Optical Switching and Networking 10 (2013) 406–415

Contents lists available at ScienceDirect

Optical Switching and Networking

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

Survivable network virtualization for single facility node failure: A network flow perspective

Qian Hu *, Yang Wang, Xiaojun Cao

Computer Science Department, Georgia State University, GA 30303, United States

ARTICLE INFO

Article history:
Received 15 November 2012
Received in revised form
8 May 2013
Accepted 11 June 2013
Available online 6 July 2013

Keywords:
Network virtualization
Network survivability
Virtual network embedding

ABSTRACT

Network virtualization facilitates the technology advancement via decoupling the traditional Internet Service Providers (ISPs) into the infrastructure provider (InP) and the service provider (SP). Revolutionary technologies hence can be easily employed by the SP and transparently mapped to the physical network managed by the InP after resolving the *network embedding* problem. In this work, we target on importing resilience to the virtualization context by solving the *survivable network embedding* (*SNE*) problem. We view the SNE problem from a *multi-commodity network flow* perspective, and present an Integer Linear Programming (ILP) model for both splittable and non-splittable flow to achieve joint optimal allocation for the working and backup resources. For large-scale problems, we propose two efficient heuristic algorithms for the case with splittable and non-splittable flow, respectively. Our performance evaluation shows that the splittable mapping outperforms the non-splittable mapping in terms of the consumed resources, while the latter bears the advantage of consistent QoS guarantee.

1. Introduction

Network virtualization is considered to be one promising solution to overcome the ossification of the current Internet [1–5]. With network virtualization, the traditional Internet Service Providers (ISPs) are decoupled into two independent parties or tiers: the infrastructure provider (InP) and the service provider (SP). The former plays the role of physically deploying and managing the network infrastructure, while the latter offers end-to-end services to the user, building upon aggregated resources from one or multiple InPs. This decoupling provides the InPs a virtualized view of the underlying network infrastructure as well as the architecture-oblivious freedom of adopting the technological advancement [3–5].

To bridge the ties of the InP and SP, one of the most challenging problems raised in the network virtualization context is the *Virtual Network Embedding* (*VNE*) problem, where the customized virtual network from the SP is mapped to the substrate or physical network managed by the InP. In general, virtual network embedding consists of two major components: the mapping of the virtual node (with computational capacity requirement) to the substrate node and the mapping of the virtual link (with bandwidth capacity requirement) to the substrate path(s) [5]. Particularly, the link mapping can be classified into two categories: splittable mapping, where one virtual link can be mapped to multiple substrate paths, non-splittable mapping, in which one virtual link can be mapped to only one substrate path. In the past, significant attention has been paid for the virtual network embedding problem [6–12], which is known to be NP-Complete [13].

With network virtualization gaining momentum, the survivability challenges in virtual network embedding should also be well addressed, which attracts a broad interest recently. A survivable virtualization environment

* Corresponding author. Tel.: +1 7063381575.
E-mail addresses: qhu2@student.gsu.edu, qhu@cs.gsu.edu (Q. Hu), ywang@cs.gsu.edu (Y. Wang), cao@cs.gsu.edu (X. Cao).

1573-4277/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.osn.2013.06.007

generally has to deal with failures at node(s) and/or link(s). In the literature, various types of failure scenarios, including single link, single facility node and single regional failure, have been investigated [14–18].

In this paper, we study the survivable virtual network embedding problem with single node failure for both splittable and non-splittable flow situations. Different from prior work, we target on a joint optimal solution for both the working and backup resource allocation. The resulted problem, namely *survivable network embedding for single facility node failure* (*SNF*), has the added dimension of accommodating both the active and backup requests. Given the NP-Completeness of the SNF problem (i.e., contains an instance of the VNE problem), we view it as a *multi-commodity network flow (MCF)* problem, and present an Integer Linear Programming (ILP) model to achieve joint optimal resource allocation. The contribution of this study is multiple folds (i) for the first time, we study both splittable and non-splittable flow mapping for the survivable network embedding problem, and present Integer Linear Programming (ILP) models for respective cases; (ii) for both cases, the proposed ILP model can obtain a joint optimal solution considering the active and backup traffic accommodation altogether; (iii) two efficient heuristic algorithms are designed for the splittable and non-splittable cases, respectively; and (iv) comparative study through simulation and analysis is presented for the proposed schemes.

The remaining of this paper is organized as follows. Section 2 reviews related literature work of this study. In Section 3, we elaborate the system model, and present the formal problem definition of survivable virtual network embedding problem. Section 4 provides a network flow view of the survivable network embedding problem, based on which we present the Integer Linear Programming model for optimal survivable virtual network embedding in Section 5. In Section 6, we propose the heuristic algorithms for the splittable and non-splittable mapping, respectively. We present the performance study in Section 7 and conclude this paper in Section 8.

2. Literature review

The network embedding problem (without protection) has been extensively studied in the literature (see [6–8] and the references therein). For example, the authors of [6] viewed the networking embedding process as an extension of the traditional *Subgraph Isomorphism* problem and hence proposed an adapted solution. The study in [7] is the first work that explored the protocol/algorithm to implement the network embedding in a distributed manner. In [8], the network embedding is transformed into the *network flow* problem. None of above studies, however, have taken the network survivability into account.

Until very recently, the survivable network embedding problem attracts a broad interest. The concept of survivable networking embedding was first introduced in [14], which focused on the protection of single link failure. Following that, various types of failure scenarios, including single link, single facility node and single regional failure, have been investigated [16–19]. For instance, the authors of [16] studied the protection of single regional failures in network virtualization. The basic idea of their approach is to re-map the virtual network for each regional failure assuming that the number of distinct regional failures is finite. This re-mapping process is done on the induced substrate networks where the links and nodes affected by the given regional failure are removed and hence result in a resilient mapping against the failure. In [17], the authors proposed a two-step method to enable the network survivability against the single facility node failure (i.e., the node with the computing capability, which differs from the switch node that impacts the network connectivity). In the first step, an auxiliary graph of the virtual network is constructed, which can embed the network survivability by incorporating redundant nodes or links. For instance, to protect the failure of virtual node *i*, a backup node is added to the virtual network, say *j*, to replace *i* after the failure. Note that under the single failure assumption, node *j* can also be used to protect the failure of other virtual nodes for resource sharing. In the second step, the auxiliary graph is mapped to the substrate network (using existing mapping algorithms). The advantage of the two-step approach is the transparency of the protection process to the InPs. Another instance of the two-step method appeared in the study of [18]. Different from [17], the authors managed to further reduce the allocated backup resources with a *failure-dependent* strategy. In specific, when Node *i* fails, the role of Node *i* may be replaced by any other nodes after a rearrangement of all the nodes (including the backup node(s)). This strategy is novel and interesting, however, it may not be practically applicable due to the large amount of possible migrations of working nodes/links. For a more detailed classification and discussion on various types of failures in network virtualization, one can refer to [20] and the references therein.

In general, we can classify the strategies of enabling survivability in virtualization into two categories. The first one is to provide protection at the physical network tier (i.e., for the switch nodes and links), which, fundamentally, has no difference with the protection schemes adopted in traditional networks. The second is based on the enhancement of the virtual network, where the facility node failure has to be carefully addressed. Among various node failure scenarios, in this paper, we target on enabling survivability under single facility node failure. Different from the existing work, we present a joint optimal model for the allocation of both active and backup resources, where both splittable and non-splittable mapping are taken into account.

3. Network model and problem definition

In this section, we present the network model, and the definition of the survivable network embedding problem.

3.1. Network model

The virtual network request is represented as an undirected weighted graph $G^V=(N^V, L^V)$, where N^V is the set of virtual nodes, and L^V is the set of virtual links. The computing resource requirement of a virtual node a is