doi:10.11959/j.issn.1000-436x.2015272

信任感知的安全虚拟网络映射算法

龚水清[1]，陈靖[1]，黄聪会[2]，朱清超[1]
(1.空军工程大学 信息与导航学院，陕西 西安 710077；2. 解放军 94543 部队，山东 济宁 272500)

摘 要：针对网络虚拟化技术带来的新的安全威胁，将信任关系和信任度引入到虚拟网络资源分配中，量化分析了网络虚拟化环境中的安全问题，构建了安全虚拟网络映射的数学模型，并在映射过程中考虑节点的局部和全局重要性，采用逼近理想排序法方法对节点进行多属性重要度排序，提出了一种信任感知的安全虚拟网络映射算法。仿真结果表明，该算法在满足虚拟网络请求可信需求的条件下，获得了较好的映射成功率、映射收益和资源利用率。
关键词：网络虚拟化；虚拟网络映射；安全；信任
中图分类号：TP393 **文献标识码**：A

Trust-aware secure virtual network embedding algorithm

GONG Shui-qing[1], CHEN Jing[1], HUANG Cong-hui[2], ZHU Qing-chao[1]
(1. College of Information and Navigation, Air Force Engineering University, Xi'an 710077, China;
2. Unit 94543 of PLA, Jining 272500, China)

Abstract: Against the new security threats brought by the network virtualization technology, the concepts of trust relationship and trust degree were introduced into the virtual network resource allocation phase. Security issues in the network virtualization environment were quantitative analyzed. A mathematical model of the secure virtual network embedding problem was modeled in order to reduce the cost. The local and global importance of network nodes were considered in the mapping phase. The network nodes were ranked by TOPSIS method, and a trust-aware virtual network embedding heuristic algorithm was proposed. Simulation results show that the proposed algorithm performs better in acceptance ratio, revenue and resource utilization.
Key words: network virtualization; virtual network embedding; security; trust

1 引言

网络虚拟化[1,2]被认为是下一代互联网的关键技术。它通过资源抽象、聚合、隔离等机制允许多个异构的虚拟网络同时运行于底层物理网络之上，共享底层基础设施资源。且每个虚拟网络可部署专用的协议和应用，为用户提供个性化的端到端网络服务，大大提高了底层网络资源利用率，增强了网络的灵活性和可控可管性，有效解决了互联网发展过程中遇到的“僵化”问题[3]，并为新兴的云计算的发展提供了技术保障，推动了云计算的发展[4]。目前，下一代互联网研究项目如 GENI 等[5]已广泛使用了网络虚拟化技术。然而，由于在网络架构中引入了额外的虚拟化层，网络虚拟化技术带来了新的安全问题，如用户攻击虚拟网络，虚拟网络之间相互攻击以及虚拟网络与底层网络之间的相互攻击等[6]。这些安全风险会破坏网络的机密性、完整性和隔离性，阻碍网络虚拟化的大规模应用和发展。因此，亟需新的安全机制和技术来应对网络虚拟化环境中新的安全威胁。

虚拟网络映射[7]作为网络虚拟化技术研究的关键问题，是指为虚拟网络中带有约束（如资源约束）的虚拟节点和链路分配底层物理网络资源的过程，

收稿日期：2015-01-15；**修回日期**：2015-05-21
基金项目：国家自然科学基金资助项目（51075395）；国家高技术研究发展计划（“863”计划）基金资助项目（2013AA040604）；陕西省自然科学基金资助项目（2015JM6340）
Foundation Items: The National Natural Science Foundation of China (51075395); The National High Technology Research and Development Program of China (863 Program) (2013AA040604); The Natural Science Foundation of Shaanxi Province (2015JM6340)

已引起了学术界的广泛关注，并进行了大量研究。由于虚拟网络映射是 NP 难问题[8]，一般不能在多项式时间内找到问题的最优解，目前大部分的研究主要以提高虚拟网络映射效率为目标，如提高物理网络收益[9]、降低映射成本[10,11]和能耗[12,13]、保持物理网络负载均衡[14]等，并设计启发式算法[9,13]或采用元启发式算法[10,14]获得近似最优解。这些虚拟网络映射算法按照不同标准[15]可分为静态[10]和动态[16,17]、集中式[11~17]和分布式[18,19]、单域[11~17]和跨域[20,21]等类别。

为了使虚拟网络免于潜在的网络攻击，确保信息的安全，用户在虚拟网络资源分配过程中往往有特定的安全需求，即需要将虚拟网络映射在具有一定安全级别的物理网络资源上。例如，虚拟网络中的节点需要映射在具有一定数据加密级别和防火墙级别的物理节点上。然而，上述虚拟网络映射算法在映射过程中均假设网络中的所有节点都安全、可信，未考虑实际应用环境中的安全需求。虚拟节点可能会被映射至不可信的物理节点上，且当物理节点受到攻击时，虚拟节点也会受到影响，进而可能导致虚拟网络服务的中断。

为此，本文将信任概念和信任度引入到虚拟网络资源分配中，在虚拟网络映射过程中除了资源约束，还考虑了虚拟节点与物理节点之间的信任关系，将节点间的信任度作为安全约束，并以此为基础，提出一种基于信任感知的安全虚拟网络映射算法（TA-SVNE, trust-aware secure virtual network embedding algorithm），可以快速高效地为有可信需求的虚拟网络请求分配物理资源。TA-SVNE 算法借鉴社会网络分析方法中的度中心性、接近度中心性和节点自身的资源能力，采用逼近理想排序法[22]TOPSIS(technique for order preference by similarity to an ideal solution)，对节点进行多属性重要度排序，并在映射过程中将较为重要的虚拟节点映射至较为重要的物理节点上，同时采用“k 最短路径法”进行链路映射，以降低虚拟网络映射成本，提高映射效率。TA-SVNE 算法通过将虚拟节点映射至满足其可信要求的物理节点上，保证了虚拟网络的安全性。

2　问题描述与网络模型

2.1　问题描述

网络虚拟化在传统的网络架构上引入了虚拟化层，允许在共享的底层物理网络之上共存多个异构的虚拟网络，大大提高了网络的灵活性，但同时也带来了新的安全风险。具体来说，网络虚拟化环境中的安全问题可以分为以下 3 种[23]。

1) 物理主机攻击虚拟机。底层网络物理主机节点负责虚拟网络虚拟机节点的管理，并在服务等级协定（SLA, service level agreement）下为其提供资源，虚拟机上运行的服务和应用最终通过物理主机上的软硬件实现。因此，当物理主机遭受攻击并被恶意用户控制时，其可以通过虚拟机管理平台修改虚拟机的信息（如网络协议）、发动嗅探攻击（sniffing attack）窃听、拦截虚拟网络上的数据分组，且虚拟机因完全由物理主机管理，无法进行防御。

2) 虚拟机攻击物理主机。恶意虚拟机通过利用物理主机的漏洞，逃脱虚拟化过程中的约束，进而攻击物理主机并获取其控制权限。此时，虚拟机可发动 DoS（denial of service）攻击，以洪泛的方式不断向物理主机注入大量的错误信息和冗余信息，占据物理主机上剩余的可用资源，导致物理网络因资源匮乏而拒绝其他虚拟网服务请求。

3) 虚拟机之间相互攻击。在网络虚拟化环境中，不同虚拟网络之间逻辑上相互隔离，但由于虚拟网络上的虚拟机节点共享相同的底层硬件资源，恶意虚拟机可通过发动跨虚拟机旁路攻击（side channel attack）来窃取同一物理主机上其他虚拟机的信息。

目前网络基础设施提供商通过不同层面为虚拟网络提供安全保障来解决上述安全问题，如通过认证和入侵检测技术防止恶意攻击、通过加密等安全策略防止敏感信息被窃取。但这些技术措施一方面过于复杂，安全成本过高；另一方面由于虚拟化环境中资源具有动态性、异构性、开放性、分布性等特点，因此这些叠加式的“被动防御”措施无法确保用户信息的安全。

信任概念源于社会科学中的人际关系网络，它被引入计算机系统，用来解决当在分布、异构、自治的大规模网络环境下跨组织之间发生的交互、共享与协作时，实体之间信任关系的建立问题[24]。在网络虚拟化环境中，信任可定义为在某时刻网络资源实体（虚拟节点或物理节点）可以可靠、安全、可信赖地提供其所宣称服务的一种信念[25]，信任度是指网络资源实体之间的信任程度。本文通过把信任度作为虚拟网络映射的依据，可以使虚拟网络资

源的分配和调度更好地围绕节点的信任关系展开，有利于将虚拟节点映射到信任度高的底层物理节点之上，满足虚拟网络请求的可信需求，从而增强网络虚拟化环境的安全性，并在一定程度上减少后续的安全开销。因此，针对上述 3 种安全问题，在虚拟网络映射过程中需考虑如下 3 种约束。

1) 虚拟机节点需映射至其信任的物理主机上。

2) 物理主机只承载其信任的虚拟机节点。

3) 只有相互信任的虚拟机节点才能映射在同一物理主机上。

节点间的信任具有主观性、非对称性和传递性等特点。信任度的评估是一个复杂的过程，它主要基于节点的直接信任度、推荐信任度、信任的衰减因素等，通过信任度的估算算法得到。通常，节点 A 对节点 B 的信任度值在 0~1 之间。值越大，说明节点 A 对节点 B 越信任，将虚拟节点 A 映射至物理节点 B 上的安全性也越高。在虚拟网络映射过程中，本文将节点间的信任关系抽象为节点的信任度需求和信任度等级。一个节点的信任度等级越高，表示网络中其他节点对其更加信任，其安全性也越高。对于虚拟节点，信任度需求表示其对物理节点和共存于同一物理节点上的其他虚拟节点的可信度要求，信任度需求越高，表示虚拟节点对周围环境的安全性要求越高。对于物理节点，信任度需求表示其对承载的虚拟节点的可信度要求，信任度需求越高，表示其对承载的虚拟节点的安全性要求越高。

基于上述讨论，得出如下 3 条在虚拟网络映射过程中需满足的基于信任度的安全约束。

1) 物理节点的信任度等级不能低于映射在其上的虚拟节点的信任度需求。

2) 虚拟节点的信任度等级不能低于其映射物理节点的信任度需求。

3) 虚拟节点的信任度需求不能高于映射在同一物理节点上其他虚拟节点的信任度等级。

2.2 网络模型

1) 物理网络

物理网络使用带权无向图 $\boldsymbol{G}_s=(N_s, L_s)$表示，其中 N_s 和 L_s 分别表示物理节点和链路的集合。对于物理节点 $n_s\in N_s$，用 CPU 资源、节点位置和信任度表示其属性，$cpu(n_s)$表示节点的可用 CPU 资源，$loc(n_s)$表示节点的地理位置，用二维坐标(x_s, y_s)表示，$trd(n_s)$和 $trl(n_s)$分别表示节点的信任度需求和信任度等级。对于物理链路 $l_s\in L_s$，带宽表示其属性，$b(l_s)$表示链路的可用带宽资源。记所有物理网络的无环路径集合为 P_s，且对任 $p\in P_s$，其可用带宽资源 $b(p)$为路径上各链路的最小可用带宽。

2) 虚拟网络请求

定义 t 时刻到达的虚拟网络请求为 $VNR(t)=(\boldsymbol{G}_v, t, t_d)$，其中 t_d 表示虚拟网络在物理网络上的生存时间，带权无向图 $\boldsymbol{G}_v=(N_v, L_v)$表示虚拟网络拓扑，$N_v$ 和 L_v 分别表示虚拟节点和虚拟链路的集合。$cpu(n_v)$、$trd(n_v)$和 $trl(n_v)$分别表示虚拟节点 $n_v\in N_v$ 的 CPU 资源需求、信任度需求和信任度等级，$loc(n_v)$表示虚拟节点的地理位置需求，$D(n_v)$表示虚拟节点可以被映射到距离位置需求的最远距离。$b(l_v)$表示虚拟链路 $l_v\in L_v$ 的带宽资源需求。

3) 安全虚拟网络映射

安全虚拟网络映射问题可以描述为在满足虚拟网络请求的资源需求和安全需求的条件下，从 $\boldsymbol{G}_v$ 到 $\boldsymbol{G}_s$ 的子图 $\boldsymbol{G}_s^{sub}$ 的映射关系，其可以进一步分为节点映射和链路映射 2 个阶段。如图 1 所示为一个安全虚拟网络映射的示例，(x, y, z)分别代表节点（物理节点或虚拟节点）的 CPU 资源需求、信任度等级和信任度需求，边上的数字代表物理链路的可用带宽资源或虚拟链路的带宽需求。图 1(b)描述了安全虚拟网络映射的一个可行方案，虚拟网络请求的节点映射方案为$\{a\to B, b\to A, c\to F\}$，链路映射方案为$\{(a, b)\to(B, A), (a, c)\to(B, F)\}$。

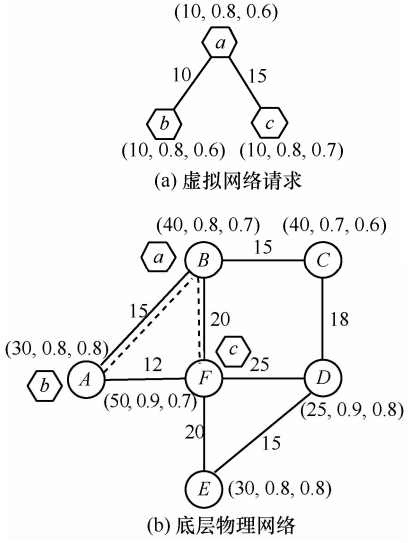

图 1 虚拟网络映射示例

2.3 映射目标

在虚拟网络映射过程中，底层物理网络需在成本最小的前提下，映射尽量多的虚拟网络请求，以

提高物理网络基础设施提供商的资源利用率和收益。因此，本文将物理网络映射收益、映射成本和虚拟网络请求接受率作为映射目标。

1) 物理网络映射收益和映射成本

虚拟网络请求 $VNR(t)$在某时刻的映射收益定义为

$$R(VNR(t))=\sum_{n_v\in N_v}(1+trd(n_v))cpu(n_v)+\sum_{l_{uv}\in L_v}b(l_{uv}) \tag{1}$$

式(1)表明虚拟网络请求的映射收益为其资源需求总和，且虚拟节点的信任度需求越高，安全收益越大，映射总收益也越大。

$VNR(t)$在某时刻的映射成本定义为

$$C(VNR(t))=\sum_{n_v\in N_v}\sum_{n_s\in N_s}x_s^v(1+trl(n_s))cpu(n_v)+\sum_{l_{uv}\in L_v}\sum_{l_{ij}\in L_s}f_{ij}^{uv}b(l_{uv}) \tag{2}$$

其中，$x_s^v\in\{0,1\}$表示虚拟节点 n_v 与物理节点 n_s 之间的映射关系，若虚拟节点 n_v 映射到物理节点 n_s 上，则 $x_s^v=1$，否则 $x_s^v=0$，$f_{ij}^{uv}\in\{0,1\}$表示虚拟链路 l_{uv} 与物理链路 l_{ij} 之间的映射关系，若虚拟链路 l_{uv} 映射到物理链路 l_{ij} 上，则 $f_{ij}^{uv}=1$，否则 $f_{ij}^{uv}=0$。式(2)表明，虚拟网络请求的映射成本为物理网络分配给虚拟网络的资源总和，且物理节点的信任度等级越高，安全成本越高，映射成本也越大。

2) 虚拟网络请求接受率

虚拟网络请求接受率定义为在一定时间内成功映射的虚拟网络请求数与总到达的虚拟网络请求数目之比，如式(3)所示。

$$\delta_{\text{accept}}=\lim_{T\to\infty}\frac{VNR_{\text{success}}}{VNR} \tag{3}$$

其中，VNR_{success} 和 VNR 分别表示从 t=0 时刻到 t=T 时刻映射成功的虚拟网络请求个数和总到达的虚拟网络请求的个数。式(3)表明，虚拟网络请求接受率越高，在一定时间内映射成功的虚拟网络请求个数越多，总映射收益也越高。

3　安全虚拟网络映射问题的数学模型

本节以最小化虚拟网络映射成本为目标，以满足虚拟网络请求的资源和安全需求为约束，将虚拟网络映射问题建模为混合整数线性规划模型（MILP, mixed integer linear program），具体过程如下。

目标函数

$$\min\sum_{n_i\in N_v}\sum_{n_j\in N_s}x_j^i(1+trl(n_j))cpu(n_i)+\sum_{l_{uv}\in L_v}\sum_{l_{ij}\in L_s}f_{ij}^{uv}b(l_{uv}) \tag{4}$$

约束条件

$\forall n_i\in N_v,\forall n_j\in N_s$，使

$$x_j^i cpu(n_i)\leqslant cpu(n_j) \tag{5}$$

$$x_j^i dis(loc(n_i),loc(n_j))\leqslant D(n_i) \tag{6}$$

$\forall l_{ij}\in L_s$，使 $\sum_{l_{uv}\in L_v}f_{ij}^{uv}b(l_{uv})\leqslant b(l_{ij})$ (7)

$\forall n_j\in N_s,\forall l_{uv}\in L_v$，使

$$\sum_{l_{ji}\in L_s}f_{ji}^{uv}-\sum_{l_{ij}\in L_s}f_{ij}^{uv}=\begin{cases}1, & x_j^u=1\\ -1, & x_j^v=1\\ 0, & \text{其他}\end{cases} \tag{8}$$

$\forall n_i\in N_v,\forall n_j\in N_s$，使

$$\begin{cases}x_j^i trd(n_i)\leqslant trl(n_j)\\ x_j^i trd(n_j)\leqslant trl(n_i)\\ x_j^i trd(n_i)\leqslant \min\limits_{n_k\in\Omega(n_j)}trl(n_k)\end{cases} \tag{9}$$

$\forall n_j\in N_s$，使 $\sum_{n_j\in N_v}x_j^i\leqslant 1$ (10)

$\forall n_i\in N_v$，使 $\sum_{n_j\in N_s}x_j^i=1$ (11)

$\forall n_i\in N_v,\forall n_j\in N_s$，使 $x_j^i\in\{0,1\}$ (12)

$\forall l_{uv}\in L_v,\forall l_{ij}\in L_s$，使 $f_{ij}^{uv}\in\{0,1\}$ (13)

式(5)为节点的 CPU 资源约束，表示虚拟节点的 CPU 资源需求不能大于物理节点的可用 CPU 资源，式(6)表示节点映射的位置约束，$dis(loc(n_i),loc(n_j))$表示虚拟节点 n_i 和底层节点 n_j 之间的欧式距离，式(7)和式(8)分别为链路的带宽资源约束和连通性约束，式(9)表示基于节点信任度的 3 种安全约束，$\Omega(n_j)$表示物理节点 n_j 上已承载的虚拟节点集合，式(10)确保同一虚拟网络内的不同节点不能映射在相同的物理节点上，式(11)确保一个虚拟节点只能映射在一个物理节点上，式(12)和式(13)为变量域约束。

4　基于 TOPSIS 的多属性节点重要性排序方法

目前，大部分虚拟网络映射算法的节点重要性排序方法主要以节点的资源能力为标准，即主要考虑节点自身的可用 CPU 资源需求和其邻接链路可用带宽资源需求或同时以这 2 种因素作为评价标准[7~9]。这类方法主要存在 2 个问题：一是由于在节点重要性排序时未考虑其拓扑属性，可能

导致逻辑上相邻的 2 个虚拟节点被映射至相距较远的底层物理节点上，从而使后续链路的映射更加困难，且造成链路资源的浪费；二是这类方法仅以节点自身资源和邻接链路资源为排序标准，只考虑了节点的局部重要性，而未考虑节点的全局重要性，不能全面衡量节点的重要程度。

社会网络分析方法的主要思想是“节点的重要性等价于显著性”。在社会网络评价方法中，节点的重要性一般用其中心性指标来衡量，一个节点越接近网络的中心，其越重要。常用的网络中心性指标有度、接近度、介数、特征向量等，这些指标从不同角度刻画了单个节点在网络中的重要程度[26]。本文借鉴社会网络节点中心度的定义，用来反映节点在物理网络和虚拟网络中的重要程度。

4.1 节点重要性分析

由于节点中心性指标的定义不同，节点重要性的评价结果也不同，本文针对虚拟网络映射问题，对所使用的几个节点中心性指标重新定义，并将节点的资源能力也作为节点的重要性评价指标。

定义 1 （度中心性）。与节点相连的所有邻接链路的带宽之和，如式(14)所示。

$$DC(n_i)=\sum_{l\in L(n_i)} b(l) \tag{14}$$

其中，$L(n_i)$表示节点 n_i 的邻接链路集合，若 n_i 为虚拟节点，则 $b(l)$表示虚拟链路 l 的带宽需求；若 n_i 为物理节点，则 $b(l)$表示物理链路 l 的可用带宽。节点的度中心性反映了其局部重要性，度中心性越大，节点与其他节点的直接通信能力越强，在网络中位置越重要。

定义 2 （接近度中心性）。节点 n_i 到网络中其他节点的距离之和的倒数，如式(15)所示。

$$CC(n_i)=\frac{1}{\sum_{n_j\in\psi(n)} d_{ij}} \tag{15}$$

其中，d_{ij} 表示节点 n_i 与 n_j 之间的最短路径的跳数，且当 $i=j$ 时，$d_{ij}=0$。若 n_i 为虚拟节点，则 $\psi(n)=N_v$。若 n_i 为物理节点，则 $\psi(n)$表示已映射物理节点的集合，且当进行初始映射时，由于 $\psi(n)$为空，此时令 $\psi(n)=N_s$。节点的接近度中心性反映了其全局重要性。若 n_i 为虚拟节点，则接近度中心性越大，节点就越接近虚拟网络的中心位置，节点就越重要；若 n_i 为物理节点，则接近度中心性越大，节点到已映射物理节点的距离越小，应越优先被选作映射物理节点，因为其使虚拟节点映射在相对集中的区域，缩短后续链路映射的距离，节省带宽资源，降低虚拟网络映射成本，所以节点也越重要。

定义 3 （资源能力）用节点的 CPU 资源表示，如式(16)所示。

$$RA(n_i)=cpu(n_i) \tag{16}$$

其中，若 n_i 为虚拟节点，则 $cpu(n_i)$表示节点的 CPU 资源需求；若 n_i 为物理节点，则 $cpu(n_i)$表示节点的可用 CPU 资源。节点的资源能力是其自身的能力因子。对于虚拟节点 n_i，节点的资源能力值越大，其映射就越困难，很可能因物理节点资源不足而导致映射失败，因此这样的节点更加重要，需优先进行映射；对于物理节点 n_i，节点的资源能力值越大，可用资源越多，可提高虚拟网络映射成功率，节点也更加重要。

4.2 MNRTOP 方法

上述 3 个节点重要性指标分别从局部或全局角度分析了节点在网络中的重要程度，但在实际网络中，仅依靠某个指标来判断节点在网络中的重要度较为片面。为此，本节综合这些指标，提出一种基于 TOPSIS 的多属性节点重要性排序方法(MNRTOP, multi-factor node ranking based on TOPSIS)。

TOPSIS 是一种多属性决策方法，它根据有限个评价对象的多个属性与理想目标的接近程度进行排序。本文将虚拟网络或物理网络中的每一个节点作为一个方案，将节点重要性的多个评价指标看作各方案的属性，那么节点重要性的评价就转化为一个多属性决策问题[26]。

MNRTOP 共分为 6 个步骤。

步骤 1 考虑网络中有 N 个节点，每个节点有 M 个重要性评价指标，记第 i 个节点的第 j 个评价指标值为 x_{ij}，则重要性决策矩阵为

$$\boldsymbol{X}_{N\times M}=\begin{bmatrix} x_{11} & \cdots & x_{1M} \\ \vdots & \ddots & \vdots \\ x_{N1} & \cdots & x_{NM} \end{bmatrix} \tag{17}$$

步骤 2 由于各指标量纲和指标优劣的取向不同，为便于比较，对各指标的初始数据做无量纲标准化处理，得到标准化决策矩阵 $\boldsymbol{X}'_{N\times M}$，如式(18)所示。其中，对于正向性指标，即指标值越大越好，$x'_{ij}=\dfrac{x_{ij}-\min\limits_{1\leqslant k\leqslant N} x_{kj}}{\max\limits_{1\leqslant k\leqslant N} x_{kj}-\min\limits_{1\leqslant k\leqslant N} x_{kj}}$；对于负向性指

标，$x'_{ij}=\dfrac{\max\limits_{1\leqslant k\leqslant N}x_{kj}-x_{ij}}{\max\limits_{1\leqslant k\leqslant N}x_{kj}-\min\limits_{1\leqslant k\leqslant N}x_{kj}}$。

$$\boldsymbol{X}'_{N\times M}=\begin{bmatrix}x'_{11}&\cdots&x'_{1M}\\ \vdots&\ddots&\vdots\\ x'_{N1}&\cdots&x'_{NM}\end{bmatrix} \tag{18}$$

步骤 3　记第 j 个评价指标的权重为 $\omega_j(j=1,2,\cdots,M,0\leqslant\omega_j\leqslant 1,\sum_{j=1}^{M}\omega_j=1)$，则加权标准化决策矩阵如式(19)所示，其中 $x''_{ij}=\omega_j x'_{ij}$。

$$\boldsymbol{X}''_{N\times M}=\begin{bmatrix}x''_{11}&\cdots&x''_{1M}\\ \vdots&\ddots&\vdots\\ x''_{N1}&\cdots&x''_{NM}\end{bmatrix} \tag{19}$$

步骤 4　记最理想的决策方案为 A^+和最劣的决策方案为 A^-，则

$$\begin{aligned}A^+&=\{x_1^+,x_2^+,\cdots,x_M^+\}\\&=\{\max_{1\leqslant i\leqslant N}x_{i1}^{"},\max_{1\leqslant i\leqslant N}x_{i2}^{"},\cdots,\max_{1\leqslant i\leqslant N}x_{iM}^{"}\}\end{aligned} \tag{20}$$

$$\begin{aligned}A^-&=\{x_1^-,x_2^-,\cdots,x_M^-\}\\&=\{\min_{1\leqslant i\leqslant N}x_{i1}^{"},\min_{1\leqslant i\leqslant N}x_{i2}^{"},\cdots,\min_{1\leqslant i\leqslant N}x_{iM}^{"}\}\end{aligned} \tag{21}$$

步骤 5　计算每个方案到最理想的方案 A^+和最劣的方案 A^-的欧式距离，即

$$D_i^+=\sqrt{\sum_{j=1}^{M}(x_{ij}^{"}-x_j^+)^2} \tag{22}$$

$$D_i^-=\sqrt{\sum_{j=1}^{M}(x_{ij}^{"}-x_j^-)^2} \tag{23}$$

步骤 6　计算各方案距理想方案的接近程度 C_i，如式(24)所示，并按照 C_i 对节点进行重要度排序。C_i 越大，则节点在网络中的重要性越高。

$$C_i=\frac{D_i^-}{D_i^++D_i^-} \tag{24}$$

5　TA-SVNE 算法设计

由于安全虚拟网络映射的 MILP 模型是 NP 难问题，本节设计了 TA-SVNE 启发式算法对此问题进行求解。TA-SVNE 算法分为基于 MNRTOP 的节点映射和基于 k 最短路径法的链路映射 2 个阶段。

5.1　节点映射

本文选用节点的度中心性、接近度中心性和资源能力作为其重要性评价属性，采用 MNRTOP 方法对虚拟网络和物理网络中的节点进行重要度排序，并基于此排序结果进行节点映射，使较为重要的虚拟节点能够映射到物理网络中较为重要的物理节点上。节点映射算法的主流程如算法 1 所示。

算法 1　TA-SVNE 的节点映射

输入：$\boldsymbol{G}_s$, $VNR(t)$

1) for 每一个虚拟节点 $n_v\in N_v$ do

2)　　计算 n_v 的 $DC(n_v)$、$CC(n_v)$和 $RA(n_v)$

3) end for

4) 采用 MNRTOP 方法对 $n_v\in N_v$ 排序，并将排序结果存入链表 *VirtualNodeList* 中

5) for *VirtualNodeList* 中的每一个虚拟节点 n_v do

6)　　构建 n_v 的候选映射节点集合 $\Theta(n_v)$

7)　　if $\Theta(n_v)$为空 then

8)　　return NODE_MAPPING_FAILED

9)　　else

10)　　for $\Theta(n_v)$中的每一个候选节点 n_s do

11)　　计算 n_s 的 $DC(n_s)$、$CC(n_s)$和 $RA(n_s)$，其中 $RA(n_s)$按照式(25)计算

12)　　end for

13)　　采用 MNRTOP 方法对 $\Theta(n_v)$中的候选节点进行排序，将 n_v 映射至重要度最高的候选节点上，并将映射结果存入 *NodeMappingList* 中

14)　　end if

15) end for

输出 *NodeMappingList*

由式(2)可知，若物理节点的信任度等级越高，则映射成本越高。因此，在节点映射过程中，在满足资源需求和安全需求的前提下，虚拟节点应映射至信任度等级较低的物理节点上，以降低安全成本。为此，对物理节点的资源能力做如下改进。

对于 $n_v\in N_v$，首先按照 CPU 资源约束式(5)、节点位置约束式(6)和安全约束式(9)选出其候选物理映射节点集合 $\Theta(n_v)$。对于 $n_s\in\Theta(n_v)$，其资源能力定义如下

$$RA(n_s)=cpu(n_s)e^{trd(n_s)-trl(n_s)},\ trd\leqslant trl \tag{25}$$

式(25)表明，若虚拟节点的信任度需求与候选物理映射节点的信任度等级差距越小，则该候选物理节点的资源能力越强，若将虚拟节点映射至此节点上，可降低映射安全成本。因此，该节点更加重要，应优先被选为映射物理节点。

5.2　链路映射

链路映射是指在满足带宽资源约束的条件下，

将虚拟链路映射到物理网络中的无环路径上。由于不同虚拟链路映射至物理网络中的不同路径之间可能存在相同链路，这些路径会同时竞争物理链路有限的带宽资源，使带宽资源需求高的虚拟链路映射更加困难，很可能由于物理网络链路带宽资源不足而导致映射失败。因此，在链路映射阶段，应优先选择带宽资源需求高的虚拟链路进行映射。在此基础上，采用 k 最短路径方法[27]，在物理网络中寻找满足带宽需求的 2 个被映射虚拟节点之间的第 k 短路径，并将虚拟链路映射至此路径上。算法 2 为链路映射算法的主流程。

算法 2 TA-SVNE 的链路映射

输入：$\boldsymbol{G}_s$, $VNR(t)$, *NodeMappingList*

1) 按照带宽需求从大到小顺序对 $l_{uv} \in L_v$ 排序，并将排序结果存入链表 *VirtualLinkList* 中

2) for *VirtualLinkList* 中的每一条虚拟链路 l_{uv} do

3) 采用 k 最短路径法计算虚拟节点 n_u 和 n_v 的映射物理节点之间的 k 条最短路径，并将结果存入 *PathList* 中

4) for k=1 & $k \leqslant$ *MAX_K* do

5) if $b(PathList(k)) \geqslant b(l_{uv})$ then

6) 将 l_{uv} 映射至第 k 短路径 *PathList*(k)上，并将映射结果存入 *LinkMappingList* 中

7) break

8) else

9) $k = k+1$

10) end if

11) end for

12) if $k >$ *MAX_K* then

13) return LINK_MAPPING_FAILED

14) end if

15) end for

输出：*LinkMappingList*

6 性能评估与分析

为了验证算法的有效性，本节对 TA-SVNE 算法和之前研究中提出的算法进行对比仿真实验，并从虚拟网络请求接受率、物理网络映射收益、映射成本、收益成本比和运行时间等方面讨论 TA-SVNE 算法的性能。

6.1 仿真环境

实验中物理网络和虚拟网络请求均使用 GT-ITM 拓扑生成器产生。物理网络包含 100 个节点，节点间的链路连接概率为 0.5，相当于一个中等 ISP 的规模。物理节点的 CPU 资源和物理链路的带宽资源均服从[50,100]的均匀分布，其位置 x 与 y 坐标均服从[0,100]的均匀分布。虚拟网络请求随机生成，其到达过程服从时间单元为 100，到达个数期望为 5 的泊松分布。每个虚拟网络请求的生存时间服从期望为 1 000 个时间单元的指数分布，虚拟节点的数目服从[2,10]的均匀分布，节点间的连接概率为 0.5。每个虚拟节点的 CPU 资源需求和链路带宽资源需求均服从[0,50]的均匀分布，其位置 x 与 y 坐标均服从[0,50]的均匀分布，且假设所有虚拟节点的位置距离约束量 D 取常量 50。此外，虚拟节点和物理节点的信任度需求和信任度等级均服从[0,1]的均匀分布，k 最短路径算法中的 k 设置为 5，式(19)中 3 种节点重要性评价指标的权重均设置为 $\frac{1}{3}$。整个仿真运行时间设定为 50 000 个时间单位，总共包含 2 500 个虚拟网络请求，这样能使实验的运行进入比较稳定的状态。由于虚拟网络请求随机生成，为避免随机因素对实验结果产生扰动，仿真实验共进行 10 次，并取实验结果的平均值作为最终仿真结果。

本文进行了 4 种算法的比较。TA-SVNE 算法和 NTA-SVNE 算法为本文提出的算法。TA-SVNE 算法的物理节点资源能力重要度评价属性采用式(25)计算。NTA-SVNE 算法采用式(16)计算物理节点资源能力重要度评价属性，节点映射过程中未考虑安全成本因素，以此测试 TA-SVNE 算法能否有效降低映射成本。BL1 算法是基于 D-ViNE 映射算法[11]，并在节点映射过程中加入了安全约束式(9)，映射收益和成本依据式(1)和式(2)进行了相应修改。BL2[8]算法在节点映射阶段采用贪婪策略，在节点排序时仅考虑自身 CPU 资源和其邻接链路带宽资源，链路映射采用 k 最短路径法。同时为便于比较，在节点映射时新增了安全约束。

6.2 仿真结果分析

本节以虚拟网络请求接受率、物理网络映射收益、映射成本、收益成本比和运行时间作为算法的性能评价指标，对 TA-SVNE、NTA-SVNE、BL1 和 BL2 算法进行性能分析。图 2~图 6 和表 1 分别表示 4 种算法在上述 5 个性能评价指标下的实验结果。

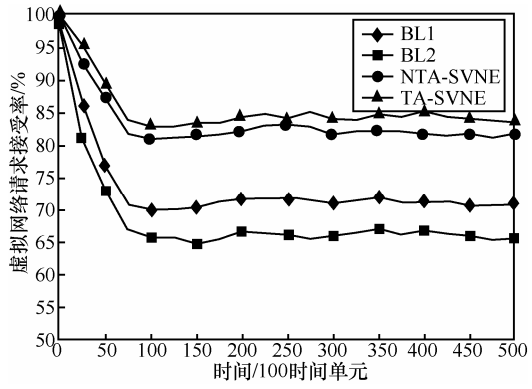

图 2　虚拟网络请求接受率

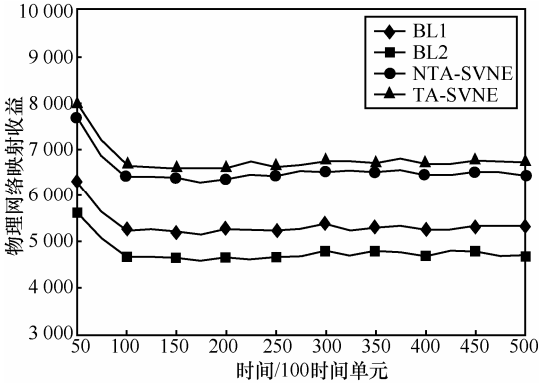

图 3　物理网络映射收益

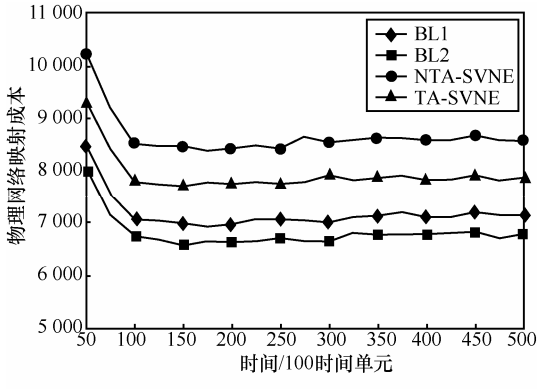

图 4　物理网络映射成本

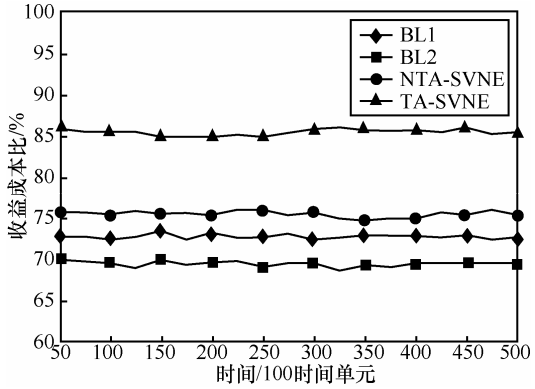

图 5　物理网络映射收益成本比

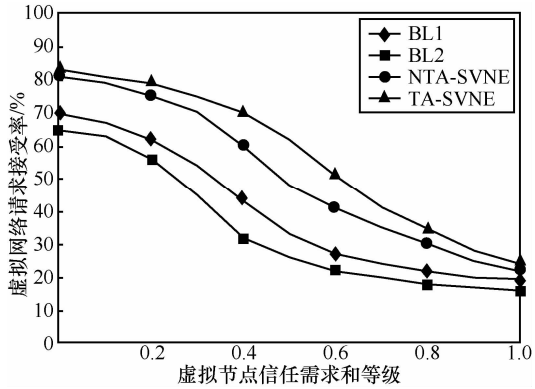

图 6　虚拟网络请求接受率随信任度需求和等级增大的变化

1) 虚拟网络请求接受率

图 2 为 4 种算法的虚拟网络请求接受率随时间的变化情况。从图 2 中可以看出，由于初始时段物理网络可用资源较为丰富，4 种算法的虚拟网络请求接受率都较高。随着资源的逐步消耗，接受率逐渐下降，在 7 500 个时间单位后，接受率趋于稳定。TA-SVNE 和 NTA-SVNE 算法的虚拟网络请求接受率比较接近，分别稳定在 83%和 81%左右，比 BL1 算法（约 70%）和 BL2（约 65%）提高了 11%~18%。主要原因在于 TA-SVNE 和 NTA-SVNE 算法在节点映射过程中考虑了节点的局部和全局重要性，将虚拟节点集中映射到 CPU 资源和邻接链路带宽资源较为丰富的底层物理节点上，使后续链路映射更容易成功，并缩短了链路映射距离，降低了映射成本，使物理网络有更多的资源接受新的虚网请求，从而提高了虚网请求接受率。而在 BL1 和 BL2 算法映射过程中未考虑节点拓扑属性，使节点映射和链路映射的协调性较差，降低了虚拟网络映射的成功率。

2) 物理网络映射收益、成本和收益成本比

图 3 为 4 种算法的物理网络映射收益随时间的变化情况，由图 3 可知 TA-SVNE 和 NTA-SVNE 算法的映射收益比较接近，比算法 BL1 和 BL2 高出约 19%~41%。图 4 为 4 种算法的物理网络映射成本随时间的变化情况，由图 4 可知 NTA-SVNE 算法的映射成本最高，TA-SVNE 算法明显降低了映射成本（约 9%），BL2 算法最低。图 5 为 4 种算法的物理网络映射收益成本比随时间的变化情况，由图 5 可知 TA-SVNE 算法的收益成本比最高（约 85%），比算法 NTA-SVNE（约 75%）、BL1（约 73%）和 BL2（约 69%）高出 10%~16%，可见 TA-SVNE 算法的映射效率最高。主要原因是在 TA-SVNE 算法

的节点映射过程中，在满足安全约束的前提下将虚拟节点优先映射在信任度等级较低的物理节点上，从而降低了映射安全成本，同时考虑了节点的全局拓扑属性，使节点映射的区域较为集中，降低了后续链路映射的成本，提高了虚网请求接受率，使在相同时间内映射成功的虚拟网络请求比其他 2 种算法多，进而映射收益较高。而 NTA-SVNE 算法在节点映射过程中未考虑安全成本因素，使整体映射成本较高。BL1 和 BL2 算法的虚拟网络请求接受率较低，因而映射收益和成本较其他 2 个算法低，但由于这 2 种算法在节点映射过程中未考虑安全成本因素，且节点映射和链路映射的协调性较差，使链路映射成本较高，因此其映射收益成本比较低。

3) 运行时间

表 1 为 4 种算法虚拟网络请求的平均映射求解时间。从表 1 可看出，与 BL1 相比，TA-SVNE、NTA-SVNE 和 BL2 的虚拟网络映射所需时间降低了约 40%~48%。主要原因是 TA-SVNE、NTA-SVNE 和 BL2 采用启发式算法求解，时间复杂度小，而 BL1 算法采用松弛技术求解虚拟网络映射的 MILP 模型，时间复杂度高，且随问题规模的增长而呈指数增加。

表 1　　算法运行时间

算法	运行时间/s
TA-SVNE	1.36
NTA-SVNE	1.33
BL1	2.25
BL2	1.18

4) 不同类型虚拟网对虚拟网络请求接受率的影响

上述研究侧重在横向上比较不同算法之间的性能指标，而未考虑不同类型的虚拟网请求对算法性能的影响。在实际中，不同类型虚拟网络请求的安全需求存在很大的不同。有的网络对安全性要求很高，如军事网络、电子商务、网上银行等，而有的网络对安全性要求较低。因此，本文研究了在不同信任度需求的虚拟网络请求下 4 种算法的映射成功率的变化，以考察算法的执行效率。在实验中，将虚拟网络中节点的信任度需求和信任度等级均设置在[x,1]的均匀分布，x 为虚拟节点的信任度需求和等级分布区间的下界，即图 6 中的 x 坐标变量。随着 x 的增大，虚拟网络请求的安全需求逐渐增大。实验中其他仿真环境参数保持不变。由图 6 可知，随着虚拟网络节点的信任度需求和信任度等级逐渐增大，4 种算法的虚拟网络请求接受率都逐渐降低，且当 $x \geqslant 0.3$ 时，接受率的下降速度明显加快，但 TA-SVNE 算法的映射接受率下降速度最慢，NTA-SVNE 次之，BL1 和 BL2 算法下降速度最快。这说明 TA-SVNE 算法的执行效率较高，且当 $0.3 \leqslant x \leqslant 0.6$ 时，TA-SVNE 算法的优势更为明显。

7 结束语

网络虚拟网技术由于在网络架构中引入了虚拟化层，带来了新的安全威胁。本文针对这一问题，将信任概念和信任度引入到虚拟网络映射中，量化分析了虚拟网络的安全问题，并以此为基础，构建了安全虚拟网络映射的 MILP 模型，提出了 TA-SVNE 映射算法。为了提高映射效率，TA-SVNE 算法在节点映射过程中借鉴社会网络中心度理论，以度中心性、接近度中心性以及资源能力作为节点的重要度属性，采用 TOPSIS 方法对节点进行多属性重要度排序，并在映射过程中将重要的虚拟节点映射在较为重要的物理节点上，同时采用 k 最短路径法进行链路映射。仿真结果表明，TA-SVNE 算法在虚拟网络请求接受率、映射收益和运行时间等方面具有一定优势，并具备较高的映射效率。但该算法只考虑了节点间的信任关系，不足以应对网络虚拟化环境中的多种安全威胁。下一步需在细粒度研究网络虚拟化环境中安全问题的基础上，扩展算法以考虑虚拟网络映射过程中更多的安全约束条件。

参考文献：

[1] KHAN A, ZUGENMAIER A, JURCA D, *et al*. Network virtualization: a hypervisor for the Internet?[J]. IEEE Communications Magazine, 2012, 50(1): 136-143.

[2] WANG A, IYER M, DUTTA R, *et al*. Network virtualization: technologies, perspectives, and frontiers[J]. Journal of Lightwave Technology, 2013, 31(4): 523-537.

[3] ANDERSON T, PETERSON L, SHENKER S, *et al*. Overcoming the Internet impasse through virtualization[J]. Computer, 2005, 38(4): 34-41.

[4] BARI M, BOUTABA R, ESTEVES R, *et al*. Data center network virtualization: a survey [J]. IEEE Communications Surveys and Tutorials, 2013, 15(2): 909-928.

[5] BERMAN M, CHASE J S, LANDWEBER L, *et al*. GENI: a federated testbed for innovative network experiments[J]. Computer Networks, 2014, 61: 5-23.

[6] NATARAJAN S, WOLF T. Security issues in network virtualization for the future Internet[A]. Proceedings of the IEEE ICNC[C]. Maui, HI, 2012: 537-543.

[7] FISCHER A, BOTERO J F, BECK M T, *et al*. Virtual network embedding: a survey[J]. IEEE Communications Surveys & Tutorials, 2013, 15(4): 1888-1906.

[8] YU M L, YI Y, REXFORD J, *et al*. Rethinking virtual network embedding: substrate support for path splitting and migration[J]. ACM SIGCOMM Computer Communication Review, 2008, 38(2): 17-29.

[9] HSU W H, SHIEH Y P. Virtual network mapping algorithm in the cloud infrastructure[J]. Journal of Network and Computer Applications, 2013, 36(6): 1724-1734.

[10] FAJJARI I, AITSAADI N, PIÓRO M, *et al*. A new virtual network static embedding strategy within the Cloud's private backbone network[J]. Computer Networks, 2014, 62: 69-88.

[11] CHOWDHURY N M M K, RAHMAN M R, BOUTABA R. Virtual network embedding with coordinated node and link mapping[A]. Proceedings of the IEEE INFOCOM[C]. Rio de Janeiro, 2009. 783-791.

[12] SU S, ZHANG Z, LIU A X, *et al*. Energy-aware virtual network embedding[J]. IEEE/ACM Transactions on Networking, 2014, 22(5): 1607-1620.

[13] BOTERO J F, HESSELBACH X. Greener networking in a network virtualization environment[J]. Computer Networks, 2013, 57(9): 2021-2039.

[14] 黄彬彬, 林荣恒, 彭凯, 等. 基于粒子群优化的负载均衡的虚拟网络映射[J]. 电子与信息学报, 2013, 35(7): 1753-1759.
HUANG B B, LIN R H, PENG K, *et al*. Load-balancing based on particle swarm optimization in virtual network mapping[J]. Journal of Electronics & Information Technology, 2013, 35(7): 1753-1759.

[15] 程祥, 张忠宝, 苏森, 等. 虚拟网络映射问题研究综述[J]. 通信学报, 2011, 32(10): 143-151.
CHENG X, ZHANG Z B, SU S, *et al*. Survey of virtual network embedding problem[J]. Journal on Communications, 2011, 32(10): 143-151.

[16] 罗娟, 徐岳阳, 李仁发. 网络虚拟化中动态资源分配算法研究[J]. 通信学报, 2011, 32(7): 64-70.
LUO J, XU Y Y, LI R F. Dynamical resource allocation algorithm research in network virtualization[J]. Journal on Communications, 2011, 32(7): 64-70.

[17] SUN G, YU H, ANAND V, *et al*. A cost efficient framework and algorithm for embedding dynamic virtual network requests[J]. Future Generation Computer Systems, 2013, 29(5): 1265-1277.

[18] HOUIDI I, LOUATI W, ZEGHLACHE D, *et al*. Adaptive virtual network provisioning[A]. Proceedings of the second ACM SIGCOMM workshop on Virtualized infrastructure systems and architectures[C]. New York, 2010. 41-48.

[19] 江逸茗, 兰巨龙, 程东年, 等. 分布式环境中基于协商的虚拟网映射算法[J]. 通信学报, 2014, 35(12): 62-69.
JIANG Y M, LAN J L, CHENG D N, *et al*. Virtual network embedding algorithm based on negotiation in distributed environment[J]. Journal on Communications, 2014, 35(12): 62-69.

[20] HOUIDI I, LOUATI W, AMEUR W B, *et al*. Virtual network provisioning across multiple substrate networks[J]. Computer Networks, 2011, 55(4): 1011-1023.

[21] SHEN M, XU K, YANG K, *et al*. Towards efficient virtual network embedding across multiple network domains[A]. Proceedings of the IEEE IWQoS[C]. Hong Kong, 2014. 61-70.

[22] LAI Y J, LIU T Y, HWANG C L. Topsis for MODM[J]. European Journal of Operational Research, 1994, 76(3): 486-500.

[23] FISCHER A, MEER H D. Position paper: secure virtual network embedding[J]. Praxis der Information sverarbeitung und Kommunikation, 2011, 34(4): 190-193.

[24] 王勇, 代桂平, 侯亚荣. 信任感知的组合服务动态选择方法[J]. 计算机学报, 2009, 32(8): 1668-1675.
WANG Y, DAI G P, HOU Y R. Dynamic methods of trust-aware composite service selection[J]. Chinese Journal of Computer, 32(8): 1668-1675.

[25] 曹洁, 曾国荪, 姜火文, 等. 云环境下服务信任感知的可信动态级调度方法[J]. 通信学报, 2014, 35(11): 39-49.
CAO J, ZENG G S, JIANG H W, *et al*. Trust-aware dynamic level scheduling algorithm in cloud environment[J]. Journal on Communications, 2014, 35(11): 39-49.

作者简介：

龚水清（1987-），男，湖南桃江人，空军工程大学博士生，主要研究方向为网络虚拟化、软件定义网络等。

陈靖[通信作者]（1963-），女，陕西西安人，空军工程大学教授、博士生导师，主要研究方向为无线自组织网络、网络虚拟化、软件定义网络等。E-mail:jingchen0803@163.com。

黄聪会（1985-），男，湖南衡阳人，94543 部队工程师，主要研究方向为计算系统虚拟化、网络虚拟化等。

朱清超（1987-），男，山东济宁人，空军工程大学博士生，主要研究方向为无线自组织网络。