SPECIAL SECTION ON INNOVATION AND APPLICATION OF INTELLIGENT
PROCESSING OF DATA, INFORMATION AND KNOWLEDGE AS RESOURCES IN EDGE COMPUTING

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received February 28, 2020, accepted March 11, 2020, date of publication March 19, 2020, date of current version March 31, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2982018

Genetic Algorithm for Holistic VNF-Mapping and Virtual Topology Design

LIDIA RUIZ, RAMÓN J. DURÁN BARROSO, IGNACIO DE MIGUEL, NOEMÍ MERAYO, JUAN CARLOS AGUADO, RAMÓN DE LA ROSA, PATRICIA FERNÁNDEZ, RUBÉN M. LORENZO, AND EVARISTO J. ABRIL
Optical Communications Group, Universidad de Valladolid, 47002 Valladolid, Spain

Corresponding authors: Lidia Ruiz (lruiper@ribera.tel.uva.es) and Ramón J. Durán Barroso (rduran@tel.uva.es)

This work was supported in part by the Spanish Ministry of Economy and Competitiveness under Grant TEC2017-84423-C3-1-P, in part by the Fellowship Program of the Spanish Ministry of Industry, Trade, and Tourism under Grant BES 2015-074514, in part by the Spanish Thematic Network under Contract RED2018-102585-T, and in part by the INTERREG V-A España–Portugal (POCTEP) Program under Grant 0677_DISRUPTIVE_2_E.

ABSTRACT Next generation of Internet of Things (IoT) services imposes stringent requirements to the future networks that current ones cannot fulfill. 5G is a technology born to give response to those requirements. However, the deployment of 5G is also accompanied by profound architectural changes in the network, including the introduction of technologies like multi-access edge computing (MEC), software defined networking (SDN), and network function virtualization (NFV). In particular, NFV poses diverse challenges like virtual network function (VNF) placement and chaining, also called VNF-mapping. In this paper, we present an algorithm that solves VNF-placement and chaining in a metro WDM optical network equipped with MEC resources. Therefore, it solves the VNF-mapping in conjunction with the virtual topology design of the underlying optical backhaul network. Moreover, a version of the method providing protection against node failures is also presented. A simulation study is presented to show the importance of designing the three problems jointly, in contrast to other proposals of the literature that do not take the design of the underlying network into consideration when solving that problem. Furthermore, this paper also shows the advantages of using collaboration between MEC nodes to solve the VNF-mapping problem and the advantage of using shared protection schemes. The new algorithm outperforms other proposals in terms of both service blocking ratio, and number of active CPUs (thus reducing energy consumption). Finally, the impact of deploying different physical topologies for the optical backhaul network is also presented.

INDEX TERMS NFV, optical networks, MEC, 5G, IoT, protection, resource allocation, survivability.

I. INTRODUCTION

The development of the next generation of Internet of Things (IoT) requires stringent features from networks that current ones cannot offer. 5G is one of the technologies proposed to address those IoT requirements and the specific needs of different vertical industries like the e-health, automotive or energy sectors [1]. 5G will provide massive connectivity, multi-tenancy, ultra-low latency, high-speed and highly reliable communications. Thus, 5G has to incorporate new networking and computation trends like multi-access edge computing (MEC), network function virtualization (NFV), and software defined networking (SDN), while relying on optical technologies to build its backhaul, due to its flexibility and high capacity [2].

The NFV networking paradigm aims at deploying common functions that networks perform, like firewalls or packet inspectors, as virtual appliances hosted at commercial-off-the-shelf (COTS) servers, instead of using traditional, proprietary-based hardware. In that way, NFV increases the network flexibility, improves the network scalability (essential for IoT applications), eases the service deployment cycle since network operators only need to instantiate VNFs instead of purchasing and installing new hardware, and reduces the capital and operational expenses (CAPEX and OPEX) of the network.

Normally, VNFs are located at data centers (DCs) or at the central offices of metro networks (COs) [3]. However,

The associate editor coordinating the review of this manuscript and approving it for publication was Honghao Gao.

with that configuration, data processing might not be close enough to the end-user to guarantee the stringent latency requirements of some IoT applications, in particular, the ones related with tactile internet [4]. On the other hand, MEC technology provides the edge network nodes with computing and storage capabilities, hence enabling these nodes to host VNFs and process tasks from the continuous edge-cloud computing paradigm [5]. In this manner, data processing is pushed close to the end-user, reducing latency [5], the concentration of resources in data centers and, consequently, security and privacy threats [6], [7], as well as helping to meet 5G requirements, essential to fully exploit the potential of next generation IoT applications.

In this kind of environment, deploying new services involves two design steps: VNF-placement and VNF-chaining. In the VNF-placement stage, operators decide the number of instances of the VNFs that must be deployed at each network node equipped with computing and storage capabilities. Then, in the VNF-chaining step, operators create the associated service chain (SC) for the requested service. The SCs are composed of a set of VNFs that must be traversed in a certain order. Therefore, network operators must set up these SCs by selecting the appropriate VNF instances with available capacity to process the requested traffic and allocate network resources to ensure the transport of traffic from one VNF to the following VNF of the SC. That last point is essential, but most of previous works, as will be shown in Section II, do not take into account the underlying backhaul network when solving the VNF-placement and chaining problems. Considering that most of backhaul networks will be based on optical technologies, generally using wavelength division multiplexing (WDM), the design of the virtual topology of those networks is also essential. The solution of this problem involves solving three subproblems [8]:

- Connectivity problem: Deciding which lightpaths (optical circuits) must be established. The virtual topology is the set of lightpaths established in the network.
- Routing and resource allocation problem: Determining a route and assigning network resources for each lightpath.
- Traffic grooming: Routing traffic over the set of lightpaths ensuring the establishment of the SCs and serving the service connection requests.

To deal with all these problems jointly, we presented a genetic algorithm in [9], which not only solves the VNF-placement and chaining problems, but also designs the virtual topology of an underlying optical WDM network. However, that method does not implement protection against failures. In the paper presented in [10], we presented a new version of that method that implements VNF protection.

In this paper, we propose a new genetic algorithm for jointly solving the problems of VNF-placement, VNF-chaining and virtual topology design, including its three associated subproblems. The method, called GASVIT (Genetic Algorithm for Service mapping with VIrtual Topology design), implements a new policy for searching available VNFs in the chaining process (different from that in [9] and [10]). Versions of GASVIT including VNF protection will also be presented. GASVIT exploits collaboration between MEC nodes reducing the service blocking ratio when compared with previous proposals. A simulation analysis is presented to show the performance of GASVIT and to demonstrate the impact of a) solving all the subproblems jointly; b) exploiting the collaboration between MEC resources; and c) using shared protection schemes. Finally, the impact of deploying different physical topologies for the optical backhaul network is also analyzed.

The paper is structured as follows. In Section II, we present a review of the studies in the literature that address the VNF-placement, chaining, and survivability problems. Section III describes GASVIT. Section IV introduces the SC survivability problem in 5G-WDM networks and describes the versions of GASVIT that provide VNF protection against single node failures. Section V describes the setup scenario, the simulation results, and the study of the impact of deploying different physical topologies in terms of cost and service blocking ratio. Finally, Section VI concludes the paper.

II. RELATED WORK

There are many studies in the literature that address the VNF-placement and chaining problems from different perspectives and assuming diverse scenarios. A set of papers propose the use of linear formulations to solve the VNF-placement and VNF-chaining problems in static scenarios (i.e., scenarios where the service requests are known *a priori*). For instance, Lin *et al.* [11] presented a mixed-integer linear programming (MILP) model to solve the static VNF-placement and chaining considering limited computing resources, to minimize resource consumption. Bari *et al.* [12] proposed an integer linear programming (ILP) model that solves the VNF-placement problem, intending to minimize the cost of the network. Savi *et al.* [13] proposed an ILP model to solve the VNF-placement and chaining to minimize the number of active VNF-enabled nodes and ensuring that the latency constraints of the offered services are met.

Nevertheless, the VNF-placement and chaining problems have been shown to be NP-hard [14]. For this reason, it is common to find proposals based on heuristics and meta-heuristics to solve these problems. Askari *et al.* [15] addressed the latency problem by presenting a heuristic to solve the dynamic VNF-placement and chaining in 5G-metro networks, which minimizes the blocking ratio, reduces the number of NFV-enabled nodes, and ensures the fulfillment of latency constraints. Otokura *et al.* [16] proposed a genetic algorithm to solve the VNF-placement problem, with the aim of minimizing the overall delay and the number of active VNF-enabled nodes. The service blocking ratio has also been addressed by Pedreno-Manresa *et al.* [17], [18], who solved the VNF-placement and chaining problems in a realistic, 5G-access network scenario, with a heuristic that considered limited computing and network resource capabilities and drastic traffic changes. Ma *et al.* [19] proposed a genetic algorithm that solves the scheduling and computing resource allocation of workflows in IoT environments. It minimizes the cost in terms of active virtual machines, and ensures that the execution time meets the IoT service requirements. However, none of the previous proposals addresses the VNF-placement and chaining problems in conjunction with the virtual topology design problem, even when some of them consider WDM backhaul networks. The design of the virtual topology in WDM networks has also been shown to be NP-hard [20] and, thus, the joint solution of the three problems can benefit from the use of heuristics or artificial intelligence techniques [21].

The aforementioned proposals do not consider the SC survivability problem, a key issue to minimize disruption and loss of data in case of failures in the network. In the context of network resilience for NFV environments, Tomassilli *et al.* [22] proposed two optimization models to provide dedicated and shared path protection to the provisioned SC against single-link failure. Gao *et al.* [23] also focused on providing path protection, proposing the employment of multipath transmission. In contrast to the previous studies, which only focus on the resilience of the routes on the network, there are other studies which only address the protection of VNFs (rather than the routes). There are two different approaches in the literature to provide VNF protection: end-to-end SC protection and individual VNF protection.

In the end-to-end SC protection, when a primary SC is disrupted due to a node failure, its associated traffic is deviated to the backup SC and traverses it completely. Ye *et al.* [24] proposed a heuristic that solves the VNF-placement and chaining, further enhanced with end-to-end, dedicated or shared SC protection. The algorithm, however, does not address the virtual topology design problem. Hmaity *et al.* [25] proposed three end-to-end SC protection techniques: an end-to-end protection scheme, in which primary and backup SCs are link and node-disjoint, a second scheme which only provides path protection, and a third scheme where primary and backup nodes are node-disjoint but whose paths can share physical links, hence providing end-to-end protection against node failure.

In individual VNF protection, the traffic affected by a node failure traverses the backup VNFs associated with the affected primary ones but continues using the not-affected primary VNFs for the service chains. Fan *et al.* [26] proposed a heuristic for SC provisioning and individual VNF protection, which aims at minimizing the number of created backup VNFs. Beck *et al.* [27] proposed a heuristic that dynamically solves the VNF-placement and chaining with individual VNF protection. Casazza *et al.* [28] proposed two heuristics to solve the VNF-placement problem providing individual VNF protection, with the objective of maximizing the VNF availability, but their proposal does not solve the chaining problem. Aidi *et al.* [29] proposed an ILP model and two heuristics to provide individual, shared VNF protection to established SCs, with the objective of minimizing the resource consumption. However, none of the aforementioned proposals design the virtual topology of the network.

In order to fill the gap of previous proposals, mainly in the joint solution of the VNF-placement, VNF-chaining and virtual topology design problems (including its associated subproblems), we proposed in [9] a basic genetic algorithm, called GASM-VTD. Two versions of that algorithm were presented in that paper: no collaborative and collaborative. While the former only builds the SC using VNFs instantiated at the local node or at the central office, the latter allows the utilization of VNFs instantiated in any network node (but giving priority at the local node and at the central office). Those methods solve these problems jointly, but they do not implement VNF protection. Hence, in [10], we proposed a new version offering individual VNF protection against node failure.

In this paper, we propose an efficient artificial intelligence technique based on genetic algorithms to jointly solve the VNF-placement, VNF-chaining, and the virtual topology design problems. The proposal, called GASVIT (Genetic Algorithm for Service mapping with VIrtual Topology design), implements, in contrast to [9] and [10], a new chaining strategy able to better exploit the collaboration capabilities of the MEC nodes, thus improving network performance. Moreover, four additional versions of GASVIT are proposed to provide protection against node failures.

III. GENETIC ALGORITHM FOR SERVICE MAPPING WITH VIRTUAL TOPOLOGY DESIGN (GASVIT)

GASVIT is a genetic algorithm that solves the VNF-placement, the VNF-chaining and the virtual topology design problems. The latter is solved considering the three associated subproblems, i.e., connectivity, routing and resource allocation, and traffic grooming. Each potential solution of the problems is represented as an individual described by a chromosome composed of genes. Each gene represents the number of instances of a given VNF that must be located at a certain network node. An example of a chromosome is shown in Fig. 1.

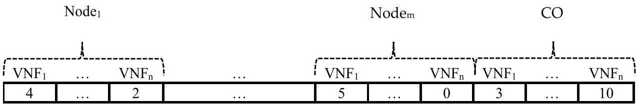


FIGURE 1. Chromosome.

The translating process of an individual (chromosome) into a solution of the VNF-placement, VNF-chaining and virtual topology design problems is as follows:

1. The algorithm creates the indicated instances of each type of VNF at each node of the network using the information from the chromosome (i.e., the genes).
2. The algorithm sorts the received service requests according to a preferred operator's priority and starts to build the required SCs, i.e., it begins the chaining process. In contrast to the method applied in [9], [10], the one proposed in this paper better exploits the

collaboration between the MEC nodes of the network by using the following search order for each VNF in the SC:

   2.1 Initially (only for the first VNF of the SC), a token is placed at the node to which the user requesting the service is connected.
   2.2 The algorithm searches available VNFs from the type requested at the node that has the token.
   2.3 When unable to find a VNF with enough free processing or storage capacity, it searches available VNFs from the type requested in the nodes that are placed at one hop in the physical topology from the node with the token.
   2.4 If it is not possible to find available VNFs in those nodes, the chaining continues with the nodes at two hops, then three hops and so on until searching all the nodes in the network.
   2.5 If there are not available VNFs in all the network nodes, it blocks the service request and continues with the following SC.
   2.6 When an available VNF is found, it reserves the VNF resources, moves the token to the node in which the VNF has been reserved and continues from step 2.2 in order to allocate resources for the next VNF of the SC. If the SC has already been fully established, it continues with the following request. When all the requests have been handled, it continues with the virtual topology design in step 3.

3. After reserving the allocated VNFs to the non-blocked SCs, the algorithm allocates the required network resources to transport the traffic from one VNF to the following VNF in the chain. If two consecutive VNFs are located at different nodes of the network, then it is necessary to create a virtual link with enough capacity to transport the associated traffic. If a lightpath between the source and destination nodes exists and has enough idle capacity, the algorithm uses it, performing traffic grooming, to deploy the virtual link. Otherwise, it tries to establish a new lightpath using the available network resources. If network resources cannot be allocated, the service request is blocked. The network resource allocation for the lightpath is solved by using the k-shortest paths and first fit techniques [30]. (Any other method proposed in the literature could be used, but this combination has been selected since it is very fast and, therefore, suitable for being used in the loop of the genetic algorithm)

In summary, at the end of this translation process, the chromosome has been translated into a problem solution; that is, it provides the final VNF placement, an SC for each (non-blocked) request and a virtual topology over the WDM backhaul network. The fitness of that solution is measured in terms of service blocking ratio, percentage of active CPU cores and percentage of used wavelengths.

GASVIT is a genetic algorithm and, therefore, it finds the final solution using the classical genetic loop [31]. The algorithm creates an initial parent population composed of randomly generated individuals and two ad-hoc individuals employed to enhance and speed up the performance of the algorithm. The ad-hoc individuals are generated using two VNF-placement and chaining algorithms based on proposals in the literature [17], [18]. We call these algorithms "MEC-First" and "CO-First". In MEC-First, the algorithm begins the chaining process at the local node to which the end-user is connected and searches an existing instance of the VNF with enough available capacity to process the associated traffic. If no available VNFs are found, the algorithm tries to create a new instance using the free computing resources at the node. If the available computing resources are insufficient to create the VNF instance, the algorithm repeats the same process at the CO. Once in the CO, MEC-First is not able to use or create VNFs at the local node again to establish the SC. If due to lack of network or computing resources, the algorithm is unable to create the SC, the service request is blocked. CO-First acts similarly to MEC-First but starting the chaining process at the CO and continuing at the local MEC node.

Once the parent population is created, the algorithm applies to the individuals two classical genetic operations: crossover and mutation. In crossover, the algorithm randomly selects two individuals from the population and a crossover point. Then, the algorithm interchanges the chromosomes of the individuals from the crossover point to the end of the chromosome, generating two new individuals. The resulting offspring undergoes the mutation operation, in which the algorithm randomly modifies the values of the genes, with a user-defined mutation probability. All the individuals created undergo then a validation process. In this stage, the algorithm checks the validity of each individual, by emulating its instantiation, i.e., by trying to create as many instances of each VNF at the corresponding host as the chromosome indicates. If the algorithm is not able to emulate the instantiation of the individual due to lack of computing resources, it is discarded and a new one is created. The algorithm repeats the crossover, mutation and validation operations until creating enough individuals to complete a certain descendant population size, which is user-defined.

At that point, all the individuals are translated using the previously described procedure and their fitness is computed. As mentioned before, there are three fitness parameters: the service blocking ratio, the percentage of active CPU cores and the percentage of used wavelengths. When the fitness calculation is completed, the algorithm selects the best individuals (a user-defined number) among the parent and the descendant populations to be parents of the following generation. In order to compare two individuals, the blocking ratio is used. If two individuals present the same service blocking ratio, the algorithm selects the individual with the lowest percentage of active CPU cores. If the individuals are tied in this parameter, then the one with the lowest percentage of used wavelengths is chosen.

The algorithm repeats the loop process a number of times, or generations, which is user-defined. At the end of the process, GASVIT provides the best solution found, which is composed of the VNF-placement, the established SCs, and the virtual topology designed.

IV. SC PROTECTION IN 5G-WDM NETWORKS

A. INTRODUCTION

When protecting SCs against failures, it is necessary to assign backup resources to each primary SC. As explained in Section II, there are two possible alternatives to protect the SCs: end-to-end SC protection and individual VNF protection. The latter is more efficient, especially if shared protection is used. Therefore, we focus on that scenario, and consider the case of protection against single node failures (like most of the proposals in the literature).

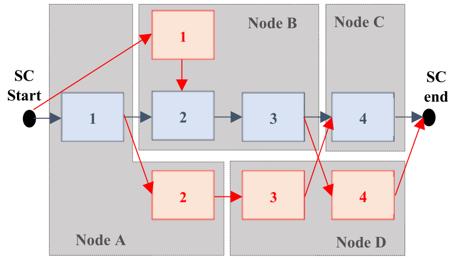


FIGURE 2. Example of a VNF protection scenario for four primary VNFs (blue blocks) and four backup VNFs (red blocks) and their corresponding network resources (blue and red arrows).

In VNF protection, a backup VNF is allocated to each primary VNF. An example of this kind of VNF protection scheme is shown in Fig. 2. In that example, it can be observed that, if Node A fails, the traffic associated with the primary VNF$_1$ (the blue block numbered as 1) will traverse the backup VNF$_1$ (the red block also numbered as 1) using the corresponding allocated backup network resources, represented with a red arrow. After traversing this VNF, the traffic will travel to the primary VNF$_2$, VNF$_3$, and VNF$_4$. If node B fails, then the traffic will traverse the primary VNF$_1$, the backup VNF$_2$ and VNF$_3$, and the primary VNF$_4$. Finally, if Node C fails, the traffic will go through the primary VNF$_1$, VNF$_2$, and VNF$_3$, and traverse the backup VNF$_4$.

One important characteristic in this scheme is that the algorithm must assign the VNFs and network resources for the primary SC (blue boxes and arrows in the figure), but it also must reserve resources for the backup elements (shown in red). Backup VNFs cannot be located in the same node than their corresponding primary VNFs. It is also mandatory to reserve network resources for all the backup connections that can be required with the failure of any node in the network.

Two different VNF protection strategies can be employed:

- **Dedicated VNF Protection:** A backup VNF only protects one primary VNF.
- **Shared VNF Protection:** A backup VNF can protect multiple primary VNFs, if they are located in different nodes, to avoid collision problems in case of a single node failure.

Moreover, the same shared and dedicated schemes can be applied to the network resources:

- **Dedicated backup network resources:** The backup connections cannot be shared among SCs.
- **Shared backup network resources:** The backup connections in a SC can be shared with other SCs, provided that they are not affected by the same node failure.

B. ENHANCING GASVIT TO PROVIDE INDIVIDUAL VNF-PROTECTION

GASVIT has been extended to incorporate the aforementioned protection schemes in order to guarantee SC survivability against single node failures. Thus, five versions of GASVIT have been developed:

- **GASVIT or GASVIT (NP):** No protection, as described in Section III.
- **GASVIT (DV, DN):** Dedicated VNF protection and dedicated network resources.
- **GASVIT (DV, SN):** Dedicated VNF protection and shared network resources.
- **GASVIT (SV, DN):** Shared VNF protection and dedicated network resources.
- **GASVIT (SV, SN):** Shared VNF protection and shared network resources.

When offering protection, the chromosome structure and the genetic loop are the same as in GASVIT, described in Section III. Moreover, the fitness function of each solution (individual) is calculated in the same way: service blocking ratio, number of active CPU cores and percentage of used wavelengths. The difference arises when translating the chromosome into a solution, as both the backup VNFs and the backup network resources have to be reserved.

During the translation stage, the algorithm creates the number of total VNF instances at the nodes of the network as indicated by the chromosome of the individual. The allocation of VNFs for the primary SC is done as in GASVIT (NP). When an SC cannot reserve all its VNFs, the service is blocked. If the SC is not blocked, i.e., the primary SC can be established, the process of reserving backup VNFs for the non-blocked SC takes place. The algorithm cannot select, as a backup resource, any VNF that has already been concatenated in a primary SC. Depending on the protection strategy, the algorithm selects either dedicated or shared backup VNFs. If a backup VNF is dedicated, it will only protect one primary VNF located at a different node. In contrast, a shared VNF can protect multiple primary VNFs, provided that they do not share location either between them or with the backup VNF. The search for computing resources for the backup VNFs follows the same procedure as for the primary one. That is, it starts searching resources in nodes at one hop distance from the node implementing the primary VNF to be protected. If there are no available resources, it searches in nodes at two hops distance, and so on until checking in the furthest nodes. If the algorithm is unable to find backup VNFs to protect all the primary VNFs in the SC, the service request is blocked.

Hereafter, the algorithm allocates the required network resources for the non-blocked SCs. This process is similar to the network allocation process in GASVIT (NP). However, when offering protection, the algorithm allocates first network resources to the primary SC and then the backup network resources. The procedure is analogous to the network resource allocation for the primary SCs (i.e., it uses available lightpaths if possible, and otherwise establishes a new lightpath if there are available resources). Lightpaths employed to allocate network resources to primary and backup SCs are completely independent. Moreover, the backup network resources can be shared or dedicated, and traffic grooming is also allowed for them. If network resources are allocated to both the primary SC and its protecting VNFs, the connection is established. Otherwise, it is blocked.

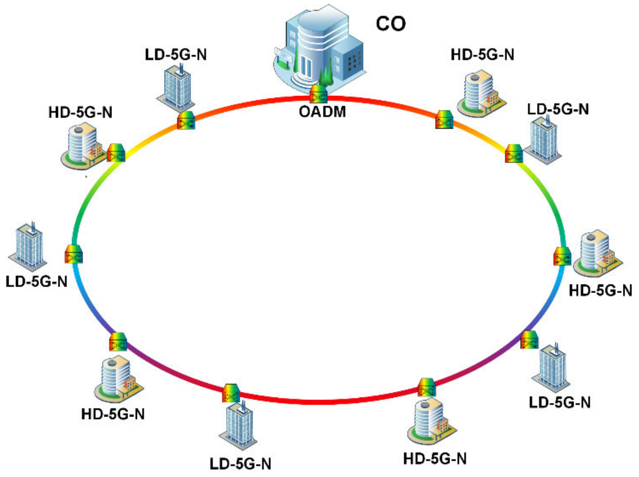


FIGURE 3. 5G-WDM ring topology network [10].

V. SIMULATION SCENARIO AND RESULTS

In order to test the performance of GASVIT, a simulation study has been conducted using the OMNeT++ platform [32]. Initially, tests have been carried out considering a 5G-WDM ring topology, shown in Fig. 3, since rings are the most extended topologies in metro networks. Furthermore, these topologies are very cost effective as nodes can be equipped with reconfigurable optical add-drop multiplexers (ROADM) instead of optical cross-connects (OXC) [33]. However, GASVIT can be used with any kind of topology. The advantages of including OXCs and additional links in the network will be studied in Section V.C.

The network used for the tests is composed of a CO, and ten 5G-nodes equipped with MEC resources, dividing them into two possible classes: five high demand (HD) 5G-nodes and five low demand (LD) 5G-nodes. LD-5G-nodes are equipped with fewer IT capabilities and serve an average of 10% of the end-users than HD-5G-nodes do. The allocated computing resources to each kind of 5G-node are shown in Table 1 [9], [17], [18]. Moreover, the nodes are equipped with 10 Gb/s optical transceivers and ROADMs.

We assume that the network is managed by one operator that offers three types of network services: VoIP, video streaming and web services. Users can request one of the services with a probability of 30%, 20% and 50%, respectively [9]. The corresponding SC and bandwidth requirements for each network service are listed in Table 2 [3], [9], [13], [17], [18], [34].

TABLE 1. IT resources allocated to the CO and the different 5G-nodes.

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

TABLE 2. Service chain requirements.

Service	Chained VNFs	Bandwidth
VoIP	NAT-FW-TM-FW-NAT	64 kb/s
Video	NAT-FW-TM-VOC-IDPS	4 Mb/s
Web Services	NAT-FW-TM-WOC-IDPS	100 kb/s

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

TABLE 3. VNF requirements.

VNF	HW Requirements	Throughput
NAT	CPU: 2 cores, RAM: 4 GB, HDD: 16 GB	2 Gb/s [35]
FW	CPU: 2 cores, RAM: 4 GB, HDD: 16 GB	2 Gb/s [35]
TM	CPU: 1 core, RAM: 2 GB, HDD: 16 GB	1 Gb/s [36]
WOC	CPU: 1 core, RAM: 2 GB, HDD: 40 GB	0.5 Gb/s [37]
IDPS	CPU: 1 core, RAM: 2 GB, HDD: 8 GB	1 Gb/s [38]
VOC	CPU: 2 cores, RAM: 4 GB, HDD: 2 GB	2 Gb/s[1]

[1] This value is derived from the figures of the other VNFs.

Lastly, the associated hardware requirements and processing capacity associated with each VNF are shown in Table 3.

The load of the network is measured in terms of the average number of users per HD-5G-node, $\bar{u}$. At the beginning of each simulation, the number of connected users to each HD-5G-node is randomly generated using a uniform distribution between $[0, 2\bar{u}]$, and the number of users of each LD-5G-node is randomly generated using a uniform distribution between $\left[0, 2\bar{u}/10\right]$.

The genetic algorithm is configured to generate an initial population composed of 5 individuals. The evolution process stops at 50 generations, and the algorithm generates 10 new individuals per generation. The mutation probability is set to 0.02. The simulations have been repeated 500 times (with different random seeds) for each value of $\bar{u}$, and the graphs are plotted in average with 95% confidence intervals.

A. PERFORMANCE OF GASVIT WITH NO PROTECTION

The performance of GASVIT has been compared with CO-First, MEC-First [17], [18], and the two versions of GASM-VTD (no collaborative and collaborative) that we previously proposed in [9]. No protection is considered in this first analysis. The network employs optical equipment configured to use up to 10 wavelengths. Fig. 4 shows the service blocking ratio (SBR), whereas Fig. 5 shows the percentage of active CPU cores when using the different methods. Finally, Fig. 6 shows the corresponding values of the average number of hops in the physical topology of the SCs, as an indicator of the propagation delay. (Processing delay in the nodes has not been compared, since the composition of the SCs in terms of number and type VNFs does not depend on the algorithm, but only on the type of service, as shown in Tables 2 and 3.)

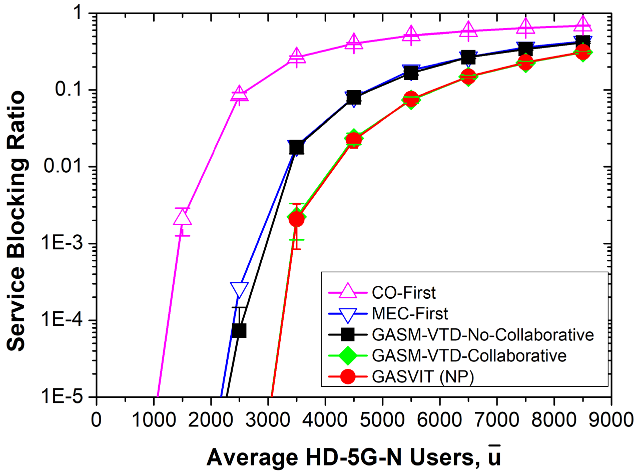


FIGURE 4. Service blocking ratio (SBR) of the solutions designed by GASVIT (NP), GASM-VTD [9], CO-First and MEC-First [17], [18].

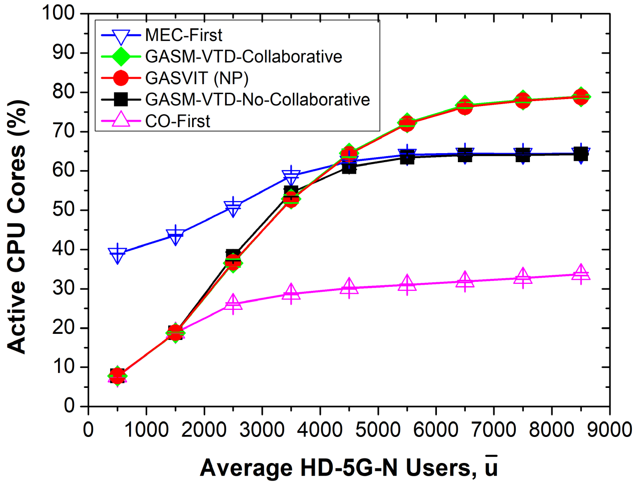


FIGURE 5. Percentage of active CPU cores of the solutions designed by GASVIT (NP), GASM-VTD [9]CO-First and MEC-First [17], [18].

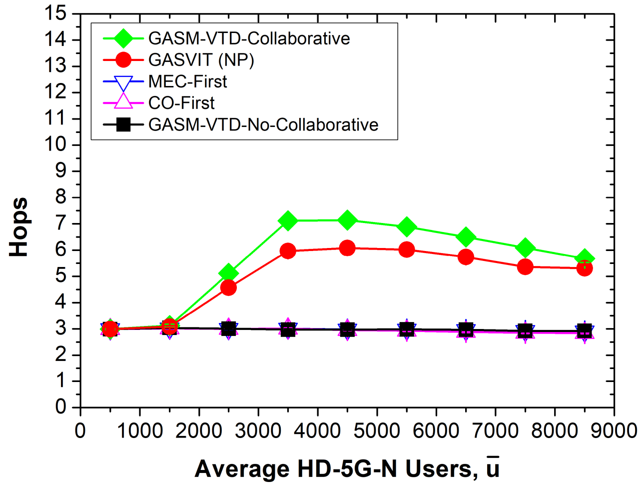


FIGURE 6. Average hops of the solutions designed by GASVIT (NP), GASM-VTD [9], CO-First and MEC-First [17], [18].

Fig. 4 shows that GASVIT and GASM-VTD-Collaborative, which exploit the collaboration between MEC nodes, are the methods that obtain solutions with the lowest SBR. Regarding the use of computing resources, those two methods employ the same number of CPU cores as GASM-VTD-No-Collaborative for values of average users per HD-5G-node lower than 5,000 (where the SBR is lower than 10^{-2}). Therefore, the collaborative strategies improve the SBR while not increasing the computing resource consumption. However, when the average number of users per 5G-HD-node increases, the collaborative algorithms require a higher percentage of active CPU cores in order to reduce the SBR. On the other hand, CO-first [17], [18] is the method that requires the lowest number of resources for all traffic loads, but it is the one with the worst SBR.

As we have just seen, the results obtained by GASVIT and GASM-VTD-Collaborative are the same in terms of both SBR and percentage of active CPU cores. However, when compared in terms of the average number of hops in the physical topology of the SCs (and thus in terms in propagation delay), GASVIT obtains better results than GASM-VTD-Collaborative (around one less hop for medium traffic loads), as shown in Fig. 6. Another advantage of GASVIT when compared to GASM-VTD-Collaborative will be shown in the next subsection, when protection schemes are analyzed. Coming back to the number of hops metric, it is worthy to note that the non-collaborative methods (CO-First, MEC-First, GASM-VTD-No-Collaborative) are the ones obtaining the lowest values in this parameter. Nevertheless, assuming that the 11-node metro WDM-ring network considered in this study, is deployed in a city with a diameter of ~10 km (i.e., less than 3 km, or 0.015 ms, between adjacent nodes, assuming they are equidistant), the average propagation delay of the SCs for GASVIT would be ~0.09 ms, well below 5G latency requirements (less than 1 ms) [39].

Finally, in terms of execution times, MEC and CO-First solve this network planning scenario (for a given average number of users per node) in less than 1 s, while GASM-VTD and GASVIT require ~14 minutes in a machine equipped with an AMD Opteron 6128 processor and 64 GB RAM. However, the computing time of GASVIT is low enough for a planning method, and it achieves high reductions of SBR when compared to MEC and CO-First. Moreover, as both GASVIT and GASM-VTD are genetic algorithms, they can be stopped at any moment, providing the best solution found until that moment if required.

B. PERFORMANCE OF GASVIT WITH PROTECTION

We now analyze the performance of the four versions of GASVIT that offer protection (each with different combinations of dedicated and shared protection, for VNFs and for network resources). Moreover, those four different versions of the method have also been compared with the following algorithms:

- **GASVIT (NP)**: The version with no protection
- **GASVIT (DV, ideal network)**: GASVIT with dedicated VNF protection, but without imposing any limit or constraint on network resources (in line with those methods that solve the VNF planning and VNF chaining problems without considering the underlying backhaul network).
- **GASVIT (SV, ideal network)**: Similar to the previous method, but using shared protection for VNFs.

Later, a comparison of the versions with protection of GASVIT and GASM-VTD-Collaborative[10], will also be presented.

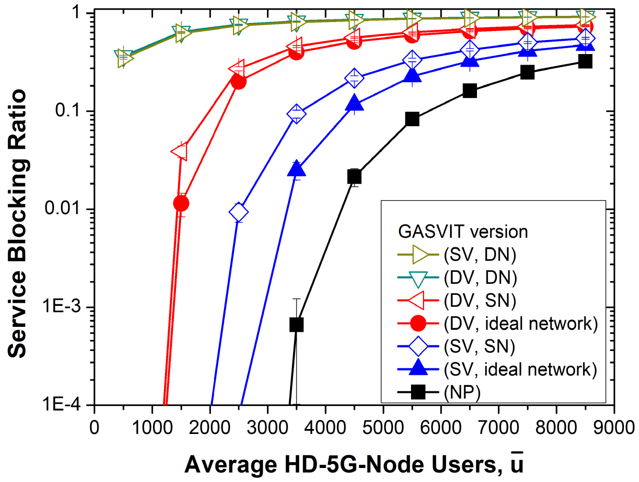


FIGURE 7. Service blocking ratio (SBR) obtained by the different protection techniques when the network is configured to use up to 10 wavelengths.

The network is initially configured to support up to 10 wavelengths in non-ideal scenarios. Fig. 7 shows the service blocking ratio obtained by the different protection algorithms while Fig. 8 shows the corresponding values of active CPU cores without distinguishing the ones used for primary and for backup SCs.

In Fig. 7, it can be observed that the inclusion of protection techniques obviously degrades the performance in terms of SBR and number of active CPUs, as computing and networking resources must be reserved for backup. In fact, the methods that use dedicated network (DN) resources for backup, i.e., GASVIT (DV, DN) and GASVIT (SV, DN), are the algorithms that show the worst results in terms of SBR. Actually, the high SBR of the solutions obtained with those protection techniques makes them unfeasible to be implemented in real networks (unless the network is equipped with a high number of resources at the expense of increasing its cost).

Focusing on the methods that use shared network (SN) resources, GASVIT (SV, SN) supports an average of 1,000 more users per HD-5G-node than GASVIT (DV,SN), maintaining the same SBR. Therefore, the protection scheme that implements resource sharing for both VNFs and network elements, GASVIT (SV, SN), is the one that achieves the best results (more than one order of magnitude of SBR reduction), because it makes an efficient use of resources.

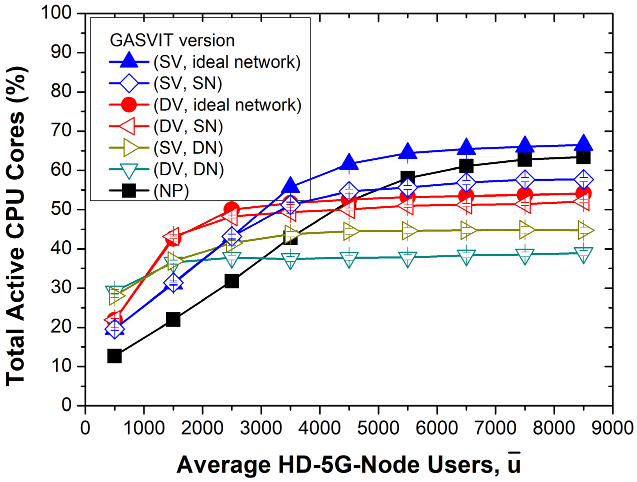


FIGURE 8. Percentage of active CPU cores obtained by the different protection techniques when the network is configured to use up to 10 wavelengths.

On the other hand, Fig. 7 also shows that the performance in a resource-limited network deviates from that obtained assuming an "ideal network" with "infinite" resources. Thus, if the virtual topology design problem is kept out the VNF-mapping problem (as most of previous proposals do), the solutions implemented in the networks will have much worst performance than that estimated in the design step. Therefore, it is of great importance to take into account the constraints imposed by the underlying network, i.e., by jointly designing the virtual topology in the case of a WDM network, when solving the VNF-placement and chaining problems, like GASVIT does.

Fig. 8 shows that the method without protection, GASVIT (NP), is the one that consumes less computational resources when the number of average users per HD-5G-node is low. Furthermore, the methods utilizing dedicated backup network resources employ less active CPU cores than their shared network counterparts. Nevertheless, this is due to the fact that the SBR for the DN versions of GASVIT is very high (as shown in Fig. 6) as a result of the lack of wavelength resources. Therefore, few SCs, and thus few VNFs are instantiated in CPU cores. In contrast, when shared network resources are used (SN versions of GASVIT), more virtual links between nodes can be established since wavelength resources are more efficiently used, thereby reducing the SBR, and increasing the number of SCs and thus VNFs instantiated in CPU cores.

On the other hand, for those scenarios where the SBR is low (low average number of users), shared VNF policies (SV versions of GASVIT) make 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 in terms of SBR (as shown in Fig. 7), but also in terms of resources in use.

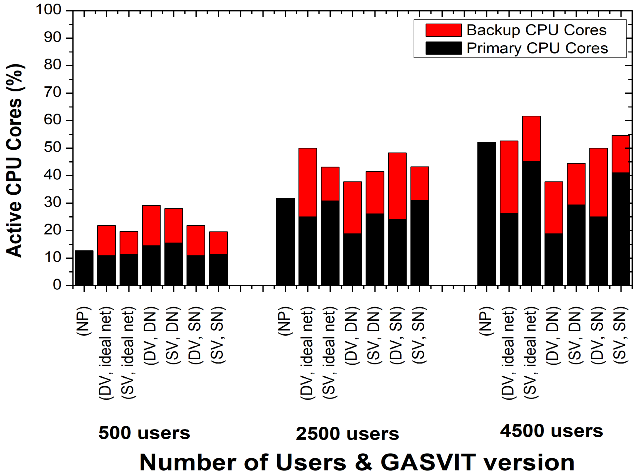


FIGURE 9. Comparison of the percentage of CPU cores allocated to primary and backup VNFs for the different protection techniques when the network is configured to use up to 10 wavelengths.

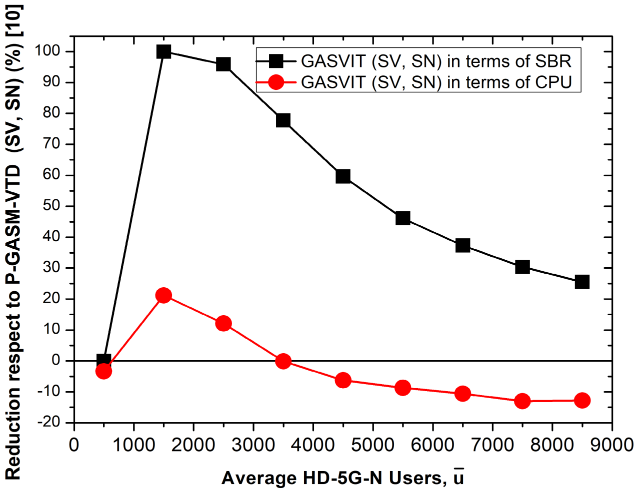


FIGURE 10. Percentage of reduction in terms of SBR and CPU usage of GASVIT (SV, SN) compared to P-GASM-VTD-Collaborative [10], considering shared VNF and shared network protection.

Fig. 9 shows a comparison of the percentage of active CPU cores allocated to primary and backup VNFs for the different protection schemes for three values of $\bar{u}$ (500, 2,500 and 4,500). It can be observed that the allocated number of active CPU cores increases with the number of average users. However, this increment is less noticeable between the $\bar{u} = 2,500$ and $\bar{u} = 4,500$ scenarios, except for GASVIT (NP), GASVIT (SV, ideal network), and GASVIT (SV, SN), since the lack of availability of network resources is the limiting factor. Comparing the percentage of CPUs for primary and backup VNFs, the percentages of CPUs allocated to backup VNFs 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.

Fig. 10 shows the percentage of reduction in terms of SBR and CPU usage when GASVIT (SV, SN) is employed, with respect to P-GASM-VTD-Collaborative [10], the version with protection of GASM-VTD-Collaborative. In both cases, the strategies of shared VNF and shared network resources are compared, as they are the ones that obtain the best results in terms of SBR. The results show that GASVIT (SV, SN) gets a very significant reduction in terms of SBR, up to more than 90% for some values of $\bar{u}$. Regarding the CPU usage, GASVIT (SV, SN) also outperforms P-GASM-VTD-Collaborative for around 2,000 users, although it uses more CPU cores for high network loads ($\bar{u} > 3,500$). In this way, the algorithm obtains an SBR reduction of more than 30% with an increment of less than 15% of CPU core usage.

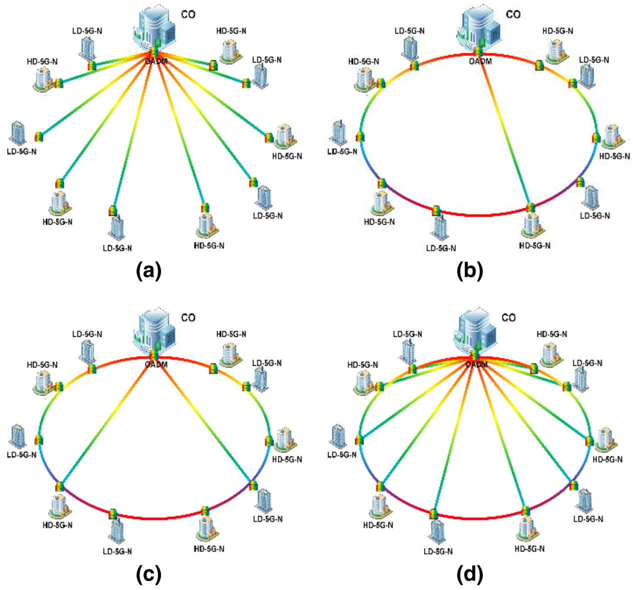
Taking into account these results, three important conclusions can be drawn: (i) the proposed method is able to improve the performance of P-GASM-VTD-Collaborative [10]; (ii) it is very important to jointly solve the VNF-placement, VNF-chaining and the virtual topology design in case of using a metro network based on WDM; and (iii) the reutilization of resources for backup (VNFs and network) is almost mandatory as it achieves significant improvement of the network performance when compared with those methods which do not use resource sharing for backup.

C. PERFORMANCE OF GASVIT ON DIFFERENT TOPOLOGIES

As mentioned before, GASVIT can operate with mesh topologies. Hence, in this section, we study the impact of deploying different types of topologies in a 5G-WDM network, in terms of network costs and service blocking ratio when protection is provided. We analyze the performance of GASVIT (SV, SN), as it is the version of GASVIT with protection that provides the best results in terms of SBR. Five topologies are studied: the metro ring topology used in the previous sections and shown in Fig. 3, a star topology, shown in Fig. 11(a), like the one used in other studies [17], [18], and three upgraded versions of the ring topology: adding one link composed of a fiber per each direction, adding two links (each one with two fibers), and a hybrid version of the ring and star topologies, shown in Fig. 11(b), Fig. 11(c), and Fig. 11(d), respectively.

For the sake of comparison, we have considered in the study that the nodes in all topologies are equipped with OXCs, and have assumed that the main contribution to the final cost of an OXC are the wavelength selective switches (WSS) [40]. Taking into account the OXC and cost model in [40], Table 4 shows the number of WSS necessary to build different types of OXC, and Table 5 shows the types of OXCs required by each topology and the total number of WSS. Fig. 12 shows the service blocking ratio reduction obtained by the different physical topologies, compared to the performance of the star topology in Fig. 11(a).

In terms of the number of WSS, the star topology is the one that requires the lowest number of WSS, but it also presents the worst values of SBR. Note that the rest of topologies achieve great reductions in terms of SBR compared with the star topology. The reason behind this is that the star topology is a centralized architecture and



(a) (b) (c) (d)

FIGURE 11. Additional topologies employed in the cost and performance study: (a) Star, (b) Ring+1 link, (c) Ring + 2 links, and (d) Hybrid.

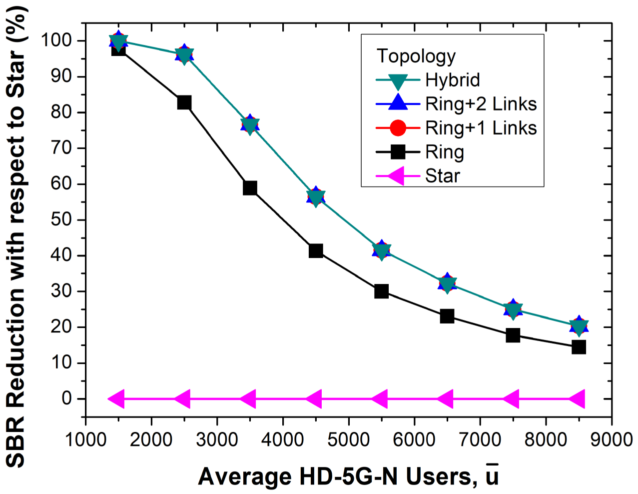


FIGURE 12. Service blocking ratio (SBR) reduction obtained by the different physical topologies.

TABLE 4. WSS in OXC.

OXC Type	WSS
OXC2 (2 links)	8
OXC3 (3 links)	11
OXC4 (4 links)	14
OXC10 (10 links)	34

TABLE 5. Type and number of OXCs required in each topology.

Topology	OXC2	OXC3	OXC4	OXC10	Total # WSS
Star	0	0		1	34
Ring	11	0			88
Ring+1 link	9	2			94
Ring+2 links	8	2	1		100
Hybrid	0	10		1	144

cannot exploit the collaboration between nodes, as all the lightpaths must traverse the central office. Therefore, when network nodes are equipped with MEC resources, establishing some direct links (fibers in the case of WDM optical networks) between MEC nodes is essential to fully exploit the collaboration between them and use the computing and storage capacities of those nodes more efficiently. The ring topology is the next best performing topology in terms of cost (as it has the second lowest number of WSS). Note that this architecture, nevertheless, can also be deployed using cost-effective ROADMs, as proposed in [33], which would reduce the cost of the network. Moreover, the SBR reduction compared to the star topology is over 50% for $\bar{u} \leq 3,500$. Moreover, if the ring topology is upgraded by incorporating more fibers, Fig. 12 shows that including only one more link (one fiber per direction), the SBR of obtained solutions is basically equivalent to that obtained with a hybrid topology, which provides the best performance in terms of SBR but is the most expensive alternative of the topologies studied in this section.

VI. CONCLUSION

In this study, we have proposed GASVIT, a genetic algorithm that jointly solves the VNF-placement, VNF-chaining and the virtual topology design problems in 5G networks equipped with MEC resources and a WDM backhaul. Moreover, a version of the method providing node protection has also been presented. GASVIT implements a new VNF-chaining technique that efficiently exploits the collaboration between network nodes that are equipped with MEC resources and are able to host VNF instances, thereby leading to lower service blocking ratio than previous proposals [9], [10], [17], [18].

Furthermore, the importance of solving the VNF-placement and VNF-chaining problems, in combination with the design of the virtual topology when WDM backhaul networks are used, has been proved. The joint solution of those three problems is a key feature of GASVIT, in contrast to other proposals.

Moreover, we have also demonstrated that the use of protection schemes using resource sharing for both VNFs and network resources, is almost mandatory, as significant improvements in network performance can be obtained when using that technique.

Finally, a study to evaluate the impact of using different physical topologies as the WDM backhaul network has been presented. The results from that study show that the topologies which establish direct connections between MEC nodes, like the ring or mesh topologies, are the ones that better exploit the collaboration between nodes allowing the implementation of much better solutions in terms of SBR, with the ring providing a very good trade-off in terms of SBR and cost.

REFERENCES

[1] J. Cosmas, N. Jawad, M. Salih, S. Redana, and O. Bulakci, "5G PPP architecture working group view on 5G architecture," 5G PPP Archit. Working Group, Heidelberg Germany, White Paper Version 1.0., 2019.

[2] B. Mukherjee, *Optical WDM Networks*. New York, NY, USA: Springer, 2006.

[3] M. Savi, A. Hmaity, G. Verticale, S. Host, and M. Tornatore, ''To distribute or not to distribute? Impact of latency on virtual network function distribution at the edge of FMC networks,'' in *Proc. 18th Int. Conf. Transparent Opt. Netw. (ICTON)*, Jul. 2016, pp. 1–4.

[4] M. Simsek, A. Aijaz, M. Dohler, J. Sachs, and G. Fettweis, ''5G-enabled tactile Internet,'' *IEEE J. Sel. Areas Commun.*, vol. 34, no. 3, pp. 460–473, Mar. 2016, doi: 10.1109/JSAC.2016.2525398.

[5] M. Patel, B. Naughton, C. Chan, N. Sprecher, S. Abeta, and A. Neal, ''Mobile-edge computing—Introductory technical white paper,'' Mobile-Edge Comput. (MEC) Ind. Initiative, White Paper v 1.0., 2014.

[6] H. Gao, Y. Duan, L. Shao, and X. Sun, ''Transformation-based processing of typed resources for multimedia sources in the IoT environment,'' *Wireless Netw.*, pp. 1–17, Nov. 2019, doi: 10.1007/s11276-019-02200-6.

[7] H. Gao, Y. Xu, Y. Yin, W. Zhang, R. Li, and X. Wang, ''Context-aware QoS prediction with neural collaborative filtering for Internet-of-Things services,'' *IEEE Internet Things J.*, early access, Dec. 2, 2019, doi: 10.1109/JIOT.2019.2956827.

[8] B. Mukherjee, D. Banerjee, S. Ramamurthy, and A. Mukherjee, ''Some principles for designing a wide-area WDM optical network,'' *IEEE/ACM Trans. Netw.*, vol. 4, no. 5, pp. 684–696, Oct. 1996, doi: 10.1109/90.541317.

[9] L. Ruiz, R. J. Duran, I. de Miguel, N. Merayo, J. C. Aguado, P. Fernandez, R. M. Lorenzo, and E. J. Abril, ''Joint VNF-provisioning and virtual topology design in 5G optical metro networks,'' in *Proc. 21st Int. Conf. Transparent Opt. Netw. (ICTON)*, Angers, France, Jul. 2019, pp. 1–4.

[10] L. Ruiz, ''Design of VNF-mapping with node protection in WDM metro networks,'' presented at the Int. Conf. Broadband Commun., Netw. Syst., 2019, pp. 285–298.

[11] T. Lin, Z. Zhou, M. Tornatore, and B. Mukherjee, ''Optimal network function virtualization realizing End-to-End requests,'' in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, San Diego, CA, USA, Dec. 2015, pp. 1–6.

[12] M. F. Bari, S. R. Chowdhury, R. Ahmed, and R. Boutaba, ''On orchestrating virtual network functions,'' in *Proc. 11th Int. Conf. Netw. Service Manage. (CNSM)*, Nov. 2015, pp. 50–56, doi: 10.1109/CNSM.2015.7367338.

[13] M. Savi, M. Tornatore, and G. Verticale, ''Impact of processing costs on service chain placement in network functions virtualization,'' in *Proc. IEEE Conf. Netw. Function Virtualization Softw. Defined Netw. (NFV-SDN)*, San Francisco, CA, USA, Nov. 2015, pp. 191–197, doi: 10.1109/NFV-SDN.2015.7387426.

[14] F. Bari, S. R. Chowdhury, R. Ahmed, R. Boutaba, and O. C. M. B. Duarte, ''Orchestrating virtualized network functions,'' *IEEE Trans. Netw. Service Manage.*, vol. 13, no. 4, pp. 725–739, Dec. 2016, doi: 10.1109/TNSM.2016.2569020.

[15] L. Askari, A. Hmaity, F. Musumeci, and M. Tornatore, ''Virtual-network-function placement for dynamic service chaining in metro-area networks,'' in *Proc. Int. Conf. Opt. Netw. Design Model. (ONDM)*, Dublin, Republic of Ireland, May 2018, pp. 136–141, doi: 10.23919/ONDM.2018.8396120.

[16] M. Otokura, K. Leibnitz, Y. Koizumi, D. Kominami, T. Shimokawa, and M. Murata, ''Application of evolutionary mechanism to dynamic virtual network function placement,'' in *Proc. IEEE 24th Int. Conf. Netw. Protocols (ICNP)*, Singapore, Nov. 2016, pp. 1–6.

[17] J.-J. Pedreno-Manresa, P. S. Khodashenas, M. S. Siddiqui, and P. Pavon-Marino, ''Dynamic QoS/QoE assurance in realistic NFV-enabled 5G access networks,'' in *Proc. 19th Int. Conf. Transparent Opt. Netw. (ICTON)*, Girona, Spain, Jul. 2017, pp. 1–4, doi: 10.1109/ICTON.2017.8025149.

[18] J.-J. Pedreno-Manresa, P. S. Khodashenas, M. S. Siddiqui, and P. Pavon-Marino, ''On the need of joint bandwidth and NFV resource orchestration: A realistic 5G access network use case,'' *IEEE Commun. Lett.*, vol. 22, no. 1, pp. 145–148, Jan. 2018, doi: 10.1109/LCOMM.2017.2760826.

[19] X. Ma, H. Gao, H. Xu, and M. Bian, ''An IoT-based task scheduling optimization scheme considering the deadline and cost-aware scientific workflow for cloud computing,'' *EURASIP J. Wireless Commun. Netw.*, vol. 2019, no. 1, p. 249, Dec. 2019, doi: 10.1186/s13638-019-1557-3.

[20] R. Dutta and G. N. Rouskas, ''A survey of virtual topology design algorithms for wavelength routed optical networks,'' *Opt. Netw. Mag.*, vol. 1, no. 1, pp. 73–89, 2000.

[21] J. Mata, I. de Miguel, R. J. Durán, N. Merayo, S. K. Singh, A. Jukan, and M. Chamania, ''Artificial intelligence (AI) methods in optical networks: A comprehensive survey,'' *Opt. Switching Netw.*, vol. 28, pp. 43–57, Apr. 2018, doi: 10.1016/j.osn.2017.12.006.

[22] A. Tomassilli, N. Huin, F. Giroire, and B. Jaumard, ''Resource requirements for reliable service function chaining,'' in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–7, doi: 10.1109/ICC.2018.8422774.

[23] T. Gao, X. Li, W. Zou, and S. Huang, ''Survivable VNF placement and scheduling with multipath protection in elastic optical datacenter networks,'' in *Proc. Opt. Fiber Commun. Conf. (OFC)*, 2019, pp. 1–3.

[24] 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 Netw.*, vol. 30, no. 3, pp. 81–87, May 2016, doi: 10.1109/MNET.2016.7474348.

[25] A. Hmaity, M. Savi, F. Musumeci, M. Tornatore, and A. Pattavina, ''Virtual network function placement for resilient service chain provisioning,'' in *Proc. 8th Int. Workshop Resilient Netw. Design Modeling (RNDM)*, Halmstad, Sweden, Sep. 2016, pp. 245–252, doi: 10.1109/RNDM.2016.7608294.

[26] J. Fan, Z. Ye, C. Guan, X. Gao, K. Ren, and C. Qiao, ''GREP: Guaranteeing reliability with enhanced protection in NFV,'' in *Proc. ACM SIGCOMM Workshop Hot Topics Middleboxes Netw. Function Virtualization (HotMiddlebox)*, New York, NY, USA, 2015, pp. 13–18, doi: 10.1145/2785989.2786000.

[27] M. T. Beck, J. F. Botero, and K. Samelin, ''Resilient allocation of service function chains,'' in *Proc. IEEE Conf. Netw. Function Virtualization Softw. Defined Netw. (NFV-SDN)*, Nov. 2016, pp. 128–133, doi: 10.1109/NFV-SDN.2016.7919487.

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

[29] S. Aidi, M. F. Zhani, and Y. Elkhatib, ''On improving service chains survivability through efficient backup provisioning,'' in *Proc. 14th Int. Conf. Netw. Service Manage. (CNSM)*, Nov. 2018, pp. 108–115.

[30] H. Zang, J. P. Jue, and B. Mukherjee, ''A review of routing and wavelength assignment approaches for wavelength-routed optical WDM networks,'' *Opt. Netw. Mag.*, vol. 1, no. 1, pp. 47–60, Jan. 2000.

[31] D. Goldberg, *Genetic Algorithms in Search, Optimization, and Machine Learning*. Reading, MA, USA: Addison-Wesley, 1989.

[32] *OMNeT++ is a C++ Based Discrete Event Simulator*. [Online]. Available: https://omnetpp.org/

[33] S. Sarmiento, J. A. Altabas, D. Izquierdo, I. Garces, S. Spadaro, and J. A. Lazaro, ''Cost-effective DWDM ROADM design for flexible sustainable optical metro–access networks,'' *J. Opt. Commun. Netw.*, vol. 9, no. 12, pp. 1116–1124, Dec. 2017, doi: 10.1364/JOCN.9.001116.

[34] L. Ruiz, R. Durán, I. de Miguel, P. Khodashenas, J.-J. Pedreño-Manresa, N. Merayo, J. Aguado, P. Pavón-Marino, S. Siddiqui, J. Mata, P. Fernández, R. Lorenzo, and E. Abril, ''A genetic algorithm for VNF provisioning in NFV-enabled Cloud/MEC RAN architectures,'' *Appl. Sci.*, vol. 8, no. 12, p. 2614, Dec. 2018, doi: 10.3390/app8122614.

[35] *vSRX Virtual Firewall*, Juniper Netw., Sunnyvale, CA, USA, Nov-2018.

[36] *Virtual Traffic Manager*, Brocade Commun. Syst., San Jose, CA, USA, 2015.

[37] *Talari SD-WAN Solutions*, Talari Netw., San Jose, CA, USA, 2018.

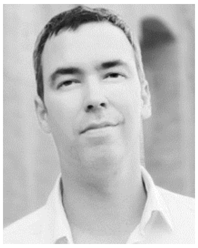
[38] *Cisco Adaptive Security Virtual Appliance (ASAv)*, Cisco, San Jose, CA, USA, 2018.

[39] M. Maternia, S. E. El Ayoubi, M. Fallgren, P. Spapis, Y. Qi, D. Martín-Sacristán, Ó. Carrasco, M. Fresia, M. Payaró, M. Schubert, J. S. Bedo, and V. Kulkarni, ''5G PPP use cases and performance evaluation models,'' 5G-PPP Archit. Working Group, Tech. Rep. v1, 2016.

[40] F. Rambach, B. Konrad, L. Dembeck, U. Gebhard, M. Gunkel, M. Quagliotti, L. Serra, and V. López, ''A multilayer cost model for Metro/Core networks,'' *J. Opt. Commun. Netw.*, vol. 5, no. 3, pp. 210–225, Mar. 2013, doi: 10.1364/JOCN.5.000210.

LIDIA RUIZ received the Telecommunication Engineer degree and the Master of Research degree in information and telecommunication technologies from the University of Valladolid, Spain, in 2013 and 2015, respectively. She is currently pursuing the Ph.D. degree with the Optical Communications Group.

She worked as an IT Consultant. Her research interests are 5G, network function virtualization, virtual topology design in WRON networks, and the design of RSA algorithms in flexible optical networks.



RAMÓN J. DURÁN BARROSO received the Telecommunication Engineer and Ph.D. degrees from the University of Valladolid, Spain, in 2002 and 2008, respectively. He is currently working as an Associate Professor at the University of Valladolid, where he is currently the Deputy Director of the Faculty of Telecommunication Engineering. He is the author of more than 100 articles in international journals and conferences. His current research focuses on the use of artificial intelligence techniques for the design, optimization, and operation of future heterogeneous networks, mobile edge computing, and network function virtualization. He is the Coordinator of the Spanish Research Thematic Network (Go2Edge: Engineering Future Secure Edge Computing Networks, Systems and Services) composed of 15 entities.

IGNACIO DE MIGUEL received the Telecommunication Engineer and Ph.D. degrees from the Universidad de Valladolid (UVa), Spain, in 1997 and 2002, respectively. Since 1997, he has been working as a Lecturer at UVa, where he is currently an Associate Professor. He is also the Coordinator of the Master in Telecommunication Engineering and the Master in Big Data Science at UVa. He has also been a Visiting Research Fellow with University College London, U.K. His research interests are mainly focused on the design and performance evaluation of optical networks and the application of artificial intelligence techniques. He has been a member of TPC of several international conferences, besides being the Chair of TPC, and the local Organizing Committee of NOC 2009. He was a recipient of the Nortel Networks Prize to the Best Ph.D. Thesis on optical internet, in 2002, and awarded by the Spanish Institute and Association of Telecommunication Engineers (COIT/AEIT).

NOEMÍ MERAYO received the Telecommunication Engineer degree in engineering from the University of Valladolid, Spain, in February 2004, and the Ph.D. degree from the Optical Communication Group, University of Valladolid, in July 2009. Her Ph.D. research focused on the design and performance evaluation of optical networks, especially passive optical networks. Since 2005, she has been working as a Junior Lecturer at the University of Valladolid. She has also been a Visiting Research Fellow with the University of Hertfordshire, London, working with the Optical Networks Group, Science and Technology Research Institute (STRI). She has also been a Postdoctoral Researcher with the Group of Transmisiones Ópticas de Banda Ancha (TOyBA), University of Zaragoza.

JUAN CARLOS AGUADO received the Telecommunication Engineer and Ph.D. degrees from the University of Valladolid, Spain, in 1997 and 2005, respectively. He has been working as a Junior Lecturer at the University of Valladolid, since 1998. His current research interests include the design and evaluation of cognitive methods applied to physical-layer modeling and traffic routing in heterogeneous optical networks.

RAMÓN DE LA ROSA received the M.Sc. degree from the School of Telecommunication Engineering (STE), Universidad de Valladolid, Spain, in 1999, and the Ph.D. degree, in 2005.

After a short period of working in QA for the main HFC network provider in Madrid, he enrolled in the Signal Theory, Communications, and Telematic Engineering Doctorate Program at the Universidad de Valladolid. His research is related to bioengineering and the measurement of non-ionizing electromagnetic fields (EMF) in populated areas, pioneering the earlier works in Spain to map the EMF levels in the main cities of the Castile and León region. He is currently with Space Communications, being in charge of the STE's ground station for satellite tracking and acting as a reviewer in the field of space communications in the yearly M.Sc. and Ph.D. awards of the Professional Association of Telecommunication Engineers. He was awarded by the 3M Foundation for his work related to neuromuscular human–machine interfaces, in 2007.

PATRICIA FERNÁNDEZ received the Telecommunication Engineer degree from the Universidad Politécnica de Cataluña, Barcelona, Spain, in 1997, and the Ph.D. degree from the University of Valladolid, in 2004. Since 1999, she has been working as a Junior Lecturer at the University of Valladolid. She is the author of more than 40 articles in international journals and conferences. Her research interests are passive optical networks and fiber-optic communications components.

RUBÉN M. LORENZO received the Telecommunication Engineer and Ph.D. degrees from the University of Valladolid, Spain, in 1996 and 1999, respectively. From 1996 to 2000, he was a Junior Lecturer with the University of Valladolid, where he joined the Optical Communications Group. Since 2000, he has been a Lecturer. He was the Head of the Faculty of Telecommunication Engineering, University of Valladolid, and the Research Director of Center for the Development of Telecommunications (CEDETEL). His research interests include integrated optics, optical communication systems, and optical networks.

EVARISTO J. ABRIL received the Telecommunication Engineer and Ph.D. degrees from the Universidad Politécnica de Madrid, Spain, in 1985 and 1987, respectively. From 1984 to 1986, he was a Research Assistant with the Universidad Politécnica de Madrid, becoming a Lecturer, in 1987. Since 1995, he has been a Full Professor with the University of Valladolid, Spain, where he founded the Optical Communications Group. He is the author of more than 100 articles in international journals and conferences. His research interests include integrated optics, optical communication systems, and optical networks.

• • •