Computer Networks 91 (2015) 151–163

Contents lists available at ScienceDirect

Computer Networks

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

Towards security-aware virtual network embedding☆

Shuhao Liu[a], Zhiping Cai[a,c,*], Hong Xu[b], Ming Xu[a]

[a] College of Computer, National University of Defense Technology, Changsha, Hunan 410073, PR China
[b] Department of Computer Science, City University of Hong Kong, Tat Chee Avenue, Kowloon, Hong Kong S.A.R., China
[c] School of Computer and Software, Nanjing University of Information Science & Technology, Nanjing, Jiangsu 210044, PR China

ARTICLE INFO

Article history:
Received 2 November 2014
Revised 23 August 2015
Accepted 24 August 2015
Available online 31 August 2015

Keywords:
Cloud computing
Network virtualization
Resource allocation
Virtual network embedding

ABSTRACT

Network virtualization is one of the fundamental building blocks of cloud computing, where computation, storage and networking resources are shared through virtualization technologies. However, the complexity of virtualization exposes additional security vulnerabilities, which can be taken advantage of by malicious users. While traditional network security technologies can help in virtualized environments, we argue that it is cost-effective to isolate virtual resources with high security demands from the untrusted ones.

This paper attempts to tackle the security issue by offering physical isolation during virtual network embedding, the process of allocating virtual networks onto physical nodes and links. We start from modeling the security demands in virtualized environments by analyzing typical security vulnerabilities. A simple abstracted concept of security demands is defined to capture the variations of security requirements, based on which we formulate security-aware virtual network embedding as an optimization problem. The proposed objective and constraint functions involve both resource and security restrictions. Then, two heuristic algorithms are developed to solve this problem with splittable or unsplittable virtual links, respectively. Our simulation results demonstrate their efficiency and effectiveness.

1. Introduction

Network virtualization is one of the most important technologies for cloud computing. Infrastructure-as-a-Service providers exploit virtualization technologies to enable efficient utilization of computing and storage resources. It is also considered a key technology to accelerate innovations and to provide more stable services, by enabling new protocols and topologies to be rapidly implemented upon existing network infrastructures [1]. For example, many research testbeds rely on network virtualization to experiment new architectures [2].

Making efficient use of the substrate resources in virtualization requires effective techniques for virtual network embedding [3]. Virtual networks are usually abstracted as an undirected graph, in which nodes represent virtual machines (VMs) and links represent virtual network paths. Virtual network embedding is essentially a resource allocation problem, where a new virtual network, with constraints on the virtual nodes and links (e.g., VM computation resource demands and dedicated link bandwidth), is mapped onto capable physical nodes and paths in the substrate network. Because of the combination of node and link constraints, and the diversity of virtual topologies, virtual network embedding is NP-hard [4], and many heuristic and meta-heuristic algorithms have been developed for specific formulations of the problem.

☆ Some preliminary results were presented at IEEE ICC 2014.

* Corresponding author at: College of Computer, National University of Defense Technology, Changsha, Hunan 410073, PR China. Tel.: +86- 139- 7519- 2193.

E-mail addresses: liushuhao@nudt.edu.cn (S. Liu), zpcai@nudt.edu.cn, nudtzpcai@gmail.com (Z. Cai), henry.xu@cityu.edu.hk (H. Xu), xuming@nudt.edu.cn (M. Xu).

http://dx.doi.org/10.1016/j.comnet.2015.08.014
1389-1286/

In this paper, we study virtual network embedding from a different perspective. We consider security, which is an important, yet largely overlooked aspect in the literature. To protect all virtual networks from potential threats and to guarantee information confidentiality and integrity, in many cases users have specific security demands and requirements that have to be satisfied. These requirements are two-fold. On the one hand, virtual networks need to be embedded onto physical nodes and links with a qualified set of protection mechanisms. For example, each VM of a virtual network must be allocated onto an end system with qualified firewalls, certain data encryption functions, etc. Security requirements intuitively make the problem even more difficult due to the additional complexity of considering network resource sharing and vulnerability of current virtualization architectures. On the other hand, studies on virtualization technologies [5] show the possibility of attacks among VMs hosted on the same substrate. We show that it is necessary to offer additional physical isolation between trusted and untrusted virtual resources. However, to the best of our knowledge, there is little work that focuses on the security aspect of virtual network embedding thus far.

In order to make virtual network embedding *security-aware*, we make three concrete contributions. First, we propose a taxonomy of abstractions to properly model the security demands of virtual networks. A concept of security level is introduced to capture the availability of different protection mechanisms in the substrate. Then, the security demand of a virtual node or link is expressed in terms of security levels, and can be satisfied with physical resources that can offer the same or a higher security level. This simple abstraction is general enough to embrace many distinct forms of security mechanisms and requirements.

Second, we develop an optimization framework for security-aware network embedding, by considering both the resources and security demands of virtual networks. We present three objective functions focusing on three different major concerns of network operators: (i) the ratio of virtual networks being successfully embedded, (ii) the long-term revenue and (iii) the revenue to cost ratio (R/C ratio) of the embedding operations, respectively. Moreover, apart from resource constraints, such as node computation capacity and link bandwidth consumptions, we propose the security constraints, based on the analysis of vulnerabilities in the current virtual network architecture.

Third, we propose two novel heuristic algorithms to solve the security-aware network embedding problem. Given the conventional embedding formulation without security constraints is NP-hard, our problem with security constraints is also NP-hard. Also, in practice with economical concerns, some virtual networks may allow to split their virtual links [6], i.e., having several physical paths to jointly satisfy its bandwidth needs. This relaxation of link mapping constraints offers operators more flexibility.

Our two algorithms are designed for practical cases where splittable links are applied or forbidden, respectively. Specifically, the algorithms are both based on the same heuristic. The notion of the heuristic is to estimate the possibility and capability of each physical node to host a given virtual node and its outgoing bandwidth resources. It involves security satisfaction and node interconnection relationship in the iterative computations. The difference between these two algorithms is the coordination between node and link mapping. One algorithm simplifies the problem by decoupling the node mapping and the link mapping completely, which is known as an *uncoordinated* mapping [1] in the line of research [7–10]. We further argue that the uncoordinated method simplifies the complexity at the cost of physical resource utilization, especially in cases where virtual links are unsplittable. The other algorithm is proposed to address this issue. Using the same heuristic, it integrates node and link mappings.

Numerical simulations indicate that our algorithms are both efficient and effective. The uncoordinated algorithm works well where virtual networks allow splittable links, with quite low computation complexity. The coordinated algorithm, on the other hand, can achieve high physical resource utilization with higher execution time, even when all virtual links are unsplittable. Synthesizing them is a practical solution in large-scale real-time virtualization systems.

The rest of the paper is organized as follows. Section 2 summarizes related works in the literature. In Section 3, the security threats and requirements of virtual networks are discussed. Then, we introduce our abstraction of security demands and formulation of the security-aware embedding problems. Section 5 proposes our algorithms and Section 6 discusses the simulation results. Finally, Section 7 concludes the paper.

2. Related works

Virtual network embedding problems. As a resource allocation problem, it basically applies to various network systems with distinct environment settings. In these cases, the formulation of the virtual network embedding problem will be slightly different with specific objectives or constraints. For example, the authors in [11] and [12] represent the early attempts for virtual network embedding in the optical and wireless domain, respectively. Soualah et al. study the problem in the cloud backbone scenario [13]. Moreover, to apply the technology to systems in practice, virtual network embedding with loosed or additional constraints are studied. Yu et al. in [6] propose a seminal algorithm that enables link splitting and migration. Zhang et al. [14] study a practical case where a virtual node can be mapped onto several substrate nodes. Su et al. in [10] focus on the energy-aware virtual network embedding problem. Cai et al., in [7], focus on redeploying virtual resources and minimizing the upgrading cost in the scenario of evolving networks. Zhang et al. [15] loose the constraints in a more practical way, considering also the time-varying nature of the amount of demanded resources.

Virtual network embedding algorithms. A rich literature exists for virtual network embedding. Most work focuses on the general embedding problem, with a similar problem formulation. These proposed algorithms are usually heuristic or meta-heuristic [1], which can be categorized into two major lines. One line of work simplifies the problem by decoupling the node and link embedding process, such as in [6,9,14,16,17]. The other line, on the other hand, employs special tricks in modeling or designing heuristics to coordinate