A Novel Predictive PCE-based Protection Strategy for Resilient Transport Networks

W. Ramirez[1], X. Masip-Bruin[1], E. Marin-Tordera[1]

Abstract

The ever increasing requirements of new Internet applications are pushing to optimize the design of optical networks. A key design criterion in network design is the ability to recover from failures in an agile and efficient manner. Protection capabilities are highly required in optical networks since the failure of an optical link might potentially lead to a significant traffic loss. Under this context, Network Coding Protection (NCP) has emerged as an innovative solution to proactively enable protection in an agile and efficient manner by means of throughput improvement techniques such as Network Coding (NC). Nevertheless, the benefits of NC can be reduced by the negative effects of inaccurate Network State Information (NSI), which are common in dynamic scenarios.

In this paper, we propose a novel proactive protection strategy based on NC jointly with a Path Computation Element (PCE) architecture called Predictive Network Coding Protection (PNCP). PNCP leverages predictive techniques in order to mitigate the negative impact of the inaccurate NSI on the blocking probability. In addition, PNCP computes resilient lightpaths with a low amount of network resources devoted for path protection.

By means of extensive simulation results we show that in comparison with proactive protection strategies such as Dedicated Path Protection (DPP), and conventional dynamic NCP, PNCP reduces the blocking probability as well as the network resources allocated for path protection in dynamic scenarios.

1. Introduction

In recent years, emerging Internet applications and services, such as Cloud Computing, Big data processing, and Video on Demand are all requesting stringent requirements such as, large transmission capacity, high performance routing and resilient services to provide support for the foreseen increase of traffic in the coming years [1]. This set of stringent requirements drives the need for protection strategies in order to guarantee service continuity even when some topological network disruption might affect the forwarding path.

Emails: (wramirez, xmasip, eva)@ac.upc.edu
[1]Advanced Network Architectures Lab (CRAAX), Universitat Politecnica de Catalunya (UPC), Spain.

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

A widely used proactive protection scheme is the so-called Dedicated Path Protection (DPP) [3]. DPP offers hit-less recovery in an agile manner, i.e., low recovery time. Nevertheless, DPP requires huge consumption of network resources dedicated to path protection, i.e., high Protection Cost (P_{cost}). To cope with the bandwidth consumption issues of DPP, reactive protection schemes, such as the so-called Shared Path Protection (SPP) have been proposed. Despite of the advantages of SPP, DPP is the option frequently adopted by network operators due to the deployment issues related to SPP [4]. However, in order to optimize DPP, a novel technique to reduce its high network resources consumption is required. In recent years, Network Coding Protection (NCP) has been proposed as a promising solution offering protection in an agile and cost-efficient manner (low P_{cost}) [5]. The novelty of NCP is based on the use of proactive protection schemes jointly with Network Coding (NC) techniques.

At present, new network architectures such as, the Path Computation Element (PCE) are replacing the conventional distributed source-based path computation as the commonly used strategy to deploy proactive protection techniques [6]. NCP strategies may leverage PCE architectures to improve the overall routing performance. Nevertheless, despite the advantages brought by PCE schemes, its performance might be substantially affected by the negative effects of having inaccurate Network State Information (NSI) [7]. A pioneering work related to the study of the inaccurate NSI in optical networks can be found in [8], where authors show that path computation algorithms that are considered optimal under accurate NSI, conduct suboptimal performance in comparison with other schemes. Recent contributions dealing with the RI problem in unprotected optical networks based on on source routing can be found in [9].

Inaccurate NSI also has a negative impact on the performance of the PCE for its two main approaches, i.e., stateful and stateless PCE [6]. In comparison with a stateful PCE scheme, a stateless PCE has less complexity. However, the NSI stored on the so-called Traffic Engineering Database (TED) may contain outdated NSI in highly dynamic scenarios. Authors in [7] propose a pre-reservation mechanism to cope with the RI problem in stateless and stateful PCE scenarios. However, this approach requires enhancements in both PCE and Path Computation Element Protocol (PCEP).

Moreover, NCP has been widely studied in in optical network planning scenarios, where NC is applied to multiple-sessions (connections) sharing resources and assuming that the demands are known beforehand [10], [11]. Unfortunately, to the best of our knowledge, there is no any study dealing with NCP under dynamic traffic. The rationale driving this paper is to fill this gap. To this end, we propose a novel NCP (stateless PCE-based) scheme so-called Predictive Network Coding Protection NCP (PNCP), leveraging a PCE-based centralized control. Moreover, PNCP adopts the concept of predictive counters for routing purposes. Predictive counters are a technique widely used to deal with the negative impact of inaccurate NSI and for avoiding its dissemination [12].

The rest of this paper is organized as follows. Section II discusses in a comprehensive manner the operation of NCP under accurate and inaccurate NSI. Section III introduces two novel strategies to deploy NCP in dynamic scenarios as well a predictive protection scheme namely PNCP. Section IV presents the network model used to validate dynamic

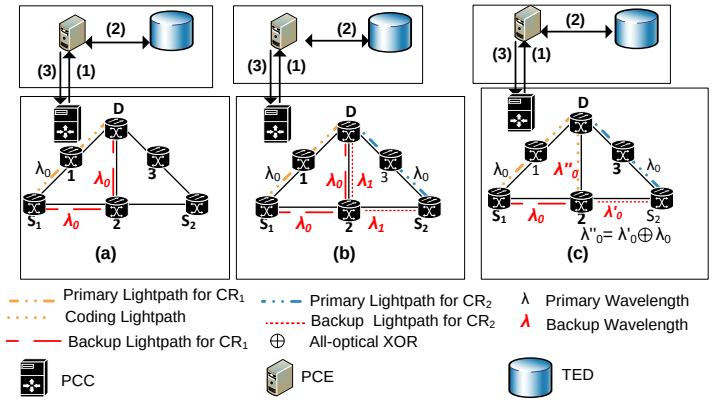


Figure 1: a) DPP operation , b) DPP operation for a second resilient path request; c) NCP operation.

proactive protection schemes, along with extensive simulation results of PNCP algorithm versus other similar type of proactive protection schemes. It is worth noticing that we only focus on the evaluation of proactive protection schemes, we do not consider reactive protection schemes such as shared path protection (SPP) because their operation is far different from proactive protection schemes. Otherwise, it would not be fair to provide a comparison (related to the P_{cost}) between both categories of protection schemes. Finally, Section V concludes the paper and suggests avenues for future work.

2. Overview of Network Coding Protection (NCP)

In this section, we first introduce in a comprehensive manner, the advantages of NCP related to the network resources allocated for path protection (P_{cost}). Then, we distill the negative effects that inaccurate NSI might have on the deployment of an NCP scheme. For the sake of understanding Table I lists the set of symbols and terminology used in this paper.

2.1. NCP Operation

In order to clearly illustrate the potential benefits brought by NCP, we consider the scenario shown in Fig. 1. In this scenario, a connection request (CR_1) reaches the PCE requesting a resilient lightpath for endpoints S_1 and D with a holding time of 50 time slots, where a time slot is defined as the time required to transmit 100 Gbits of traffic. For this purpose, a (proactive) Dedicated Path Protection (DPP) scheme deployed at the PCE based on Least Congested Path (the path with more wavelengths available) routing jointly with First-Fit (FF) for wavelength assignment, will look for the NSI located at the Traffic Engineering Database (TED) in order to compute two link-disjoint paths: 1) a primary lightpath consisting on the path $S_1 - 1 - D$ using wavelength λ_0, and; 2) a backup lightpath consisting on a path $S_1 - 2 - D$ using wavelength λ_0, see steps 1 and 2 in Fig. 1a. Finally, the computed lightpaths are sent to the Path Computation Client (PCC) which will trigger the paths set-up (step. 3).

Table 1: List of Symbols and Terminology.

Symbols and Terminology	Meaning
$G(V, E)$	Directed graph where E is the set of optical links and V is a set of optical nodes.
d	An optical node destination, where $d \in V$.
W	The set of optical wavelengths available for any node.
λ_k	An optical wavelength, where $k \in \{0, ..\|W\| - 1\}$.
W_i	The set of optical wavelengths along a link i locally computed by the PCE, where $i \in E$.
$P_{i,\lambda}$	Predictive counter for link i and wavelength λ locally computed by the PCE, where $\lambda \in W$, and $P^s_{i,\lambda} \in \{0, 1, 2, 3\}$.
$A_{j,\lambda}$	Availability of a lightpath using path j and wavelength λ locally computed by the PCE.
N_j	Is the amount of links of a path j.
$M_{s,d}$	The set of candidate paths for endpoints s, d, where $d \in V$.
B	The set of NC wavelengths.
α_m	NC wavelength, where $\alpha_m \in B$.
$l_{\lambda,p}$	Primary lightpath, p is a primary path.
$l'_{\lambda,q}$	Backup lightpath, where q is a backup path.
Q	Is a set of backup lightpaths demanding NC features.
P	Is a set of primary lightpaths, which its respective set of backup lightpaths (Q) demands NC features.
$h\,()$	Function that given a path returns its destination node.
Suboptimal NC Operation	When a coded traffic cannot be decoded or coded properly.
Wavelength Availability	When a wavelength is not in use in neither of all links of a given path based on global or local NSI.

Afterwards, a subsequent connection request (CR_2) reaches the PCE requesting a resilient lightpath between endpoints $S_2 - D$ with a holding time of 70 time slots. As a result, the PCE computes paths $S_2 - 3 - D$ using λ_0 and path $S_2 - 2 - D$ using λ_1 for primary and backup lightpaths respectively, see Fig. 1b. The total network resources (P_{cost}) solely allocated for the backup lightpaths for both CR_1 and CR_2 using DPP is $4\,u$, where u stands for the allocation of a wavelength along a link.

Assuming the same scenario shown in Fig. 1a and Fig. 1b, a PCE with an NCP strategy will select lightpath $S_1 - 2$ using λ_0 for the protection of CR_1, and lightpath

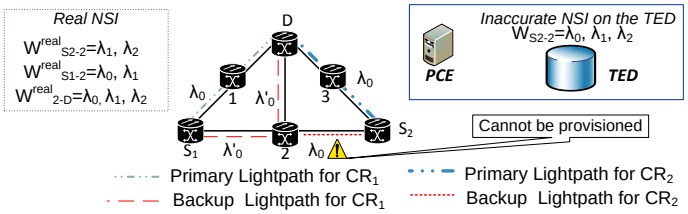


Figure 2: Suboptimal operation of an NCP scheme under inaccurate NSI.

$S_2 - 2$, also using wavelength λ'_0 for the protection path of CR_2. Finally, the protected traffic received along the links $S_1 - 2$ and $S_2 - 2$ (corresponding to CR_1 and CR_2) will be coded (all-optical XOR operation) along optical link $2 - D$ on wavelength λ''_0, see Fig. 1c (for the sake of understanding we use the notation λ, λ' and λ'' to differentiate protection traffic sent along different links allocated on the same wavelength). Under this setting, the total P_{cost} would be $3\,u$. The obtained P_{cost} reduction is motivated by the fact that NC facilitates to convey in a single resource unit more than one data stream. Indeed, the advantage of NCP relies on the coding of traffic.

In the case of a failure affecting either the primary lightpath of CR_1 or CR_2, node D can successfully recover the affected traffic by doing the all-optical XOR operation for λ''_0 and the traffic sent along the unaffected primary lightpaths. It is worth mentioning that the execution of all-optical NC operations (based on XOR gates) can be successfully handled at line speed, for data rates above 10 Gbps and up to 100 Gbps, using modulation schemes such as QPSK or QAM [13].

Moreover, the reader should notice that the lightpath $2 - D$ using λ''_0 is referred to as a *coding lightpath*. A coding lightpath is a lightpath that conveys coded traffic. Conversely, an *uncoded lightpath* is the one that does not convey coded traffic.

An issue that deserves attention related to the deployment of NCP strategies is that the holding time corresponding to a coding lightpath must be equalized (extended) to the holding time corresponding to the CR with the longest holding time allocated on this coding lightpath. For instance, when the backup traffic of CR_2 is coded along lightpath $2 - D$, the holding time of this coding lightpath –set previously to the holding time of CR_1– must be equalized to the holding time of CR_2, since this connection will remain longer on the network. Once the holding time of CR_1 expires, the coded lightpath $2 - D$ will be torn down, hence impacting on the traffic sent along the backup lightpath assigned to CR_2. Therefore, once a coding lightpath is torn-down, the remaining protected traffic sent along this coding lightpath will be sent in a DPP manner –since NC is not longer available.

2.2. Negative Effects of Inaccurate NSI on NCP

The accuracy of NSI related to wavelengths availability per link strongly affects the performance (blocking probability) of all types of protection schemes (NCP based or not). To illustrate the negative effects that inaccurate NSI might have on a protection scheme, we consider the scenario shown in Fig. 2. Let's assume that the NSI stored in the TED regarding the wavelengths availability on link $S_2 - 2$ is outdated (inaccurate). In this scenario, two resilient CRs must be provisioned, CR_1 with endpoints $S_1 - D$, and

CR_2 with endpoints $S_2 - D$. For CR_1, path $S_1 - 1 - D$ using optical wavelength λ_0 is selected as a primary lightpath, and path $S_1 - 2 - D$ using optical wavelength λ_0' is selected as a backup lightpath. Then for CR_2, path $S_2 - 3 - D$ using optical wavelength λ_0 is selected as a primary lightpath, and path $S_2 - 2 - D$ using optical wavelength λ_0 is selected as a backup lightpath in order to enable NC, i.e., to apply NC with the data stream allocated to the backup lightpath $S_1 - 2 - D$, see Fig. 2. Unfortunately, this will lead to the blocking of the backup lightpath for CR_2, since wavelength λ_0 might not be really available along link $S_2 - 2$ ($W^{real}_{S_2-2}$=λ_1, λ_2), despite it appears as available in the TED, see Fig. 2. For the sake of understanding we must clarify that W^{real} stands for the real (accurate) wavelengths availability on an optical link.

In addition to the NSI related to wavelengths availability per link, additional NSI is required, namely the NSI related to the lightpaths allocated to the primary connections, hereinafter referred to as PNSI. PNSI is useful to avoid Shared Risk Link Groups (SRLGs), since in order to protect two or more primary connections (assuming a systematic coding approach), the primary paths allocated to these connections must be link-disjoint. Otherwise, in the case of a failure affecting two or more primary connections, it would not be possible to decode the protected (coded) data. To avoid a scenario where protected data cannot be properly decoded, two possible solutions might apply: 1) re-optimizing the provisioned primary lightpath (which is a disruptive action), and; 2) selecting a different backup path not restricted to the SRLG constraints. The NCP scheme proposed in this paper adopts the last solution.

It can be stated that even though the inaccuracy of PNSI does not increase the blocking probability, it may (collaterally) impact on the protection degree achieved by an NCP scheme. Recall that for each protection group (set of primary data streams to be jointly coded) the primary lightpaths must be link-disjoint in order to achieve proper traffic decoding. Indeed, this dependency of primary lightpaths is a handicap of NCP schemes in comparison to conventional protection strategies such as DPP.

3. NCP Strategies in Dynamic Scenarios

In this section, we discuss two novel strategies for the deployment of dynamic NCP schemes. Then we introduce a predictive protection scheme so-called Predictive Network Coding Protection (PNCP).

3.1. Deployment strategies for NCP in dynamic scenarios

We propose two NC strategies to deploy NCP in dynamic scenarios: *1) Preference Coding*; and, *2) Non-Preference Coding*. Preference Coding, consists in considering the following rule. When NC is enabled along a selected backup path, a Preference Coding scheme will select the optical wavelength that enables NC, without considering if the optical wavelength is available along the selected path. Therefore, Preference Coding gives priority to NC features over wavelength availability. On the other hand, *Non-Preference Coding* enables NC as long as it does not lead to blocking, where a possible blocking scenario is estimated based on the NSI available on the TED, which might be accurate or not. This is, Non-Preference Coding gives priority to wavelength availability over the P_{cost} reduction provided by NC features.

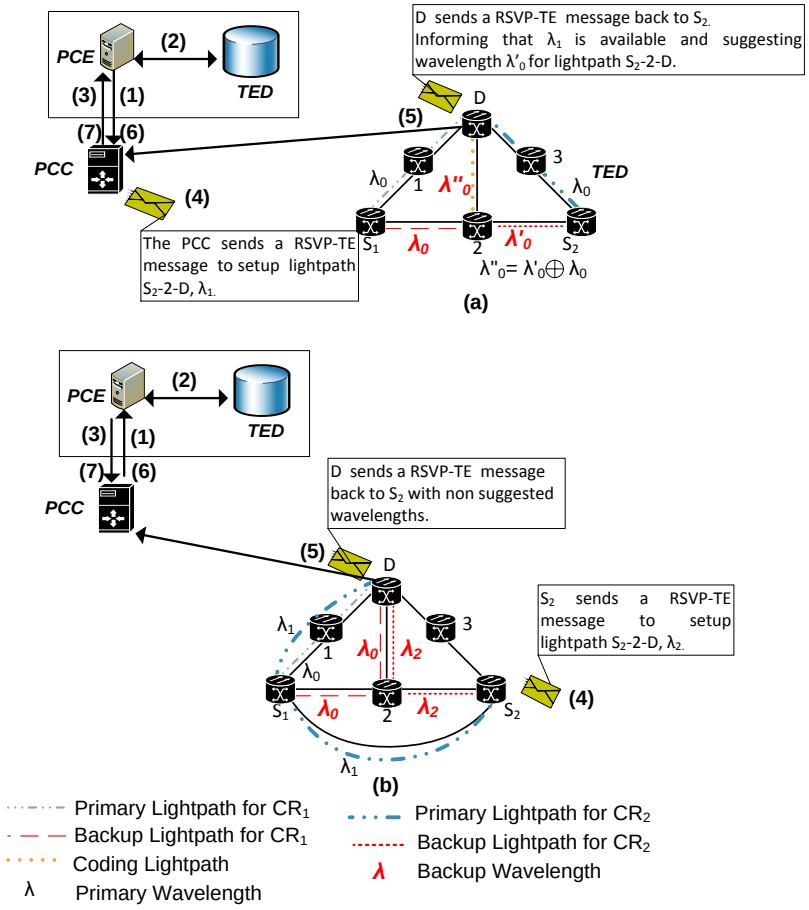


Figure 3: a) Protection with a dynamic NCP scheme; b) Suboptimal Protection with a dynamic NCP scheme.

The Preference and Non-Preference Coding adopt the features of NCP proposed by [11] and extended to dynamic scenarios.

We assume that the NSI required to properly enable NC is requested by the PCE to the destination optical node. This is, optical wavelengths that enable NC are not periodically disseminated. For instance, suppose that for the scenario shown in Fig. 3a, the PCE selects path $S_2 - 2 - D$ and optical wavelength λ_1 for the backup lightpath of CR_2, steps 1, 2. When the PCC attempts to set-up this lightpath (step 4), the destination node (D) will check and inform to the PCC (specifically it sends a *RSVP-TE message*) that optical wavelength λ_1 is available for the selected lightpath.

In addition, optical node D does the so-called *NC sanity check* (step 5). We propose this strategy with the aim of notifying the set of optical wavelengths suitable for NC (hereinafter referred to NC wavelengths, α_m). In Fig. 3a, node D suggests λ_0' as a potential NC wavelength.

Resilient lightpaths must meet the following constraints in order to enable NC: 1) Pri-

mary lightpaths must have common destination node, i.e., node D, as shown in Equation (1); 2) Protection lightpaths must have at least one common link, as shown in Equation (2); and, 3) primary lightpaths must be link disjoint, as shown in Equation (3).

$$\left| \bigcup_{n \epsilon P} h\left(q_n\right) \right| = 1 \tag{1}$$

$$\left| \bigcap_{n \epsilon Q} q_n \right| > 0 \tag{2}$$

$$\left| \bigcap_{k \epsilon P} p_n \right| = 0 \tag{3}$$

On one hand, the rationale behind the common destination constraint is to minimize both complexity and P_{cost}. Even though the protection of lightpaths with different destination nodes using NCP is possible, we believe that this strategy is more scalable in order to minimize the complexity of the control plane operations required on the decoding of protected traffic. In addition, by enabling NC only among lightpaths with common destination nodes, we avoid to retransmit any data stream to a destination node to properly decode protected traffic.

For more information related to protection of lightpaths with different destinations using NCP the reader is referred to [14]. On the other hand, the common links constraint must be met to enable the coding of protected traffic.

The PCC sends the list of NC wavelengths to the PCE (step 6). Based on the list of NC wavelengths (B), the PCE can do the following (step 7):

1. In the case that there is at least one NC wavelength and the selected optical wavelength is none of them ($|B| \neq 0$ and $\lambda_1 \notin B$), i.e., the lightpath can be provisioned but NC is neither possible or optimal, using the selected wavelength), a PCE might (based on a NCP strategy) send a response to the PCC to trigger the set-up of a lightpath, by either selecting one of the NC wavelengths or using the wavelength initially selected instead.
2. In the case the selected wavelength is one among others NC wavelengths ($|B| \neq 0$ and $\lambda_1 \in B$), the PCE might send a response to the PCC to trigger the set-up of the selected lightpath with NC capabilities.
3. In the case there are no NC wavelengths available (meaning that NC is not possible along the selected path), the PCE sends a response to the PCC to either trigger the set-up of the selected lightpath without NC capabilities, or proceed to recompute a different lightpath in order to enable NC. In this paper we do not consider reattempts. This is, the PCE does not recompute a path, it can only change or not the computed wavelength by one NC wavelength.

The set optical wavelengths suitable for NC is suggested assuming the constraint that the primary lightpaths of a set of resilient connections must be link-disjoint. Notice that in the illustrative scenario shown in Fig. 3a, the primary lightpath of CR_1 ($S_1 - 1 - D$) is link-disjoint from the primary lightpath of CR_2, as depicted in Equation (3). Otherwise, a failure affecting for instance link $1 - D$ can affect the proper decoding of coded traffic.

Algorithm 1 Overall Procedure of Preference Coding.

Input: (Destination node)
Output: (*ResilientLightPath*)

Compute a primary lightpath ($l_{\lambda,p}$)
Select a wavelength in a First-Fit Fashion.
Provision($l_{\lambda,p}$){Attempt to establish the primary lightpath.}
if $l_{\lambda,p}$ not established **then**
  Return 0.
Compute $l'_{\lambda,q}$ in a First-Fit fashion, where $|q \cap p| = 0$.
B=Check NC wavelengths along protection path($l'_{\lambda,q}$)
if $|B|>0$ **then**
  Provision($l'_{\alpha,q}$){Set-up the backup lightpath}
  Return($(l_{\lambda,p}),(l'_{\alpha,q})$) if the $l'_{\alpha,q}$ successfully established.
else
  Provision($l'_{\lambda,q}$){Set-up of the backup lightpath.}
  Return $((l_{\lambda,p}),(l'_{\lambda,q}))$ if $l'_{\lambda,q}$ successfully established.
Return (0) if $l'_{\lambda,q}$ not successfully established and release primary lightpath.

An example of the third case related to the usage of NC wavelengths is depicted in Fig. 3b, where for CR_2, optical wavelength λ_0 cannot be selected by the PCE to achieve NC, i.e., the set of NC wavelengths is empty ($|B| = 0$). This is because both primary lightpaths CR_1 and CR_2 are not link disjoint. In this case, there are not NC features available, and conventional DPP is used instead.

The computation of NC wavelengths is not related to the overall blocking probability. In addition, a backup lightpath suitable for NC is usually shorter than a backup lightpath computed by a DPP scheme, i.e., spans fewer optical links, since part of the path used for the backup lightpath is already reserved by a different backup lightpath, i.e., lightpath $2-D$ using λ''_0 is already reserved, see Fig. 3a, hence the lightpath to be provisioned the *(uncoded lightpath)*– is path S_2-2 using λ'_0. Recall that the advantage of NCP relies on sharing backup network resources. Therefore, in the absence of wavelength conversion, the use of NC vs non NC (DPP) might be counterproductive in the presence of inaccurate NSI. This assessment is validated by the extensive simulation results shown in Section IV.

Both Preference and Non-Preference Coding follows the operation of NC wavelengths described above. The Set of NC wavelengths is the same for both Preference and Non-Preference Coding. However, both schemes differ in the selection of an NC wavelength. Preference coding always selects an NC wavelength without checking its availability. On the other hand, Non-Preference Coding, only selects an NC wavelength that it is computed as available based on global NSI, i.e., NSI that is disseminated by the optical nodes to the PCE. Recall that a wavelength is available when it is not in use in any link of a given path based on global or local NSI, i.e., NSI that is computed by the PCE, hence, avoiding NSI dissemination. In summary Preference and Non-Preference coding works as shown in Algorithm 1 and 2 respectively.

3.2. Predictive Network Coding Protection

An intuitive solution to reduce the negative effects of inaccurate NSI consists on deploying a protection scheme in such way that its TED does not require NSI dissemi-

Algorithm 2 Overall Procedure of Non-Preference Coding.

Input: (Destination node)
Output: ($ResilientLightPath$)

Compute a primary lightpath ($l_{\lambda,p}$)
Select a wavelength in a First-Fit Fashion.
Provision($l_{\lambda,p}$){Attempt to establish the primary lightpath.}
if $l_{\lambda,p}$ not established **then**
  Return 0.
Compute $l'_{\lambda,q}$ in a First-Fit fashion, where $|q \cap p| = 0$.
B=Check NC wavelengths along protection path
if $a \in W_i \forall i \in q \, and \, |B|>0$ **then**
  Provision$(l'_{a,q})$ {Set-up the backup lightpath, where $\alpha \in B$}
  The rest of the algorithm is similar to Algorithm 1

nation (global NSI). This kind of scheme is referred to as Predictive routing algorithms. Therefore, motivated by the good performance of Predictive routing algorithms under the presence of inaccurate NSI, as well the advantages in network throughput improvement brought by NC, we propose a protection scheme devoted for PCE architectures so-called Predictive Network Coding Protection (PNCP).

PNCP extends the predictive concepts widely used in unprotected optical scenarios, and uses them in protected scenarios. However, unlike authors in [12], which use a coarse-granularity approach (predictive counters per lightpath), PNCP adopts a fine-granularity approach for predictive counters (predictive counters per link-wavelength).

Indeed, the use of two-bit predictive counters for computing availability or unavailability has been widely studied in the area of branch prediction on computer architecture. A pioneer study in branch prediction techniques can be found in [15] . This study shows that two-bit predictive counters are more suitable than one-bit predictive counters. In an optical network scenario, the use of a one-bit counter means that it predicts what happened last time, i.e., the last time a connection request was blocked or provisioned. Then the next time that the history is repeated the predictive counters will show out unavailability or availability. Nevertheless, two-bit predictive counters enable to change the direction of the prediction. This is, a lightpath is predicted as unavailable or available only if it is blocked or provisioned two times for the same history.

The proposed strategy so-called PNCP uses predictive counters ($P_{i,\lambda}$) to predict the availability of a wavelength along a link instead of along a lightpath (as the study on [12]). However, similar to [12], PNCP uses two-bit predictive counters, where values from 0 up to 1 predict that a lightpath is available along link i using wavelength λ, whereas values from 2 up to 3 predict the contrary, see Fig. 5. Moreover, predictive counters value are computed as shown in Equation (4), and are locally computed by the PCE scheme.

The reason driving us to adopt two-bit predictive counters is to control the degree of hysteresis of predictive counters. This was first assessed by [15] in computer architecture scenarios. In optical scenarios, this was proven by authors in [16]. Both studies conclude that two-bit counters are sufficient for predicting lightpaths availability. For instance, predictive counters larger than two-bits do not necessarily provide better results, because of the "inertia" that can be built up with a large predictive counter. Therefore, more

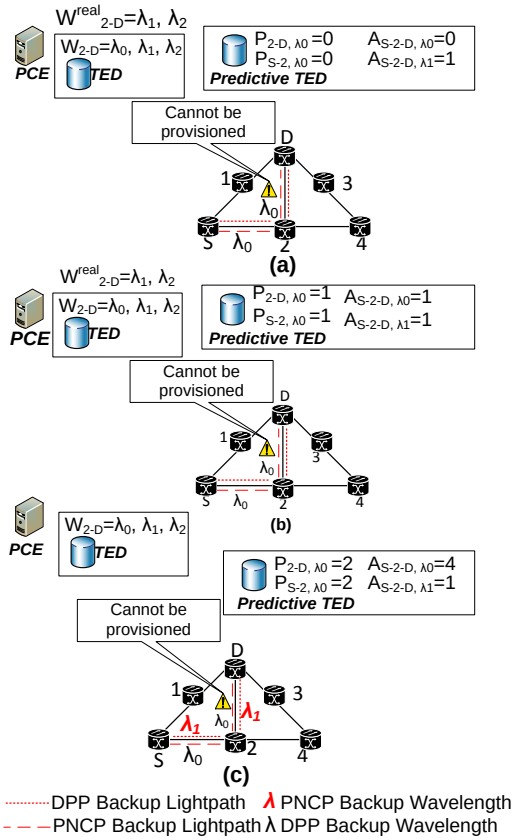


Figure 4: Operation of PNCP under inaccurate NSI.

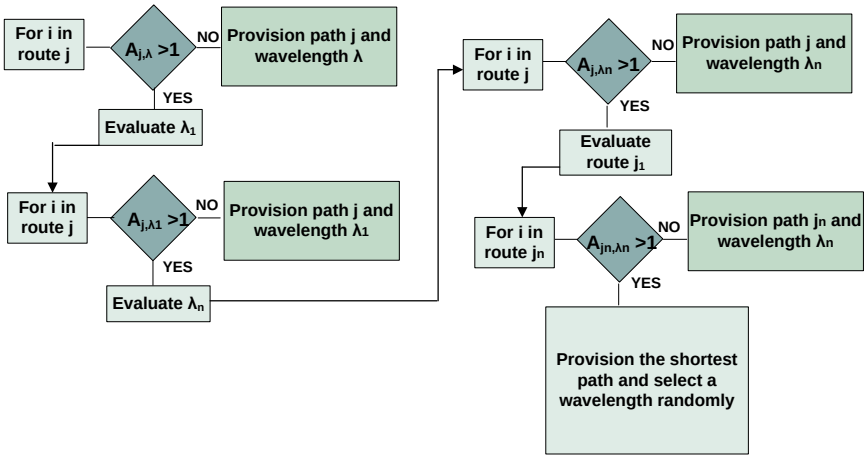


Figure 5: Procedure to compute the availability of a protection lightpath.

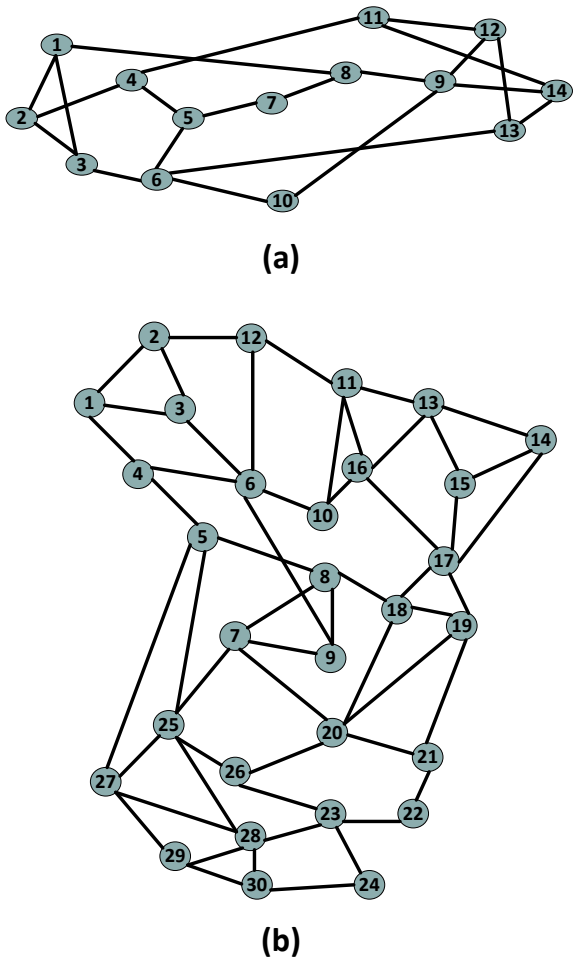


Figure 6: Evaluated topologies: a) NSFNET topology; b) Spanish Backbone topology.

than two changes in the same direction are necessary to change the prediction.

The availability of a lightpath using path j and optical wavelength λ ($A_{j,\lambda}$) is computed as it is shown in Equation (5), where low values of $A_{j,\lambda}$ mean high availability for a path j (high chances to setup a lightpath), and the contrary occurs with high values (low chances to setup a lightpath). Notice that the predictive counter values are squared in order to minimize the selection of lightpaths with predictive counters greater than 2.

$$P_{i,\lambda} = \begin{cases} \textit{blocked lightpath and } P_{i,\lambda} < 3 \rightarrow P_{i,\lambda} + 1 \\ \textit{established lightpath and } P_{i,\lambda} > 0 \rightarrow P_{i,\lambda} - 1 \end{cases} \tag{4}$$

$$A_{j,\lambda} = \frac{\sum_{i \in j} \left(P_{i,\lambda}\right)^2}{N_j} \tag{5}$$

Fig. 5 presents the process for a protection lightpath evaluation. Notice that for a particular path all wavelengths are evaluated. Specifically, a wavelength/link is evaluated by means of predictive counters. If the computed availability has a value greater than 1, then another wavelength is selected, otherwise the lightpath is provisioned. Moreover, in the case that all wavelengths along a candidate path are considered unavailable, another path is evaluated. Then, in the case that no lightpath can be computed, a lightpath is computed by selecting the shortest path in terms of hops and selecting a wavelength in a random manner (not shown in Fig.5). This is done in order to unblock the predictive counters. Moreover, predictive counters are updated immediately by PCE after a connection request is blocked or provisioned. In light of this, optical routers do not need to disseminate NSI to the PCE in order to build the TED, i.e., only predictive counters values are stored in the TED.

For more details related to the operation of PNCP see Algorithm 3, which is described in the following lines.

- PNCP selects a primary lightpath based on its availability computed according to the predictive counters.
- Optical wavelengths are selected in a random manner (the probability of selection of each wavelength is uniformly distributed). The set of candidate paths of the PCE is sorted from the shortest to the longest path taking into account the number of hops as a routing metric.
- When a primary lightpath can be successfully provisioned, PNCP proceeds to compute a potential backup lightpath that must be link-disjoint from the primary lightpath. For this purpose the operation of PNCP is similar, but instead of using a random wavelength selection algorithm, PNCP selects protection wavelengths in a First-Fit fashion, where wavelengths are sorted in a low frequency manner. This is done in order to efficiently pack the optical spectrum, hence avoiding disperse optical spectrum allocation. In this way, there are more chances to deploy NC in the absence of wavelength conversion capabilities.

In order to illustrate the operation of PNCP we consider the scenario shown in Fig. 4. In this scenario, a resilient lightpath must be computed between endpoints S and D. In the case that a conventional protection scheme using global NSI, such as DPP or

Algorithm 3 Overall Procedure of PNCP.

Input: (Destination node)
Output: (*ResilientLightPath*)

Compute a primary lightpath ($l_{\lambda,p}$)
Randomly select a wavelength for primary lightpaths.
Provision($l_{\lambda,p}$){Attempt to establish the primary lightpath.}
if $l_{\lambda,p}$ not established **then**
  Increase the predictive counter of the primary lightpath
  Return 0.
Compute $l'_{\lambda,q}$ in a FF fashion, where $|q \cap p| = 0$.
B=Check NC wavelengths. along $(l'_{\lambda,q})$
if $|B| > 0$ *and* $A_{q,\alpha} < 2$ **then**
  Provision$(l'_{\alpha,q})$ {Set-up the backup lightpath.}
  Return$((l_{\lambda,p}),(l'_{\alpha,q}))$ if the $l'_{\alpha,q}$ successfully established.
  Decrease the predictive counter of the backup lightpath
else
  Provision$(l'_{\lambda,q})$ {Set-up of the backup lightpath.}
  Decrease the predictive counter of the backup lightpath if $l'_{\lambda,q}$ successfully established.
  Return $((l_{\lambda,p}),(l'_{\lambda,q}))$ if $l'_{\lambda,q}$ successfully established.
Increase the predictive counter of the backup lightpath if $l'_{\lambda,q}$ not successfully established.
Return (0) if $l'_{\lambda,q}$ not successfully established and release primary lightpath.

PNCP is used, the path $S-1-D$ using λ_0 for the primary lightpath (not shown in Fig. 4) and path $S-2-D$ using λ_0 for the backup lightpath will be selected. Unfortunately, when using any of the two schemes (DPP and PNCP), the backup lightpath will not be provisioned because λ_0 is not available on link $2-D$, see Fig. 4a. This occurs because the NSI available on the TED related to link $2-D$, i.e., W_{2-D} is inaccurate. As a result, PNCP will increment the predictive counters along the selected path P_{S-2,λ_0} and P_{2-D,λ_0}. In the case another subsequent connection requests arrives (before the next updating time) for a resilient lightpath between endpoints S and D (see Fig. 4b), both DPP and PNCP will result on the blocking of the backup lightpath, similar to Fig. 4a.

However, in the case a third subsequent connection requests arrives (before the next update time) requesting a resilient lightpath between endpoints S and D. DPP and PNCP will work differently. DPP will continue selecting lightpath $S-2-D$ using λ_0 as a backup lightpath, this will undoubtedly lead to blocking the lightpath because the NSI available on the TED still hasn't updated its NSI related to optical link $2-D$. Conversely, PNCP will be able to capture the unavailability of wavelength λ_0 along link $2-D$ due to NSI available on the predictive TED. Thus, it will select λ_1 instead, see Fig. 4c. Notice that the predictive TED contains NSI locally computed by the PCE scheme, i.e., predictive counters and lightpath availability.

3.3. Complexity and Deployment Issues of Predictive Network Coding Protection

The PNCP algorithm comprises two phases: 1) an offline path generation phase –assuming fixed-alternate path routing, and 2) an online lightpath selection phase (as shown in Algorithm 1). In the path generation phase, $|M_{s,d}|$ pre-computed (candidate) link-disjoint paths using a two-step approach are generated offline by means of Dijkstra's algorithm with a complexity of: $O\left(|M_{s,d}||E| + |V|log(|V|)\right)$. For the worst case scenario, the

online phase has a complexity of (assuming a single-fiber network): $O\left(4(|M_{s,d}| \times |W|)\right.$. In case of topology changes, the set of candidate paths are computed again. In addition, at the time of selecting a backup lightpath, the PCE does not consider the paths that are not link-disjoint from the recently selected primary lightpath.

On the other hand, in order to consider a feasible deployment of PNCP, physical impairments such as the Maximum Transmission Distance (MTD) need to be taken into consideration. The MTD specifies the maximum distance an optical signal can travel with an accepted quality level (mostly based on the so-called Q Personick's factor) without optical signal regeneration. The performance impact of physical impairments is highly relevant in terms of Bit Error Rate and Power Consumption.

In this paper, we consider that there is not optical signal regeneration, and a fixed-grid spectrum of 50 GHz using Dual-Polarization Quadrature Phase-Shift Keying (16-QAM) modulation format. Under this setting the maximum transparent reach is 500 km [17]. We must remark that there are already studies available in the literature dealing with predictive based RWA algorithms taking into account physical impairments as well as inaccurate NSI [18]. The related studies solely consider unprotected scenarios. Therefore, we think that an evaluation in protected scenarios jointly with NC will is an interesting research work. Unfortunately, in this paper we left this issue as a future line of work due to space constraints.

Another deployment issue to be considered is the ability of PNCP to adapt to new transmission technologies, such as Elastic Optical Networks (EONs), where different rate or different modulation format are considered. It has been already shown by authors in [19], that the practical implementation of optical XOR operations for optical data streams with different modulation schemes, such as BPSK and QPSK is also possible under test lab scale. Moreover, studies such as [20], show the benefits related to the P_{cost} when combining EONs and NC.

4. Simulation Results

In this section, we introduce extensive simulation results with regard to the performance of different proactive protection schemes, namely DPP and NCP using distinct routing algorithms evaluated on both the well-known NSFNET topology, and a model of the Spanish Backbone topology, see Fig. 6a and Fig. 6b respectively. The simulation results presented in this section are obtained using the widely used network simulation framework called Omnetpp [21]. Moreover, all plotted values have a 95% confidence interval not larger than 0.5% of the plotted value. The implemented simulation model used to validate and obtain the presented simulation results can be found in [22].

The evaluated protection schemes are the following: a dynamic DPP implemented as a conventional routing algorithm LCP-FF (Least-Congested and First-Fit) requiring global NSI, dynamic DPP schemes with NC capabilities namely DPPNC and DPPNC+ (DPPNC is based on a Preference Coding strategy, where as DPPNC+ is based on a Non-preference Coding strategy); and finally PNCP. Notice that we only consider proactive protection schemes in our evaluation since, it would not be fair to compare them.

4.1. Evaluation Methodology

In this subsection, we describe the network model used in this paper for which the following settings apply:

- Connections requests arrive at the PCE according to a Poisson process. The arrival time of a request is not known in advance. The holding time of each connection is negative exponentially distributed with a mean of 50 time slots. Notice that holding time for each connection request does mention the time required for its data transmission. For instance, consider transactional traffic such as file transfer backup [23].

- A time slot is defined as the time required to transmit 100 Gbits of traffic.

- All CRs demand the provisioning of both a primary and backup lightpath (resilient CRs). A backup lightpath is computed solely when its primary lightpaths is successfully provisioned. In addition, each connection request requires a full wavelength on each link –grooming is not assumed. Therefore, the cost to send traffic along an optical link is 1 u. This assumption is motivated by the high bandwidth demands within DCNs –above 100 Gbps.

- A Fixed-grid spectrum of 50 Ghz and 10 Ghz channel band guard. This setting leads to a bit rate of 100 Gbps, using Dual-Polarization Quadrature Phase-Shift Keying (16-QAM) modulation format.

- A periodical updating policy, i.e., update NSI messages are triggered (disseminated) periodically.

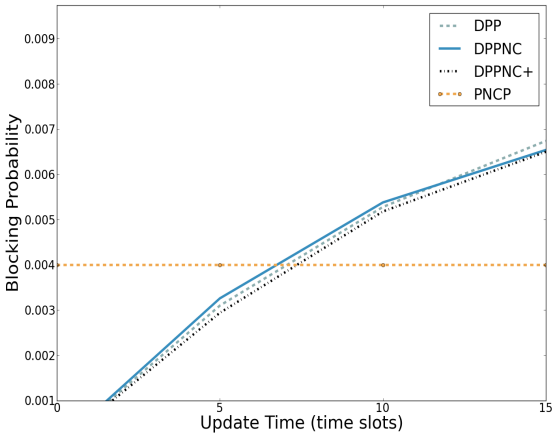
- Blocked CRs are not reattempted. The rationale behind this assumption is to avoid long setup times. Despite that connection reattempts are in the order of hundred of milliseconds, the impact of connection reattempts cannot be neglected when the propagation delay is high or in highly dynamic scenarios where it is expected to provision lightpaths on a short-term basis.

- Optical nodes do not have wavelength conversion capabilities. In addition, for any source-destination pair the PCE has at least 2 link-disjoint candidate paths. The candidate paths are computed off-line by means of Dijkstra's algorithm. The candidate paths will be recomputed if the network topology changes.

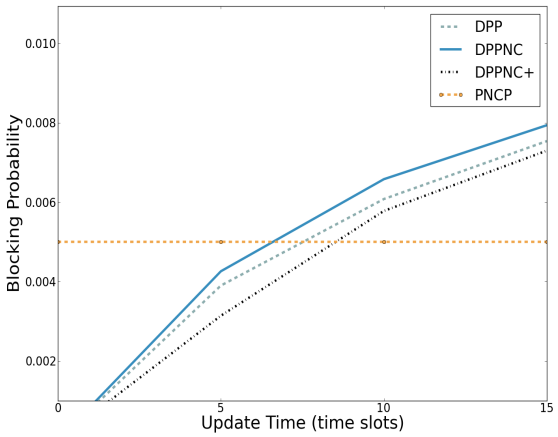
- 80 wavelengths per fiber (single-fiber per optical link). This assumption is based on the channel spacing standards defined by the International Telecommunication Union (ITU).

- NC operations are based on the Exclusive-Or operation (XOR) and are done over $GF(2)$, i.e., the Galois field of two or more data streams. Moreover, we solely consider to use NC for backup lightpaths with the same destination node.

- Lightpath reconfiguration is not allowed. Once a resilient lightpath is established, we do not reconfigure the lightpath to enable NC with other data streams allocated along a different lightpath. This assumption is done to avoid unwanted transient behavior during the reconfiguration process. Therefore, in order to avoid switching matrix reconfigurations, we also assume that solely lightpaths with same destination are suitable for NC.

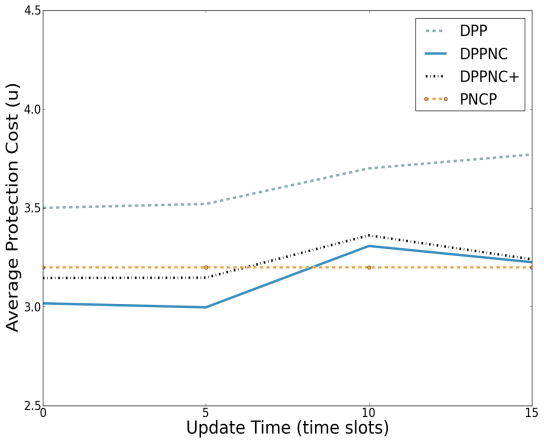


(a)

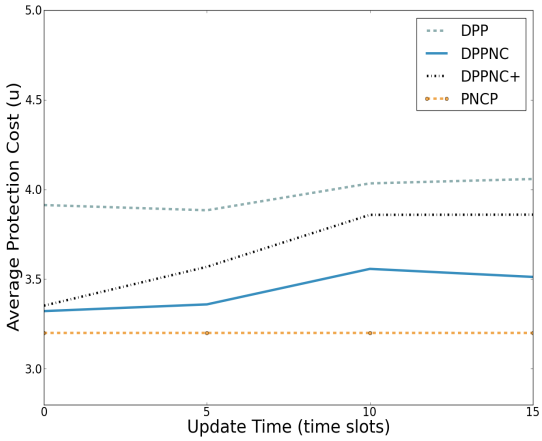


(b)

Figure 7: Blocking Probability vs Update time for: a) NSFNET topology; b) Spanish Backbone topology.

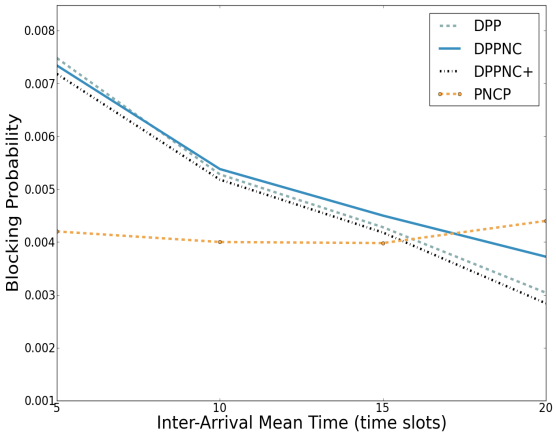


(a)

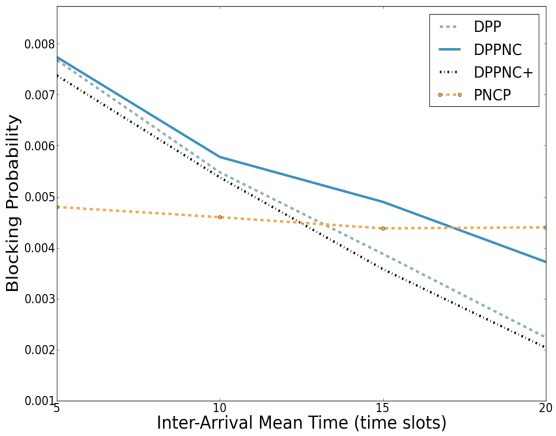


(b)

Figure 8: Average Protection Cost vs Update time for: a) NSFNET topology; b) Spanish Backbone topology.



(a)



(b)

Figure 9: Blocking Probability vs Connection inter arrival mean time for: a) NSFNET topology; b) Spanish Backbone topology.

4.2. Evaluation of the Blocking and Protection Cost Performance

Fig. 7 shows the blocking probability related to the computation of resilient lightpaths for all the evaluated schemes and topologies for different spectrum of update time values and an inter-arrival time of 10 slots. As it can be observed, the performance of DPP, DPPNC and DPPNC+ is highly sensitive to the update time and it is only optimal for low update time values. However, the performance of PNCP is not affected by an increase of the update time. This is because PNCP computes lightpaths based solely on local NSI; hence, it avoids periodically dissemination of NSI.

In addition, it is worth mentioning that the blocking probability for all evaluated schemes is lower in the NSFNET topology in comparison with the Spanish Backbone topology. This is due to topology properties, mainly rooted on the fact that the Average Shortest Path Length of the NSFNET topology is 2 hops, whereas for the Spanish Backbone topology is 3.30 hops. This confirms that in protected scenarios –similar to unprotected scenarios– under the presence of inaccurate NSI, it is better to use paths that span less hops, i.e., there is higher blocking probability of blocking with long paths that with shorter paths.

Notice that the blocking probability of DPP is slightly lower than DPPNC, as a result of the constraint related to the wavelength assignment imposed by preference-coding strategy. DPPNC has a limited set of optical wavelengths for path computation actions, since it only considers optical wavelengths that enable network coding; hence, there is a higher probability of blocking.

Fortunately, the blocking probability of an NCP scheme can be further reduced following an Non-preference Coding strategy as it is demonstrated by the performance of DPPNC+. DPPNC+ has a slightly higher performance compared with DPPNC because DPPNC+ considers the complete set of optical wavelengths for path computation actions. Recall, that according to a preference coding strategy an optical wavelength is selected only if it supports NC and it would not lead to blocking (based on the global NSI). However, it is intuitive that as the NSI is more inaccurate (a higher update time), the performance of DPPNC+ tends to decrease. Indeed, this is the case for all the evaluated protection schemes based on global NSI. Based on the simulation results shown in Fig. 7, the reader may notice that the performance of DPP, DPPNC and DPPNC+ tends to be similar for high update time values.

Moreover, Fig. 8 depicts the *Average Protection Cost* (*APC*) versus the Update time, assuming an inter-arrival time and holding time of 10 time slots respectively. The *APC* is computed as the total P_{cost} divided by the number of protection paths successfully provisioned. We consider that the *APC* is a fair way to compare the P_{cost} of distinct proactive protection schemes under different blocking probabilities.

It is not surprising that among the evaluated schemes DPP yields the highest *APC* –an average of $3.5\,u$ and $3.9\,u$ per backup path for the NSFNET and Spanish Backbone topologies respectively– because of its inability to code traffic, whereas PNCP yields the lowest *APC* –an average of $3\,u$ – due its preference for selecting shortest-routes as long as it successfully enables NC. Notice that the *APC* of DPPNC+ is not as low as DPPNC since the former does not give preference to NC. Therefore, it can be stated that there is a tradeoff between blocking probability and APC achieved by an NCP scheme. In addition, notice that the APC is not as sensitive to the Update time as it is the case for the blocking probability.

Based on the results shown in Fig. 8, we conclude that inaccurate NSI does not has a significant impact on the P_{cost}. It is topology characteristics such as, the Average Shortest Path Length which impact on the P_{cost}. Fortunately, independently of the network topology and the NSI inaccuracy, NC is a suitable strategy for reducing the P_{cost}, even under inaccurate NSI conditions. In addition, topology characteristics such as the Average Shortest Path Length affect the performance of a protection scheme in terms of P_{cost}. Indeed, the results depicts in Fig. 8 shows that the advantages of NC related to the P_{cost} is higher on the Spanish backbone topology in comparison with the NSFNET topology.

Finally, Fig. 9 shows the blocking probability versus the connection inter-arrival arrival mean time, and a update time of 16 time slots. For this scenario, we attempt to evaluate the inaccuracy added by the dynamicity of CR arrivals. Low connection arrival mean times leads to high inaccurate NSI, the contrary occurs with high connection arrival mean times. To this end, we fix the update time to 16 time slots and we evaluate the blocking probability of for distinct connection arrival mean time values. Similar to the results shown in Fig. 7, it can be stated that PNCP and DPPNC yield the lowest and highest blocking probability respectively. Notice that the performance of the evaluated protection schemes is less sensitive to the inaccuracy added by low connection arrival mean times in comparison to high update times. Nevertheless, the simulation results shown Fig. 9 validate that under inaccurate NSI, local NSI is more reliable than global NSI in order to achieve less blocking.

Based on the obtained simulation results, the following lessons were learned related to the study of dynamic proactive protection schemes under inaccurate NSI.

- The frequency of NSI dissemination as well as the connection arrival mean time substantially impact on the blocking probability of dynamic protection schemes.
- Predictive NCP schemes such as PNCP can outperform conventional protection schemes as well as NCP schemes which rely on global NSI under the assumption of realistic (greater than 5 time slots, or on average less than 10 update messages during the lifetime of a connection) update time slots.
- The blocking Probability of an NCP scheme with a Preference Coding strategy is slightly higher than conventional DPP under inaccurate NSI.
- Network Coding is a feasible strategy for reducing the P_{cost}, but its use should be moderated in order to avoid an increase of the blocking probability when global NSI is assumed.
- Topology characteristics such as the Average Shortest Path Length, has an impact on the blocking probability and P_{cost}.

5. Conclusions

In this paper, we present a novel proactive protection scheme referred to as Predictive Network Coding Protection (PNCP). PNCP is devised to mitigate the negative effects of inaccurate Network State Information (NSI) on the blocking probability in dynamic protected scenarios, where resilient lightpaths (primary and link-disjoint backup lightpaths) are setup and tear-down in a short-term basis. Based on the obtained results,

it can be stated that the proposed protection scheme significantly improves the performance obtained by conventional protection schemes in network scenarios with routing inaccuracy, as well as it yields a lower utilization of those network resources dedicated for path protection. As a future line of work we plan to evaluate the benefits of NC under flexible optical spectrum grids, i.e., elastic optical network scenarios.

Acknowledgments

This work was supported by the Spanish Ministry of Science and Innovation under contract TEC2012-34682, project partially funded by FEDER and the EU PACE project FP7.

[1] *C. Kachris, K. Kanonakis, and I. Tomkos, "Optical interconnection networks in data centers: recent trends and future challenges,"* Communications Magazine, IEEE, *vol. 51, no. 9, pp. 39–45, September 2013.*

[2] *W. Ramirez, X. Masip-Bruin, E. Marin-Tordera, and S. Sa nchez-Lopez, "Managing resilience in carrier grade networks: Survey, open issues and trends,"* Computer Communications, *vol. 61, pp. 1 – 16, 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S014036641500095X*

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

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

[5] *P. Babarczi, G. Biczok, H. Overvy, J. Tapolcai, and P. Soproni, "Realization Strategies of Dedicated Path Protection: A Bandwidth Cost Perspective,"* Comput. Netw., *vol. 57, no. 9, pp. 1974–1990, Jun. 2013. [Online]. Available: http://dx.doi.org/10.1016/j.comnet.2013.03.015*

[6] *R. Munoz, R. Casellas, R. Martinez, and R. Vilalta, "PCE: What is It, How Does It Work and What are Its Limitations?"* Lightwave Technology, Journal of, *vol. 32, no. 4, pp. 528–543, Feb 2014.*

[7] *M. Cuaresma Saturio, V. López, O. de Dios, and J. Fernández-Palacios, "Implementation and Assessment of Pre-reservation Mechanism for PCE Environments,"* Journal of Network and Systems Management, *vol. 22, no. 3, pp. 488–508, 2014. [Online]. Available: http://dx.doi.org/10.1007/s10922-013-9296-y*

[8] *J. Zhou and X. Yuan, "A Study of Dynamic Routing and Wavelength Assignment with Imprecise Network State Information," in* in Proceedings of International Conference on Parallel Processing Workshops (ICPPW 02), *2002, pp. 202–207.*

[9] *M. Peroza Marval, J. Chen, L. Wosinska, and A. Fumagalli, "Adaptive routing based on summary information mitigates the adverse impact of outdated control messages," in* Transparent Optical Networks (ICTON), 2011 13th International Conference on, *June 2011, pp. 1–4.*

[10] *W. Ramirez, X. Masip-Bruin, E. Marin-Tordera, M. Yannuzzi, A. Martinez, S. Sanchez, M. Siddiqui, and V. Lopez, "A techno-economy study of network coding protection schemes," in* Global Communications Conference (GLOBECOM), 2014 IEEE, *Dec 2014, pp. 2148–2153.*

[11] *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.*

[12] *E. Ahvar, E. Marin-Tordera, M. Yannuzzi, X. Masip-Bruin, and S. Ahvar, "FRA: A new fuzzy-based routing approach for optical transport networks," in* Networks and Optical Communications (NOC), 2012 17th European Conference on, *June 2012, pp. 1–6.*

[13] *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.*

[14] *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.*

[15] *J. E. Smith, "A Study of Branch Prediction Strategies," in* Proceedings of the 8th Annual Symposium on Computer Architecture*, ser. ISCA '81. Los Alamitos, CA, USA: IEEE Computer Society Press, 1981, pp. 135–148. [Online]. Available: http://dl.acm.org/citation.cfm?id=800052.801871*

[16] *E. Marin-Tordera, X. Masip-Bruin, S. Sanchez-Lopez, J. Sole-Pareta, and J. Domingo, "The prediction-based routing in optical transport networks."* Computer Networks*, vol. 29, pp. 865–878, 2006.*

[17] *J. Lopez, Y. Ye, V. Lopez, F. Jimenez, R. Duque, P. Krummrich, F. Musumeci, M. Tornatore, and A. Pattavina, "Traffic and power-aware protection scheme in Elastic Optical Networks," in* Telecommunications Network Strategy and Planning Symposium (NETWORKS), 2012 XVth International*, Oct 2012, pp. 1–6.*

[18] *E. Marin, S. Sanchez, X. Masip, J. Sole, G. Maier, W. Erangoli, S. Santoni, and M. Quagliotti, "Applying Prediction Concepts to Routing on Semi-Transparent Optical Transport Networks," in* Transparent Optical Networks, 2007. ICTON '07. 9th International Conference on*, vol. 3, July 2007, pp. 32–36.*

[19] *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.*

[20] *W. Ramirez, X. Masip-Bruin, M. Yannuzzi, D. Montero, A. Martinez, and V. Lopez, "Network coding-based protection scheme for Elastic Optical Networks," in* Design of Reliable Communication Networks (DRCN), 2014 10th International Conference on the*, April 2014, pp. 1–8.*

[21] *http://www.omnetpp.org/, [Online; accessed November-2015].*

[22] *(2015) http://www.craax.upc.edu/, [Online; accessed November-2015].*

[23] *A. Ebrahimzadeh, A. G. Rahbar, and B. Alizadeh, "Request differentiation in dynamic light-path establishment for {WDM} routed all optical networks of data centers,"* Optical Fiber Technology*, no. 0, pp. –, 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1068520014001321*