Deploying Disaster-Resilient Service Function Chains using Adaptive Multi-Path Routing

Mohamed Abderrahmane Madani, Fen Zhou, Ahmed Meddahi

Deploying Disaster-Resilient Service Function Chains using Adaptive Multi-Path Routing

Mohamed Abderrahmane Madani, Fen Zhou, *Senior Member, IEEE,* and Ahmed Meddahi

***Abstract*—Network Function Virtualization (NFV) is a new technology that deploys network services and functions as software components in data centers and cloud environments. One of its key applications is Service Function Chain (SFC), which chains a set of Virtual Network Functions (VNFs) in a specific order to deliver a desired service. However, deploying NFV and SFC networks faces challenges, particularly in terms of disaster resiliency. This encompasses natural disasters and hardware failures, which can disrupt network operations and lead to service interruption or degradation across an entire disaster zone (DZ). Therefore, designing NFV and SFC networks that can withstand disasters while providing high levels of service availability and reliability is important. This paper presents a new method for protecting SFCs using adaptive multi-path routing. The proposed Multi-path Protection (MP) method has the advantage of reducing the amount of reserved bandwidth on backup paths by distributing SFC traffic over multiple DZ-disjoint working paths. The problem being addressed involves VNFs placement, routing SFCs, and implementing protection mechanisms. The objective is to minimize network resource consumption, including both the bandwidth used by request routing paths and the computing resources for VNF execution. To solve this multi-dimensional optimization problem, a path-adaptive and flow-based integer linear program (ILP) is proposed to provide the optimal solution in sall-size network settings. We also propose a heuristic approach that offers the near-optimal solution in a time-efficient way. Comprehensive simulation results show that the proposed MP strategy outperforms traditional Dedicated Protection (DP) in terms of bandwidth and processing resource consumption, resulting in a significant gain up to 20%.**

***Index Terms*—Network Function Virtualization (NFV), Service Function Chain (SFC), Disaster Resiliency, Multi-path Routing, Integer Linear Programming (ILP), Heuristic**

I. Introduction

The increasing demand for network services has resulted in the rapid development of technologies such as cloud and edge computing, which require both high network resources and reliability. Traditionally, network services require multiple network functions (NFs) located on proprietary hardware equipments, increasing operational and capital expenses: OPEX (Operating Expenditures) and CAPEX (Capital Expenditures) [3] [4]. To address this challenge, Network Function Virtualization (NFV) is proposed, where NFs are decoupled from their dedicated hardware appliances to be deployed on Virtual Machines (VMs) on top of generic hardwares such as servers and storage devices in Data Centers (DCs). This approach allows for better flexibility, cost-effectiveness, and scalability by enabling network service providers to reduce the cost of deploying and maintaining network functions while improving flexibility and reliability of their networks. Furthermore, by using VNFs, the number of functions can be scaled in or out on servers to match the network service deployment requirements [5].

To satisfy certain network requirements, Virtual Network Functions (VNFs) must be arranged in a specific order to form a service, termed a Service Function Chain (SFC). The SFC allocation is managed by the Management and Orchestration (MANO) system to satisfy specific business needs. Many studies have been conducted on the SFCs mapping problem, and most of them focus on backup and recovery by considering only a single link failure or single node failure [6]. However, under real conditions, natural disasters such as floods, earthquakes, or power outages may cause an area failure or even large-scale failures, called Disaster Zone (DZ) [7] [8]. In this case, all the nodes located in a DZ and the outgoing links from this DZ will fail, causing network functions to fail to recover from single node or link protection strategy. Therefore, a DZ-disjoint working and backup paths embedding should be considered to protect against disaster failures. In this paper, we present a new protection strategy that is not frequently seen in current research. This strategy is based on an efficient disaster protection scheme for embedding SFC using adaptive multi-path. Most of the existing works in this area are based on single path routing for SFC, making the new multi-path approach a unique and promising candidate in this context.

Our goal is to propose novel modeling and algorithms for disaster protection of SFC by implementing multi-path routing. The proposed approach differs from traditional methods that only use a single working path. We focus on minimizing the total network cost, including bandwidth and processing, while fully provisioning and protecting a set of SFCs. The disaster protection strategy addresses multiple aspects of network planning optimization, such as NFV placement, SFC routing and protection, which results in a complex combinatorial optimization problem. To solve this problem, we propose a path-adaptive and flow-based ILP to obtain the optimal solutions. Additionally, heuristics are proposed to provide high-quality solutions in a reasonable time. Our work leads to the following four contributions:

- First, we propose a novel adaptive multi-path based disaster protection scheme for SFC provisioning. Instead of relying on a single working path to route an SFC, we use multiple DZ-disjoint paths, along with a backup

A preliminary version of partial of this work has been published in the conferences IEEE CNSM 2023 [1] and IEEE CSCN 2023 [2].

*Fen Zhou is with LIA, Avignon University, France (email: fen.zhou@univ-avignon.fr). *Corresponding author.

Mohamed Abderrahmane Madani and Ahmed Meddahi are with Centre for Digital Systems, IMT Nord Europe, Institut Mines-Télécom, Lille, France (email: mohamed.madani@imt-nord-europe.fr, ahmed.meddahi@imt-nord-europe.fr)

path for protection in case of a DZ failure. The proposed multi-path protection scheme offers two main advantages: it balances traffic load across multiple working paths and reduces the reserved bandwidth on the backup path by at least 50%. Through numerical simulations, we make an important observation: When increasing the number of paths for routing an SFC, the operational cost decreases first and then starts to rise after reaching its minimum. This demonstrates the necessity to find the optimal number of routing paths so as to find a tradeoff among the bandwidth savings and the operational cost.

- The studied SFC disaster protection problem is NP-hard. We propose a new layered-flow based ILP model to get the optimal protection solution. Our proposed formulation is more adapted to actual needs than the existing formulations. The key advantage of our approach is that it uses an optimized number of paths for SFC provisioning that can adapt to different requests based on the network's capabilities and availability. In contrast, existing formulations use a fixed number of paths that is predefined without regard to specific network conditions.
- In order to overcome the limitations of the ILP model and to respond to real case scenarios where a large number of SFC requests have to be processed in a short period of time, new heuristics have been developed, for the first time, that address the SFC disaster protection problem.
- The proposed ILP and heuristic algorithms were tested using numerical simulations on multiple novel realistic network topologies. The results show a significant enhancement of 20% cost saving in the proposed multi-path protection scheme compared to the traditional disaster protection methods. Moreover, the heuristics keep this gain consistently, even for large-scale experiments, within a reasonable time.

The organization of the remainder of the paper is outlined as follows: Section II provides a review of the related literature. Section III explores the Disaster-Resilient SFC with Multi-Path Routing strategy. The ILP model and heuristics are presented as solutions in Section IV. The effectiveness of the proposed solutions is evaluated through numerical simulations in Section V. Finally, we conclude this paper in Section VI.

II. Related Work

SFC Embedding problem, as a sub-problem of Network Embedding (NE), and is a well-known NP-hard problem. It has been widely studied using various approaches and criteria. Different use case scenarios have been considered in these studies, taking into consideration specific constraints in different areas such as packet/optical data centers. In terms of optimization methods, various solutions have been also proposed including the use of mixed integer linear program (MILP/ILP) models as in [9] [10], Column Generation (CG) as in [8] to find optimal solutions, fast heuristics as in [4] [6] [11] to find approximating solutions, and meta-heuristics as in [12].

Regarding the objectives of these studies, optimization of network cost has been a major focus as in [4] [6] [13] [11], while service availability in [12], latency in [9], and jitter reduction have also been studied. In particular, [6] focused on designing Virtual Network Functions forwarding graphs (VNF-FGs) to describe resilient SFC and take into account VNF dependencies and proposed back-tracking SFC mapping methods to allocate VNFs. [3] proposed various heuristic algorithms to allocate VNFs based on different route selection schemes. [4] presented an ILP formulation for VNF orchestration in a small scale network and then used a heuristic to deal with large instances to solve it in a reasonable time. [11] considered the path latency and resource capacity limits, while minimizing the number of used nodes and arcs. [9] proposed protection strategies against single-node, single-arc, and single-node/link failures. Additionally, [13] proposed a path-based MILP to minimize the node activation and VNF installation cost, and also provided a heuristic to reduce the computational time. In [14], a detailed survey on VNF placement and SFC routing problems are presented, either dealt with independently or jointly, optimization objective and mathematical formulations, also recent existing solutions were summarized and compared. [15] discusses the importance of various parameters in the effective placement of virtualized network functions in 5G and beyond, with a review of existing VNF placement strategies and algorithms.

The topic of disaster-resilient networking has seen great attention in recent papers, such as in [7] [8] [16] [17] investigating various approaches to the problem. However, relatively few studies have focused specifically on disaster-resilient SFC embedding. Previous works, such as [12] proposed a RA-GEN scheme with a proposed heuristic algorithm, aims at minimizing VNF deployment cost, routing cost, and link usage. [18] addresses Connectivity-aware Virtual Network Embedding problem, which consists in embedding a virtual network (VN) on a substrate network while ensuring VN connectivity against multiple substrate link failures. [19] proposed a multi-path link embedding to improve the survivability of virtual networks. However, most of the proposed schemes reserve the same bandwidth on the backup path as the working path, leading to a significant waste of bandwidth. [20] focused on the reliability of 5G transport-network slices in Elastic Optical Networks while providing dedicated protection and the proposed solution incorporates techniques such as bandwidth squeezing and survivable multi-path provisioning to reduce the amount of backup resources required.

The first work that proposed using the multi-path approach for SFC protection was presented in [21], suggested the use of multiple DZ-disjoint working paths and balancing the SFC traffic load to reduce the reserved bandwidth on the backup path by at least 50%. An ILP model was proposed for this purpose, but it had a fixed number of paths which is predetermined without taking into account the network conditions. Therefore, the model did not accurately represent real-world scenarios. This paper aims to propose practical solutions for disaster-resilient SFC embedding and to investigate the potential benefits of using an adaptive multipath strategy to protect SFC. This will help to increase their applicability and effectiveness in real-world scenarios and may lead to infeasible solutions. It's worth noting that heuristics have been

proposed in [1] for this purpose, and preliminary evaluations indicate the potential effectiveness of this strategy. In addition, a path-adaptive ILP was also proposed in [2] for solving the problem optimally in small networks. However, there is still a pressing need for a more thorough theoretical examination of the proposed Multi-path Protection strategy, including the bi-objective optimization in the objective function, the impact of the number of paths on the operational cost, and the protection efficiency, which motivates this paper.

III. Disaster-Resilient Service Function Chains with Adaptive Multi-Path Routing

The ability to provide reliable and efficient SFC is crucial for modern networks. Ensuring SFC availability during natural disasters is challenging due to potential threats to network reliability. To address this, an effective disaster protection scheme for SFC provisioning that optimizes resources is necessary. By managing and allocating network resources carefully, we can enhance network resiliency and ensure continued SFC provision during disasters. We first outline the general network structure, including physical nodes and arcs, as well as VNFs and virtual links used for SFC requests. Then, we introduce our adaptive multi-path SFC disaster protection strategy. The following sections will detail our strategy's implementation.

In our study, we focus on bandwidth and CPU processing as the primary cost components of NFV operations, aligning with the emphasis in most literature [22] [23]. Other costs, such as VNF storage on the node, are taken into account by constraints to ensure this cost remains within the limits of resources. However, it is essential to recognize that the operational cost includes additional expenses such as instantiation costs, data fragmentation costs, data merge costs, monitoring costs, etc. These factors are often highlighted in various studies [24] [25]. Our objective is to minimize operational costs by reducing bandwidth and CPU processing expenditures, acknowledging the potential for other costs to influence the net savings. Notably, VNF storage is also taken into account by the constraints to ensure capacity limits.

A. Network Modeling

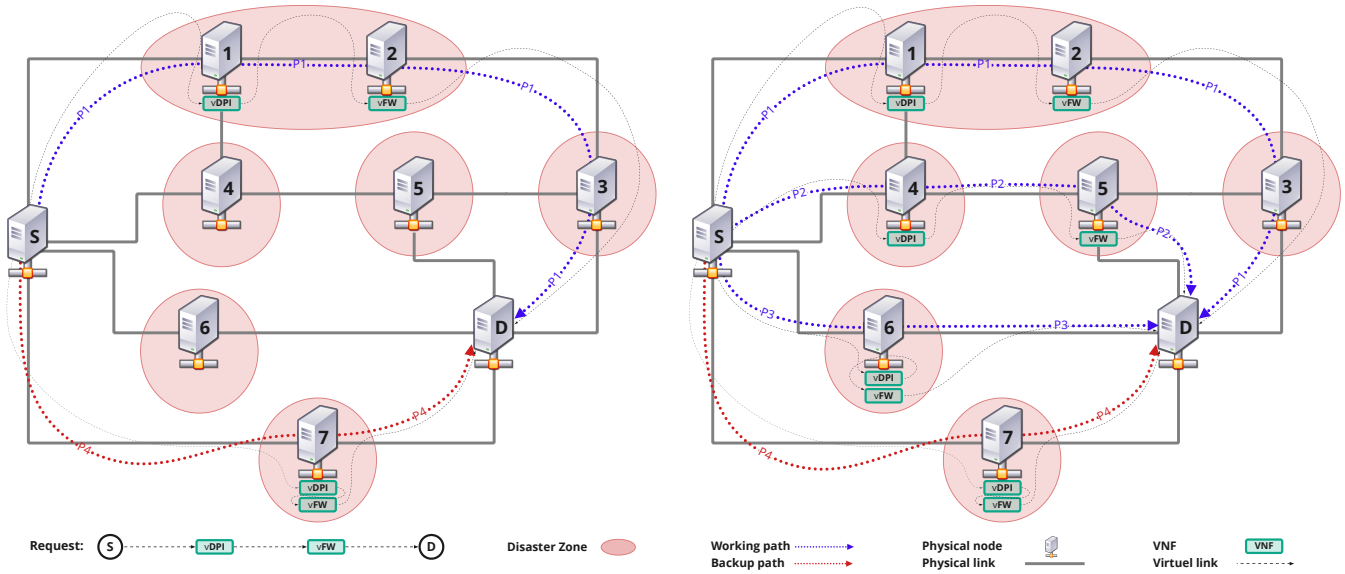
In our study, networks are represented as a connected directed graph $G = (V, A)$, where V is a set of N physical nodes $\{v_1, v_2, \cdots, v_N\}$, A is a set of physical arcs, and $uv \in A$ represents one specific arc from node u to node v. The set of disaster zones (DZs) is denoted by $Z = \{z_1, z_2, \cdots z_q\}$. Each DZ contains the set of nodes and arcs that are potentially affected by a single disaster. For each node $v_i \in V$, $c(v_i)$ is the total processing capacity, and $z(v_i)$ are the associated DZs. For each arc $uv \in A$, $b(uv)$ is the bandwidth capacity and $z(uv)$ are the associated DZs. The set of processed l SFC requests is $R = \{r_1, r_2, \cdots, r_l\}$. An SFC request $r \in R$ with a single replica of each VNF and a single virtual link between consecutive VNFs is typically represented as $r = \{s^r, f_1^r, f_2^r, \cdots, f_m^r, d^r\}$, with $F^r = \{f_1^r, f_2^r, \cdots, f_m^r\}$ as the set of m required VNFs, s^r as the source node, and d^r as the destination node of the request. The virtual links are represented as $\{e_1^r, e_2^r, \cdots, e_{m+1}^r\}$, where $e_i^r = (f_{i-1}^r, f_i^r)$ connects two consecutive VNFs, $e_1^r = (s^r, f_1^r)$ and $e_{m+1}^r = (f_m^r, d^r)$ connect the source and destination nodes, respectively. A virtual link can be associated with a single physical link, or can extend across multiple links and nodes to interconnect the VNFs. The traffic flow might change after passing through a VNF. To measure and represent the traffic change of VNF f_i^r, we use $var_{flow}(f_i^r) = \frac{forwarding\_data\_rate}{initial\_data\_rate}$. For example, the data rate could increase by 200% after passing through f_1^r before arriving at f_2^r. However, we assume $var_{flow} = 1$ for all VNFs, as a common assumption in most of the literature [26] [27]. For each VNF replica, the demanded processing capacity, denoted as $cpu(f_i^r)$, is determined by four factors [21]: the initial traffic data rate Δ^r, a coefficient $\sigma_{f_i^r}$ representing the amount of processing capacity required per unit of bandwidth for a specific VNF f_i^r, the traffic change $var_{flow}(f_i^r)$, and the path splitting number k^r when using multipath routing. Hence, the processing capacity is $cpu(f_i^r) = \frac{\sigma_{f_i^r} \cdot \Delta^r}{k^r - 1} \times var_{flow}(f_i^r)$.

TABLE I
Network Sets and Parameters

$G(V, A)$	Network with node set V and arc set A.
R	Set of requests $r(s^r, z_s^r, d^r, z_d^r, k^r, F^r)$, where s^r, z_s^r, d^r, z_d^r, k^r and F^r are source node and its DZ, destination node and its DZ, predefined maximum number of DZ-disjoint paths, and the required VNF set.
Δ^r	Initial traffic data rate for request r from s^r.
T^r	$T^r = \{1, 2, 3, \cdots, k^r\}$, index set of paths and VNF replicas for request r.
p_t^r	t-th path of request r, and $t \in T^r$.
f_i^r	i-th VNF required by SFC request r.
f_{it}^r	t-th replica of VNF f_i^r, and $t \in T^r$.
e_i^r	Virtual link from f_i^r to f_{i+1}^r.
$z \in Z$	DZ/set of DZs. Each z contains a set of arcs and nodes.
z_s^r	Disaster zone for source node s^r. Note that z_s^r is 0 if source node is outside of any DZ.
z_d^r	Disaster zone where destination node d^r is located at. Note that z_d^r is 0 if destination node is outside any DZ.
N_v^+ / N_v^-	Set of outgoing/incoming arcs from node $v \in V$.
$K_{f_i^r}$	Maximum number of replicas for VNF f_i^r in the network G.
$\sigma_{f_i^r}$	Coefficient related to processing capacity per bandwidth unit for VNF replica f_i^r.
θ	Weighting parameter to adjust cost combination.
c_{uv}	Maximum available bandwidth for arc uv.
c_v	Maximum available processing capacity for node v.
w_v	Maximum VNF installation limit on node v.
S	Set of incompatible VNF pairs.

B. Multi-Path based Disaster Protection Strategy (MP) for SFC

To address the issue of protecting network infrastructures and services from the impacts of potential disasters, our main objective is to minimize the total bandwidth usage and processing cost of VNFs while guaranteeing protection for all SFC requests. Dedicated Protection (DP) is the well-known strategy used for addressing the problem of link or path failures in network infrastructures and services. The concept of DP involves constructing a pair of links -or nodes- disjoint paths for each SFC request, one primary working path and one backup protection path, that visit all the required VNFs in a predefined order. In normal conditions, only the primary working path is used to route the SFC request, while the same bandwidth should also be reserved in advance on the



(a) Disaster Dedicated Protection (DP)

(b) Disaster Multi-path Protection (MP)

Fig. 1. SFC Disaster Protection

dedicated backup path. In the context of protecting against disaster failures, the two paths should be DZ-disjoint such that the SFC request can be switched to the reserved backup path instantly once the working path is affected by a failure, ensuring that at least one path is available in case of any single DZ failure. However, DP strategy is known to be resource-intensive. The same amount of resources as required by the SFC request is reserved for use in case of disaster failure, and it will only be used in such situations. Thus, it is critical to investigate other effective strategies to ensure protection while minimizing resource waste. We set aside some trivial cases, such as when a failed DZ contains the source or destination node of an SFC request or when the working path does not cross any DZ. We did not consider these trivial situations in our study because they do not require implementing disaster protection. We only focus on scenarios where disaster protection is necessary. Moreover, in some specific use cases the VNF does not support traffic splitting thus preventing the request from utilizing multipath routing. To take into consideration this specific scenario, the solution is to set $k^r = 2$ to ensure traditional protection as DP with a working path and a backup path.

The concept of multi-path routing constitutes an interesting and relevant solution, as it gives the ability to distribute network traffic evenly across multiple working paths. Inspired by this fact, we propose a multi-path based disaster protection strategy (MP), which provisions an SFC request with multiple DZ-disjoint working paths plus one shared backup path. This approach ensures minimal impact in case of a DZ failure. As the working paths are DZ-disjoint, they do not share any common zone of failure. In case of a DZ failure, only one working path is affected, and can be rapidly switched to the backup path. Adopting this MP strategy not only leads to a more effective protection solution in terms of bandwidth reservation on the backup path, as it reduces by at least 50% of the typical bandwidth required by the classical DP strategy. Similarly, this also results in the same amount of reduction of the VNF processing cost for the nodes of the backup path. Fig. 1 presents an illustration of the MP protection concept. Let us take an example of an SFC request with initial bandwidth demand of Δ^r that requires two VNFs (vDPI and vFirewall). As shown in Fig. 1 (a), The DP scheme provides two paths, P1 and P4(BP), that traverse all the required VNFs in the specified order, with P1 serving as the primary path (in blue) and P4 as the backup path (in red). To ensure seamless disaster recovery, the same bandwidth is reserved on both the primary and backup paths, resulting in a total bandwidth usage of $2\Delta^r$. It is clear that the two paths should not cross the same DZ (colored oval zones in Fig. 1).

Different from the DP, the MP approach in Fig. 1 (b) uses three DZ-disjoint paths (P1, P2, and P4(BP)) for the SFC request. Each SFC request goes through all the required VNFs in the specified order. The paths P1 and P2 function as the working paths, while P4 serves as the backup path. By distributing the SFC traffic load across the two working paths, each one carries $\frac{1}{2}\Delta^r$ bandwidth. For protection, the reservation on the backup path is reduced to $\frac{1}{2}\Delta^r$, leading to saving a half of the backup bandwidth compared to the traditional DP scheme. More paths result in greater backup bandwidth savings, because only one of the working paths will be affected and should be instantly switched to the backup path in case of a DZ failure. The same reduction of processing costs can be achieved for the required VNFs.

The resource consumption between the two strategies is outlined in Table II. In DP, 6 links are used (4 for the working path and 2 for the backup path), each one with a data rate of 1 unit per path, and 4 units of CPU are utilized (2 VNFs for the working path and 2 for the backup path). In MP, 4.5 represents the bandwidth utilization for the three paths, with a data rate of $\frac{1}{2}$ and 9 used links, while CPU utilization is 3

(2 VNFs per path $\times$ 3 paths $\times$ $\frac{1}{2}$ data rate). For four paths, $\frac{11}{3}$ denotes the bandwidth utilization, with a data rate of $\frac{1}{3}$ and 11 used links, and CPU utilization is $\frac{8}{3}$ (2 VNFs per path $\times$ 4 paths $\times$ $\frac{1}{3}$ data rate). This example shows a 25% savings in both total bandwidth and CPU processing usage compared to DP. Furthermore, when the number of working paths is increased to 3 (P1, P2, P3, and P4(BP)), with $\frac{1}{3}\Delta^r$ bandwidth, the new strategy saves 40% in total bandwidth and 34% in CPU processing, highlighting the superiority of MP in terms of resource optimization over the traditional approach. However, using more paths also impacts other costs due to the need for additional VNF replicas, physical nodes, and arcs.

TABLE II
DP & MP RESOURCE CONSUMPTION

	Paths	Data Rate per Path	Links	Bandwidth	VNFs	CPU
DP	2	1	4+2	6	4	4
MP	3	1/2	4+3+2	9/2	6	3
	4	1/3	4+3+2+2	11/3	8	8/3

There is a trade-off between the number of paths used and the operational cost, as shown in Fig. 2, which includes additional costs such as VNF storage and instantiation, and data fragmentation/merge cost etc. More paths require more VNFs to be instantiated and lead to greater data fragmentation/merge, but the bandwidth and CPU processing needs are reduced. Conversely, less paths require less VNFs and thus less data fragmentation/merge cost, but result in higher bandwidth and CPU processing demands. Therefore, while increasing the number of paths can enhance load distribution and disaster resilience, it is essential to find an optimal balance that minimizes the operational cost without compromising network performance and reliability. The optimal number of paths depends on the network topology and the SFC requests. Moreover, in some situations, it is not possible to generate multiple DZ-disjoint routing paths for all source-destination pairs. Also, the number of paths varies based on network configurations and requests. So, it is necessary to define a maximum number of paths for each request. This leads to seeking for the maximum number of paths (starting from a minimum of two paths) without exceeding the predefined upper limit k^r to ensure the provisioning, protection, and resource optimization.

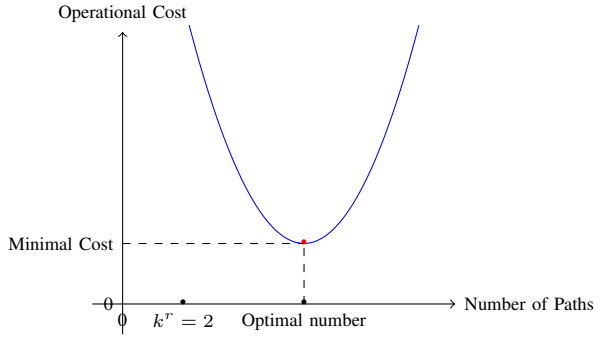


Fig. 2. The Relationship Between the Number of Paths and Operational Cost

C. Problem Statement

We consider a network $G(V, A)$, a set of DZs Z each involving a set of nodes and arcs, and a set of SFCs requests $r \in R$ with a specified bandwidth demand Δ^r and an ordered sequence of VNFs F^r. Given this, the studied problem, namely **Disaster-Resilient SFC MP**, entails determining the optimal placement of VNFs on the physical nodes and implementing efficient multi-path routing and protection for SFCs. We assume a single DZ failure at a time, thus this routing must ensure that the paths are DZ-disjoint to provide disaster protection. The objective is to minimize the total network resource consumption, which encompasses both the bandwidth utilized by the routing paths and the computational resources required for the execution of VNFs.

The Disaster-Resilient SFC MP problem is a variant of the SFC Embedding (SFCE) problem [28], with the integration of supplementary constraints including multipath and DZ-disjoint constraints. Our problem can thus be reduced to the SFCE problem, which is NP-hard [22]. Since the execution of VNFs in SFC follows a specific order, the SFCE problem is equivalent to the traditional Virtual Network Embedding (VNE) problem, which is proved NP-hard [23].

IV. PROPOSED SOLUTIONS

We present practical solutions that are applicable in real-world scenarios compared to the existing ones. To validate our problem modeling, we propose a novel and adaptive ILP model that provides the optimal solutions. Furthermore, we propose new heuristics for the MP that give near-optimal solutions, in terms of solution quality and computation efficiency.

A. Optimal Solution: Adaptive ILP

In this section, we present a mathematical formulation of the multi-faceted optimization problem for the disaster protection of SFC, combining the VNFs placement, SFC routing, and protection. This problem is known to be NP-hard, and becomes even more complex when multiple paths are introduced. In [21] an ILP formulation was proposed, nevertheless, it requires a predefined and fixed number of paths for each request (which is hard in real-world dynamic scenarios). However, we develop a new formulation that addresses this issue and enhances the model's flexibility. In our adaptive ILP, we define only an upper limit for the number of paths that can be used, rather than a fixed number. This requires to introduce new constraints with linearizations. Tables I & III contain the network parameters and ILP variables.

1) Objective Function: The goal of introducing multi-path routing for SFC disaster protection is to reduce the total bandwidth and processing cost. We define θ as an adjustable weighting parameter that can be determined by network operators. Therefore, the objective function for our multi-path disaster protection problem can be expressed as follows:

$$\min \quad \sum_{r \in R} \left[B(r) + \theta \cdot C(r) \right] \tag{1}$$

TABLE III
VARIABLES IN ILP FORMULATIONS

$\alpha_z^{p_t^r} \in \{0,1\}$	Equals 1 if path p_t^r of request r crosses DZ z, otherwise 0.
$\beta_{f_{it}^r v}^{p_t^r} \in \{0,1\}$	Equals 1 if the t-th replica of f_i^r on node v is used on the working/backup path p_t^r , otherwise 0.
$\gamma_v^{f_{it}^r} \in \{0,1\}$	Equals 1 if the t-th replica of f_i^r exists on node v, otherwise 0.
$\xi_{uv}^{p_t^r f_i^r} \in \{0,1\}$	Equals 1 if arc (u,v) is used on the working/backup path p_t^r from s^r to the node storing f_i^r, otherwise 0.
$\xi_{uv}^{p_t^r} \in \{0,1\}$	Equals 1 if arc (u,v) is used on the working/backup path p_t^r, otherwise 0.
$m_h^r \in \{0,1\}$	Equals 1 if the number of paths is h $(2 \le h \le k^r)$ for request r, otherwise 0.
$\lambda_t^r \in \{0,1\}$	Equals 1 if path t is used for request r, otherwise 0.
$W_{uv}^{p_t^r h} \in \{0,1\}$	Auxiliary variables: $W_{uv}^{p_t^r h} := \xi_{uv}^{p_t^r} \cdot m_h^r$
$Z_{f_{it}^r v}^{p_t^r h} \in \{0,1\}$	Auxiliary variables: $Z_{f_{it}^r v}^{p_t^r h} := \beta_{f_{it}^r v}^{p_t^r} \cdot m_h^r$

The first term in (1) represents the total bandwidth usage of all arcs for all SFC requests

$$B(r) = \sum_{t \in T^r} \sum_{uv \in A} \sum_{h=2}^{k^r} W_{uv}^{p_t^r h} \frac{\Delta^r}{h-1} \tag{2}$$

The second term in (1) represents the total processing cost for VNF executions, and it is expressed as follows

$$C(r) = \sum_{v \in V} \sum_{f_i^r \in F^r} \sum_{t \in T^r} \sum_{h=2}^{k^r} Z_{f_{it}^r v}^{p_t^r h} \frac{\sigma_{f_i^r} \Delta^r}{h-1} \tag{3}$$

Let define maxB $= 2(|V|-1) \times \sum_{r \in R} \Delta^r$ and maxC $= 2 \times \sum_{r \in R} \sum_{f \in F^r} \Delta^r \times \sigma_f$, we distinguish three scenarios for the objective function: the Bandwidth-dominant scenario, where $\theta \ll \frac{1}{\text{maxC}}$; the CPU-dominant scenario, where $\theta \gg$ maxB; and a trade-off case, where $\frac{1}{\text{maxC}} < \theta <$ maxB.

In order to fully provision and protect SFCs, our ILP model must satisfy constraints (4)-(25), that are presented and explained in the following subsection.

2) Constraints:

- Paths constraints

$$\sum_{h=2}^{k^r} m_h^r \cdot h = \sum_{t \in T^r} \lambda_t^r, \qquad \forall r \in R \tag{4}$$

$$\sum_{h=2}^{k^r} m_h^r = 1 \qquad \forall r \in R \tag{5}$$

$$\lambda_t^r \ge \lambda_{t+1}^r \qquad \forall r \in R, \forall t \in [1, k^r - 1] \tag{6}$$

Constraint (4) guarantees that the total number of used paths equals the number of selected paths. (5) ensures that only one specific number of paths is selected from the range between 2 and the maximum number of paths k^r. Constraint (6) ensures that the paths are explored in a sequential order.

- VNF set constraints

$$\sum_{t \in T^r} \lambda_t^r \le \sum_{v \in V} \sum_{t \in T^r} \gamma_v^{f_{it}^r} \le K_{f_i^r}, \quad \forall r \in R, \forall f_i^r \in F^r \tag{7}$$

Constraint (7) sets the lower and upper bounds for the number of VNF replicas f_{it}^r. The number of replicas must be at least as large as the total number of used paths to ensure that each path can be routed through at least one replica of VNF f_i^r. However, the number of replicas should not exceed capacity.

- VNF allocation

$$\beta_{f_{it}^r v}^{p_t^r} \ge \gamma_v^{f_{it}^r} + \sum_{u \in N_v^-} \xi_{uv}^{p_t^r} - 1, \qquad \forall r \in R, \forall v \notin s^r, \quad \forall t \in T^r, \forall f_i^r \in F^r \tag{8}$$

$$\beta_{f_{it}^r v}^{p_t^r} \le \gamma_v^{f_{it}^r}, \quad \forall r \in R, \forall v \in V, \forall t \in T^r, \forall f_i^r \in F^r \tag{9}$$

$$\sum_{v \in V} \gamma_v^{f_{it}^r} \le \lambda_t^r, \qquad \forall r \in R, \forall f_i^r \in F^r, \forall t \in T^r \tag{10}$$

Constraints (8)-(9) determine the location of the i-th required VNF replica f_{it}^r on the working/backup path. Constraint (10) ensures that for a required i-th VNF, the number of allocated replicas f_{it}^r does not exceed the number of used paths.

- Incompatibility constraints

$$\gamma_v^{f_{it}^r} + \gamma_v^{f_{i't'}^{r'}} \le 1, \qquad \forall v \in V, \forall t \in T^r, \forall t' \in T^{r'} | (f_{it}^r, f_{i't'}^{r'}) \in S \tag{11}$$

Constraint (11) ensures that two VNFs, f_{it}^r and $f_{i't'}^{r'}$, are not compatible, and cannot be instantiated on the same node.

- Capacity constraints

$$\sum_{r \in R} \sum_{f_i^r \in F^r} \sum_{t \in T^r} \beta_{f_{it}^r v}^{p_t^r} \le w_v, \qquad \forall v \in V \tag{12}$$

$$\sum_{r \in R} \sum_{f_i^r \in F^r} \sum_{t \in T^r} \sum_{h=2}^{k^r} Z_{f_{it}^r v}^{p_t^r h} \frac{\sigma_{f_i^r} \Delta^r}{h-1} \le c_v, \qquad \forall v \in V \tag{13}$$

$$Z_{f_{it}^r v}^{p_t^r h} \ge \beta_{f_{it}^r v}^{p_t^r} + m_h^r - 1 \quad \forall r \in R, \forall f_i^r \in F^r, \forall t \in T^r, \forall h \in [2, k^r] \tag{14}$$

$$Z_{f_{it}^r v}^{p_t^r h} \le \frac{1}{2}(\beta_{f_{it}^r v}^{p_t^r} + m_h^r) \quad \forall r \in R, \forall f_i^r \in F^r, \forall t \in T^r, \forall h \in [2, k^r] \tag{15}$$

$$\sum_{r \in R} \sum_{t \in T^r} \sum_{h=2}^{k^r} \frac{\Delta^r}{h-1} W_{uv}^{p_t^r h} \le c_{uv}, \qquad \forall uv \in A \tag{16}$$

$$W_{uv}^{p_t^r h} \ge \xi_{uv}^{p_t^r} + m_h^r - 1 \qquad \forall r \in R, \forall t \in T^r, \forall h \in [2, k^r], \forall uv \in A \tag{17}$$

$$W_{uv}^{p_t^r h} \le \frac{1}{2}(\xi_{uv}^{p_t^r} + m_h^r) \quad \forall r, \forall t \in T^r, \forall h \in [2, k^r], \forall uv \tag{18}$$

(12) represents the maximum capacity for VNF replicas on the node v . (13) ensures that the node's processing capacity is compliant with all instantiated VNFs. (14) and (15) are linearization constraints. The former ensures that $Z_{f_{it}^r v}^{p_t^r h}$ equals zero if either $\beta_{f_{it}^r v}^{p_t^r}$ or m_h^r is zero. The latter will verify that $Z_{f_{it}^r v}^{p_t^r h}$ equals 1 if both binary variables are set to 1. Constraint (16) ensures that the bandwidth requirement for an arc remains

under the physical bandwidth capacity of the arc. (17) and (18) also represent linearization constraints.

- Flow-conservation constraints

$$\sum_{u\in N_v^+} \xi_{vu}^{p_t^r f_i^r} - \sum_{u\in N_v^-} \xi_{uv}^{p_t^r f_i^r} = \begin{cases} \lambda_t^r, & v = s^r \\ -\beta_{f_{it}^r v}^{p_t^r}, & v \neq s^r, \forall r \in R, \\ & \forall t \in T^t, \\ & \forall f_i^r \in F^r, \forall uv \end{cases} \tag{19}$$

$$\sum_{u\in N_v^+} \xi_{vu}^{p_t^r} - \sum_{u\in N_v^-} \xi_{uv}^{p_t^r} = \begin{cases} \lambda_t^r, & v = s^r \\ -\lambda_t^r, & v = d^r \quad \forall r \in R, \forall t \in T^r, \forall uv \\ 0, & \text{otherwise} \end{cases} \tag{20}$$

$$\xi_{uv}^{p_t^r f_i^r} \leq \xi_{uv}^{p_t^r f_{(i+1)}^r} \leq \xi_{uv}^{p_t^r}, \qquad \forall r \in R, \forall t \in T^r, \forall uv, \quad \forall f_{(i+1)}^r \in F^r, |F^r| \geq 2 \tag{21}$$

$$\xi_{uv}^{p_t^r f_1^r} \leq \xi_{uv}^{p_t^r}, \qquad \forall r, \forall t \in T^r, \forall uv, \forall f_1^r \in F^r, \ |F^r| = 1 \tag{22}$$

Constraint (19) generates working/backup paths from the source node s^r to the node hosting the VNF replica f_{it}^r. Note that the t-th VNF replica corresponds to the path p_t^r to avoid mixing different paths and replicas. Constraint (20) generates working/backup paths from the source node s^r to the destination node d^r. Constraint (21) specifies the sequence order of VNFs if the number of required VNFs is $|F^r| \geq 2$. If $|F^r| = 1$, constraint (22) ensures that the path from s^r to VNF f_1^r is included in the working/backup path. Fig. 3 illustrates the concatenation of sub-paths from the source to the nodes hosting the VNFs. Each sub-path is included sequentially in the subsequent sub-paths, forming a complete path from the source to the destination, that traverses the VNFs in a sequential order. We prove it by the following Lemma.

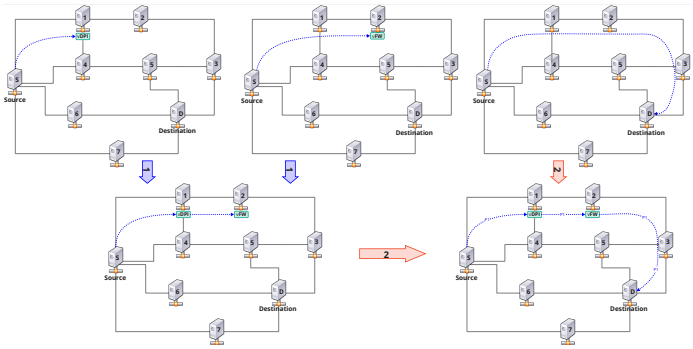


Fig. 3. Flow-conservation constraints explanation

Lemma: Given an SFC request $r = \{s^r, f_1^r, f_2^r, \cdots, f_m^r, d^r\}$, $[m] = \{1, 2, \ldots, m\}$, let P_i be the path from s^r to the node hosting f_i^r for all $\forall i \in [m]$, and P_{m+1} be the path from s^r to d^r. If $\forall i \in [m], P_i \subseteq P_{i+1}$, then P_{m+1} traverses all the VNFs of F^r in the given order.

Proof: We make the proof by contradiction and assume that P_{m+1} is not the path that traverses F^r in the given order. As $\forall i \in [m], P_i \subseteq P_{i+1}$, the node hosting f_i^r in P_i must also be included in P_{i+1}. Hence, we can construct a set of segments $\{S_i : i \in [m]\}$ as follows: S_1 is the path from s^r to the node hosting f_1^r in P_1; $S_{i+1} : 1 \leq i < m$ is the segment from the node hosting f_i^r to the node hosting f_{i+1}^r in P_{i+1}; and finally S_{m+1} is the segment from the node hosting f_m^r to d^r in P_{m+1}. Indeed, the union of these segments, $\cup_{i\in[m+1]} S_i$, form a continuous path from s^r to d^r that ensures the VNFs F^r are traversed in the correct order. Since $\forall i \in [m+1], S_i \subseteq P_i \subseteq P_{m+1}$, we have $\cup_{i\in[m+1]} S_i \subseteq P_{m+1}$. Consequently, P_{m+1} contains the path formed by the segment union, which crosses F^r in the given order. This contradicts with our initial assumption, and thus the proof follows.

- DZ-disjoint constraints

$$\alpha_z^{p_t^r} \leq \sum_{uv\in z} \xi_{uv}^{p_t^r}, \quad \forall r \in R, \forall z \in Z, \forall t \in T^r \tag{23}$$

$$\alpha_z^{p_t^r} \geq \xi_{uv}^{p_t^r}, \quad \forall r \in R, \forall z \in Z, \forall uv \in z, \forall t \in T^r \tag{24}$$

$$\sum_{t\in T^r} \alpha_z^{p_t^r} \leq 1, \quad \forall r \in R, \forall z \in Z \backslash \{z_s^r, z_d^r\} \tag{25}$$

Constraints (23)-(24) are used to define the Disaster Zone for the working or backup path. Constraint (25) ensures that paths are DZ-disjoint (each DZ affects only one path of the same SFC request r).

B. Time-efficient Solutions : Heuristics

The problem we address is a complex NP-hard problem. While the proposed ILP model is able to provide the optimal solution, it cannot be applied to real-world scenarios where a large number of requests need to be processed in large networks within a limited time. Therefore, we propose heuristics that provide practical, near-optimal solutions with high scalability. These heuristics address the problem efficiently while maintaining a high level of accuracy.

*1) **Divide-and-Conquer Based Joint Optimization Heuristic**:* We first propose a Divide-and-Conquer Based heuristic (namely **DCBJOH**) and give its flowchart in Figure 4. The DCBJOH innovatively integrates routing, protection, and VNF placement into a single joint optimization framework, which allows for simultaneous optimization and is thus particularly effective for disaster-resilient SFC deployment. This approach consists of two main steps: (1) find DZ-disjoint multipath for routing SFC requests and (2) place VNFs on specific nodes along the determined routing paths by considering the sequence order of the VNFs for each request. The proposed heuristic aims to support various network topologies and configurations, including intersections of DZs or nodes outside any DZ. The first step of DCBJOH prioritizes and processes the routing of the SFC requests. We process the requests in a sequential order. Based on a reduced graph (DZ-Graph), all nodes of a DZ are concatenated into a single vertex, i.e., each node of DZ-Graph represents a DZ. This approach allows the extraction of all DZ-paths that are DZ-disjoint. For a request r, for the DZ-Graph, we explore the maximum number of DZ-paths without exceeding k^r. These DZ-paths are obtained by computing the shortest path between the source DZ (z_s^r) and the destination DZ (z_d^r). Once this shortest path is found, all the traversed DZs are removed, except z_s^r and z_d^r, before exploring the next DZ-path. Thus, each DZ-path consists of a subgraph that contains the source (s^r) and destination (d^r). The working paths are selected only from the shortest path from s^r to d^r in each DZ-path. This ensures that the selected

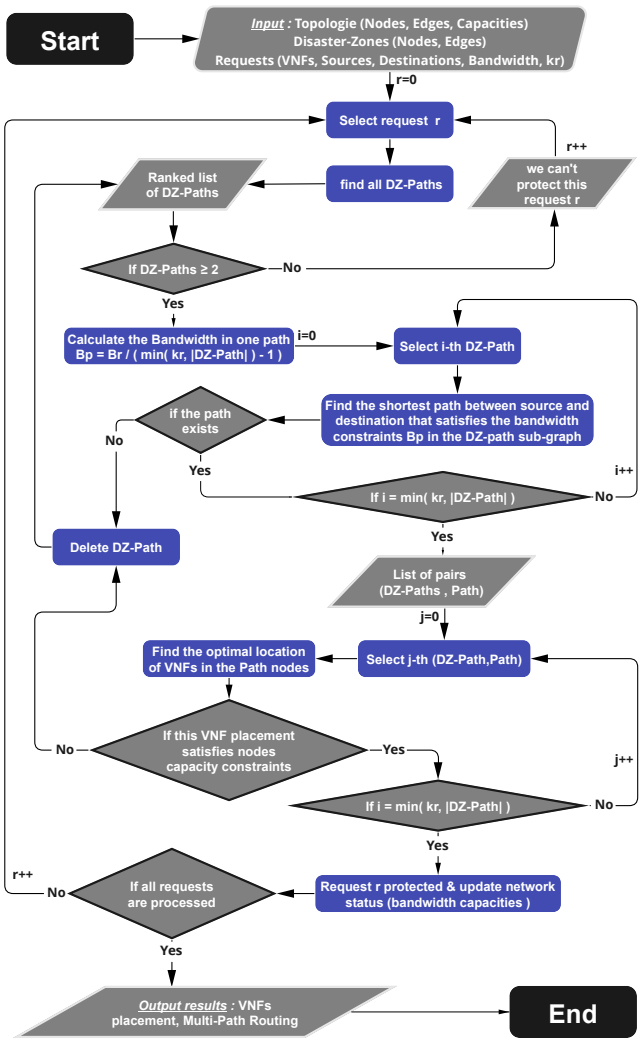


Fig. 4. DCBJOH Flowchart

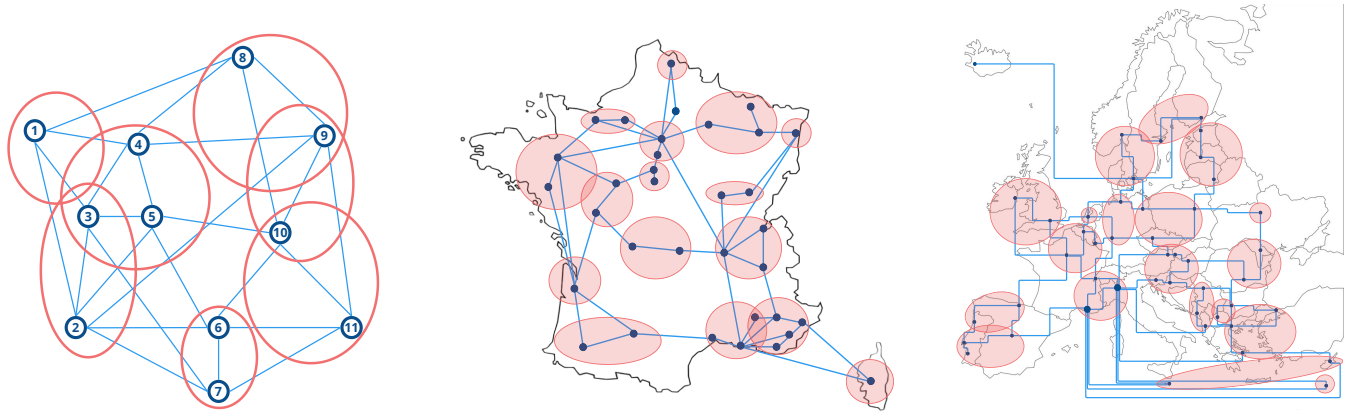
Algorithm 1: DCBJOH

```
Input : G (V, A, DZs)  /*Graph (nodes, arcs, DZs)*/
        DZ Graph  /* Graph concatenates the nodes of a DZ into a single vertex */
        R={r(s^r, d^r, F^r, Δ^r, k^r)}  /*Requests Set*/
Output: VNFs placement, Multi-Path DZ-disjoint path routing and protection
1  forall r ∈ R do
2      G'= DZ Graph ; DZ-Paths ⟵ Ø ;
3      while ∃ path(s^r, d^r) ∈ G'  /* path(s^r, d^r) : Path between source and destination*/ do
4          if p_c ∉ DZ-Paths  /* p_c : the shortest path(s^r, d^r) in G' */ then
5              DZ-Paths ⟵ DZ-Paths ∪ p_c ;
6              G' ⟵ G' ∪ {DZ(s^r), DZ(d^r)}\{p_c ∩ DZs} ;
7      Finish ⟵ False ;
8      while | DZ-Paths | ≥ 2 and !Finish do
9          Rank(DZ-Paths) ; Paths ⟵ Ø ;
10         if | DZ–Paths | > k^r then
11             DZ–Paths' ⟵ DZ–Paths[1 : k^r] ;
12             B_p = Δ^r / (k^r − 1) ;  /*Calculate the Bandwidth in one path*/
13         else
14             DZ–Paths' ⟵ DZ–Paths ;
15             B_p = Δ^r / (|DZ−Paths'|−1) ;
16         forall P_DZ ∈ DZ-Paths' do
17             G'' = G(V(P_DZ), E(P_DZ));  /*Extract a sub-graph G'' from G contain all nodes and edges of DZs of P_DZ */
18             if ∃ path(s^r, d^r) ∈ G'' where ∀e ∈ path(s^r, d^r), c(e) ≥ B_p then
19                 Paths ⟵ Paths ∪ p_s ;  /* p_s : the shortest path(s^r, d^r) where ∀e ∈ p_s, c(e) ≥ B_p */
20                 Temporary updates arcs capacities ;
21             else
22                 DZ-Path ⟵ DZ-Path\{P_DZ} ;
23                 Cancel temporary updates ;
24                 Go to (line 8) ;
25         forall P_DZ ∈ DZ-Paths' do
26             if Find_optimal_placement(F^r, V(Path) ); /*Function to assign VNFs in nodes of Path*/ then
27                 Temporary updates nodes capacities ;
28             else
29                 DZ-Path ⟵ DZ-Path\{P_DZ} ;
30                 Cancel temporary updates ;
31                 Go to (line 8) ;
32         Finish ⟵ True
33     if Finish then
34         Validate updates ; Accept the protection of request r ;
35     else
36         Ignore the protection of request r ;
```

working paths are DZ-disjoint (do not share the same DZs). In a second step, the placement of the VNFs on the determined paths is solved as an assignment problem using an ILP model (a typical SFC has a maximum limit of 15 VNFs [23]). A loop is defined until all SFC requests are processed.

Algorithm 1 shows the detailed procedure of DCBJOH algorithm, which handles requests iteratively one at a time. For a request r, lines 2–6 determine the set of DZ-paths by providing the shortest path between z_s^r and z_d^r. To satisfy the DZ-disjoint constraint, the DZs traversed in the previous iteration are removed by line 6. As long as the number of DZ-paths is no less than two, line 9 sorts the DZ-paths by hops, and lines 10–15 determine the path bandwidth. Lines 10–12 address situations when the number of DZ-paths exceeds its upper bound k^r, while lines 13–15 address the opposite situations. Lines 16–24 generate the working-backup paths based on the DZ-paths (subgraphs containing s^r and d^r). For each DZ-path, if there is a shortest path from s^r to d^r, it becomes a working-backup path (line 18), and the capacities of the corresponding edges are updated (line 20). If there is no path from s^r to d^r (line 21), the DZ-path is removed, and temporary updates are cancelled in lines 23. In this case, the process then restarts from line 8. After generating the working-backup paths in the previous step, the $Find\_optimal\_placement$ function is called in line 26. This function takes the path nodes and VNFs of request r as input to determine the optimal VNF assignment on the nodes along the path. If there is a possible assignment, we update node capacities accordingly (line 27). Otherwise, we delete the DZ-path, cancel temporary updates (lines 29, 30), and then go to line 8 to restart the process. Lines 33–36 verify the completion of the working-backup paths and the placement of the VNFs within the nodes. If true, the updates and the request protection are validated. Otherwise, the request protection is denied.

The DCBJOH algorithm's complexity can be dissected into three distinct parts. The first part, i.e., lines 1-6, is dedicated



(a) Cost239 topology (b) Renater topology (c) Geant topology

Fig. 5. Network Topologies for Simulations

to finding DZ-Paths, with a worst-case scenario complexity for the shortest path algorithm as $O(|V|^2)$. The complexity for this part scales to $O(|R| \cdot K \cdot |V|^2)$. The next part, i.e., lines 7-24, focuses on generating the working/backup paths, which employ the shortest path algorithm once again, leading to a complexity of $O(|R| \cdot K^2 \cdot |V|^2)$. The final part of the algorithm, i.e., lines 25-31, is responsible for the placement of VNFs on the nodes of the generated paths. The complexity for this portion is defined as $O(|R| \cdot K^2 \cdot F)$. Collectively, DCBJOH's time complexity is $O(|R| \cdot (K^2 \cdot |V|^2 + K \cdot |V|^2 + K^2 \cdot F))$. It is important to note that this complexity is for the worst-case scenario and does not reflect the typical time complexity of the algorithm from a practical point of view. As observed in practice, DCBJOH tends to run much faster than this theoretical upper bound.

*2) **Two-Stage Optimization Heuristic (TSOH)**:* TSOH differs from DCBJOH in that it reverses the sequence of steps, starting by placing VNFs on physical nodes and then routing SFC requests through DZ-disjoint paths. First, for the placement step, the algorithm estimates the total number of replicas of each VNF type from the total requests. Then, VNFs placement is explored one by one. TSOH computes a weight for each node based on four parameters: the available capacity in the node, the availability of the VNF type in the node, the availability of the VNF type in the DZ, and finally the distance between the node and the source-destination pair. These weights are used to calculate a non-uniform probability distribution for the placement of the VNFs, taking into account the different weights of nodes. The weights are updated dynamically following each VNF placement, leading to a distribution of the VNFs that satisfies the constraints. Second, for the routing step, the shortest path algorithm (Dijkstra's) is used to get the most efficient route from the source to destination nodes, ensuring the DZ-disjoint multi-paths routing and the VNF sequence order. The process is repeated to get the maximum number of paths k^r for each request.

The TSOH algorithm operates in two main stages: VNF Placement and Path Routing, as outlined in **Algorithm 2**.

Algorithm 2: TSOH

Input : G (V, A, DZs) /*Graph (nodes, arcs, DZs)*/
DZ Graph /* Graph concatenates the nodes of a DZ into a single vertex */
R={$r(s^r, d^r, F^r, \Delta^r, k^r)$} /*Requests Set*/
$\mathbb{F} = \bigcup_{r \in R} F^r$ /*Set of VNFs of all requests*/
Output: VNFs placement, Multi-Path DZ-disjoint path routing and protection

1 Stage 1: VNF Placement **forall** *VNF* f *in* $\mathbb{F}$ **do**
2 Compute weight for each node v in V based on:
3 Available capacity of node v ;
4 Availability of VNF type f on node v ;
5 Availability of VNF type f in the DZ assoicated to v ;
6 Distance between node v and (s^r, d^r) ;
7 Calculate non-uniform probability distribution for placement of VNF f ;
8 Place VNF f on node v based on the computed probability ;
9 Update weights dynamically after each placement ;
10 Update nodes capacities ;
11 Stage 2: Path Routing **forall** $r \in R$ **do**
12 Initialize empty set of paths P^r for request r ;
13 **while** *number of paths* $\leq k^r$ **do**
14 Use Dijkstra's algorithm to find the shortest path p from s^r to d^r ensuring the VNF sequence order ;
15 Add the computed path to the set of paths P^r ;
16 Delete the DZs crossed by p ;
17 Update links capacities ;

Stage 1: VNF Placement (lines 1-10): For each VNF f in the set F of all VNFs (line 1), the algorithm computes a weight for each node v based on four factors: the available capacity of the node, the availability of the VNF type f in the node, the availability of the VNF type f within the node's DZ, and the distance between the node and the source-destination pair (lines 2-6). This weight calculation creates a non-uniform probability distribution for placing each VNF f (line 7). The VNF f is then placed on node v based on this computed probability (line 8), and the weights are updated dynamically after each placement to reflect the current network state (line 9). The capacities of the nodes are updated accordingly (line 10).

Stage 2: Path Routing (lines 11-17): For each request $r \in R$ (line 11), the algorithm initializes an empty set of paths P_r (line 12). It then iteratively finds paths using Dijkstra's algorithm (line 14) until the number of paths reaches the maximum k_r (lines 13-14). For each path found, the algorithm checks that the VNF sequence order is maintained and ensures that the path does not traverse the same DZ as other paths for the same request. The found path p is added to the set P_r (line

15), and the DZs crossed by p are deleted from consideration (line 16). Finally, the capacities of the links used in p are updated (line 17).

The placement part is based on the computation and dynamic update of nodes weights for each VNF placement. This will potentially lead to a time complexity of $O(|R|\cdot F\cdot K\cdot|V|)$. The routing part uses Dijkstra's algorithm (considering its worst-case scenario), which contributes to the overall time complexity of $O(|R|\cdot K\cdot|V|^2)$. Hence, the overall time complexity of TSOH is $O(|R|\cdot K\cdot(|V|^2+F\cdot|V|))$.

V. Numerical Results

We provide extensive simulations to evaluate the performance and effectiveness of the MP strategy. For this, we evaluate the ILP model and the heuristic approaches. First, we compared the efficiency of MP against DP using the ILP model. Then, we validate the effectiveness and time efficiency of the proposed heuristic approaches by comparing with the ILP model. We also evaluate the performance of the MP strategy for solving large-scale instances using the heuristics. We study the relationship between the network nodal degree and the gain obtained using the MP strategy. We conduct a deep analysis of the global effectiveness of the multipath strategy in diverse network settings, by varying the SFC size, the number of routing paths, and the parameter θ in the objective function. Finally, We studied the case without SFC protection, the impact of DZ failure, and the resources required to ensure protection.

A. Simulation Settings

The ILP model was implemented in C++ using CPLEX 22.01, and the heuristics were implemented in Python. The simulation was conducted on an AMD Ryzen 9 16-Core Processor PC with a 3.4 GHz CPU and 128G bytes of RAM. The simulation was performed on the network topologies in Fig. 5 : Cost-239 network [21], and two new topologies using the Renater and Geant networks [29]. We consider various disaster risks to extract the DZs in Renater and Geant networks, by mapping the French risks maps [30] and the European risks maps [31, 32] respectively.

TABLE IV
Network Characteristics

	Nodes	Edges	DZs	Average Nodal Degree
Cost-239 (EU)	11	52	7	4.72
Renater (FR)	34	50	16	2.94
Geant (EU)	46	68	19	2.95

For each request, the content and source/destination nodes are generated randomly, and the number of required network functions was also chosen randomly. The weight, θ, used in the objective function is determined by the network operator. We set θ to 0.1 to prioritize bandwidth optimization. The bandwidth capacity for each arc is 1000 Mbps, while node processing capacity is fixed to 1000 MIPS (typical values [33]). The initial bandwidth requirement for the request is set to 1 Mbps, but it may vary depending on the service type (ex: 20 Mbps for video streaming). The maximum number of VNF replicas for an SFC is set to be the same as maximum path splitting number, 4 in our evaluations, with a coefficient $\sigma_{f_i^r}=1$ for each VNF instance. The maximum VNF installation capacity is assumed to be 1000 in a single node. The backup path is selected randomly from the generated paths. The simulation parameters are based on existing works [21] [33] [34].

B. MP compared with DP (using ILP)

In order to compare the performance of the two protection strategies, we conduct simulations for Cost239 and Renater networks, with a number of requests ranging from 10 to 70, by solving the ILP model using CPLEX. We assume a scenario with 3 VNFs and an initial traffic data rate of $\Delta^r=1$ Mbps. As the number of requests and paths increases, the difficulty in finding the optimal solution also increases, because the ILP model becomes pretty hard and more complex to solve. For example, in case of 4 paths and 70 requests, using the ILP model to find the optimal solution takes 7000 seconds for the Renater topology and 14000 seconds for the Cost239 topology. Fig. 6 compares the Cost of the DP and MP strategies using ILP for Cost239 topologies. Besides, when the number of SFC requests increases, the results highlight the benefits of the MP strategy, leading to at least 20% resource savings.

When transitioning from DP (i.e. 2 paths) to MP with 3 paths, an important gain is observed, with 20% reduction for the total bandwidth and 19% reduction for the total processing. The backup path shows 50% savings for bandwidth and 47% for processing. The implementation of MP with 4 paths provides an additional 2% average improvement compared to MP with 3 paths. The use of multiple paths results in an optimization of resource usage in terms of bandwidth and processing capacity.

Fig. 7 shows that the average nodal degree for the Renater topology is quite low (2.94), limiting the use of more than two paths for most requests. This restriction results in a modest cost saving of 5% when transitioning from DP to MP, which is significantly less than the potential savings offered by the Cost239 topology, which has a relatively high average nodal degree (4.72). Thus, the effectiveness of the protection mechanisms within a network topology is dependent on a variety of factors, including the average nodal degree, the availability of DZ-disjoint paths, and the distribution of DZs.

C. Validation of Heuristics Efficiency Compared With ILP

We investigate the heuristic's performance compared with ILP for small-scale instances (number of requests varies from 10 to 70) for both Cost239 and Renater topologies. Fig. 8 gives a comparison between DCBJOH, TSOH, and the ILP solution using Cplex for the Cost239 topology under different scenarios: DP, MP with 3 paths, and MP with 4 paths. We evaluate two metrics : Quality of the solution and the Cost, while varying the number of SFC requests. The quality of solution is measured as the proportion of protected requests over the total number of requests. For all three scenarios, both heuristics provide high-quality solutions with 100% of requests being

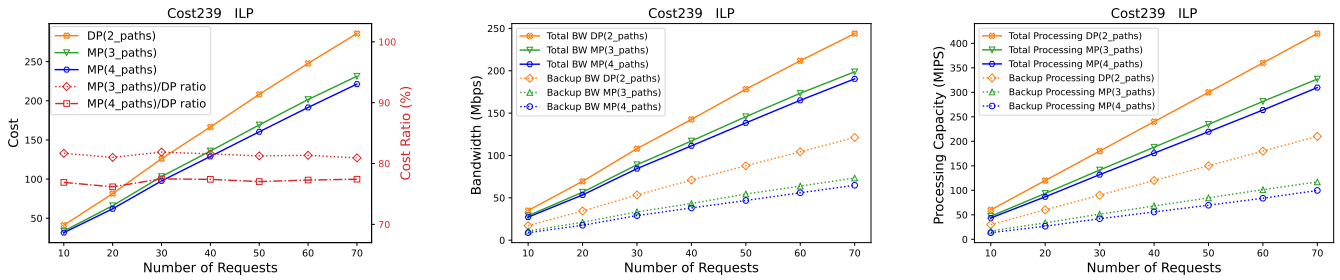


Fig. 6. DP vs. MP using ILP model (Cost239 network)

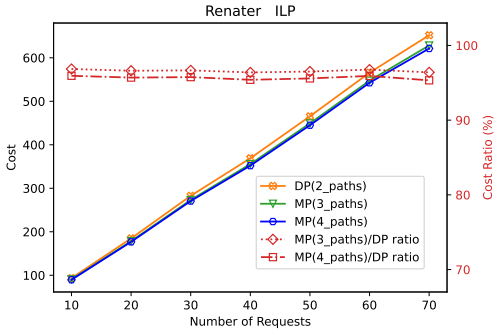


Fig. 7. DP vs. MP using ILP model (Renater network)

protected. For the Cost metric, DCBJOH provides solutions that are very close to the optimal solution (ILP), with a gap that does not exceed 4% even in the worst cases. However, even with good solution quality, TSOH shows a larger gap from 19% to 25% compared to the optimal solution. Similarly, for Renater topology, Fig. 9 shows that even in case of low average nodal degree, DCBJOH gives high-quality solutions close to the optimal solution and for all three scenarios. On the other hand, TSOH produces low-quality solutions that do not exceed 60%, meaning that 40% of requests are not satisfied. This justifies the lower Cost compared to the optimal Cost for the three scenarios. The execution time results are summarized in Table V.

TABLE V
EXECUTION TIME IN ILP, TSOH AND DCBJOH (COST239 NETWORK)

Number of Requests		10	20	30	70	80	90	100
Scheme	**Method**							
DP (2 paths)	TSOH	0.17	1.21	3.49	26.98	31.71	38.90	40.66
	DCBJOH	1.43	2.92	4.30	9.31	10.37	11.80	12.97
	ILP	0.46	1.63	2.59	1137	1374	1811	2117
MP (3 paths)	TSOH	0.25	2.26	7.74	110	92	128	136
	DCBJOH	2.04	4.34	6.33	210	232	239	177
	ILP	284	910	1020	4365	5589	-	-
MP (4 paths)	TSOH	0.34	3.26	18.48	31.97	97.81	54.50	35.80
	DCBJOH	2.46	30.05	68.25	16.63	17.69	35.36	21.88
	ILP	946	5582	11459	13255	-	-	-

Time unit : second (**s**)
- No feasible ILP solution after 4 hours or exhausting all the memory

D. Validation of MP Compared With DP for Large-Scale Instances (Using Heuristics)

To validate the effectiveness of the MP strategy, we compare different approaches: DP, MP with 3 paths and MP with 4 paths. We considered a large number of requests, ranging from 100 to 1000 in the Cost239 and Geant networks. The results for the Cost239 topology are presented in Fig. 10. Both DCBJOH and TSOH achieve similar gains for small and high numbers of requests, demonstrating the robustness of the two heuristics. From DP to MP with 3 paths, the reduction is 20% of the Cost, whereas MP with 4 paths gives a reduction of 24%. The Cost for DCBJOH is much smaller than TSOH, although both heuristics provide good solution quality. However, TSOH's performance degrades when the number of requests reaches 600, as network saturation makes path routing more challenging. DCBJOH is 60% faster compared to TSOH. Fig. 11 shows the results for the Geant topology, a large and sparse-connected topology with an average nodal degree of 2.95. The DCBJOH provides an excellent solution quality, as 100% of requests are protected while also reducing the Cost. From DP to MP with 3 paths the cost saving is 7%, and 9% with MP 4 paths, with a limited time. For TSOH, only 79% of the requests are protected due to the specific topology characteristics of Geant: large network size, low connectivity and larger number of DZs. Thus, the computation time for a solution increases significantly.

Performance of DCBJOH is better than TSOH in terms of cost optimization, time consumption, and solution quality. DCBJOH performs well even in large and sparsely connected networks, such as the Renater and Geant topologies, as well as for large number of requests (scalability). In contrast, TSOH gives a worse solution quality, a higher cost, and longer computing time, particularly for large sparse networks.

E. Impact of Nodal Degree on SFC Protection

Using MP, the obtained results showed that the Cost239 topology demonstrates a higher gain compared to the Renater and Geant topologies. This finding has led us to investigate the impact of nodal degree on resource protection and optimization. To conduct this investigation, we progressively increased the nodal degree in the Renater topology, as shown in Fig. 12. We began with an average nodal degree of 2.94 then 3.35, 3.64, and finally achieved an average nodal degree of 4.70, which is the same as the Cost239 topology. This was accomplished by adding edges at increments of 14%, 24%, and 60%. Our goal was to examine the Cost and gain associated with using MP with 3 paths and MP with 4 paths, as opposed to DP. The results presented in Fig. 13 (for 70 requests) reveal a direct relationship between the average nodal degree and the

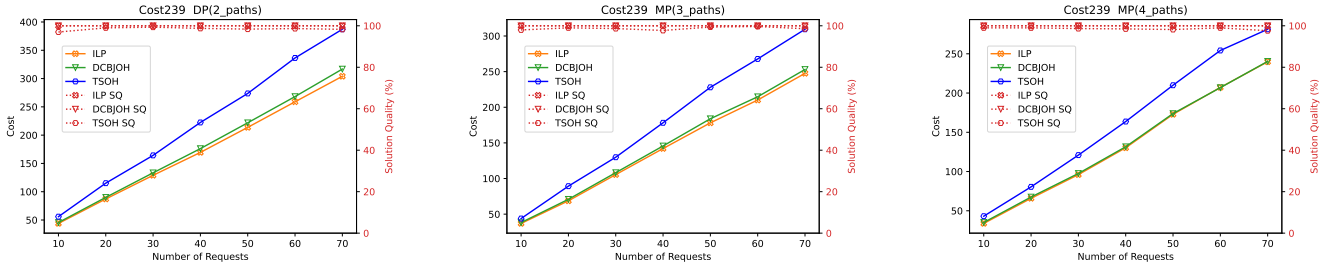


Fig. 8. DCBJOH, TSOH and ILP model for DP & MP (Cost239 network)

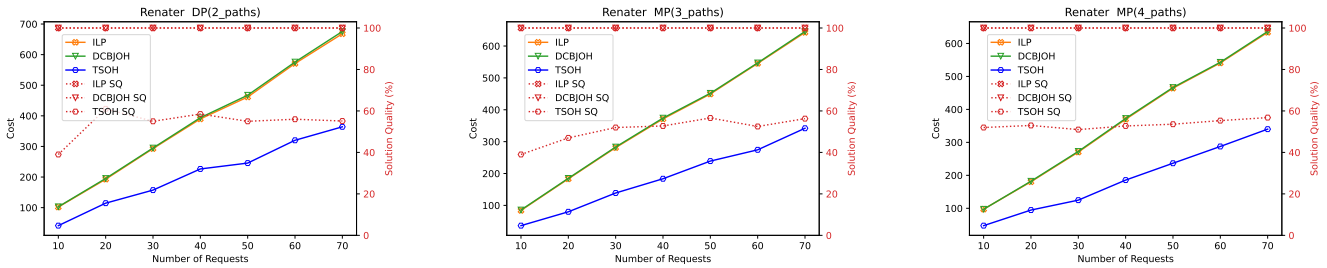


Fig. 9. DCBJOH, TSOH and ILP model for DP & MP (Renater network)

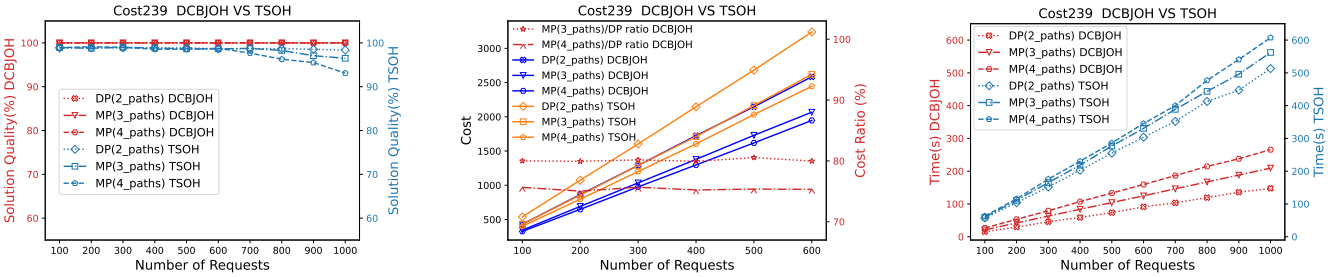


Fig. 10. Heuristics scalability for DP vs. MP (Cost239 network)

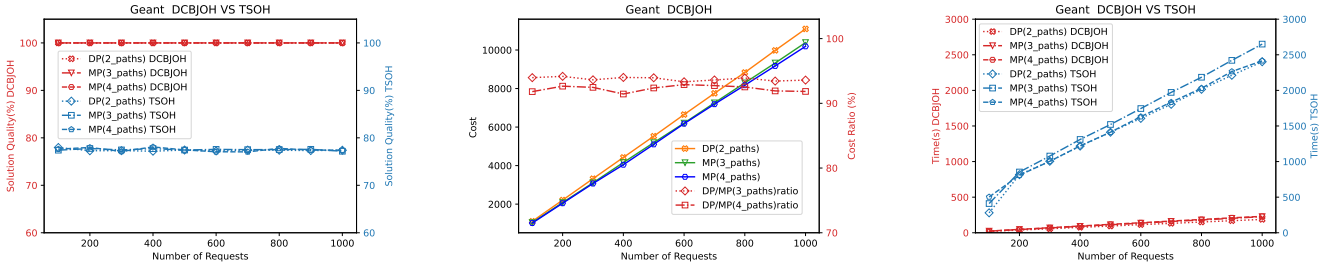
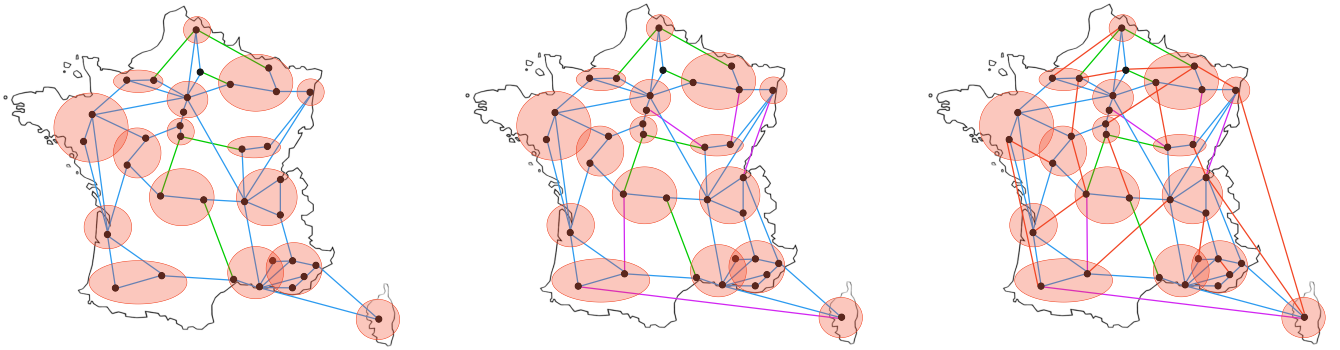


Fig. 11. Heuristics scalability for DP vs. MP (Geant network)

gain from using MP, which leads to resource minimization. With the same nodal degree as the Cost239 topology (4.70), we observed an equivalent gain. Specifically, using MP with 3 paths instead of DP resulted in a 20% reduction in resource usage, while using MP with 4 paths give a 22% reduction. These findings underscore the significance of nodal degree in optimizing network resources and enhancing protection. Further research could focus on refining the balance between nodal degree and resource utilization in various network topologies to promote more efficient and resilient network designs.

F. Performance Analysis of MP protection (DCBJOH Heuristic) vs. Diverse Network Settings

Given that DCBJOH has demonstrated its superior performance, we will focus our analysis on various parameters to further comprehend its strengths. We execute simulations for 100 requests, repeating this process 100 times. We consider standard parameters, varying one of these parameters at a time to examine its impact. The maximum number of paths k^r is 4, with 3 VNFs as SFC size and $\theta = 0.1$, keeping sufficient capacity for nodes and edges.



(a) Average Nodal Degree = 3.35 (+14% edges) (b) Average Nodal Degree = 3.64 (+24% edges) (c) Average Nodal Degree = 4.70 (+60% edges)

Fig. 12. Nodal Degree variation (Renater network)

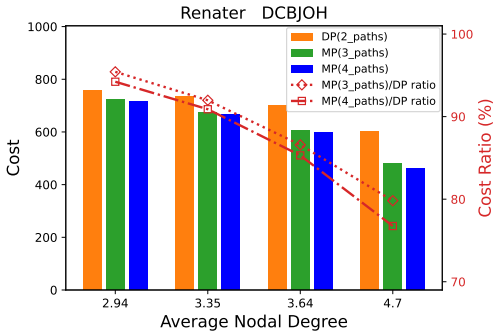


Fig. 13. DP vs. MP using DCBJOH (Renater): Nodal Degree Variation

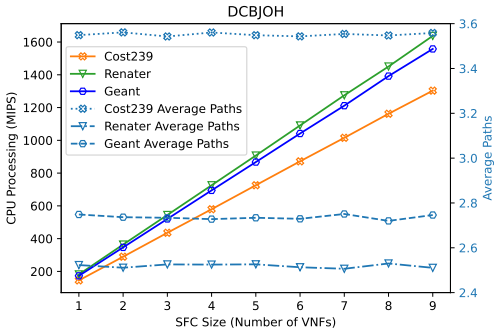


Fig. 14. SFC size variation results using DCBJOH

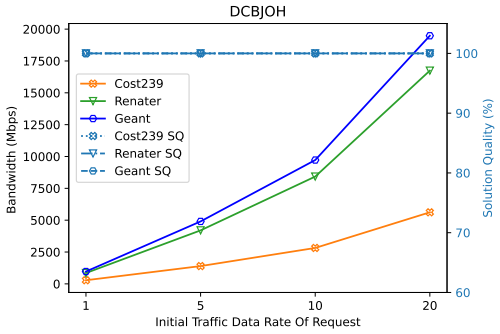


Fig. 15. Initial Traffic Data Rate variation results using DCBJOH

1) Varying SFC size: For different network topologies - Cost239, Geant, and Renater, we analyze the Processing Capacity and Average Paths by increasing the SFC size. The number of VNFs in a request varies from 1 to 9. In traditional protection strategies such as DP, the processing cost depends only on the size of the SFC and not on the characteristics of the topology. For instance, if there are 3 VNFs, the processing cost will be the same on networks such as cost239, Renater, and Geant, as the same amount of data needs to be processed by the 3 VNFs for both the working and backup paths for all requests. Fig. 14 shows that as the size of the SFC increases, more processing capacity is required to support it, as indicated by the upward trend of the processing cost curve. The graph shows that Renater has a very low average paths per request of 2.5, which implies higher processing costs. In fact, Renater has the highest processing cost among the three topologies. On the other hand, Cost239 has a high average paths per request of 3.6, but the processing cost is relatively low, at less than 19%. Geant has a relatively low average paths per request of 2.8 and a processing cost that is less than 4% in Renater. Therefore, having more average paths per request tends to imply less processing costs. The graph highlights the benefits of using multiple working paths (MP) to minimize processing costs. The more working paths used, the greater the savings on processing costs.

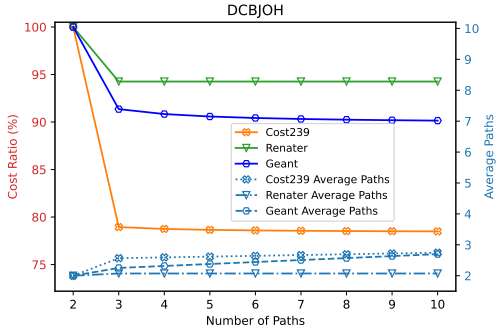
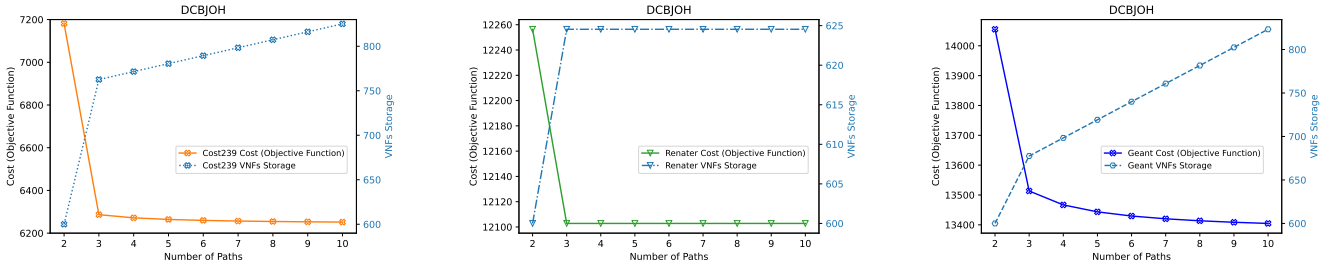


Fig. 16. Number of Paths variation results using DCBJOH

2) Varying initial bandwidth rate: To verify our ability to meet the diverse business needs, we varied the initial bandwidth rate and observed its impact on the quality of the



(a) Cost239 (b) Renater (c) Geant

Fig. 17. Cost (Objective Function) & VNFs Storage vs. Number of Paths (SFC size = 3)

solution and the heuristic behavior. The initial bandwidth rate was varied between 1 and 20 Mbps, which is sufficient for basic internet browsing, email, and text-based communication and may also support low-quality video or audio streaming, on the other hand, is ideal for high-speed internet activities such as high-quality video streaming, online gaming, and video conferencing. According to Fig. 15, the total bandwidth in three different topologies increases as the initial data rate increases. This indicates that the initial data rate is a crucial factor in determining the overall bandwidth consumption of a network. Additionally, the Cost239 topology exhibits lower bandwidth consumption than the other topologies, which can be attributed to its small size and high connectivity that allows for multiple working paths (MP advantage) and minimizes resource usage. Despite these differences in bandwidth consumption, all three topologies demonstrate high solution quality regardless of the initial data rate. This implies that the initial data rate does not significantly impact reliability, provided that there is sufficient storage and processing capacity on the nodes and enough bandwidth capacity on the edges.

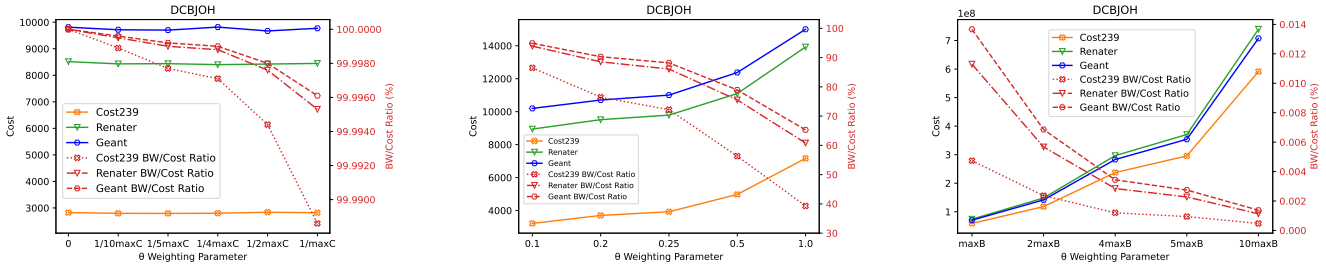
3) Varying the number of working paths: We conducted further investigations to determine the impact and limitations of increasing the number of working paths. The number of paths ranged from 2 to 10. Fig. 16 shows the Cost ratio and average paths in Cost239, Renater, and Geant topologies, by varying the maximum number of paths used for a request. For all three topologies, the most significant gain is observed when going from 2 paths to 3 paths, after which the gain diminishes as the number of paths increases due to topology-specific conditions that lead to saturation. In Cost239, the cost gain from 2 paths to 3 paths is 21%, with a higher average number of paths than the other two topologies, as Cost239 is considered highly connected. In contrast, Renater is considered low-connected, with a large number of DZs relative to the number of nodes, and the cost gain from 2 paths to 3 paths is only 6%. Geant, on the other hand, is also considered low-connected but relatively large, and the cost gain from 2 paths to 3 paths is 9%. These findings demonstrate the advantages of using multiple paths, but they also highlight that the gain depends on the topology's characteristics. Adding more connections to create a hyper-connected topology can increase reliability and resource efficiency.

Fig. 17 illustrates the relationship between the number of paths and VNF storage: more paths require more VNF storage, even though the cost of the objective function decreases. This necessitates finding a balance between the number of paths and the operational cost, which also depends on the characteristics of the network.

4) Varying weighting parameter θ: The weighting parameter may play an important role in helping network operators choose their economic preferences, which is why we are studying its significance. In Fig. 18 (b), we analyze the Cost and bandwidth/cost ratio to gain an understanding of the contribution of bandwidth to the Cost, while varying θ between 0.1 and 1. As we increase θ, the Cost increases because it is a combination of the total bandwidth and processing capacity. Moving θ from 0.1 to 1 reduces the contribution of bandwidth to the Cost from 88% to 40% in Cost239. However, on Renater and Geant, the proportion of bandwidth in the Cost decreases from 95% to 65%. This suggests that Cost239 is more expensive in terms of processing capacity than bandwidth, which is the opposite of Renater and Geant. We can explain this by considering that Geant and Renater are relatively larger, and therefore the paths are longer and consume more bandwidth. The impact of the weighting parameter depends on the topology and its characteristics.

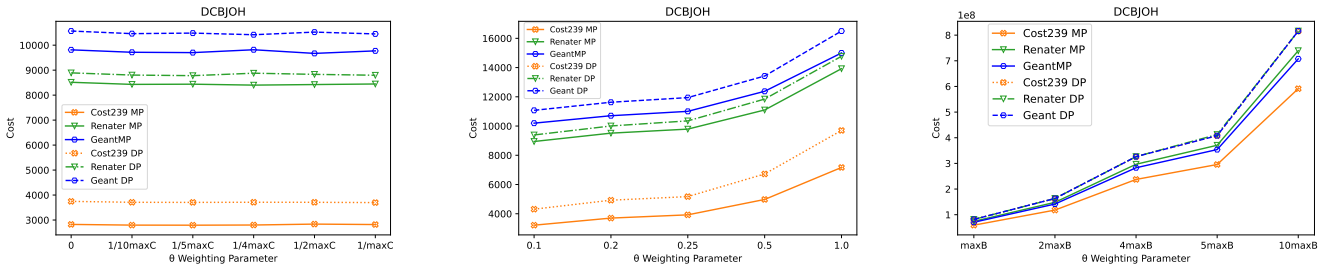
As $maxB$ represents the maximum possible bandwidth value, in our case of 100 requests, $\Delta^r = 1$ and SFCs size $|F^r| = 3$ VNFs, the worst-case scenario involves 2 paths per request on the largest network, which is Geant topology with 46 nodes, resulting in $maxB = 2 \times 45 \times \sum_{r=1}^{100} 1 = 9000$, and $maxC = 2 \times \sum_{r=1}^{100}(3 \times 1 \times 1) = 600$ the maximum of CPU. We consider three distinct scenarios: two extreme cases and one trade-off case. The first case occurs when $\theta \ll \frac{1}{\text{maxC}}$, for simplicity we can put $\theta = 0$. In this scenario, bandwidth is prioritized over CPU usage, as bandwidth becomes the dominant factor, as shown Fig. 18 (a). The second case arises when $\theta \gg$ maxB, where $B \ll C$ in all situations, causing CPU consumption to dominate the bandwidth consideration (Fig. 18 (c)). The third case represents a tradeoff situation where $\frac{1}{\text{maxC}} < \theta <$ maxB, in our simulation $0.1 \leq \theta \leq 1$ Fig. 18 (b). In this range, both bandwidth and CPU usage are balanced according to the specific needs and constraints of the network.

Fig. 19 clearly demonstrates that in all three scenarios, the cost savings are consistently maintained when transitioning from DP to MP, indicating that the efficiency of the MP strategy is independent of the choice of θ, which simply reflects the operator's preference in terms of prioritization.



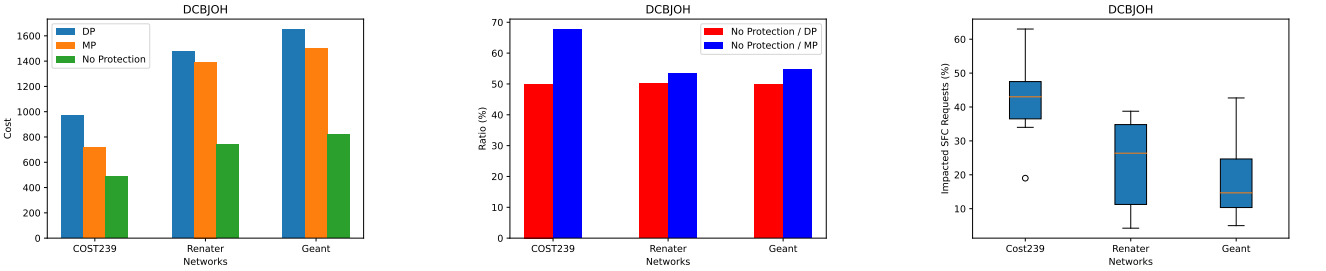
(a) Bandwidth dominates CPU (b) $0.1 \leq \theta \leq 1$ (c) CPU dominates Bandwidth

Fig. 18. Weighting Parameter variation results for MP using DCBJOH



(a) Bandwidth dominates CPU (b) $0.1 \leq \theta \leq 1$ (c) CPU dominates Bandwidth

Fig. 19. Weighting Parameter variation results using DCBJOH for DP vs. MP



(a) Protection Cost (b) Ratio of No-protection/DP&MP (c) DZ failure impact

Fig. 20. Comparison of No Protection vs. DP & MP Protection and the Impact of DZ Failure

G. Impact Analysis of No-Protection Scenario and DZ Failure

Fig. 20 provides a detailed analysis of the scenarios with and without SFC protection, comparing the No-Protection scenario, DP, and Multi-Path (MP) protection strategies. Subfigure 20(a) illustrates the protection cost, showing that No-Protection incurs the lowest cost, but at the expense of reliability. As shown in Subfigure 20(b), DP requires 50% extra resources to ensure the protection of all SFC requests in three topologies, whereas MP only needs 32% on Cost239, 45% on Geant, and 47% on Renater to protect all requests. Subfigure 20(c) examines the impact of a DZ failure on the disruption of the SFC requests when no protection is deployed. We observe that a DZ failure will cause the interruptions of about 45% of the SFC requests on average in Cost239, 29% of the SFC requests on Renater and 20% on Geant. It is also demonstrated that MP is more efficient in Cost239, since it permits to protect on average 45% of the requests with just 32% extra resources. Thus, the MP strategy, requiring even fewer resources, proves to be more efficient and effective in providing robust protection while optimizing resource usage.

VI. Conclusion

In this paper, we propose a new multi-path-based disaster protection strategy for SFC provisioning. To find the optimal MP protection solution, we first propose a path-adaptive and layered-flow based ILP model. This model is better adapted than the existing one because the number of SFC routing paths can be adjusted and optimized for different requests instead of using a unique pre-defined value. We also develop heuristics to address the limitations of the ILP model in real-world scenarios. Our proposed algorithms were tested with numerical simulations on realistic network topologies and show a significant improvement over traditional disaster protection methods, resulting in a resource gain up to 20%, especially in dense networks.

Acknowledgment

This work has been carried in the context of the project Beyond5G, funded by the French government as part of the economic recovery plan, namely “France Relance” and the investments for the future program.

REFERENCES

[1] M. A. Madani, F. Zhou, and A. Meddahi, "Deploying disaster-resilient service function chains using adaptive multi-path routing," in *2023 19th International Conference on Network and Service Management (CNSM)*, 2023, pp. 1–5.

[2] ——, "Adaptive ilp formulation for disaster-resilient service function chains in beyond 5g networks," in *2023 IEEE Conference on Standards for Communications and Networking (CSCN)*, 2023, pp. 346–352.

[3] J. Kong, I. Kim, X. Wang, Q. Zhang, H. C. Cankaya, W. Xie, T. Ikeuchi, and J. P. Jue, "Guaranteed-availability network function virtualization with network protection and vnf replication," in *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, 2017, pp. 1–6.

[4] F. Bari, S. R. Chowdhury, R. Ahmed, R. Boutaba, and O. C. M. B. Duarte, "Orchestrating virtualized network functions," *IEEE Transactions on Network and Service Management*, vol. 13, no. 4, pp. 725–739, 2016.

[5] ETSI-GS-NFV, "Network functions virtualization (nfv); architectural framework," 2014.

[6] 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)*, 2016, pp. 128–133.

[7] Y. Liu, F. Zhou, C. Chen, Z. Zhu, T. Shang, and J.-M. Torres-Moreno, "Disaster protection in inter-datacenter networks leveraging cooperative storage," *IEEE Transactions on Network and Service Management*, vol. 18, no. 3, pp. 2598–2611, 2021.

[8] M. Ju, F. Zhou, and S. Xiao, "Disaster-resilient cloud services provisioning in elastic optical inter-data center networks," in *2019 IEEE 27th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)*, 2019, pp. 116–124.

[9] A. Hmaity, M. Savi, F. Musumeci, M. Tornatore, and A. Pattavina, "Protection strategies for virtual network functions placement and service chains provisioning," *Wiley Networks*, vol. 70, 09 2017.

[10] M. Ju, F. Zhou, Z. Zhu, and S. Xiao, "Distance-adaptive, low capex cost p -cycle design without candidate cycle enumeration in mixed-line-rate optical networks," *Journal of Lightwave Technology*, vol. 34, no. 11, pp. 2663–2676, 2016.

[11] B. Addis, D. Belabed, M. Bouet, and S. Secci, "Virtual network functions placement and routing optimization," in *2015 IEEE 4th International Conference on Cloud Networking (CloudNet)*, 2015, pp. 171–177.

[12] D. Oliveira, M. Pourvali, J. Crichigno, E. Bou-Harb, M. Rahouti, and N. Ghani, "An efficient multi-objective resiliency scheme for routing of virtual functions in failure scenarios," in *2019 Sixth International Conference on Software Defined Systems (SDS)*, 2019, pp. 123–129.

[13] A. Mouaci, Gourdin, I. LjubiĆ, and N. Perrot, "Virtual network functions placement and routing problem: Path formulation," in *2020 IFIP Networking Conference (Networking)*, 2020, pp. 55–63.

[14] W. Chen, X. Yin, Z. Wang, X. Shi, and J. Yao, "Placement and routing optimization problem for service function chain: State of art and future opportunities," in *Artificial Intelligence and Security*, X. Sun, J. Wang, and E. Bertino, Eds. Singapore: Springer Singapore, 2020, pp. 176–188.

[15] A. Laghrissi and T. Taleb, "A survey on the placement of virtual resources and virtual network functions," *IEEE Communications Surveys Tutorials*, vol. 21, no. 2, pp. 1409–1434, 2019.

[16] T. Sakano, Z. M. Fadlullah, T. Ngo, H. Nishiyama, M. Nakazawa, F. Adachi, N. Kato, A. Takahara, T. Kumagai, H. Kasahara, and S. Kurihara, "Disaster-resilient networking: a new vision based on movable and deployable resource units," *IEEE Network*, vol. 27, no. 4, pp. 40–46, 2013.

[17] Q. Zhang, O. Ayoub, J. Wu, F. Musumeci, G. Li, and M. Tornatore, "Progressive slice recovery with guaranteed slice connectivity after massive failures," *IEEE/ACM Transactions on Networking*, vol. 30, no. 2, pp. 826–839, 2022.

[18] N. Shahriar, R. Ahmed, S. R. Chowdhury, M. M. A. Khan, R. Boutaba, J. Mitra, and F. Zeng, "Virtual network embedding with guaranteed connectivity under multiple substrate link failures," *IEEE Transactions on Communications*, vol. 68, no. 2, pp. 1025–1043, 2020.

[19] M. Khan, N. Shahriar, R. Ahmed, and R. Boutaba, "Multi-path link embedding for survivability in virtual networks," *IEEE Transactions on Network and Service Management*, vol. 13, pp. 253 – 266, 04 2016.

[20] N. Shahriar, S. Taeb, S. R. Chowdhury, M. Zulfiqar, M. Tornatore, R. Boutaba, J. Mitra, and M. Hemmati, "Reliable slicing of 5g transport networks with bandwidth squeezing and multi-path provisioning," *IEEE Transactions on Network and Service Management*, vol. 17, no. 3, pp. 1418–1431, 2020.

[21] S. Cai, F. Zhou, Z. Zhang, and A. Meddahi, "Disaster-resilient service function chain embedding based on multi-path routing," in *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2021, pp. 1–7.

[22] M. Ghaznavi, N. Shahriar, S. Kamali, R. Ahmed, and R. Boutaba, "Distributed service function chaining," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 11, pp. 2479–2489, 2017.

[23] J. Gil Herrera and J. F. Botero, "Resource allocation in nfv: A comprehensive survey," *IEEE Transactions on Network and Service Management*, vol. 13, no. 3, pp. 518–532, 2016.

[24] N. Promwongsa, A. Ebrahimzadeh, R. H. Glitho, and N. Crespi, "Joint vnf placement and scheduling for latency-sensitive services," *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 4, pp. 2432–2449, 2022.

[25] Y. Xu, Z. He, and K. Li, "Resource allocation and placement in multi-access edge computing," in *Resource Management in Distributed Systems*, A. Mukherjee, D. De, and R. Buyya, Eds. Singapore: Springer Nature Singapore, 2024, pp. 39–62. [Online]. Available: https://doi.org/10.1007/978-981-97-2644-8 3

[26] F. Wang, R. Ling, J. Zhu, and D. Li, "Bandwidth guaranteed virtual network function placement and scaling in datacenter networks," in *2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC)*, 2015, pp. 1–8.

[27] A. El Amine and O. Brun, "A game-theoretic algorithm for the joint routing and vnf placement problem," in *NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium*, 2022, pp. 1–9.

[28] D. Bhamare, R. Jain, M. Samaka, and A. Erbad, "A survey on service function chaining," *Journal of Network and Computer Applications*, vol. 75, pp. 138–155, 2016.

[29] "RENATER Network," Available: https://www.renater.fr, Jan 2023.

[30] "InfoTerre : Geographic information system (GIS) serves as the geomatic portal for the BRGM (Bureau de Recherches Géologiques et Minières), which is France's reference institution for Geoscientific Data." Available: https://infoterre.brgm.fr/, Jan 2023.

[31] A. Alessandro, V. Luca, T. D. P. Jutta, S. Peter, C. Andrea, V. Juergen, K. Elisabeth, W. Maureen, G. Enrico, G. Georgios *et al.*, "Overview of disaster risks that the eu faces: Internal assessment based on jrc databases," 2013.

[32] "DRMKC : Disaster Risk Management Knowledge Centre," Available: https://drmkc.jrc.ec.europa.eu/, Jan 2023.

[33] V. Eramo, E. Miucci, M. Ammar, and F. G. Lavacca, "An approach for service function chain routing and virtual function network instance migration in network function virtualization architectures," *IEEE/ACM Transactions on Networking*, vol. 25, no. 4, pp. 2008–2025, 2017.

[34] X. Z. Y. H. Zhihao Zeng, Zixiang Xia, "Sfc design and vnf placement based on traffic volume scaling and vnf dependency in 5g networks," *Computer Modeling in Engineering & Sciences*, vol. 134, no. 3, pp. 1791–1814, 2023. [Online]. Available: http://www.techscience.com/CMES/v134n3/49739