Disaster-Resilient Service Function Chain Embedding Based on Multi-Path Routing

Sixu Cai[†*], Fen Zhou[*], Zonghua Zhang[‡], Ahmed Meddahi[*]
[*] IMT Lille Douai, Institut Mines-Télécom, Univ. Lille, Center for Digital Systems, F-59000 Lille, France.
[†]Institut Supérieur d'Electronique de Paris (ISEP), France.
[‡] Huawei France Research Center, Paris, France.
Emails: sixu.cai@isep.fr, fen.zhou@imt-lille-douai.fr, zonghua.zhang@gmail.com, ahmed.meddahi@imt-lille-douai.fr

***Abstract*—By using virtualization technology, Network Function Virtualization (NFV) decouples the traditional Network Functions (NFs) from dedicated hardware, which allows the software to progress separately from the hardware. One of the major challenges for NFV deployment is to map Service Function Chains (SFCs), which are chains of sequenced Virtual Network Functions (VNFs), onto the physical network components. Meanwhile, network availability faces the threats of various natural disasters, one of which makes all network devices in the Disaster Zone (DZ) fail if it occurs. Thus, it is critical to establish an efficient disaster protection scheme for NFV deployment.**

In this paper, we introduce a novel disaster protection scheme for SFC embedding using multi-path routing. The major advantage of this scheme is to cut at least half of the reserved bandwidth on the backup path by balancing the SFC traffic load on multiple simultaneous DZ-disjoint working paths. The studied problem involves VNF entity placement, SFCs routing, content splitting and protection mechanisms. The objective is to minimize the network resource consumption, including bandwidth consumption for requests routing and computing resource for VNF execution. As we treat an optimization problem of multiple dimensions (i.e., NF placement, routing and protection), it is a challenging work to obtain the optimal solution. To this end, we propose a novel flow-based integer linear program (ILP) to model the SFC protection leveraging multi-path routing and the concept of layered graph. Numerical results demonstrate that our proposed multi-path based SFC protection strategy outperforms the traditional dedicated protection in terms of bandwidth and processing resources, saving up to 21.4% total network cost.

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

I. Introduction

With the increasing demand for a series of network services such as large-scale social networks and cloud gaming, technologies such as cloud and edge computing have developed rapidly, which require both huge network service resources and high network reliability. Traditionally, a network service (NS) requires multiple network functions (NFs), such as firewalls, protocol converters, Intrusion Detection Systems (IDSs) and the traffic of the service is steered through a set of sequenced NFs. Those NFs are usually located on proprietary hardware appliances, which are quite expensive on both OPEX and CAPEX [1] [2]. To ensure a better flexibility while cutting the cost of NFs deployment and guaranteeing higher NS reliability, Network Function Virtualization (NFV) is proposed. In this scenario, NFs are decoupled from its dedicated hardware appliances and Virtual Network Functions (VNFs) are deployed on Virtual Machines (VMs) on top of universal hardware such as servers and storage devices in Data Centers (DCs). In an NFV environment, the number of VNFs can be scaled in or out on these servers, giving sufficient flexibility and convenience to the network service deployment [3] [4].

In order to satisfy some particular business needs in the network, a sequence of VNFs should be linked together and visited in a specific order to build a service, which is called Service Function Chain (SFC). The SFC allocation is managed by the Management and Orchestration (MANO) system. Many studies have been carried out on the SFCs mapping problem, but most works are to perform backup and recovery only considering single link failure or single node failure [5]. However, under real conditions, natural disasters such as floods, earthquakes, or man-made disasters such as civil war and power outages may cause an area failure or even large-scale failures. This failed area is called a Disaster Zone (DZ) [6, 7]. In this case, multiple adjacent nodes located in a DZ and the outgoing links from this DZ will fail, causing NSs to fail to recover from single node or link protection. Hence, a DZ-disjoint working and backup paths embedding should be considered to protect against disaster failures.

In this paper, we aim to design a novel efficient disaster protection scheme for SFC embedding using multi-path, while all the existing works utilize a single working path for routing SFC. Given a set of SFCs to be fully provisioned and protected, we focus on minimizing the total network cost, which consists of the bandwidth and processing cost. The studied disaster protection involves multiple dimensions of network planning optimization: NFV deployment, SFC routing and protection. Thus, it becomes a complex combinatorial optimization problem. In order to solve it optimally, we succeed to formulate it by a flow-based integer linear program (ILP) leveraging the concept of layered graph. The contributions of this paper can be summarized as follows

- We propose for the first time a multi-path based disaster protection scheme for SFC provisioning. Instead of using a single working path for routing an SFC, multiple DZ-disjoint ones are computed and utilized, while one backup path is also generated for protection in case of a DZ failure. The advantage of the proposed multi-path protection scheme lies in two aspects: balance the traffic load on multiple working paths, and thus cut at least half of the reserved bandwidth on the backup path.

- The studied SFC disaster protection problem is NP-hard. To find the optimal protection solution, a layered-flow based ILP model is proposed, which optimizes the NFV placement, SFC routing and protection simultaneously.
- The proposed ILP is verified by numerical simulations. The obtained results demonstrate the significant benefit of the proposed multi-path protection scheme over the traditional disaster protection strategy. We also explore the relationship between resource saving efficiency and the traffic load.

The rest of this paper is organized as follows. We first review the related work in Section II , and then present the disaster protection problem for SFC embedding in Section III. The studied problem is formulated by an ILP in Section IV, while numerical results are analyzed in Section V. Finally, Section VI concludes this paper.

II. Related Work

Embedding SFCs, as a Network Embedding (NE) subproblem, can be regarded as a well-known NP-hard problem. Numerous studies have been done on this topic. While most of the works addressed it as an optimization problem, they can be classified according to different criteria, such as use scenario, optimization strategy, objective, and etc. For different use scenarios, most existing works considered only the specific constraints in packet/optical data centers, operator network, WLAN, or others. From the perspective of optimization methods, either different types mixed integer linear program (MILP/ILP) models [8]–[10] were proposed to find the optimal solution, or heuristic [5] [2] [11] [8], meta-heuristic [12] and Column Generation (CG) [7] were commonly used to find an approximated solution within a fast time. In terms of optimization objective, network cost [5] [2] [11] [9], service availability [12], latency [8] and jitter reduction were paramount. In [5], they designed virtual network functions forwarding graphs (VNF-FGs) to describe a resilient service function chaining, taking VNF dependencies in consideration. A back-tracking SFC mapping method was then proposed to allocate the VNFs. Authors of [1] proposed various heuristic algorithms to allocate VNFs (path-balance, vulnerable-vnf-first, vulnerable-vnf-path-balance) based on different route selection schemes. Paper [2] presented an ILP formulation for VNF orchestration in a small scale network, and then used a heuristic to deal with large instances in order to solve it in a reasonable time. The authors in [11] considered the path latency and resource capacity limits, while minimizing the number of used nodes and arcs. Work [8] proposed three protection strategies against single-node, single-arc, and single-node/link failures. In [9], the authors proposed a path-based MILP to minimize the node activation and VNF installation cost, and gave also a heuristic to shorten the computational time.

Disaster-resilient networking is widely studied recently [6, 7, 13]–[15], while few work focused on disaster-resilient SFC embedding. In [12], a RA-GEN scheme and its corresponding heuristic were developed to minimize the VNF deployment cost, routing cost and link usage. Besides, work [14] proposed a multi-path link embedding to improve the survivability of virtual networks. However, most of the proposed schemes reserved the same bandwidth on the backup path as the working path, which leads to a significant waste of bandwidth. Our paper is motivated by the observation that we can cut at least half of the bandwidth reservation waste on the backup path through the utilization of multiple DZ-disjoint working paths and the SFC traffic load balancing on them.

III. Disaster Protection for SFC Embedding Leveraging Multi-Path

To protect against network failures due to the threats of various natural disasters, it is critical to establish an efficient disaster protection scheme for SFC provisioning. In this section, we first give the general network model, and then present our SFC disaster protection strategy, which leverages the usage of multi-path routing.

A. Network Model

The studied substrate networks can be modeled as a connected digraph $G = (V, A)$, where V denotes the set of N physical nodes $\{v_1, v_2, \cdots, v_N\}$, A is the set of physical arcs, and $uv \in A$ represents one specific arc from node u to v. The set of DZs is denoted by $Z = \{z_1, z_2, \cdots\}$, and each $z_i \in Z$ consists of all the nodes and arcs that will be affected by a single disaster. For each physical node $v_i \in V$, $c(v_i)$ denotes its total processing capacity, $R(v_i)$ presents the reliability of node v_i and $z(v_i)$ is the DZ in which the node is located. For each physical arc $uv \in A$, $b(uv)$ denotes its total bandwidth capacity, $R(uv)$ and $z(uv)$ present the reliability and the located DZ of physical arc uv. It is necessary to point out that in disaster protection, the reliability $R(v_i)$ and $R(uv)$ are either 0, which means the related node or arc is damaged during the disaster, or 1, which means it survives. We model the set of SFC requests that need to be handled as $R = \{r_1, r_2, \cdots, r_k\}$. For a regular SFC $r \in R$ with a single replica for each VNF and a single virtual link between two consecutive VNFs inside, it is usually modeled as $r = \{s_r, f_1^r, f_2^r, \cdots, f_t^r, d_r\}$, where $F_r = \{f_1^r, f_2^r, \cdots, f_t^r\}$ represents the required VNF set in the SFC, and s_r and d_r denote the source and destination node of the request, respectively. The virtual links in r are marked as $\{e_1^r, e_2^r, \cdots, e_{t+1}^r\}$, where $e_i^r = (f_{i-1}^r, f_i^r)$ stands for the virtual link connecting two consecutive VNFs. Similarly, $e_1^r = (s_r, f_1^r)$ and $e_{t+1}^r = (f_t^r, d_r)$ are virtual links connecting to the source and destination node, respectively. It should be noted that a virtual link can be either inside a single physical node or across multiple nodes in order to connect the VNFs.

B. Problem Statement

1) Disaster Protection: Each year, numerous natural disasters, such as hurricanes, forest fires and earthquakes, are threatening the network infrastructures and the provided services. In case of disaster failures, huge amount of data and lots of money will be lost. Thus, given a set of SFC requests to be fully satisfied and protected, we aim to treat the disaster protection problem. We consider a single disaster zone failure, which will make the nodes and arcs inside this DZ fail. Similar to most of the existing work, the objective of this paper is also to minimize the total bandwidth usage and processing cost of VNFs while provisioning and protecting all SFC requests. In traditional dedicated protection (DP), a pair of paths visiting all the required NFs in the given order are constructed to satisfy and protect an SFC request: one primary working path and one backup protection path. In normal status, only the primary working path is used to route the SFC request, while the bandwidth should also be reserved in advance on the dedicated backup path. The two paths should be DZ-disjoint such that the SFC request could be switched to the reserved backup path immediately once the working path is affected by a DZ failure. Hence, we can assure that at least one path is available in case of any single DZ failure, since the generated working path and backup path would not fail at the same time.

Without loss of generality, some extreme trivial cases are not necessary to be taken into account in our problem, where there is either no need or no path-based solution for implementing disaster protection. For example, if the source node or destination node of an SFC request is located in a failed DZ, then the request failure cannot be avoided by using a path-based protection. Moreover, if the working path of an SFC request does not cross any disaster zone, then there is no need to implement disaster protection and the backup path is not necessary. Therefore, we only focus on the scenarios where a disaster protection is necessary, while the trivial situations without the need of protection are excluded in our study.

2) Multi-path based SFC Disaster Protection (MP): However, a huge waste of bandwidth is observed by using this traditional dedicated protection. This is because the same amount of bandwidth as that on the working path should also be reserved in advance on the protection backup path, while it can not be used for the other requests. Currently, the multi-path routing has attracted a lot of attention, which permits to balance the traffic among multiple routing paths. Hence, why not using multiple working paths to route an SFC request instead of using a single one. If these working paths are DZ-disjoint, only one of them will be affected and must be switched to the backup path in case of a single DZ failure. As the SFC request load has been equally divided on each working path, the bandwidth reservation on the protection backup path can be significantly reduced to at least half of the DP solution. Similar reduction can be also obtained for the VNF processing cost on the nodes of the backup path. Motivated by this fact, we propose a novel SFC disaster protection scheme leveraging multi-path routing, namely MP. We give an example in Fig. 1 to illustrate the basic idea of the proposed MP scheme. We suppose there is an SFC with initial bandwidth demand of B_{s_r} and requiring 3 VNFs (vDHCP, vNAT, and vFirewall). With the dedicated protection scheme,

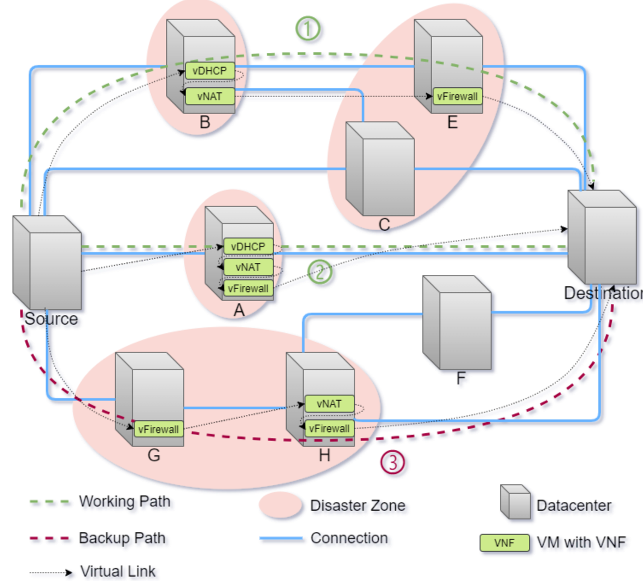


Figure 1: Multi-path based SFC Disaster Protection

there are only two paths (say 1 and 3) traversing all the required VNFS in the pre-defined order: 1 serves as the primary path, while 3 works as the backup path. As the bandwidth of working path 1 is B_{s_r}, the same amount of bandwidth should be reserved on the backup path 3 as well. In this way, the total bandwidth usage is $2B_{s_r}$. However, when applying the multi-path protection scheme, three DZ-disjoint paths (1, 2 and 3) are used for the SFC request, each of which goes through all the three required VNFs in the same order also. The paths 1 and 2 perform as working paths, and path 3 serves as the backup path. As the SFC traffic load is equally balanced on the two working paths, each one carries $\frac{1}{2}B_{s_r}$ bandwidth. To protect any one of them, bandwidth reservation on the backup path is cut to $\frac{1}{2}B_{s_r}$. As a result, half of the backup bandwidth has been saved comparing to the DP scheme. If we increase further the number of paths to 4 in total, the bandwidth reservation for backup will continue to decrease to $\frac{1}{3}B_{s_r}$. With respect to the processing cost of the three required VNFs, similar cost reduction can be obtained by using the MP protection scheme. The more paths are used, the more bandwidth for backup can be saved. However, considering more replicas, physical nodes and arcs are required, the total cost will increase as well. Besides the number of DZ-disjoint paths for an SFC request is also limited if the network topology is sparse or the nodal degree is small. Hence a trade-off between the number of used paths and the total cost should be found. It should be also noted that generating multiple DZ-disjoint routing paths is not always feasible for all source-destination pairs, and the number of these DZ-disjoint routing path varies for different network configurations and requests. Therefore, a pre-tested paths splitting number for each SFC request is mandatory to make sure the multi-path routing could be implemented.

To model the multi-path SFC protection scenario, we duplicate one VNF into multiple replicas, presented as $f_i^r = \{f_{i1}^r, f_{i2}^r, \cdots, f_{is}^r\}$, and f_{ik}^r is the k-th replica of VNF f_i^r. It should be noticed that the number of the replicas should be larger than the number of splitting paths of request r such that VNF replicas are sufficient for each path to pass through. For each replicas, its demanded processing capacity is $c(f_{ik}^r)$, which is defined by three parts: the initial traffic data rate B_{s_r}, a coefficient rate for indicating the amount of processing capacity per bandwidth unit for a certain VNF f_i^r, which denotes as $\alpha_{f_i^r}$, and the path splitting number k_r. The virtual link in r is marked as e_{ik}^r and $e_{ik}^r = (f_{ik}^r, f_{(i+1)k}^r)$, in which f_{ik}^r is the source VNF replica and $f_{(i+1)k}^r$ denotes the destination VNF replica of virtual link e_{ik}^r. $b(e_{ik}^r)$ is the bandwidth demand of virtual link e_{ik}^r. It should be noted that there are dependencies between VNFs and some SFC requests need to visit a set of specific sequenced VNFs. This is the reason why we assume $e_{ik}^r = (f_{ik}^r, f_{(i+1)k}^r)$ in our case. The traffic flow may also change after passing through a VNF. For example, the traffic must pass through f_{1s}^r before it arrives f_{2k}^r, and the data rate increases 150% after passing f_{1k}^r. To measure the traffic change of VNF f_{ik}^r, we use $r_{rel}(f_{ik}^r) = \frac{forwading\ data\ rate}{initial\ data\ rate}$ to represent it. However, to simplify our model, we assume $r_{rel} = 1$ for all VNFs. In this way, the bandwidth demand of backup path can be reduced as long as the path splitting number $k_r \geq 2$.

IV. ILP Formulation

The SFC disaster protection problem involves multiple dimensions of network optimization: VNF placement, SFC routing and protection. As the DP based disaster protection is already a NP-hard problem, it becomes even more challenging when integrating the concept of multi-path routing. To find the optimal protection solution, we show in this section how the multi-path based SFC disaster protection problem can be formulated as a layered-flow based ILP formulation. Network parameter and ILP variables are given in Tab. I.

A. Objective Function

By introducing the multi-path routing for SFC disaster protection, we aim to further reduce the total bandwidth and processing cost. Let θ be an adjustable weighting parameter, which can be defined by the network operators. Hence, the objective function of our multi-path disaster protection problem can be expressed by

$$\min \quad \sum_{r \in R} \left[B(e_i^r) + \theta \cdot P(f_{ik}^r) \right] \tag{1}$$

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

$$B(e_i^r) = \sum_{p_r \in P_r} \sum_{uv \in A} \xi_{uv}^{p_r} \cdot \frac{B_{s_r}}{k_r - 1} \tag{2}$$

Table I: Notations

Network Sets and Parameters	
$G(V, A)$	Network with node set N and arc set A.
R	Set of requests $r(s_r, z_r^s, d_r, z_r^d, k_r, F_r)$, where s_r, z_r^s, d_r, z_r^d, k_r and F_r are source node, disaster zone that source node is placed, destination node, disaster zone that destination node is placed, path splitting number, and the required VNF set.
k_r	The maximum number of DZ-disjoint paths for SFC request r, which is upper bounded by the nodal degrees of s_r and d_r, and can be determined in advance.
$p_r \in P_r$	$P_r = \{1, 2, \cdots, k_r\}$, representing the set of splitting path index of request r.
f_i^r	i-th VNF required by SFC request r.
f_{ik}^r	k-th replica of VNF f_i^r, and $k \in \{1, 2, \cdots, k_r\}$.
e_i^r	Virtual link from f_i^r to f_{i+1}^r.
$R(v_n)/R(uv)$	Reliability of physical nodes and arcs.
$z \in Z$	DZ/set of DZs. Each z contains a set of arcs and nodes.
z_r^s	Disaster zone that source node s_r is located. Note that z_r^s is 0 if source node is not in any DZ.
z_r^d	Disaster zone that destination node d_r is located. Note that z_r^d is 0 if source node is not in any DZ.
$N(v)^+/N(v)^-$	Set of outgoing/incoming arcs from node $v \in V$.
$K_{f_i^r}$	Maximum number of VNF replicas that VNF f_i^r is allowed in the network G.
B_{s_r}	Initial traffic data rate of request r from source node s_r.
$\alpha_{f_i^r}$	Coefficient for indicating the amount of 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 number of VNFs that allowed to be installed on node v.
S^k	Set of incompatible VNF pairs associated with request r.
Variables in ILP formulations	
$\alpha_z^{p_r} \in \{0, 1\}$	Equals 1 if path p_r of request r goes through DZ z, and 0 otherwise.
$\beta_{f_{ik}^r v}^{p_r} \in \{0, 1\}$	Equals 1 if the k-th replica of f_i^r on node v is used on the working or backup path p_r , and 0 otherwise.
$\gamma_v^{f_{ik}^r} \in \{0, 1\}$	Equals 1 if the k-th replica of f_i^r is installed on node v, and 0 otherwise.
$\xi_{uv}^{p_r f_i^r} \in \{0, 1\}$	Equals 1 if arc (u, v) is used on the working/backup path p_r from s_r to the node storing f_i^r, and 0 otherwise.
$\xi_{uv}^{p_r} \in \{0, 1\}$	Equals 1 if arc (u, v) is used on the working or backup path p_r, and 0 otherwise.

The second part is the total processing cost for VNF executions, which can be written as

$$P(f_{ik}^r) = \sum_{p_r \in P_r} \sum_{v \in V} \sum_{f_i^r \in F_r} \sum_{f_{ik}^r \in f_i^r} \beta_{f_{ik}^r v}^{p_r} \cdot \frac{\alpha_{f_i^r} B_{s_r}}{k_r - 1} \tag{3}$$

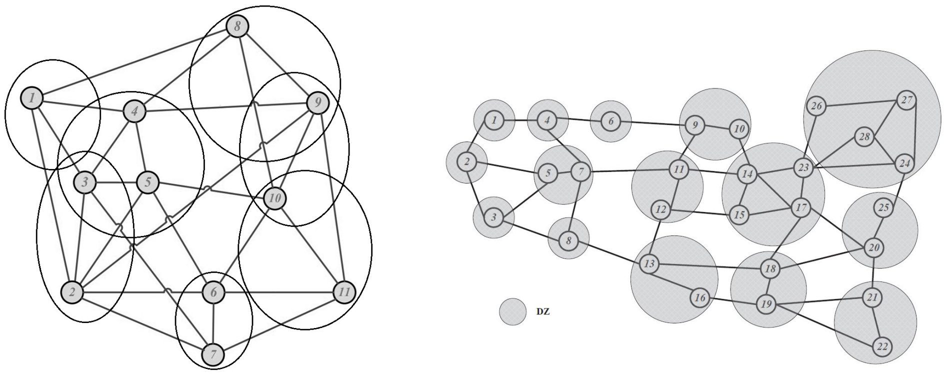
To achieve full SFC provisioning and protection, our ILP model is subject to constraints (4)-(18), which will be presented and explained in the following subsection.

B. Constraints

1) VNF quantity constraints:

$$k_r \leq \sum_{v \in V} \sum_{f_{ik}^r \in f_i^r} \gamma_v^{f_{ik}^r} \leq K_{f_i^r}, \quad \forall r \in R, \forall f_i^r \in F_r \tag{4}$$

Constraint (4) gives the lower bound and upper bound of the number of replicas for VNF f_i^r. The number of replicas should



(a) COST239 topology

(b) US backbone topology

Figure 2: Network Topologies for Simulations

be no smaller than the total number of paths. This allows to ensure that each path can be routed through at least one replica of VNF f_i^r. Meanwhile, the number of replicas should be no bigger than the quantity threshold to prevent the waste of storage space.

2) VNF allocation:

$$\beta^{p_r}_{f^r_{ik}v} \geq \gamma_v^{f^r_{ik}} + \xi^{p_r}_{uv} - 1, \quad \forall r \in R, \forall v \notin S_r, \forall p_r \in P_r \quad \forall f^r_{ik} \in f^r_i, \forall f^r_i \in F_r \tag{5}$$

$$\beta^{p_r}_{f^r_{ik}v} \leq \gamma_v^{f^r_{ik}}, \quad \forall r \in R, \forall v \in V, \forall p_r \in P_r \quad \forall f^r_{ik} \in f^r_i, \forall f^r_i \in F_r \tag{6}$$

Constraints (5)-(6) determine the location of the i-th required VNF replica f^r_{ik}, which is used by a working/backup path of requet r.

3) Incompatibility constraints:

$$\gamma_v^{f^r_{ik}} + \gamma_v^{f^{r'}_{i'k'}} \leq 1, \qquad \forall v \in V, \forall (f^r_{ik}, f^{r'}_{i'k'}) \in S^k \tag{7}$$

Constraint (7) guarantees if two VNFs f^r_{ik} and $f^{r'}_{i'k'}$ are not compatible with each other, they can not be installed on a same node.

4) Capacity constraints:

$$\sum_{r\in R}\sum_{p_r\in P_r}\sum_{f^r_i\in F_r}\sum_{f^r_{ik}\in f^r_i} \beta^{p_r}_{f^r_{ik}v} \leq w_v, \qquad \forall v \in V \tag{8}$$

$$\sum_{r\in R}\sum_{p_r\in P_r}\sum_{f^r_i\in F_r}\sum_{f^r_{ik}\in f^r_i} \beta^{p_r}_{f^r_{ik}v} \frac{\alpha_{f^r_i} B_{s_r}}{k_r - 1} \leq c_v, \quad \forall v \in V \tag{9}$$

$$\sum_{r\in R}\sum_{p_r\in P_r} \frac{B_{s_r}}{k_r - 1} \xi^{p_r}_{uv} \leq c_{uv}, \qquad \forall uv \in A \tag{10}$$

Constraint (8) is used to restrict the total replicas of VNFs on node v can not exceed its capacity. Constraint (9) guarantees that the processing capacity of a node should be above that are required by all installed VNFs. Constraint (10) assures the bandwidth requirement for an arc stays in the safe zone of its physical bandwidth capacity.

5) Flow-conservation constraints:

$$\sum_{e\in N(v)^+} \xi^{p_r f^r_i}_{uv} - \sum_{e\in N(v)^-} \xi^{p_r f^r_i}_{u'v} = \begin{cases} 1, & v = s_r \\ -\beta^{p_r}_{f^r_{ik}v}, & v \neq s_r, \forall r, \\ & \forall p_r \in P_r, \\ & \forall f^r_i \in F_r, \\ & \forall uv \end{cases} \tag{11}$$

$$\sum_{e\in N(v)^+} \xi^{p_r}_{vu} - \sum_{e\in N(v)^-} \xi^{p_r}_{u'v} = \begin{cases} 1, & v = s_r \\ -1, & v = d_r \quad \forall r, \forall p_r \in P_r, \forall uv \\ 0, & \text{otherwise} \end{cases} \tag{12}$$

$$\xi^{p_r f^r_i}_{vu} \leq \xi^{p_r f^r_{(i+1)}}_{vu} \leq \xi^{p_r}_{vu}, \quad \forall r, \forall p_r \in P_r, \forall uv, \forall f^r_{(i+1)} \in F_r, t \geq 2 \tag{13}$$

$$\xi^{p_r f^r_1}_{vu} \leq \xi^{p_r}_{vu}, \qquad \forall r, \forall p_r \in P_r, \forall uv, f^r_1 \in F_r, t = 1 \tag{14}$$

Constraint (11) generates working/backup paths from the source node s_r to the node where the VNF replica f^r_{ik} locates. It should be noted that the VNF replica number k matches the path number p_r, to avoid mixing different paths and replicas. Constraint (12) generates the working/backup paths from the source node s_r to the destination node d_r. Constraint (13) gives the sequence order of VNFs if the required VNF number by request r (denoted by t) is bigger than 2. When $t = 1$, which means there is only 1 VNF for request r, and the path from source node to location of VNF f^r_1 should be involved in the working or backup path of request r.

6) VNF disjoint constraints:

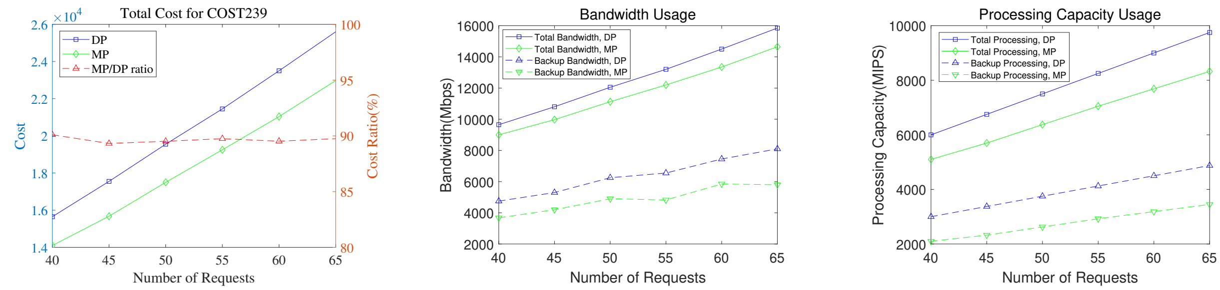
$$\sum_{f^r_{ik}\in f^r_i} \beta^{p_r}_{f^r_{ik}v} \leq 1, \qquad \forall r \in R, \forall p_r \in P_r, \forall f^r_i \in F_r \tag{15}$$

Constraint (15) makes sure that there is one and only one replica of a VNF f^r_i for any working path or backup path.

7) DZ-disjoint constraints:

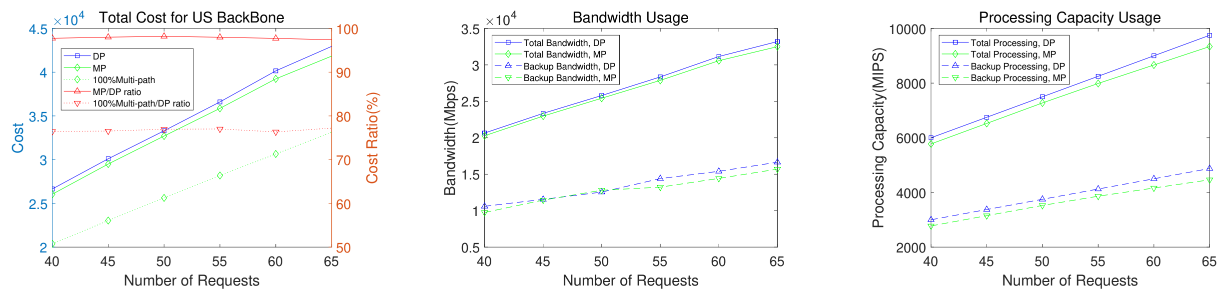
$$\alpha^{p_r}_z \leq \sum_{uv\in z} \xi^{p_r}_{uv}, \qquad \forall r, \forall z, \forall p_r \in P_r \tag{16}$$

$$\alpha^{p_r}_z \geq \xi^{p_r}_{uv}, \qquad \forall r, \forall z, \forall uv \in z, \forall p_r \in P_r \tag{17}$$



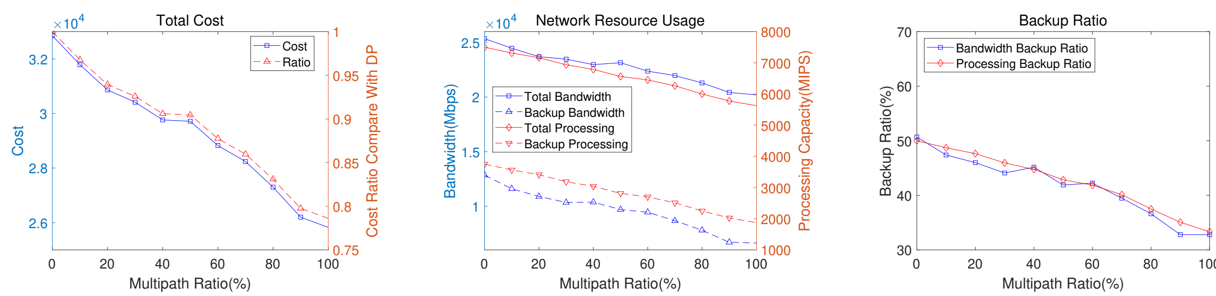
(a) Cost vs. No. Request (b) Bandwidth vs. No. Request (c) Processing vs. No. Request

Figure 3: Evaluation results vs. number of requests in COST239



(a) Cost vs. No. Request (b) Bandwidth vs. No. Request (c) Processing vs. No. Request

Figure 4: Evaluation results vs. number of requests in US Backbone



(a) Cost vs. Multi-path Ratio (b) Resource Usage vs. Multi-path Ratio (c) Backup Ratio vs. Multi-path Ratio

Figure 5: Evaluation results vs. multi-path ratio in US Backbone

$$\sum_{p_r \in P_r} \alpha_z^{p_r} \leq 1, \qquad \forall r, \forall z \in \{x | x \in Z, x \notin z_r^s, z_r^d\} \tag{18}$$

Constraints (16)and (17) are used to determine the disaster zone that the working/backup path goes through. The DZ-disjoint condition is represented by constraint (18).

V. Numerical Results

In this section, we evaluate the performance of the proposed multi-path based SFC disaster protection scheme (MP). The optimal MP protection solution is obtained by solving our proposed ILP model using Cplex. The network topologies used for numerical simulation are COST239 (11 nodes, 26 links (52 directed arcs), and 7 DZs), and US Backbone (28 nodes, 45 links and 15 DZs) [6, 7], which are also given in Figures 2 (a) and (b) respectively. We compared our multi-path protection (MP) scheme with the dedicated protection (DP) solution, and focused our evaluation metrics on the savings of network resource consumption. The impact of the SFC traffic load and multi-path ratio was also analyzed.

Table II: Simulation Parameter Settings

θ	c_{uv}	c_v	B_{s_r}	$\alpha_{f_i^r}$	$K_{f_i^r}$	w_v
1	1000Mbps	2000MIPS	50Mbps	0.3	3	100

Our simulations were conducted on a PC with Intel(R) Core(TM) i9-9900k processor of 3.6 GHz and 64 GB RAM. The proposed ILP model was implemented on CPLEX Optimizer 12.6 through C++ API. We set $\theta = 1$ to give a general result of the optimization performance, while it can be adjusted to any value by the network operator. In addition, we set the available bandwidth capacity for each communication arc (i.e., an arc in the graph) as 1000 Mbps. The available processing capacity for each node was 2000 MIPS, because the processing capacity is usually sufficient and cheap enough. The default initial bandwidth of a request was 50 Mbps, and the coefficient α was set to 0.3 for each VNF instance. The maximum available VNF replicas of each VNF for an SFC was chosen to be equal to the maximum available path splitting number, which was 3 in our evaluations. Considering the storage space limits, we assumed that the maximum VNF installation capacity was 100. The backup path was randomly chosen from the multiple generated paths. For ease of convenience, all the above simulation settings are also summarized in Table II.

In Figures 3 (a), (b) and (c), we plotted the overall cost and bandwidth usage of different protection solutions in the COST239 topology by varying the number of SFC requests. From Figures 3 (a), (b), and (c), we observed that around 10% of the total cost was saved by our proposed MP protection scheme, which implies a bandwidth reduction in the range 6.7% - 7.5% and a processing capacity reduction of 15%. To further verify the performance of MP solution, comparisons were also done in the US backbone network, and we also plotted the obtained results in Figures 4 (a), (b) and (c). We found that the MP protection consumes 2.5% less cost than its counterpart DP protection, representing 2% less bandwidth and 3.2%-4.8% less processing resources. It should be noticed that the cost reduction in US backbone is not as much as that in COST239. In fact, this is due to the characteristics of the network topology (for instance the average nodal degree and the average number of node-disjoint paths for a pair of nodes) and the distribution of disaster zones, the number of requests which can only be transferred through two paths in US backbone is more than that in COST239. When we generated SFC requests following a uniform distribution, the ratio of the SFC requests which can be routed through multiple DZ-disjoint paths was around 15% in US Backbone network. While this ratio was as high as 60% in average in COST239 network. This is because the COST239 network is densely connected and its average nodal degree (4.7) is much higher that that of US Backbone network (3.2).

To make a more clear statement, we define Multi-path Ratio in Figure 5: the ratio of requests which are routed through three or more paths in the whole traffic. Figures 5 (a), (b) and (c) asserted the network performance when changing the multi-path ratios in the US Backbone network. This was achieved by favoring the SFC requests that can be routed through multiple paths during the request generation phase. Figure 5(a) showed that as the number of multi-path requests ratio increases, the cost of MP protection goes down from 100% to 78.6% of the DP cost. Figure 5 (b) tells that the total bandwidth usage decreases from 100% to 79.7% when increasing the multi-path ratio, and similar reduction of processing cost is also observed from 100% to 75%. In Figure 5 (c), it is shown that as the multi-path ratio increases, the resource backup ratio of all requests is inversely reduced from 50% to 33%. The obtained results match well with the theoretical analysis and confirm that our multi-path protection strategy enables us to cut significantly the network resource consumption by reducing backup resource consumption. This is perfectly consistent with the previously declared advantages of the MP protection scheme.

VI. Conclusion

In this paper, we proposed for the first time a multi-path based disaster protection scheme for SFC embedding. We formulated this problem by a layered-flow based ILP so as to find the protection solution with the minimum network cost in terms of bandwidth and processing resource. Compared with its counterpart in the literature, our proposed SFC protection scheme can cut up to one-fifth of network cost while guaranteeing the SFC provisioning against a single disaster failure.

References

[1] 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 *in Proc. of IEEE Global Communications Conference (Globecom'17)*, 2017, pp. 1–6.

[2] M. F. Bari, S. R. Chowdhury, R. Ahmed, and R. Boutaba, "On orchestrating virtual network functions," in *in Proc. of IEEE 11th International Conference on Network and Service Management (CNSM'15)*, 2015, pp. 50–56.

[3] E. G. NFV, "Network functions virtualization (nfv); architectural framework," 2013.

[4] J. Gil Herrera and J. F. Botero, "Resource allocation in nfv: A comprehensive survey," *IEEE Trans. Netw. Service Manag.*, vol. 13, no. 3, pp. 518–532, 2016.

[5] M. T. Beck, J. F. Botero, and K. Samelin, "Resilient allocation of service function chains," in *in Proc. of IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN'16)*, 2016, pp. 128–133.

[6] Y. Liu, F. Zhou, C. Chen, Z. Zhu, T. Shang, and J. Torres-Moreno, "Disaster protection in inter-datacenter networks leveraging cooperative storage," in *in Proc. of IEEE Global Communications Conference (Globecom'20)*. IEEE, 2020, pp. 1–6.

[7] M. Ju, F. Zhou, and S. Xiao, "Disaster-resilient cloud services provisioning in elastic optical inter-data center networks," in *in Proc. of 27th IEEE International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS'19)*. IEEE Computer Society, 2019, pp. 116–124.

[8] A. Hmaity, M. Savi, F. Musumeci, M. Tornatore, and A. Pattavina, "Protection strategies for virtual network functions placement and service chains provisioning," *Networks*, vol. 70, no. 4, pp. 373–387, 2017.

[9] A. Mouaci, Ã. Gourdin, I. LjubiÄ, and N. Perrot, "Virtual network functions placement and routing problem: Path formulation," in *in Proc. of IFIP Networking Conference (Networking'20)*, 2020, pp. 55–63.

[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 *in Proc. of IEEE 4th International Conference on Cloud Networking (CloudNet'15)*, 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 *in Proc. of 6th International Conference on Software Defined Systems (SDS)*, 2019, pp. 123–129.

[13] 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.

[14] M. M. Alam Khan, N. Shahriar, R. Ahmed, and R. Boutaba, "Multipath link embedding for survivability in virtual networks," *IEEE Trans. Netw. Service Manag.*, vol. 13, no. 2, pp. 253–266, 2016.

[15] M. Yu, Y. Yi, J. Rexford, and M. Chiang, "Rethinking virtual network embedding: Substrate support for path splitting and migration," *SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 2, p. 17â29, Apr. 2008.