An Efficient Protection Strategy Using Multiple Network Coding

W. Ramirez, X. Masip-Bruin, M. Yannuzzi, R. Serral-Gracia, A. Martinez

***Abstract*—Network coding has been recently proposed as a proactive network protection scheme. Its main objective is to improve the resilience of wired networks against link failures in a proactive manner, while simultaneously providing network resource savings (IP bandwidth, optical wavelengths) compared to traditional protection schemes. Warned by the potential network coding might bring as well as by the high chances this strategy might be widely deployed on failure-sensitive network scenarios, this paper is positioned with the aim of: i) exploring the advantages of network coding protection (NCP) versus the network resources used for protection; ii) comparing NCP with traditional protection schemes, such as shared path protection; iii) exploring the tradeoff between the protection cost and the level of resilience provided by a NCP scheme, and; iv) exploring the benefits of coding a coded traffic, in other words, introducing multiple coding for protection. Several protection schemes are evaluated in different incremental network topologies. The obtained results show that network coding with a M+N strategy can significantly reduce the amount of network resources used for protection.**

***Index Terms*—Protection Schemes, Network Coding, Resilience.**

I. Introduction & Motivation

Network resilience is an essential feature highly appreciated and demanded by network providers, contemplated at the network planning phase with the aim of protecting the network offered services against network failures. Typical protection schemes commonly deployed by network operators to enable fault-tolerant services include 1+1, 1:N, and M:N protection [1], all behaving different in terms of recovery time, cost of protection and the level of resilience they provide.

In a 1+1 protection scheme a dedicated backup link for every primary link to be protected is set. Normal operation requires the traffic to be simultaneously sent through the primary and the backup links, while at the reception node, only the traffic received from one link is chosen, according to a particular selection criteria. Therefore, a 1+1 protection scheme provides a very small recovery time, but unfortunately also requires to over-dimensioning the network, which can be disastrous for a small network operator.

W. Ramirez, X. Masip-Bruin, M. Yannuzzi, R. Serral-Gracia, A. Martinez are with the Advanced Network Architectures Lab (CRAAX), Spain (emails: wramirez, xmasip, yannuzzi, rserral, annym@ac.upc.edu).

This work was supported by the European Commission through the ONE project (www.ict-one.eu) in the Seventh Framework Program (FP7), contract nr. INFSO-ICT-258300. UPC authors also acknowledge the support received by the Spanish Ministry of Science and Innovation under contract TEC2012-34682, and the Catalan Research Council (CIRIT) under contract 2009 SGR1508.

Reducing the network dimension drives to resources sharing. Thus, in a M:N protection scheme (also known as shared-path protection) M backup paths are dedicated to protect N primary links (of course, M<N). Whenever a primary link fails, the traffic sent along this link is switched to one of the M backup paths. Therefore, a M:N protection scheme requires less network resources for protection, i.e., less links, but the recovery time is higher than a 1+1 protection scheme.

Looking at the two schemes presented so far, it seems obvious that the optimal objective should be to find out an approach adopting the small recovery time obtained by 1+1 and the low resources consumption obtained by the M:N. Hence, a evolutionary proposal could be based on extending M:N to reduce its recovery time. To this end, normal operation would require the traffic on the N primary links to be simultaneously sent in parallel along the M backup paths (similar to 1+1 protection and known as M+N protection). Unfortunately, a M+N protection scheme is severely constrained by real network resources availability (IP bandwidth, optical wavelengths). For instance, a single backup path shared by two primary links may not have enough resources to transport the traffic sent along the two primary links, hence again, an over-dimensioning of the network is required, what does not solve the problem. It looks evident that providing high levels of protection while minimizing resources consumption requires novel strategies different than those built by extending traditional protection techniques.

A tentative solution to provide protection features falls in the area of network coding, a technique utilized in several networking areas for throughput reduction [2], [3]. In fact network coding has been recently proposed for reducing the network resources dedicated for protection [4], [5] and [6]. Authors in [7] improve the work in [5], by using a shared-path protection strategy instead of p-cycles. Other initiatives, such as [8] expand network coding protection to multidomain networks with a combination of 1+1 protection and dual homing. More recently [9] proposes a formulation of a mathematical optimization model for 1+1 protection using network coding and [10] provides a comparative analysis of 1+1 protection and 1+1 protection with network coding.

In this paper, we have two key objectives. First we present a deep comparison of shared-path protection (SP) and shared-path protection with network coding (SPNC) in terms of network resource savings, hence extending the works presented in [10], [9]. In addition, our work combines the use of SP and SPNC to overcome the limitations of the number of links to be protected by SPNC, hence maximizing the network resilience

level. Second, we propose by first time the use of multiple coding for protection, i.e., the coding of a coded traffic, in order to maximize the network resource savings.

The rest of this paper is organized as follows. Section II introduces network coding as a protection scheme. Section III describes the set of conditions that must be fulfilled for protecting a link using network coding, and also introduces the proposed protection scheme. Section IV provides an evaluation of the proposed protection scheme versus other protection schemes using several network topologies. Finally, section V provides some insights and final conclusions.

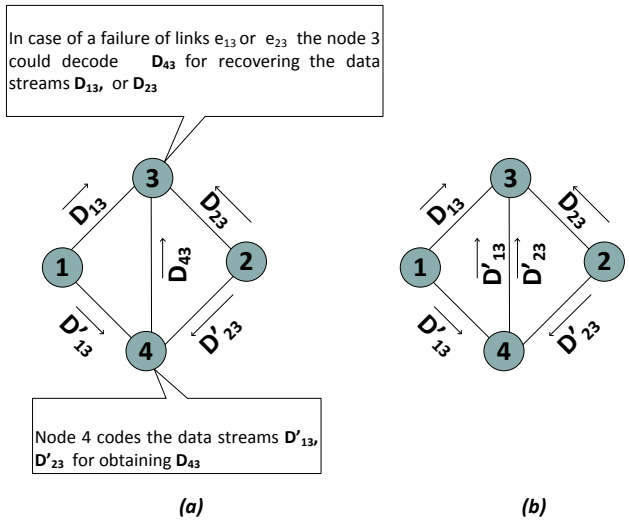
II. Network Coding as a Protection scheme.

For the purpose of illustrating the advantages of network coding as a protection scheme (NCP) we consider the network scenario in Fig. 1a, showing a single layer network represented with a graph $G = (V, E)$, where V is the set of nodes and E is the set of edges. All nodes in V could either correspond to an optical node or a router, and all edges in E could either correspond to an IP link between two routers or an optical fiber between two optical nodes. It must be remarked that in the scenario depicted in Fig. 1a the network elements are homogeneous, i.e., all nodes are of the same technology, either a router or an optical node.

Implementing network coding along with a shared-path protection strategy as a protection scheme for protecting two links, such as links e_{13} and e_{23}, requires nodes 1 and 2 to retransmit to node 4 the data streams (a data stream may be IP traffic or an optical burst) sent along these links. Hence, nodes 1 and 2 send to $node$ 4 the data streams D'_{13}, D'_{23} respectively. Afterwards, node 4 performs the coding (an exclusive-or logical operation) of the data streams $D'_{13} \oplus D'_{23}$. As a result, the data stream D_{43} encoding the data streams D'_{13} and D'_{23} is obtained. Then, $node$ 4 sends the data stream D_{43} to $node$ 3. Notice that $node$ 3 can decode the data streams D'_{13} and D'_{23} by executing the XOR operation of $D_{43} \oplus D_{13}$ to obtain D'_{23}, and $D_{43} \oplus D_{23}$ to obtain D'_{13}. Therefore, if a failure occurs on links e_{13} or e_{23}, node 3 can instantly recover the corresponding traffic.

It must be remarked that network coding operations can be done electrically, or optically. For instance, an optical node could perform the coding operations without any optical to electrical conversion [11], this represents a performance improvement in IP over optical networks. On the other hand, it is also important to notice that the example shown in Fig. 1a is valid only for the case of a single failure scenario. In the case of two simultaneous failures, for example on links e_{23} and e_{13} it would be impossible to restore the traffic sent along the affected links using NCP, since an original data stream (D_{13} or D_{23}) is needed in order to decode the data stream D_{43}.

In comparison with traditional protection schemes, network coding with a shared-path protection strategy can reduce the amount of network resources dedicated for protection. This is due to the fact that multiple data streams could be aggregated into one data stream. For instance, suppose that the data



• D'_{13}, D'_{23} are replicas of the data streams D_{13}, D_{23} respectively

Figure 1. a) Network Coding as a protection scheme with shared-path protection; b) shared-path protection with no network coding.

streams D_{13} and D_{23} are optical bursts that require the allocation of U optical wavelengths respectively. In a scenario of shared-path protection without network coding, $4U$ optical wavelengths will be needed to protect links e_{13} and e_{23}; i.e., the data stream D'_{13} will be sent along the links e_{14}, e_{43} ($2U$), and the data stream D'_{23} will be sent along the links e_{24}, e_{43} ($2U$), see Fig. 1b. However, when applying network coding only $3U$ of optical wavelengths are required to protect the links e_{13} and e_{23}, since only one U of optical wavelengths is required to send D'_{13} and D'_{23} along the link e_{43}, since D'_{13} and D'_{23} are aggregated into one data stream (D_{43}), see Fig. 1a. In fact, the advantage of network coding resides in the aggregation of data streams.

It must be also highlighted that the scenario shown in Fig. 1a is used just as a proof of concept for illustrating the advantages of using network coding for protection. In a real network scenario, employing network coding protection would require to select the most suitable nodes coding traffic and links will carrying the coded traffic, which can be an arduous task because the current carrier networks consist of hundred of links and nodes.

III. Network coding with a shared-path strategy

Deploying network coding as a protection scheme using a M+N (shared-path) strategy for single failure scenarios requires the following conditions to be met:

- Protecting N primary links demand N' backup paths satisfying equation (1). The path τ is the coding path, i.e., the coding path is the path that carries the coding of the traffic sent along the N primary links. Moreover, the first node of the coding path is the node that will code the traffic of all the N primary links.

$$\bigcap_{i=1}^{\|N'\|} N'_i = \tau \; and \; \tau \neq 0. \tag{1}$$

- A primary link N_j, and its backup path N'_i are link-disjoint.

$$N_j \bigcap N'_i = 0 \tag{2}$$

$$\forall\, j\epsilon\ \{1, ..., \| E \|\},\ i\epsilon\ \{1, ..., \| N' \|\}$$

As it can be observed in Fig 1.a the backup paths for links e_{13} and e_{23} are $N_1 = e_{14}, e_{43}$ and $N_2 = e_{23}, e_{43}$ respectively. The intersection of these two paths form the coding path τ, $\tau = e_{43}$. Based on the conditions previously described it can be deduced that the number of links that can be protected using network coding for single failure scenarios is: $\sum_i^{\|V'\|} (D_{in}(V'_i) - 1)$, such that V' is a set gathering by all nodes with an indegree equal or higher than 3. Therefore, it will be impossible to protect all links of a network using network coding with a shared-path strategy. As a consequence, we propose to combine the use of shared-path strategy with network coding (SPNC) and shared-path protection (SP).

The proposed protection strategy consists in a two step process. The objective of the first step is twofold: 1) to employ SPNC protection to protect the maximum number of links, and 2) to use the minimum amount of network resources for protection. The second step consists in using SP protection for those links not yet protected in the first step.

Other initiatives as those in [9], [10] already proposed the use of network coding along with a 1+1 protection scheme. Although our approach is similar to those initiatives we adopt a different terminology (shared-path instead of 1+1 protection), because from our point of view, the backup paths are not link-disjoint between them, since all share the coding path.

Moreover, our proposed protection scheme also introduces and exploits multiple coding for reducing the protection cost, and hence it is not limited to the exclusive use of one protection scheme, i.e., combining the use of SPNC and SP schemes.

It is also important to mention that according to [9] a condition for applying network coding is that two or more links must have one common destination. However network coding can be also employed in other scenarios. For instance, consider the network scenario shown in Fig. 2a. The links to be protected using network coding are e_{13} and e_{25}. To this end, nodes 1 and 2 must send to node 4 the data streams D'_{13} and D'_{25} respectively, and then node 4 codes these two data streams to obtain the data stream D_{43}, that is sent to node 3 along the link e_{43}. If a failure in link e_{13} comes up, node 3 will need the data stream D_{25} in order to decode D_{43} and obtain D_{13}. Therefore, node 5 must retransmit the data stream D_{25} to node 3. On the other hand, if a failure comes up in link e_{25}, node 3 can decode D_{43} for obtaining D_{25}, and then send this data stream to node 5.

Unlike the network scenario shown in Fig.1a the links to be protected have different endpoints, hence, in order to compute the cost of protecting links e_{13} and e_{25} it is required to add the decoding cost (in Fig. 1a the decoding cost is 0), $Cost_{protection}\ (e_{13},\ e_{25}) = cost_{coding} + cost_{decoding} + cost_{codingpath} = 5U$.

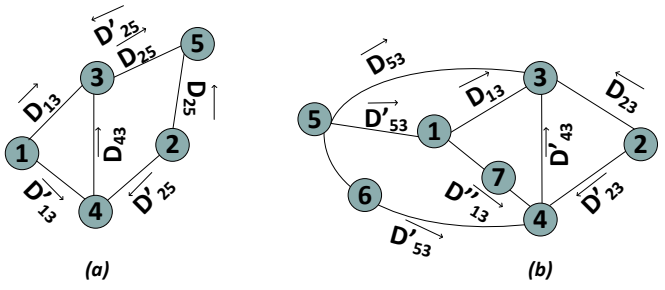


Figure 2. a) Protection of links of different endpoints; b) NCP with multiple coding.

Thus the decoding cost is the cost necessary for decoding the coded data stream, which is equal to zero when the coding node is the destination node of the protected links. The coding cost is the cost required for sending the protected data streams to the coding node (node 4 for the case of Fig. 2). Finally, the coding path cost is the cost for sending the coded data stream (D_{43}) along the coding path (e_{43}). Since the decoding cost increases the protection cost, in our protection strategy we prioritize the protection of links with common endpoints.

As mentioned above, the proposed protection strategy employs multiple coding in order to maximize the network resource savings, i.e., minimizing the cost of protection. Multiple coding refers to action of coding already coded data. For instance, consider the scenario depicted in Fig. 2b. If links e_{13}, e_{23}, e_{53} are desired to protect with network coding, then nodes 1 and 4 must perform the following coding operations. Node 1 can code the data streams D'_{53} and D'_{13} in order to obtain D''_{13}, and node 4 can code D''_{13} and D'_{23} in order to obtain D'_{43}, hence, the protection cost is reduced to $5U$. It is important to notice, that even thought the shortest path that can be used by node 5 to send the data stream D_{54} is $SP\,(5, 4) = e_{56}, e_{64}$ (taking into account a hop metric), it would be better using the path e_{51}, e_{17}, e_{74} because of the multiple coding feature, e.g., using $SP\,(5, 4)$, $Cost_{protection}\ (e_{13},\ e_{23},\ e_{53}) = 6U$.

IV. Evaluation Results.

For the purpose of evaluating the performance of network coding protection, the programming language python [12] and the library NetworkX [13] (a tool for creating and manipulating graphs and networks) were used for building a testbed in which the three evaluated protection strategies (SP, SPNC, SPNC*) were implemented. Moreover, the performance of the proposed protection scheme is evaluated on the three network topologies shown in Fig.3: a topology with butterfly characteristics (B1), the well known NSFNET topology, and a real network topology deployed at Telefonica I+D premises (TID). Performed trials assumed the following conditions:

- Each traffic demand generated from a given node requires the assignment of $1U$ of network resource, i.e., the traffic sent by node x destined to a node y along a link e_{xy}, will consume $1U$ of network resource of link e_{xy}.

Table I
PERCENTAGE OF PROTECTION COST OVER THE TOTAL OF NETWORK RESOURCES AVAILABLE.

Protection schemes	Evaluated network topologies		
	B1 topology	NSFNET topology	Telefonica I+D topology
SP	28%	36%	23%
SPNC	27%	33%	22%
SPNC*	26%	32%	20%

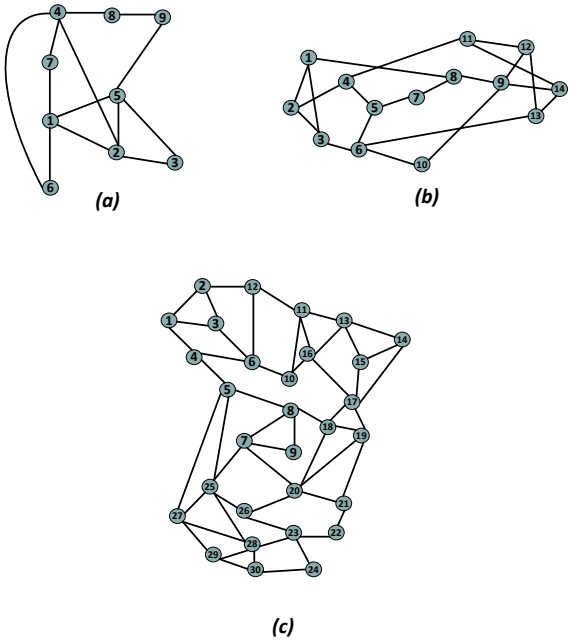


Figure 3. Evaluated network topologies: a) B1 topology; b) NSFNET topology; c) Telefonica I+D topology.

- The shortest-path routing algorithm for computing routes uses hops as metric.
- A link is considered congested when more than the 50% of its capacity is used for protection.

It must be noticed that the proposed protection scheme will be employed at the network planning phase, hence, traffic is not generated dynamically, rather it is assumed a certain link capacity to cope with the expected traffic demand and the protection traffic. Moreover, the performed evaluation is done under the premise that the network topology is static, i.e., it maintains its structure during time; therefore, a modification in the network topology will require a new network planning for defining the protection levels.

The proposed approach is compared vs other strategies. In particular, we obtain results for a shared-path protection (SP), shared-path protection with network coding (SPNC), and shared-path protection with multiple coding (SPNC*). Notice that as described in section III there is a certain amount of links that cannot be protected in the case that SPNC or SPNC* schemes are used, hence, for these links a shared-path protection without network coding is employed.

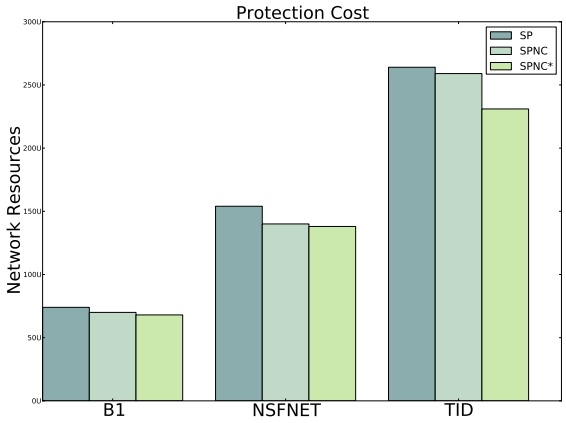


Figure 4. Comparison of protection cost.

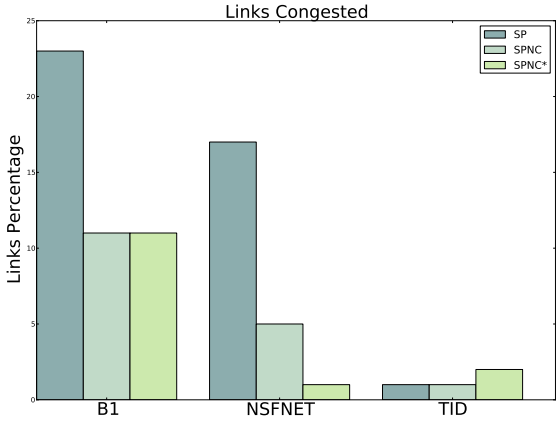


Figure 5. Comparison of links congested.

Evaluation results for all three network topologies are depicted in Fig. 4, and Fig. 5. The metrics used in the evaluation are: 1) the network resources used for protection (protection cost), and 2) the number of congested links. We observe that a reduction of 4% is achieved when using SPNC compared to SP regarding the network resources used for protection in the B1 topology. However, a better performance is achieved with SPNC*, up to 8% compared to SP. Moreover, only 11% of the links were congested when using SPNC and SPNC* compared with NC, while only 23% of the links were congested with SP.

For the NSFNET topology the performance of SPNC* is also greater than SPNC protection. The protection cost when using SPNC* is $138U$ compared with $140U$ and $154U$ when using SPNC and SP respectively. Moreover, it must be noticed that only 1% of links were congested when using SPNC*, compared with 17% using SP and 5% using SPNC.

Finally, for the TID topology SPNC* achieves a reduction of 12% regarding protection cost ($231U$) compared to shared-path protection ($264U$), while SPNC achieves a reduction of 2% ($259U$).

In addition to the evaluation results obtained in Fig. 4 and Fig. 5, table I is summarizes the percentage of protection costs over the total network resources available for each network topology evaluated. We can see that the proposed protection strategy, SPNC*, shows a more efficient utilization of the available network resources.

Based on the evaluation results obtained in this study we can conclude that a considerable reduction of the protection cost can be achieved when multiple coding with a SP strategy is employed, compared to either SP protection or SPNC protection. Moreover, the number of congested links due to deploying protection can also be significantly reduced when multiple coding is used in some network scenarios.

V. Conclusions.

This paper compares protection costs obtained when employing three protection strategies, shared-path protection (SP), network coding with shared-path protection (SPNC), and multiple coding with shared-path protection (SPNC*). We conclude that the use of multiple coding can improve the reduction of the protection cost compared with SPNC and SP, and decrease the number of congested links in some network scenarios. Possible future work includes the evaluation of network coding in multi-layer networks, such as IP over WDM networks, considering the coordination of protection actions between network layers. As another future work we plan to extend the presented comparison model in order to contemplate other cost metrics such as consolidated capital expenditure (CAPEX) and operational expenditure (OPEX).

References

[1] A. Haider and R. Harris. Recovery techniques in next generation networks. *Communications Surveys Tutorials, IEEE*, 9(3):2 –17, quarter 2007.

[2] A.A. Kadhim, T.A. Sarab, and H. Al-Raweshidy. Improving Throughput Using Simple Network Coding. In *Developments in E-systems Engineering (DeSE), 2011*, pages 454–459, 2011.

[3] A. Agarwal and M. Charikar. On the advantage of network coding for improving network throughput. In *Information Theory Workshop, 2004. IEEE*, pages 247–249, 2004.

[4] R.C. Menendez and J.W. Gannet. Efficient, Fault-Tolerant All-Optical Multicast Networks via Network Coding. In *Optical Fiber communication/National Fiber Optic Engineers Conference, 2008. OFC/NFOEC 2008. Conference on*, pages 1 –3, feb. 2008.

[5] Ahmed E. Kamal. 1 + N network protection for mesh networks: network coding-based protection using p-cycles. *IEEE/ACM Trans. Netw.*, 18(1):67–80, February 2010.

[6] M. Belzner, H. Haunstein, and A.J. van Wijngaarden. On the Performance of Network Coding with Protection Cycles. In *Communications (ICC), 2011 IEEE International Conference on*, pages 1 –6, june 2011.

[7] A.E. Kamal, A. Ramamoorthy, Long Long, and Shizheng Li. Overlay Protection Against Link Failures Using Network Coding. *Networking, IEEE/ACM Transactions on*, 19(4):1071 –1084, aug. 2011.

[8] I.B. Barla, F. Rambach, D.A. Schupke, and M. Thakur. Network Coding for Protection against Multiple Link Failures in Multi-Domain Networks. In *Communications (ICC), 2010 IEEE International Conference on*, pages 1 –6, may 2010.

[9] A.H.A. Muktadir, A.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*, pages 1 –5, march 2012.

[10] H. Overby, G. Biczok, P. Babarczi, and J. Tapolcai. In *Communications (ICC), 2012 IEEE International Conference on*, pages 3067–3072.

[11] Jae Hun Kim, Young Min Jhon, Young Tae Byun, Seok Lee, Deok Ha Woo, and Sun Ho Kim. All-optical XOR gate using semiconductor optical amplifiers without additional input beam. *Photonics Technology Letters, IEEE*, 14(10):1436 –1438, oct. 2002.

[12] "Python web page", http://www.python.org/.

[13] http://networkx.github.io/.