基于风险感知的关键虚拟网络功能动态迁移方法

丁绍虎，谢记超，张鹏，普黎明，谷允捷
（信息工程大学信息技术研究所，河南 郑州 450002）

摘 要：针对传统动态迁移方法在应对侧信道攻击问题时存在迁移节点多、迁移频率高、迁移后服务功能链路径过长的问题，提出了一种基于风险感知的关键虚拟网络功能动态迁移方法。所提方法仅对含隐私信息的关键虚拟网络功能进行迁移，以减少迁移节点数量；结合侧信道攻击检测系统，对遭受攻击的关键虚拟网络功能执行触发式迁移，同时依据侧信道信息泄露模型对关键虚拟网络功能进行定期式迁移；采用基于逼近理想解排序的多属性节点排序方法选择迁移目的服务器，以避免迁移后路径过长。实验结果表明，所提方法在达到相同的侧信道攻击防御性能的情况下，具有更低的节点迁移数量与迁移频率，同时有效避免了迁移后服务功能链路径过长问题。

关键词：服务功能链；虚拟网络功能；侧信道攻击；动态迁移；多属性节点排序
中图分类号：TP393
文献标识码：A
doi: 10.11959/j.issn.1000−436x.2020063

Dynamic migration method of key virtual network function based on risk awareness

DING Shaohu, XIE Jichao, ZHANG Peng, PU Liming, GU Yunjie
Institute of Information Technology, Information Engineering University, Zhengzhou 450002, China

Abstract: Aiming at the problems that traditional dynamic migration methods have many migration nodes, high migration frequency, and long service function chain (SFC) link path after migration when dealing with side channel attack, a dynamic migration method of critical virtual network function (VNF) based on risk awareness was proposed. In order to reduce the number of migrated nodes, only the key VNF with private information was migrated. Combined with the side channel attack detection system, the triggering migration was performed on the critical VNF which were under attack, and the key VNF was also periodically migrated according to the side channel information leakage model. Finally, a multi-attribute node sorting method base on the technique for order preference by similarity to ideal solution was used to select the migration destination server to avoid the path being too long after migration. Experiments show that the proposed method has a lower number of migration nodes and migration frequency when achieving the same side channel attack defense performance, and effectively avoids the problem that the SFC path is too long after migration.

Key words: service function chain, virtual network function, side-channel attack, dynamic migration, multi-attribute node sorting

1 引言

随着新兴网络服务和业务模式的飞速发展，传统的基于专用硬件的服务功能链（SFC, service function chain）部署方式存在的问题日益凸显[1-2]，如成本高、资源利用率低、新服务上线周期长等。

收稿日期：2019−12−06；**修回日期**：2020−03−03
通信作者：谢记超，912104210329@njust.edu.cn
基金项目：国家自然科学基金资助项目（No.61802429, No.61872382, No.61521003）；国家重点研发计划基金资助项目（No.2017YFB0803201, No.2017YFB0803204）
Foundation Items: The National Natural Science Foundation of China (No.61802429, No.61872382, No.61521003), The National Key Research and Development Program of China (No.2017YFB0803201, No.2017YFB0803204)

网络功能虚拟化基础设施即服务（NFVIaaS, network function virtualization infrastructure as a service）模式的出现为解决当前网络服务提供方式所面临的困境提供了有效途径，其主要思想是，租户按需租用云服务提供商池化的资源，将所需的网络功能以虚拟网络功能（VNF, virtual network function）软件的形式运行在通用硬件设备中，即可灵活、高效地构建网络服务所需的 SFC。然而，这种新型的 SFC 部署方式面临许多新的安全挑战，主要分为 NFV 特有的安全威胁、通用网络安全威胁和通用虚拟化安全威胁[3-4]，本文重点关注通用虚拟化安全威胁中 VNF 面临的侧信道攻击[5-8]问题。侧信道攻击是当前云计算环境下多租户间信息泄露的重要途径。

在 NFVIaaS 的多租户环境下，云服务提供商借助虚拟化技术的逻辑隔离手段实现了物理资源在多租户间的高效复用，然而，这也为恶意租户实施侧信道攻击提供了可能。恶意租户在成功实现与目标租户 VNF 共存后，可利用共享硬件资源（如 CPU、内存、磁盘、网络）构建各种类型的侧信道突破逻辑隔离，进而从共存的 VNF 中获取隐私信息和敏感数据，范围可从粗粒度的工作负载、流量速率到细粒度的加密密钥等[3]。因此，能否抵抗 NFVIaaS 所面临的侧信道攻击，将直接影响 NFVIaaS 商业模式的推广。

在相关虚拟机部署和虚拟网映射领域，针对侧信道攻击的防御方法主要分为以下四类，可在侧信道攻击的实施进程中依次展开。第一类方法是使用部署策略提高共存难度[9-11]，该类方法可显著提高恶意租户在实施侧信道攻击前创造共存条件的难度，但是无法解决已共存节点所面临的侧信道攻击风险；第二类方法是增加验证共存的难度[12]，但是相关研究表明，恶意租户仍可不断开发出新的验证共存手段；第三类方法是消除侧信道[13]，该类方法通常需要详细的针对特定攻击方法的修复，不能覆盖未来不断被发掘出的侧信道攻击手段，不具备防御各类侧信道攻击手段的通用性；第四类方法是定期迁移[14-16]和触发迁移[17]，该类方法在防御各类侧信道攻击时具有良好的通用性，但是在迁移过程中会造成一定时间的服务中断，影响服务质量。相关防御方法可相互结合，从而构建复合的防御体系，全方位提高恶意租户实现侧信道攻击的难度。

已有的研究工作中，伊鹏等[18]针对现有服务功能链部署方法下恶意租户实现 VNF 共存的难度小、代价低的问题，提出了一种基于租户分类与历史信息的服务功能链部署方法，该部署方法在初始部署阶段较大幅度提高了潜在恶意租户对目标租户实施侧信道攻击的难度和代价，但不能解决已共存 VNF 所面临的侧信道攻击风险，租户 VNF 若长期与某一未知租户的 VNF 共存，则其所含隐私信息依然面临着一定的安全隐患。因此，本文从 VNF 在同一位置部署时长的时间纬度出发，引入 VNF 的迁移方法，以解决租户 VNF 长期与某一未知租户 VNF 共存时其隐私信息面临的安全隐患。

在相关领域，迁移方法是防御侧信道攻击的一类重要可行手段，但是相关迁移方法应用于 VNF 领域时仍存在一些缺陷。Moon 等[15]首次对侧信道信息泄露进行建模，总结了影响信息泄露速率的 3 个重要因素，即共存时间、攻击者虚拟机（VM, virtual machine）间是否协同以及目标 VM 间隐私信息是否一致，基于此所建立的信息泄露模型具有很好的参考价值，但所设计的定期式迁移方法存在以下缺陷：需要对所有节点进行迁移，存在迁移节点过多和开销过大的问题；若以较低的迁移频率进行迁移，则不能防御一些快速的侧信道攻击；应用于 VNF 迁移领域时，不能简单地将需求抽象为 VM 插槽，需要深入考虑服务器支持 VNF 的类型约束和资源约束等；此外，进行迁移时需要考虑 SFC 严格有序的链式结构，避免迁移后 SFC 路径过长问题。赵硕等[14]在 Moon 等[15]的研究基础上，为了降低节点迁移数量与迁移频率，提出了基于安全等级的虚拟节点迁移方法，通过 VM 安全等级分类，对租户定义的关键 VM 执行定期式迁移，显著降低了 VM 迁移数量和频率，但该方法采用的基于安全等级的分域部署策略存在一定缺陷，关键 VM 由租户自行设定，分类具有租户主观性，使恶意租户可通过高安全需求的资源请求实现与高安全需求租户的轻易共存。Zhang 等[17]提出对侧通道攻击进行实时检测，并采用触发式的 VM 迁移方法来防止信息泄露，虽然可显著降低迁移频率与迁移开销，但是需要掌握相关侧信道攻击手段的具体特征，难以应对众多特征未知的侧信道攻击手段，此外相关侧信道攻击检测系统需要额外部署软件甚至硬件，会产生一定的服务器资源开销，对性能有一定影响。

本文在相关研究的基础上，针对现有迁移方法存在的局限性，提出了一种基于风险感知的关键虚

拟网络功能动态迁移方法，目标是在较大幅度降低已共存 VNF 所面临的侧信道攻击风险的前提下，解决 VNF 迁移节点多、迁移频率高、迁移后 SFC 路径过长的问题。

2 问题描述与模型建立

2.1 符号定义

本文所采用的相关符号定义与先前的研究工作[18]一致。表 1 对本文所采用的关键符号及其定义进行了表述。

2.2 VNF 迁移问题描述

利用云计算的技术优势，租户可根据实际需求按需租用资源，灵活高效地构建网络服务所需的服务功能链（如 Web 服务、邮件服务等）。服务功能链部署如图 1 所示。2 条服务功能链请求实例如图 1 上部所示，每条服务功能链分别含有 3 个 VNF 节点，为了便于描述，本文简化了租户实际需要的 VNF 数量以及所需的 VNF 类型。云服务提供商根据租户请求，结合云平台资源状态，按照设定的规则和策略将租户的服务功能链请求部署到云平台，图 1 展示了 2 条服务功能链请求在云平台中的部署情况，服务功能链 1 的 3 个 VNF 分别部署在服务器节点 N_1、N_5 和 N_3，服务功能链 2 的 3 个 VNF 分别部署在服务器节点 N_4、N_5 和 N_6。

为了充分发挥云计算的优势，实现云资源的高效复用，云服务提供商借助虚拟化技术实现逻辑隔离，使多租户间可共享底层基础设施。如图 1 中所示，2 条服务功能链中的 VNF 共用了服务器节点 N_5，然而这种共享资源模式在为租户带来巨大成本优势的同时也引入了安全风险。

表 1 关键符号定义

符号	描述	符号	描述
$\bar{G}=(\bar{N},\bar{S},\bar{L})$	底层物理网络	$\bar{u}^r,\bar{v}^r$	接入交换机和出口交换机
$\bar{N},\bar{S},\bar{L}$	通用服务器集合、交换机集合和物理链路集合	β^r	服务链 r 所需处理的流量大小
n,s,l	底层网络中服务器、交换机和物理链路总数	τ^r	请求 r 的生命周期
$\boldsymbol{B}_{s\times s}$	交换机连接矩阵	ψ^r	处理流量所需的 VNF 序列
$B_{i,j}\in R^+$	交换机节点 i 到 j 的通信链路容量	m	请求中 VNF 的总数量
$V=\Lambda(u)=\{v\mid B_{u,v}>0\}$	与交换机 u 直连的交换机集合	$\mathrm{VNF}_i^r\in P=\{1,2,\cdots,p\}$	请求 r 中第 $i\in\{1,2,\cdots,m\}$ 个 VNF 的类型
$\boldsymbol{H}_{n\times s}$	服务器与交换机连接矩阵	$G^r=(N^r,L^r)$	SFC 请求有向图
$H_{i,j}\in\{0,1\}$	服务器节点 i 是否连接在交换机 j 上	N^r	节点（接入交换机、VNF、出口交换机）集合
K,k	服务器资源类型集合和资源类型总数量	L^r	连接节点的虚拟链路集合
$\boldsymbol{C}_{n\times k}$	底层服务器资源容量矩阵	$M:G^r\to\bar{G}^r\subseteq\bar{G}$	SFC 请求拓扑 G^r 映射到物理网络拓扑 $\bar{G}$ 之上
$C_{i,j}\in R^+$	服务器节点 i 上可提供的第 j 类资源的数量	$\boldsymbol{F}^r_{m\times n}$	请求 r 中 m 个 VNF 与 n 个服务器节点间的映射关系矩阵
$\boldsymbol{C}^{\mathrm{rem}}_{n\times k}$，$\boldsymbol{B}^{\mathrm{rem}}_{s\times s}$	当前网络服务器资源和链路资源的剩余情况	$F^r_{i,j}\in\{0,1\}$	VNF_i^r 是否部署在服务器节点 j 上
P,p	VNF 类型集合和 VNF 类型总数量	$n_i^r\in\bar{N}$	VNF_i^r 部署的服务器节点
$\boldsymbol{Q}_{p\times k}$	VNF 资源需求系数矩阵	$s_i^r\in\bar{S}$	VNF_i^r 部署的服务器节点 n_i^r 所直连的交换机
$Q_{i,j}$	i 类型 VNF 处理单位带宽流量所占用 j 类资源数量	$s_0^r=\bar{u}^r$，$s_{m+1}^r=\bar{v}^r$	接入交换机和出口交换机
$\boldsymbol{S}_{n\times p}$	服务器节点可承载的 VNF 类型矩阵	$l^r_{i,i+1}\in L^r$	请求 r 中 VNF_i^r 与 VNF_{i+1}^r 之间的虚拟链路
$S_{i,j}\in\{0,1\}$	服务器节点 i 是否支持 j 类型 VNF 的部署	$\bar{l}_{u,v}\in\bar{L}$	交换机 u 与交换机 v 之间的物理链路
R	租户 SFC 的请求集合	$\boldsymbol{E}^{s_i^r,s_{i+1}^r}_{s\times s}$	虚拟链路 $l^r_{i,i+1}$ 与物理链路 $\bar{l}_{u,v}$ 之间的映射关系矩阵
$r=<\bar{u}^r,\bar{v}^r,\beta^r,\tau^r,\psi^r>$	租户 SFC 请求信息	$E^{s_i^r,s_{i+1}^r}_{u,v}\in\{0,1\}$	虚拟链路 $l^r_{i,i+1}$ 是否部署在物理链路 $\bar{l}_{u,v}$ 之上

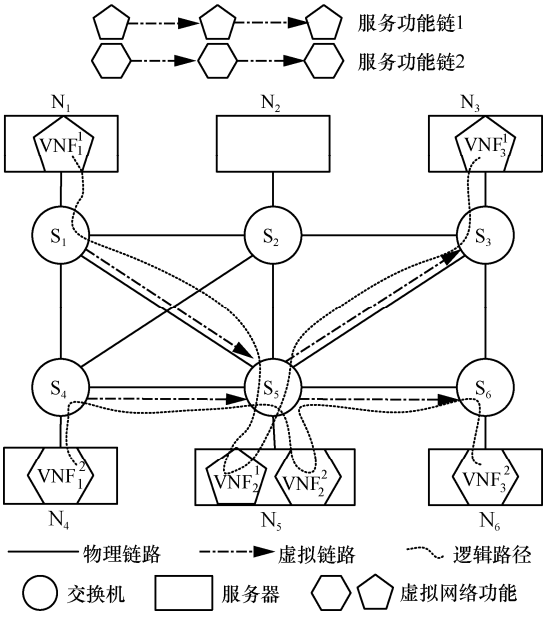

图 1　服务功能链部署

现实中，恶意租户可绕过逻辑隔离，借助共享资源（如 CPU、内存、磁盘等）构建各类侧信道，进而从共存租户的 VNF 中窃取敏感信息，图 2 中右半部分表示侧信道攻击的实施。为了解决租户隐私信息面临的失窃风险，一种有效的防御方法是为租户的 VNF 提供迁移服务，在恶意租户实现对目标租户隐私信息的完整窃取前，迁移租户 VNF 以中断侧信道攻击进程，图 2 展示了 VNF 迁移过程，服务功能链 1 的虚拟网络功能 VNF_2 由节点 N_5 迁移到节点 N_2。图 3 展示了迁移完成后相关服务功能链的部署情况。

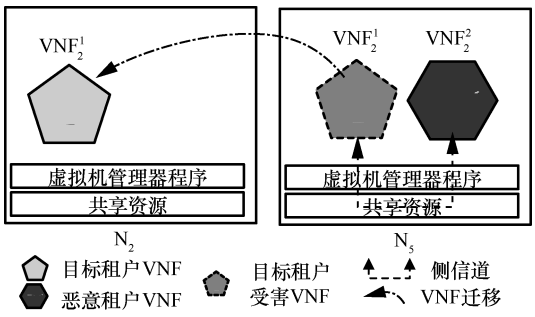

图 2　侧信道攻击与虚拟网路功能迁移

然而，VNF 的迁移并非没有代价，迁移 VNF 在降低租户所面临的侧信道攻击风险同时，也带来了一些负面影响。例如，迁移会造成短暂的服务中断，影响租户服务体验；迁移过程存在迁移开销（计算资源消耗和带宽资源消耗），影响云服务提供商成本；若迁移目的服务器节点选取不当则会导致服务功能链路径过长，增加服务时延和服务提供商链路资源成本。

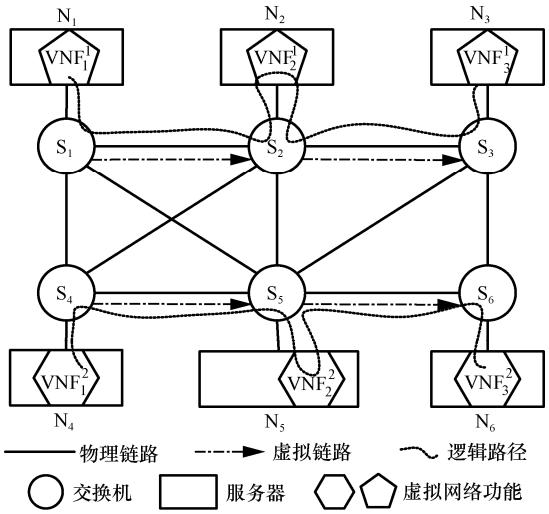

图 3　虚拟网络功能迁移后服务功能链部署

为了保证租户 VNF 隐私信息的安全，云服务提供商可为租户提供 VNF 迁移服务。对 VNF 进行迁移时需要解决以下问题。1) 待迁移 VNF 的选择问题，如何减少待迁移 VNF 的数量。2) 迁移时机的选择问题，如何在保证隐私信息安全的情况下降低迁移频率，以减少云服务提供商成本及对租户服务质量的影响。3) 迁移目的节点的选择问题，如何选择最优的迁移目的服务器节点。为此，需要设计合理的迁移方法，在保证安全性的同时降低迁移带来的负面影响。

2.3　VNF 迁移模型

VNF 迁移模型如图 4 所示。VNF_i^r 表示服务功能链请求 r 的第 i 个 VNF，n_i^r 表示 VNF_i^r 所部署的服务器节点，VNF_{i-1}^r 表示 VNF_i^r 的前置 VNF，n_{i-1}^r 表示 VNF_{i-1}^r 所部署的服务器节点，VNF_{i+1}^r 表示 VNF_i^r 的后置 VNF，n_{i-1}^r 表示 VNF_{i-1}^r 所部署的服务器节点，n_i^{rm} 则表示 VNF_i^r 要迁移的目的服务器节点。分别用 s_{i-1}^r、s_i^r、s_{i+1}^r、s_i^{rm} 表示 n_{i-1}^r、n_i^r、n_{i+1}^r、n_i^{rm} 所直连的交换机，此时 $H_{n_{i-1}^r,s_{i-1}^r}$、$H_{n_i^r,s_i^r}$、$H_{n_{i+1}^r,s_{i+1}^r}$、$H_{n_i^{\mathrm{rm}},s_i^{\mathrm{rm}}}$ 均为 1。当 $i=0$ 时，令 $s_0^r=\overline{u}^r$，表示接入交换机；当 $i=m+1$ 时，令 $s_{m+1}^r=\overline{v}^r$，表示出口交换机。二值矩阵 $\boldsymbol{E}_{s\times s}^{s_i^r,s_{i+1}^r}$ 表示请求 r 中 VNF_i^r 与 VNF_{i+1}^r 间的虚拟链路 $l_{i,i+1}^r\in L^r$ 与物理链路 $\overline{l}_{u,v}\in\overline{L}$ 之间的映射关系，元素 $E_{u,v}^{s_i^r,s_{i+1}^r}\in\{0,1\}$ 表示虚拟链路 $l_{i,i+1}^r$ 是否部署在物理链路 $\overline{l}_{u,v}$ 之上。

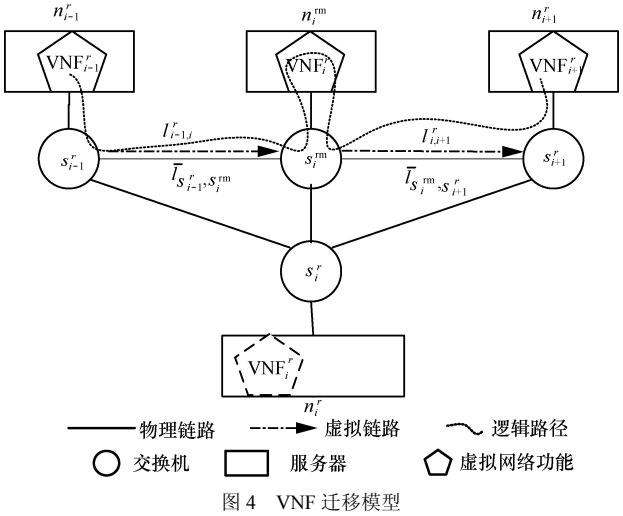

图 4 VNF 迁移模型

VNF 部署在任何服务器节点的计算资源消耗是一致的，而部署位置极大地影响着链路资源开销，因此，本文以最小化迁移后链路资源开销为优化目标，建立了 VNF_i^r 迁移模型。

目标为最小化链路资源开销，目标函数如式(1)所示。

$$\min \sum_{u \in \bar{S}} \sum_{v \in V-\Lambda(u)} \left(E_{u,v}^{s_{i-1}^r, s_i^{\mathrm{rm}}} + E_{u,v}^{s_i^{\mathrm{rm}}, s_{i+1}^r} \right) \beta^r \tag{1}$$

选取迁移目的服务器节点的约束条件如下。

$$S_{n_i^{\mathrm{rm}}, \mathrm{VNF}_i^r} = 1, \quad n_i^{\mathrm{rm}} \in \bar{N}, \quad \mathrm{VNF}_i^r \in P \tag{2}$$

$$Q_{\mathrm{VNF}_i^r, k} \beta^r \leqslant C_{n_i^{\mathrm{rm}}, k}^{\mathrm{rem}}, \quad \forall k \in K \tag{3}$$

$$\left(E_{u,v}^{s_{i-1}^r, s_i^{\mathrm{rm}}} + E_{u,v}^{s_i^{\mathrm{rm}}, s_{i+1}^r} \right) \beta^r \leqslant B_{u,v}^{\mathrm{rem}}, \quad \forall u \in \bar{S}, \ \forall v \in V-\Lambda(u) \tag{4}$$

式(2)表示承载 VNF_i^r 的服务器 n_i^{rm} 必须支持该类型 VNF。式(3)表示 VNF_i^r 占用的各类资源数量不可超过服务器 n_i^{rm} 各类资源余量。式(4)表示 2 条虚拟链路 $l_{i-1,i}^r$ 和 $l_{i,i+1}^r$ 所占用的带宽不可超过所占用的各条物理链路的带宽余量。

3 VNF 动态迁移方法

侧信道攻击手段从防御者角度可分为两类，即特征已知的侧信道攻击和特征未知的侧信道攻击。本文从以下两方面实现侧信道攻击风险的感知与规避：对于特征已知的侧信道攻击手段，可利用现有侧信道攻击检测系统对攻击实施进程进行检测，并基于检测结果对相关 VNF 执行触发式迁移；对于特征未知的侧信道攻击手段，基于侧信道攻击信息泄露模型评估潜在攻击成功实施的可能性，并据此对相关 VNF 进行定期式迁移，以降低侧信道攻击成功实施的可能性。

为了解决 2.2 节所述 VNF 迁移面临的问题，本文提出了基于风险感知的关键 VNF 动态迁移方法，包含以下 3 个策略：1) VNF 安全需求分类，仅对具有安全需求的 VNF 进行迁移，以降低待迁移节点数量；2) 定期式迁移结合触发式迁移，充分利用不断演进的侧信道攻击检测系统，提升侧信道防御性能的同时降低迁移频率；3) 基于逼近理想解排序（TOPSIS, technique for order preference by similarity to ideal solution）的多属性节点的排序法，优化迁移目的服务器节点的选取。

3.1 VNF 安全需求分类

针对待迁移 VNF 的选择问题，将全部的 VNF 进行迁移是不合理的，且并非所有 VNF 均含有隐私数据，因此不需要对所全部的 VNF 进行迁移。本文参考赵硕等[14]的工作，引入 VNF 分类策略，将 VNF 分为有安全需求和无安全需求两类。有安全需求的 VNF 含有隐私信息，信息被窃取会造成一定的危害；无安全需求 VNF 中仅含可公开信息，信息泄露不会造成危害。

定义二值矩阵 $\mathbf{SR}_{r \times m}$ 表示安全需求矩阵，元素 $\mathrm{SR}_{r,i}$ 表示第 r 个请求中的第 i 个 VNF 的安全需求，若 $\mathrm{SR}_{r,i}=1$，则表示 VNF_i^r 有安全需求，需要对其进行迁移操作。为租户提供自定义 VNF 安全需求接口，租户在请求 SFC 时，可根据实际需要对相关 VNF 的安全需求进行设定。因此，VNF 迁移模型应添加安全需求约束条件，如式(5)所示。

$$\mathrm{SR}_{r,i} = 1, \quad r \in R, \quad i \in \{1, 2, \cdots, m\} \tag{5}$$

式(5)表示仅在 VNF_i^r 有安全需求时才为其提供迁移服务。因此，服务提供商仅需要为有安全需求的 VNF 提供迁移服务，可显著降低待迁移 VNF 数量。

3.2 定期式迁移结合触发式迁移

针对迁移时机的选择问题，本文参考赵硕等[14]和 Moon 等[15]建立的侧信道攻击信息泄露模型，使用 Δ 表示迁移系统所采用的时间间隔，λ 表示迁移系统所设置的单位时间间隔信息泄露量，Γ 表示租户间 VNF 共存的时间间隔数量，$I_{r,i}$ 表示 VNF_i^r 信息被成功窃取所需的最小信息量。

为了保证虚拟网络功能 VNF_i^r 隐私信息的安全性，应满足

$$\lambda\Delta\Gamma \leqslant I_{r,i} \tag{6}$$

由式(6)可得到租户间 VNF_i^r 共存时间间隔数量的阈值为

$$\Gamma_{r,i}^{\mathrm{THR}} = \frac{I_{r,i}}{\lambda\Delta} \tag{7}$$

迁移系统以 Δ 为周期检查 VNF 的共存时间间隔情况，并对达到共存时间间隔数量阈值的 VNF 进行定期式迁移。由于每个服务器节点都存在不需要迁移的 VNF，因此可对共存时间的维护做以下简化，仅需统计有安全需求的 VNF 在所部署服务器节点的部署时间即可，当有安全需求的 VNF 在服务器节点部署的时间超过共存时间阈值时，应对该 VNF 进行定期式迁移。用 $\Gamma_{r,i}^n$ 表示 VNF_i^r 在服务器节点 n 部署的时间间隔数量，则为了保证 VNF 隐私信息的安全性，应满足

$$\Gamma_{r,i}^n \leqslant \Gamma_{r,i}^{\mathrm{THR}} = \frac{I_{r,i}}{\lambda\Delta} \tag{8}$$

为了降低迁移频率，当 $\Gamma_{r,i}^n = \Gamma_{r,i}^{\mathrm{THR}}$ 时执行定期式迁移即可。

此外，可结合现有侧信道攻击检测系统[16-17]，对相关 VNF 执行触发式迁移。假设有 π 种类型的检测系统，定义二值矩阵 $\mathbf{ALERT}_{\pi\times n}$ 表示侧信道攻击检测矩阵，元素 $\mathrm{ALERT}_{i,j}$ 表示检测系统 i 观察到的服务器 j 中的侧信道攻击发生状况，$\mathrm{ALERT}_{i,j}=1$ 表示检测系统 i 发现服务器 j 内正在发生侧信道攻击，$\mathrm{ALERT}_{i,j}=0$ 表示检测系统 i 认为服务器 j 内未发生侧信道攻击。则当式(9)成立时，说明在服务器节点 j 正在发生侧信道攻击问题，需要对该服务器中的关键 VNF 执行触发式迁移。

$$\sum_{i=1}^{\pi} \mathrm{ALERT}_{i,j} \geqslant 1 \tag{9}$$

3.3　多属性节点排序

针对迁移目的节点的选择问题，目前的迁移方法仅考虑节点的资源属性，如计算资源、邻接带宽资源，而未深入考虑底层网络的拓扑属性以及服务功能链 VNF 严格而有序的链式结构，进行迁移节点的选取时，可能会造成迁移节点距离过远，进而在链路部署阶段导致路径过长（跳数过大），不仅浪费链路资源，还会造成服务功能链数据传输时延增加。

本文参考龚水清等[19]的工作，引入基于 TOPSIS 的多属性节点排序方法。进行迁移目的服务器节点选择时，本文所关注的影响节点排序的关键属性如下：节点的资源余量、与前置 VNF 所部署服务器节点的距离和可用带宽、与后置 VNF 所部署服务器节点的距离和可用带宽，以实现服务器节点资源属性与拓扑属性的综合考虑。此外，本文方法具有可扩展性，后续可根据实际需要对影响节点排序的关键属性进行调整。本节以图 5 为例进行说明，VNF_2^1 在选择目的迁移服务器节点时，若 N_2、N_4 均支持 VNF_2^1 的部署，且 CPU 资源余量也基本一致时，此时将 N_2 选为目的服务器节点更为合适，这是因为将该 VNF 迁移到 N_2 比迁移到 N_4 的 SFC 整体的链路更短，可在降低服务时延的同时节约带宽资源。

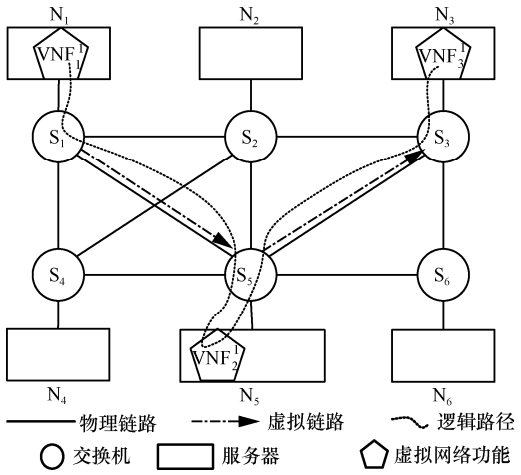

图 5　迁移目的服务器节点的选择

接下来，对影响目的迁移服务器节点选择的关键属性进行量化，并引入基于 TOPSIS 的多属性节点排序方法，以实现目的迁移服务器节点的最优选择。

1) 服务器节点的资源余量（为了简化问题仅考虑具有代表性的 CPU 资源）可表示为

$$\mathrm{RC}(n) = C_{n,1}^{\mathrm{rem}} \tag{10}$$

2) 服务器节点 n 距离待迁移 VNF 的前置 VNF 和后置 VNF 的距离之和如式(11)所示，其中，$\mathrm{DIS}_{\mathrm{prev}}(n)$ 表示距离前置 VNF 所部署服务器节点的最短路径跳数，$\mathrm{DIS}_{\mathrm{next}}(n)$ 表示距离后置 VNF 部署服务器节点的最短路径跳数。

$$\mathrm{DIS}(n) = \mathrm{DIS}_{\mathrm{prev}}(n) + \mathrm{DIS}_{\mathrm{next}}(n) \tag{11}$$

3) 可用带宽如式(12)所示，其中，$\mathrm{RB}_{\mathrm{prev}}(n)$ 表示距离前置 VNF 部署服务器节点的最短路径可用

带宽余量，$\mathrm{RB}_{\mathrm{next}}(n)$ 表示距离后置 VNF 部署服务器节点的最短路径可用带宽余量。

$$\mathrm{RB}(n)=\min(\mathrm{RB}_{\mathrm{prev}}(n),\mathrm{RB}_{\mathrm{next}}(n)) \quad (12)$$

参考龚水清等[19]的工作，引入基于 TOPSIS 的多属性节点排序方法，以存在 n 个待选服务器节点、h 个关键属性评价指标为例（本文中仅使用了上述 3 个关键属性作为评价指标）。基于 TOPSIS 的多属性节点排序方法分为以下 6 个步骤。

1) 构建特征矩阵。特征矩阵如式(13)所示，其中 $x_{i,j}$ 表示第 i 个节点的第 j 个评价指标的数值。

$$\boldsymbol{X}_{n\times h}=\begin{bmatrix} x_{1,1} & \cdots & x_{1,h} \\ \vdots & \ddots & \vdots \\ x_{n,1} & \cdots & x_{n,h} \end{bmatrix} \quad (13)$$

2) 计算规范化矩阵。规范化矩阵如式(14)所示，由于各评价指标的类型、量纲、值均不同，为了便于比较，需对各属性值进行规范化，属性值规范化的方法多样，本文采用与龚水清等[19]相同的方法，y_{ij} 的计算方法如式(15)所示。

$$\boldsymbol{Y}_{n\times h}=\begin{bmatrix} y_{1,1} & \cdots & y_{1,h} \\ \vdots & \ddots & \vdots \\ y_{n,1} & \cdots & y_{n,h} \end{bmatrix} \quad (14)$$

$$y_{ij}=\frac{x_{i,j}-\min\limits_{1\leqslant k\leqslant n}x_{k,j}}{\max\limits_{1\leqslant k\leqslant n}x_{k,j}-\min\limits_{1\leqslant k\leqslant n}x_{k,j}} \quad (15)$$

3) 计算权重规范化矩阵。权重规范化矩阵如式(16)所示，其中，w_j 表示第 j 个评价指标的权重，w_j 约束条件如式(17)所示，z_{ij} 的计算方法如式(18)所示。

$$\boldsymbol{Z}_{n\times h}=\begin{bmatrix} z_{1,1} & \cdots & z_{1,h} \\ \vdots & \ddots & \vdots \\ z_{n,1} & \cdots & z_{n,h} \end{bmatrix} \quad (16)$$

$$w_j(j=1,2,\cdots,h),\ 0\leqslant w_j\leqslant 1,\ \sum_{j=1}^{h}w_j=1 \quad (17)$$

$$z_{ij}=w_j y_{ij}(i=1,2,\cdots,n\ j=1,2,\cdots,h) \quad (18)$$

4) 确定正理想解 A^+ 和负理想解 A^-。正理想解 A^+ 如式(19)所示，负理想解 A^- 如式(20)所示。

$$A^+=\left\{z_1^+,z_2^+,\cdots,z_h^+\right\}=\left\{\max_{1\leqslant k\leqslant n}x_{k,1},\max_{1\leqslant k\leqslant n}x_{k,2},\cdots,\max_{1\leqslant k\leqslant n}x_{k,h}\right\} \quad (19)$$

$$A^-=\left\{z_1^-,z_2^-,\cdots,z_h^-\right\}=\left\{\min_{1\leqslant k\leqslant n}x_{k,1},\min_{1\leqslant k\leqslant n}x_{k,2},\cdots,\min_{1\leqslant k\leqslant n}x_{k,h}\right\} \quad (20)$$

5) 计算距离尺度。为每个候选服务器节点 i 计算距离正理想解和负理想解的距离，即

$$D_i^+=\sqrt{\sum_{j=1}^{h}\left(z_{i,j}-z_j^+\right)^2} \quad (21)$$

$$D_i^-=\sqrt{\sum_{j=1}^{h}\left(z_{i,j}-z_j^-\right)^2} \quad (22)$$

6) 计算理想解贴近度。为每个候选服务器节点 i 计算距离理想解的贴近度，即

$$O_i=\frac{D_i^-}{D_i^++D_i^-} \quad (23)$$

最后，根据理想解贴近度 O_i 的大小对候选服务器节点进行排序，并选出最优的迁移目的服务器节点 n_i^{rm}。

4 算法设计

本节以最小化链路资源开销为优化目标，设计了风险感知的关键虚拟网络功能迁移（RVNFM, risk-aware key virtual network function migration）算法，RVNFM 算法由迁移决策算法和 VNF 迁移算法 2 个子算法构成。算法主要流程如下：以时间间隔 Δ 为周期，周期性地调用迁移决策算法，迁移决策算法实现 VNF 的迁移决策，并调用 VNF 迁移算法实现 VNF 迁移。

迁移决策算法如算法 1 所示。

算法 1 迁移决策算法

1) for n in $\bar{N}$ #遍历网络中的服务器节点

2) if $\sum_{i=1}^{\pi}\mathrm{ALERT}_{i,n}\geqslant 1$ #若检测到服务器节点 n 发生侧信道攻击

3) for VNF_i^r in n #则遍历部署于服务器节点 n 的 VNF

4) if $\mathrm{SR}_{r,i}==1$ #若 VNF_i^r 具有安全需求

5) 迁移 VNF_i^r #则调用 VNF 迁移算法执行触发式迁移

6) else #否则执行定期式迁移

7) for VNF_i^r in n #遍历部署于服务器节点 n 的 VNF

8) if $\Gamma_{r,i}^n\geqslant\Gamma_{r,i}^{\mathrm{THR}}=\dfrac{I_{r,i}}{\lambda\Delta}$ #若 VNF_i^r 位于服务器节点 n 的部署时间超过阈值

9)　　迁移 VNF_i^r　#则调用 VNF 迁移算法执行定期式迁移

迁移决策算法具体描述如下。遍历网络中的服务器节点（第 1)行），若检测到服务器节点发生侧信道攻击，则对部署于该服务器节点且具有安全需求的 VNF 执行触发式迁移（第 2)~ 5)行），遍历部署于该服务器节点的 VNF（第 3)行），若 VNF 具有安全需求（第 4)行），则调用 VNF 迁移算法执行触发式迁移（第 5)行）；若服务器节点未检测到侧信道攻击，则对 VNF 执行定期式迁移（第 6)~9)行），遍历部署于该服务器节点的 VNF（第 7)行），若具有安全需求的 VNF 位于该服务器的部署时间超过阈值（第 8)行），则调用 VNF 迁移算法执行定期式迁移（第 9)行）。

VNF 迁移算法如算法 2 所示。

算法 2　VNF 迁移算法

输入　待迁移 VNF_i^r

输出　VNF_i^r 迁移方案

1) #VNF 部署阶段

2) 筛选 $\bar{N}$ 中支持 VNF_i^r 部署且资源足够的服务器集合 $\bar{N}_{\mathrm{VNF}_i^r}$

3) for n in $\bar{N}_{\mathrm{VNF}_i^r}$　#遍历可用服务器节点

4)　　计算 n 的关键属性 $\mathrm{RC}(n),\mathrm{DIS}(n),\mathrm{RB}(n)$

5) 使用基于TOPSIS的多属性节点排序方法对 $\bar{N}_{\mathrm{VNF}_i^r}$ 中候选服务器节点进行排序

6) 选择最优节点作为目的迁移服务器节点 n_i^{rm}，并更新节点资源余量

7) #虚拟链路部署阶段

8) 为 n_{i-1}^r 与 n_i^{rm} 间的虚拟链路 $l_{i-1,i}^r$、n_i^{rm} 与 n_{i+1}^r 间的虚拟链路 $l_{i,i+1}^r$ 分别确定可用链路集合

9) 从中筛选部署代价最小的链路集合

10) 选择带宽资源余量最大的物理链路

11) 记录所使用的链路并更新链路资源余量

VNF 迁移算法的具体描述如下。算法分为 VNF 部署阶段（第 1) ~6)行）与虚拟链路部署阶段（第 7)~11)行）2 个阶段。筛选网络中支持该类型 VNF 部署且资源足够的服务器（第 2)行），计算满足条件服务器节点的关键属性（第 4)行），使用基于 TOPSIS 的多属性节点排序方法对服务器节点进行排序（第 5)行），选择最优服务器节点作为目的迁移服务器，更新节点资源余量（第 6)行）。为 2 条虚拟链路筛选带宽资源充足的物理链路（第 8)行），并从中筛选部署代价最小的链路集合（存在多条长度相等的链路）（第 9)行），选择带宽资源余量最大的物理链路（第 10)行），记录所使用的物理链路并更新链路资源余量。

算法复杂度分析如下。算法 1 中，执行触发式迁移算法的最大计算复杂度为 $O(|\bar{N}||\mathrm{VNF}_i^r|)$，其中，$|\bar{N}|$ 表示网络中服务器节点的总数量，$|\mathrm{VNF}_i^r|$ 表示虚拟网络功能的总数量；执行定期式迁移算法的最大计算复杂度为 $O(|\bar{N}||\mathrm{VNF}_i^r|)$，因此算法 1 的最大计算复杂度为 $O(|\bar{N}||\mathrm{VNF}_i^r|)$。算法 2 中，基于 TOPSIS 的多属性节点排序 VNF 部署方法的最大计算复杂度为 $O(|\bar{N}|h)$，其中，h 为评价指标的数量；虚拟链路部署阶段的最大计算复杂度为 $O(|\bar{L}|)$，$|\bar{L}|$ 为网络中物理链路的总数量。因此，本文算法的计算复杂度为 $O(|\bar{N}||\mathrm{VNF}_i^r|+|\bar{L}|)$，为多项式函数复杂度。

5　实验仿真

5.1　实验环境设置

实验算法使用 Python 实现，运行于 Intel Core i5-3230 2.6 GHz、16 GB 内存的计算机。采用与 Li 等[20]一致的数据中心胖树拓扑网络结构，包含 54 个服务器、45 个交换机和 162 条链路，每个服务器节点的计算资源为 45 个，每条链路带宽容量为 45 个。实验中设置了 8 种不同类型的 VNF，其中 4 种为常用 VNF 实例，另外 4 种为用户自定义（UD, user defined）VNF 实例。根据文献[21]对 VNF 资源需求系数进行设置，相关 VNF 资源需求系数如表 2 所示，每个服务器节点从 8 种类型的 VNF 中随机选取 6 种作为可承载 VNF。每个 SFC 请求需要处理的流量大小从{1,2,3}中随机选取，所含的 VNF 从 8 种类型的 VNF 中随机选取 4 种，并随机选取其中的 2 个定义为具有安全需求的 VNF，相关 VNF 信息被成功窃取的最小信息量 I 从{500, 1 000, 1 500}中随机选取。迁移系统所采用的时间间隔 Δ=10，单位时间间隔信息泄露量 λ 根据下述实验具体需求进行设置。参考常见云平台的负载情况，本文对工作负载进行设置，使稳定状态下服务器的平均资源使用率为 50%，此时网络中已部署约 58 条 SFC 请求。

本文对网络中存在的侧信道攻击方法做如下

简化。将其分为已知特征和未知特征的侧信道攻击手段，根据单位时间间隔信息窃取量δ将相关侧信道攻击方法的泄露速率分为快速、中速和慢速，仿真实验中潜在恶意租户可采用的单位时间间隔信息窃取量δ如表 3 所示。实验中采用饱和式攻击，假设每个服务器节点均存在侧信道攻击，随机从表 3 中选取一种可用的侧信道攻击手段。

表 2 VNF 资源需求系数

VNF 类型	计算资源需求/单位带宽
AT	1
Firewall	2
Proxy	2
IDS	6
UD1	1
UD2	2
UD3	3
UD4	4

表 3 侧信道攻击方法分类

特征是否已知	窃取速率分类	单位时间间隔信息窃取量δ
特征已知	慢速	{1,2,3}
特征已知	中速	{4,5,6}
特征已知	快速	{7,8,9}
特征未知	慢速	{1,2,3}
特征未知	中速	{4,5,6}
特征未知	快速	{7,8,9}

为了评估本文所提方法的有效性，将本文所提的 RVNFM 迁移方法与下述相关方法进行对比实验，采用定期式迁移策略的迁移方法（DMBSL, dynamic migration of virtual machine based on security level）[14]、采用触发式迁移策略的迁移方法（MBHMU, migration based on heavy memory utilization）[17]和不执行迁移的方法（NM, no migration）。

5.2 评价指标

主要从以下 4 个方面对比相关方法在防御侧信道攻击时的性能。1) 迁移 VNF 的数量，随着时间推移，系统为抵御侧信道攻击所迁移的 VNF 数量。2) 时间间隔Δ内迁移 VNF 的平均数量，在系统时间间隔Δ内，迁移 VNF 数量的统计平均值。3) 泄露信息的 VNF 所占比例，随着时间推移，由于不能防御的侧信道攻击手段而发生信息泄露的 VNF 占总体有安全需求 VNF 的比例。4) 迁移后距前后 VNF 的跳数和，在完成 VNF 迁移后，目的迁移服务器节点距离前置 VNF 所部署服务器节点和后置 VNF 所部署服务器节点的跳数和。

5.3 实验结果分析

本文实验部分通过 2 个实验进行对比分析。

1) 不同迁移方法防御侧信道攻击的性能

首先，对比不同迁移方法在防御侧信道攻击时的性能，令λ=6。图 6 展示了饱和侧信道攻击环境下，随时间推移不同迁移方法泄露信息 VNF 所占比例，以 NM 方法为基线。从图 6 可以看出，本文所提 RVNFM 算法防御侧信道攻击的性能最优，这是因为 RVNFM 方法结合触发式迁移与定期式迁移，触发式迁移可有效抵御所有特征已知的侧信道攻击，而定期式迁移方法能有效防御信息窃取速率$\delta<\lambda$的侧信道攻击（无论特征是否已知），结合两者可有效防御绝大多数侧信道攻击手段，但是对于特征未知的快速侧信道攻击（$\delta>\lambda$），仍不能较好地解决，需要系统采用更大的λ值。此外，还可以看出，在本实验所设置的参数下，仅使用定期式迁移策略的 DMBSL 算法防御效果稍劣于仅使用触发式迁移策略的 MBHMU 算法。

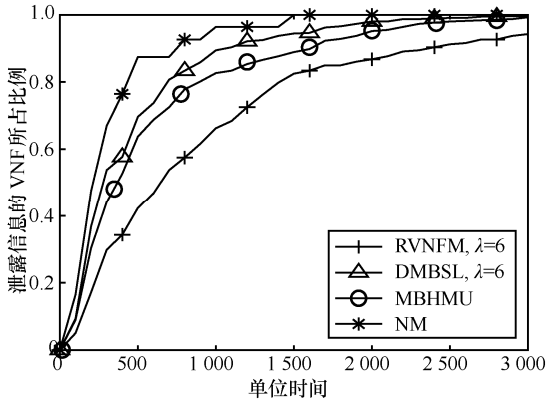

图 6 随时间推移系统中泄露信息的 VNF 所占比例

图 7 展示了不同迁移方法下系统迁移 VNF 的数量情况。不进行迁移的 NM 方法无 VNF 迁移；采用触发式迁移策略的 MBHMU 算法迁移的 VM 数量非常少，因此产生的迁移开销很小；采用定期式迁移策略的 DMBSL 算法和本文所提出的 RVNFM 算法均进行了大量的 VNF 迁移，相较于 MBHMU 算法而言具有很大的迁移开销。此外，RVNFM 算法虽然比 DMBSL 算法增添了触发式迁移策略，直观上应有更多的 VNF 迁移数量，但实际上迁移数量基本一致，这是由于 RVNFM 算法在

对 VNF 进行迁移决策时，对于信息泄露速率低于 $\delta < \lambda$ 的已知特征侧信道攻击不进行触发式迁移，而采用定期式迁移，可降低 VNF 的迁移数量。

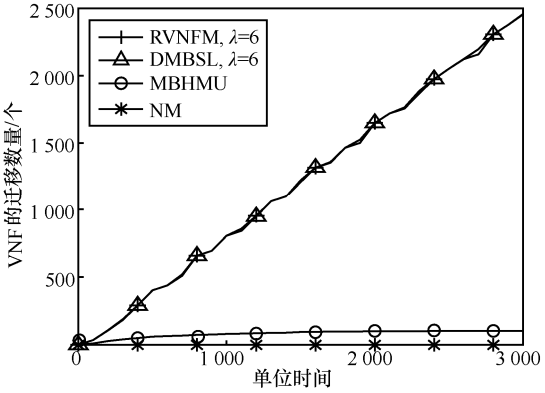

图 7　随时间推移系统迁移的 VNF 数量情况

从图 8 可以看出，MBHMU 算法迁移后的链路跳数和较大，会造成较大的链路资源开销，增加服务的时延，这是由于 MBHMU 采用随机策略选择目的迁移服务器节点，无论是在本文所使用的数据中心网络拓扑还是其他网络拓扑，通常情况下随机选择迁移目的节点极易造成迁移后路径过长问题。而 DMBSL 算法与本文提出的 RVNFM 算法迁移后的跳数之和均较小，这是由于 DMBSL 算法在对迁移节点进行选择时考虑了链路部署开销，有效避免选择路径过长的目的迁移服务器节点。而 RVNFM 算法在选择迁移目的节点时，采用了基于 TOPSIS 的多属性节点排序算法，其中一项节点评价指标是迁移后链路跳数，因此可有效避免迁移后链路过长问题。对于图 8 中存在跳数为 0 的情况，是由于本文忽略了服务器到交换机这一跳，若 2 个服务器在同一个交换机下则跳数距离为 0。

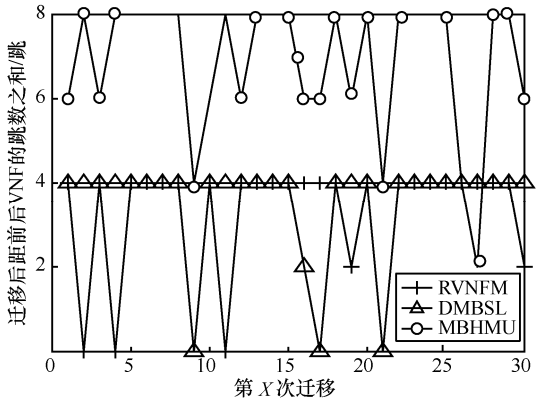

图 8　迁移后距前后 VNF 的跳数之和

2) λ 对相关迁移算法的影响

λ 对相关迁移算法防御效果的影响如图 9 所示。其中，采用触发式迁移策略的 MBHMU 算法不受 λ 影响，不再列出不同参数下的状况。而 DMBSL 算法和本文提出的 RVNFM 算法随 λ 的增大防御效果逐渐提升，可以看出相同的 λ 下，RVNFM 算法优于 DMBSL 算法。RVNFM 算法甚至可在 $\lambda = 6$ 的情况下达到接近 DMBSL 算法在 $\lambda = 8$ 时的防御性能，而更大的 λ，意味着更多的 VNF 迁移数量（如图 10 所示），也将面临着更高的迁移开销和更大的服务影响。在相同的防御性能下，RVNFM 具有更低的节点迁移数量与迁移频率。

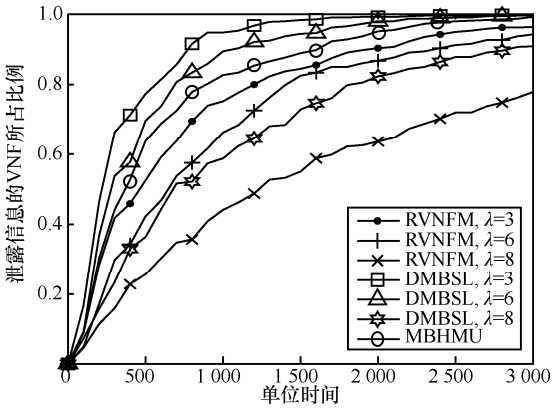

图 9　λ 对相关迁移算法防御效果的影响

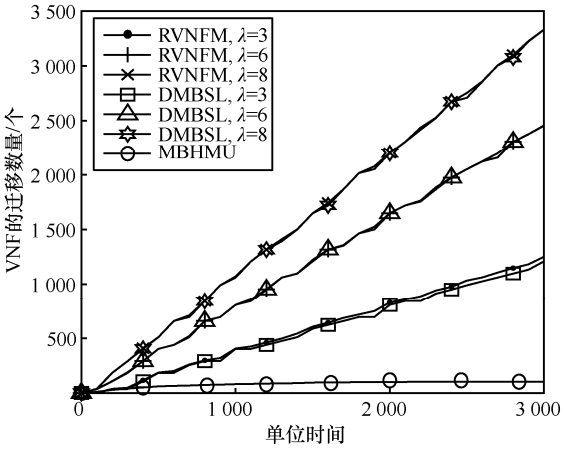

图 10　λ 对 VNF 迁移数量的影响

如图 10 所示，虽然增大 λ 可显著提高相关算法防御侧信道攻击的性能，但是也显著提高了 VNF 迁移数量，由此会造成较大的迁移开销。服务提供商应根据实际情况及租户需求，合理地对 λ 进行设置，可对不同 λ 进行差异化定价。图 11 展示了不同 λ 下，相关迁移算法在时间间隔 Δ 内迁移 VNF 的平均数量情况。可以看出，MBHMU

算法在时间间隔 Δ 内迁移 VNF 的平均数量较少，且不受 λ 的影响。而 RVNFM 和 DMBSL 算法在时间间隔 Δ 内迁移 VNF 的平均数量随 λ 的增大而显著提高。

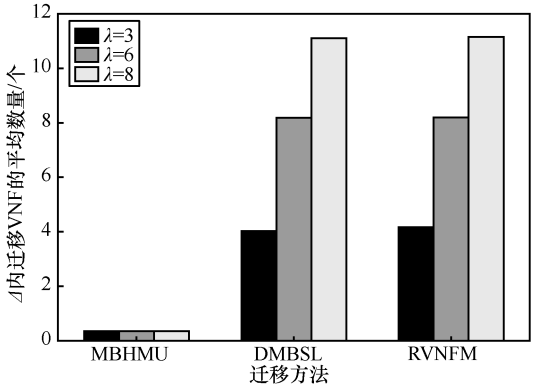

图 11　时间间隔 Δ 内迁移 VNF 的平均数量情况

6　结束语

本文对多租户环境下租户 VNF 长期共存所面临的侧信道攻击问题进行了描述，分析了现有迁移算法存在的问题与不足，并概述了 VNF 进行迁移时需要解决的 3 个关键问题：待迁移 VNF、迁移时机及迁移目的节点的选择问题。由此提出了基于风险感知的关键虚拟网络功能动态迁移算法，并验证了算法的有效性。本文围绕 SFC 中虚拟网络功能面临的安全性问题展开研究，而未深入考虑 SFC 中虚拟链路所面临的安全威胁。然而租户间虚拟链路共享底层资源时也同样面临着信息泄露风险，在未来的研究工作中将试图解决 SFC 虚拟链路面临的安全风险，进一步提高 SFC 隐私信息的安全性。

参考文献：

[1] MIJUMBI R, SERRAT J, GORRICHO J, et al. Network function virtualization: state-of-the-art and research challenges[J]. IEEE Communications Surveys & Tutorials, 2016, 18(1): 236-262.

[2] WU J X. Thoughts on the development of novel network technology[J]. Science China (Information Sciences), 2018, 61(10):144-154.

[3] FIROOZJAEI M D, JEONG J P, KO H, et al. Security challenges with network functions virtualization[J]. Future Generation Computer Systems, 2017, 67(7): 315-324.

[4] 胡威. 基于 SGX 的虚拟网络功能安全保护机制研究[D]. 武汉: 武汉大学, 2017.
HU W. Research on security protection mechanism of virtual network function based on SGX[D]. Wuhan: Wuhan University, 2017.

[5] BAZM M, LACOSTE M, SUDHOLT M. Isolation in cloud computing infrastructures: new security challenges[J]. Annals of Telecommunications, 2019, 74(1): 197-209.

[6] 梁鑫, 桂小林, 戴慧珺, 等. 云环境中跨虚拟机的 Cache 侧信道攻击技术研究[J]. 计算机学报, 2017, 40(2): 317-336.
LIANG X, GUI X L, DAI H J, et al. Cross-VM cache side channel attacks in cloud: a survey[J]. Chinese Journal of Computer, 2017, 40(2): 317-336.

[7] LYU Y, MISHRA P. A survey of side-channel attacks on caches and countermeasures[J]. Journal of Hardware and Systems Security, 2018, 2(1): 33-50.

[8] 何佩聪, 黄汝维, 陈宁江, 等. 云环境中的侧通道攻击研究进展[J]. 计算机应用研究, 2018, 35(4): 969-973.
HE P C, HUANG R W, CHEN N J, et al. Research progress on side-channel attacks in cloud environment[J]. Application Research of Computer, 2018, 35(4): 969-973.

[9] LIU S, CAI Z, XU H, et al. Towards security-aware virtual network embedding[J]. Computer Networks, 2015, 91(11): 151-163.

[10] HAN Y, CHAN J, ALPCAN T, et al. Using virtual machine allocation policies to defend against co-resident attacks in cloud computing[J]. IEEE Transactions on Dependable and Secure Computing, 2017, 14(1): 95-108.

[11] HAN Y, ALPCAN T, CHAN J, et al. A game theoretical approach to defend against co-resident attacks in cloud computing: preventing co-residence using semi-supervised learning[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(3): 556-570.

[12] XU Z, WAND H, WU Z. A measurement study on co-residence threat inside the cloud[C]//Proceedings of the 24th USENIX Conference on Security Symposium. Berkeley: USENIX Association, 2015: 929-944.

[13] AINAPURE B S , SHAH D , RAO A A . Understanding perception of cache-based side-channel attack on cloud environment[M]. Berlin: Springer, 2017.

[14] 赵硕, 季新生, 毛宇星, 等. 基于安全等级的虚拟机动态迁移方法[J]. 通信学报, 2017, 38(7): 165-174.
ZHAO S, JI X S, MAO Y S, et al. Research on dynamic migration of virtual machine based on security level[J]. Journal on Communications, 2017, 38(7): 165-174.

[15] MOON S, SEKAR V, REITER M. Nomad: mitigating arbitrary cloud side channels via provider-assisted migration[C]//The 22nd ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2015: 1595-1606.

[16] ATYA A O F, QIAN Z, KRISHNAMURTHY S V, et al. Malicious co-residency on the cloud: attacks and defense[C]//IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2017:1-9.

[17] ZHANG T, ZHANG Y, LEE R B. CloudRadar: a real-time side-channel attack detection system in clouds[C]//International Symposium on Research in Attacks, Intrusions, and Defenses. Berlin: Springer, 2016:118-140.

[18] 伊鹏, 谢记超, 张震, 等. 抗侧信道攻击的服务功能链部署方法[J]. 电子与信息学报, 2019, 41(11): 2699-2707.
YI P, XIE J C, ZHANG Z, et al. A service function chain deployment method against side channel attack[J]. Journal of Electronics and Information Technology, 2019, 41(11): 2699-2707.

[19] 龚水清, 陈靖, 黄聪会, 等. 信任感知的安全虚拟网络映射算法[J]. 通信学报, 2015, 36(11): 180-189.
GONG S Q, CHEN J, HUANG H C, et al. Trust-aware secure virtual network embedding algorithm[J]. Journal on Communications, 2015, 36(11): 180-189.

[20] LI D, HONG P, XUE K, et al. Virtual network function placement considering resource optimization and SFC requests in cloud datacenter[J]. IEEE Transactions on Parallel and Distributed Systems, 2018, 29(7): 1664-1677.

[21] BARI F, CHOWDHURY S R, AHMED R, et al. Orchestrating virtualized network functions[J]. IEEE Transactions on Network and Service Management, 2016, 13(4): 725-739.

[作者简介]

丁绍虎（1979− ），男，北京人，信息工程大学博士生，主要研究方向为网络安全、新型网络体系结构。

谢记超（1993− ），男，河南周口人，信息工程大学实习研究员，主要研究方向为网络安全、网络功能虚拟化。

张鹏（1982− ），男，河南郑州人，信息工程大学副研究员，主要研究方向为网络安全。

普黎明（1976− ），男，云南崇明人，信息工程大学副研究员，主要研究方向为网络安全、网络体系结构。

谷允捷（1994− ），男，山东济宁人，信息工程大学工程师，主要研究方向为网络功能虚拟化。