Title

Disaster-survivable cloud-network mapping

Journal

Photonic Network Communications, 27(3)

ISSN

1387-974X

Authors

Colman-Meixner, Carlos

Dikbiyik, Ferhat

Habib, M Farhan

et al.

Publication Date

2014-06-01

DOI

10.1007/s11107-014-0434-6

Noname manuscript No.
(will be inserted by the editor)

Disaster-Survivable Cloud-Network Mapping[1]

Carlos Colman Meixner · Ferhat Dikbiyik · M. Farhan Habib · Massimo Tornatore · Chen-Nee Chuah · Biswanath Mukherjee

Received: date / Accepted: date

Abstract Cloud-computing services are provided to consumers through a network of servers and network equipment. Cloud-network (CN) providers virtualize resources (e.g., virtual machine (VM) and virtual network (VN)) for efficient and secure resource allocation. Disasters are one of the worst threats for CNs as they can cause massive disruptions and CN disconnection. A disaster may also induce post-disaster correlated, cascading failures which can disconnect more CNs. Survivable virtual-network embedding (SVNE) approaches have been studied to protect VNs against single physical-link/-node and dual physical-link failures in communication infrastructure, but massive disruptions due to a disaster and their consequences can make SVNE approaches insufficient to guarantee cloud-computing survivability.

In this work, we study the problem of survivable CN mapping (SCNM) from disaster. We consider risk assessment, VM backup location, and post-disaster survivability to reduce the risk of failure and probability of CN disconnection and the penalty paid by operators due to loss of capacity. We formulate the proposed approach as an integer linear program and study two scenarios: a natural disaster, e.g., earthquake and a human-made disaster, e.g., weapons-of-mass-destruction (WMD) attack. Our illustrative examples show that our approach reduces the risk of CN disconnection and penalty up to 90% compared to a baseline CN mapping approach, and increases the CN survivability up to 100% in both scenarios.

Keywords cloud computing · disaster survivability · cloud-network mapping · virtual-network mapping · virtual machine

[1]This work has been supported by Defense Threat Reduction Agency (DTRA) Grant No. HDTRA1-10-1-0011. A preliminary version of this work was presented in [1].

C. Colman Meixner - E-mail: cecolmanmeixner@ucdavis.edu
M.F. Habib - E-mail: mfhabib@ucdavis.edu
C-N. Chuah - E-mail: chuah@ucdavis.edu
B. Mukherjee - E-mail: bmukherjee@ucdavis.edu
University of California, Davis, USA

M. Tornatore - E-mail: tornator@elet.polimi.it
Politecnico di Milano, Italy

F. Dikbiyik - E-mail: fdikbiyik@sakarya.edu.tr
Sakarya University, Turkey

1 Introduction

Reliable provisioning of cloud-computing services depends on robust resource allocation over a common physical infrastructure, formed by datacenters and communication networks [2–4]. Physical infrastructure is often abstracted as "infrastructure as a service (IaaS)" layer which provides computational and communication resources to the upper service layers (e.g., platform as a service (PaaS) and software as a service (SaaS)) of the cloud-computing framework [5], [6]. Cloud-network (CN) mapping is the combination of virtual-network (VN) mapping and virtual-machines (VMs) allocation (i.e., network and server virtualization) over a physical infrastructure. CN survivability is crucial for computational resource allocation in a consistent and secure environment for cloud-computing services [4, 6, 7]. Figure 1 presents an example of two CNs consisting of interconnected VMs mapped over a optical network that interconnects datacenters (DC) of a cloud-infrastructure provider. Failures in the physical infrastructure can reduce the available resources (optical network and DCs) and disconnect multiple CNs. This may severely affect the upper-layer services [8]. CN survivability for a small number of failures in the physical infrastructure has been modeled as a survivable virtual-network embedding (SVNE) problem defined as

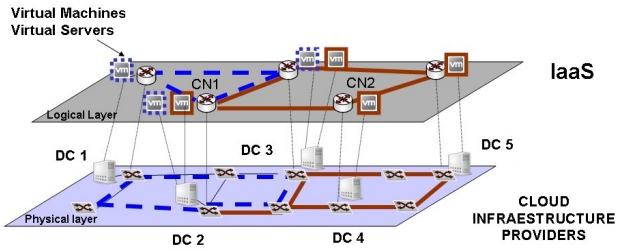

Fig. 1 Cloud networks and cloud services.

the resilient VN mapping over the physical infrastructure to avoid disconnection due to failures [9]. Most SVNE studies considered single and multiple physical-link (-node) failures (e.g., datacenter and shared-risk group (SRG)), and a regional failure that may or may not be a disaster [9–13].

Disaster failure is an special case of SRG failure which may produce multiple failures in cascade, i.e., when a disaster occurs, some network elements may fail simultaneously in the first phase, and, later, other failures in different parts of the physical network (and upper layers) may occur (e.g., power outage, aftershocks after an earthquake, etc.). An important feature of cascading failures is that they tend to be more predictable from the damage and location of the initial failure, and this prediction can be used to reorganize the network to reduce disruptions [14].

An example of a disaster failure is the 2012 Hurricane Sandy, where post-disaster cascading failures (caused by flooding and power blackouts) shut down many datacenters and network nodes in the New York area [15], and caused disruption in communication services in the northeastern US [16]. Given the scale of their impact in CNs, network operators should take measures to protect cloud-computing services from disaster and post-disaster failures despite their rare occurrences.

In this study, we consider a disaster-survivable CN mapping approach using risk assessment (similar to [17]), virtual-machine (VM) backup location, and post-disaster survivability constraints to substantially reduce risk of failure, penalty, and probability of CN disconnection in case of disaster and post-disaster failures.

1.1 Main Contributions

In this work, to the best of our knowledge, we study for the first time:

- Integration of disaster and post-disaster survivable CN mapping with a risk-assessment model to reduce the risk of CN disconnection.
- Use of a virtual-backup-node approach that can relocate VMs (i.e., VM backup location) to increase the cloud-computing survivability in case of disasters.

1.2 Organization

The rest of this study is organized as follows. Section 2 presents a brief review on cloud-network protection schemes and related works. Section 3 presents the survivable CN mapping problem. Section 4 describes our approach with an example. Sections 5 introduces the variables and symbols and the ILP formulations of the baseline approach with risk minimization objective function. Section 6 introduces the ILP formulation of the proposed approach including VM backup location, and post-disaster survivability constraints. An illustrative example is presented in Section 7, and our study concludes in Section 8.

2 Background and Related Works

A survey on network virtualization highlighting the importance of survivable virtual-network embedding (SVNE) is presented in [18]. Ref. [14] surveyed works on disaster survivability, and pointed out works on disaster SVNE combined with VM location for datacenter networks.

Most studies on the SVNE problem suggested protection or restoration (e.g., reactive) approaches to deal with single physical-link (-node) failure. To deal with single physical-link failure, Ref. [19] proposed a fast rerouting approach to recover failed VN, and Ref. [20] suggested to mix protection and restoration with backup capacity sharing to maximize revenue. Ref. [21] studied the SVNE problem for IP-over-WDM optical networks considering single and dual-link failures, introducing cut-disjoint as a survivability constraint and a routing metric MINCUT. Cut-disjoint constraint avoids the mapping of two virtual links on the same physical resource if failures on both links disconnect the virtual topology (i.e., a cut of the topology). Ref. [22] used dedicated-path-protection and cut-disjoint approaches to increase the survivability. Ref. [23] showed the advantage of cut-disjoint approach over path-disjoint approach to provide protection in VN.

Refs. [12, 24] proposed two versions of SVNE approach for physical-node failures (i.e., a datacenter failure in a regional failure) by adding backup node: l-backup node (one backup node for each VN), and k-backup nodes (1+1 node protection). Ref. [25] presented an extension of these approaches, considering the network-flow perspective to increase survivability.

Ref. [26] studied the SVNE problem in the context of grid- and cloud-computing survivability over optical networks, highlighting the importance of the survivable CN mapping (SCNM) problem which combines the SVNE problem and VM survivability. In this regard, the study in [13] suggested server capacity relocation and lightpath re-provisioning for virtualized datacenters to offer survivability. Ref. [10] presented a model that helps to reduce

the disaster failure in cloud services (i.e., cloud contents) provisioned over optical datacenter networks using a SRG-disjoint approach. Refs. [27, 28] studied the SCNM problem combining with anycast routing, where VN mapping and anycast routing are optimized together to provide CN survivability. Ref. [11] studied disaster survivability in CN mapping, suggesting a disaster-disjoint combined with non-survivable mapping to maximize revenue.

In this work, we address the SCNM problem for disaster failures using risk minimization, cut-disjoint constraint, virtual-machine (VM) backup location, and post-disaster survivability approaches.

3 Survivable CN Mapping (SCNM)

The survivable CN mapping (SCNM) problem combines SVNE and VM resiliency. To address this problem, we consider a baseline SCNM approach to provide CN resiliency for any single physical-link failure while minimizing resources (Min-Res). To extend the baseline approach for disaster survivability, we also consider minimization of the risk of damage given the occurrence of a disaster (Min-Risk).

3.1 SCNM Problem Statement

Inputs:

- CN mapping requests and VM allocation requests with required communication and processing capacity.
- Physical network with link and node capacity (i.e., datacenter capacity).

Output:

- Single physical-link failure survivable CN mapping.

Goal:

Minimize the communication resources used (i.e., wavelength channels).

3.2 Survivable Mapping Constraint

The survivable mapping constraint guarantees a survivable CN mapping for any single physical-link failure by enforcing cut-disjoint mapping as studied in [21–23]. This constraint ensures that virtual links of the same cut (i.e., set of links whose simultaneous failures disconnects the virtual topology) do not share the same physical link. A simple example of SCNM approach is shown in Fig. 2. Two CNs are considered: CN 1 = {3, 4, 6, 7} and CN 2 = {1, 2, 5} mapped over an optical network with physical nodes (i.e., optical cross-connects (OXCs) connected to routers) {A, B, C, D, E, F, G, H}, where some physical nodes {A, B, C, F, G, H} connect datacenters. Each virtual link is mapped using a lightpath. Figure 2(a) shows a non-survivable mapping where, if any of the physical links (shown in circles) fails (C - D or B - D or A - B), one or both CNs will be disconnected. Figure 2(b) shows an example of SCNM where no single physical-link failure will disconnect a CN.

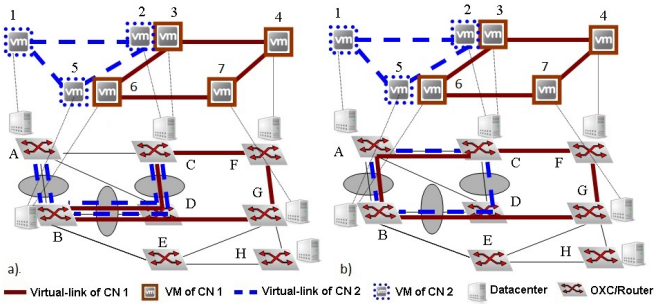

Fig. 2 (a) Non-survivable and (b) survivable CN mapping over a WDM optical network.

3.3 Resource minimization (Min-Res)

The baseline objective is to minimize resource usage (Min-Res):

$$min \sum_{\gamma \in \Gamma} (\text{Resources used by } \gamma) \quad (1)$$

where γ represents a CN request and Γ is the set of requests.

3.4 Disaster-Survivable CN Mapping with Risk Minimization (Min-Risk-DS)

The disaster-survivable CN mapping with risk minimization approach (Min-Risk-DS) extends Min-Res by including a disconnection constraint. Risk minimization offers two important advantages for the case of disaster survivability. The first advantage is the reduction of capacity (for backup) usage. The second advantage is the feasibility of the mapping in disaster zones (DZs) where the SRG-disjoint approach will not give a feasible mapping without additional resources for backup.

3.4.1 Risk assessment

Risk is defined as the expected value of an outcome seen as undesirable. In this work, we analyze the risk of CN based

on damage/loss caused by a disaster [17], as shown below:

$$min \sum_{n \in N} \sum_{\gamma \in \Gamma} (\text{Loss of } \gamma \text{ due to disaster } n)\, p_n \quad (2)$$

where the loss of CN γ ($\gamma \in \Gamma$) represents the sum of two values: (1) the penalty for CN disconnection which is the sum of the total disconnection penalty which represent capacity lost from the CN (i.e., total bandwidth) multiplied by a CN disconnection coefficient (i.e., value defined in the service-level agreement (SLA) which indicates the additional cost paid by the network provider to the customer or tenant when their CN is disconnected), and (2) the penalty of virtual-links disconnection in term of capacity lost. Finally, the risk is calculated by multiplying the resulting loss (i.e., total penalty) of γ by the probability p_n that disaster n can occur in the given disaster zone from the set of N possible disasters. Disasters are defined according to the approach used in [17] where the probability of a disaster and probability of damage are calculated based on hazard maps (see Section 7).

3.4.2 Example of risk minimization in CN mapping

To illustrate the impact of a disaster failure in CNs and the advantage of the Min-Risk-DS approach, we compare the mapping using Min-Res (Fig. 2(b)) with the mapping using Min-Risk-DS (Fig. 3(a)). Two disaster zones are included in Fig. 3, DZ1 and DZ2, with probability of occurrences (p_n) 0.3 and 0.5, respectively. Since DZ1 affects an entire node C, a SRG-disjoint approach will demand more resources for backup. To compare the two mappings, we calculate the total

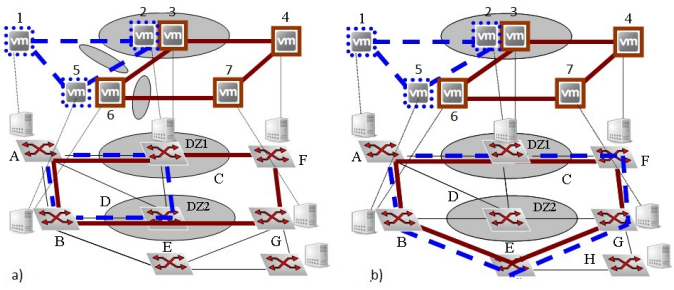

Fig. 3 (a) Min-Res approach (SCNM), (b) Disaster-survivable CN mapping with risk minimization (Min-Risk-DS), with two DZs.

risk of CN disconnection using Eq. (2), assuming the bandwidth of each virtual link is 10 Mbps and a CN disconnection coefficient of 10 (we assume a value between 1 and 10). The risk of CNs mapped in Fig. 3(a) into the physical infrastructure in DZ1 is: Penalty for CN 1 disconnection, 40 Mbps (4 virtual links of 10 Mbps each) $\times$ 10 = 400 + Penalty for CN 2 disconnection, 30 Mbps $\times$ 10 = 300. The total risk of CN disconnection is 700 $\times$ 0.3 (p_1) = 210. DZ2 does not disconnect any CN, hence only 20 Mbps is affected, 20 Mbps (i.e., penalty for virtual-link disconnection) $\times$ 0.5 (p_2) = 10. Then, the total risk will be 220.

Similarly, we can calculate the risk of CN mapping in Fig. 3(b) which is 210. The mappings of Figs. 3(a) and 3(b) use the same amount of resources (i.e., 120 Mbps each). However, the risk minimization can force the use of more resources in case of having more DZs. Hence, in this example, we confirm the necessity of VM backup location for further reduction of the risk of CN disconnection which is introduced in Section 4.

4 Disaster and Post-Disaster Survivable CN Mapping with Risk Minimization (Min-Risk-D-PDS)

Min-Risk-D-PDS extends Min-Risk-DS by adding two new functions to increase the disaster and post-disaster survivability of CNs. Note that, in the mapping of Fig. 3(b), the risk is reduced by 10 units only and a disaster in DZ1 can still disconnect both CNs. To reduce the risk and increase CN survivability for case of disaster failures, Min-Risk-D-PDS introduces the concept of VM backup location (VBL) and post-disaster survivability (PDS).

4.1 Virtual Backup Node for VM Backup Location (VBL)

VBR maps one or more virtual backup node to relocate VMs of a CN, following three main steps: selection, connection, and sharing. For comparative purpose, we use the CN 1 nodes (3, 4, 6, 7) already used in Fig. 3 with one and two VM backup location (Fig. 4). These three steps are the main novelty and advantages of our proposed VBL approach over previous works in [11, 12, 25], in which risk of disaster and post-disaster survivability are not considered.

4.1.1 Selection of datacenter for VM backup location

The physical node (i.e., datacenter) selected as backup must not only have enough excess processing capacity but also should be located in a safer place to lower the risk of disconnection.

4.1.2 Connectivity of VM backup location

Every virtual backup node has to be connected using one virtual link to a set of working VMs in its own CN (Fig. 4(a)). The virtual links which connect the CN with its backup VM have 50% of the bandwidth of the working virtual link.

4.1.3 Physical node (i.e., datacenter) sharing for VM backup location

The selected physical node to provide VM backup location for one CN can be shared by another CN as working VM

location and/or VM backup location. To increase the survivability to post-disaster failures, this approach will not allow to share the same physical node if both CNs can be disconnected by the same disaster. VBL has the flexibility to choose more than one physical node to relocate VMs based on the demand (Fig 4(b)).

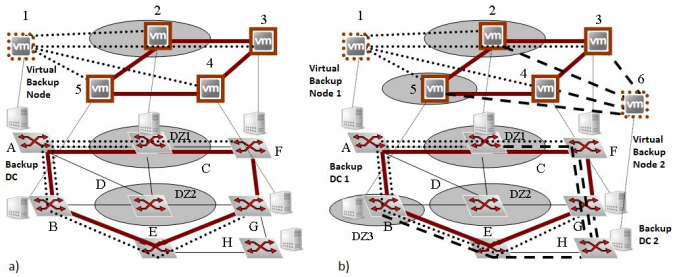

Fig. 4 Virtual backup node for VM backup location: (a) one VM backup location per CN, (b) two VM backup locations per CN.

4.1.4 Example of VM backup location

By adding VBL into Min-Risk-DS approach (Fig. 4(a)), the risk of disconnection of CN 1 (Fig. 3(b)) is reduced from 120 (note that we assume a penalty of disconnection of 400 and a p_n is equal to 0.3, so 120 = 400×0.3) to 10 (30 of penalty × 0.3). Thanks to our approach, the CN does not get disconnectd, so the risk of CN disconnection is reduced by 92% with an additional capacity of 30 Mbps (assuming 5 Mbps for each backup-virtual link).

As an example of two VM backup locations, in Fig. 4(b), we add a third disaster zone, DZ3, with $p_3 = 0.5$, which increases the risk to 210 in the mapping of Fig. 4(a). Then, we map a second virtual backup node which reduces the risk to 28 or 91.4% because only independent virtual links can be affected by disaster and the CN may remain connected. Also, the CN may survive if a disaster and post-disaster disconnect two VMs and create additional physical-link failures.

4.2 Post-Disaster Survivability (PDS)

However, if a disaster in DZ1 occurs, a post-disaster-correlated cascading failure of the physical link A - B will still disconnect the CN of Fig. 4(a). Additionally, a post-disaster failure of physical links A - B and F - G will disconnect the CN of Fig. 4(b). Hence, post-disaster survivability (PDS) constraint is added in our model to increase the survivability during recovery periods, given the vulnerability of CNs to post-disaster failures [14, 16]. Our (PDS) approach consists of two functions: cut extension and a survivability constraint.

Table 1 Example of basic and extended cuts

Basic cuts in Fig. 5(a)	Extended cuts in (VM 1 replaces VM 3 (Fig. 5(c))
(2-3)(2-5)	(2-1)(2-5)
(2-5)(5-4)	(2-5)(5-4)
(5-4)(4-3)	(5-4)(4-1)
(3-2)(4-3)	(1-2)(4-1)
(2-5)(4-3)	(2-5)(4-1)
(3-2)(4-5)	(1-2)(4-5)
(3-2)(4-5)(2-5)	(1-2)(4-5)(2-5)
(3-4)(2-5)(5-4)	(1-4)(2-5)(5-4)
(3-4)(2-5)(5-4)(2-3)	(1-4)(2-5)(5-4)(2-1)

4.2.1 Cut extension

We implement a new algorithm called ExCuts, which is an extension of the approach proposed in [22]. ExCuts extends the basic cuts of the CN 1 topology in three steps. To describe the steps, we use CN 1 (Fig. 5(a)) and one possible replacement of VM 3 by VM 1 (i.e., as virtual backup node).

Step i: ExCuts replaces the working VM 3 for VM 1 as possible relocation and builds a new topology (Fig. 5(c)).

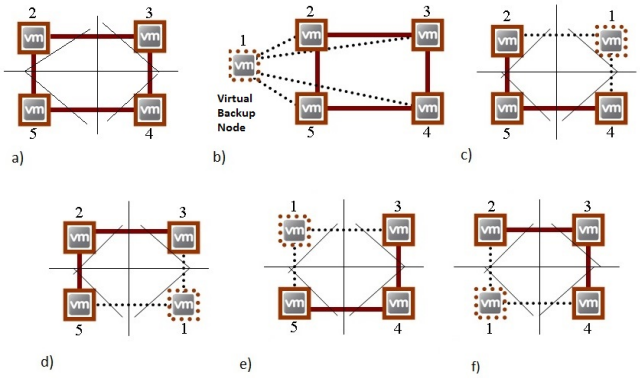

Fig. 5 Basic cuts, post-disaster cuts, and one VM backup location per CN. (a) CN with basic cuts, (b) CN with one VM backup location and (c - f) extended cuts for any replacement.

Step ii: ExCuts renumbers the basic cuts with virtual links of the resulting topology of Fig. 5(c). In Table 1, we show the basic and extended cuts of the resulting topology when VM 3 is disconnected and replaced by VM 1.

Step iii: ExCuts eliminates redundant cuts and repeats the three steps for each possible VM relocation of Fig. 5(c - f).

In this example, we consider only one datacenter for VM backup location. However, ExCuts will generate new cuts considering all possible VM relocation given a disaster failure.

4.2.2 Survivability constraint

The extended cuts are input to the novel survivability constraint which enforces survivable mapping against any post-

disaster single physical-link failure. The constraint applies the concept of cut-disjoint approach introduced in Section 3 but considering post-failure cuts to increase the post-disaster survivability. Figure 6 presents the cut extension of Fig. 5 for two VM backup locations.

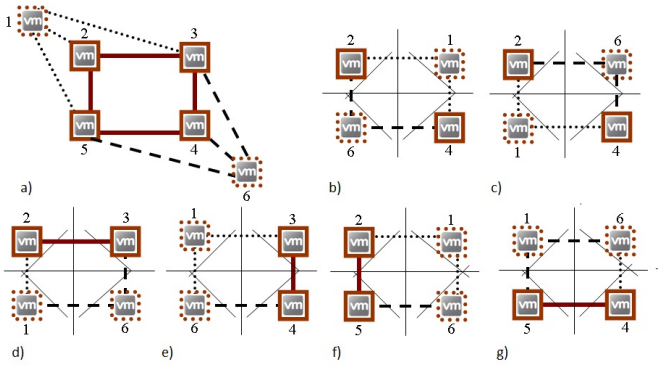

Fig. 6 Post-disaster cuts for two VM backup locations per CN. (a) CN with two VM backup locations, and (b - g) extended cuts for the replacement of the two failed VMs.

4.3 Example of Min-Risk-D-PDS Approach

In the mapping of Fig. 4(a), if a disaster, e.g., in DZ1, occurs, the physical node C and its physical links will fail, but the CN will not be disconnected, because the failed VM in node 2 will be relocated into physical node A (VM in node 1). However, a post-disaster failure in physical link A - B will disconnect the CN, because virtual links 1 - 5 and 1 - 4 will be disconnected. Similarly, failure of any of physical-links B - E, F - G, and E - G may disconnect the CN.

Min-Risk-D-PDS obtains the mapping in Fig. 7(a), where the CN will not be disconnected by *any* single physical-link failure, disaster failure, or post-disaster single physical-link failure, and the expected loss of bandwidth and processing capacity will be reduced.

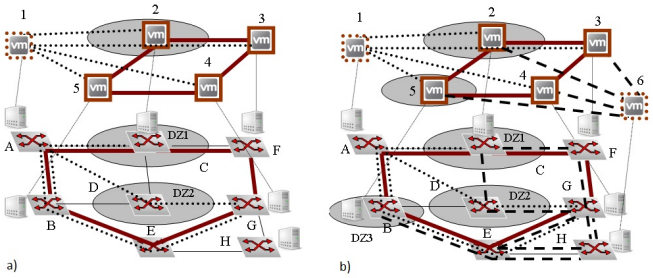

Fig. 7 Resulting mapping by Min-Risk-D-PDS with (a) one and (b) two VM backup locations.

5 ILP Formulation of Min-Risk-DS

In this section, we present the ILP formulation of the baseline approach Min-Risk-DS which has three elements: Min-Risk formulation, CN mapping, and survivability constraints. Before we describe the formulation, we introduce the parameters and variables of the problem.

5.1 Variables and Symbols

Given

- $G(V,E)$: Physical topology, where V is the set of physical nodes and E is the set of physical links.
- $\hat{V}$: Set of VM datacenter locations, $\hat{V} \subset V$.
- $G_\gamma(V_\gamma, E\gamma)$: Topology of CN γ where V_γ is the set of working VM locations (virtual nodes, $V_\gamma \subset \hat{V}$), and E_γ the set of virtual links of CN.
- C_γ: Set of basic cuts of CN topology γ.
- $\hat{E}_\gamma$: Set of virtual links including the links in E_γ and virtual links from each node in V_γ to each node in $\{\hat{V} - V_\gamma\}$
- $\hat{C}_\gamma$: Set of extended cuts of CN topology γ formed by a possible relocation of working VM of V_γ to a physical node b with free processing capacity in $\{\hat{V} - V_\gamma\}$.
- $\Gamma = \{\gamma = < V_\gamma, E_\gamma, C_\gamma, \hat{E}_\gamma, \hat{C}_\gamma, \}$: Set of cloud networks (CNs).
- $s^n_{i,j}$: 1 if the physical link $\{i,j\}$ is disconnected by disaster n, zero otherwise.
- S_n: $\left\{ s^n_{i,j}, \right\}$, $S_n \subset E$.
- p_n: Probability of occurrence of disaster n.
- $N = \{< S_n, p_n >\}$: Set of disasters zones (i.e., DZs).
- P^γ_u: Processing capacity required to allocate VM u used by CN γ ($u \in V_\gamma$).
- P^v_{free}: Excess processing capacity in physical node v.
- $F_{i,j}$: capacity of physical link (i,j).
- d: CN disconnection coefficient ($1 \geq d \leq 10$).
- b_e: Bandwidth requirement of virtual link e.
- b_c: Total capacity that can be lost if the links of the cut c are disconnected (i.e., the CN is disconnected).
- m_c: Number of virtual links in cut c.

Binary variables

- D^n_e: 1 if virtual link e is disconnected by disaster n.
- $M^e_{i,j}$: 1 if virtual link e is mapped on physical link (i,j).
- $K^{\gamma,e}_{u,v}$: 1 if virtual link e from node u to v in γ.
- Y^γ_b: 1 if b is assigned as as virtual backup node of γ.
- Q^n_c: 1 if virtual links of the cut c is disconnected by disaster n.
- X^n_γ: 1 if CN γ may be disconnected by disaster n.
- $T^n_{g,h}$: is an auxiliary variable.
- $Z^\gamma_{u,b}$: 1 if VM u can be relocated to datacenter b, $b \in \hat{V}$.

5.2 Min-Risk Formulation and Constraints

5.2.1 Objective function

The objective is to minimize the total capacity that can be lost if a disaster occurs. The risk as defined in Section 4 is the total penalty for capacity loss multiplied by the probability of occurrence. The total penalty for capacity lost is the sum of penalty for CN and virtual links' disconnections. The penalty for CN disconnection is calculated by $\sum_{c\in C_\gamma} dQ_c^n b_c$ which is the sum of capacity b_c that is lost if a CN is disconnected by disaster n multiplied by a CN disconnection coefficient d. The penalty for virtual-link disconnection is calculated by $\sum_{c\in C_\gamma} D_c^n b_e$ which is the sum of capacity b_e that is lost when virtual links e is disconnected by disaster n. Finally, the objective function is:

$$\min \sum_{n\in N}\sum_{\gamma\in\Gamma}\left(\sum_{c\in C_\gamma} dQ_c^n b_c + \sum_{e\in\hat{E}_\gamma} D_e^n b_e\right) p_n + \left(\varepsilon \times \sum_{(i,j)\in E}\sum_{\gamma\in\Gamma}\sum_{e\in\hat{E}_\gamma} M_{i,j}^e \times b_e\right) \tag{3}$$

To avoid the mapping of virtual links over long lightpaths, a resource-minimization formula is added with a coefficient ε. A very small value of ε will give more importance for risk minimization in the mapping over resources used.

5.2.2 Constraint to determine whether a virtual link is affected by a disaster

$$D_e^n \geq \frac{1}{M}\sum_{(i,j)\in E} s_{i,j}^n M_{i,j}^e,\ \forall e\in\hat{E}_\gamma, \gamma\in\Gamma, n\in N \tag{4a}$$

$$D_e^n \leq \sum_{(i,j)\in E} s_{i,j}^n M_{i,j}^e,\ \forall e\in\hat{E}_\gamma, \gamma\in\Gamma, n\in N \tag{4b}$$

where M is a large number.

5.2.3 Constraint to determine a CN disconnection (i.e., cut failure) due to a disaster

$$Q_c^n \leq \frac{\sum_{e\in E_c} D_e^n}{m_c},\ \forall c\in C_\gamma, \gamma\in\Gamma, n\in N \tag{5a}$$

$$Q_c^n \geq \sum_{e\in E_c} D_e^n - m_c + 1,\ \forall c\in C_\gamma, \gamma\in\Gamma, n\in N \tag{5b}$$

The CN is disconnected when the value of Q_c^n is 1, i.e., disaster n disconnects all the virtual links e (D_e^n) belonging to a cut c.

5.3 CN Mapping Constraints

The basic constraints used in the mapping are:

5.3.1 Virtual-link mapping constraint

$$K_{u,v}^{\gamma,e} = 1,\ \forall u,v\in V_\gamma, u\neq v, \gamma\in\Gamma, e\in\hat{E} \tag{6}$$

This constraint maps the CN γ, connecting the VMs u and v.

5.3.2 Flow-conservation constraints

$$\sum_{(i,s_e)\in E} M_{i,s_e}^e - \sum_{(s_e,j)\in E} M_{s_e,j}^e = -K_{s_e,d_e}^{\gamma,e} \tag{7a}$$

$$\sum_{(i,d_e)\in E} M_{i,d_e}^e - \sum_{(d_e,j)\in E} M_{d_e,j}^e = K_{s_e,d_e}^{\gamma,e} \tag{7b}$$

$$\sum_{(k,j)\in E} M_{k,j}^e - \sum_{(i,k)\in E} M_{i,k}^e = 0,\ \forall e\in\hat{E}_\gamma, \gamma\in\Gamma, k\in\hat{V}-\{s_e,d_e\} \tag{7c}$$

These constraints ensure that each virtual link is mapped on a lightpath, and it does not pass the same physical node more than once.

5.3.3 Physical-link capacity constraint

$$\sum_{e\in\hat{E}_\gamma} M_{i,j}^e \leq F_{i,j},\ \forall (i,j)\in E, \gamma\in\Gamma \tag{8}$$

5.4 Survivability Contraint

The survivability constraint uses the basic cuts of the CN topology C_γ. The constraint enforces that all links (m_c) of the cut c do not use the same physical link.

$$\sum_{e\in E_c} M_{i,j}^e \leq m_c - 1, \forall c\in C_\gamma, \gamma\in\Gamma, (i,j)\in E \tag{9}$$

6 ILP Formulation of Min-Risk-D-PDS

Min-Risk-D-PDS is our comprehensive approach which extends the ILP formulation of the baseline approach Min-Risk-DS by adding the VM backup location (VBL) and post-disaster survivability (PDS) constraints.

6.1 VBL Constraints

6.1.1 Disaster-disjoint VM backup location constraint

This set of constraints enforces that two or more CNs do not share the same physical node as VM backup location if the CNs are affected by the same disaster (Eqs. (10), (11), and (12)). Equation (10) identifies which disaster n disconnects the CN γ, giving value 1 to X^n_γ, 0 otherwise.

$$X^n_\gamma \geq \frac{1}{M}\sum_{c\in C_\gamma} Q^n_c,\ X^n_\gamma \leq \sum_{c\in C_\gamma} Q^n_c,\ \forall\gamma\in\Gamma, n\in N \tag{10}$$

Equation (11) uses the value of X^n_γ and an auxiliary variable $T^n_{g,h}$ to identify the disaster which disconnect CNs h and g.

$$T^n_{g,h} \leq X^n_g,\ T^n_{g,h} \leq X^n_h,\ \forall g,h\in\Gamma, g\neq h, n\in N \tag{11a}$$

$$T^n_{g,h} \geq X^n_g + X^n_h - 1,\ \forall g,h\in\Gamma, g\neq h, n\in N \tag{11b}$$

Equation (12) restricts two CNs (g and h) to share the same physical node (b) for VM backup location if both CNs are disconnected by the same disaster.

$$Y^g_b + Y^h_b \leq 2 - T^n_{g,h},\ \forall g,h\in\Gamma, g\neq h, n\in N, \quad b\in\left[\hat{V}-(V_g\cup V_h)\right] \tag{12}$$

6.1.2 Mapping of VM backup location constraint

This constraint gives the bound for the number of VM backup location per CN. It has two set of equations: VM backup location selection and bound on number of VM location per CN. Equation (13) chooses the less-risky VM backup location b for each CN γ. Equation (13a) ensures that the VM backup location b will not be chosen from the working VM V_γ of CN γ.

$$Y^\gamma_b = 0,\ \forall b\in V_\gamma, \gamma\in\Gamma \tag{13a}$$

$$Y^\gamma_b \geq \sum_{(u\in V_\gamma} \frac{Z^\gamma_{u,b}}{M}, \forall b\in(\hat{V}-V_\gamma), \gamma\in\Gamma, u\in E \tag{13b}$$

$$Y^\gamma_b \leq \sum_{u\in V_\gamma} Z^\gamma_{u,b}, \forall b\in(\hat{V}-V_\gamma), \gamma\in\Gamma \tag{13c}$$

Equation (14) bounds the number of VM backup location between 2 and certain maximum number.

$$\sum_{b\in(\hat{V}-V_\gamma)} Y^\gamma_b \geq 2,\quad \sum_{b\in(\hat{V}-V_\gamma)} Y^\gamma_b \leq |V_\gamma|, \forall\gamma\in\Gamma \tag{14}$$

6.1.3 Connecting the VM backup node for relocation

When VM backup location is selected, virtual links connect it to working VMs (Eq. (15)). The connection follows two conditions:

(i) When one or more VMs chose a VM backup location. In this regard, $Z^\gamma_{v,b}$ is 1, meaning that working VM used by CN in physical node v chose to be relocated to physical node b. As a result, the variable $K^{\gamma,e}_{v,b}$ will be 1, forcing the mapping of virtual link e into the physical network.

(ii) When the VM backup location mapped in b is already connected to v, ($K^{\gamma,e}_{v,b}$ = 1), and the VM in physical node u is neighbor of v. Hence, a virtual link connects one working VM u with a VM backup location b of the same CN ($K^{\gamma,e}_{u,b}$ = 1).

$$K^{\gamma,e}_{u,b} \leq Z^\gamma_{v,b}, K^{\gamma,e}_{u,b} \leq K^{\gamma,e}_{v,u}, K^{\gamma,e}_{u,b} \geq Z^\gamma_{v,b} + K^{\gamma,e}_{v,u} - 1 \tag{15a}$$

$$K^{\gamma,e}_{u,b} = Z^\gamma_{v,b}\ \forall v,u\in V_\gamma, (b\in(\hat{V}-V_\gamma), \gamma\in\Gamma \tag{15b}$$

6.2 Processing Capacity Required for VM Backup Location

This constraint manages the free capacity of each physical node used for VM backup location. If P^b_{free} is zero, the physical node (Y^γ_b=0) cannot be used (e.g., the required capacity of the CN (P^γ_u) is higher or the free capacity (P^b_{free}) is not enough.

$$P^b_{free} - \sum_{u\in V_\gamma} P^\gamma_u . Y^\gamma_b \geq 0 \tag{16}$$

6.3 PDS Constraint

PDS uses the same formulation presented in Eq. (9) with the extended cuts $\hat{C}^\gamma_b$ as additional input.

7 Illustrative Examples

7.1 Experimental Setup

We test our approaches on a 24-node US mesh opaque WDM optical network (Fig. 8(b)) with 32 wavelengths per link. Two types of disasters are considered: natural disasters (earthquake), and human-made disasters (weapons-of-mass-destruction (WMD) attacks), originally modeled in [17] and shown in Fig. 8(b). For earthquakes, the probability of occurrence and damage are obtained with seismic hazard maps. And for WMD attacks, the probability of attack and damage are based on cities population and importance [17].

We consider five full-mesh cloud networks (CNs), each consisting of four virtual nodes (i.e., VMs) distributed over 16 datacenters (Fig. 8(a)). We assume that each virtual link requires a full lightpath (i.e., wavelength channels), and each datacenter has enough processing capacity.

7.2 Survivable CN Mapping Approaches

We tested eight approaches: four minimizing resources (Min-Res) and four minimizing risk (Min-Risk). All approaches use a set of baseline survivability constraints (SC).

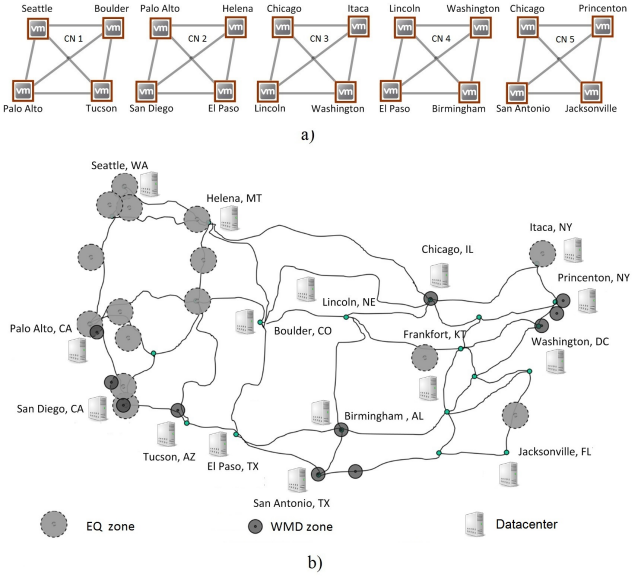

Fig. 8 (a) CNs studied and (b) physical topology with disaster zones for earthquake and potential WMD attacks [17], and datacenter locations.

Table 2 Approaches used in illustrative examples

Name	Approach	PDS	VBL	Cuts
RESA	Min-Res			Basic
RISKA	Min-Risk-DS			Basic
RESA-1L	Min-Res-DS-1L		1L	Basic
RISKA-1L	Min-Risk-DS-1L		1L	Basic
RESA-PDS	Min-Res-D-PDS	X	1L	Extended
RISKA-PDS	Min-Risk-D-PDS	X	1L	Extended
RESA-2L	Min-Res-D-PDS-2L	X	2L	Extended
RISKA-2L	Min-Risk-D-PDS-2L	X	2L	Extended

Some of them use a disaster survivable mapping (DS), disaster and post-disaster survivable constraints (D-PDS), and VM backup location (VBL) with number of backup location: one (1L) or two (2L). Min-Res-DS-1L indicates minimization of resources, disaster survivable mapping with 1 VM backup location which we call RESA-1L. The list of approaches is presented in Table 2 including our proposed approaches.

7.3 Evaluation and Comparative Methodologies

Our examples are evaluated using risk and penalty, disaster and post-disaster survivability, and resource usage analysis.

7.3.1 Risk and penalty

The risk of CN disconnection is evaluated using the first part of Eq. (3). The penalty for capacity loss is the total capacity that can be lost due to a disaster.

Table 3 Simulated failures

			Post-disaster failures	
Symbols	Description	Disaster	Physical link/s	Disaster
DF	Any single disaster occurs	Single	-	-
DSLF	One physical link fails after a disaster	Single	Single	-
DDLF	Two physical links fail after a disaster	Single	Dual	-
DFDF	Second disaster occurs after a disaster	Single	-	Single

7.3.2 Disaster and post-disaster survivability analysis

The second analysis is the evaluation of the probability of CN disconnection (PoD). The PoD is calculated by an algorithm called cloud-network resiliency test algorithm (CNRT) which tests the vulnerability of the CN to all possible combinations of disaster and post-disaster failures. CNRT gets the mapping of each CN and simulates disaster damage over the physical infrastructure based on given disaster scenarios (Table 3). Then, the algorithm tests the connectivity of every VM and counts the number of possible failure scenarios caused by a disaster in which the CN is disconnected. With these numbers, CNRT obtains one PoD for each CN and type of failure using Eq. (17).

$$PoD = \frac{Total\ Number\ CN\ Disconnection}{Total\ Number\ of\ Possible\ Failures} \tag{17}$$

7.4 Numerical Analysis

To study the risk and penalty, we use the mapping of the five CNs presented in Fig. 8(a). However, we select CN 1 for earthquake and CN 3 for WMD to study the disaster and post-disaster scenarios, as these two CNs are more affected by the disasters.

7.4.1 Risk and penalty analysis

Figure 9 compares the expected risk of CN disconnection of different approaches. In Fig. 9 we observe that:

(i) RISKA approach reduces the risk of CN disconnection and penalty by 2.75% to 3.77%. These results shows a low risk reduction without VBL constraint, and the limitation of SVNM based approaches to deal with disaster and post-disaster failures.

(ii) By adding the VM backup location (VBL), RISKA-1L approach reduces the risk of CN disconnection and penalty up to 87% for earthquake, and up to 88% for WMD. Also, RESA-1L approach reduces risk up to 85% for earthquake, and up to 87% for WMD. It confirms that VBL approach reduces considerably the CN disconnection and penalty for capacity loss. However, VBL works better with RISKA (risk and penalty reduction by 10% to 30%).

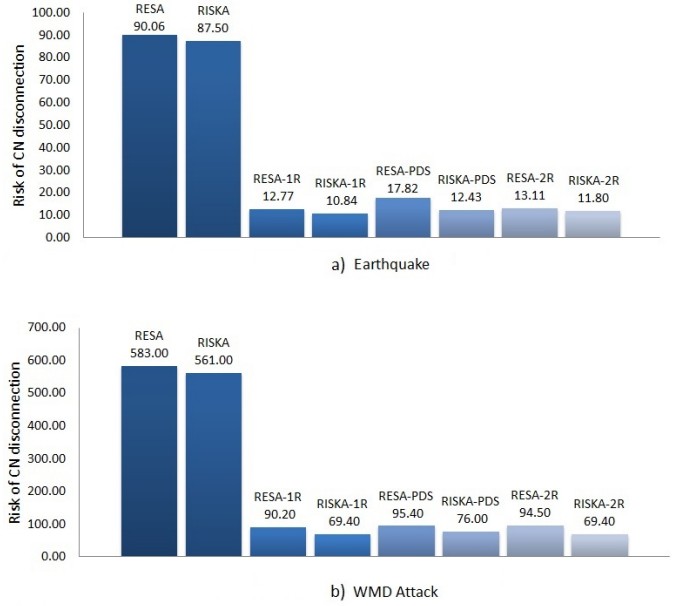

Fig. 9 Risk of CN disconnection (a) earthquake and (b) weapon of mass destruction (WMD).

(iii) PDS constraint slightly increases the risk because the extended cuts force virtual links to be mapped in longer lightpaths. However, PDS constraint increases survivability against post-disaster failures by 60% to 100% (Table 4).

(iv) The combination of PDS and VBL with two VM backup locations per CN obtains more reduction in risk and penalty. However, the risk and penalty reduction tend to be lower in earthquake case and higher for WMD for one VM backup location per CN.

7.4.2 Disaster and post-disaster survivability study

After risk and penalty analysis, we study the probability of disconnection (PoD) due to a disaster failure and three kind of post-disaster failures presented in Table 3.

Table 4 presents the PoD of CN 1 and CN 3. We observe that:

(i) DF: CNs with VBL will completely survive any failure as any VM can be relocated from one datacenter to another i.e., PoD = 0. In addition, RISKA approach increases the survivability by 50% in WMD case compared to RESA approach.

(ii) DSLF: RISKA approach reduces PoD by 0% to 22% compared to RESA approach. And, RISKA-1L (i.e., with VBL) increases the survivability by 37% to 100% compared to RESKA-based approaches. PDS constraint increases the survivability to 100% independent of the number of VM backup locations and the objective function (RISKA or RESA).

(iii) DDLF: RISKA achieves a reduction of PoD by 2.3% in WMD case and 16% in earthquake case compared to RESA. However, when VBL is used, the reduction of PoD is higher (between 24% and 64%). PDS constraint has positive impact, because the reduction is higher for RISKA-PDS compared to other approaches without PDS constraints.

(iv) DFDF: VBL reduces the PoD remarkably by 78% to 100%. Also, including PDS constraint with RISKA-based approach does not enhance the performance significantly. However, RESA-based approaches with PDS achieve an important reduction of 33% in PoD.

Table 4 Probability of Disconnection (PoD)

Approach	CN 1 - Earthquake		CN 3 - WMD attack	
	DF	DSLF	DF	DSLF
RESA	0.27	0.45	0.18	0.38
RISKA	0.27	0.35	0.09	0.38
RESA-1L	0	0.30	0	0.29
RISKA-1L	0	0.26	0	0.20
RESA-PDS	0	0	0	0.14
RISKA-PDS	0	0	0	0
RESA-2L	0	0	0	0
RISKA-2L	0	0	0	0
	DDLF	DFDF	DDLF	DFDF
RESA	0.50	0.52	0.42	0.35
RISKA	0.42	0.49	0.41	0.22
RESA-1L	0.38	0.19	0.35	0.04
RISKA-1L	0.35	0.11	0.24	0.02
RESA-PDS	0.35	0.13	0.17	0
RISKA-PDS	0.20	0.13	0.15	0
RESA-2L	0.23	0.01	0.17	0
RISKA-2L	0.20	0	0.15	0

7.4.3 Resource consumption analysis

In this analysis, we study the resources used to provide reduction in risk, penalty for capacity loss, and PoD. From the previous analysis and the results of Fig. 10, we observe that:

(i) RISKA-based approaches require additional resources by 7.8% to 16% to reduce the risk and penalty and PoD. RISKA with VBL constraints increases resource usage by 16% to 37% for one VM backup location (RISKA-1L) to provide risk and penalty reduction by 85% to 87%, and a reduction of the PoD by 24% to 100% (i.e., increasing the survivability by 24% to 100%). This results confirms that SVNM cannot deal with disasters and their consequences.

(ii) PDS constraint with RISKA and VM backup location (RISKA-PDS) increase the resources by 25% to 50% in CN 1 (earthquake) and by 23% to 38% for CN 3 (WMD). However, the risk and penalty are reduced up to 88%, and the survivability increase up to 100% in cases of disaster and post-disaster failures.

(iii) Two VM backup locations require more resources, but increase the survivability for more severe disaster scenarios which may disconnect two VMs.

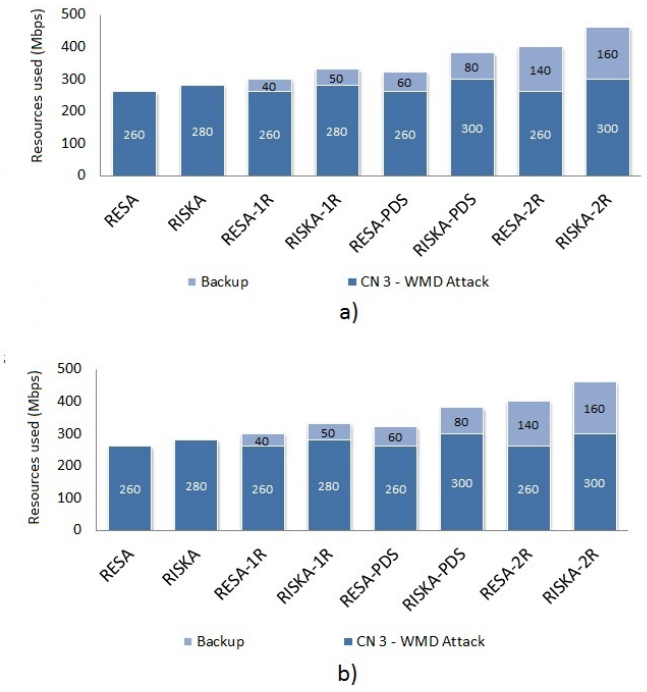

Fig. 10 Resources used (in Mbps) by the mapping of (a) CN 1 in earthquake case (b) CN 3 in WMD case.

8 Conclusion

We studied the disaster and post-disaster survivable cloud-network (CN) mapping problem. We proposed a CN mapping approach Min-Risk-D-PDS using (i) VM backup location for each CN (VBL) and (ii) post-disaster survivability constraint (PDS), which offer an economically-sustainable disaster and post-disaster survivable CN mapping approach.

We formulated the Min-Risk-D-PDS as an integer linear program. We compared our approach with seven different approaches characterized by different combinations of VBL and PDS constraints with risk and resources minimization as objective function.

Results on a case study formed by five CNs mapped over a US network and two disaster cases (earthquake and WMD) showed that Min-Risk-D-PDS (RISKA-PDS) reduces the risk of CN disconnections and penalty for capacity loss by 85% to 90%. As a consequence, our approach increases the CN survivability by 60% and 100% against three kind of post-disaster failures with the cost of 23% to 50% of additional resources usage.

Hence, our illustrative examples confirm the importance of VM backup location and post-disaster survivability constraints for CN survivability against any disaster and post-disaster correlated, cascading failures that may occur in the network.

References

1. C. Colman M., F. Dikbiyik, M. Tornatore, C. Chuah, and B. Mukherjee, "Disaster-resilient virtual-network mapping and adaptation in optical networks," in *17th International Conference on Optical Network Design and Modeling (ONDM)*, Brest, France, Apr. 2013.
2. C. Develder, M. De Leenheer, B. Dhoedt, M. Pickavet, D. Colle, F. De Turck, and P. Demeester, "Optical Networks for Grid and Cloud Computing Applications," *Proceedings of the IEEE*, vol. 100, no. 5, pp. 1149–1167, May 2012.
3. L. Contreras, V. Lopez, O. De Dios, A. Tovar, F. Munoz, A. Azanon, J. Fernandez-Palacios, and J. Folgueira, "Toward cloud-ready transport networks," *IEEE Communication Magazine*, vol. 50, no. 9, pp. 48–55, Sep. 2012.
4. J. C. Mogul and L. Popa, "What we talk about when we talk about cloud network performance," *SIGCOMM Computer Communication Review*, vol. 42, no. 5, pp. 44–48, Sep. 2012.
5. B. P. Rimal, E. Choi, and I. Lumb, "A taxonomy and survey of cloud computing systems," in *Proc. IEEE International Joint Conference on INC, IMS and IDC*, Washington, DC, USA, Aug. 2009.
6. I. Abbadi, "Clouds infrastructure taxonomy, properties, and management services," *Springer, Advances in Computing and Communications*, vol. 193, pp. 406–420, Jun. 2011.
7. G. Sun, H. Yu, V. Anand, L. Li, and H. Di, ""optimal provisioning for virtual network request in cloud-based data centers"," *Elsevier, Photonic Network Communications*, vol. 24, no. 2, Oct. 2012.
8. S. Kounev, P. Reinecke, F. Brosig, J. T. Bradley, K. Joshi, V. Babka, A. Stefanek, and S. Gilmore, "Providing dependability and resilience in the cloud: Challenges and opportunities," *Springer, Resilience Assessment and Evaluation of Computing Systems*, pp. 65–81, 2012.
9. N. Chowdhury, M. Rahman, and R. Boutaba, "Virtual network embedding with coordinated node and link mapping," in *Proc. IEEE International Conference on Computer Communications (INFOCOM)*, Rio de Janeiro, Brazil, Apr. 2009.
10. M. Habib, M. Tornatore, M. De Leenheer, F. Dikbiyik, and B. Mukherjee, "Design of disaster-resilient optical datacenter networks," *IEEE/OSA Journal of Lightwave Technology*, vol. 30, no. 16, pp. 2563–2573, Aug. 2012.
11. F. Gu, H. Alazemi, A. Rayes, and N. Ghani, "Survivable cloud networking services," in *Proc. IEEE International Conference on Computing, Networking and Communications (ICNC)*, San Diego, USA, Jan. 2013.
12. H. Yu, V. Anand, and C. Qiao, "Virtual infrastructure design for surviving physical link failures," *The Computer Journal, Oxford University Press*, vol. 55, no. 8, pp. 965–978, Aug. 2012.
13. J. Xu, J. Tang, K. Kwiat, W. Zhang, and G. Xue, "Survivable virtual infrastructure mapping in virtualized data centers," in *Proc. IEEE Cloud Computing Conference (CLOUD)*, Honolulu, Hawaii, USA, June 2012.
14. M. F. Habib, M. Tornatore, F. Dikbiyik, and B. Mukherjee, "Disaster survivability in optical communication networks," *Elsevier, Computer Communications*, vol. 36, no. 6, pp. 630 – 644, Mar. 2013.
15. S. Carew, "Hurricane Sandy disrupts Northeast U.S. Telecom Networks," *Reuters*, Oct. 2012. [Online]. Available: http://uk.reuters.com/article/2012/10/30/us-storm-sandy-telecommunications-idUKBRE89T0YU20121030
16. N. Henderson, "Noise Filter: Hurricane Sandy Floods NYC Data Center, Impacts Hosts, Colocation Providers," *WebHost Industry Review*, Oct. 2012. [Online]. Available: http://www.thewhir.com/web-hosting-news/noise-filter-hurricane-sandy-floods-nyc-data-center-impacts-hosts
17. F. Dikbiyik, M. D. Leenheer, A. Reaz, and B. Mukherjee, "Minimizing the disaster risk in optical telecom networks," in *Proc.*

IEEE/OSA Optical Fiber Communication Conference (OFC), Mar. 2012.
18. N. Chowdhury and R. Boutaba, "A survey of network virtualization," *Elsevier, Computer Networks*, vol. 54, no. 5, pp. 862 – 876, Apr. 2010.
19. M. Rahman, I. Aib, and R. Boutaba, "Survivable virtual network embedding," in *NETWORKING 2010*, ser. Lecture Notes in Computer Science, M. Crovella, L. Feeney, D. Rubenstein, and S. Raghavan, Eds. Springer Berlin / Heidelberg, May 2010, vol. 6091, pp. 40–52.
20. T. Guo, N. Wang, K. Moessner, and R. Tafazolli, "Shared backup network provision for virtual network embedding," in *Proc. IEEE International Conference on Communications (ICC)*, Kyoto, Japan, June 2011.
21. K. Lee, E. Modiano, and H. Lee, "Cross-layer survivability in WDM based networks," *IEEE/ACM Transaction in Networking*, vol. 19, no. 6, pp. 1000–1013, Dec. 2011.
22. C. S. Vadrevu and M. Tornatore, "Survivable ip topology design with re-use of backup wavelength capacity in optical backbone networks," *Elsevier, Optical Switching and Networking*, vol. 7, no. 4, pp. 196 – 205, Dec. 2010.
23. B. Jaumard, A. Hoang, and M. Bui, "Path vs. cutset approaches for the design of logical survivable topologies," in *Proc. IEEE International Conference on Communications (ICC)*, Ottawa, Canada, June 2012.
24. H. Yu, V. Anand, C. Qiao, and G. Sun, "Cost efficient design of survivable virtual infrastructure to recover from facility node failures," in *Proc. IEEE International Conference on Communications (ICC)*, Kyoto, Japan, June 2011.
25. Q. Hu, Y. Wang, and X. Cao, "Survivable network virtualization for single facility node failure: A network flow perspective," *Elsevier, Optical Switching and Networking*, vol. 10, no. 4, pp. 406 – 415, Nov. 2013.
26. C. Develder, J. Buysse, A. Shaikh, B. Jaumard, M. De Leenheer, and B. Dhoedt, "Survivable optical grid dimensioning: Anycast routing with server and network failure protection," in *Proc. IEEE International Conference on Communications (ICC)*, Kyoto, Japan, June 2011.
27. M. Bui, B. Jaumard, and C. Develder, "Anycast end-to-end resilience for cloud services over virtual optical networks (invited)," in *Proc. 15th International Conferent Transparent Optical Networks (ICTON)*, Cartagena, Spain, June 2013.
28. I. Barla, D. Schupke, M. Hoffmann, and G. Carle, "Optimal design of virtual networks for resilient cloud services," in *Proc. 9th International Conference on the Design of Reliable Communication Networks (DRCN)*, Budapest, Hungary, Mar. 2013.