A Techno-Economic Study of Network Coding Protection Schemes

W. Ramirez*, X. Masip-Bruin*, E. Marin-Tordera*, M. Yannuzzi†, A. Martinez*†, S. Sanchez*, M.S. Siddiqui*†, 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, annym, sergio, siddiqui}@ac.upc.edu
‡Telefonica I+D, Spain, vlopez@tid.es

***Abstract*—The recent advances in optical technologies pave the way to the deployment of high-bandwidth services. As reliability becomes a mandatory requirement for some of these services, network providers must endow their networks with resilience capabilities. In recent years, network coding protection (NCP) has emerged as a tentative solution aiming at enabling network resilience in a proactive and efficient way. The goal of this paper is to conduct a techno-economic study to evaluate the protection cost required by NCP schemes deployed either at the IP/MPLS or at the Optical layer of a multi-layer network, as well as its impact on both the capital and operational expenditures (CAPEX, OPEX) of a network provider. Our evaluation results show that a significant reduction in both CAPEX and OPEX is obtained with NCP. Indeed, at least a 49% and 52% of CAPEX and OPEX reduction is achieved respectively in comparison with conventional proactive protection schemes.**

***Index Terms*—Multi-layer networks, Network Protection, Techno-Economic, Network Coding.**

I. INTRODUCTION

The use of optical technologies such as Wavelength Switched Optical Networks (WSON) is a widespread practice among network providers. This practice is mainly motivated by the vast bandwidth offered by optical technologies for suitably handling the increasingly demand of IP-based services such as IPTV or VoIP. To meet the quality as well as the Service Level Agreements (SLAs) associated to these services, IP/Optical networks must be endowed with resilience capabilities. On this basis, network operators spend significant efforts in network planning with the aim of designing protection schemes providing reliable solutions to protect their offered services in the presence of network failures.

Protection schemes are categorized into two major approaches: 1) Proactive schemes, assuming the traffic is sent simultaneously along the main and protection paths; and 2) Reactive schemes, assuming the traffic is sent along the protection paths only reacting upon a failure on the primary path [1].

A commonly used proactive protection scheme, the so-called Dedicated Protection (1+1 DP) [2], offers hit-less recovery in an agile way, i.e., low recovery times. Despite the relevant advantage of DP, its major drawback boils down to the huge consumption of network resources, i.e., usage of spare capacity. On the other hand, a commonly used reactive protection scheme, the so-called Shared Protection (SP) is more efficient regarding bandwidth utilization in comparison with DP.

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 [3]. Therefore, optimizing DP would require some technique to reduce its high resource consumption. In recent years, NCP have been proposed as a novel approach to enable protection, while simultaneously reducing the Protection Cost (P_{cost}), i.e., the network resources required to enable link protection. The novelty of NCP is based on the use of proactive protection schemes jointly with Network Coding (NC) techniques. NC allows the P_{cost} to be significantly reduced.

Motivated by the network throughput improvements of NC, there are several studies available in the literature related to NCP. For instance, authors in [4], [5] and [6] introduce NCP based on a DP scheme. Hereinafter, the use of NCP based on a DP scheme is referred to as DP+NC; we will also use the words NCP and DP+NC interchangeably. Moreover, authors in [7] proposed a coding approach named non-systematic coding enabling network protection with high capacity efficiency.

Notwithstanding the wide range of studies related to NCP, there is not any study that assesses the impact of DP+NC on the capital and operational expenditures (CAPEX and OPEX) of a network provider. Indeed, this is the rationale driving this paper. It is worth mentioning that we focus our study in proactive schemes because the advantage of NC related to throughput improvement is highly noticeable with proactive protection, rather than in reactive schemes.

The contribution of this paper consists in providing a techno-economic study evaluating how the P_{cost} impacts on both the CAPEX and OPEX of a network provider [1]. For this purpose, this paper compares results obtained by deploying (in planning scenarios) DP versus a DP+NC strategy, so-called DPNC [5], and an extension of DPNC consisting in enabling the coding of already coded traffic, so-called DPNC* [6]. To ensure realistic findings, the performed trials were obtained using a realistic multi-layer topology of the Spanish backbone

---

[1] We focus on single-link failures because they are the most frequent type of failures in communication networks.

network.

The rest of this paper is organized as follows. Section II provides in a nutshell the state of the art regarding NCP. Section III introduces the basic operation of a DP+NC scheme to the non-expert reader, as well as it describes the so-called DPNC*. Section III also provides some insights related to the implementation of NCP schemes. Section IV introduces the network model used. Section V provides a techno-economic study related to proactive protection solutions deployed either at the IP/MPLS or at the Optical layer of a multi-layer network. Finally, Section VI provides some insights and final conclusions.

II. RELATED WORK

NC is a technique commonly used for network throughput improvement, specifically in multicast and wireless network scenarios. In recent years, there is a trend in network research referred to as NCP, consisting in using NC jointly with a protection strategy to enable resilience in wired networks.

Studies such as [8], propose the use of NC combined with a 1+N protection strategy on p-cycles. Moreover, the studies available in [4], [5] and [6] proposed network coding combined with a DP scheme.

In summary, most of the works introduced in this section present evaluations of NCP in distinct network topologies in a technology agnostic manner, i.e., it is not considered the topology technology, either IP/MPLS or Optical. In fact, there is limited information in network research regarding the performance of NCP deployed on Optical and IP/MPLS topologies, and the advantages that this strategy may bring to a network provider concerning its CAPEX and OPEX. In order to provide some lights on this issue, this paper conducts a novel techno-economic study with the aim of evaluating both CAPEX and OPEX required by proactive protection schemes, with and without NC features, and deployed either at the IP/MPLS or at the Optical layer of a multi-layer network.

III. NETWORK CODING PROTECTION

This section introduces to non expert readers the basic operation of DP+NC schemes (DPNC and DPNC*). Finally, some insights related to the implementation of NCP is provided.

A. Operation of a DP+NC scheme.

For the purpose of illustrating the basic operation of DP+NC scheme, we consider the network topology depicted in Fig. 1a showing a single layer connected digraph, $G(V, E)$, where V is the set of nodes and E is the of edges. In the three topologies depicted in Fig. 1 we do not consider any layer technology.

To protect links $e_{4,5}$, $e_{1,5}$ and $e_{3,5}$,, the traffic sent along these links ($T_{4,5}$, $T_{1,5}$ and $T_{3,5}$) is sent simultaneously along link-disjoint paths (from their respective primary links) which are ($e_{4,7}$, $e_{7,3}$, $e_{3,2}$, $e_{2,5}$), ($e_{1,2}$, $e_{2,5}$) and ($e_{3,2}$, $e_{2,5}$), respectively. It is worth noting that node 3 codes the traffic $T'_{3,5}$ (not shown in Fig. 1a) and $T'_{4,5}$, producing $T''_{3,2}$, and node 2 codes all protected traffic (as well as already coded data), i.e., $T'_{1,5} \oplus T''_{3,2}$, producing $T''_{2,5}$, and then sends $T''_{2,5}$ to node 5 along the link $e_{2,5}$. Whenever there is a failure affecting only one of the protected links, for instance, $e_{1,5}$, node 5 can recover the affected traffic by decoding $T'_{2,5}$, e.g., $T''_{2,5} \oplus T_{3,5} \oplus T_{4,5} = T'_{1,5}$. Thus, all protected traffic is aggregated into a single data stream $T''_{2,5}$, resulting in a lower P_{cost}. Indeed, the main advantage of a DPNC scheme resides on the aggregation (coding) of traffic.

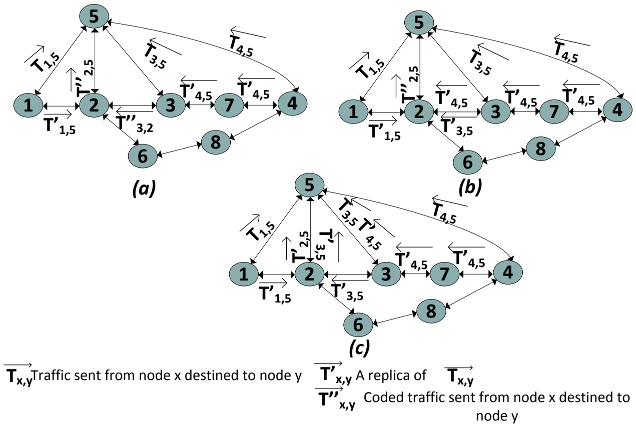

Figure 1. Protection strategies: a) DPNC*; b) DPNC; c) DP.

Consider that the P_{cost} for protecting links $e_{4,5}$, $e_{1,5}$ and $e_{3,5}$ using DPNC* is: P_{cost} ($e_{4,5}$, $e_{1,5}$, $e_{3,5}$) = $5U$ –count the number of $T'_{x,y}$ and $T''_{x,y}$–, being U a network resource unit, such as IP/MPLS bandwidth or number of optical wavelengths allocated for protection. This cost is lower than the obtained by a conventional DP scheme ($7U$), and DPNC ($6U$) (due to the inability of multiple-coding), see Fig. 1c and Fig. 1b respectively. Therefore, it can be stated that NC, and the capacity to code data already coded significantly reduces the P_{cost}.

In order to ease the comprehension of DP+NC is important to remark other several issues: 1) For simplicity, all coding operations are based on the *exclusive-or* over *GF(2)*; 2) Note that $T''_{2,5}$ encodes the already coded traffic ($T''_{3,2}$), this is the concept of multiple-coding introduced in [6], which minimizes the P_{cost}, and; 3) The DP+NC schemes described on this paper are based on systematic coding. For more information concerning other coding strategies the reader is referred to [7].

B. Overall Procedure of Proactive Protection schemes

Algorithm 1 shows the overall procedure of the DPNC* scheme, i.e., the deployment of a DP+NC scheme with multiple-coding in a planning scenario. The main aim of DPNC* is to avoid the forwarding of coded traffic by the terminal vertices of the links jointly coded (protected), i.e., only links or paths with common terminal vertices are protected. Even though the protection of links with different terminal vertices using a DP+NC scheme is possible, we believe that this strategy is more scalable to minimize the complexity of the control plane and the state information related to the data streams being coded, i.e., we attempt to minimize the amount of traffic required on the decoding process.

With regard to the selection of protection paths, DPNC* selects paths that enable traffic coding along as the P_{cost}

Algorithm 1 Overview of DPNC*.

Input: $(G(E,V),\ layerTechnology)$**, Output**: (P_{cost})

```
$P_{cost} = 0$ {Initialize the total protection cost}
$ProtectionGroup$ =Create protection groups (traffic suitable for coding) according to the network layer technology$(layerTechnology)$.
for $i$ in $ProtectionGroup$ do
  $G'\left(E,V\right) = G\left(E,V\right)$
  for $j$ in $i$ do
    Remove each $j \in i$ from $G(E,V)$ {Remove primary links.}
  $Backup_i$ =Compute a set of candidate protection paths$(G(E,V))$.
  $\delta$ =Create protection subgroups formed by a single protection path belonging to each set (protection paths/link)$(Backup_i)$.
  for $k$ in $\delta$ do
    $\alpha_k = \cap_{n=1}^{|k|}\delta_k$ {find common links among the protection paths, this implies that along these links traffic is suitable for coding.}
    $P^{'}_{cost} = \emptyset$ {Initialize the protection cost set of each protection subgroup.}
    if $\alpha_k ! = \emptyset$ then
      $\beta_k = \delta_k \setminus \alpha_k$ {find no common links.}
      $P^{'}_{cost}.add\left(Cost\left(\alpha_k\right) + Cost\left(\beta_k\right)\right)$ {Compute the protection cost and add it to the set $P'_{cost}$}
    else
      $P^{'}_{cost}.add\left(Cost\left(\delta_k\right)\right)$
  $P_{cost} = P_{cost} + min\left(P^{'}_{cost}\right)$ {add the protection cost of Protection group $i$.}
  $G(E,V) = G'(E,V)$ {add primary links.}
```

required to do so is less or equal than the P_{cost} required by DP. Furthermore, we create what we call protection groups (traffic suitable for coding) following two strategies. Within the Optical layer our goal is to maximize the size of protection groups. This is handy for topologies with a low Average Node Degree (AVND). For topologies with a high AVND, as the usual case with virtual (IP/MPLS) topology configurations, we attempt to find a balance between the size protection groups and the use of conventional DP for those data streams not coded.

The overall procedure of the DPNC is similar to DPNC*, but DPNC only considers protection groups of a maximum length of two; hence, the advantages of multiple coding are suppressed. Moreover, for information related to the operation of DP schemes the reader is referred to [2].

C. Practical Implementation of NCP.

Conventional protection schemes such as DP have been widely and successfully deployed in real optical network scenarios. Thereby, a key issue regarding the deployment of an NCP scheme is related to the execution of NC (XOR) operations.

The deployment of optical NC operations is more complex in comparison with electrical NC. In the optical domain, the implementation of all-optical XOR gates is widely studied in network research [9], [10]. Typically, the building components of All-optical XOR gates are Semiconductor Optical Amplifiers (SOAs). SOAs offer low-power consumption, easy deployment and short-latency.

The optical XOR operations using SOAs can be done at line speed for transmission above 10 $Gbps$ and up to 100 $Gbps$, with modulation schemes such as QPSK. Therefore, from a practical perspective, the deployment of NCP schemes in a near future seems feasible.

To the best of our knowledge, at present, the practical implementation of optical XOR operations of optical signals with different modulation schemes such as BPSK and QPSK is possible [11]. However, the all-optical XOR of other modulation schemes needs further study.

IV. NETWORK MODEL

It must be highlighted that the intention of this paper is not to discuss the performance of different coding schemes nor coding strategies, but rather to adopt the strategies proposed in [5] and [6], in order to perform an extensive evaluation regarding the impact of NCP schemes (specifically DP+NC schemes) on CAPEX and OPEX of a network provider. For this evaluation the authors consider the network layer technology and the deployment of NCP schemes in different network layers.

An NCP scheme can be deployed as a protection scheme either at the IP/MPLS or at the Optical layer since NC operations can be executed optically or electrically –as discussed in Section III.C. This capability can be exploited by distinct types of multi-layer recovery schemes, such as Top-Down, Bottom-Up or Integrated approaches. Nevertheless, despite the network layer agnosticism there are some issues to be considered, before deciding on the most suitable layer to deploy an NCP scheme.

For instance, recovery actions executed at the IP/MPLS layer have a high granularity level, i.e., distinct recovery paths can be selected per IP flow. Conversely, this cannot be achieved by a recovery action executed at the Optical layer because the traffic is more aggregated at this layer, i.e., wavelength granularity, several IP flows may be aggregated into a single wavelength. On the other hand, recovery actions executed at the Optical layer have a coarser-granularity. This implies a lower recovery time compared to recovery actions executed at the IP/MPLS layer, because recovering the traffic affected by a failure on an optical link may lead the recovery of multiple IP flows.

In this paper, we assume that the evaluated protection schemes are deployed either at the IP/MPLS layer or at the Optical layer; hence, cross-layer information is not required.

Another assumption is that all cost values used in this paper are normalized to the cost of a 10 Gbps transponder, i.e., 1 cost unit = cost of a 10 Gbps transponder [12]. The network components used in this paper and their respective costs are summarized in table I. Moreover, since the costs of both IP/MPLS and Optical technology equipment tend to decrease, it is reasonable to employ a forecasting model for predicting the cost evolution of the optical nodes over a period of time. Otherwise, it would not be fair to compare CAPEX in different year periods.

Forecasting models are traditionally used as a network planning tool to estimate the cost evolution of technology

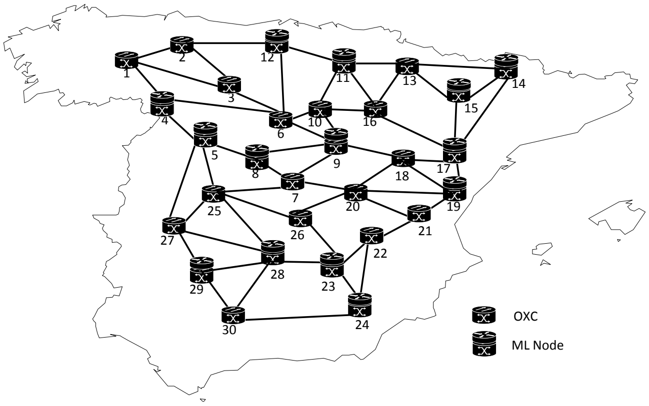

Figure 2. Multi-layer Spanish backbone topology.

equipments. In light of this, [13] presents a cost prediction model which utilizes learning curves and logistic functions. A derivation of this model was employed within this paper in order to estimate the IP/MPLS and Optical equipment cost. The used model includes parameters such as, equipment cost in a reference year, relative accumulated production volume sold in the reference year, etc. These parameters must be adapted accordingly to each equipment.

In addition, we used a separate model architecture for the Multi-Layer (ML) nodes. This reason of this assumption is because an integrated model architecture is not a mature technology. There are several issues that need to be addressed for an integrated model architecture, such as multi-vendor interoperability. Finally, the multi-layer Spanish backbone topology shown in Fig. 2 was used to obtain the numerical results presented in Section V. We assume that for both network layers (IP/MPLS and Optical) the traffic sent along all links will be protected.

A. Network Model for the IP/MPLS Layer

The following assumptions apply to the settings for the IP/MPLS layer network model.

- Each IP/MPLS router embeds 2 IP/MPLS router 4x100 GE line cards. The cost of each card is 36 cost units.
- A 50% traffic increase per year [14].
- The total IP/MPLS network capacity is: $C \times E = 100 \times 84$ = 8.4 Tbps, where C and E are the capacity and total amount of IP/MPLS interfaces respectively.
- We do not consider both CAPEX and OPEX concerning electrical NC features, since they do not have a significant impact.
- We use a *protection-threshold* policy, which defines the percentage of the total network capacity that is allocated for protection. In our particular testing scenario, a 50% *protection-threshold* was used. Whenever the *protection-threshold* is exceeded it is necessary to invest in new network equipment. e.g., IP/MPLS Router Line Cards.

B. Network Model for the Optical Layer

The following assumptions apply for the Optical layer network model.

Table I
BUILDING BLOCKS OF THE MULTI-LAYER NETWORK MODEL.

Component Type	**Cost**
4x 100GE line cards	36
Short-Reach Transceiver	1
All-optical NC	3
WDM Transponder	15
Amplifiers: (A_p, A_b)	0.8
A_{WG}(40 channels)	0.9
Interleaver (80 channels)	0.5
W_{SS} 1×9 (including splitter and filter)	4

- 50 GHz fixed-grid optical nodes.
- Each optical link requires the allocation of 5 optical channels.
- A single fiber system, i.e., one optical fiber per link.
- The ROADMs type is a 80 channel Optical Cross Connect (OXC) with a link degree equal to 5.
- The total capacity of the optical network is: $N \times \lambda = 30 \times 80$ = 2400 channels, where N is the number of nodes in the network, and λ is the amount of available channels per node.
- A 50% traffic increase per year, i.e., year-0 = 5 optical channels, year-1 ≈ 8 optical channels, and so on.
- Aiming at providing realistic results the multilayer cost model presented in [12] is extended to encompass the cost of optical nodes with all-optical coding functionalities. For this purpose, we use all-optical XOR logic gates using Semiconductor Optical Amplifiers (SOAs) based on Cross-Phase Modulation (XPM) with integrated interferometers. This type of XOR gate is widely used because of its low power consumption, high operations speed –over 40 Gbps–, and its support of 3R functions [11]. The cost of an all-optical XOR gate is 3 cost units. In addition, all nodes (both ML and OXC) in Fig. 2 have All-Optical NC features, even though not all nodes code traffic.
- The cost of a 50 GHz fixed-grid ROADM/OXC node with a capacity of 80 channels is obtained using the Equation (1), where d is the optical node degree, W_{ss} is the wavelength selective switch, A_{WG} is the arrayed wavelength grating (optical multiplexers), $A_b + A_p$ are different amplifier types, I stands for interleaver, and G_X is the cost of all-optical coding features, which is zero when conventional DP is used.

$$C_{oxc} = d\,(W_{ss} + A_b + A_p) + 2dI + 4dA_{WG} + 2G_X \quad (1)$$

- We use WDM transponders with 100 Gbps and 2000 km of distance reach. The cost of the used WDM transponders is 15 cost units.

V. TECHNO-ECONOMIC STUDY

In the following subsections we introduce numerical results related to the evaluation of proactive protection schemes and their impact on both CAPEX and OPEX of a network provider. The evaluated proactive protection schemes are: DP, DPNC and DPNC*. Moreover, it is worth mentioning that this techno

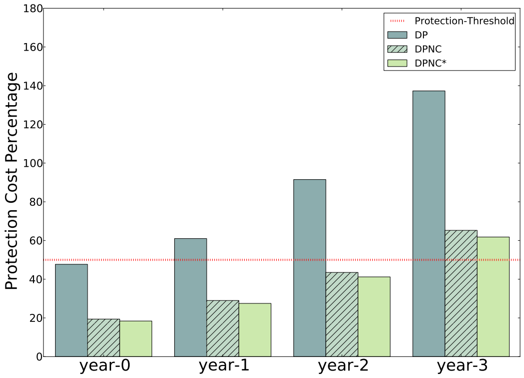

Figure 3. IP/MPLS P_{cost} over the total of network resources.

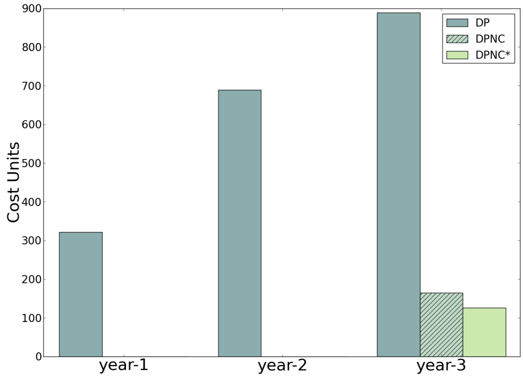

Figure 4. CAPEX related to the IP/MPLS layer.

economic study is valid for a wide variety of situations (costs, topologies, etc.).

A. Protection at the IP/MPLS Layer

In this subsection we evaluate: 1) The IP/MPLS $\%P_{cost}$ required to endow with protection capabilities the IP/MPLS layer and 2) the CAPEX and OPEX required to enhance the routers capacity, for DP, DPNC and DPNC* schemes, deployed at the IP/MPLS layer on the network topology shown in Fig. 2.

Fig. 3 shows the IP/MPLS $\%P_{cost}$ (the amount of IP/MPLS bandwidth used for link protection) for a 4 year period. As it can be observed, in year 1 a DP scheme already exceeds the *protection-threshold* level, whereas for DPNC and DPNC* schemes this occurs two years later. Also worth noting that a DPNC* scheme utilizes less network resources compared to a DPNC scheme.

Fig. 4 shows the cost evolution for the IP/MPLS Router Line Cards. Notice that the IP/MPLS Router Line Cards cost evolution was also estimated with the forecasting model introduced in Section IV. In year 1, the IP/MPLS P_{cost} already exceeds by 11% the *protection-threshold* for a DP scheme (see Fig. 3). Therefore, it is required the investment of 16% in terms of capacity (assuming a 5% safe margin) or an investment of 322 cost units in order to not exceed the *protection-threshold.* However, no investment is necessary in year 1 for a DPNC and DPNC* schemes, rather in both cases this would be only required in year 3 measured in terms of 164 and 125 cost units for both schemes respectively.

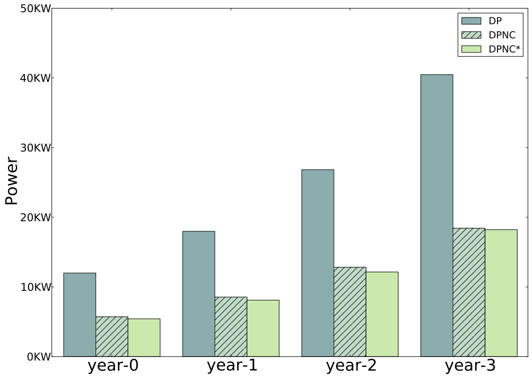

Figure 5. Overall Power Consumption of IP/MPLS line Cards.

Based on the results depicted in Fig. 4, with DP+NC (DPNC or DPNC*) the CAPEX required to add new IP/MPLS Router Line Cards is delayed two years, although worth mentioning that a DPNC* scheme requires 72% less CAPEX compared with the required by a DP scheme in the first year.

Finally, to properly evaluate the impact of the evaluated schemes on OPEX we perform a power cost analysis. To this end, based on the values in [15], we consider that the 100 Gbps IP/MPLS line cards have a power consumption of 351 W. It is worth mentioning that the power consumption of NC operations is neglected since the power consumption of the IP/MPLS line cards is dominant.

Figure. 5 shows the overall power consumption of the three evaluated schemes for a 4 year period. As expected, since the network capacity allocated for protection of DP+NC schemes is less, –which implies less transceivers and IP/MPLS line cards– DP+NC schemes have low power consumption. Notice that the Power Consumption of a DPNC* scheme is 52% less compared with a DP scheme.

From the results introduced in this section it can be concluded that the use of a DPNC* scheme can significantly reduce both CAPEX and OPEX of a network provider. At least 72% and 52% of both CAPEX and OPEX reduction is achieved respectively in comparison with a proactive protection scheme without network coding features such as a DP scheme.

B. Protection at the Optical Layer

This subsection introduces two evaluation tests assessing: 1) The percentage of network resources allocated for protecting optical links (Optical $\%P_{cost}$); 2) The CAPEX related to the Optical layer, i.e., transceivers and WDM transponders.

The first evaluation test assesses the Optical $\%P_{cost}$ as shown in Fig. 6. From the results depicted in Fig. 6 it can be concluded that using DPNC* the Optical P_{cost} is reduced

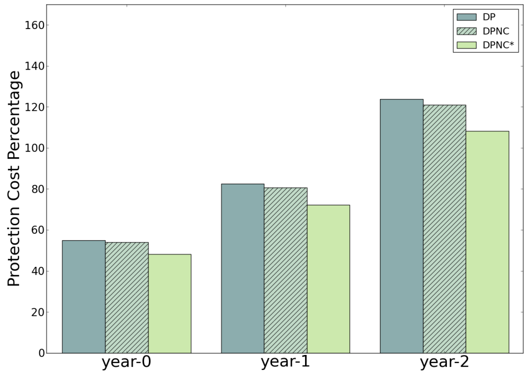

Figure 6. Optical P_{cost} over the total of network resources.

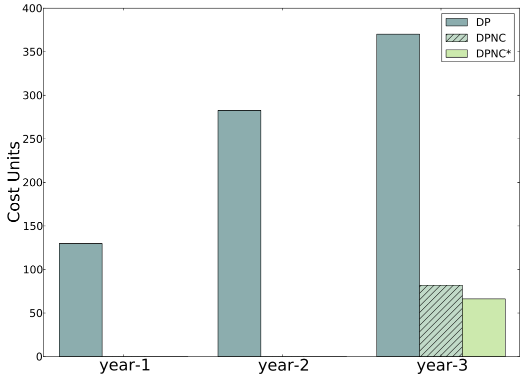

Figure 7. CAPEX related to the Optical layer.

13% and 3% respectively compared with DP and DPNC respectively.

The second evaluation test depicts the CAPEX required by each evaluated scheme, see Fig. 7. From the results depicted in Fig. 7 it can be concluded that a DPNC* scheme requires lowest investment compared with DP and DPNC schemes. For instance, a DPNC* scheme requires 49% less CAPEX compared with the DP scheme in year 1; despite of the cost associated to enable NC features.

VI. CONCLUSIONS

This paper presents a techno-economic study for assessing the protection cost obtained when employing three proactive protection strategies, Dedicated Protection (DP), network coding with a DP scheme (DPNC), and multiple-coding with a DP scheme (DPNC*). It was assumed that the evaluated protection schemes were deployed either at the IP/MPLS or at the Optical layer of a multi-layer network.

Based on the obtained results, we conclude that the use of DPNC, specifically the multiple-coding feature, can significantly reduce both CAPEX and OPEX independently of the network layer where they are deployed in comparison with conventional protection proactive schemes and despite of the cost associated to enable Network Coding (NC) capabilities. An average of 60.5% of CAPEX reduction can be achieved independently of the network layer technology. Indeed, 49% and 72% of CAPEX reduction is obtained when deploying DPNC* at the Optical and the IP/MPLS layer respectively. On the other hand, a 52% of OPEX reduction is obtained at the IP/MPLS layer.

Therefore, since NC operations are supported at both IP/MPLS and Optical layers, the network layer where a Network Coding Protection (NCP) scheme will be deployed, may be selected according to the specific requirements of a network operator. In this light, as a future line of work, we plan to extend the work proposed in this paper by adding cross-layer information in order to maximize the benefits of NCP in terms of network resource savings.

ACKNOWLEDGMENTS

This work was supported by the Spanish Ministry of Science and Innovation under contract TEC2012-34682, project partially funded by FEDER.

REFERENCES

[1] A. Fumagalli and L. Valcarenghi, “IP restoration vs. WDM protection: is there an optimal choice?” *Network, IEEE*, vol. 14, no. 6, pp. 34–41, Nov 2000.

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

[3] O. Gerstel and R. Ramaswami, “Optical layer survivability: a post-bubble perspective,” *Communications Magazine, IEEE*, vol. 41, no. 9, pp. 51–53, Sept 2003.

[4] 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.

[5] 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.

[6] 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.

[7] S. Nazim and E. Ayanoglu, “Network Coding-Based Link Failure Recovery over Large Arbitrary Network.” Globecom, 2013.

[8] A. E. Kamal, “1 + N network protection for mesh networks: network coding-based protection using p-cycles,” *IEEE/ACM Trans. Netw.*, vol. 18, no. 1, pp. 67–80, Feb. 2010. [Online]. Available: http://dx.doi.org/10.1109/TNET.2009.2020503

[9] 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.

[10] X. Yang, R. Manning, and W. Hu, “Simple 40 Gbit/s all-optical XOR gate,” *Electronics Letters*, vol. 46, no. 3, pp. 229–230, Feb 2010.

[11] D. Kong, Y. Li, H. Wang, S. Zhou, J. Zang, J. Zhang, J. Wu, and J. Lin, “All-optical XOR gates for QPSK signal based optical networks,” *Electronics Letters*, vol. 49, no. 7, pp. 486–488, 2013.

[12] F. Rambach, B. Konrad, L. Dembeck, U. Gebhard, M. Gunkel, M. Quagliotti, L. Serra, and V. Lopez, “A multilayer cost model for metro/core networks,” *Optical Communications and Networking, IEEE/OSA Journal of*, vol. 5, no. 3, pp. 210–225, 2013.

[13] B. Olsen and K. Stordahl. (2004) Models for forecasting cost evolution of components and technologies [Online]. Available: http://www.telektronikk.com/.

[14] “Telefonica network planning report [Internal].” Tech. Rep., 2013.

[15] C. Dorize, W. Van Heddeghem, F. Smyth, E. Le Rouzic, and B. Arzur, “draft report on baseline power consumption, version 1.8,” Greentouch, Tech. Rep., 2011.