This is a postprint version of the following published document: Ruiz Pérez, Lidia; Durán Barroso, Ramón José; Miguel Jiménez, Ignacio de; Merayo Álvarez, Noemí; Aguado Manzano, Juan Carlos; Lorenzo Toledo, Rubén Mateo; Abril Domingo, Evaristo José. Comparison of different protection schemes in the design of VNF-mapping with VNF resiliency. In: 2020 22nd International Conference on Transparent Optical Networks (ICTON). Bari, Italia: IEE Xplore, 2020, 4 p.

Comparison of Different Protection Schemes in the Design of VNF-Mapping with VNF Resiliency

L. Ruiz, R.J. Durán, I. de Miguel, N. Merayo, J.C. Aguado, P. Fernández, R.M. Lorenzo and E.J. Abril
Optical Communications Group. Universidad de Valladolid. Paseo de Belén, 15, 47011, Valladolid, Spain
e-mail: lruiper@ribera.tel.uva.es, rduran@tel.uva.es

ABSTRACT
Network Function Virtualization (NFV) is a promising networking paradigm that will ease the network manageability and increase its flexibility, while reducing costs. In this paradigm, operators must solve the Virtual Network Function (VNF) placement and chaining problems. It is also important to provide backup resources to ensure the survivability of the offered services when a node failure happens. In this paper, we compare two different protection approaches to ensure the service resilience: individual VNF protection and end-to-end protection. Results show the benefits in terms of use of computing resources and energy consumption of protecting each VNF individually, compared to the end-to-end protection approach.

Keywords: VNF-Placement, VNF-Chaining, VNF-Protection, end-to-end protection, individual VNF protection.

1. INTRODUCTION

Operators are currently adapting their networks to 5G technology. 5G will bring high-capacity, low latency communications and will support a high number of connected devices. [1]. Technologies like Network Function Virtualization (NFV), Software Defined Networking (SDN) and Multi-access Edge Computing (MEC) will contribute to build more flexible, adaptable and manageable networks while reducing capital and operational expenditures. NFV proposes to deploy network functions as virtual appliances called Virtual Network Functions (VNFs), installed in servers that can be located at data centers (DCs), the central office (CO) or at the nodes of the network thanks to the MEC technology, which provides the edge nodes with computing and storage. Thus, processes are put close to the end-user helping to reduce the latency, one of the most stringent key performance parameters of 5G [2].

In NFV-enabled networks, deploying a service requires the establishment of a Service Chain (SC), composed of VNF instances that must be traversed in a certain order. Therefore, operators must solve the VNF-placement, i.e., the number and location of the VNF instances required to deploy the requested service, and the VNF-chaining, i.e., selecting the instances that will be concatenated, attending to restrictions like the IT capabilities of the hosts and the availability of network resources. We refer to the combination of both as service mapping. Solving these problems poses extra challenges in terms of survivability of SCs against failures. In distributed scenarios with DCs and MEC nodes, the failure of a node causes the disruption of the SCs using the VNFs traversing that node, degrading or totally interrupting the overlying services [3]. This issue can be addressed by providing protection for each VNF by reserving backup resources. The backup resources can be kept idle to reduce the energy consumption and the set-up time in case of a primary VNF failure.

The SC resilience problem can be addressed following different strategies: i) Individual VNF protection, in which a backup VNF is assigned to each primary VNF in the network and, if a VNF fails, the traffic is sent to the corresponding backup VNF, and comes back to the primary SC, as in [4], [5] and [6]. ii) end-to-end SC protection, in which a full backup SC is reserved for each primary SC, as in [7] and [8].

In [9], we proposed a Genetic Algorithm for Service Mapping and Virtual Topology Design (GASM-VTD) for 5G networks with WDM backhaul. In the design of the virtual topology, the algorithm decides which lightpaths should be set up, solves the routing and wavelength assignment problem (RWA) for each lightpath, and performs traffic grooming over the virtual topology to create the required virtual links between the nodes hosting the VNFs that compose the SCs. This work was further extended in [10] by providing resiliency against single node failure, following the individual VNF protection strategy and considering the availability of the required network resources to connect primary and backup VNFs when designing the virtual topology.

In this paper, we present a comparison between the two strategies to provide resilience against node failures, comparing the individual VNF protection method used in [10] with a new version of the method that uses end-to-end protection. For that aim, we implement an end-to-end, node disjoint SC protection scheme based on the proposals in [8]. In this comparison, we evaluate the performance of these two strategies using shared and dedicated backup VNFs and network resources.

2. A GENETIC ALGORITHM TO SOLVE THE SERVICE MAPPING PROBLEM

In this paper, we propose a new version of the Genetic Algorithm for Service Mapping and Virtual Topology Design (GASM-VTD) [9] including end-to-end SC protection using the techniques presented in [8]. Two different versions of GASM-VTD were presented in [9], a collaborative and a no-collaborative one. In this paper, we focus on the collaborative version, as it leads to better results in terms of blocking ratio [9].

GASM-VTD follows the classical genetic loop [11] and uses analogous individuals to those proposed in [10]. Therefore, it creates an initial parent population composed of randomly generated individuals, described by genes that represent the number of instances of a certain VNF that must be created at a given node, either a MEC node or the CO. The individuals undergo crossover and mutation operations. In crossover, the algorithm randomly selects two individuals of the group and a random crossover point and interchanges the genes of the individuals from the crossover point to the end of the chromosome. The offspring goes through the mutation stage, in which the algorithm randomly changes (or mutates) the genes with a user-defined mutation probability. This process is repeated until achieving a user-defined descendant population size. Then, the individuals undergo a translation stage and the fitness evaluation of each solution in terms of service blocking ratio (SBR), number of active CPU cores and number of wavelengths in use. The best individuals among the parent and the descendant population are chosen to be parents of the following generation. The algorithm selects the individuals with best (lowest) SBR and uses the CPU consumption first and the active wavelengths last to solve any ties.

In the translation stage, the algorithm creates the instances of the VNFs according to the information encoded in the chromosome, and then sorts the received service requests according to a certain operator's preference. Next, for each request, the algorithm creates the primary SC necessary to support the service request by applying the chaining technique in [9], looking for available VNFs at the MEC node to which the user is connected, then, if required, at the CO, and finally at the rest of nodes of the network, starting with the ones equipped with more IT resources and finishing with the nodes equipped with less IT resources. When a primary SC is built and the selected VNFs are reserved, the algorithm looks for backup resources.

In this paper, the end-to-end SC protection is selected (the individual VNF protection version can be found in [10]). Therefore, the algorithm looks for a backup SC to protect the primary SC, searching a backup VNF for each primary VNF of the working SC, so that the primary and backup SCs are totally node disjoint. A VNF cannot be chained in two different backup SCs. The protection of an SC can be either shared or dedicated. In shared SC protection, a backup SC can protect multiple primary SCs provided they are all node disjoint. In dedicated protection, a backup SC can only protect one primary SC. If the VNFs of the primary and the backup SC can be reserved, the algorithm assigns network resources, starting with the primary SC and establishing virtual links between two consecutive VNFs only if they are hosted at different nodes. Then, the algorithm creates the backup virtual links between the consecutive backup VNFs that are located at different nodes. Backup virtual links can be shared or dedicated and use independent lightpaths from those used to create primary links. If the algorithm finds network resources to establish the primary SC and the backup SCs, the request is accepted; otherwise, it is blocked. The algorithm repeats this process for all the service requests.

3. SIMULATION STUDY AND RESULTS

A simulation study has been conducted using OMNeT++ [12] to compare the performance of the version without protection (NP) with the different versions with protection using both individual VNF and end-to-end SC protection strategies. The protection methods are shown in Table 1. The "ideal network" versions assume unlimited network resources. We have tested these algorithms in a 5G network with a WDM-ring backhaul, composed of a CO, 5 high demand 5G-nodes (HD-5G-nodes) and 5 low demand 5G-nodes (LD-5G-nodes). Each pair of nodes is connected through a link composed of two unidirectional fibers transporting either 10 or 20 wavelengths at 10 Gb/s each. The 5G-nodes can host VNFs using the IT resources shown in Table 2. We assume that the network is managed by an operator that offers three kinds of services, VoIP, video streaming and web searching, which users request with a probability of 30%, 20% and 50%, respectively. The services have an associated SC and bandwidth resources shown in Table 3. The VNFs have the associated hardware requirements and throughput shown in Table 4.

Table 1. Protection schemes.

Backup resource modality	Protection Scheme	
	Individual VNF	**End-to-end SC**
Dedicated VNF or SC, Ideal Network	(DV, Ideal Network)	(DSC, Ideal Network)
Shared VNF or SC, Ideal Network	(SV, Ideal Network)	(SSC, Ideal Network)
Dedicated VNF or SC, Dedicated Net	(DV, DN)	(DSC, DN)
Dedicated VNF or SC, Shared Net	(DV, SN)	(DSC, SN)
Shared VNF or SC, Dedicated Net	(SV, DN)	(SSC, DN)
Shared VNF or SC, Shared Net	(SV, SN)	(SSC, SN)

Table 2. IT resource distribution in CO and 5G-

Table 3. Requirements of the deployed service chains

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

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*.

Table 4. Hardware requirements associated to the VNFs.

Service	HW requirements.	Throughput
NAT	CPU: 2 cores, RAM: 4 GB, HDD: 16 GB	2 Gbps [13]
FW	CPU: 2 cores, RAM: 4 GB, HDD: 16 GB	2 Gbps [13]
TM	CPU: 1 core, RAM: 2 GB, HDD: 16 GB	1 Gbps [14]
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 [15]
IDPS	CPU: 1 core, RAM: 2 GB, HDD: 8 GB	1 Gbps [16]

**The values are derived from the values of other VNFs*.

At the beginning of each simulation, the average number of users connected to each HD-5G-node and LD-5G-node is randomly generated using the uniform distributions $[0, 2\bar{u}]$ and $U[0, 2\bar{u}/10]$, respectively, where $\bar{u}$ represents the average number of users per HD-5G-node. The parent population size is 5 individuals. The descendant population size is 10 individuals. The stopping criteria of the algorithm is set to 50 generations. We repeat the simulation 900 times with different traffic demands. All figures are plotted with 95% confidence intervals.

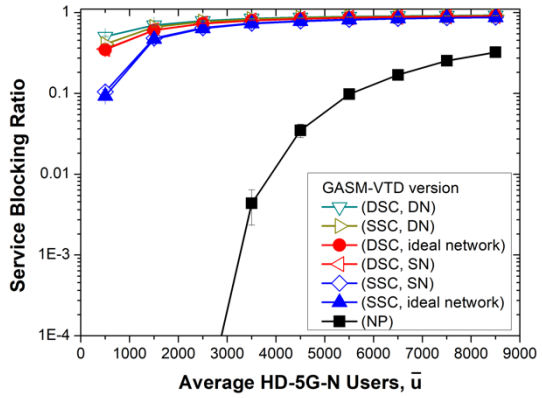

Figure 1. SBR for 10 wavelengths.

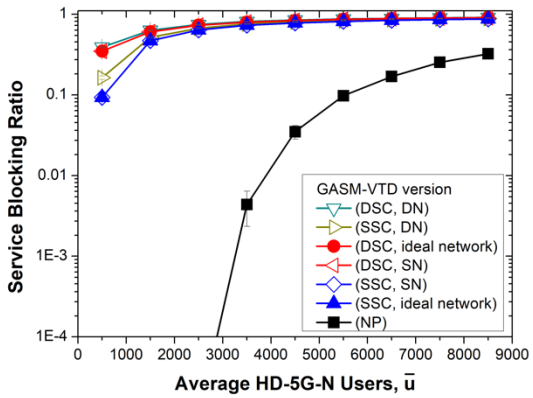

Figure 2. SBR for 20 wavelengths.

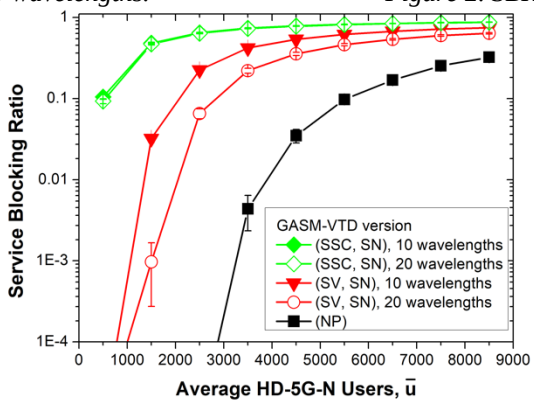

Figure 3. SBR of the best performing configurations of GASM-VTD with protection for 10 and 20 wavelengths.

Figures 1 and 2 show the SBR of GASM-VTD with end-to-end SC protection when the network uses up to 10 and 20 wavelengths, respectively. The SBR obtained by the end-to-end SC protection schemes shown in Figure 1 is too high ($>10^{-1}$) and very close to the SBR obtained in the ideal network scenario, therefore, the end-to-end SC protection requires many computing resources to achieve a reasonable SBR. This conclusion is also supported by Figure 2, in which incrementing the number of wavelengths barely improves the performance of

the end-to-end protection schemes. Comparing the different versions of the algorithms, those using shared SC protection schemes (SSC, SN), (SSC, DN) are the ones that show lower values of SBR (in fact, the same as the one of the same algorithm in ideal networks). Therefore, the number of computing resources is the most limiting factor of end-to-end protection strategies.

Figure 3 shows the comparison of the best performing configurations of GASM-VTD when individual VNF (SV, SN) (as in [10]) and end-to-end SC protection (SSC, SN) are implemented, when the network uses 10 and 20 wavelengths. The individual VNF protection schemes achieve better performance, up to two orders of magnitude for low $\bar{u}$ compared to the end-to-end SC protection schemes. Moreover, in contrast to the end-to-end SC schemes, the performance of individual VNF protection can be improved by allowing the operation of the networks with higher number of wavelengths.

4. CONCLUSIONS

In this paper, two different protection strategies to guarantee resilience in 5G network with WDM backhaul and implementing NFV in MEC nodes have been compared: individual VNF protection and end-to-end SC protection. For that aim, the collaborative version of GASM-VTD, presented in [10], has been modified to include end-to-end SC protection schemes based on the mechanisms proposed in [8]. Results show that the individual VNF protection schemes perform up to two orders of magnitude better than the end-to-end SC approaches, making them the most appropriate protection strategies to be implemented in real networks. Finally, we would like to mention that we have very recently presented an improved version of GASM-VTD, called GASVIT, in [17]. That algorithm employs individual VNF protection to provide resilience, and we opted for implementing that resilience strategy in that algorithm due to the results that are presented in this paper.

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) ,the research network Go2Edge (RED2018-102585-T), and the European Regional Development Fund (ERDF) through the project DISRUPTIVE of the cooperation programme Interreg V-A Spain-Portugal (POCTEP) 2014-2020.

REFERENCES

[1] M. Maternia *et al.*, "5G PPP use cases and performance evaluation models," *5G-PPP, Tech. Rep*, 2016.

[2] M. Patel, B. Naughton, C. Chan, N. Sprecher, S. Abeta, and A. Neal, "Mobile-edge computing introductory technical white paper.," *Mobile-edge Computing (MEC) industry initiative*, 2014.

[3] M. Casazza, M. Bouet, and S. Secci, "Availability-driven NFV orchestration," *Computer Networks*, vol. 155, pp. 47–61, May 2019, doi: 10.1016/j.comnet.2019.02.017.

[4] J. Fan, Z. Ye, C. Guan, X. Gao, K. Ren, and C. Qiao, "GREP: Guaranteeing Reliability with Enhanced Protection in NFV," in *Proceedings of the 2015 ACM SIGCOMM Workshop on Hot Topics in Middleboxes and Network Function Virtualization*, New York, NY, USA, 2015, pp. 13–18, doi: 10.1145/2785989.2786000.

[5] M. T. Beck, J. F. Botero, and K. Samelin, "Resilient allocation of service Function chains," in *2016 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, Nov. 2016, pp. 128–133, doi: 10.1109/NFV-SDN.2016.7919487.

[6] M. Casazza, P. Fouilhoux, M. Bouet, and S. Secci, "Securing virtual network function placement with high availability guarantees," in *2017 IFIP Networking Conference (IFIP Networking) and Workshops*, Jun. 2017, pp. 1–9, doi: 10.23919/IFIPNetworking.2017.8264850.

[7] Z. Ye, X. Cao, J. Wang, H. Yu, and C. Qiao, "Joint topology design and mapping of service function chains for efficient, scalable, and reliable network functions virtualization," *IEEE Network*, vol. 30, no. 3, pp. 81–87, May 2016, doi: 10.1109/MNET.2016.7474348.

[8] A. Hmaity, M. Savi, F. Musumeci, M. Tornatore, and A. Pattavina, "Virtual Network Function placement for resilient Service Chain provisioning," in *2016 8th International Workshop on Resilient Networks Design and Modeling (RNDM)*, Halmstad, Sweden, Sep. 2016, pp. 245–252, doi: 10.1109/RNDM.2016.7608294.

[9] L. Ruiz *et al.*, "Joint VNF-Provisioning and Virtual Topology Design in 5G Optical Metro Networks," in *Proceedings of the 2019 21th International Conference of Transparent Optical Networks (ICTON)*, Angers, France, 2019, pp. 1–4.

[10] L. Ruiz *et al.*, "Design of VNF-Mapping with Node Protection in WDM Metro Networks," presented at the International Conference on Broadband Communications, Networks and Systems, 2019, pp. 285–298.

[11] D. Goldberg, "Genetic algorithms in optimization, search and machine learning," *Reading: Addison-Wesley*, 1989.

[12] *OMNeT++. Discrete Event Simulator.* .

[13] “vSRX Virtual FIrewall,” p. 6.
[14] “Brocade_-_Virtual_Traffic_Manager.pdf.” Accessed: Feb. 22, 2019. [Online]. Available: https://www.accyotta.com/assets/uploads/docs/Brocade_-_Virtual_Traffic_Manager.pdf.
[15] Talari Networks, “Talari SD-WAN Solutions.” 2018.
[16] Cisco, “Cisco Adaptive Security Virtual Appliance (ASAv).” 2018.
[17] L. Ruiz *et al.*, “Genetic Algorithm for Holistic VNF-Mapping and Virtual Topology Design,” *IEEE Access*, vol. 8, pp. 55893–55904, 2020, doi: 10.1109/ACCESS.2020.2982018.