DWDM layer while maintaining a fast restoration time (typically in the order of 50-80 ms). Moreover, the *p*-cycle protection approach achieves an efficient use of the network capacity compared to the other protection approaches such as the one-plus-one (1+1) and the one-by-one (1:1) restoration methods.

In this paper, we apply *p*-cycles in IP-over-DWDM networks to provide a robust IPTV service. In addition, we propose a novel concept for node protection using *p*-cycles to achieve more efficient resource utilization. We also propose a new algorithm, named node and link protecting candidate *p*-cycle based algorithm (NPCC). This algorithm integrates our new concept for the node protection. Extensive simulations show that our proposition outperforms the existing approaches in terms of blocking probability, resource utilization efficiency, and computational time rapidity.

Keywords: IPTV service; multicast routing; IP-over-DWDM networks; reliability; *p*-cycles; node and link protection

1 Introduction

Nowadays, many telecom companies offer the IPTV (Television over IP) service and distribute TV channels using backbone networks. The IPTV service requires stringent Quality of Service (QoS) constraints (such as packet loss, jitter, and end-to-end delay) to satisfy the customer's needs. Service providers must also ensure the reliability of the IPTV service. A simple link or router failure could disrupt the TV content distribution for several seconds, if no protection mechanism is implemented.

*Correspondence: Ahmed.frikha@ahmedfrikha.com

IRISA, University of Rennes 1, Campus universitaire Beaulieu, 35042 Rennes, France

Full list of author information is available at the end of the article

IPTV contents could be carried using the IP multicast to save bandwidth capacity. In fact, multicasting enables a single packet to be sent to multiple destinations at once. Although many multicast routing algorithms are proposed for the IPTV service, most of the carriers today implement the Protocol Independent Multicast Source Specific Mode (PIM-SSM) [1]. For many reasons, this protocol has proved its efficiency for Internet broadcast-style applications such as IPTV. Obviously, PIM-SSM is simple to implement for network operators thanks to the Source Specific Mode (SSM) [1], which makes this protocol ideal for the IPTV service. The Source Specific Mode does not require the network to maintain knowledge about which sources are actively sending multicast traffic contrar-

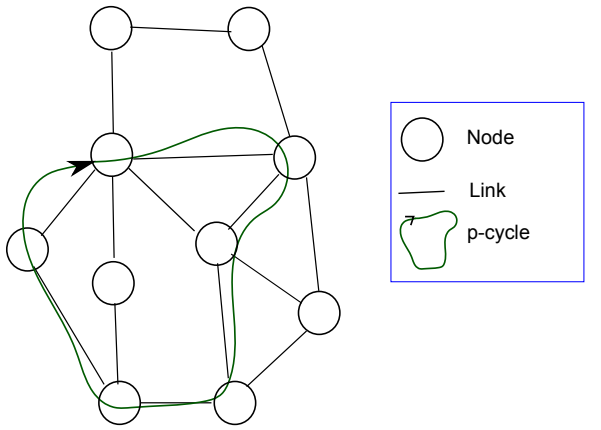

Figure 1 An example of p-cycle

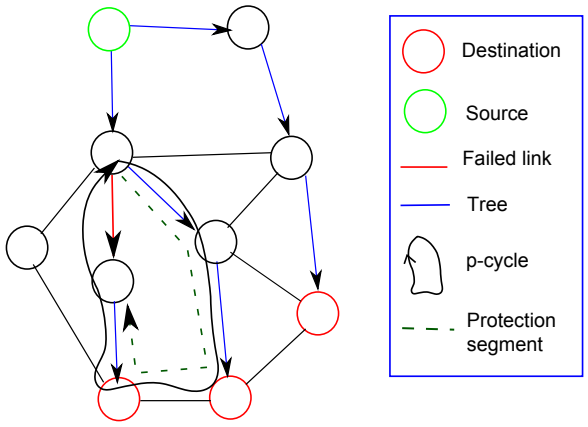

Figure 2 On-cycle link protection

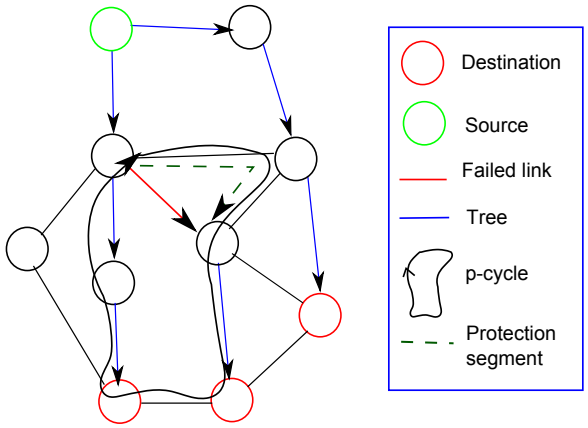

Figure 3 Straddling link protection

ily to the Internet Standard Multicast (ISM) protocol. This advantage makes PIM-SSM more scalable than ISM.

To ensure IPTV reliability, survivable multicast routing must be guaranteed. Moreover, service providers must ensure a fast restoration time for link and router failure recovery. The PIM-SSM protocol uses the routing information provided by the Interior Gateway Protocol (IGP) to compute a multicast tree. Thus, restoration at the IP layer using IGP reconfiguration requires IGP to be aware of the failure, after that PIM-SSM can use the new IGP shortest paths to rebuild a new multicast tree using the prune and join process. This operation is slow, and typically takes from 10 to 60 seconds [2]. To avoid the multicast tree rebuilding and ensure a fast restoration, we consider node and link failure recovery at the DWDM layer. The backup path is provided at this layer. This makes restoration time faster as the multicast tree does not change at IP layer (logical links do not change).

The p-cycle protection approach was introduced by W.D. Grover [3] for link failure recovery at the DWDM layer. Concretely, a p-cycle is cycle-oriented spare capacity pre-configured at the DWDM layer. In Fig.1 we show an example of p-cycle in an optical network. We note that a p-cycle does not traverse a node or a link more than one time. Moreover, a p-cycle is oriented. The advantage of using p-cycles for protection can be summarized in two main points. First, p-cycles ensure a fast restoration time (typically in the order of 50-80 ms) as the protection is done at the DWDM layer and p-cycles are pre-configured [4]. Second, the p-cycle protection approach can achieves an efficient use of the network capacity compared to the other protection approaches such as the one-plus-one (1+1) and the one-by-one (1:1) restoration methods. In fact, a p-cycle can protect both on-cycle links and straddling links. An on-cycle link belongs to the p-cycle, and is directed oppositely to the p-cycle. In Fig.2, we show an example of an on-cycle link protected using a p-cycle. The on-cycle link is represented using a red line and the protection segment provided by the p-cycle is represented using a dashed green line. In this figure, we see that the p-cycle and the failed link have opposite directions. A straddling link does not belong to the p-cycle. However, its extremity nodes are traversed by the p-cycle. The p-cycle provides two protection segments: one protection segment for each directed-link. In Fig.3, we show an example of a straddling link protected using a p-cycle. In this figure, we represent the protection segment which protects the directed-link used by the light-tree. The protection segment of the opposite direction of the link is not represented in this figure. This characteristic of p-cycles allows us to reduce the required backup bandwidth capacity.

The p-cycles technique was extended for supporting node protection in DWDM layer using the node en-

circling p-cycle concept (NEPC) [5]. According to this concept, a protecting p-cycle of a given node must link all neighbor nodes of the failed node. This constraint is too hard. It could discard some nodes that are able to be protected by the p-cycle but they do not satisfy the constraint. This will affect the efficiency of p-cycles in terms of capacity saving.

In this paper, we consider link and node failure recovery at the DWDM layer using p-cycles. We extend the node protection concept of the p-cycle approach to achieve more efficient resource utilization. Then, we propose a novel algorithm, named node and link protecting candidate p-cycle based algorithm (NPCC). The NPCC algorithm integrates our proposed concept for the node protection. This algorithm ensures node and link failure recovery based on a set of candidate p-cycles to overcome the high computational time problem.

The rest of this paper is organized as follows. In section 2, we present the IPTV architecture and discuss the restoration mechanisms to ensure a reliable IPTV service. In section 3, we extend the p-cycle protection concept for protecting nodes in light trees. In section 4, we present our novel algorithm for combined node and link failure recovery that deploy the novel node protection concept. Extensive simulations and numerical results are presented in section 5. The conclusions are given in section 6.

2 IPTV architecture and restoration mechanisms

In this section, we present the main components of the IPTV architecture and we give an example. Then, we discuss the restoration mechanisms, and we highlight the advantages of applying the p-cycle protection approach for IPTV.

2.1 IPTV architecture

An IPTV architecture includes mainly [2]-[6]:

- A super headend (SHE): The SHE is located in the core network, called also IPTV backbone, it collects television content from TV networks, such as satellites and off-air distributions. After video processing, encoding, and management, the SHE distributes the TV content using IP routers to multiple video hub offices (VHOs).
- A video hub office (VHO): A VHO receives the IPTV content transmitted by the SHO through the IPTV backbone routers. Then, it combines this content with the local television and the video on demand (VoD) contents. The SHE routers and the VHO routers and the links that connect them form the IPTV backbone. Each VHO in turn serves a metro area by transmitting the IPTV content to multiple video serving offices (VSOs).
- A video serving office (VSO): A VSO contains the aggregation routers that aggregate local loop traffic from subscriber homes, i.e., local digital subscriber line access multiplexers (DSLAMs).

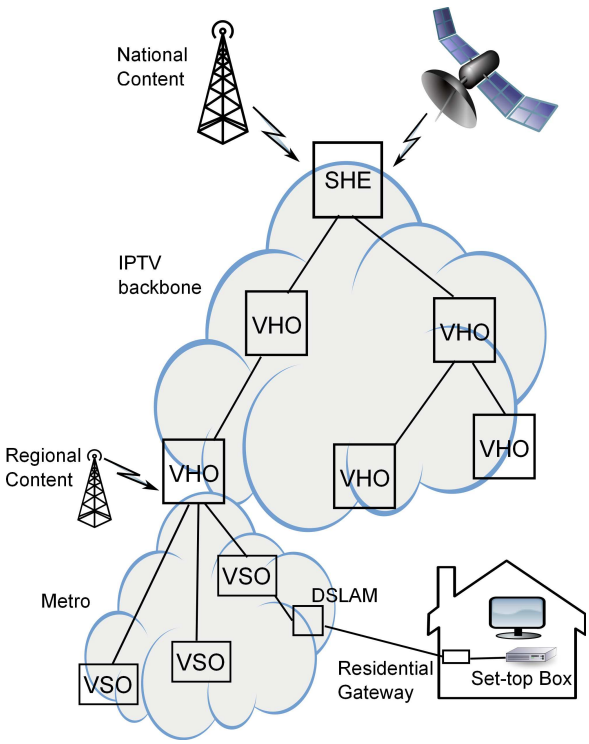

Figure 4 Example of an IPTV architecture

A simplified example of an IPTV architecture is illustrated in Fig. 4. In this example, the super headend (SHE) gathers the national channel content from the off-air and the international channel content from satellites. Then, it sends this content to multiple video hub offices (VHOs) using IP multicast and through the underlying DWDM layer. IP multicast is very important to save network bandwidth as it allows a packet to traverse a link once to reach multiple destinations. In the example, we did not represent the traversed IP routers that connect the SHE to each VHO. A home with a TV and a set-up box is shown in Fig. 4. The set-up box is connected via a residential gateway to a DSLAM, connected in turn to a video serving office.

The Protocol Independent Multicast Source Specific Mode (PIM-SSM) is largely deployed for IPTV video distribution in IPTV backbone. A multicast tree is computed by this protocol based on the routing information provided by the Interior Gateway Protocol (IGP). The multicast tree is used to deliver IPTV content from the SHE to each VHO. Each TV channel is assigned to a unique multicast group.

The IPTV service requires a high bandwidth and stringent quality of service constraints. In particular, IPTV is very sensitive to the packet loss, as one lost packet could disrupt the video quality. The delay and the jitter are also critical for the quality of the IPTV service. These three QoS constraints are involved by the network dependability. Precisely, a link or node failure could disrupt the IPTV service, if no restoration mechanism is considered for the multicast tree.

2.2 Restoration mechanisms

With IGP reconfiguration, after a link or node failure, PIM-SSM must rebuild the multicast tree. But before that, IGP must be aware of the failure and compute the new shortest paths at the level of each router. PIM-SSM will use these new shortest paths to rebuild the multicast tree using the prune and join process. This approach is not suitable with the real-time aspect of the IPTV service as it takes too much time for the restoration process, typically between 10 and 60 seconds [2]. With the MPLS Fast Reroute (FRR) protection approach, the restoration time can be reduced to be between 50 ms and 100 ms [2]. Backup LSPs are pre-established, and stored in the router forwarding tables that make fast rerouting possible at the IP MPLS layer.

Some other restoration mechanisms are applied at the DWDM layer and can achieve lower restoration time. The one-plus-one (1+1) and the one-by-one (1:1) restoration methods can be implemented at the DWDM layer. The restoration time of these approaches is lower than 20 ms [2]. However, they are not efficient in terms of bandwidth saving, as backup paths cannot be shared. In these approaches, a backup path is dedicated for one and only one working path. The p-cycle protection approach, described in the previous section, ensures node and link failure recovery while maintaining a fast restoration time (typically in the order of 50-80 ms)[4]. Moreover, this approach achieves an efficient use of the network capacity compared to the other protection approaches.

These restoration mechanisms are proposed for unicast traffic. Some other restoration mechanisms focus on protecting multicast trees against network failures. In 2009, F. Zhang and W.D. Zhong proposed the efficiency-score based heuristic algorithm of node and link protecting p-cycle (ESHN) [7]. Although the ESHN algorithm has the lowest blocking probability among the OPP-SDP algorithm [8] and the ESHT algorithm [9] in dynamic multicast traffic, ESHN does not use efficiently the protection capacity provided by a p-cycle, especially when protecting nodes. Precisely, the ESHN algorithm does not take in consideration all nodes that a p-cycle can protect, when selecting a protecting p-cycle. This is due to the two hard constraints imposed by the concept deployed by ESHN for protecting nodes. The first constraint imposes that a node protecting p-cycle has to link all one level downstream nodes of the failed node. The second constraint imposes that the p-cycle must contain one of the upstream nodes of the failed node in the light tree. Of course this concept reduces the computation time of the algorithm as it limits the search space of the p-cycles. However, it prevents the ESHN algorithm to achieve the best resource utilization. Furthermore, when traffic load is high, the computational time of the ESHN algorithm remains high and does not deal with the IPTV service requirements.

In this work, we focus on the design of a reliable IPTV service. we consider the link and node failure recovery at the DWDM layer to enable a low restoration time. We use p-cycles to ensure an efficient use of the network capacity. We also extend the node protection concept of the p-cycle approach to achieve more efficient resource utilization. In section 3, we provide a detailed study of the node protection using p-cycles and we present our proposed concept for protecting nodes in light-tree.

3 Node protection using p-cycles

3.1 Existing approaches for node protection using p-cycles

In this section, we present some existing well-known concepts for node protection using p-cycles.

The node encircling p-cycle concept (NEPC) [5] was proposed for node protection using p-cycles. Fig.5 illustrates an example of node protection using this concept. The p-cycle must traverse all neighbor nodes of the failed node to protect it. The drawback of this concept is that in some cases finding such a p-cycle is not possible. Moreover, some p-cycles that do not meet this constraint could protect the failed node while reserving less spare capacity. The constraint imposed by this concept is too hard and prevents the protection algorithms to achieve good resource utilization.

Some existing works that ensure link and node failure recovery in multicast session, simplify the node protection concept to reduce the computational time of the algorithm. For example, in the ESHN algorithm, the p-cycle has to link 1) all one level downstream nodes of the failed node and 2) one of its upstream nodes in the light tree. Fig. 6 illustrates a simple example for protecting a node using the ESHN algorithm. In this example, the failed node (or protected node) is represented by a grey circle, the source node by a green circle, the destination nodes by red circles and the multicast tree by a blue line. The p-cycle links the two one level downstream nodes of the failed node (nodes belonging to the Tree) and the source node (upstream

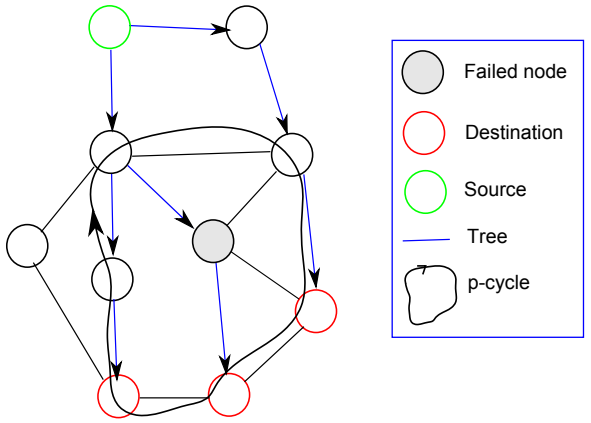

Figure 5 Node encircling p-cycle concept (NEPC)

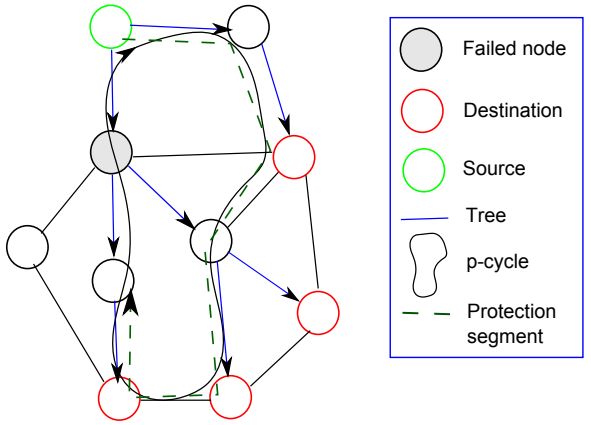

Figure 6 Protecting a node using the ESHN algorithm

node of the failed node). Thus, the p-cycle satisfies the constraints and could protect the failed node. Upon the node failure the source node detects the failure and reroute the multicast traffic through the protection segment (dashed green line). Although this approach relaxes the constraint imposed by the NEPC concept, the protection capacity provided by a p-cycle is still not used efficiently as some p-cycles could protect a node without meeting the first or second constraints of this approach.

3.2 The proposed concept for node protection using p-cycles

In this section, we present our novel concept for protecting nodes in multicast traffic. Before presenting our concept, let us introduce some notations. Let T be a multicast light-tree to be protected, s be the source node in T, N_f be an intermediate node in T, and $D = \{d_1, d_2, .., d_i\}$ be the set of destinations in T that are affected when a failure occurs on the node N_f.

Theorem:
A p-cycle C_j in the network can protect the node N_f if and only if it exists a protection segment $[N_a, N_e] \in C_j$ such that:

1 The node $N_a \in T$, the node $N_e \in T$, and $N_f \notin [s, N_a]$ where $[s, N_a]$ is the segment in T linking the source s to the node N_a.
2 $\forall d_k \in D$, $\exists$ a node $N_k \in [N_a, N_e]$ and $N_k \in]N_f, d_k]$, where $]N_f, d_k]$ is the segment in T linking N_f to d_k.
3 $N_f \notin [N_a, N_e]$.

Proof:
Once a failure occurs on the node N_f, the multicast traffic is rerouted through the p-cycle C_j to ensure the survivability of the multicast session. For that, the p-cycle must provide a protection segment to deliver the multicast content to all destinations that are affected by the failure of N_f. This segment is denoted by $[N_a, N_e]$.

First, we justify why the constraint (1) is required. The extremities N_a and N_e of this segment must be in T. In fact, the node N_a is responsible of injecting the multicast traffic in the protection segment $[N_a, N_e]$ when N_f fails. In addition, N_a must not be affected by the failure of N_f, *i.e.*, N_a continues to receive the multicast traffic even if a failure occurs on node N_f ($N_f \notin [s, N_a]$). The node N_a must split the incoming light signal into two outgoing signals. The first one is injected in the protection segment and the second one is forwarded to the downstream node of N_a in the light-tree T. The node N_e is the last intersection node between T and C_j.

Second, we prove the necessity of the constraint (2). To ensure failure recovery, we must make sure that all destinations affected by the failure of N_f continue to receive the multicast traffic through the protection segment $[N_a, N_e]$. Two scenarios are possible to deliver the multicast traffic to an affected destination d_k. In the first one, the segment $[N_a, N_e]$ carries the multicast traffic directly to d_k, *i.e.*, the protection segment traverses the node d_k. In the second scenario, the segment $[N_a, N_e]$ carries the traffic to the destination through an intermediate node N_k. The node N_k must be an upstream node of d_k and a downstream node of N_f in light-tree. This constraint ensures that the failed node N_f does not belong to the segment $[N_k, d_k]$ of the light-tree. The node N_k splits the incoming signal into two signals. The first one is sent to the next node in the protection segment to ensure that the remaining affected destinations will receive the multicast content. The second one is forwarded to the downstream node of N_k in the light-tree to reach d_k.

Finally, we prove that the constraint (3) is necessary. We must make sure that the protection segment is not

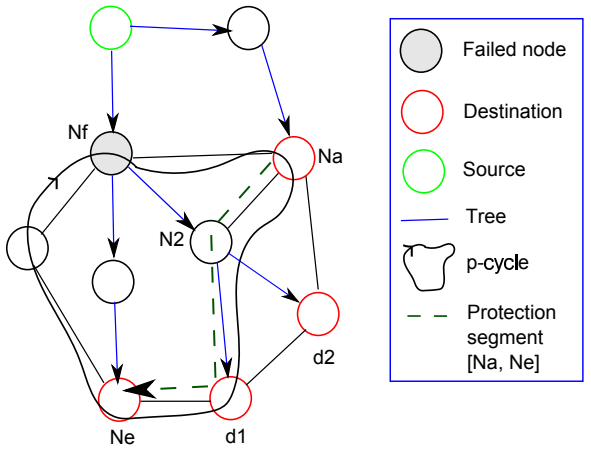

Figure 7 Protecting a node using the proposed concept

affected by the failure of N_f. Therefore, the protection segment $[N_a, N_e]$ should not traverse the node N_f.

3.3 Example

In Fig.7, we provide an example of a p-cycle that can protect the node N_f based on our concept. The set of destinations affected by the failure of N_f is $D = \{d_1, d_2, N_e\}$. This p-cycle has two original characteristics that other node protection concepts [5]-[7] do not have. First, it can traverse the protected node. Second, it is not mandatory to traverse all affected destinations or neighboring nodes of the protected node. The p-cycle provides a protection segment represented with a dashed green line in the figure. The node N_a activates the p-cycle by injecting the multicast traffic into the protection segment $[N_a, N_e]$. This segment carries the traffic to d_2 through the intermediate node N_2, and to d_1 and N_e directly as it traverses them.

4 The proposed protection algorithm

In this section, we present our proposed algorithm NPCC for protecting node and link in DWDM layer for a reliable IPTV service. Our algorithm deploys the aforementioned concept for node protection using p-cycles.

4.1 The candidate p-cycle selection

First, the NPCC algorithm enumerates a set of candidate p-cycles in an offline phase, i.e. before the reception of any requests. Using this candidate p-cycles will reduce considerably the computational time of the algorithm. In fact, considering the total p-cycle set when selecting a new p-cycle to be established, is a very slow task, especially when the number of p-cycles in the network is high. Therefore, we select a set of candidate p-cycles to reduce the computational time of our algorithm.

To select a candidate p-cycle set, we define a new score, named protection capacity PC, for each p-cycle in the network. This score is computed in advance for each unity-p-cycle before routing the requests. A unity-p-cycle is a p-cycle in the network that reserves only one bandwidth unity (e.g. one wavelength) on each traversed link. The score PC of a unity-p-cycle C_j, specified by equation (1), is defined as the ratio of the largest amount of link capacity on the network LC_j that C_j can protect over the spare capacity required for setting up C_j. $|C_j|$ is given by the number of links traversed by C_j.

$$PC(C_j) = \frac{LC_j}{|C_j|} \tag{1}$$

A p-cycle with a high PC, is useful as it maximizes the amount of protected capacity while reserving less spare capacity. The l p-cycles with highest PC are selected as candidate p-cycle set, where l is a parameter for the algorithm. The goal of selecting this set is to maximize the capacity that can be protected on the network.

4.2 The flow chart of the NPCC algorithm

Fig. 8 presents the flow chart of the NPCC algorithm. Let us introduce some notations before detailing the operation performed by this algorithm. Let us consider a multicast request and its corresponding light-tree T. The light-tree is constructed using the PIM-SSM [1] multicast routing protocol. Let L denote the set of links in T and N denote the unprotected intermediate node in T. The links in T that can be protected by the existing p-cycles in the network are removed from L and the nodes in T that are protected the existing p-cycles are removed from N. Note that the existing p-cycles are previously established to protect other light trees in the network. If $L \neq \phi$ or $N \neq \phi$, the algorithm computes new p-cycles to protect the remaining unprotected links in L as well as the remaining unprotected nodes in N.

To select a new protecting p-cycle, the algorithm uses the ES-based unity-p-cycle procedure. In this procedure, we deploy the same efficiency-score (ES) used in the ESHN algorithm to measure the efficiency of each p-cycle in the candidate p-cycle set. This score adapts the efficiency-ratio based unity-p-cycle heuristic algorithm (ERH) [15] to deal with node and link failures in multicast traffic. This score takes in consideration the highest number of unprotected nodes as well as the highest number of unprotected links in the multicast tree that a unity-p-cycle can protect. Let C_j be a unity-p-cycle in the network. The score ES of

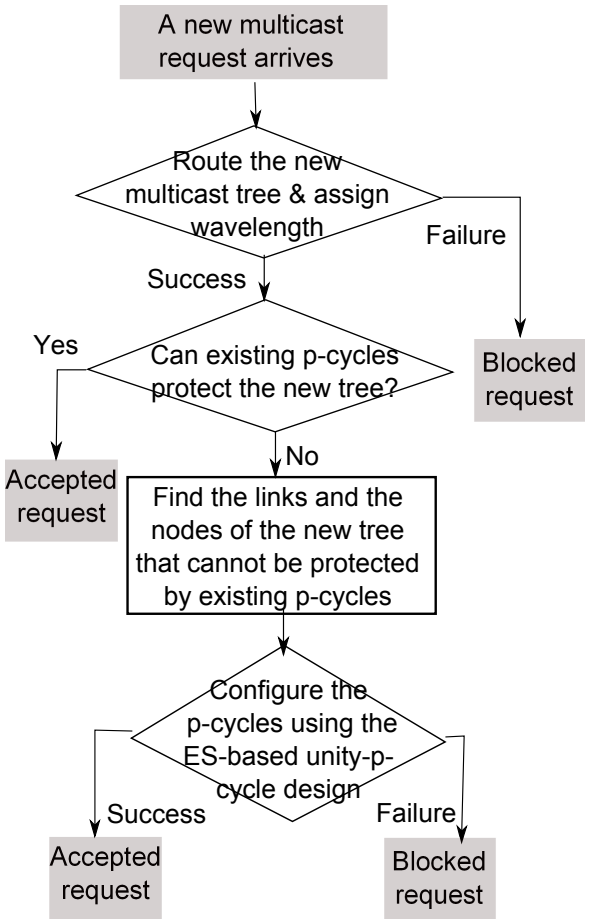

Figure 8 Flow chart of the NPCC algorithm for combined node and link failure recovery in dynamic multicast traffic

C_j is given by equation (2), where $W_{j,L}$ is the highest number of unprotected links in L that C_j can protect, $W_{j,N}$ is the highest number of unprotected nodes in N that C_j can protect, and $|C_j|$ is the spare capacity required for setting up a unity-p-cycle C_j. $|C_j|$ equals the number of links traversed by C_j

$$ES(C_j) = \frac{W_{j,L} + W_{j,N}}{|C_j|} \quad (2)$$

The ES-based unity-p-cycle procedure calculates the score ES of each unity-p-cycle in the candidate p-cycle set and selects the p-cycle with maximum ES. The set of links protected by the selected unity-p-cycle is removed from L and the set of protected nodes is removed from N. This process is iterated until all the links and all the nodes of T are protected, i.e. $L = \phi$ and $N = \phi$. The selected unity-p-cycles are configured and the corresponding wavelengths are reserved. Note that the reserved p-cycles may serve to protect next coming multicast requests. This is why after routing a multicast tree, we compute the set of links in L and the set of nodes in N that can be protected by the existing p-cycles in the network. Finally, the reserved capacity of an existing p-cycle in the network is released when the p-cycle does not protect any working link and nodes in the network.

5 Performance Evaluation

In this section, we evaluate our algorithm NPCC proposed for providing the reliable IPTV service. Our proposition guarantees the link and node failure recovery at the DWDM layer and maintains a fast restoration lime. We compare our algorithm with the ESHN algorithm, which was reported to be the most efficient algorithm for dynamic multicast traffic protection in terms of resource utilization efficiency and blocking probability.

In our simulation, we assume that the request arrival follows a Poisson process with an average arrival rate λ, and the request holding time follows an exponential distribution with an average holding time μ. Hence, the network offered traffic load is given by $\lambda\mu$.

We run simulations on the following well known and very often used European optical topologies developed within the COST-266 [16] and COST-239 [17] projects:

- The COST-266 core topology [16] contains 16 nodes and 23 links, with an average nodal degree equals to 2.88. The total number of p-cycles in this topology equals 236 (118 p-cycles in each direction).
- The COST-239 topology [17] contains 11 nodes and 26 links, with an average nodal degree equals to 4.727. The total number of p-cycles in this topology equals 5058 (2029 p-cycles in each direction).

In our study, without lack of generality we assume that each link has two fibers. The two fibers transmit in opposite directions; 16 wavelengths are available on each fiber. The source and the destinations of each multicast session are randomly selected (uniform distribution law). We choose the number of destinations in each multicast request $D = 5$, which seems to be reasonable as the total number of nodes in the used topologies is lower than 16 nodes. We compare the performance of the algorithms according to the following performance criteria:

- The Blocking Probability (BP) represents the percentage of requests that cannot be routed or protected among the total number of requests.
- The Resource Utilization (RU) represents the percentage of reserved wavelengths in the network among the total number of wavelength links.

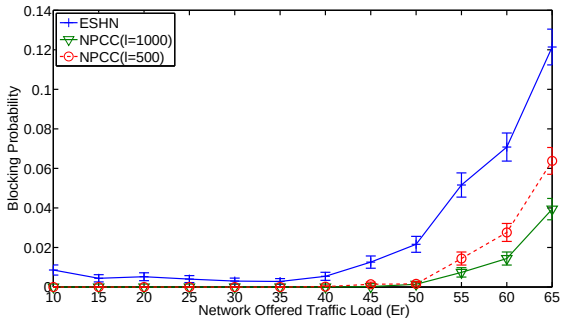

Figure 9 Comparison of the blocking probability BP in the COST-239 network.

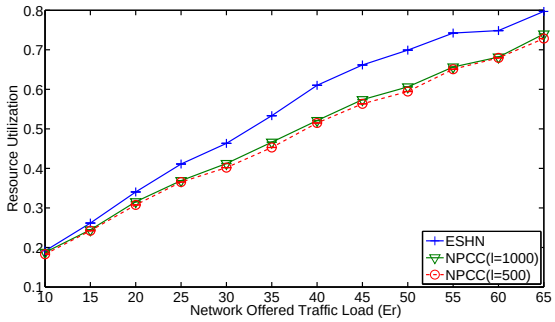

Figure 10 Resource utilization RU comparison in the COST-239 network.

$RU = \frac{W_R}{E*W}$, where W_R represents the total number of wavelength links reserved in the network, E represents the number of fiber in the network, and W the number of wavelengths per fiber.

- The average Computational Time (CT) required for routing and protecting a traffic request.

Performance criteria BP, RU, and CT are computed according to the traffic load. For each traffic load value, 5×10^5 requests are generated. This number of requests is enough to measure BP, RU, and CT, with a 95% confidence interval.

First, we consider the COST-239 topology. The total number of p-cycles in this topology equals 5085 p-cycles. We run the NPCC algorithm with two different values for the number of candidate p-cycles, respectively $l = 1000$ and $l = 500$. The blocking probability measured on the COST-239 network is represented in Fig. 9. For all the algorithms, the blocking probability increases when the traffic load is high. The NPCC algorithm, with both $l = 1000$ and $l = 500$, outperforms the ESHN algorithm having a lower blocking probability, especially when traffic load is high. The NPCC algorithm with $l = 1000$, has the lowest blocking probability. When $l = 500$, the blocking probability of NPCC increases but remains lower than that of ESHN. This is because $l = 500$ is very low compared to the total number of p-cycles in the COST-239 network which is equal to 5058 p-cycles, and this will increase BP.

Fig. 10 shows the resource utilization of the algorithms. When the traffic load increases, the percentage of wavelengths reserved per link is higher for each algorithm. The percentage of wavelength reserved by NPCC with $l = 1000$ and NPCC with $l = 500$ are very close. This percentage is very low compared with that of the ESHN algorithm, especially when the traffic load is high. For a traffic load equals 65 Erlang, almost 70% of the wavelengths on each link are reserved for the NPCC algorithm and 80% for the ESHN algorithm.

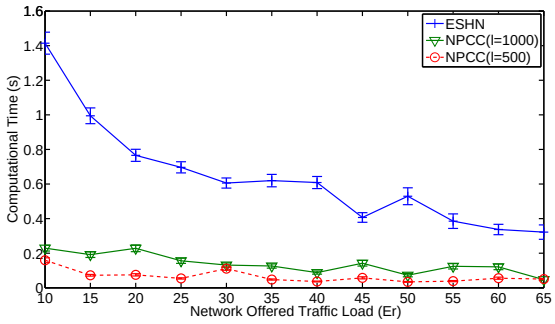

Figure 11 Comparison of the average computational time CT for setting up a multicast request in the COST-239 network.

To assess the rapidity of our proposed algorithm, we focus on the average computational time CT for setting up a multicast request. Fig. 11 illustrates the value of CT for each algorithm, measured in the COST-239 network according to the network traffic load. As shown in this figure, the NPCC algorithm with $l = 500$ has the lowest computational time among the NPCC algorithm with $l = 1000$ and the ESHN algorithm. This is due to the low number of p-cycles considered for the protection ($l = 500$). The average computational time CT of the NPCC algorithm with both $l = 500$ and $l = 1000$ is very low compared with that of the ESHN algorithm. The NPCC algorithm outperforms the ESHN algorithm in terms of blocking probability, resource utilization and computational time.

Now, we consider the COST-266 topology. The total number of p-cycles in this topology equals 236 p-cycles. We run the NPCC algorithm with two different values for the number of candidate p-cycles, respectively $l = 236$ and $l = 200$.

Fig. 12 illustrates the blocking probabilities measured in the COST-266 network. The connectivity of this topology is very low (2.88). Therefore the block-

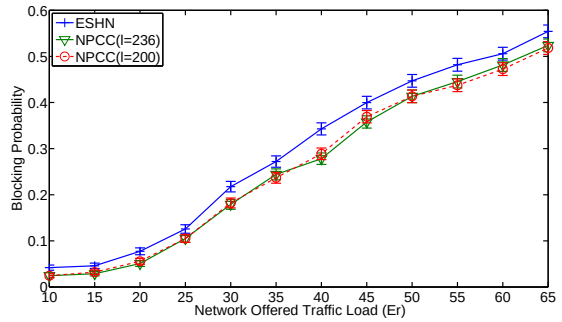

Figure 12 Comparison of the blocking probability BP in the COST-266 network.

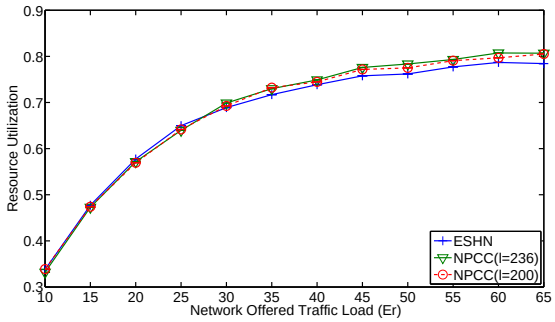

Figure 13 Resource utilization RU comparison in the COST-266 network.

ing probabilities of the algorithms are very high compared with that measured in the COST-239 topology for the same network traffic load values. For all the algorithms, the blocking probability increases rapidly with the traffic load values increasing. The ESHN algorithm has the highest blocking probability among the NPCC algorithm with $l = 236$ and the NPCC algorithm with $l = 200$. The blocking probability of NPCC with $l = 236$ and the blocking probability of NPCC with $l = 200$ are very close since the values of l are close.

Fig. 13 shows the resource utilization of the algorithms in the COST-266 topology. The percentage of wavelength reserved by the algorithms is almost the same. The percentage of reserved wavelengths per link increases with the traffic load increasing.. We note that the resource utilization of the ESHN algorithm is slightly lower than that of our algorithm NPCC when traffic load is higher than 35 Erlang. This is because the blocking probability is high. In other words, the probability of the rejected requests for ESHN increases, and there is no resource reservation for the rejected requests. This will decrease the resource utilization of ESHN.

6 Conclusion

In this work, we focused on the reliability of the IPTV service. First, we presented the main components of the IPTV architecture, then we discussed the existing restoration mechanisms in the IP and in the DWDM layers. The restoration methods proposed for the DWDM are more efficient and more suitable for IPTV in terms of restoration time rapidity. We also highlighted the advantage of applying the p-cycle protection approach to reach a reliable IPTV service.

Second, we extended the concept of node protection using p-cycles to deal with multicast traffic. Our novel concept allows the protection capacity provided by a p-cycle to be used efficiently. We proposed a novel algorithm, named NPCC, which deploys our concept for the node protection. The NPCC algorithm ensures both link and node failure recovery for a dynamic multicast traffic in the DWDM layer. This algorithm speeds up the computational time of setting up a multicast traffic request by enumerating a set of candidate p-cycles based on the score PC.

Finally, we compared our proposed algorithm with the ESHN algorithm, which was reported to be the most efficient algorithm for node and link failure recovery in dynamic optical multicast traffic. Extensive simulations showed that the NPCC algorithm achieves the lowest blocking probability and outperforms the ESHN algorithm in terms of resource utilization efficiency and computational time rapidity.

References

1. S. Bhattacharyya, et al., An Overview of Source-Specific Multicast (SSM), *IETF RFC 3569*, July 2003.
2. R. Doverspike, K. K. Ramakrishnan, and C. Chase, Structural overview of ISP networks. In *Guide to Reliable Internet Services and Applications* (C. Kalmanek, S. Misra, and R. Yang), Springer, 2010.
3. W. D. Grover and D. Stamatelakis, Cycle-oriented distributed preconfiguration: ring-like speed with mesh-like capacity for self-planning network restoration, *in proceedings of IEEE ICC,* 1998.
4. M. Clouqueur, and W. D. Grover, Availability analysis and enhanced availability design in *p*-cycle-based networks, *Photonic Network Communications,* Vol. 10, no. 1, pp. 55-71, 2005.
5. J. Doucette, P. A. Giese, W. D. Grover, Combined Node and Span Protection Strategies with Node-Encircling *p*-cycles, *in proceedings Workshop on Design of Reliable Communication Networks (DRCN), Ischia (Naples), Italy,* pp. 213-221, 2005.
6. Cisco Systems White Paper, Optimizing Video Transport in your IP Triple Play Network, 2006, http://www.cisco.com.
7. F. Zhang and W. D. Zhong, Performance evaluation of optical multicast protection approaches for combined node and link failure recovery, *J. Lightw Technol.,* vol. 27, no. 18, pp. 4017-4025, 2009.
8. N. K. Singhal, L. H. Sahasrabuddhe, and B. Mukherjee, Provisioning of survivable multicast sessions against single link failures in optical WDM mesh networks, *J. Lightw. Technol.,* vol. 21, no. 11, pp. 2587-2594, 2003.
9. F. Zhang, and W. D. Zhong, *p*-cycle based tree protection of optical multicast traffic for combined link and node failure recovery in WDM mesh networks, *IEEE Commun. Lett.,* vol. 13, no. 1, pp. 40-42, 2009.

10. N. K. Singhal, C. Ou, and B. Mukherjee, Cross-sharing vs. self-sharing trees for protecting multicast sessions in mesh networks, *in proceedings Comput. Netw.*, vol. 50, no. 2, pp. 200-206, 2006.
11. M. Y. Saidi, B. Cousin, M. Molnar, Improved Dual-Forest for Multicast Protection, *in proceedings 2nd Conference on Next Generation Internet Design and Engineering Conference, Valencia, Spain,*, pp. 371-378, Apr. 2006.
12. M. Medard, S. G. Finn, R. A. Barry, and R. G. Gallager, Redundant trees for preplanned recovery in arbitrary vertex-redundant or edge-redundant graphs, *IEEE/ACM Trans, Netw.*, vol. 7, no. 5, pp. 641-652, Oct. 1999.
13. T. Rahman and G. Ellinas, Protection of multicast sessions in WDM mesh optical networks, *in proceedings OFC'05, Anaheim, CA,* p. 3, Mar. 2005.
14. P. Leelarusmee, C. Boworntummarat, and L. Wuttisittikulkij, Design and analysis of five protection schemes for preplanned recovery in multicast WDM networks, *in proceedings IEEE SAWWC' 04, Princeton, NJ,* pp. 167-170, Apr. 2004.
15. Z. R. Zhang,W. D. Zhong, and B. Mukherjee, A heuristic method for design of survivable WDM networks with *p*-cycles, *IEEE Commun. Lett.,* vol. 8, pp. 467-469, 2004.
16. S. De Maesschalck et al., Pan-European Optical Transport Networks: an Availability based Comparison, *Photonic Network Communications,* Vol. 5, no. 3, pp. 203-226, 2003.
17. P. Batchelor et al.: Ultra High Capacity Optical Transmission Networks. *Final report of Action COST 239,* 1999.