Improving Reliability in Multi-Layer Networks With Network Coding Protection

W. Ramirez*†, X. Masip-Bruin*, E. Marin-Tordera*, M. Yannuzzi†, M.S. Siddiqui*†, A. Martinez*†, V. Lopez‡

*Advanced Network Architectures Lab (CRAAX), Technical University of Catalonia (UPC), Spain

†Networking and Information Technology Lab (NetIT Lab), Technical University of Catalonia (UPC), Spain

Emails: {wramirez, xmasip, eva, yannuzzi, siddiqui, annym}@ac.upc.edu

‡Telefonica I+D, Spain, vlopez@tid.es

***Abstract*—A major concern among network providers is to endow their networks with the ability to withstand and recover from failures. In recent years, there is a trend in network research referred to as Network Coding Protection (NCP). NCP combines the use of network coding techniques with a proactive protection scheme with the aim of improving network reliability. Although today's network backbone is a multi-layer network formed by the convergence of IP/MPLS and Optical technologies, the information available in the literature related to the performance of NCP schemes in multi-layer network scenarios is yet scarce. In this paper, we propose a novel NCP scheme referred to as DPNC+. The novelty of DPNC+ is that it exploits cross-layer information in order to improve the reliability of multi-layer (IP/MPLS over Optical) networks against link failures. Our evaluation results show that reduction up to 50% –related to protection cost– can be obtained when using the proposed scheme compared to conventional proactive protection techniques.**

***Index Terms*—Multi-Layer networks, Network Coding Protection, Cross-Layer Information.**

I. Introduction

Multi-layer networks formed by the convergence of IP/MPLS and Optical technologies are nowadays a commonly adopted solution by network providers, because of the huge transmission capacity offered by optical technologies such as Wavelength Switched Optical Networks (WSON). In order to protect their offered services, network providers may rely on several protection schemes mainly categorized into reactive or proactive. Thus, we can mention 1:1, Shared Protection (SP) schemes as reactive approaches [1], and the well-known 1+1 dedicated protection (DP) scheme as a proactive approach [2]. The main feature of proactive DP schemes is that they achieve near hit-less recovery in an agile manner, i.e., low recovery times, although requiring a significant amount of bandwidth due to their proactive nature. Conversely, reactive protection schemes are not severely limited by bandwidth availability, but their recovery time is not as low as the one obtained by proactive protection schemes. As a matter of fact, despite its high cost in terms of network resources, in practice DP is the option frequently used by network operators because of its low recovery time, high availability of resources upon a failure– dedicated allocation of resources–, and ease of implementation in comparison with SP.

It seems intuitive that an optimal strategy would be to combine the advantages of reactive protection schemes concerning network resources, and the low recovery time offered by proactive protection schemes. In light of this, the advent of throughput improvement techniques such as Network Coding (NC) paves the way to facilitate the deployment of bandwidth efficient proactive schemes. It is worth mentioning that the advantages of NC related to throughput improvement are more noticeable when NC is combined with proactive protection strategies. The advantages of NC are neglected when it is combined with a reactive protection scheme due to the low probability of sharing network resources (at least for single failures scenarios).

Several contributions can be found in the recent literature emphasizing the NCP research area. Authors in [3-5] propose NCP schemes based on a DP strategy agnostic of the network layer technology (IP/MPLS or Optical) they are deployed in. Moreover, they consider single layer scenarios, although this is not the network model commonly adopted at present. A different approach can be found in [6], where authors provide an NCP scheme based on a 1+N protection strategy that considers a multi-layer network formed by MPLS and Optical technologies.

To the best of our knowledge, there are no studies addressing the deployment of NCP schemes, that leverage cross-layer information in multi-layer networks, despite the fact that the current network backbone is mainly a multi-layer network. This challenge is the rationale driving this paper.

Cross-Layer information is required to guarantee that both primary and backup paths are link-disjoint at all network layers. This is very relevant in multi-layer networks in order to avoid Shared Risk Link Groups (SRLG) that can lead to multiple failure scenarios. For instance, a failure affecting an optical link may affect a primary connection, i.e., a logical link and its backup path at the packet (virtual) layer– in this paper we will use the words *packet layer* and *virtual layer* interchangeably. Moreover, cross-layer information is useful to compute the protection cost (P_{cost}) at different network layers, i.e., the amount of bandwidth at the packet layer or the number of optical wavelengths required to enable link protection. Notice that even though the Packet P_{cost} required to protect a certain group of logical links using two different backup paths may be the same, the Optical P_{cost} may be different. Thus, computing the P_{cost} for a single layer may lead to an improper deployment of an NCP scheme in multi-layer scenarios.

The main objective of this paper is to improve network

reliability in multi-layer networks. To this end, we propose a novel multi-layer NCP scheme referred to as DPNC+, specifically for link protection in single failure scenarios – even though it can be easily extended for path protection. The proposed scheme exploits cross-layer information for computing backup paths. In particular, the main goals of DPNC+ are: 1) maximizing the amount of coded traffic; and 2) minimizing the P_{cost} in multi-layer networks.

The rest of this paper is organized as follows. Section II introduces related works concerning NCP. Section III, describes the proposed system model and the basic operation of an NCP scheme. Section IV presents the proposed scheme. The evaluation and numerical results are presented in Section V. Finally, Section VI, presents the final conclusions and future work.

II. Related Work

DP schemes are one of the most widespread protection strategy used due to: (1) simplicity, (2) low recovery time, and, (3) near hit-less recovery features. Nevertheless, DP schemes are severely limited by bandwidth availability. To address this issue, throughput improvement techniques have been studied over the years. In the last years, a throughput improvement technique that is gaining momentum in network research is NC.

The pioneer work found in [7] introduced the benefits of NC to improve network throughput. This work inspired other studies that evaluated NC techniques in different network scenarios such as wireless and multicast. In recent years, several research initiatives are focusing on combining NC and protection strategies to improve resilience in wired networks.

In this paper, authors present an NCP scheme (so-called DPNC+) to be deployed in a wired multi-layer network scenario. Although DPNC+ is similar to the approach presented in [6], both proposals differ in several aspects. First, DPNC+ scheme exploits cross-layer information to avoid SRLGs and minimize the P_{cost}. Second, in order to ensure realistic findings, the Virtual topology configurations used in the evaluation section of this work are based on the realistic network topologies found in [8]. Third, the protection strategy used and the arrangement of coding groups –all possible combinations of connections suitable for NCP– are different, as we use a DP strategy with systematic coding.

Moreover, DPNC+ is similar to the works found in [9], [3]. However, none of the these works consider cross-layer information or a multi-layer network scenario. Finally, DPNC+ only uses coding when the P_{cost} is less in comparison with the P_{cost} obtained by using a conventional DP scheme. Otherwise, DPNC+ uses a DP scheme to protect certain connections.

It is important to remark that the main objectives of this work are both to study the performance of NCP schemes in multi-layer networks, and how cross-layer information can be exploited to increase network reliability.

For more information related to selection of coding groups and coding strategies, the readers are referred to [4]. In addition, readers are also referred to [10] and [11] for more information regarding technical issues to deploy NCP schemes.

III. NCP in Single-Layer Scenarios

In this section, we introduce our network model, the basic operation of an NCP scheme, as well as a number of variables that will be used throughout this paper. We consider a NCP strategy similar to [9][5], hereinafter are referred to as DPNC.

A. System Model.

We assume a directed graph $G(E,V)$ representing a Virtual network topology, where V is the set of nodes, specifically IP/MPLS-TP nodes, and E is the set of edges, specifically packet connections, i.e., logical links. Our objective is to obtain a new graph $G'(E',V)$, which is a directed multigraph, where G is an edge-induced subgraph of G' with $E \subseteq E'$, such that the amount of coded traffic can be maximized. Our proposal can be useful to any NCP scheme (such as the ones using a systematic coding strategy) highly impacting on protecting those topologies where the network connectivity hinders the coding of traffic. It is worth mentioning that the use of different coding strategies such as non-systematic coding are considered as a future line of work of this paper.

On the other hand, we make the following operational assumptions.

1) All links are bidirectional.
2) Traffic data units are fixed and equal in size.
3) The proposed protection strategy is deployed at the client layer, i.e., the packet layer.
4) The backup paths associated to a certain set of primary connections that are jointly coded (protected) are link-disjoint.
5) All primary connections follow a transparent model, i.e., transparent lightpaths are assigned to all primary connections.
6) For simplicity, coding operations are done electrically, based on the *exclusive-or operation* (XOR) and are done over $GF(2)$. We consider that in practice, it is easier to deploy an NCP scheme at the packet layer, since the network coding techniques are mostly studied for electrical operations. Even though there are recent advances in the optical domain as well [12], there are several issues that must be addressed before all optical NC is as reliable as electronic NC.

The symbols and terminologies used in the rest of this paper are listed in Table I.

B. Operation of an NCP scheme

To illustrate the basic operation and limitations of an NCP scheme we consider the directed graph topology shown in Fig. 1a. In this scenario, as well as those shown in Fig. 1b, c, d and e, we assume that the cost to send a data stream along any link is $1U$, the network resources required to send traffic along both ways of a link are the same, and we consider a systematic coding strategy.

In the topology shown in Fig. 1a the traffic sent along links $e_{1,3}$ and $e_{2,3}$ ($T_{1,3}$, $T_{2,3}$) cannot be coded (protected) because there is not a link-disjoint backup path from $e_{1,3}$ and $e_{2,3}$ with node 3 as its terminal vertex. It is important to highlight that

Table I
LIST OF SYMBOLS.

Symbols and Terminology	Meaning
$G(V, E)$	Directed graph where V is the set of nodes and E is the set of edges.
$T_{x,y}$	Traffic sent by node x destined to node y, where $x, y \in V$.
$T'_{x,y}$	Replica of traffic $T_{x,y}$.
$T''_{x,y}$	Coded traffic sent by node x destined to node y.
Coding Path	Path that carries the protected (coded) traffic.
Coding Node	Node that codes protected traffic.
$\phi()$	Function that returns the shortest-path between two nodes (we consider the number of hops as the routing metric).
$h()$	Function that given a path returns the set of nodes belonging to this one.
Ω	Set of potential coding nodes.
L	Set of links suitable for NC.
χ	Set of provisioned links to be used as backup paths.
$\mathcal{L}_m$	Set of lightpaths assigned to each logical link, such that $m \in \{1, ...\|E\|\}$.
β	Set containing all combinations of shortest-paths among the source vertices of the links to be coded. β=$\phi(n_k, n_{k+1})$,$\phi(n_k, n_{k+2})$, ..,. where $k \in \{1, ...\|L\|\}$, and n_k is a source vertex of link k.

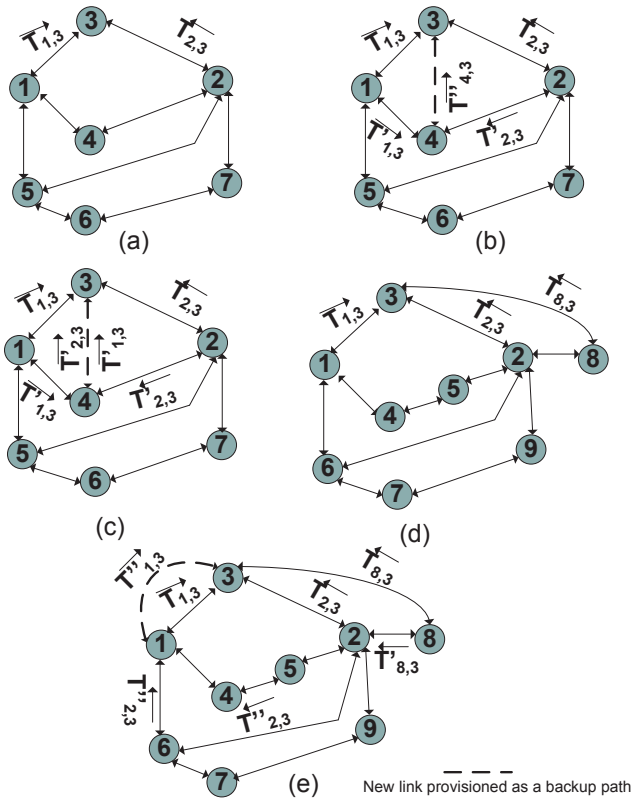

Figure 1. a) and d) Scenarios where it is not possible to code traffic; b) and e) Path provisioning to enable NC; c) DP operation.

the main goal of an NCP scheme is to code traffic aiming at reducing the bandwidth used for protection. In the case that the traffic $T_{1,3}$ and $T_{2,3}$ are jointly coded ($T_{1,3} \oplus T_{2,3}$) and sent along either link $e_{1,3}$, $e_{2,3}$, or sent on both links, this would be inefficient compared to the use of conventional proactive protection schemes such as DP. It is important to notice that coded traffic must be sent along a path link-disjoint from the primary links to be protected, i.e., $\rho_{1,3} \cap e_{1,3} \cap e_{2,3} = \emptyset$, and $\rho_{2,3} \cap e_{1,3} \cap e_{2,3} = \emptyset$, where $\rho_{x,y}$ is a backup path of link $e_{x,y}$.

As a consequence, two possible solutions can be followed. One is to use a DP scheme for those links that could not be coded. Contrary to an NCP scheme, a DP scheme does not code traffic. Thus, the path $(e_{1,4}\ e_{4,2}\ e_{2,3})$ and $(e_{2,4}\ e_{4,1}\ e_{1,3})$ can be the backup path for links $e_{1,3}$ and $e_{2,3}$ respectively.

The other possible solution includes the provisioning of a new link that serves as backup path. For instance, if a new link is provisioned between nodes 4 and 3 ($e_{4,3}$), it would be possible to code the traffic $T_{1,3}$ and $T_{2,3}$ and obtain $T''_{4,3}$ see Fig. 1b. This can be achieved by setting up node 4 as a *coding node* and link $e_{4,3}$ as a *coding path*. As a result node 3 receives the data stream $T''_{4,3}$, that codes $T_{1,3}$ and $T_{2,3}$ ($T''_{4,3} = T_{1,3} \oplus T_{2,3}$). Thus, in the case of a failure of links $e_{1,3}$ or e_{23}, node 3 can decode $T''_{4,3}$ and obtain $T_{1,3}$ or $T_{2,3}$ by executing $T''_{4,3} \oplus T_{2,3}$ or $T''_{4,3} \oplus T_{1,3}$ respectively.

Indeed, when traffic $T_{1,3}$ and $T_{2,3}$ are coded at node 4 (see Fig. 1b) the P_{cost} is $3U$ of bandwidth. But when conventional DP is used the P_{cost} is $4U$ of bandwidth (count the number of $T'x, y$ and $T''x, y$ on Fig. 1c).

Note that one of the endpoints (the terminal vertex) of the provisioned coding path is the terminal vertex of the protected links (node 3 in the topology shown in Fig. 1b), that is termed as node d. This holds true if it is assumed that only links with common terminal vertices are protected, since according to [5] and [3] this reduces the P_{cost}[1]. Moreover, despite the fact that links with different terminal vertices can be protected by an NCP scheme, we do not consider this strategy in order to minimize the complexity of control plane operations such as the signaling overhead on the data (to be able to decode), as well as the state information related to the traffic being coded, i.e., we attempt to minimize the amount of traffic required on the decoding process.

The other endpoint of the coding path is the *coding node* (node 4 in the topology shown in Fig. 1b). However, there can be more than one single *coding node*. Indeed, in a connected graph, all nodes i are potential *coding nodes*, where $i \epsilon \{1, ..., |V|\}$, and $i \neq d$. Aligned to this, we propose the following procedures to obtain the set of *coding nodes* offering minimum P_{cost} according to the links to be protected.

1. Only two links (with common terminal vertex) are to be protected:

- Remove links to be protected from $G(V, E)$, then compute $\Omega = h\{\phi(n_k, n_{k+1})\}$.

2. More than two links (with common terminal vertex) will be protected by enabling NC:

[1]It is worth mentioning that there are studies available in the literature that deal with NCP with different destinations [13].

- First, obtain the set β, where $|\beta| = \binom{|L|}{2}$, and L is the number of links suitable for NC.
- Second, remove links to be protected from $G(V, E)$, then obtain $\Omega = \cap_{s=1}^{|\beta|} h(b_s)$, where $b_s \epsilon \beta$.

In the following lines we illustrate the procedure to obtain the set of *coding nodes* with a simple example. Consider the topology depicted in Fig. 1d, the links suitable for NC are: $L = (e_{1,3},\ e_{2,3},\ e_{8,3})$. For this case $\beta = \phi(1,2)\,, \phi(2,8)\,, \phi(1,8)$, and $\Omega = 1,\ 6,\ 2,\ 8$. Therefore, a backup link may be provisioned between node 3 and any of the nodes belonging to the set Ω (such as $e^2_{1,3}$ see Fig. 1e) to be used as the backup path for the protected primary links.

The cost of provisioning new links may be expensive when there is no infrastructure currently in place, such as dark fiber. However, if the links to be provisioned are logical links, e.g., IP/MPLS label switched paths (LSPs) in a multi-layer network scenario, the backup link provisioning process is related to: 1) the availability of physical resources (transponders, optical wavelengths); and 2) the graph properties of the optical topology, e.g., graph connectivity.

Moreover, all coding nodes belonging to the set Ω offer the same P_{cost}. This holds true assuming that the cost to send a data stream along a given link is the same independently of the path length. Nevertheless, this does not apply for an Elastic Optical Network (EON) scenario, however, EON scenarios are out of the scope of this work.

In the scenario depicted in Fig. 1e, the P_{cost} required to protect links $e_{1,3}$, $e_{2,3}$ and $e_{8,3}$, i.e., $P(e_{1,3},\ e_{2,3},\ e_{8,3})$, is $4U$ (U is a network resource unit) if link $e^2_{1,3}$ is provisioned to be used as a backup path. Notice that node 2 codes the traffic $T'_{2,3}$ (not shown in Fig. 1e) and $T'_{8,3}$, producing $T''_{2,3}$.

In a similar manner, node 1 codes $T'_{1,3}$ (not shown in Fig. 1e) and $T''_{2,3}$ producing $T''_{1,3}$. This traffic is then sent along the recently provisioned backup path. Therefore, the path traversed by the coded traffic is $(e_{8,2}, e_{2,6}, e_{6,1}, e^2_{1,3})$. Moreover, if a new link $e_{6,3}$ is provisioned as a backup path the P_{cost} is also $4U$, since $1U$ is needed for paths $e_{1,6}$ and $e_{6,3}$ respectively, and $2U$ for path $e_{8,2}$, $e_{2,6}$. Nevertheless, we must consider that in a multi-layer scenario, equal protection costs computed at the virtual topology when using two different coding paths –such as the ones obtained when using links $e^2_{1,3}$ or $e_{6,3}$– may be different when the lightpaths assigned to each coding path are considered. For instance, even though Packet P_{cost_1}=Packet P_{cost_2}, it can be possible that the Optical $P_{cost_1}\neq$Optical P_{cost_2}, where P_{cost_1} and P_{cost2} are protection costs obtained when using two different coding paths.

The scenario described in Fig. 1 illustrates how to provision backup links to be used as backup paths in such a way that the amount of coded traffic is maximized. As a result, P_{cost} is minimized when an NCP scheme is used in single layer networks. In the following section, we plunge into several issues that need to be addressed to provision backup links in multi-layer scenarios.

IV. DPNC+: NCP for Multi-Layer Networks

This section introduces a novel NCP scheme for multi-layer networks namely DPNC+. The main purpose of DPNC+ is to improve network reliability by provisioning backup links based on cross-layer information. In particular we intend to: 1) maximize coded traffic; and 2) reduce the P_{cost} on a multi-layer network scenario.

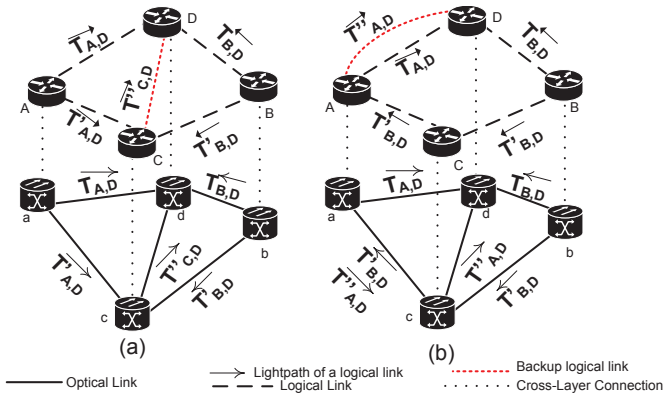

Figure 2. a) Multi-layer protection with router C as a coding node; b) Multi-layer protection with router A as a coding node.

To illustrate the operation of the proposed multi-layer protection scheme we consider the multi-layer network scenario shown in Fig. 2. The main objective pursued with this example is to elucidate the need of using cross-layer information when provisioning links to be used as backup paths.

In order to protect the traffic sent along the logical links $e_{A,D}$ and $e_{B,D}$ using DPNC+ two approaches can be followed, represented in Fig. 2a and Fig. 2b respectively. The configuration shown in Fig. 2a consists of the following: 1) Logical link $e_{C,D}$ is provisioned as a backup path; 2) router C is configured as a coding node. The Packet and the Optical P_{cost} are $3U$ each (count the number of $T'_{x,y}$and $T''_{x,y}$).

On the other hand, the configuration shown in Fig. 2b consists of the following: 1) a new logical link $e^2_{A,D}$ is provisioned to be used as a backup path; 2) router A is configured as a coding node. With this configuration the Packet P_{cost} is $3U$, but the Optical P_{cost} is $4U$ (count the number of $T'_{x,y}$ and $T''_{x,y}$), because the primary and its respective protected traffic need to be sent along different paths (Packet and Optical paths) to avoid SRLGs. Thus, the configuration shown in Fig. 2a should be the option chosen to protect the traffic sent along logical links $e_{A,D}$ and $e_{B,D}$.

To compute the Optical P_{cost} the set of lightpaths ($\mathcal{L}$) associated to each logical link is required, i.e., cross-layer information must be known beforehand. However, cross-layer information might be also obtained on demand by a multi-layer coordinator.

After carefully observing the example described in Fig. 2 it can be concluded that the backup link provisioning process must consider cross-layer information in order to address two issues. First, the backup path (including the provisioned backup link) and the primary links protected by this path must be link-disjoint at both Packet and Optical layers in order to avoid SRLGs. Moreover, primary logical links suitable for coding must be link-disjoint at the Optical layer as well, in order to properly decode protected traffic, i.e., enable protection against double link failures. Second, both Packet

and Optical P_{cost} must be computed to provision the most suitable backup path, i.e., obtain the smallest P_{cost}.

As described in Section III, two solutions may be applied when NCP does not show enough resources to react to a link failure: 1) use DP; or 2) use backup link provisioning. The protection scheme proposed in this paper provisions backup links with the aim of enabling the coding of traffic, but also introduces a function to decide when this backup link must be used instead of DP. This is also useful because the avoidance of SRLGs strongly depends on the connectivity of the packet and optical topologies. Thus, when traffic cannot be coded or coding is expensive (a high P_{cost}), conventional DP is used.

Finally, Algorithm 1 shows the overall procedure for DPNC+. Notice that a backup link is only provisioned as long as a P_{cost} reduction is achieved in comparison with conventional DP. This is the reason why in an NCP scenario, the provisioning of a backup link must be done solely when it enables the coding of traffic.

Algorithm 1 Overview of DPNC+

Input: $(G(E,V)$, $G_2(E_2,V_2)$, $\mathcal{L})$
Output: (P_{cost})

{G and G_2 are the IP/MPLS (Packet) and Optical topology respectively.}
$P_{cost} = 0$ {Initialize the total Packet Protection Cost}
S =Group logical links (E) by common destination node
for i in S **do**
  L =Create Sub-groups of minimum length equal to 2. {since at least 2 working links with common destination are required to enable NC.}
for L in S **do**
  for j in L **do**
    $DPNCP_{cost}$ =Run DPNC for each j (links suitable to NC or link subgroup), then compute the protection cost for each link subgroup {Protect each link subgroup with NCP strategy described in [5]}
    DPP_{cost} =Run DP for each link that could not be protected by DPNC, then compute the protection cost
    $\Omega = ObtainCodingNodes(j)$ {Obtain the set of coding nodes by using the procedure described in Section III.B.}
    $\chi_j = ProvisionBackupLink\,(\mathcal{L}, G, G_2, j)$ {Provision a backup link which endpoints are one of the coding nodes obtained and the terminal vertex of protected links, consider the both Virtual (packet) and Optical topologies in order to select the optimal backup link}

    $DPNC^+P_{cost}$ =Run DPNC+ for each j then compute the protection cost {protect each link subgroup using the logical backup links}
    if $DPNC\,P_{cost}$+DP_{cost}> $DPNC^+P_{cost}$ **then**
      $\mathcal{F}_j = DPNCP_{cost} + DPP_{cost}$ {$\mathcal{F}_j$ is the protection cost of sub-group j.}
      {protection group j is protected with DPNC combined with DP.}
      Tear-Down backup link χ_j
    else
      $\mathcal{F}_j = DPNC^+P_{cost}$
      protection group j is protected DPNC+.
  P^L_{cost}=$min\,(\mathcal{F})$ {Select the sub-group with the minimum P_{cost}.}

V. Numerical Results

This section provides numerical results related to the proposed scheme and other similar protection solutions. The proposed protection scheme (DPNC+) is evaluated in terms of IP and Optical P_{cost} (using the well known python graph library NetworkX [14]), in comparison with DP (conventional proactive protection), and DPNC (NCP without cross-layer information) schemes. To ensure realistic findings the evaluated schemes were modeled over the multi-layer Spanish backbone topology see Fig. 3a.

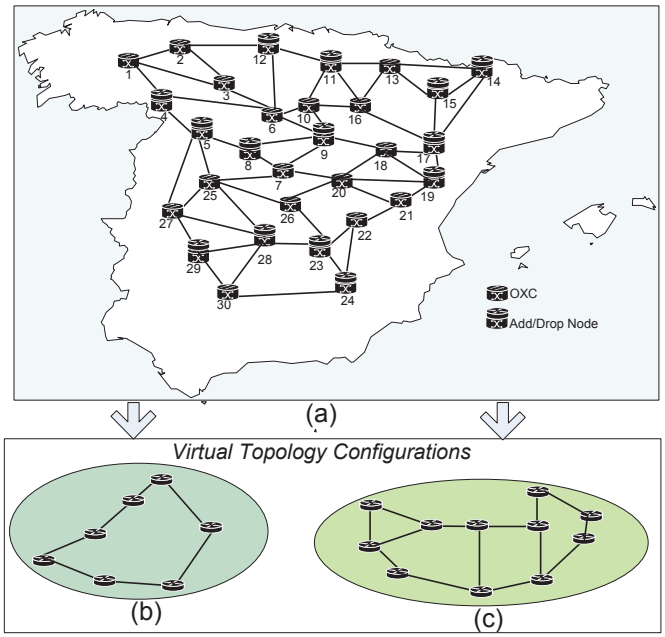

Figure 3. a) Multi-layer Spanish backbone topology; b) Virtual topology based on Sanren topology; c) Virtual topology based on Abilene topology

The Virtual topology configuration of the multi-layer Spanish backbone topology was based on realistic network topologies extracted from [8], which is a vast online repository of real telecommunication networks. On this basis, we configured the Virtual Topologies, shown in Fig. 3b and Fig. 3c. We considered it more reasonable to evaluate more than one Virtual topology, while using only one physical topology design, because on a real multi-layer network scenario the Virtual topology design changes faster than the physical topology (fueled by the low economic cost, and ease of provisioning tasks).

Several trials have been carried out assuming the following settings: 1) the shortest-path routing algorithm used for route computations is based on the hop metric; 2) IP/MPLS router line cards of 100 Gbps capacity; 3) homogenous traffic demands of 20 Gbps along each logical link; and 4) cross-layer information is known beforehand.

The Packet P_{cost} for the three evaluated protection schemes is depicted in Fig. 4. It can be seen that with DPNC+, a considerable reduction of the Packet P_{cost} is achieved, up to 50% reduction. Note that for the Sanren topology [8] the Packet P_{cost} for DP and DPNC schemes is the same, which is reasonable since all nodes in this topology have a indegree equal to two. As a consequence, DPNC cannot code traffic, i.e., DPNC does not perform better than DP in this type of topology. Conversely, DPNC+ is able to code traffic due to its

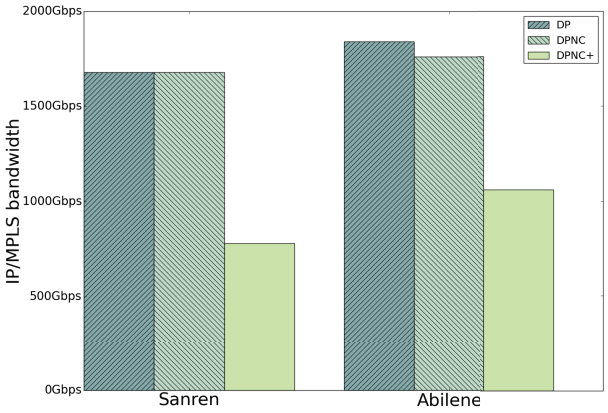

Figure 4. Comparison of Packet P_{cost}.

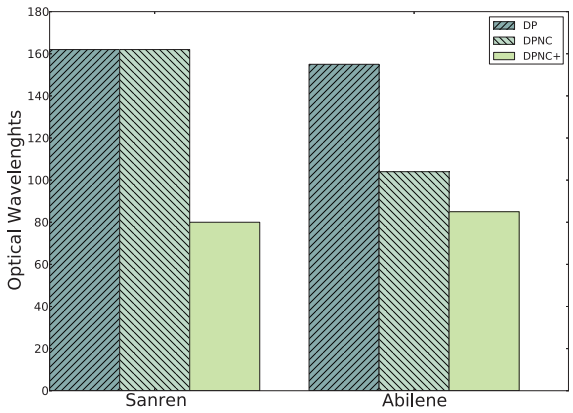

Figure 5. Comparison of Optical P_{cost}.

Table II
PERCENTAGE OF NON-CODED CONNECTIONS.

Protection schemes	Evaluated network topologies	
	Abilene	Sanren
DPNC	100%	35.7%
DPNC+	14.2%	10.7%

capability related to backup link provisioning.

Regarding the Abilene topology [8], DPNC offers a smaller Packet P_{cost} compared to a DP scheme. However, using DPNC+ is possible to obtain a 40% and 35% P_{cost} reduction compared to DP and DPNC schemes respectively.

Furthermore, Fig. 5 quantifies the Optical P_{cost}. It can be observed that the DPNC+ scheme requires less Optical resources in comparison with the other schemes evaluated.

Finally, Table 2 shows the percentage of non-coded connections by DPNC and DPNC+ respectively. Based on the obtained results it can be stated that the proposed scheme maximizes coding in an effective manner, i.e., enable coding solely when the P_{cost} is reduced. Moreover, the evaluation results substantiate that DPNC+ significantly reduces both the Packet and Optical P_{cost} compared to other proactive protection schemes.

VI. CONCLUSIONS

In this paper we propose a novel proactive protection scheme referred to as DPNC+. DPNC+ leverages network coding techniques, backup path provisioning, and cross-layer information in order to reduce the network resources allocated to link protection. Simulation results obtained using real network topologies show that the proposed scheme provides a significant reduction (about 50%) of both IP/MPLS and Optical bandwidth required for network protection, in comparison with other proactive protection schemes. We believe that network operators should consider NCP schemes combined with cross-layer information as an appealing solution to design efficient proactive protection schemes. As a future line of work we intend to study the use of NCP combined along with distinct protection and coding strategies.

ACKNOWLEDGMENTS

This work was supported by the Spanish Ministry of Economy under contract TEC2012-34682, and the Catalan Research Council (CIRIT) under contract 2009 SGR1508.

REFERENCES

[1] *A. Haider and R. Harris, "Recovery techniques in next generation networks,"* Communications Surveys Tutorials, IEEE*, vol. 9, no. 3, pp. 2 –17, quarter 2007.*

[2] *D. Zhou and S. Subramaniam, "Survivability in optical networks,"* Network, IEEE*, vol. 14, no. 6, pp. 16–23, 2000.*

[3] *A. Muktadir, A. Jose, and E. Oki, "An Optimum Mathematical Programming Model for Network-Coding Based Routing with 1+1 Path Protection," in* World Telecommunications Congress (WTC), 2012*, march 2012, pp. 1 –5.*

[4] *S. Nazim and E. Ayanoglu, "Network Coding-Based Link Failure Recovery over Large Arbitrary Network." Globecom, 2013.*

[5] *W. Ramirez, X. Masip-Bruin, M. Yannuzzi, R. Serral-Gracia, and A. Martinez, "An Efficient Protection Strategy Using Multiple Network Coding," in* International Workshop on Network Management Innovations, SACONET 2013, Paris, France*, June 2013.*

[6] *A. Kamal, A. Ramamoorthy, L. Long, and S. Li, "Overlay Protection Against Link Failures Using Network Coding,"* Networking, IEEE/ACM Transactions on*, vol. 19, no. 4, pp. 1071 –1084, aug. 2011.*

[7] *A. Agarwal and M. Charikar, "On the advantage of network coding for improving network throughput," in* Information Theory Workshop, 2004. IEEE*, 2004, pp. 247–249.*

[8] *http://www.topology-zoo.org/, [Online; accessed January-2014].*

[9] *H. Overby, G. Biczok, P. Babarczi, and J. Tapolcai, "Cost comparison of 1+1 path protection schemes: A case for coding," in* Communications (ICC), 2012 IEEE International Conference on*, pp. 3067–3072.*

[10] *S. El Rouayheb, A. Sprintson, and C. Georghiades, "Robust Network Codes for Unicast Connections: A Case Study,"* Networking, IEEE/ACM Transactions on*, vol. 19, no. 3, pp. 644–656, 2011.*

[11] *P. Babarczi, J. Tapolcai, A. Pasic, S. Darehchi, and P.-H. Ho, "New addressing scheme to increase reliability in MPLS with network coding," in* Design of Reliable Communication Networks (DRCN), 2013 9th International Conference on the*, 2013, pp. 36–43.*

[12] *M. Zhang, L. Wang, and P. Ye, "All optical XOR logic gates: technologies and experiment demonstrations,"* Communications Magazine, IEEE*, vol. 43, no. 5, pp. S19–S24, 2005.*

[13] *S. Avci, X. Hu, and E. Ayanoglu, "Hitless recovery from link failures in networks with arbitrary topology," in* Information Theory and Applications Workshop (ITA), 2011*, 2011, pp. 1–6.*

[14] *http://networkx.github.io/, [Online; accessed January 2014].*