Design of VNF-Mapping with Node Protection in WDM Metro Networks

Lidia Ruiz(✉), Ramón J. Durán, Ignacio de Miguel,
Noemí Merayo, Juan Carlos Aguado, Patricia Fernández,
Rubén M. Lorenzo, and Evaristo J. Abril

Optical Communications Group, Universidad de Valladolid, Paseo de Belén, 15,
47011 Valladolid, Spain
lruiper@ribera.tel.uva.es, rduran@tel.uva.es

Abstract. Network Function Virtualization (NFV) is considered to be one of the enabling technologies for 5G. NFV poses several challenges, like deciding the virtual network function (VNF) placement and chaining, and adding backup resources to guarantee the survivability of service chains. In this paper, we propose a genetic algorithm that jointly solves the VNF-placement, chaining and virtual topology design problem in WDM metro ring network, with the additional capacity of providing node protection. The simulation results show how important is to solve all of these subproblems jointly, as well as the benefits of using shared VNF and network resources between backup instances in order to reduce both the service blocking ratio and the number of active CPUs.

Keywords: NFV · Resilience · VNF-Provisioning · VNF-Chaining · Virtual topology design · VNF-Protection

1 Introduction

The advent of 5G promises to increase the bandwidth to support the ever-increasing number of connected devices, and to drastically reduce latency, among other advantages. That evolution is the key factor for the development of machine-to-machine services like IoT, industry 4.0, e-healthcare services or connected vehicles. Nevertheless, 5G poses great challenges to network operators, who must face deep architectural changes in their networks. This architectural transformation, however, can be addressed thanks to the appearance of new architectural paradigms and technologies like Network Function Virtualization (NFV), Software Defined Networking (SDN) and Multi-access Edge Computing (MEC).

NFV is an architectural paradigm that deploys network functions such as firewalls or packet inspectors as virtual appliances, called Virtual Network Functions (VNF), in Commercial-Off-The-Shelf (COTS) servers, instead of using traditional proprietary hardware. This technology can increase network flexibility, reduce capital and operational expenditures, and decrease the time required for the instantiation of new services, since operators can easily deploy new network functions without the need of installing new equipment.

Q. Li et al. (Eds.): BROADNETS 2019, LNICST 303, pp. 285–298, 2019.
https://doi.org/10.1007/978-3-030-36442-7_19

Although COTS are commonly hosted at datacenters, they can also be located at the nodes of the network or even at the edge nodes, closer to the end-user, thanks to the MEC paradigm [1]. This technology provides cloud computing capabilities to edge nodes by adding IT resources to them. Therefore, it is able to bring data processing closer to the end-user, hence reducing latency [2], one of the key performance indicators of 5G.

When network functions are deployed as software using NFV, operators must solve the VNF-Placement problem, i.e., they must decide the number of instances of each VNF to run on each COTS (located in both datacenters and MEC) according to an estimation of the required services. Then, for each service request, the traffic must traverse a sequence of VNFs in a fixed order. This concatenated set of VNFs is referred to as Service Chain (SC), and operators must decide which of the instances should be employed to set up the chain (known as the VNF-chaining problem), according to the SC requirements, VNF availability and also to the available network resources. The combination of both VNF placement and chaining problems are usually known as service mapping.

In [3], we proposed a genetic algorithm for effective service mapping with virtual topology design (GASM-VTD). That algorithm solves the VNF-placement problem in WDM ring 5G-access network topologies and, after allocating the VNFs to hosting MEC nodes of the network, it also solves the virtual topology design, i.e., it decides which lightpaths must be established between MEC/datacenter nodes, the routing and wavelength assignment problem (RWA) for each lightpath and performs traffic grooming over the lightpaths to support the establishment of the SCs required by the service requests. The simulation results presented in that paper show that thanks to the use of GASM-VTD, the service blocking ratio (i.e., the probability that a service cannot be established due to the lack of resources) can be reduced while optimizing the number of active CPU cores and, therefore, the energy consumption in COTS.

However, the VNF placement and chaining problems also present extra challenges in terms of survivability against failures, and GASM-VTD does not take that problem into account. In a distributed scenario, e.g., one with datacenters and MEC resources, the failure of one node will cause the failure of multiples SCs and the overlying services [4, 5]. Moreover, if that problem is not solved properly, the failure can spread across the network. This challenge can be addressed by instantiating (but not using) backup VNFs when solving both the VNF placement and the chaining problems for each SC, using both primary and backup VNFs in case of the failure of any network node. The reason behind instantiating instead of simply reserving is avoiding the set-up time of backup VNFs in case of failure.

In this paper, we focus on the survivability problem, extending the work proposed in [3] to solve the service mapping problem including resilience against simple node failure, and therefore, protecting the SCs. For that aim, we explore two kinds of protection schemes: dedicated, in which each backup VNF protects only one primary VNF or shared, in which a backup VNF can protect multiple primary VNFs without causing any collision problem (i.e., when a backup VNF must deal with more traffic than its capacity) in case of failure. To avoid that collision problem in single-node protection scenario, a backup VNF cannot protect two or more primary VNFs hosted at the same MEC node. Furthermore, the proposed algorithm also solves the virtual topology design problem, including the virtual links required to build the backup SCs also considering dedicated and shared protection schemes for the use of these backup VNFs. In many previous studies the protection of VNFs does not take into account the network connecting the nodes. However, in this study, we present the results of a simulation study comparing different types of protection schemes and showing the importance of considering the network when solving the survivable VNF placement and chaining problems.

2 Related Work

Resilience in NFV placement and chaining have raised great interest in the scientific community. Hmaity et al. [6] propose three SC end-to-end protection schemes: the first one provisions a backup SC ensuring that both the physical links and hosting nodes are completely disjoint from those of the primary SC; the second only provides link protection to the primary SC; and in the third one backup nodes are disjoint, but the virtual links can share the same physical path than the primary ones. Ye et al. [7] propose a heuristic for SC mapping but not for solving the virtual topology design of the optical network. In that paper, the authors further enhance their method with a second step to provide either dedicated or shared end-to-end protection. In contrast to the previous works, which consider end-to-end protection, Beck et al. [8] propose a heuristic method for online SC provisioning which is enhanced with individual link/node protection. However, in that work, they do not consider the configuration (planning) of the network, i.e., the virtual topology design of the WDM network in case of using that technology. Casazza et al. [9] solve the reliable VNF-placement problem in geo-distributed datacentres with the objective of maximizing the VNF availability but they do not consider the chaining problem. Tomassilli et al. [10] focus only on network resilience (not VNF protection) and propose two optimization models to provide dedicated and shared protection against single-link failure. Similarly, Gao et al. [11] propose an ILP formulation and a heuristic to determine a multipath transmission scheme as a way to protect essential traffic between the VNFs hosted in data centres and connected through an elastic optical network. However, they concentrate on the SC problem but do not solve the VNF placement problem and do not implement VNF protection. Finally, Qing et al. [12] propose a method to identify the VNF hosting nodes to be protected in a network to ensure that, in case of failure, the number of surviving SCs is superior to a given threshold but they do not take into account the network design.

In contrast to previous studies, we address the VNF mapping problem with node protection in a WDM metro network equipped with MEC resources solving: (i) the VNF-placement, (ii) the VNF-chaining, (iii) the virtual topology design problems and (iv) determining the set of backup resources (VNFs and links) to protect the system against a node failure.

There are two ways of protecting a SC:

- **End-to-end SC protection**: in case of a node failure, the full SC is replaced by a complete backup SC [6, 7].

- **Individual node protection:** in case of node failure, only the affected VNFs are preplaced by its backup VNFs and the not-affected VNFs still continue being part of the SC [8, 9].

In this paper, we use the second approach, as it allows a reduction of the number of resources required (mainly when shared protection techniques are applied). In the following section we formally describe the problem statement.

3 Problem Statement

We assume 5G nodes connected between them and to a Central Office via a WDM ring network, as shown in Fig. 1. These nodes are MEC-enabled and host COTS to instantiate VNFs (besides offering other services). In that scenario, the algorithm must solve the VNF-placement and chaining problems for both primary and backup SCs, and design the virtual topology to be established in the WDM network.

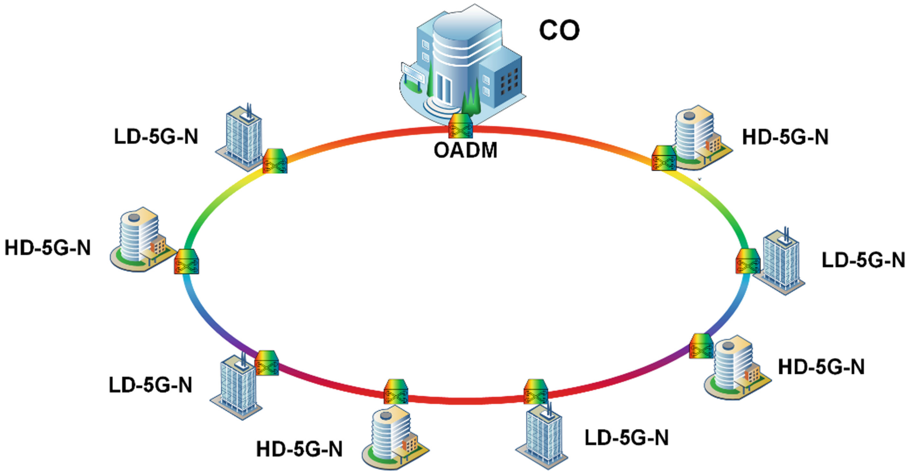

Fig. 1. WDM metro ring network.

In order to provide VNF protection against a node failure, a backup VNF must be assigned for each primary VNF. The backup VNF must be instantiated in a different node than the primary one. The corresponding virtual links to establish the alternative SCs must be also reserved. When a node fails, all the SCs using VNFs from that node must start using the backup VNFs. The SCs will continue using those not-affected VNFs. Suitable backup virtual links must also be used. Figure 2 shows an example of the protection-enabled SC problem for a service with three VNFs. For example, if node A fails, the SC will use backup VNF_1 and the rest of primary VNFs of the SC. If node B fails, the SC will start with primary VNF_1 and will continue with backup VNF_2 (node A) and backup VNF_3 (node D) and primary VNF_4 (node C). Finally, if node C fails, the SC will use primary VNF_{1-3} and backup VNF_4 (node D).

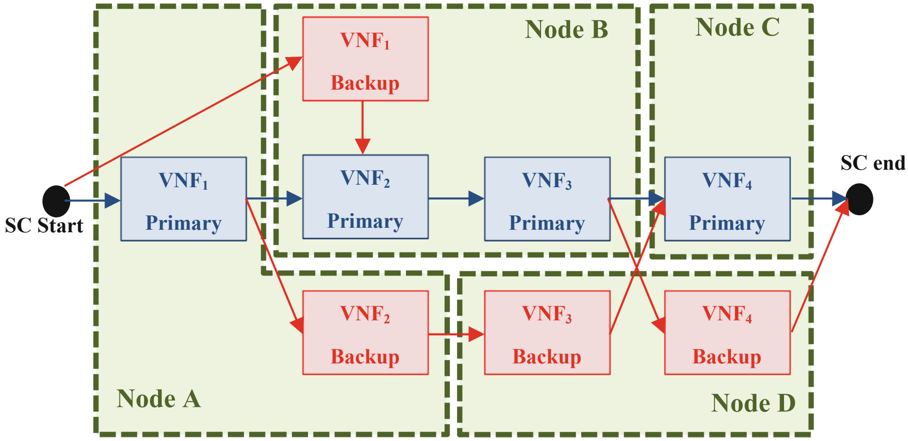

Fig. 2. Network resource allocation between primary and backup VNF hosting nodes.

Like in other problems related to survivability, there are two ways of delivering protection: using dedicated resources or sharing resources between those SCs that are not affected by the same node failure. Therefore, we have the following schemes regarding VNF protection:

- **Dedicated VNF Protection**: A backup VNF instance can protect only one primary VNF instance.
- **Shared VNF Protection**: A backup VNF instance can protect multiple primary VNF instances, provided the primary instances are not located in the same node.

Moreover, the network resources assigned for backup connections can be also assigned in dedicated or shared protection schemes:

- **Dedicated network resources**: connections between primary to backup resources (red arrows in Fig. 2) are dedicated for a SC.
- **Shared network resources**: different SCs can share the same network resources (wavelengths, transceivers) between primary to backup resources provided that they do not have to make use of the same backup resources at the same time in case of an individual node failure.

4 A Genetic Algorithm to Provide VNF Protection Against VNF/Node Failure

In this paper, we propose a new VNF-Protected Genetic Algorithm for Service Mapping and Virtual Topology Design (VNF-P-GASM-VTD) that enhances our previous proposal, GASM-VTD [3]. In contrast, VNF-P-GASM-VTD provisions backup resources for VNF protection and solves the VNF-chaining problem including the VNF chaining using backup resources as explained in the previous section.

The genetic algorithm operates with individuals, which are evolved along a number of generations, and which represent potential solutions to the VNF-placement problem. Each individual is encoded by a set of genes (composing a chromosome). Figure 3 shows an example of the chromosome encoding: each gene indicates the number of instances of a particular VNF that the associated node should host.

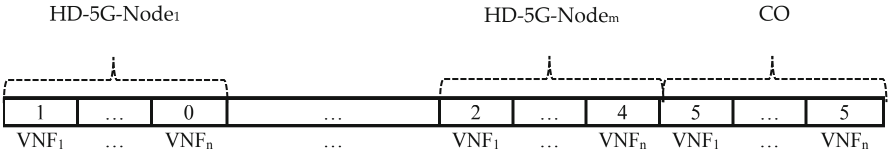

Fig. 3. Example of chromosome.

VNF-P-GASM-VTD follows the classical genetic loop [13]: we create an initial population of individuals which undergo classical genetic operations as crossover and mutation. In crossover, the algorithm randomly chooses two individuals of the population and a crossover point, and the genes of the second part of the chromosome, i.e., from the crossover point to the end of the chromosome, are interchanged to produce two new individuals. The offspring undergoes then a mutation operation, in which the algorithm randomly changes the values of the genes with a user-defined probability. If the algorithm cannot create the number of instances of each VNF at every hosting node as the chromosome of the resulting individual indicates, due to lack of computing resources as CPU cores, hard disk or RAM, then it is discarded and a new one is created. The algorithm repeats this process until completing a user-defined population size.

Valid individuals go then through a translation stage. The algorithm translates each individual, i.e., it creates the instances of the VNFs at the nodes as the chromosome indicates. When all instances are created, the algorithm sorts the incoming service connection requests according to the operator's chosen priority and begins the chaining process. To establish the primary chain of each SC, the algorithm uses the chaining strategy proposed in [3], referred to as GASM-VTD-Collaborative. This strategy starts looking for available VNFs, i.e., VNFs with enough free processing capacity to set up the primary chain at the 5G node to which the user is connected, also known as the local node. If the algorithm cannot find available VNFs at the local node, it looks for available ones at the CO. If it is not possible to chain VNFs hosted at the CO, then the algorithm looks for the VNFs at the other nodes of the network, starting with those of higher allocated IT capacity and then those equipped with less IT resources.

When the primary SC search finishes, the reservation of the backup VNFs starts. The VNFs already in use for any primary SC cannot be selected for backup. Then, the version with dedicated VNF protection can only use the VNFs hosted by a different node from the primary VNF to be protected and which do not protect any other VNF. The shared version can use those VNFs and also those backup VNFs that do not protect a primary VNF hosted in the same node than the primary VNF in evaluation. Like in the primary SC reservation the order of search is: CO and VNFs at the other nodes of the network, starting with those of higher allocated IT capacity and then those equipped with less IT resources. If the algorithm can create the primary SC and reserve backup VNFs, VNF-P-GASM-VTD allocates network resources to the SC.

When two consecutive VNFs of the SC are located at different nodes, then the algorithm must establish a virtual link with enough capacity to connect the nodes and establish the service. Consequently, if a lightpath with enough available bandwidth exists between the nodes, the algorithm will use it to create the virtual link, i.e., traffic grooming is allowed. Otherwise the algorithm will create a new lightpath, if there are enough network resources. Lightpaths are created using the Shortest-Path and First-Fit methods [14]. That mechanism is also used to establish the connections required by the backup SC (red arrows in Fig. 2), together with dedicated or shared protection schemes, and also employing traffic grooming. It is important to note that the lightpaths used for primary and backup SC are completely independent. When resources (VNF and network) are found for both primary and backup SC, the resources (primary and backup) are reserved and the connection is established. Otherwise, the connection is blocked.

The algorithm determines the fitness of the solution through three parameters: the service blocking ratio, the percentage of active CPU cores and the number of employed wavelengths. Then, the best individuals are selected to repeat the genetic loop, and this procedure is repeated for a number of times, or generations, defined by the user. If there are ties between two individuals in terms of service blocking ratio, the algorithm chooses the individual with less active CPU cores (and therefore, with lower energy consumption). If the individuals are also tied in this parameter, then it selects the solution which uses less wavelengths. At the end of the process, the algorithm provides the best solution, composed by the VNF-Placement, the SCs for each connection request and its corresponding backup VNF resources, and the virtual topology with primary and backup connections.

5 Simulation Set up and Results

In order to compare the different protection alternatives, a simulation study has been conducted using the OMNeT++ simulator. The simulation scenario has been a WDM-ring topology network (like the one of Fig. 1) with a Central Office (CO) and ten 5G nodes equipped with MEC resources with two different levels of equipment and demands: five High Demand (HD) 5G nodes and five Low Demand (LD) 5G nodes. Table 1 shows the computational resources allocated in each one of those nodes [3, 15, 16]. All the nodes have 10 Gbps optical transceivers and a ROADM, and support the switching of different number of wavelengths.

Table 1. IT resources for CO and XD-5G-Nodes

Location	Computational resources
CO	100 CPU cores, 480 GB RAM and 27 TB HDD
HD-5G-Ns	16 CPU cores, 64 GB RAM and 10 TB HDD
LD-5G-Ns	8 CPU cores, 32 GB RAM and 7 TB HDD

Regarding traffic, we assume an operator that offers three kind of services, VoIP, Video and Web services, and users may request them with a probability of 30%, 20% and 50% respectively [3]. Each service has an associated SC and bandwidth requirements, which are shown in Table 2 [3, 15–19].

Table 2. Service Chain requirements.

Service	Chained VNFs*	Bandwidth
VoIP	NAT-FW-TM-FW-NAT	64 kbps
Video	NAT-FW-TM-VOC-IDPS	4 Mbps
Web Services	NAT-FW-TM-WOC-IDPS	100 kbps

** NAT:Network Address Translator, FW: Firewall, TM: Traffic Monitor, WOC: WAN Optimization Controller, VOC: Video Optimization Controller, IDPS: Intrusion Detection Prevention System.*

Furthermore, each VNF has associated hardware requirements and processing capacity, which are shown in Table 3.

Table 3. VNF HW requirements and processing capacity.

Service	HW requirements	Throughput
NAT	CPU: 2 cores, RAM: 4 GB, HDD: 16 GB	2 Gbps [20]
FW	CPU: 2 cores, RAM: 4 GB, HDD: 16 GB	2 Gbps [20]
TM	CPU: 1 core, RAM: 2 GB, HDD: 16 GB	1 Gbps [21]
VOC	CPU: 2 cores, RAM: 4 GB, HDD: 2 GB	2 Gbps*
WOC	CPU: 1 core, RAM: 2 GB, HDD: 40 GB	0.5 Gbps [22]
IDPS	CPU: 2 cores, RAM: 4 GB, HDD: 8 GB	1 Gbps [23]

* Values shown in table are derived from the figures of the other VNFs.

We defined the parameter $\bar{u}$ as the number of average users per HD-5G-node. The connected users to each HD-5G node is randomly generated in each simulation using a uniform distribution between $[0, 2\bar{u}]$. The connected users to LD-5G-nodes are also randomly generated using a uniform distribution between $[0, 2\bar{u}/10]$. For each number of $\bar{u}$, we repeated the simulation 500 times and all the graphs are shown with 95% confidence intervals.

VNF-P-GASM-VTD has been configured to create 10 individuals per generation and the finish criterion was set to the evolution during 50 generations. Different versions of the algorithm have been compared to analyze the influence of selecting the different types of protections:

- **No protection**: no backup resources are applied. This algorithms is GASM-VTD [3].
- **Dedicated-VNF protection with no network restrictions** (**Ideal D-VNF** in figures): ideal case where the VNF-P-GASM-VTD is designed to provide

node-protection but without imposing any kind of restriction to the WDM network, i.e., considering unlimited number of optical transceivers and wavelength channels.

- **Shared-VNF protection with no network restrictions** (**Ideal S-VNF** in figures) similar as the previous one (no network restrictions) but using shared-VNF protection.
- VNF-P-GASM-VTD implementing **Dedicated-VNF protection with Dedicated network resources** for the backup (**D-VNF & D-Net** in figures).
- VNF-P-GASM-VTD implementing **Dedicated-VNF protection with Shared network resources** for the backup (**D-VNF & S-Net** in figures).
- VNF-P-GASM-VTD implementing **Shared-VNF protection with Dedicated network resources** for the backup (**S-VNF & D-Net** in figures).
- VNF-P-GASM-VTD implementing **Shared-VNF protection with Shared network resources** for the backup (**S-VNF & S-Net** in figures).

Initially, we have assumed that the network is equipped with optical equipment that allows the use of 10 wavelengths. Figure 4 shows the Service Blocking Ratio (SBR) as a function of the number of users and with the different protection schemes. The corresponding values of the percentage of actives CPU cores are shown in Fig. 5. In that figure it is shown the total number of CPUs in use considering both the ones dedicated for primary VNFs and the ones reserved for backup.

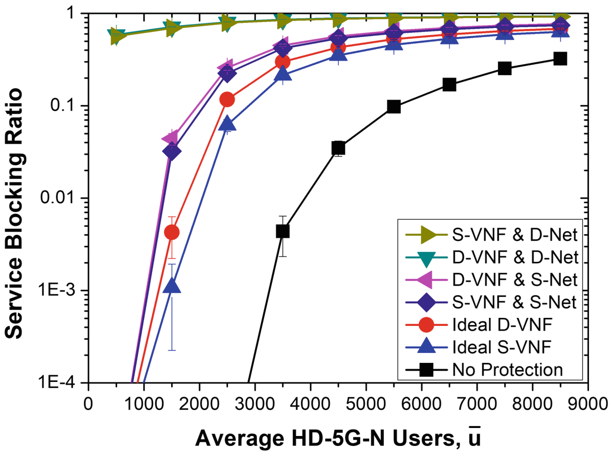

Fig. 4. Service Blocking Ratio for the different protection schemes when the WDM network can use 10 wavelengths.

Figure 4 shows that implementing protection leads to an increment in the service blocking ratio even in the case of not considering network restrictions (like other studies do). This is due to the fact that the computing resources in nodes (CO and MEC) are limited. Comparing the versions with protection and without considering network restrictions (ideal) with the ones that consider those restrictions, it is possible to see the huge difference in performance. Therefore, when implementing protection (even when only nodes or VNFs are protected) is essential to take into account the network connecting the nodes as it will be a very restricting factor. It should be noticed that, in the case of using end-to-end protection, the results are even worse as more resources have to be employed for establishing the backup SC.

Then, comparing the different versions of the algorithm with protection, it can be seen that those versions using dedicated network resources for protection are the ones that show a higher SBR. In fact, the values obtained make unfeasible to use these options in a real network. Again, the impact of network communication resources is evident. Finally, the use of shared VNF protection instead of dedicated protection allows a reduction in the SBR for both ideal and the version using shared network resources.

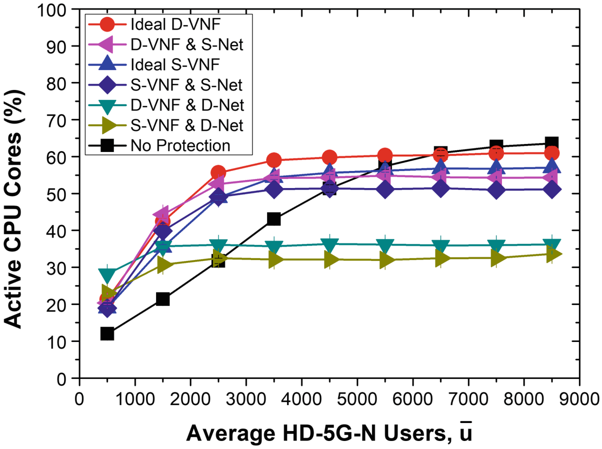

Fig. 5. Percentage of total active CPU cores for the different protection schemes when the WDM network can use 10 wavelengths.

Regarding Fig. 5, the scheme without protection is the one that uses the smallest number of CPU cores as it does not reserve backup VNFs. Then, shared VNF policies make a better use of the CPU cores than their dedicated counterparts. Therefore, the use of shared VNF schemes is not only better than using dedicated ones only in terms of resources in use (what is obvious due to the fact of sharing) but also in terms of SBR. Finally, the versions that use dedicated network resources for backup network require less CPU cores than the other alternatives when the number of users grows. This happens because, network resources become the limiting factor before the computing resources, so that there are still CPU resources available to instantiate more VNFs, but there is not enough network capacity to support communication between VNFs.

Figure 6 shows a comparison of the percentage of active CPU cores (out of the total number of CPU cores) allocated for primary and backup VNFs with the different protection schemes with three number of users: $\bar{u} = 500$, $\bar{u} = 2{,}500$ and $\bar{u} = 4{,}500$.

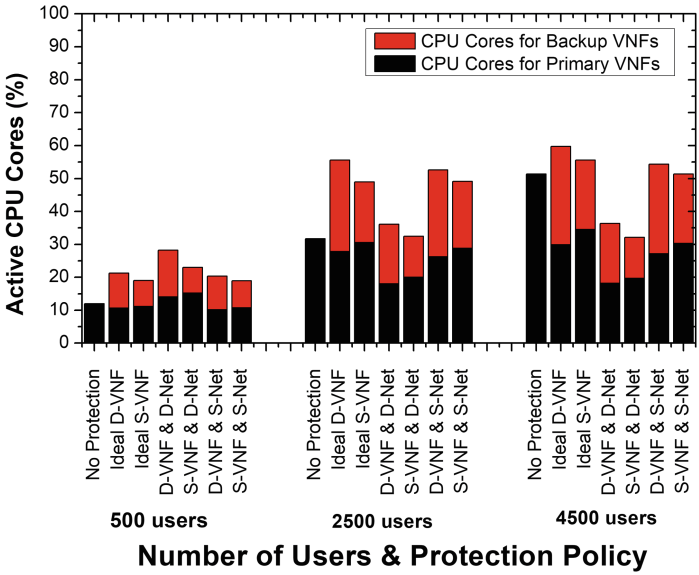

Fig. 6. Percentage active CPU cores (out of the total CPU cores of the network) for the different protection schemes when the WDM network can use 10 wavelengths distinguishing the ones used for primary and backup.

Figure 6 shows that, as the number of users increases, higher is the number of active CPUs. However, the difference between the $\bar{u} = 500$ case and the $\bar{u} = 2{,}500$ case is higher than the difference between $\bar{u} = 2{,}500$ case and the $\bar{u} = 4{,}500$ (except for the case of no protection) because in the second case the unavailability of network resources is the limiting factor when establishing new SCs. When no protection is used, the number of used resources (CPUs and wavelengths/transceivers) is lower as none of them has to be used for backup. When comparing CPU utilization for the policies with dedicated network resources (D-Net policies), it is lower than the CPU utilization for shared-network (S-Net) policies. This behavior is again due to the fact that network resources become the limiting factor before the computing resources (there are still CPU resources available to instantiate more VNFs, but there is not enough network capacity to support communication between VNFs). Comparing the percentage of CPUs for primary and backup VNFs, the percentages of CPUs for backup with shared-VNF policies is lower than those of the dedicated-VNF policies (which, obviously, use the same number of active CPUs for backup and primary VNFs, since there is a one-to-one relationship). Finally, shared-VNF policies use a lower number of active CPUs than the dedicated versions (D-VNF) since the formers aim at reutilizing backup resources among different primary VNFs hosted at different nodes.

The corresponding values of SBR and percentage of CPUs in use when the number of network resources increases (the number of wavelength grows up to 20) are shown in Fig. 7 and Fig. 8 respectively.

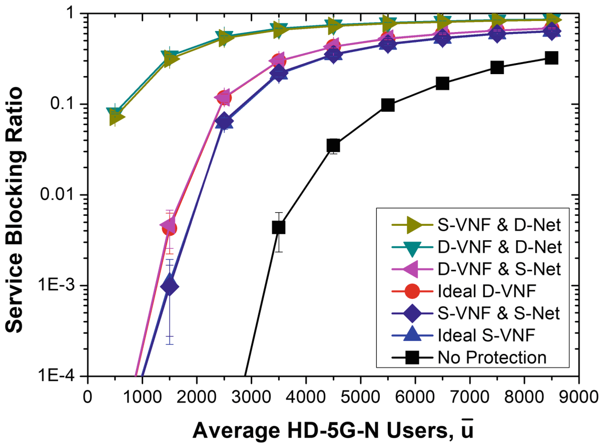

Fig. 7. Service Blocking Ratio for the different protection schemes when the WDM network can use 20 wavelengths.

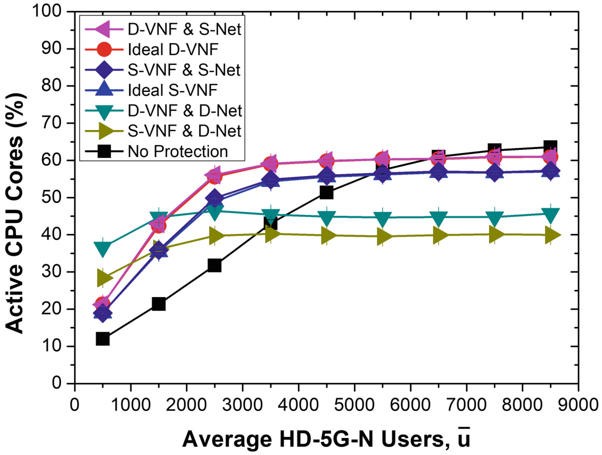

Fig. 8. Percentage of total active CPU cores for the different protection schemes when the WDM network can use 20 wavelengths.

When the number of network resources increases (Figs. 7 and 8), the results in terms of both SBR and active CPU cores improve and the versions that implement the protections using shared network resources for the backup get the same performance of the ideal ones (when no network restrictions is taking into account). However, this is done at the expense of increasing the CAPEX (note that 20 wavelengths are required for a metro network with only 10 nodes). The results of the versions using dedicated network resources for backup also improves its results, although high SBR (>10^{-1}) are still obtained.

In conclusion, the results show that when solving the VNF placement and chaining problems with node protection is essential to take into account the network topology and design it at the same time when solving the problem. Moreover, for an efficient use of resources, the reutilization of network resources for backup connections is almost mandatory and sharing backup VNFs can also reduce both the service blocking ratio and the number of active CPUs (and, therefore, the energy consumption).

6 Conclusions

In this paper, we have addressed the VNF-provisioning and chaining problems including node protection in a WDM metro network. The method also solves the virtual network design of the WDM network. Different methods for protection have been implemented and compared using shared or dedicated resources for the backup in both the VNF and network levels.

The results of a simulation study show that, in contrast with other proposal, it is essential to solve all those problems (including node protection) taking into consideration the network restrictions and its design. Among the different schemes of protection, the one that shares backup resources at both NFV and network levels is the one that achieves the best results in terms of both service blocking ratio and number of active resources (and therefore, in energy consumption).

Acknowledgements. This work has been supported by Spanish Ministry of Economy and Competitiveness (TEC2017-84423-C3-1-P), the fellowship program of the Spanish Ministry of Industry, Trade and Tourism (BES 2015-074514) and the INTERREG V-A España-Portugal (POCTEP) program (0677_DISRUPTIVE_2_E).

References

1. Savi, M., Tornatore, M., Verticale, G.: Impact of processing costs on service chain placement in network functions virtualization. In: Proceedings of the 2015 IEEE Conference on Network Function Virtualization and Software Defined Network (NFV-SDN), pp. 191–197. IEEE, San Francisco (2015)
2. Patel, M., Naughton, B., Chan, C., Sprecher, N., Abeta, S., Neal, A.: Mobile-edge computing introductory technical white paper. Mob.-Edge Comput. (MEC) Ind. Initiative (2014)
3. Ruiz, L., et al.: Joint VNF-provisioning and virtual topology design in 5G optical metro networks. In: Proceedings of the 2019 21st International Conference of Transparent Optical Networks (ICTON), pp. 1–4. IEEE, Angers (2019)
4. ETSI: GS NFV-REL 003 V1.1.1 Network Functions Virtualisation (NFV); Reliability; Report on Models and Features for End-to-End Reliability
5. Casazza, M., Bouet, M., Secci, S.: Availability-driven NFV orchestration. Comput. Netw. **155**, 47–61 (2019). https://doi.org/10.1016/j.comnet.2019.02.017
6. Hmaity, A., Savi, M., Musumeci, F., Tornatore, M., Pattavina, A.: Virtual network function placement for resilient service chain provisioning. In: 2016 8th International Workshop on Resilient Networks Design and Modeling (RNDM), pp. 245–252. IEEE, Halmstad (2016). https://doi.org/10.1109/RNDM.2016.7608294

7. Ye, Z., Cao, X., Wang, J., Yu, H., Qiao, C.: Joint topology design and mapping of service function chains for efficient, scalable, and reliable network functions virtualization. IEEE Netw. **30**, 81–87 (2016). https://doi.org/10.1109/MNET.2016.7474348
8. Beck, M.T., Botero, J.F., Samelin, K.: Resilient allocation of service Function chains. In: 2016 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), pp. 128–133 (2016). https://doi.org/10.1109/NFV-SDN.2016.7919487
9. Casazza, M., Fouilhoux, P., Bouet, M., Secci, S.: Securing virtual network function placement with high availability guarantees. In: 2017 IFIP Networking Conference (IFIP Networking) and Workshops, pp. 1–9 (2017). https://doi.org/10.23919/IFIPNetworking.2017.8264850
10. Tomassilli, A., Huin, N., Giroire, F., Jaumard, B.: Resource requirements for reliable service function chaining. In: 2018 IEEE International Conference on Communications (ICC), pp. 1–7 (2018). https://doi.org/10.1109/ICC.2018.8422774
11. Gao, T., Li, X., Zou, W., Huang, S.: Survivable VNF placement and scheduling with multipath protection in elastic optical datacenter networks. In: 2019 Optical Fiber Communications Conference and Exhibition (OFC), pp. 1–3 (2019)
12. Qing, H., Weifei, Z., Julong, L.: Virtual network protection strategy to ensure the reliability of SFC in NFV. In: Proceedings of the 6th International Conference on Information Engineering - ICIE 2017, pp. 1–5. ACM Press, Dalian Liaoning (2017). https://doi.org/10.1145/3078564.3078583
13. Goldberg, D.: Genetic Algorithms in Optimization Search and Machine Learning. Addison-Wesley, Reading (1989)
14. Zang, H., Jue, J.P., Mukherjee, B., et al.: A review of routing and wavelength assignment approaches for wavelength-routed optical WDM networks. Opt. Netw. Mag. **1**, 47–60 (2000)
15. Pedreno-Manresa, J.-J., Khodashenas, P.S., Siddiqui, M.S., Pavon-Marino, P.: Dynamic QoS/QoE assurance in realistic NFV-enabled 5G access networks. In: 2017 19th International Conference on Transparent Optical Networks (ICTON), pp. 1–4. IEEE, Girona (2017). https://doi.org/10.1109/ICTON.2017.8025149
16. Pedreno-Manresa, J.-J., Khodashenas, P.S., Siddiqui, M.S., Pavon-Marino, P.: On the need of joint bandwidth and NFV resource orchestration: a realistic 5G access network use case. IEEE Commun. Lett. **22**, 145–148 (2018). https://doi.org/10.1109/LCOMM.2017.2760826
17. Savi, M., Tornatore, M., Verticale, G.: Impact of processing costs on service chain placement in network functions virtualization. In: Proceedings of the 2015 IEEE Conference on Network Function Virtualization and Software Defined Network (NFV-SDN), pp. 191–197. IEEE, San Francisco (2015). https://doi.org/10.1109/NFV-SDN.2015.7387426
18. Savi, M., Hmaity, A., Verticale, G., Höst, S., Tornatore, M.: To distribute or not to distribute? Impact of latency on Virtual Network Function distribution at the edge of FMC networks. In: 2016 18th International Conference on Transparent Optical Networks (ICTON), pp. 1–4. IEEE (2016)
19. Ruiz, L., et al.: A genetic algorithm for VNF provisioning in NFV-Enabled Cloud/MEC RAN architectures. Appl. Sci. **8**, 2614 (2018). https://doi.org/10.3390/app8122614
20. Juniper Networks: vSRX Virtual Firewall (2018)
21. Brocade Communications System: Virtual Traffic Manager (2015). https://www.accyotta.com/assets/uploads/docs/Brocade_-_Virtual_Traffic_Manager.pdf
22. Talari Networks: Talari SD-WAN Solutions (2018)
23. Cisco: Cisco Adaptive Security Virtual Appliance (ASAv) (2018)