Computer Networks 103 (2016) 56–66

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Probabilistic region failure-aware data center network and content placement☆

Lisheng Ma[a,b], Xiaohong Jiang[a], Bin Wu[c,*], Achille Pattavina[d], Norio Shiratori[e,f]

[a] School of Systems Information Science, Future University Hakodate, 116-2, Kameda Nakano-Cho, Hakodate, Hokkaido 041-8655 Japan
[b] School of Computer and Information Engineering, Chuzhou University, Chuzhou 239000, PR China
[c] School of Computer Science and Technology, Tianjin University, Tianjin 300072, PR China
[d] Department of Electronics and Information, Politecnico di Milano, Piazza Leonardo da Vinci 32, 20133 Milano, Italy
[e] GITS, Waseda University, Tokyo 169-0051, Japan
[f] RIEC, Tohoku University, Sendai-shi 980-8579, Japan

ARTICLE INFO

Article history:
Received 12 October 2015
Revised 8 February 2016
Accepted 22 March 2016
Available online 6 April 2016

Keywords:
Data center networks (DCNs)
Failure probability
Region failure
Placement

ABSTRACT

Data center network (DCN) and content placement with the consideration of potential large-scale region failure is critical to minimize the DCN loss and disruptions under such catastrophic scenario. This paper considers the optimal placement of DCN and content for DCN failure probability minimization against a region failure. Given a network for DCN placement, a general probabilistic region failure model is adopted to capture the key features of a region failure and to determine the failure probability of a node/link in the network under the region failure. We then propose a general grid partition-based scheme to flexibly define the global nonuniform distribution of potential region failure in terms of its occurring probability and intensity. Such grid partition scheme also helps us to evaluate the vulnerability of a given network under a region failure and thus to create a "vulnerability map" for DCN and content placement in the network. With the help of the "vulnerability map", we further develop an integer linear program (ILP)-based theoretical framework to identify the optimal placement of DCN and content, which leads to the minimum DCN failure probability against a region failure. A heuristic is also suggested to make the overall placement problem more scalable for large-scale networks. Finally, an example and extensive numerical results are provided to illustrate the proposed DCN and content placement.

1. Introduction

Data center networks (DCNs), which consist of hundreds or even thousands of servers and massive storage resources, are becoming increasingly important infrastructures to support the wide spreading cloud computing services [1,2]. In general, DCN design involves the issues of DCN and content placement, path and content/service protection, QoS guarantee, etc. This paper focuses on the DCN and content placement. The DCN placement can be roughly divided into two categories, to place the components of a DCN at different nodes of a given network [3], or to place multiple DCNs at different nodes of a given network [4,5]. This paper concerns the latter.

It is notable that DCNs are facing more and more potential large-scale disaster threats, both natural and human-made. Some recent major network disruptions due to disasters include 2012 Sandy Hurricane, 2011 Japan Tsunami, 2008 China Wenchuan earthquake, etc. [6–12]. Such disasters usually affect a specific geographical region, causing failures of a set of network components and degradations or even breakdowns of vital network services [13]. For instance, China Wenchuan earthquake in 2008 leads to the damages of more than 3000 telecom offices and around 30,000 km optic cables [8]. Thus, the study of DCN and content placement with the consideration of region failure is critical for DCN designers to take proactive measures against the region failure in the DCN design phase.

Given a network, the placement of DCN and content in the network with the consideration of potential region failure usually concerns with the following two aspects: (1) to assess the network vulnerability due to a region failure; (2) based on the network vulnerability information, to properly place the DCN and content in the network such that the DCN failure probability due to region failure is minimized. Some works are available on the assessment

☆ This work partially appeared in the HPSR 2015 conference.

* Corresponding author.
E-mail addresses: mls@chzu.edu.cn (L. Ma), jiang@fun.ac.jp (X. Jiang), binwu.tju@gmail.com (B. Wu), pattavina@elet.polimi.it (A. Pattavina), norio@Shiratori.riec.tohoku.ac.jp (N. Shiratori).

http://dx.doi.org/10.1016/j.comnet.2016.03.008
1389-1286/

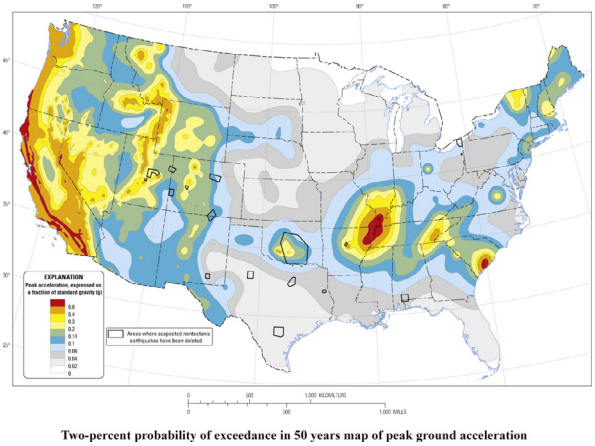


Fig. 1. U.S. national seismic hazard map.

of network vulnerability and identification of vulnerable network zones due to region failure [14–18]. Based on the deterministic circular/line cut region failure models, the network vulnerability assessments are conducted in [14,15]. In [16] and [17], a probabilistic failure model and grid partition based framework are developed to efficiently estimate the network vulnerability. Recently, network vulnerability assessment with the consideration of multiple simultaneous probabilistic failures is investigated in [18]. It is notable that the above works on network vulnerability assessment all assume that both occurring probability and intensity of region failure(s) follow the uniform distribution in the network area. As illustrated in Fig. 1 for U.S. national seismic hazard map [19], we can observe that in the real world, however, a disaster may happen in different areas with different probabilities and different intensities.

Regarding the DCN and content placement with the consideration of potential network failure(s), Xiao et al. [5] study the optimal DCN placement problem with service routing and protection to minimize the network cost, while ensuring fast protection of all services against any single link failure or service failure at a particular DCN. By assuming multiple region failures in fixed locations, the work in [20] concerns with the joint design of content placement, routing, and protection of paths and contents to achieve more efficient protection of optical DCNs than dedicated single-link failure protection, while the work in [21] investigates the DCN and content placement to minimize both the DCN contents unavailability due to DCN hosting nodes damage and requests unreachability due to paths damage from disasters.

Notice that two limitations of above works on DCN and content placement are that they failed to take into account the global nonuniform distribution of potential disasters in terms of their locations and intensities, and they also did not consider the inherent tradeoff between failure probabilities of DCN hosting nodes and failure probabilities of requesting paths (e.g. paths between content requesting nodes and DCN hosting nodes). In a large-scale network there are multiple paths between an arbitrary pair of nodes, which indicates that the probability that these paths simultaneously fail due to disaster is very small. In contrast, if a DCN hosting node fails after disaster, the contents provided by this node will be unavailable and the adverse impact of such failure on the DCN is even greater than the path failure. Thus, the tradeoff between failure probabilities of DCN hosting nodes and failure probabilities of requesting paths should be considered. Also, since content or service providers in DCNs wish to satisfy user demands with low latency, we need to consider the traffic transmission delay issue as well in the DCN design.

To address the above limitations, this paper combines the probabilistic region failure model and grid partition scheme to capture the key features of the general nonuniform distribution of a potential disaster in terms of its location and intensity, and then apply them to conduct the network vulnerability assessment. Based on the vulnerability information of a given network for DCN and content placement, an optimal DCN and content placement scheme is proposed with the consideration of the tradeoff among failure probabilities of DCN hosting nodes, failure probabilities of requesting paths and traffic transmission delay. In our work, DCN placement is static, which is implemented at the network planning stage for only once. However, since the information on disaster and content properties (e.g. content request) is time-varying, content placement can be adjusted when the information on disaster and content properties is updated. In general, content placement can be optimized either periodically according to daily content requests variation, or within the early warning time of an upcoming disaster if the DCN failure risk is observed higher than the current risk evaluation. The main contributions of our work can be summarized as follows.

- We first propose a general grid partition-based scheme to evaluate the vulnerability of a given network due to the global nonuniform distribution of a region failure, in which the probabilistic region failure model is applied to determine the failure probability of a node/link. Then we can create a vulnerability map for DCN and content placement in the network.
- Based on the grid partition-based scheme and the corresponding vulnerability map , we develop an integer linear program (ILP)-based theoretical framework to achieve optimal placement of DCN and content, which leads to minimum DCN failure probability against a region failure. To make the scheme more scalable for large-scale networks, a heuristic is proposed by dividing the problem into two subproblems (i.e., DCN placement and content placement).
- Extensive numerical experiments are carried out based on the real gridded data of U.S. national seismic hazard map [22] to demonstrate our proposed network vulnerability assessment scheme and to validate the efficiency of the proposed ILP and heuristic for DCN and content placement under nonuniform spatial and intensity distribution of a potential disaster.

The rest of the paper is organized as follows. Section 2 introduces the scheme for network vulnerability evaluation. The ILP for optimal DCN and content placement and the corresponding heuristic are presented in Sections 3 and 4, respectively. We provide the numerical results in Section 5, and conclude this paper in Section 6.

2. Network vulnerability evaluation

We consider a network with deployment area Z and denote it as a graph $G = (V, E)$, where V is a set of nodes and E is a set of network links.

2.1. Probabilistic region failure model

A real-world disaster (or attack) is usually confined in a specific geographical region. A network component (like a link or node) in this disaster region will fail with certain probability, and such a failure probability depends on the intensity of failure, the distance to failure center and also the dimension of the component (such as the length of a link). To capture these key features of a region failure, we adopt the general probabilistic region failure (PRF) model proposed in [17].

- ***PRF model definition*:**

(1) As illustrated in Fig. 2, the PRF is defined by a set of consecutive concentric annuluses with radius $r_i, i = 1, \ldots, m$.

(2) The ith annulus is associated with failure probability p_i, and such probability is monotonously decreasing with annulus, i.e., $p_i \geq p_{i+1}$, $1 \leq i \leq m-1$. Here, the region failure is only confined within the circle area of radius r_m, beyond which the failure probability is regarded as 0.

It is notable that under a probabilistic region failure, multiple network components (e.g. nodes and links) may simultaneously fail, but with a certain probability for each. In this paper we evaluate failure probabilities of node and link separately without any dependency between the two. Since failure probability evaluations of nodes and links are different from each other as follows, the proposed approaches can properly handle various scenarios.

Based on the PRF model, the failure probability P_v for a node v in the ith annulus can be formulated as

$$P_v = p_i. \tag{1}$$

In general, a link spans multiple annuluses of a region failure, and each annulus contains a segment of the link. Then, failure probability of the link is determined by that of all those segments. Therefore, the failure probability P_l for a link l can be formulated as

$$P_l = 1 - \prod_{i=1}^{m}(1 - P_{l_i}), \tag{2}$$

where m is the number of annuluses in the PRF model and P_{l_i} is the failure probability of segment l_i on link l that falls into the ith annulus.

Consider a segment l_i on link l that falls into the ith annulus. We first divide such a segment into multiple shorter segments, and each of them is approximated as a node to evaluate the failure probability of l_i. Then, the failure probability P_{l_i} for l_i can be formulated as

$$P_{l_i} = 1 - (1 - p_i)^{\frac{|l_i|}{\xi}}, \tag{3}$$

where ξ is a pre-defined factor representing the length of the shorter segment and $|l_i|$ represents the length of segment l_i. Note that in a practical fiber-optical network, each fiber link has a set of amplifiers. Generally, a link failure is mainly caused by failures of those amplifiers. Similar to [18], we can equivalently treat a segment on a particular link as a sequence of amplifiers, with each approximated as a node to evaluate its failure probability. This explains Eq. (3).

For example in Fig. 2, the failure probabilities of segments on link l are evaluated as

$$\begin{aligned} P_{l_1} &= 1 - (1 - p_1)^{\frac{|l_1|}{\xi}}, \\ P_{l_2} &= 1 - (1 - p_2)^{\frac{|l_2|}{\xi}}, \\ P_{l_3} &= 1 - (1 - p_3)^{\frac{|l_3|}{\xi}}, \end{aligned} \tag{4}$$

where

$$|l_2| = |l_{2a}| + |l_{2b}|, |l_3| = |l_{3a}| + |l_{3b}|. \tag{5}$$

Based on link failure probability, failure probability P_r for a path r can be formulated as

$$P_r = 1 - \prod_{l \in r}(1 - P_l), \tag{6}$$

where P_l is the failure probability of a link l on path r.

2.2. Vulnerability metrics

To evaluate the vulnerability of a network, we consider the following two vulnerability metrics:

- **NFP (node failure probability):** The probability that a node fails due to a PRF.

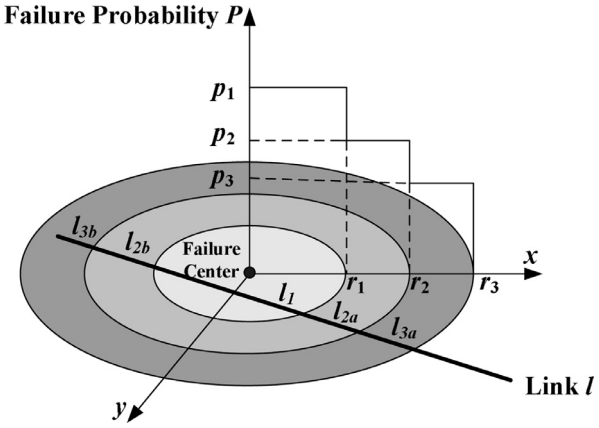


Fig. 2. Probabilistic region failure model, m=3.

Fig. 3. A grid partition for U.S. InternetMCI network.

- **LFP (link failure probability):** The probability that a link fails due to a PRF.

For a given network, one straight-forward approach to assessing the vulnerability of a metric $\triangle$ is to first partition the overall network area into some disjoint region failure location (RFL) zones.

- ***RFL zone definition*:** An RFL zone for a specified metric $\triangle$ (e.g. NFP or LFP) is a network subarea that any PRF with center in it will always induce the same value of $\triangle$ to the network.

For a specified metric $\triangle$, suppose that we have already divided the network deployment area Z into a set of disjoint RFL zones Z_n, where a PRF in Z_n induces the value $\triangle_{Z_n}$ of $\triangle$ to the network. Then the overall metric $\triangle$ can be calculated as

$$\triangle = \sum_{Z_n} P_{Z_n} \cdot \triangle_{Z_n}. \tag{7}$$

Here, P_{Z_n} denotes the probability that a PRF falls within the RFL zone Z_n.

It is notable that to directly apply (7) for calculating a metric $\triangle$, we first need to find out all RFL zones of the metric, which involves the complicated geometric computation and quickly becomes computationally intractable for a large-scale network [16,17]. In the following section, we propose a general grid partition-based scheme, which helps us to flexibly define the nonuniform distribution of PRF and to efficiently estimate the vulnerability of a network.

2.3. Grid partition-based vulnerability estimation

As illustrated in Fig. 3 for U.S. InternetMCI network [23], we apply a grid partition scheme to evenly divide the network area Z into M small square cells. Based on this grid partition scheme, if we regard each cell as an "RFL" zone and take the center point of the cell as the failure center to calculate the metric $\triangle$, then we can

get an estimation of metric $\triangle$ based on (7). Since the intensity of a disaster may be different in different regions, a PRF with center falling within different cells may have different parameters of r_i and p_i.

If we use (x_{Z_n}, y_{Z_n}) to denote the center point of cell Z_n, with the help of the grid partition scheme the estimations of NFP and LFP are summarized as Algorithms 1 and 2, respectively. Here, the number of square cells M, PRF model parameters Z_n^{para} and the probability P_{Z_n} that a PRF falls within the zone Z_n can be determined according to the information of real disaster data, such as the gridded data of U.S. national seismic hazard map [22].

It is notable that the grid partition scheme can also help us to create a "vulnerability map" of a given network, in which the NFP for each node and LFP for each link in the network are illustrated. For example, for the network shown in Fig. 3, its "vulnerability map" is shown in Fig. 4 (See Table 1 for link information and Section 5.1 for related parameter settings). Such "vulnerability map" will be helpful for identifying the optimal placement of DCN and content in the network to lead to the minimum DCN failure probability.

Algorithm 1 NFP evaluation.

Input:
Network topology information, a set of nodes V and failure model parameters.

Output:
NFP: $\triangle_{NFP_v}$ evaluation for node $v \in V$.

```
for each node v in V do
    △_NFPv = 0;
    for n ∈ [1, 2, ..., M] do
        calculate NFP △^v_Zn for v by using (x_Zn, y_Zn) as the center
        point of concentric circles in PRF model with parameters
        Z_n^para;
        △_NFPv = △_NFPv + P_Zn · △^v_Zn;
    end for
end for
return △_NFPv, v ∈ V.
```

Algorithm 2 LFP evaluation.

Input:
Network topology information, a set of links E and failure model parameters.

Output:
LFP: $\triangle_{LFP_l}$ evaluation for link $l \in E$.

```
for each link l in E do
    △_LFPl = 0;
    for n ∈ [1, 2, ..., M] do
        calculate LFP △^l_Zn for l by using (x_Zn, y_Zn) as the center
        point of concentric circles in PRF model with parameters
        Z_n^para;
        △_LFPl = △_LFPl + P_Zn · △^l_Zn;
    end for
end for
return △_LFPl, l ∈ E.
```

3. ILP for DCN and content placement

With the help of the "vulnerability map" of a given network, we consider here the optimal DCN and content placement in the network to minimize the DCN failure probability due to a region failure. The inherent tradeoff among failure probabilities of DCN hosting nodes, failure probabilities of requesting paths and traffic transmission delay is also considered in the optimal placement problem.

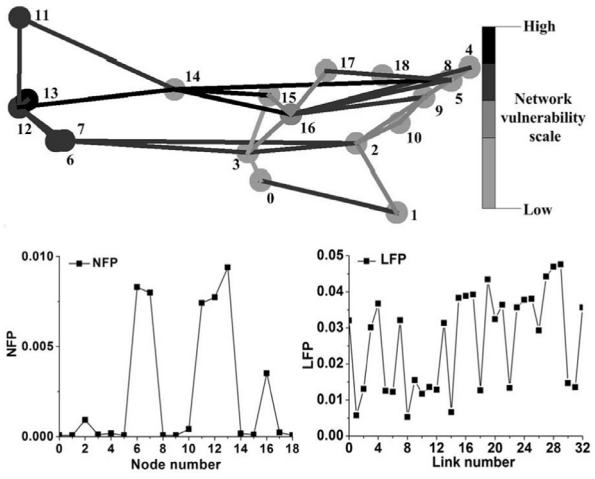


Fig. 4. Vulnerability map.

Table 1
Links in the U.S. InternetMCI network.

Link number	Link	Link number	Link	Link number	Link
0	(0,1)	11	(4,8)	22	(9,10)
1	(0,3)	12	(4,9)	23	(9,16)
2	(1,2)	13	(4,16)	24	(11,12)
3	(2,3)	14	(5,8)	25	(11,14)
4	(2,7)	15	(6,7)	26	(12,13)
5	(2,9)	16	(6,12)	27	(12,14)
6	(2,10)	17	(7,12)	28	(14,15)
7	(3,7)	18	(8,9)	29	(14,16)
8	(3,15)	19	(8,14)	30	(15,16)
9	(3,16)	20	(8,16)	31	(16,17)
10	(4,5)	21	(8,18)	32	(17,18)

3.1. Problem description

Our objective is to minimize the DCN failure probability under a region failure, in which the traffic transmission delay is also considered to avoid the long communication latency between the requesting node and content hosting node. We use the length of a path to approximate the transmission delay of the traffic along it, and formulate the optimal DCN and content placement problem as an ILP problem as follows.

3.2. Notation list

Inputs:

- V: The set of all nodes in network G(V, E).
- E: The set of all links in network G(V, E).
- V': The set of DCN candidate hosting nodes, $V' \subseteq V$.
- C: The set of contents provided by DCNs.
- δ: The scaling factor for adjusting the weight among total failure probability of DCN hosting nodes, total failure probability of requesting paths and total traffic transmission delay.
- S: The set of requesting nodes, $S \subseteq V$.
- R_{sv}: The set of paths between requesting node s and DCN hosting node v.
- N_d: The number of DCNs to be placed.
- N_c: The maximum number of replicas of content c.
- N_{sv}: The number of paths between requesting node s and DCN hosting node v.

- β: Predefined constant greater than the number of contents $|C|$.
- PF_v: The failure probability of DCN candidate hosting node v ($\triangle_{NFP_v}$) obtained by "vulnerability map".
- PF_{rsv}: The failure probability of path r between requesting node s and DCN hosting node v obtained by $P_r = 1 - \prod_{l \in r}(1 - P_l)$.
- PF_{sv}: The average failure probability of paths between requesting node s and DCN hosting node v.
- L_{rsv}: The length of path r between requesting node s and DCN hosting node v.
- L_{sv}: The average length of paths between requesting node s and DCN hosting node v.

Variables:

- U_v: Binary variable. It takes 1 if a DCN is placed at node v and 0 otherwise.
- U_v^c: Binary variable. It takes 1 if content c is hosted at DCN hosting node v and 0 otherwise.
- U_v^{sc}: Binary variable. It takes 1 if requesting node s requests content c provided by DCN hosting node v and 0 otherwise.

3.3. ILP formulation

$$\text{Minimize} \quad \left\{\delta \sum_{v \in V'} U_v PF_v + \sum_{v \in V'} \sum_{s \in S} \sum_{c \in C} U_v^{sc}(PF_{sv} + L_{sv})\right\}. \tag{8}$$

Subject to

$$PF_{sv} = \frac{\sum_{r \in R_{sv}} PF_{rsv}}{N_{sv}}, \forall s \in S, \forall v \in V'; \tag{9}$$

$$L_{sv} = \frac{\sum_{r \in R_{sv}} L_{rsv}}{N_{sv}}, \forall s \in S, \forall v \in V'; \tag{10}$$

$$U_v \geq \frac{1}{\beta} \sum_{c \in C} U_v^c, \forall v \in V'; \tag{11}$$

$$\sum_{v \in V'} U_v \leq N_d; \tag{12}$$

$$\sum_{v \in V'} U_v^c \geq 2, \forall c \in C; \tag{13}$$

$$\sum_{v \in V'} U_v^c \leq N_c, \forall c \in C; \tag{14}$$

$$U_v^{sc} \leq U_v^c, \forall v \in V', \forall s \in S, \forall c \in C; \tag{15}$$

$$\sum_{v \in V'} U_v^{sc} = 1, \forall s \in S, \forall c \in C. \tag{16}$$

Objective (8) (abbreviated as *failure risk*) minimizes the total failure probability of DCN hosting nodes and requesting paths, as well as the total traffic transmission delay. The scaling factor δ is used to control the weight among total failure probability of DCN hosting nodes, total failure probability of requesting paths and total traffic transmission delay. Eq. (9) determines the average failure probability of paths between requesting node s and DCN hosting node v while Eq. (10) calculates the average length of paths between requesting node s and DCN hosting node v. Constraint (11) implies that if any content c is provided by a node v, then a DCN must be placed at this node. Here, we use β larger than $|C|$ to ensure that constraint (11) can be properly established when $U_v = 1$ and $1 \leq \sum_{c \in C} U_v^c \leq |C|$. Constraint (12) indicates a bound on the total number of DCNs placed in the network. Constraint (13) guarantees that any content c is replicated at least twice while constraint (14) limits the number of replicas of content c to its maximum possible number. Constraint (15) ensures that if requesting node s requests content c provided by DCN hosting node v, node v should contain content c. Constraint (16) guarantees that a request from node s for content c can be satisfied by only one DCN containing content c.

It is notable that the content requests (i.e., connection requests from requesting nodes for contents) only depend on the requesting nodes and the amount of contents, and are independent from the final locations of DCN and content placement. As requesting nodes and contents are given, the content requests can be modeled/obtained based on those given parameters by simple statistics.

4. Heuristic

To make the overall placement problem more scalable for large-scale networks, we propose here a heuristic to divide the problem into two subproblems. We first solve the DCN placement problem, and then consider the content placement problem by taking the results of DCN placement as the input.

4.1. Algorithm description

The proposed heuristic is summarized in Algorithms 3 and 4. Algorithm 3 gives the pseudo code of DCN placement, and then based on the results of Algorithm 3, the content placement scheme is shown in Algorithm 4. Here, the notations PF_{sv}, L_{sv}, PF_v, N_d, N_c, V', C, S and δ are defined in Section 3.2, and let $|B|$ denote the number of elements in an arbitrarily given set B.

DCN placement: In order to determine DCN hosting nodes, we need to evaluate the failure risk of each candidate DCN hosting

Algorithm 3 DCN placement (DP).

Input:
$G(V, E)$, $V' \subseteq V$, $S \subseteq V$, PF_{sv} and L_{sv} for $\forall s \in S, \forall v \in V'$, PF_v for $\forall v \in V'$, C, δ, N_d and $(sc) \in R_c$: the set of connection requests for content $c \in C$, $s \in S$.

Output:
The set of DCN hosting nodes: L.

```
1: L = ∅; Risk_min = ∞;
2: c = arg_{c∈C} max{|R_c|};
3: for each v ∈ V' do
4:    Risk_v = δPF_v + Σ_{(sc)∈R_c, ∀s∈S}(PF_sv + L_sv);
5:    if (Risk_v < Risk_min) then
6:       Risk_min = Risk_v; u = v;
7:    end if
8: end for
9: L = L ⋃ {u};
10: while (|L| < N_d) do
11:    Risk_min = ∞;
12:    for each v ∈ (V' − L) do
13:       Risk_v = Σ_{(sc)∈R_c, ∀s∈S, ∀c∈C} min_{∀u∈(L⋃{v})}(PF_su
14:                +L_su);
15:       Risk_v = Risk_v + δ Σ_{∀w∈(L⋃{v})} PF_w;
16:       if (Risk_v < Risk_min) then
17:          Risk_min = Risk_v; v' = v;
18:       end if
19:    end for
20:    L = L ⋃ {v'};
21: end while
22: return L;
```

Algorithm 4 Content placement (CP).

Input:

$G(V, E)$, $V' \in V$, $S \in V$, PF_{sv} and L_{sv} for $\forall s \in S, \forall v \in V'$, L, N_c, C, $(sc) \in R_c$: the set of connection requests for content $c \in C$, $s \in S$ and k: the minimum number of replicas of content.

Output:

The set of DCN hosting nodes for the content c placement: $A_c, \forall c \in C$.

1: $A_c = \varnothing, \forall c \in C$;
2: **for** each $c \in C$ **do**
3: **for** each $(sc) \in R_c$ **do**
4: $v = \arg_{v \in L} \min\{PF_{sv} + L_{sv}\}$;
5: **if** $(v \notin A_c)$ **then**
6: $A_c = A_c \bigcup \{v\}$;
7: **end if**
8: **end for**
9: **end for**
10: **for** each $c \in C$ **do**
11: **while** $(|A_c| < k)$ **do**
12: $Risk_{min} = \infty$;
13: **for** each $v \in (L - A_c)$ **do**
14: $Risk_v = \sum_{\{(sc) \in R_c, \forall s \in S\}} (PF_{sv} + L_{sv})$;
15: **if** $(Risk_v < Risk_{min})$ **then**
16: $Risk_{min} = Risk_v$; $u = v$;
17: **end if**
18: **end for**
19: $A_c = A_c \bigcup \{u\}$;
20: **end while**
21: **while** $(|A_c| > N_c)$ **do**
22: $Risk_{min} = \infty$;
23: **for** each $v \in A_c$ **do**
24: $Risk_v = 0$;
25: $Risk_v = \sum_{(sc) \in R_c, \forall s \in S} min_{\forall u \in (A_c - \{v\})} (PF_{su} + L_{su})$
26: **if** $(Risk_v < Risk_{min})$ **then**
27: $Risk_{min} = Risk_v$; $v' = v$;
28: **end if**
29: **end for**
30: $A_c = A_c - \{v'\}$;
31: **end while**
32: **end for**
33: return $A_c, \forall c \in C$.

node and then the selected DCN hosting nodes induce small failure risk for connection requests. Since the connection requests for each content are given which are independent from the final locations of DCNs and contents, we can use these connection requests (i.e., the information of content requests) to evaluate the failure risk of each candidate DCN hosting node. For DCN placement, first, we find a content that has the maximum number of connection requests from requesting nodes. For each DCN candidate hosting node, we calculate the failure risk when the content found before is provided by this node, respectively. Then, we determine a node that induces the minimum failure risk as the first DCN hosting node from the set of DCN candidate hosting nodes. After that we use the iteration to determine all the DCN hosting nodes. In each iteration, a DCN hosting node from the set of DCN candidate hosting nodes is found which induces the minimum failure risk when all connection requests are provided by the determined DCN hosting nodes and this node. For a given network for DCN placement, our algorithm can find the DCN hosting nodes from the set of DCN candidate hosting nodes. Then, the small failure risk is achieved if all connection requests from a set of requesting nodes are provided by these nodes.

Content placement: After determining the DCN hosting nodes, we then assign the contents to DCNs which should satisfy constraints (13) and (14) in Section 3.3. For each content, we first assign it to these DCN hosting nodes, which induce the minimum value of total failure probability of requesting paths and total traffic transmission delay for this content provided by these nodes. To satisfy constraints (13) and (14), for each content, we check the number of DCN hosting nodes which host this content. If a content does not satisfy constraint (13), we successively assign this content to DCN hosting node that does not contain this content until satisfying constraint (13), which induces the minimum value of total failure probability of requesting paths and total traffic transmission delay for this content. If a content does not satisfy constraint (14), we successively reduce the DCN hosting node containing this content until satisfying constraint (14). Compared with the original DCN hosting nodes containing this content, we ensure that the remaining nodes bring about the smallest gap in the value of total failure probability of requesting paths and total traffic transmission delay for this content.

In Algorithm 3, the initialization is shown in line 1. The content $c \in C$ is found which has the maximum number of connection requests from requesting nodes in line 2. From lines 3–8, for each DCN candidate hosting node v, we calculate the failure risk for content c provided by this node, respectively, and find the node u that induces the minimum failure risk. The failure risk is obtained in line 4. The node u is determined as the first DCN hosting node in line 9. All the DCN hosting nodes are determined through the iteration in lines 10–21. In each iteration, we select a DCN hosting node v' from the DCN candidate hosting node set $V' - L$, and we can obtain the minimum failure risk when all connection requests provided by these DCN hosting nodes in $L \bigcup \{v'\}$. Here, the failure risk is obtained in lines 13–15.

In Algorithm 4, we can implement the content placement to satisfy constraints (13) and (14) in Section 3.3. First, we find the candidate deployment nodes in L for each content $c \in C$, which induce the minimum value of total failure probability of requesting paths and total traffic transmission delay for contents provided by these nodes in lines 2–9. Then, for each content $c \in C$, in lines 11–20 we ensure the number of replicas of content c to satisfy constraint (13). In each iteration, a DCN hosting node u in $L - A_c$ is selected as the content c hosting node, which induces the minimum value of total failure probability of requesting paths and total traffic transmission delay for content c when content c is provided by this node. Here, the value of total failure probability and total traffic transmission delay is obtained in line 14. Then, constraint (14) is satisfied by the iteration from lines 21 to 31. In each iteration, a DCN hosting node $v' \in A_c$ is selected, and then removed from A_c. The value of total failure probability of requesting paths and total traffic transmission delay for content c is calculated in line 25 when content c is provided by arbitrary $|A_c| - 1$ nodes in A_c, in which the minimum value is obtained when the node v' is removed from A_c.

Remark 1. Notice that content placement can be optimized either periodically according to daily content requests variation, or within the early warning time of an upcoming disaster if the DCN failure risk is observed higher than the current risk evaluation. For an upcoming disaster with an early warning time, in order to minimize content loss, we need to re-optimize content placement within the early warning time. Since ILP is not scalable in terms of its long running time (i.e., optimal solution may not be found within the given early warning time), time-efficient heuristic is necessary to produce real-time response. On the other hand, solving the ILP for optimal joint design of DCN and content placement with transmission delay optimization is not an easy task for large-scale

networks. To this end, we need a time-efficient heuristic as well for scalability.

4.2. Complexity analysis of the heuristic

In this subsection, we analyze the complexity of heuristic DCN and content placement. The complexity of Algorithm 3 is dominated by the iterations. The complexity in line 2 is $O(|C|)$. The complexity of the iteration from lines 3 to 8 is $O(|V'| \times |R_c|)$ and the complexity of the iteration from lines 10 to 21 is $O((N_d - 1) \times (|V'| - 1) \times |S| \times |C| \times N_d)$. Thus, the total complexity of Algorithm 3 is no more than $O(|C| \times (N_d)^2 \times |V|^2)$.

The complexity of Algorithm 4 is also dominated by the iterations. The complexity of the iteration in lines 2–9 is $O(|C| \times max_{c \in C}(|R_c|) \times |L|)$. The time for the iteration in lines 11–20 is $O((k - min_{c \in C}(|A_c|)) \times (|L| - min_{c \in C}(|A_c|)) \times max_{c \in C}(|R_c|))$. The time for the iteration in lines 21–31 is $O((max_{c \in C}(|A_c|) - N_c) \times max_{c \in C}(|A_c|) \times max_{c \in C}(|R_c|) \times (max_{c \in C}(|A_c|) - 1))$. Thus, the total complexity of Algorithm 4 is no more than $O(|C| \times |N_d|^3 \times |V|)$. From the complexities of these two algorithms, we can find that the complexity of heuristic DCN and content placement is no more than $O(|C| \times |V|^2 \times (N_d)^2)$. Thus, the proposed heuristic runs in polynomial time.

5. Numerical results

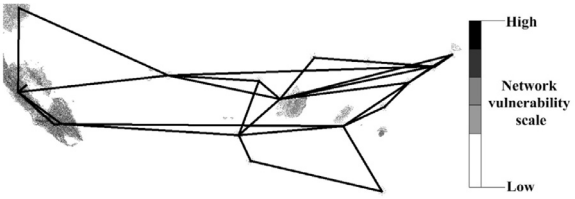
In this section, we carry out numerical experiments based on the gridded data of U.S. national seismic hazard map [22]. Assume that the network is deployed in a rectangle area with length 2402 and height 1018. We first demonstrate the proposed vulnerability assessment scheme in Section 5.1. Based on the vulnerability information of a given network, we further validate the efficiency of the proposed ILP in Section 5.2 and heuristic for DCN and content placement in Section 5.3. For DCN and content placement, Gurobi 6.0 is used to solve the ILP in (8)–(16). We run the ILP and heuristic algorithms on an Intel Core(TM) i3-4030U CPU @ 1.90 GHz and also develop a simulator to emulate the random connection requests between nodes and DCN contents. Given a network for DCN and content placement, the simulator generates a random integer of x between 1 and $|C|$ as the number of content requests from each requesting node. The simulator also ensures that each content is requested.

5.1. Vulnerability assessment

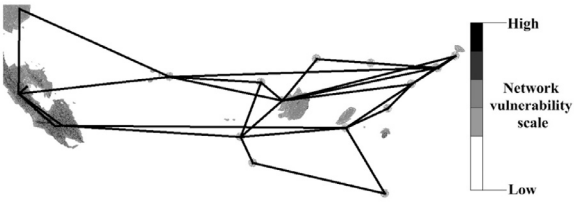
For network vulnerability assessment, we consider the U.S. InternetMCI network in Fig. 3 with 19 nodes and 33 links, where the length of the shorter segment of link ξ is fixed as 20. According to the gridded data of U.S. national seismic hazard map, the network area is divided into 1201 × 509 square cells with a side length 2 for each. Each PRF is defined by two concentric circles with radiuses (r_1, r_2) and probabilities (p_1, p_2). Since the gridded data of U.S. national seismic hazard map only contains the information of grid partition and peak ground acceleration (g), we cannot obtain concrete occurring probability of a PRF falling within one cell from the gridded data of U.S. national seismic hazard map. To facilitate the vulnerability assessment, due to the fact that the gridded data of U.S. national seismic hazard map is obtained based on the map in Fig. 1 with an exceedance probability of 2% in 50 years, we set the occurring probability of a PRF falling within one cell as a random value between 0.02 and 0.5. For the PRF with center falling within one cell, we take the center point of the cell as the center of the PRF and set its parameters r_1, r_2, p_1 and p_2 according to the peak acceleration data (g) in the cell from the gridded data of U.S. national seismic hazard map. The parameter settings are shown in Table 2. We compare our vulnerability assessment results with

Table 2
Parameter settings for PRF MODEL.

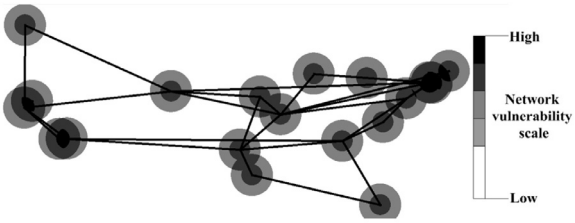
g from Fig. 1	r_1	r_2	p_1	p_2
0.8	100	200	0.95	0.75
0.4	60	120	0.8	0.6
0.3	50	100	0.6	0.3
0.2	25	50	0.5	0.25
Others	10	20	0.25	0.1



(a) Vulnerable network zone distribution evaluated based on the simulation



(b) Vulnerable network zone distribution evaluated based on the new scheme

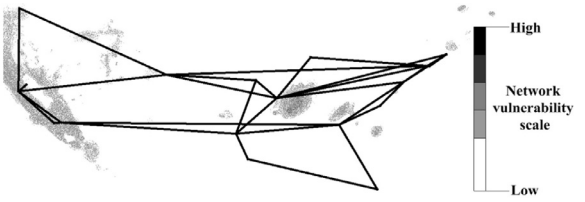


(c) Vulnerable network zone distribution evaluated based on the old scheme

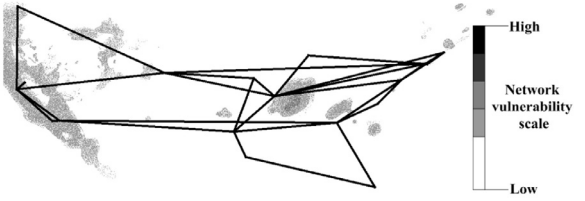
Fig. 5. Illustration of NFP vulnerable network zone distribution for all nodes.

that in [16] and [17] and that based on simulation, respectively. For simplicity, the vulnerability assessment based on our proposed scheme is referred to as new scheme, while that based on [16] and [17] is referred to as old scheme. In our simulation, we randomly generate a location in each cell as the center of a PRF when the PRF occurs in this cell. Other parameter settings keep the same as above. Here, we have carried out 10 different simulations, and then the vulnerability for nodes (or links) is evaluated by the average of all simulation results. For vulnerability assessment in [16] and [17], the parameters r_1, r_2, p_1, and p_2 of the PRF are the same and fixed as $r_1 = 50$, $r_2 = 100$, $p_1 = 0.60$, and $p_2 = 0.30$, and the occurring probability of a PRF falling within one cell is uniformly distributed.

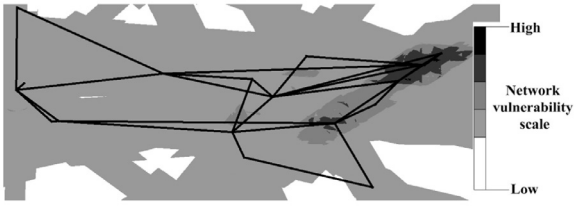
Fig. 5 illustrates the NFP vulnerable network zone distributions for all nodes under the simulation, the new scheme and the old scheme, respectively. The results in Fig. 5 clearly indicate that the NFP vulnerable network zone distribution for all nodes based on the new scheme generally complies with the simulation results and both of them match the potential earthquake distribution in U.S. as illustrated in Fig. 1. These results show that our proposed vulnerability assessment scheme is efficient to evaluate the vulnerability of nodes due to the real disaster. It is notable that since the old scheme does not take the global nonuniform distribution of a disaster in terms of its occurring probability and intensity into account, the NFP vulnerable network zone distribution for all nodes



(a) Vulnerable network zone distribution evaluated based on the simulation



(b) Vulnerable network zone distribution evaluated based on the new scheme



(c) Vulnerable network zone distribution evaluated based on the old scheme

Fig. 6. Illustration of LFP vulnerable network zone distribution for all links.

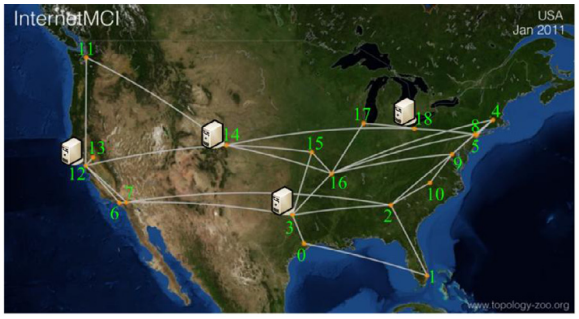
based on the old scheme is quite different from that based on the new scheme.

Fig. 6 shows the LFP vulnerable network zone distribution for all links, with Fig. 6(a) for the simulation, Fig. 6(b) for the new scheme and Fig. 6(c) for the old scheme, respectively. From Fig. 6 we can get similar conclusions as those in Fig. 5. We can also observe that our proposed scheme is efficient to evaluate the vulnerability of links due to a region failure. Based on such vulnerable network zone distribution for all nodes or links, we can easily identify the most vulnerable network zones, i.e., the zones in which the PRF falling within each cell has the most significant impact to the network nodes or links. Since our proposed vulnerability assessment can efficiently evaluate the impact to a network from a real disaster, "vulnerability map" based on the new scheme will be very helpful for us to identify the optimal placement of DCN and content in a given network against the disaster.

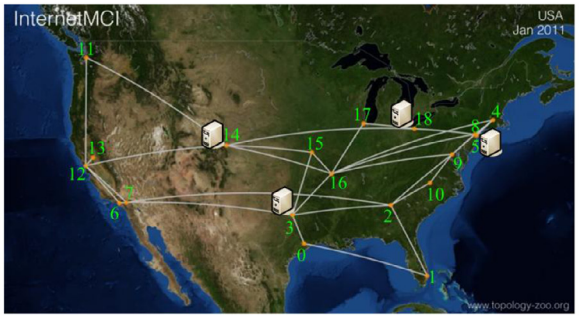
Remark 2. In our experiments, the old scheme only takes uniformly distributed data, but a real disaster generally entails the nonuniform case. The new scheme considers nonuniform distribution and it covers the old scheme as a special case. By using uniform distribution for the old scheme in our experiments, we indeed intend to show the drawback of vulnerability assessment under uniform distribution, rather than comparing with the new scheme.

5.2. DCN and content placement in small-scale networks

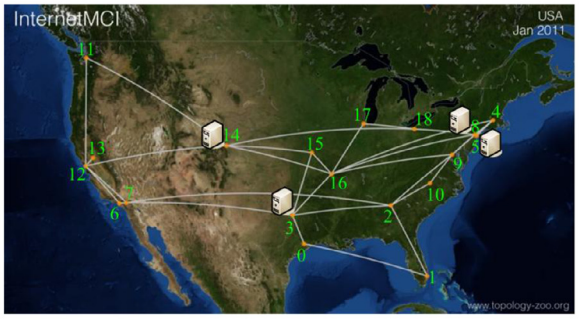
For our proposed ILP framework for DCN and content placement, we also consider the U.S. InternetMCI network with 19 nodes and 33 links. In our simulation, we set $\beta = 100$ and $\delta = 1000$ (i.e., the second DCN and content placement scenario in Section 5.4). We consider 4 DCNs and 20 contents, and each content has at least 2 and at most 3 replicas. All nodes in the network are set as



(a) DCN placement for InternetMCI network based on the ILP and the old vulnerability assessment scheme



(b) DCN placement for InternetMCI network based on the ILP and the new vulnerability assessment scheme



(c) DCN placement for InternetMCI network based on the heuristic and the new vulnerability assessment scheme

Fig. 7. DCN placement scenarios.

candidate placement nodes for DCNs. The "vulnerability map" for such network is obtained by the vulnerability assessment with the same parameters as in Section 5.1. To facilitate the calculation, we convert the values of L_{sv} to values between 0 and 1.

The DCN placement based on the ILP and the old vulnerability assessment scheme is shown in Fig. 7(a) and that based on the ILP and the new vulnerability assessment scheme is shown in Fig. 7(b). From Fig. 7(a) and (b) we can find that DCNs are placed at nodes 3, 12, 14 and 18 for the former and 3, 5, 14 and 18 for the latter. Besides, the failure risk is 97.49 (calculated based on the new vulnerability information) for the former and 96.15 for the latter. Although the gap of failure risk is only $(97.49 - 96.15)/96.15 \cong 1.39\%$ between the above two scenarios, the total failure probability of DCN hosting nodes can be dramatically reduced under the new vulnerability assessment scheme (the total failure probability of DCN hosting nodes is 0.008111 for the former and 0.000438 for the latter).

Fig. 7(c) shows the DCN placement based on the heuristic solution and the new vulnerability assessment scheme. The DCNs are placed at nodes 3, 5, 8 and 14 and the failure risk is 100.21. Thus, the gap of failure risk between the ILP and heuristic under the

Table 3
Content placement in DCNs for ILP and heuristic.

ILP		Heuristic	
DCNs	Contents	DCNs	Contents
3	0,1,3,4,5,8,10,11 12,13,14,16,17	3	0,1,3,4,5,8,10,11,12 13,14,15,16,17
5	0,3,4,5,7,8,9,11 12,13,15,19	5	0,3,4,5,7,8,9,11 12,13,15,19
14	1,2,3,4,5,6,7,8,9,10,11 13,14,15,16,17,18,19	8	0,1,2,6,7,8,10,13 16,17,18,19
18	0,1,2,6,7,9,12 15,16,18,19	14	1,2,3,4,5,6,7,9,10,11,12 14,15,16,17,18,19

Table 4
Performance analysis in large-scale network with four DCNs and different numbers of contents for ILP and heuristic.

$\|C\|$	ILP		Heuristic	
	Failure risk	Running time (s)	Failure risk	Running time (s)
10	60.74	16.64	68.86	0.44
20	115.43	181.61	128.55	0.51
30	163.03	242.99	185.96	0.53
40	210.15	476.88	228.55	0.56
50	264.74	3297.55	286.57	0.59

Table 5
Performance analysis in large-scale network with ten contents and different numbers of DCNs for ILP and heuristic.

N_d	ILP		Heuristic	
	Failure risk	Running time (s)	Failure risk	Running time (s)
4	60.74	16.64	68.86	0.44
8	60.45	12.11	74.66	0.56
12	60.67	11.86	76.76	0.61
16	60.94	11.83	79.85	0.71
20	61.21	12.62	80.32	0.8
24	61.49	11.95	78.24	0.88
28	61.77	12.02	80.05	1.04
32	62.05	12.38	79.66	1.039
36	62.34	10.39	80	1.22
40	62.62	10.14	78.22	1.49

Table 6
Tradeoff between *DFP* and $PFP + TD$.

Placement scenarios	*DFP*	*PFP*	*TD*
1	0.008111	19.31	70.07
2	0.000438	20.73	74.98
3	0.000329	22.31	79.69
4	0.000283	23.7	84.29
5	0.000282	24.54	87.26

new vulnerability assessment scheme is $(100.21 - 96.15)/96.15 \cong 4.22\%$. The contents hosted at each DCN are shown in Table 3 for ILP and heuristic under the new vulnerability assessment scheme, respectively. Table 3 shows that the same DCN hosting node determined by the ILP and heuristic contains similar contents. From Figs. 4 and 5, we can also find that the DCN hosting nodes based on the ILP and heuristic under the new vulnerability scheme avoid the nodes with high NFP and the most vulnerable network zones for all nodes. Besides, under the new vulnerability assessment scheme we also have carried out other experiments for 10 different groups of connection requests generated randomly with similar network size. The average gap of failure risk between the ILP and heuristic is 3.5%, which confirms the superior performance of the proposed heuristic.

5.3. DCN and content placement in large-scale networks

To verify the performance of our proposed heuristic for large-scale networks under the new vulnerability assessment scheme, we randomly generate a network by simulator with 100 nodes and 202 links. In order to reduce the complexity, in this experiment we only consider link-disjoint k-shortest paths between an arbitrary pair of nodes to implement routes ($k = 3$). The "vulnerability map" for this network is obtained in a similar way as that of U.S. InternetMCI network. Except the number of DCNs and contents to be placed, other parameter settings are similar to those in Section 5.2.

The performance of ILP and heuristic for the cases $|C| = \{10, 20, 30, 40, 50\}$ are summarized in Table 4 when the number of DCNs to be placed is 4. In Table 5, we show the performance of ILP and heuristic for the cases $N_d = \{4, 8, 12, 16, 20, 24, 28, 32, 36, 40\}$ when the number of contents to be placed is 10. From Tables 4 and 5, we can observe that our proposed heuristic is more scalable, and the ILP is sensitive to $|C|$. Table 5 also shows that the running time of ILP decreases and that of heuristic increases when N_d increases, but the running time of heuristic increases slowly. Besides, from Tables 4 and 5 we can find that although the gaps of failure risk between the ILP and heuristic vary with the increases of $|C|$ and N_d, their sensitivities to the variations of $|C|$ and N_d are different. For a fixed number of DCNs to be placed of N_d=4 and when we increase the number of contents to be placed $|C|$ from 10 to 50, the average gap of failure risk is 11.2%. When we increase the number of DCNs to be placed N_d from 4 to 40 at a fixed number of contents to be placed of $|C|$=10, the average gap of failure risk is 26.4%.

5.4. Effect of δ on DCN and content placement

The scaling factor δ is used to control the weight among the total failure probability of DCN hosting nodes, the total failure probability of requesting paths and the total traffic transmission delay. Thus, for different values of δ, we can obtain different DCN and content placement scenarios. Considering the ILP with same simulation settings in Section 5.2, for different values of δ, there are five different DCN and content placement scenarios. In Table 6, we show the total failure probability of DCN hosting nodes $\sum_{v \in V'} U_v PF_v$ (abbreviated as *DFP*) and the total failure probability of requesting paths $\sum_{v \in V'} \sum_{s \in S} \sum_{c \in C} U_v^{sc} PF_{sv}$ (abbreviated as *PFP*) as well as the total traffic transmission delay $\sum_{v \in V'} \sum_{s \in S} \sum_{c \in C} U_v^{sc} L_{sv}$ (abbreviated as *TD*) for five DCN and content placement scenarios, respectively. From Table 6, we can find a desirable tradeoff between *DFP* and $PFP + TD$ by adjusting the value of δ in the DCN design phase.

6. Conclusions

We studied the DCN and content placement problem under global nonuniform distribution of potential region failure due to disaster in large-scale geographical areas. By proposing a general grid partition-based vulnerability estimation scheme, we can determine the "vulnerability map" of a given network for DCN and content placement, which provides an important input for our proposed ILP and heuristic. Based on the vulnerability map, our proposed ILP can generate optimal DCN and content placement solutions to minimize the DCN failure risk due to disaster. This achieves best-effort protection of DCN and content against the region failure. To make our solution more scalable for large-scale networks, a heuristic was further proposed. Numerical results showed that our work can lead to a more feasible solution. It can well protect DCN and content under global nonuniform distribution of the potential region failure scenario.

Acknowledgments

This work was supported in part by the Natural Science Fund of China (no. 61372085), the Key Project of Anhui University Science Research (nos. KJ2015A285 and KJ2015A190), the Natural Science Foundation of Anhui Province (no. 1508085MF123), the Japan Society for the Promotion of Science Grants-in-Aid for Scientific Research (A), 2015 (no. 26240012), the Professor Scientific Research Foundation of Chuzhou University (no. 2014qd013) and the Talented Team of Computer System Architecture of Chuzhou University.

References

[1] K. Chen, C. Guo, H. Wu, J. Yuan, Z. Feng, Y. Chen, S. Lu, W. Wu, Dac: Generic and automatic address configuration for data center networks, IEEE/ACM Trans. Netw. 20 (1) (2012) 84–99.
[2] M. Bari, R. Boutaba, R. Esteves, L. Granville, M. Podlesny, M. Rabbani, Q. Zhang, M. Zhani, Data center network virtualization: A survey, IEEE Commun. Surv. Tutor. 15 (2) (2013) 909–928.
[3] J. Xiao, B. Wu, X. Jiang, A. Pattavina, H. Wen, L. Zhang, Scalable data center network architecture with distributed placement of optical switches and racks, IEEE/OSA J. Opt. Commun. Netw. 6 (3) (2014) 270–281.
[4] X. Dong, T. El-Gorashi, J. Elmirghani, Green IP over WDM networks with data centers, IEEE/OSA J. Lightw. Technol. 29 (12) (2011) 1861–1880.
[5] J. Xiao, H. Wen, B. Wu, X. Jiang, P.-H. Ho, L. Zhang, Joint design on DCN placement and survivable cloud service provision over all-optical mesh networks, IEEE Trans. Commun. 62 (1) (2014) 235–245.
[6] K. Tanaka, Y. Yamazaki, T. Okazawa, T. Suzuki, T. Kishimoto, K. Iwata, Experiment on seismic disaster characteristics of underground cable, in: The 14th World Conference on Earthquake Engineering, Beijing, China, October 12-17, 2008. http://www.iitk.ac.in/nicee/wcee/article/14_06-0069.PDF.
[7] A. Kwasinski, W.W. Weaver, P.L. Chapman, P.T. Krein, Telecommunications power plant damage assessment for hurricane katrina-site survey and follow-up results, IEEE Syst. J. 3 (3) (2009) 277–287.
[8] Y. Ran, Considerations and suggestions on improvement of communication network disaster countermeasures after the wenchuan earthquake, IEEE Commun. Mag. 49 (1) (2011) 44–47.
[9] K. Morrison, Rapidly recovering from the catastrophic loss of a major telecommunications office, IEEE Commun. Mag. 49 (1) (2011) 28–35.
[10] T. Adachi, Y. Ishiyama, Y. Asakura, K. Nakamura, The restoration of telecom power damages by the Great East Japan Earthquake, in: IEEE 33rd International Telecommunications Energy Conference, IEEE, Amsterdam, Netherlands, October 9-13, 2011, pp. 1–5.
[11] Flooding, power outages from hurricane sandy lead to internet, phone service disruptions, 2012, (http://www.nypost.com/p/news/business/flooding_from_hurricane_sandy_leads_CG8gj1SSEenIcuZzj1yRbM).
[12] A. Kwasinski, Lessons from field damage assessments about communication networks power supply and infrastructure performance during natural disasters with a focus on hurricane sandy, in: FCC Workshop Network Resiliency, Brooklyn, New York, NY, USA, February 5-6, 2013. http://users.ece.utexas.edu/~kwasinski/1569715143%20Kwasinski%20paper%20FCC-NR2013%20submitted.pdf.
[13] B. Mukherjee, M.F. Habib, F. Dikbiyik, Network adaptability from disaster disruptions and cascading failures, IEEE Commun. Mag. 52 (5) (2014) 230–238.
[14] S. Neumayer, E. Modiano, Network reliability with geographically correlated failures, in: IEEE INFOCOM, IEEE, San Diego, CA, USA, March 15-19, 2010, pp. 1–9.
[15] S. Neumayer, G. Zussman, R. Cohen, E. Modiano, Assessing the vulnerability of the fiber infrastructure to disasters, IEEE/ACM Trans. Netw. 19 (6) (2011) 1610–1623.
[16] J. Liu, X. Jiang, H. Nishiyama, N. Kato, Reliability assessment for wireless mesh networks under probabilistic region failure model, IEEE Trans. Vehic. Technol. 60 (5) (2011) 2253–2264.
[17] X. Wang, X. Jiang, A. Pattavina, Assessing network vulnerability under probabilistic region failure model, in: IEEE 12th International Conference on High Performance Switching and Routing, IEEE, Cartagena, Spain, July 4-6, 2011, pp. 164–170.
[18] P. Agarwal, A. Efrat, S. Ganjugunte, D. Hay, S. Sankararaman, G. Zussman, The resilience of WDM networks to probabilistic geographical failures, IEEE/ACM Trans. Netw. 21 (5) (2013) 1525–1538.
[19] 2014 U.S. Geological National Seismic Hazard Maps, 2014, (http://earthquake.usgs.gov/hazards/products/conterminous/index.php#2014).
[20] M.F. Habib, M. Tornatore, M.D. Leenheer, F. Dikbiyik, B. Mukherjee, Design of disaster-resilient optical datacenter networks, IEEE/OSA J. Lightw. Technol. 30 (16) (2012) 2563–2573.
[21] S. Ferdousi, F. Dikbiyik, M.F. Habib, M. Tornatore, B. Mukherjee, Disaster-aware datacenter placement and dynamic content management in cloud networks, IEEE/OSA J. Opt. Commun. Netw. 7 (7) (2015) 681–694.
[22] 2014 U.S. Geological National Seismic Hazard Map Gridded Data, 2014, (http://earthquake.usgs.gov/hazards/products/conterminous/2014/data/2014_pga2pct50yrs.dat.zip).
[23] InternetMCI Network, 2011, (http://www.topology-zoo.org/dataset.html).

Lisheng Ma received the B.S. and M.S. degrees both in computer science and technology from Taiyuan Normal University, China in 2004 and from Southwest University, China in 2007, respectively. He is currently working towards the Ph.D. degree at the School of Systems Information Science, Future University Hakodate, Japan and is also faculty member at the School of Computer and Information Engineering, Chuzhou University, China. His research interests include switching networks and data center networks.

Xiaohong Jiang received the B.S., M.S. and Ph.D degrees all from Xidian University, China. He is currently a full professor of Future University Hakodate, Japan. He was an associate professor of Tohoku University, Japan, from February 2005 to March 2010, an assistant professor in Japan Advanced Institute of Science and Technology (JAIST), from October 2001 to January 2005. He was a JSPS research fellow at JAIST from October 1999 to 2001. He was a research associate in the University of Edinburgh from March 1999to October 1999. His research interests include computer communications networks, mainly wireless networks, optical networks, etc. He has published more than 260 technical papers at premium international journals and conferences, which include over 50 papers published in IEEE journals like IEEE/ACM Transactions on Networking, IEEE Journal of Selected Areas on Communications, etc. He was the winner of the Best Paper Award and Outstanding Paper Award of IEEE HPCC 2014, IEEE WCNC 2012, IEEE WCNC 2008, IEEE ICC 2005 Optical Networking Symposium, and IEEE/IEICE HPSR 2002. He is a senior member of IEEE and a member of ACM and IEICE.

Bin Wu (S'04–M'07) received the Ph.D. degree in electrical and electronic engineering from The University of Hong Kong (Pokfulam, Hong Kong) in 2007. He worked as a postdoctoral research fellow from 2007 to 2012 in the ECE Department, University of Waterloo (Waterloo, Canada). He is now a professor in the School of Computer Science and Technology, Tianjin University (Tianjin, China). His research interests include computer systems and networking as well as communication system design.

Achille Pattavina received the Dr. Eng. degree in electronic engineering from University La Sapienza of Rome (Italy) in 1977, where he worked until 1991. Since 1995, he has been a full professor in Politecnico di Milano, Milano (Italy). He has been author/coauthor of more than 300 papers in the area of communications networks published in leading international journals/conferences. He has been engaged in many research activities, including European Union funded projects. He has authored two books, Switching Theory, Architectures and Performance in Broadband ATM Networks (New York: Wiley, 1998) and Communication Networks (McGraw-Hill, 2007, in Italian). He has been an editor for Switching Architecture Performance of the IEEE Transactions on Communications from 1994 to 2011 and editor-in-chief of the Wiley European Transactions on Telecommunications from 2001 to 2010. He is a senior member of the IEEE Communications Society. His current research interests include the area of green ICT and cloud computing, software defined networking and broadband convergent access/metro networks.

Norio Shiratori is currently an emeritus and research professor at the RIEC (Research Institute of Electrical Communication), Tohoku University, Japan. He is also a board member of Future University of Hakodate and a Visiting Professor of Chuo University, Japan. He is a fellow of the IEEE (Institute of Electrical and Electronic Engineers), the IPSJ (Information Processing Society of Japan) and the IEICE (The Institute of Electronics, Information and Communication Engineers). He was the president of the IPSJ from 2009 to 2011. He has published more than 15 books and over 400 refereed papers in computer science and related fields. He was the recipient of the "IPSJ Memorial Prize Winning Paper Award" in 1985, the "Telecommunication Advancement Foundation Incorporation Award" in 1991, the "Best Paper Award of ICOIN-9" in 1994, the "IPSJ Best Paper Award" in 1997, and many others including the most recent "Outstanding Paper Award of UIC-07" in 2007.