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†‡ and Ahmed Meddahi*
† *CERI-LIA, Avignon University, Avignon, France*
‡ *Léonard de Vinci Pôle Universitaire, Research Center, Paris, France*
* *Centre for Digital Systems, IMT Nord Europe, Institut Mines-Télécom, Lille, France*
{mohamed.madani@imt-nord-europe.fr, fen.zhou@univ-avignon.fr, ahmed.meddahi@imt-nord-europe.fr}

***Abstract*—Network Function Virtualization (NFV) is a 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 Virtual Network Functions (VNFs) in a specific order to deliver a desired service. However, disaster resiliency is a critical challenge when deploying NFV and SFC, as natural disasters and hardware failures can disrupt network operations and lead to service interruption or degradation across an entire disaster zone (DZ). This paper presents a new method for protecting SFCs using multi-path routing, which enables to split an SFC on multiple DZ-disjoint working paths and leverage a shared backup path for protection. The proposed Multi-path Protection (MP) minimizes network resource consumption, including both the bandwidth for request routing and the computing resources for VNF execution. We propose a heuristic approach that offers a near-optimal SFC MP solution in a time-efficient way. Numerical results show that the proposed MP strategy outperforms traditional Dedicated Protection (DP) in terms of resource consumption, resulting in significant gain up to 20%.**

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

I. Introduction

Increasing demand for network services requires advanced technologies like cloud and edge computing, driving up costs in traditional network setups. Network Function Virtualization (NFV) solves this by deploying Network Functions (NFs) on Virtual Machines (VMs) for cost-effectiveness and flexibility. Virtual Network Functions (VNFs) are sequenced to create Service Function Chains (SFCs) managed by the Management and Orchestration (MANO) system. Most studies focus on single link or node failure for SFC mapping [1], but real-world disasters can cause large-scale failures called Disaster Zones (DZ) [2] [3].

The SFC Embedding (SFCE) [4] problem is a sub-problem of Network Embedding (NE) that is NP-hard and has been extensively studied with various approaches and criteria. Different use cases and optimization methods have been proposed, including MILP/ILP models [5], Column Generation (CG) [3] to seek for optimal solutions, as well as heuristics [1] [6], and meta-heuristics [7], to get approximate solutions efficiently. The studies on SFC Embedding have focused on optimizing different objectives, such as network cost [1] [8] [6], service availability [7], and latency [5]. Various approaches and criteria have been proposed for protection strategies against failures, including heuristic algorithms [1] and ILP formulations, as paper [5] proposed protection strategies against single-node, single-arc, and single-node/link failures.

Disaster-resilient networking has received significant attention in recent papers, such as in [2] [3] [9], but few have focused specifically on disaster-resilient SFC embedding [10]. In case of natural disasters such as earthquakes, or wildfires, ensuring the availability of SFCs can be challenging due to the potential threats to network reliability. Previous works include approaches such as RA-GEN [7] scheme with a heuristic algorithm to minimize deployment cost, routing cost, and link usage, and multi-path link embedding [11] to improve virtual network survivability. However, most schemes reserve the same bandwidth on backup paths, leading to significant bandwidth waste. The multi-path approach for SFC protection was first proposed in [12], suggested the use of 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 used a fixed number of paths which is predefined without taking into account network conditions. Therefore, that model did not accurately represent real-world scenarios and may lead to no feasible solution.

The goal of this paper is to develop new modeling and algorithms for disaster protection of SFC using adaptive multi-path routing, which differs from traditional single-path methods. The focus is on minimizing network costs while fully provisioning and protecting SFCs. The strategy addresses network planning optimization aspects such as NFV placement, SFC routing, and protection, resulting in a complex optimization problem. Our work leads to the following contributions: 1) We propose an adaptive multi-path disaster protection scheme for SFC provisioning that uses multiple DZ-disjoint working paths and a backup path. The scheme uses an adaptive, optimized number of paths for SFC provisioning based on network capacity and connectivity, which is unlike existing models that use fixed, predefined paths without considering network conditions. This approach offers benefits such as balanced traffic load and a minimum 50% reduction in reserved backup path bandwidth. 2) The SFC disaster protection problem we studied is NP-hard. We develop new heuristics to address real-world scenarios with a large number of SFC requests in a limited time. 3) Heuristics were tested on new practical realistic network topologies, showing up to 20% cost reduction improvement for Multi-path Protection (MP) over traditional methods.

The paper is organized as follows: Section II explores the Disaster-Resilient SFC with Multi-Path Routing strategy. Heuristics are presented as solutions in Section II. The effectiveness of the proposed solutions is evaluated through numerical simulations in Section IV. Finally, we conclude this paper in Section IV-C.

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

The ability to provide reliable and efficient SFC is essential for the proper operation of today's networks. In case of natural disasters, ensuring the availability of SFCs can be challenging due to the potential threats to network reliability. It is essential to have an effective disaster protection scheme for SFC provisioning that minimizes resource usage.

A. Network Structure

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 $Z = \{z_1, z_2, \cdots\}$. 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 $z(v_i)$ is the associated DZ. For each arc $uv \in A$, $b(uv)$ is the total bandwidth capacity and $z(uv)$ is the associated DZ. The set of processed SFC requests is $R = \{r_1, r_2, \cdots, r_l\}$. An SFC request $r(s_r, z_r^s, d_r, z_r^d, k_r, F^r) \in R$ with a single replica of each VNF and a single virtual link between consecutive VNFs is typically represented as $r = \{s_r, f_1^r, f_2^r, \cdots, f_t^r, d_r\}$, with $F^r = \{f_1^r, f_2^r, \cdots, f_t^r\}$ as the set of t required VNFs, s_r as the source node and its DZ z_r^s, d_r as the destination node and its DZ z_r^d, and k_r maximum predefined number of DZ-disjoint paths. B_{s_r} represent initial traffic data rate for request r from s_r. We denote $\sigma_{f_i^r}$ coefficient related to processing capacity per bandwidth unit for VNF replica. The virtual links are represented as $\{e_1^r, e_2^r, \cdots, e_{t+1}^r\}$, where $e_i^r = (f_{i-1}^r, f_i^r)$ connects two consecutive VNFs, $e_1^r = (s_r, f_1^r)$ and $e_{t+1}^r = (f_t^r, d_r)$ connect the source and destination nodes, respectively. A virtual link can belong to a single physical node or span across multiple nodes to connect the VNFs.

B. Problem Statement

To address the issue of protecting network infrastructures and services from the impacts of potential disasters, our main objective is to reduce bandwidth consumption and processing costs of VNFs while protecting SFC requests. Dedicated Protection (DP) is a well-known strategy that uses a primary working path and backup path for each SFC request. The two paths must be DZ-disjoint to ensure a viable path in case of a single DZ failure. However, DP is resource-intensive, so other strategies are needed to minimize resource waste. This study excludes trivial cases like failed DZs containing SFC's source or destination node or working paths crossing no DZs.

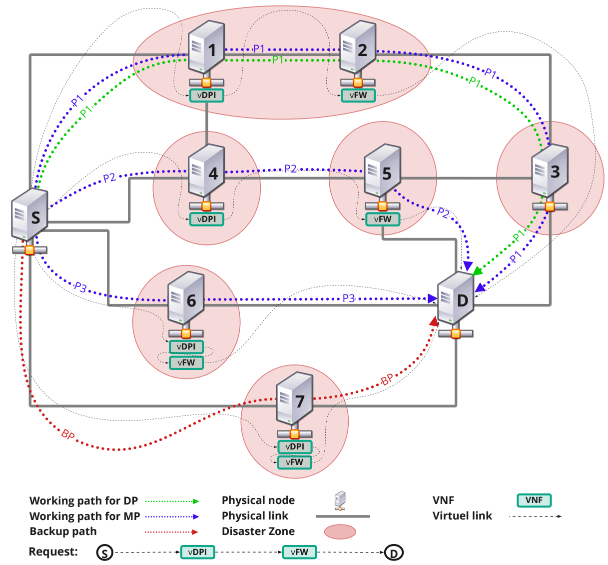


Fig. 1. SFC Disaster Protection (DP & MP)

The concept of multi-path routing is an effective solution for distributing network traffic across multiple paths. Motivated by this fact, we put forward a multi-path based disaster protection strategy (MP), which provisions SFC requests with multiple DZ-disjoint working paths and one shared backup path. This approach minimizes the impact of a DZ failure, as the working paths are DZ-disjoint and only one is affected in the event of a failure. Adopting the MP strategy reduces bandwidth reservation on the backup path by at least 50%, leading to cost savings in terms of both bandwidth and VNF processing for backup path nodes. Fig. 1 presents an illustration of the MP protection concept. Let us take an example of an SFC request with initial bandwidth demand of B_{s_r} that requires two VNFs (vDPI and vFirewall). The DP scheme provides two paths, P1 and BP, that traverse all the required VNFs in the specified order, with P1 serving as the primary path (in green) and BP 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 $2B_{s_r}$. 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 uses three DZ-disjoint paths (P1, P2, and 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 BP serves as the backup path. By distributing the SFC traffic load across the two working paths, each one carries $\frac{1}{2}B_{s_r}$ bandwidth. For protection, the reservation on the backup path is reduced to $\frac{1}{2}B_{s_r}$, 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 I. 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 BP), with $\frac{1}{3}B_{s_r}$ 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 impacts various costs like additional VNF replicas, nodes, and arcs, creating a trade-off with general costs (VNF storage, instantiation, data fragmentation, etc.). The optimal path count depends on network topology and SFC requests. Generating multiple DZ-disjoint paths for all source-destination pairs isn't always possible, and path numbers vary with network settings and requests. Thus, defining a maximum path count for each request is necessary, seeking a maximum (from a minimum of two paths) without surpassing the predefined upper limit, k_r, for provisioning, protection, and resource optimization.

TABLE I
DP & MP RESOURCE CONSUMPTION

	Paths	One Path Data Rate	Total Bandwidth	VNFs	CPU
DP	2	1	6	4	4
MP	3	1/2	4.5	6	3
	4	1/3	11/3	8	8/3

To summarize, the challenge in the Disaster-Resilient SFC MP problem is to get an optimal placement of VNFs in physical nodes, implementing efficient multi-path routing, and ensuring that paths are DZ-disjoint for the protection.

III. Proposed Solutions

The problem we address is considered a complex NP-hard problem. Therefore, we propose new heuristics for the MP that provide practical solutions close to the optimal solution with high scalability within limited time.

*1) **Divide-&-Conquer Based Joint Optimization Heuristic (DCBJOH)**:* The first approach consists of two main steps: (1) find DZ-disjoint multipaths 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_r^s) and the destination DZ (z_r^d). Once this shortest path is found, all the traversed DZs are removed, except z_r^s and z_r^d, 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 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. A loop is defined until all SFC requests are processed. **Algorithm 1** shows the detailed procedure of DCBJOH algorithm.

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={$r(s_r, d_r, F^r, B_r, k_r)$} /*Requests Set*/
Output: VNFs placement, Multi-Path DZ-disjoint path routing and protection

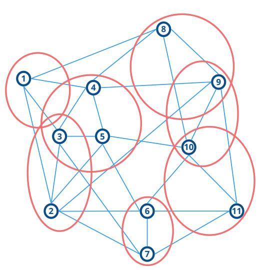
1 **forall** $r \in R$ **do**
2 G'= DZ Graph ; DZ-Paths $\longleftarrow \varnothing$;
3 **while** $\exists$ $path(s_r, d_r) \in G'$ ***and*** |*DZ-Paths*| $\leq k_r$ /* $path(s_r, d_r)$: Path between source and destination*/ **do**
4 **if** $p_c \notin$ *DZ-Paths* /* p_c : the shortest $path(s_r, d_r)$ in G' */ **then**
5 DZ-Paths $\longleftarrow$ DZ-Paths $\cup$ p_c ;
6 $G' \longleftarrow G' \cup \{DZ(s_r), DZ(d_r)\} \backslash \{p_c \cap$ DZs$\}$;
7 Finish $\longleftarrow$ **False** ;
8 **while** | *DZ-Paths* | ≥ 2 ***and !Finish*** **do**
9 *Rank*(DZ-Paths) ; Paths $\longleftarrow \varnothing$;
10 **if** | *DZ–Paths* | $> k_r$ **then**
11 DZ–Paths' $\longleftarrow$ DZ–Paths[$1 : k_r$] ;
12 $B_p = \frac{B_r}{k_r - 1}$; /*Calculate the Bandwidth in one path*/
13 **else**
14 DZ–Paths' $\longleftarrow$ DZ–Paths ;
15 $B_p = \frac{B_r}{|DZ-Paths'|-1}$;
16 **forall** $P_{DZ} \in$ *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** $\exists$ $path(s_r, d_r) \in G''$ *where* $\forall e \in path(s_r, d_r)$, $c(e) \geq$ B_p **then**
19 Paths $\longleftarrow$ Paths $\cup$ p_s; /* p_s: the shortest $path(s_r, d_r)$ where $\forall e \in p_s, c(e) \geq B_p$ */
20 Temporary updates arcs capacities ;
21 **else**
22 DZ-Path $\longleftarrow$ DZ-Path$\backslash\{P_{DZ}\}$;
23 Cancel temporary updates ;
24 **Go to** (line **8**) ;
25 **forall** $P_{DZ} \in$ *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 $\longleftarrow$ DZ-Path$\backslash\{P_{DZ}\}$;
30 Cancel temporary updates ;
31 **Go to** (line **8**) ;
32 Finish $\longleftarrow$ **True**
33 **if** *Finish* **then**
34 Validate updates ; Accept the protection of request r ;
35 **else**
36 Ignore the protection of request r ;

*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 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.

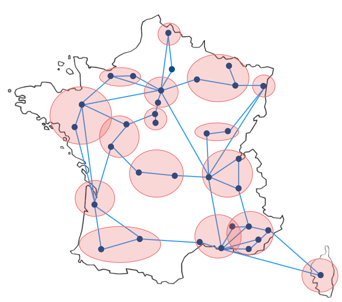
IV. Numerical Results

A. Simulation Settings

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 two network topologies in Fig. 2 : Cost-239 network (11 nodes, 52 arcs, 7 DZs, 4.72 average nodal degree) [12], and French Renater network (34 nodes, 50 arcs, 16 DZs, 2.94 average nodal degree) [13]. We consider various disaster risks to extract the DZs in Renater network, by mapping the French risks maps [14].



(a) Cost239 topology



(b) Renater topology

Fig. 2. Network Topologies for Simulations

For each request, the content and source/destination nodes are generated randomly, and the number of required network functions was also chosen randomly. The bandwidth capacity for each arc is 1000 Mbps, while node processing capacity is fixed to 1000 MIPS (typical values). 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 [12].

B. Validation of MP Compared with DP for Large-Scale Instances (Using Heuristics)

To validate the effectiveness of the MP strategy, we come on heuristics with the DP, MP with 3 paths and MP with 4 paths approaches. Thus, for processing a large number of requests, from 100 to 1000 for the Cost239 and Renater networks. The results for the Cost239 topology are presented in Fig. 3. 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 total Cost, whereas MP with 4 paths gives a 24% reduction. 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. 4 shows the results for the Renater topology, a large and sparse-connected topology with an average nodal degree of 2.94. The DCBJOH provides an excellent solution quality, as 100% of requests are protected while also reducing the total cost. From DP to MP with 3 paths the cost saving is 5%, and 7% with MP 4 paths, with a limited time. For TSOH, only 59% of the requests are protected due to the specific topology characteristics of Renater: 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 total cost optimization, time consumption, and solution quality.

C. Impact of Nodal Degree on SFC Protection

Using MP, the obtained results showed that the Cost239 topology demonstrates a higher gain compared to Renater topology. This finding has led us to investigating the impact of nodal degree on resource protection and optimization. To conduct this investigation, we progressively increased the nodal degree in the Renater topology. 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. 5 (for 70 requests) reveal a direct relationship between the average nodal degree and the 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.

Conclusions

In this paper, we propose a new multi-path-based disaster protection strategy for SFC provisioning. This strategy is better adapted than the existing one, the number of SFC routing paths

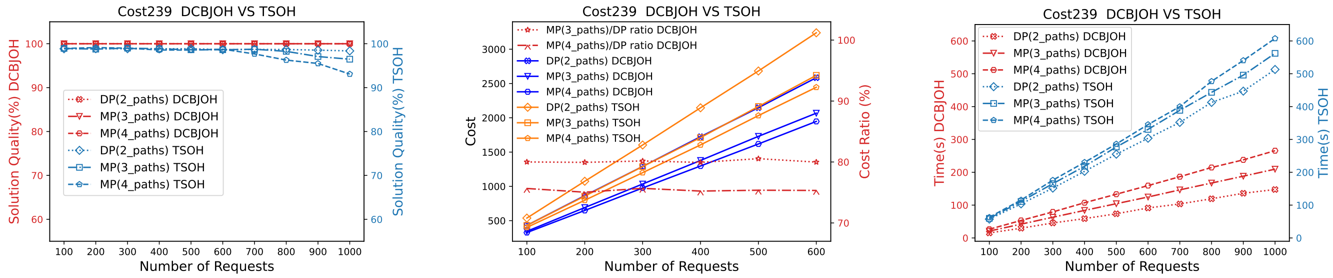


Fig. 3. Heuristics scalability for DP vs. MP (Cost239 network)

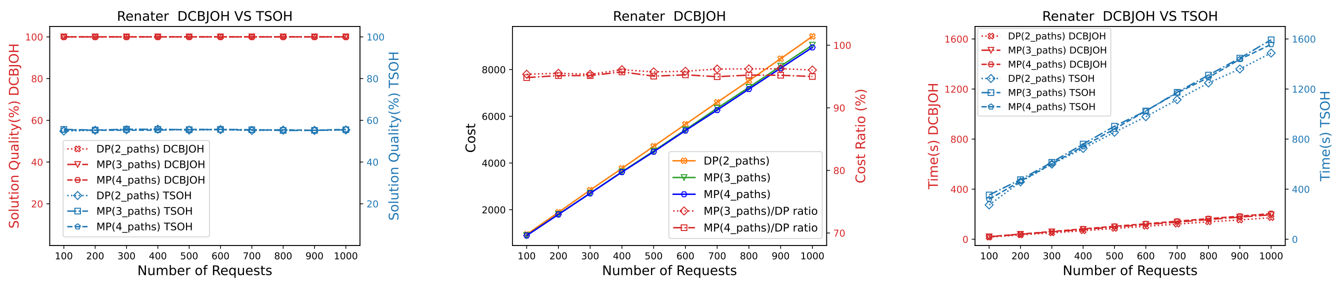


Fig. 4. Heuristics scalability for DP vs. MP (Renater network)

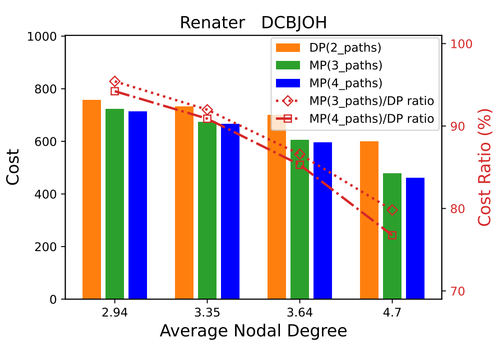


Fig. 5. DP vs. MP using DCBJOH (Renater): Nodal Degree Variation

can be adjusted and optimized for different requests instead of using a unique pre-defined value. To find a near-optimal MP protection solution, we develop heuristics designed to address 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 would not have been possible without the financial support and the harness conditions of Beyond 5G project supported by the French Banque Publique d'Investissement (BPI) and MINFIRE.

References

[1] M. Beck, J. Botero, and K. Samelin, "Resilient allocation of service function chains," in *Proc. of IEEE NFV-SDN*, 2016, pp. 128–133.

[2] Y. Liu, F. Zhou, C. Chen, Z. Zhu, T. Shang, and J. Torres-Moreno, "Disaster protection in inter-datacenter networks leveraging cooperative storage," *IEEE Trans. Netw. Service Manag*, vol. PP, 06 2021.

[3] M. Ju, F. Zhou, and S. Xiao, "Disaster-resilient cloud services provisioning in elastic optical inter-data center networks," *Proc. IEEE MASCOTS*, pp. 116–124, 2019.

[4] 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.

[5] 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.

[6] B. Addis, D. Belabed, M. Bouet, and S. Secci, "Virtual network functions placement and routing optimization," in *IEEE 4th International Conference on Cloud Networking (CloudNet)*, 10 2015, pp. 171–177.

[7] 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 *Sixth International Conference on Software Defined Systems (SDS)*, 06 2019, pp. 123–129.

[8] A. Mouaci, I. Ljubic, Gourdin, and N. Perrot, "Virtual network functions placement and routing problem: Path formulation," in *IFIP Networking Conference (Networking)*, 06 2020.

[9] 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 Trans. Netw.*, vol. 30, pp. 826–839, 2022.

[10] 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 Trans. Commun.*, vol. 68, no. 2, pp. 1025–1043, 2020.

[11] M. Khan, N. Shahriar, R. Ahmed, and R. Boutaba, "Multi-path link embedding for survivability in virtual networks," *IEEE Trans. Netw. Service Manag*, vol. 13, pp. 253 – 266, 04 2016.

[12] S. Cai, F. Zhou, Z. Zhang, and A. Meddahi, "Disaster-resilient service function chain embedding based on multi-path routing," in *Proc. of IEEE INFOCOM Workshops*, 2021, pp. 1–7.

[13] "RENATER Network," Available: https://www.renater.fr, Jun 2023.

[14] "InfoTerre : Geographic Information System (GIS)." Available: https://infoterre.brgm.fr/, Jun 2023.