doi:10.11959/j.issn.1000-436x.2017091

基于安全等级的虚拟机动态迁移方法

赵硕[1]，季新生[1]，毛宇星[2]，程国振[1]，扈红超[1]
（1. 国家数字交换系统工程技术研究中心，河南 郑州 450002；2. 解放军理工大学指挥信息系统学院，江苏 南京 210007）

摘 要：侧信道攻击是当前云计算与数据中心环境下多租户间信息泄露的主要途径，现有基于虚拟机动态迁移的防御方法存在迁移算法收敛时间长，开销大的问题，为此，提出一种基于安全等级的虚拟机动态迁移方法。首先，对虚拟机进行安全等级分类，减少虚拟机动态迁移的数量；然后采用相应的虚拟机映射策略，降低虚拟机迁移的频率。实验表明，与现有基于虚拟机动态迁移的防御方法相比，该方法能够降低虚拟机迁移算法的收敛时间和迁移开销。

关键词：侧信道攻击；虚拟机迁移；安全等级；迁移算法；迁移开销
中国分类号：TP302 **文献标识码**：A

Research on dynamic migration of virtual machine based on security level

ZHAO Shuo[1], JI Xin-sheng[1], MAO Yu-xing[2],CHENG Guo-zhen[1],HU Hong-chao[1]
(1.National Digital Switching System Engineering and Technological Research Center, Zhengzhou 450002, China;
2. Command Information System Institute, PLA University of Science and Technology, Nanjing 210007, China)

Abstract: Side-channel attacks were the main ways of multi-tenant information leakage in the cloud computing and data center environments. The existing defense approaches based on dynamic migration of virtual machine have long convergence time of migration algorithm and high migration cost. Hence, a dynamic migration of virtual machine based on security level was proposed. Firstly, security level classification of virtual machines was used to reduce the number of migrating virtual machines. Then the corresponding virtual machines embedding strategy was used to reduce the frequency of virtual machines migration. Simulation experiments demonstrate that the proposed approach can reduce convergence time of migration algorithm and migration cost.

Key words: side-channel attack, virtual machine migration, security level, migration algorithm, migration cost

1 引言

随着互联网的发展，客户对互联网的需求种类越来越多。例如，音频和视频服务类[1]的需求有带宽和时延限制；网上银行类的需求有保证安全的要求。但满足需求的应用却被部署到相同的底层物理网络上，这大大影响了应用的性能，无法保证服务的质量。网络虚拟化技术[2~4]为当前互联网的刚性提供了一条有效的解决途径。其主要思想是将互联网划分为多个虚拟网络(VN, virtual network)，各个 VN 共享同样的底层物理网络资源，但可以有不同的应用、服务和架构，以满足多样化的技术部署和应用。网络虚拟化技术虽然大大提高了网络的灵活性、应用的多样性，能够满足用户更多的需求，但同时也带来了一定的安全威胁[5~8]，其中，侧信道攻击[9~11]就是当前云计算与数据中心环境[12]下多租

收稿日期：2016-08-08；**修回日期**：2016-12-12
基金项目：国家自然科学基金创新研究群体基金资助项目（No.61521003）；国家自然科学基金资助项目（No.61602509）；国家重点研发计划基金资助项目（No.2016YFB0800100, No.2016YFB0800101）
Foundation Items: The Foundation for Innovative Research Groups of the National Natural Science Foundation of China (No.61521003), The National Natural Science Foundation of China (No.61602509), The National Key R&D Program of China (No.2016YFB0800100, No.2016YFB0800101)

户间信息泄露的主要途径。

目前，防御侧信道攻击的研究主要有 2 种方法[13~16]，第一种方法是修改物理主机的软硬件。这类方法可以成功防御特定类型的侧信道攻击，但不适用于防御不同类型的侧信道攻击和未知类型的侧信道攻击。第二种方法是基于移动目标防御的思想，对虚拟机进行动态迁移。这类方法能够成功防御不同类型的侧信道攻击，也不需要修改物理主机的软硬件，但受制于虚拟机迁移算法的收敛时间和迁移开销，难以适用于大规模的网络场景。

针对现有方法存在的局限性，根据文献[17]提出的信任感知的安全虚拟网络映射算法，本文在第二种方法的基础上，提出了一种基于安全等级的虚拟机动态迁移方法。首先，在虚拟网请求映射之前，客户根据虚拟机的安全需求将虚拟机划分为不同的安全等级，以此来减少虚拟机迁移的数量。然后，在虚拟网映射时，引入安全等级相同的虚拟机共享物理主机资源的约束条件，以此来降低虚拟机迁移的频率。

2 相关工作

在云计算与数据中心环境下，共享相同物理主机的虚拟机之间存在侧信道。有关研究表明[9~11]，利用虚拟机之间的侧信道来窃取用户信息是一种可行的攻击手段。发动侧信道攻击的攻击者可以通过虚拟机运行的特征来识别攻击目标[9]，也可以从共享信息中得知攻击目标的应用[18]和操作系统[19]。文献[10]表明，利用侧信道攻击，可以在 2~3 min 内恢复高级加密标准(AES, advanced encryption standard)密钥。

目前，针对侧信道攻击的防御方法主要分为 2 种[13~16]。第一种方法是修改物理主机的软硬件。根据侧信道攻击种类的不同，防御主要分为基于超级管理者防御、操作系统防御、应用层防御和硬件防御。文献[20]提出，基于超级管理者，可以隐藏程序运行的时间和改变程序暴露的时间来进行防御；文献[21]表明，在操作系统层内，可以在保护的进程中加入噪音来进行防御；文献[22]提出，在应用层，采用跨多个虚拟机的分区加密来进行防御；文献[23]表明，可以在硬件设计时采用接入随机化和资源分割来进行防御。该类方法能够成功防御特定类型的侧信道攻击，但不适用于防御不同类型的侧信道攻击和未知类型的侧信道攻击，另外，修改物理主机的软硬件可能会导致虚拟机性能的下降。第二种方法是基于移动目标防御的思想[15,16,24]，对虚拟机进行动态迁移[14]来防御侧信道攻击。文献[14]提出，通过动态迁移虚拟机，减少虚拟机之间共存的时间，从而减少攻击者窃取目标虚拟机的信息量，导致攻击者无法成功获取目标的信息。该方法能够防御不同类型的侧信道攻击，而且不用修改物理主机的软硬件，但随着虚拟网络中虚拟机数量的增多，将会使虚拟机动态迁移算法的收敛时间过长，迁移开销过大，导致难以适用于大规模的网络场景。

3 问题描述

3.1 网络模型

1) 物理网络

物理网络可以表示为一个不带权重的无向图 $G^s=(N^s,L^s)$，其中，N^s、L^s 分别表示物理节点和物理链路的集合，本文物理节点为物理主机。对于每一个物理主机 $n^s\in N^s$，对应有一个可用的物理资源 $C(n^s)$，如 CPU 的处理能力等。同样，对于每个物理链路 $l^s\in L^s$，对应有一个可用的链路资源 $B(l^s)$，表示链路可承受的物理资源，如链路带宽、时延等。其中，$C(n^s)$、$B(l^s)$ 都是非负值。

2) 虚拟网请求

虚拟网络模型表示为 $G^v=(N^v,L^v)$。类似地，N^v、L^v 分别表示虚拟节点和虚拟链路的集合，本文虚拟节点为虚拟机。对于每一个虚拟机 $n^v\in N^v$，对应有一个虚拟资源需求 $C(n^v)$，表示该虚拟机所需的物理资源。每条链路 $l^v\in L^v$ 对应一个链路资源需求 $B(l^v)$，表示该虚拟链路所需的带宽资源。

3.2 侧信道攻击问题描述

虚拟网映射可以描述为将虚拟网请求的拓扑 G^v 映射到物理网络拓扑 G^s 上，定义为 $M:G^v\rightarrow(N^{s'},L^{s'})$，其中，$N^{s'}\subseteq N^s$，表示物理网络 G^s 中的物理主机子集，是虚拟网 G^v 的虚拟机的映射对象，$L^{s'}\subseteq L^s$，表示物理网络 G^s 中的链路子集，是虚拟网 G^v 的虚拟链路的映射对象。$N^{s'}$ 和 $L^{s'}$ 都必须满足对应虚拟机和虚拟链路的资源需求。虚拟网映射可以细分为虚拟机映射和链路映射。图 1 给出了虚拟网映射实例。图 1 中右半部分表示一个物理网实例，物理主机边的方框中数字代表该物理主机的物理资源，即 $C(n^s)$，链路上的数字代表该链路的带宽，

即 $B(l^s)$，图 1 左半部分是 2 个虚拟网请求实例。

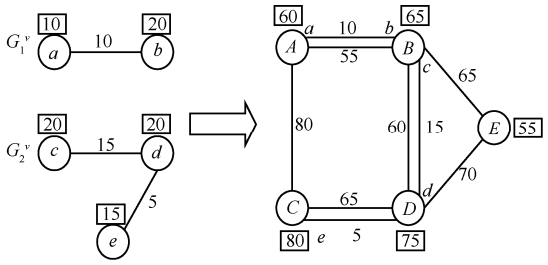

图 1　虚拟网映射实例

对于图 1 的虚拟网映射，虚拟网 G_1^v 的虚拟机 b 和虚拟网 G_2^v 的虚拟机 c 共享物理网络 G^s 中物理主机 B 的资源。假设虚拟机 b 为恶意虚拟机，虚拟机 c 为目标虚拟机，则攻击者可以利用虚拟机 b 向虚拟机 c 发动侧信道攻击。攻击者发动侧信道攻击的步骤主要分为 3 步，为了更清楚地描述攻击者是如何发动侧信道攻击的，将图 1 中的物理主机 B 和虚拟机 b、c 进行放大，如图 2 所示。

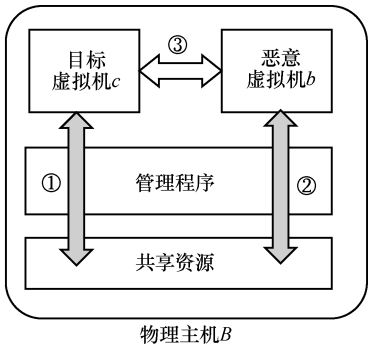

图 2　侧信道攻击

攻击者发动侧信道攻击的步骤如下所示。

① 目标虚拟机 c 在工作时对共享的物理资源(CPU cache、网络队列)产生影响。

② 恶意虚拟机 b 通过共享的物理资源对共存的虚拟机 c 进行评估和测量。

③ 恶意虚拟机 b 根据评估和测量的结果，建立与目标虚拟机 c 的隐蔽信道，窃取目标虚拟机 c 的隐私信息。

3.3　虚拟机安全问题描述

由文献[14]信息泄露模型知，虚拟机泄露信息的速率不是固定不变的，其主要影响因素为用户的虚拟机之间是否存在信息复制（information replication）和恶意的虚拟机之间是否有串通（collaborating）。由此存在 4 种信息泄露的情形，分别为用户的虚拟机之间不存在信息复制并且恶意虚拟机之间无串通、用户的虚拟机之间存在信息复制并且恶意的虚拟机之间无串通、用户的虚拟机之间不存在信息复制并且恶意的虚拟机之间有串通、用户的虚拟机之间存在信息复制并且恶意的虚拟机之间有串通，分别用符号 $\langle NR,NC\rangle$、$\langle R,NC\rangle$、$\langle NR,C\rangle$、$\langle R,C\rangle$ 表示。因此，信息泄露速率分为 4 种，分别为 $K_{<NR,NC>}$、$K_{<R,NC>}$、$K_{<NR,C>}$、$K_{<R,C>}$。文献[14]提到，若恶意的虚拟机之间有串通，将会导致信息泄露速率的成倍增加，大大增加虚拟机信息的安全威胁。其中，当处于 $\langle R,C\rangle$ 情形下，虚拟机的信息泄露速率最快，达到其他 3 种信息泄露速率的 2 倍及以上，对虚拟机信息的安全威胁最大。当处于 $\langle NR,NC\rangle$ 情形下，虚拟机的信息泄露速率最慢，对虚拟机信息的安全威胁最小。

虚拟机信息的安全主要取决于如下几个参数，如表 1 所示。

表 1　　安全影响参数

符号	含义
K	信息泄露的速率
Γ	共存的时间间隔数量
ε	最小的时间间隔
I	信息被成功窃取的最小信息量

因此，要想成功防御侧信道攻击，保证虚拟机信息的安全，需要满足

$$K\Gamma\varepsilon \leqslant I \tag{1}$$

4　虚拟机动态迁移方法

现有基于虚拟机动态迁移的防御方法是通过动态的虚拟机迁移，来改变式(1)中 Γ 的大小，减少虚拟机共存的时间，以此来保证目标虚拟机的信息不被恶意虚拟机成功窃取。但随着虚拟网络中虚拟机数量的增多，对所有虚拟机不断地进行迁移，将使虚拟机迁移算法的收敛时间过长，虚拟机迁移产生的开销过大，导致此方法难以适用于大规模的虚拟网络中。因此，本文在现有方法的基础上，为减少虚拟机迁移算法的收敛时间和迁移开销，提出了一种基于安全等级的虚拟机动态迁移方法。

4.1　虚拟机的安全等级分类

1) 基础设施提供商根据客户的安全需求将虚拟机分为 3 类：第一类，安全等级无，虚拟机含有的信息完全公开，即信息泄露不会带来危害，安全

等级标识为 N(none)；第二类，安全等级中，虚拟机含有隐私信息，信息泄露会带来一定的危害，安全等级标识为 M(medium)；第二类，安全等级高，虚拟机含有重要隐私信息，一旦泄露将造成严重的危害，安全等级标识为 H(high)。安全等级无、中、高的虚拟机集合分别用 N^{vN}、N^{vM}、N^{vH} 表示。例如，$n^{vH} \in N^{vN}$，表示虚拟机 n^v 的安全等级为高。

2) 基础设施提供商为客户提供一个自定义的虚拟机安全等级接口，如图 3 所示。

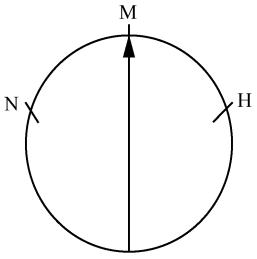

图 3 自定义的虚拟机安全等级接口

3) 虚拟网映射之前，客户利用自定义的虚拟机安全等级接口，根据自身安全需求，将虚拟网请求中的虚拟机分为 N^{vN}、N^{vM}、N^{vH}。当然，对于安全等级不同的虚拟机，单位资源租费不同，安全等级为无、中、高的虚拟机，单位资源租费分别为 $\partial_{n^v}^{vN}$、$\partial_{n^v}^{vM}$、$\partial_{n^v}^{vH}$。如安全等级为高的虚拟机 n^{vH}，单位资源租费为 $\partial_{n^v}^{vH}$。

4.2 基于安全等级的虚拟机映射策略

为了使不同安全等级的虚拟机得到与其对应的安全性保证，本文采用了相应的虚拟机映射策略和虚拟机迁移策略。本节对虚拟机映射策略进行描述，将在 4.3 节对虚拟机的迁移策略进行描述。本文采用的虚拟机映射策略为：相同安全等级的虚拟机共享物理主机。具体描述如表 2 所示。很显然，该映射策略将会导致虚拟网络映射成功率的下降，但本文依然采取该映射策略的原因有 2 个。1) 虚拟机的安全等级越高，则所需要支付的租费越高，由 3.3 节虚拟机安全问题的描述可知，若攻击者采用虚拟机之间有串通方式进行侧信道攻击，将会导致信息泄露速率的成倍增加，使虚拟机信息的安全威胁大大增加。因此，本文采用相同安全等级的虚拟机共享相同的物理主机，如果攻击者采取串通的方法发动侧信道攻击，则串通的恶意虚拟机都需要与目标虚拟机具有相同的安全等级，这将使攻击者付出成倍的高租费，大大增加攻击代价，迫使攻击者无法采取串通的方法来发动侧信道攻击，这将大大降低信息泄露的速率，从而降低了虚拟机迁移的频率。2) 虚拟机能够映射的物理主机数量减少，可以减少虚拟机重映射的时间，一定程度上可以降低虚拟机迁移算法的收敛时间。

表 2 虚拟机映射策略

安全等级	映射策略
高	只与安全等级高的虚拟机共享同一物理主机
中	只与安全等级中的虚拟机共享同一物理主机
无	映射到无安全等级要求的物理主机上

4.3 基于安全等级的虚拟机迁移策略

1) 进行迁移的虚拟机范围

由 4.1 节可知，对于安全等级高和中的虚拟机集合，都含有隐私信息，因此，都需要进行虚拟机迁移，但安全等级无的虚拟机集合，不存在隐私信息，迁移时可以不予考虑，减少了虚拟机迁移的数量。

2) 虚拟机迁移时间间隔分类

在 4.2 节中，将相同安全等级的虚拟机共享同一物理主机，迫使攻击者无法采取串通的方法来发动侧信道攻击，因此，信息泄露的速率快慢取决于客户虚拟机之间是否存在信息复制，那么信息泄露的情况只有 2 种，速度分别为 $K_{<NR,NC>}$ 和 $K_{<R,NC>}$，显然 $K_{<R,NC>} > K_{<NR,NC>}$。定义 $K_f = K_{<R,NC>}$，$K_s = K_{<NR,NC>}$。由式(1)知，因此存在 2 种共存的时间间隔数量，分别为 Γ_f 和 Γ_s。根据虚拟机的安全需求，安全等级高、中的虚拟机分别采用时间间隔数量为 Γ_f 和 Γ_s 来进行迁移。

3) 虚拟机迁移策略

综上所述，基于安全等级的虚拟机迁移策略为：安全等级无的虚拟机，不需要进行虚拟机迁移；安全等级中的虚拟机，迁移时间间隔数量为 Γ_s；安全等级高的虚拟机，迁移时间间隔数量为 Γ_f。

5 基于安全等级的虚拟机映射模型和迁移模型

本文在虚拟机映射时，引入根据虚拟机安全等级进行映射的约束条件，以最大化单位时间收益作为映射目标，即需要提高虚拟网请求的成功映射率，建立了虚拟机映射模型。在进行虚拟机迁移时，引入虚拟机之间共存时间的约束条件，以最小化迁移开销作为迁移目标，建立了虚拟机

迁移模型。

5.1　基于安全等级的虚拟机映射模型

1) 变量说明

$\alpha(n^v,n^s)$：0-1 变量，当虚拟机 n^v 映射到物理主机 n^s 上，$\alpha(n^v,n^s)$ 为 1，否则为 0。

$\beta(l^v,l^s)$：0-1 变量，当虚拟链路 l^v 映射到物理链路 l^s 上，$\beta(l^v,l^s)$ 为 1，否则为 0。

$\sigma(n^v,n^{sv})$: 0-1 变量，当虚拟机 n^v 与虚拟机 n^{sv} 的安全等级相同，$\sigma(n^v,n^{sv})$ 为 1，否则为 0。其中，n^{sv} 表示已映射到物理主机 n^s 上的虚拟机。

2) 约束条件

资源能力约束

$$\sum_{n^v\in N^v} C(n^v)\alpha(n^v,n^s)\leqslant C(n^s),\ \forall n^s\in N^s \tag{2}$$

$$\sum_{l^v\in L^v} B(l^v)\beta(l^v,l^s)\leqslant B(l^s),\ \forall l^s\in L^s \tag{3}$$

式(2)和式(3)表示对任意的物理主机或物理链路，映射到虚拟机资源或虚拟链路资源之和不能超过该物理主机或链路所能承受的物理资源。

虚拟机映射约束

$$\sum_{n^s\in N^s}\alpha(n^v,n^s)=1,\forall n^v\in N^v \tag{4}$$

$$\sum_{n^v\in N^v}\alpha(n^v,n^s)\leqslant 1,\forall n^s\in N^s \tag{5}$$

$$\prod_{n^{sv}\in N^{sv}}\sigma(n^v,n^{sv})=1,\ \forall n^v\in N^v,n^s\in N^s \tag{6}$$

其中，N^{sv} 表示映射到物理主机 n^s 上所有虚拟机的集合。式(4)表示保证每一个虚拟机都被完整地映射到物理主机上，式(5)表示一个虚拟网内的虚拟机不能共享同一物理主机，式(6)表示相同安全等级的虚拟机才能够共享同一物理主机。

3) 目标函数

收益函数：对于一个有安全等级分类的虚拟网 $G_i^v\in G^v$ 被映射，基础设施提供商得到的收益为

$$\mathrm{Re}v(G_i^v)=\sum_{n_i^v\in N_i^v}\partial_{n_i^v}^{\mathrm{dem}}C(n_i^v)+\sum_{l_i^v\in L_i^v}\beta C(l_i^v) \tag{7}$$

其中，$\partial_{n_i^v}^{\mathrm{dem}}\in\left\{\partial_{n_i^v}^{vN},\partial_{n_i^v}^{vM},\partial_{n_i^v}^{vH}\right\}$，表示不同安全等级的虚拟机的单位资源收益，如 $\partial_{n_i^v}^{\mathrm{dem}}=\partial_{n_i^v}^{vH}$ 表示安全等级为高的虚拟机的单位资源收益；β 表示虚拟链路单位资源收益。

目标函数：最大化单位时间的收益为

$$\overline{P}_{\max}=\max\left\{\lim_{T\to\infty}\frac{\sum_{i=1}^{|G^v|}\mathrm{Re}v(G_i^v)}{T}\right\} \tag{8}$$

其中，$\sum_{i=1}^{|G^v|}\mathrm{Re}v(G_i^v)$ 为 0 到 T 时间内虚拟网映射的收益总和，基础设施提供商可以通过 $\partial_{n_i^v}^{\mathrm{dem}}$ 和 β 分别控制不同安全等级的虚拟机单位资源收益和链路单位资源收益的权重，调整自身的收益情况。

5.2　基于安全等级的虚拟机迁移模型

1) 变量说明

$\alpha_r^t(n^v,n^s)$：0-1 变量，当虚拟网 r 的虚拟机 n^v 在 t 时刻映射在物理主机 n^s 上，$\alpha_r^t(n^v,n^s)$ 为 1，否则为 0。

$\beta_r^t(l^v,l^s)$：0-1 变量，当虚拟网 r 的虚拟链路 l^v 在 t 时刻映射在物理链路 l^s 上，$\beta_r^t(l^v,l^s)$ 为 1，否则为 0。

2) 约束条件

虚拟机迁移进行重映射时，也需要满足式(2)~式(6)的映射约束条件，另外，为了确保用户虚拟机的信息不被攻击者成功窃取，还需要加上虚拟机之间共享物理主机的时间约束条件，即虚拟机之间共存时间约束：虚拟网 r 的虚拟机 n_i^v 和虚拟网 m 中的虚拟机 n_j^v 共存的时间间隔数量小于迁移的时间间隔数量。

① 安全等级高的虚拟机之间共存时间约束如下

$$\begin{aligned}&\sum_{\lambda=1}^{\Gamma_f}\sum_{n^s\in N^s}\alpha_r^{\lambda\varepsilon}\left(n_i^v,n^s\right)\alpha_m^{\lambda\varepsilon}\left(n_j^v,n^s\right)<\Gamma_f\\&\forall r,m\in[1,k],r\neq m,n_i^v\in N_r^v,n_j^v\in N_m^v\end{aligned} \tag{9}$$

② 安全等级中的虚拟机之间共存时间约束如下

$$\begin{aligned}&\sum_{\lambda=1}^{\Gamma_s}\sum_{n^s\in N^s}\alpha_r^{\lambda\varepsilon}\left(n_i^v,n^s\right)\alpha_m^{\lambda\varepsilon}\left(n_j^v,n^s\right)<\Gamma_s\\&\forall r,m\in[1,k],r\neq m,n_i^v\in N_r^v,n_j^v\in N_m^v\end{aligned} \tag{10}$$

其中，$\lambda\in[1-\Gamma]$，ε 为最小的时间间隔。

3) 目标函数

进行虚拟机迁移时，在保证虚拟机隐私信息安全的前提下，要最小化迁移带来的开销，才能使基础设施提供商的利润最大化，因此，本文将最小化迁移开销作为目标函数。

最小化迁移开销。最小化虚拟机迁移开销等于

虚拟机迁移过程中虚拟机和虚拟链路的迁移开销之和。

① 安全等级高的虚拟机迁移带来的开销为

$$\min\left(\begin{array}{l}\gamma\sum_{r=1}^{k}\sum_{n^v\in N^v}\sum_{n^s\in N^s}C_i(n^v)\alpha_r^t(n^v,n^s)\left(1-\alpha_r^{t+\Gamma_f}(n^v,n^s)\right)+\\ \phi\sum_{r=1}^{k}\sum_{l^v\in L^v}\sum_{l^s\in L^s}C_i(l^v)\beta_r^t(l^v,l^s)\left(1-\beta_r^{t+\Gamma_f}(l^v,l^s)\right)\end{array}\right) \tag{11}$$

②安全等级中的虚拟机迁移带来的开销为

$$\min\left(\begin{array}{l}\gamma\sum_{r=1}^{k}\sum_{n^v\in N^v}\sum_{n^s\in N^s}C_r(n^v)\alpha_r^t(n^v,n^s)\left(1-\alpha_r^{t+\Gamma_s}(n^v,n^s)\right)+\\ \phi\sum_{r=1}^{k}\sum_{l^v\in L^v}\sum_{l^s\in L^s}C_r(l^v)\beta_r^t(l^v,l^s)\left((1-\beta_r^{t+\Gamma_s}(l^v,l^s)\right)\end{array}\right) \tag{12}$$

其中，γ 和 ϕ 分别表示虚拟机和虚拟链路的单位资源迁移开销。式(11)和式(12)的第一项表示迁移虚拟机带来的迁移开销，第二项表示迁移虚拟链路带来的迁移开销。

6 基于安全等级的虚拟机映射算法和迁移算法

6.1 基于安全等级的虚拟机映射算法

基于安全等级的虚拟机映射算法流程如算法 1 所示。

算法 1 基于安全等级的虚拟机映射算法

1) 对 N^s 中的物理主机按照剩余资源降序进行排序，集合为 N^{ts};

2)对 N^v 中的虚拟机按照资源需求降序进行排序，集合为 N^w;

3) for ($i=0;n^v=get(N^w,i);i++$) do //资源需求大的虚拟机优先进行映射

4) for ($j=0;j\leqslant|N^{ts}|$)do

5) $n^s=get(N^{ts},j)$; //剩余资源多的物理主机优先作为备选物理主机

6) if(($n^s.security==$ true)&&($n^s.rest\_cpu==$ ture)) //物理主机 n^s 是否能够满足安全等级要求且剩余的带宽资源是否能够满足虚拟机 n^v 的资源需求

7) $n^v\rightarrow n^s$; //虚拟机 n^v 映射到物理主机 n^s 上

8) update physical resources; //更新物理资源

9) else j ++; //不满足安全或资源需求，则选择下一个物理主机作为备选物理主机

10) end if

11) end for

12) end for

本文以最大化单位时间收益为映射目标，即需要提高虚拟网请求的成功映射率。虚拟机映射阶段，在满足虚拟机安全等级的要求下，尽量将需求最大的虚拟机映射到剩余资源最多的物理主机上，符合贪婪式算法的思想，最大化资源的利用率。在虚拟链路映射阶段，采用 K 短路径映射算法进行链路映射。

6.2 基于安全等级的虚拟机迁移算法

对虚拟机进行迁移，以安全等级为高的虚拟机集合为例，具体流程如算法 2 所示。

算法 2 基于安全等级的虚拟机迁移算法

1) for each $n^{sH}\in N^{sH}$ do //对含有安全等级高虚拟机的物理主机 n^{sH}

2) for each $n_i^{vH}\in locate\left(n^{sH}\right)$ do //对映射在该物理主机上的虚拟机 n_i^{vH}

3) for each $n_j^{vH}\in locate\left(n^{sH}\right)$ do

4) if $\sum_{\lambda=1}^{\Gamma_f}\alpha^{\lambda\varepsilon}(n_i^{vH},n^{sH})\alpha^{\lambda\varepsilon}(n_j^{vH},n^{sH})\geqslant\Gamma_f$ do

//2 个虚拟机之间共存的时间间隔数量等于或超过阈值 Γ_f

5) $n_i^{vH}.collision++$;

6) end if

7) end for

8) end for //该物理主机上所有的虚拟机的 *collision* 值计算完毕

9) 对位于物理主机 n^{sH} 上所有虚拟机放到集合 Q 中

10) for ($i=0;\ i<length(Q);\ i++$)do

11) if ($collision\_value\left(Q[i]\right)==0$)

12) continue;

13) else if (($migrate\_security\left(Q[i]\right)==$ true)&& ($migrate\_node\left(Q[i]\right)==$ true) && ($migrate\_links\left(Q[i]\right)==$ true)) //物理主机是否满足安全等级要求、虚拟机资源需求和虚拟链路需求

14) $migrate\_cost(Q[i]) == min\{migrate\_cost\ (N^{s})\}$; //迁移到产生最小开销的物理主机上

15) $collision\_value(Q[i]) = 0$;

16) end if

17) end if

18) end for

19) end for

算法具体描述为：遍历所有已映射安全等级为高的虚拟机所在的物理主机，检查相同物理主机上的虚拟机之间共存的时间间隔数量是否超过阈值 Γ_f，如果虚拟机之间的共存时间超过阈值，则超时值加 1；检查完所有物理主机后，对于超时值非 0 的虚拟机，在满足安全等级要求、虚拟机资源需求、链路资源需求的物理主机中，选择产生迁移开销最小的物理主机进行迁移。

类似地，对于安全等级为中的虚拟机，也采用算法 2 的虚拟机迁移流程，只是改变遍历搜索范围且将共存的时间间隔数量的阈值改为 Γ_s。

7　实验及结果分析

7.1　实验环境设置

本次实验在 Intel(R) Core(TM) i7-4790CPU 3.6 GHz、4 GB RAM 的主机上进行，采用 GT-ITM 工具生成虚拟网络及物理网络拓扑、虚拟机映射算法和迁移算法采用 C++语言编程实现，并利用 Matlab 工具对实验结果进行分析。

底层网络设置为具有 100 个物理主机，347 条链路组成。底层物理主机 CPU 资源和链路的带宽资源符合[50, 100]的均匀分布。VN 中虚拟机的数目服从[5,10]的均匀分布，虚拟机的安全等级服从[0,2]的整数随机分布，0、1、2 分别表示虚拟机的安全等级为低、中、高，虚拟机之间的连接概率为 0.5，虚拟机和虚拟链路所需资源分别服从[1,20]和[1,15]的均匀分布，每 100 个时间单元平均到达 4 个 VN 请求。VN 请求的生命周期服从参数为 4 000 的指数分布。

7.2　实验结果分析

本文实验通过虚拟网络映射成功率、虚拟机迁移开销、虚拟机迁移算法收敛时间、侧信道攻击防御效果 4 个方面，对现有基于虚拟机动态迁移的防御方法[14]与基于安全等级的虚拟机动态迁移方法进行比较和分析。

为了方便描述，本文将现有基于虚拟机动态迁移的防御方法称为方法 1，本文提出的基于安全等级的虚拟机动态迁移方法称为方法 2。

1) 虚拟网络映射成功率

图 3 中展示了方法 1 与方法 2 在虚拟网络映射成功率方面的比较。从图 3 可以看出，方法 2 在虚拟网络映射成功率方面是低于方法 1 的，最大下降约 15%。很显然，相同安全等级的虚拟机才能共享物理主机的虚拟机映射策略是造成方法 2 虚拟网络映射成功率下降的原因。根据实验数据计算得出，方法 2 相较于方法 1，虚拟网络映射成功率平均下降 10.9%。

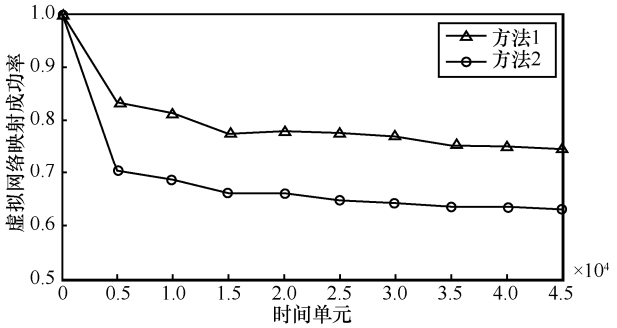

图 3　虚拟网络映射成功率

2) 虚拟机迁移算法收敛时间

图 4 中描述了方法 1 与方法 2 在虚拟机迁移算法收敛时间方面的比较。本实验将方法 1 的虚拟机共存时间阈值设置为 1 000 个时间单元，根据 3.3 节信息泄露速率和 4.3 节虚拟机迁移策略，方法 2 的虚拟机共存时间阈值对于安全等级高、中的虚拟机分别设置为 4 000 和 2 000 个时间单元。一次完整的虚拟机迁移所需的时间等于对虚拟机进行共存时间检查开始，到所有进行迁移的虚拟机完成了重映射为止。本文进行了 100 次完整的虚拟机迁移实验。实验数据表明，对于方法 1，迁移算法的收敛时间最大值为 715 个时间单元，最小值为 394 个时间单元，平均值为 583 个时间单元；对于方法 2，迁移算法的收敛时间最大值为 361 个时间单元，最小值为 115 个时间单元，平均值为 199 个时间单元。因此，方法 2 迁移算法的收敛时间相较于方法 1 来说，平均下降了 65.87%。造成方法 2 迁移算法的收敛时间明显下降的原因主要有 2 个：1) 对虚拟机进行共存时间检查的范围缩小，方法 2 中不需要对安全等级无的虚拟机进行共存时间的检查；2) 需要进行迁移的虚拟机

数量的减少，一方面，方法 2 中安全等级为无的虚拟机不需要进行迁移，另一方面，方法 2 中虚拟机的共存时间阈值大于方法 1，导致相同时间内共存时间超过阈值的虚拟机数量减少，从而减少了虚拟机迁移的数量。

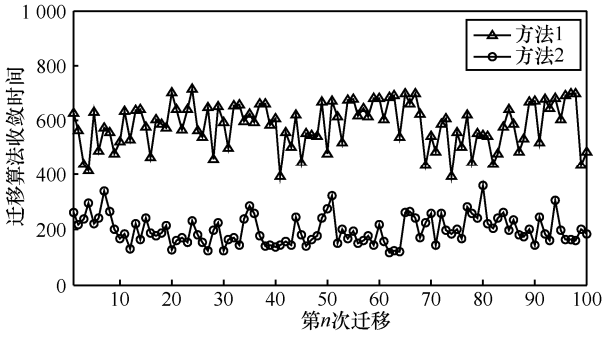

图 4 虚拟机迁移算法收敛时间

3) 虚拟机迁移开销

图 5 对虚拟机迁移开销进行了比较。其中，r 和 Φ 分别表示虚拟机和虚拟链路的单位资源迁移开销。虚拟机迁移开销等于虚拟机迁移过程中虚拟机和虚拟链路的迁移开销之和。在图 5 中，方法 1 从 1 500 个时间单元时存在虚拟机迁移，方法 2 从 2 500 个时间单元时存在虚拟机迁移，这是由于方法 1 和方法 2 虚拟机共存时间阈值设置不同导致的。从图 5 可以看出，很显然，方法 1 的虚拟机迁移开销总和要大于方法 2，而且有着较快的增加速度。对于方法 1，虚拟机迁移开销总和的平均增加速度为每 500 个时间单元，迁移开销增加 68；对于方法 2，平均增加速度为每 500 个时间单元，迁移开销增加 26.5。方法 2 相较于方法 1，迁移开销总和的平均增加速度下降 61.02%。造成方法 2 迁移开销总和的平均增加速度下降的原因有 2 个：1) 虚拟机迁移数量的减少，安全等级为无的虚拟机迁移不需要进行迁移；2) 虚拟机迁移频率的降低，方法 2 中安全等级高、中的虚拟机共存时间阈值大于方法 1 中的虚拟机，使迁移开销降低。

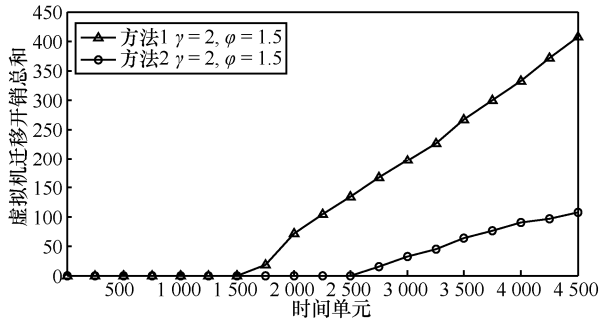

图 5 虚拟迁移开销

图 6 描述了虚拟机迁移单位资源开销 γ 权重的不同对虚拟机迁移开销的影响。由实验数据计算得，随着虚拟机单位资源的迁移开销 γ 权重的变大，方法 1 平均每 500 个时间单元增加开销 28.5，方法 2 平均每 500 个时间单元增加开销 12.5，所以，虚拟机迁移单位资源开销权重的增加将使方法 1 比方法 2 花费更多的迁移开销。在实际的虚拟网络环境中，虚拟机单位资源的迁移开销的权重往往是比较大的，因此，对于实际的虚拟网络，方法 2 的虚拟网络迁移开销代价更小。

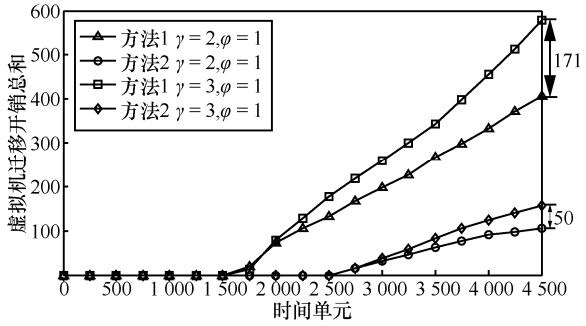

图 6 不同虚拟机迁移开销权重下的虚拟机迁移开销

4) 侧信道攻击防御效果

由式(1)知，若要保证虚拟机信息的安全，成功防御侧信道攻击，则虚拟机之间共存的时间不能超过共存时间阈值，否则虚拟机的私密信息有被恶意攻击者成功窃取的风险。在云计算与数据中心环境下，对于租户来说，若超过共存时间阈值的虚拟机数量越多，则租户的私密信息被成功窃取的风险就越大。

定义 1 风险虚拟机。虚拟网 r 的虚拟机 n_i^v 和虚拟网 m 中的虚拟机 n_j^v 共存的时间间隔数量大于迁移的时间间隔数量，则定义虚拟机 n_i^v、n_j^v 为风险虚拟机。根据式(9)，则风险虚拟机的集合 A 为

$$A=\left\{\begin{array}{l} n_i^v\in N_r^v, n_j^v\in N_m^v, \forall r,m\in[1,k], r\neq m| \\ \sum_{\lambda=1}^{\Gamma}\sum_{n^s\in N^s}\alpha_r^{\lambda\varepsilon}\left(n_i^v,n^s\right)\alpha_m^{\lambda\varepsilon}\left(n_j^v,n^s\right)>\Gamma \end{array}\right\} \tag{13}$$

定义 2 待迁虚拟机。虚拟网 r 的虚拟机 n_i^v 和虚拟网 m 中的虚拟机 n_j^v 共存的时间间隔数量大于等于迁移的时间间隔数量，则定义虚拟机 n_i^v、n_j^v 为待迁虚拟机。待迁虚拟机的集合 B 为

$$B=\left\{\begin{array}{l} n_i^v\in N_r^v, n_j^v\in N_m^v, \forall r,m\in[1,k], r\neq m| \\ \sum_{\lambda=1}^{\Gamma}\sum_{n^s\in N^s}\alpha_r^{\lambda\varepsilon}\left(n_i^v,n^s\right)\alpha_m^{\lambda\varepsilon}\left(n_j^v,n^s\right)\geqslant\Gamma \end{array}\right\} \tag{14}$$

定义 3　风险系数。风险虚拟机的数量占待迁虚拟机的数量比例 $\rho(0 \leqslant \rho \leqslant 1)$

$$\rho = \begin{cases} \dfrac{|A|}{|B|}, & |B| > 0 \\ 0, & |B| = 0 \end{cases} \tag{15}$$

本文将风险系数 ρ 作为侧信道攻击防御效果的衡量指标。若风险系数 ρ 越大，则风险虚拟机的数量越多，用户私密信息被成功窃取的风险越大，对侧信道攻击的防御效果越差，反之，风险系数 ρ 越小，则对侧信道攻击的防御效果越好。本实验在迁移开销预算存在限制的条件下，对方法 1 与方法 2 在侧信道攻击防御效果方面进行了比较，如图 7 所示。

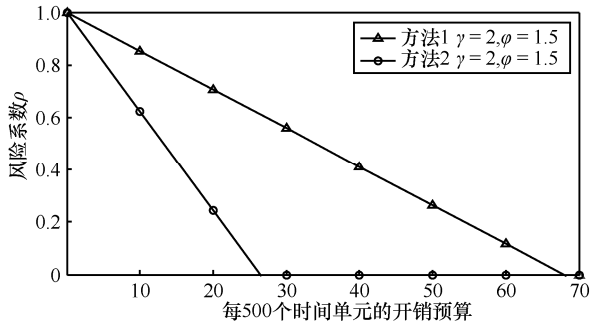

图 7　侧信道攻击防御效果

图 7 中，横坐标表示在 500 个时间单元内，云服务提供商为虚拟机迁移所提供的开销预算，纵坐标表示用户私密信息被成功窃取的风险系数。首先，由图 5 知，方法 1 每 500 个时间单元虚拟机迁移开销平均增加 68，方法 2 每 500 个时间单元虚拟机迁移开销增加 26.5，然后经过实验计算得出每迁移一个虚拟机，平均需要 7.24 个开销，从而得出每 500 个时间单元内，方法 1 和方法 2 各自平均待迁移的虚拟机数量，最后根据开销预算的大小，得出风险虚拟机占总待迁虚拟机的比例。显然，开销预算越大，能够进行迁移的虚拟机数量越多，则风险虚拟机数量越少，风险系数 ρ 越小，侧信道攻击的防御效果越好。如在每 500 个时间单元提供的开销预算为 20，方法 1 的风险系数 ρ 为 0.71，方法 2 为 0.25，显然方法 2 对侧信道攻击的防御效果较好，另外，当预算开销大于或等于 26.5 时，方法 2 风险虚拟机的比例达到 0，即所有待迁的虚拟机都可以得到迁移，可以使所有虚拟机成功地防御侧信道攻击，同样，当预算开销大于或等于 68 时，方法 1 可以使所有虚拟机成功地防御侧信道攻击。因此，在开销预算有限的情况下，方法 2 对侧信道攻击的防御效果较好，当开销预算足够大或无开销预算限制的情况下，方法 1 和方法 2 都可以成功地防御侧信道攻击。

8　结束语

本文对云计算与数据中心环境下存在的侧信道攻击问题进行了描述，分析了当前防御侧信道攻击方法存在的不足，提出了一种基于安全等级的虚拟机动态迁移方法。本文以最大化收益目标建立了虚拟机映射模型，设计了虚拟机映射算法，以最小化虚拟机迁移开销目标建立了虚拟机迁移模型，设计了虚拟机迁移算法，并进行了仿真实验。实验结果表明，相较于现有基于虚拟机动态迁移的防御方法，该方法在虚拟网映射成功率方面平均有 10.9% 的下降率，但在虚拟机迁移算法的收敛时间方面平均有 65.87%的减少，在虚拟机迁移开销方面，每 500 个时间单元迁移开销总和的平均增加速度降低了 61.02%。因此，本文提出的方法在成功防御侧信道攻击的前提下，可以适用于不同规模的网络场景。

参考文献：

[1] SONG B, HASSAN M M, HUH E N. Delivering IPTV service over a virtual network: a study on virtual network topology[J]. Journal of Communications & Networks, 2012, 14(14):319-335.

[2] CHOWDHURY N M M K, BOUTABA R. A survey of network virtualization[J]. Computer Networks, 2010, 54(5): 862-876.

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

[4] CHOWDHURY N M M K, BOUTABA R. Network virtualization: state of the art and research challenges[J]. IEEE Communications Magazine, 2009, 47(7):20-26.

[5] WANG Y, CHAU P, CHEN F. A framework for security-aware virtual network embedding[C]// International Conference on Computer Communication and Networks. IEEE, 2015.

[6] PIGNOLET Y A, SCHMID S, TREDAN G. Adversarial VNet embeddings: a threat for ISPs?[J]. Proceedings - IEEE INFOCOM, 2013, 12(11):415-419.

[7] CHAU P, WANG Y. Security-awareness in network virtualization: a classified overview[C]// IEEE, International Conference on Mobile Ad Hoc and Sensor Systems. IEEE Computer Society, 2014:545-550.

[8] TAHIR R, KHAN M T, GONG X, et al. Sneak-peek: high speed covert channels in data center networks[C]//2016 IEEE Conference on Computer Communications (INFOCOM). IEEE, 2016.

[9] RISTENPART T, TROMER E, SHACHAM H, et al. Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds[C]//ACM Conference on Computer and Communications Security, 2009:199-212.

[10] IRAZOQUI G, EISENBARTH T, SUNAR B. S$A: a shared cache attack that works across cores and defies VM sandboxing--and its application to AES[C]// IEEE Symposium on Security & Privacy. IEEE, 2015:591-604.

[11] LIU F, YAROM Y, GE Q, et al. Last-level cache side-channel attacks are practical[J]. IEEE Symposium on Security & Privacy, 2015:605-622.

[12] 张玉清, 王晓菲, 刘雪峰, 等. 云计算环境安全综述[J]. 软件学报, 2016, 27(6): 1328-1348.
ZHANGY Y Q, WANG X F, LIU X F, et al. survey on cloud computing security[J]. Journal of Software, 2016, 27(6): 1328-1348.

[13] VARADARAJAN V, RISTENPART T, SWIFT M. Scheduler-based defenses against cross-VM side-channels[C]//23rd USENIX Security Symposium (USENIX Security 14). 2014: 687-702.

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

[15] ZHANG Y, LI M, BAI K, et al. Incentive compatible moving target defense against VM-colocation attacks in clouds[M]//Information Security and Privacy Research. Springer Berlin Heidelberg, 2012: 388-399.

[16] EVANS D, NGUYENTUONG A, KNIGHT J. Effectiveness of moving target defenses[M]//Moving Target Defense. 2011:29-48.

[17] 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 C H, et al. Trust-aware secure virtual network embedding algorithm[J]. Journal on Communications, 2015, 36(11):180-189.

[18] SUZAKI K, IIJIMA K, YAGI T, et al. Memory deduplication as a threat to the guest OS[C]//The Fourth European Workshop on System Security (EUROSEC). 2011:1-6.

[19] OWENS R, WANG W. Non-interactive OS fingerprinting through memory de-duplication technique in virtual machines[J]. IEEE International Performance Computing & Communications, 2011, 8069(5):1-8.

[20] LI P, GAO D, REITER M K. Stopwatch: a cloud architecture for timing channel mitigation[J]. ACM Transactions on Information & System Security, 2014, 17(2):1-28.

[21] ZHANG Y, REITER M K. Düppel: retrofitting commodity operating systems to mitigate cache side channels in the cloud[C]//ACM Sigsac Conference on Computer & Communications Security. 2013:827-838.

[22] PATTUK E, KANTARCIOGLU M, LIN Z, et al. Preventing cryptographic key leakage in cloud virtual machines[C]//23rd USENIX Security Symposium (USENIX Security 14). 2014: 703-718.

[23] WANG Z, LEE R B. A novel cache architecture with enhanced performance and security[C]//2008 41st IEEE/ACM International Symposium on Microarchitecture. IEEE, 2008: 83-93.

[24] GILLANI F, AL-SHAER E, LO S, et al. Agile virtualized infrastructure to proactively defend against cyber attacks[C]//2015 IEEE Conference on Computer Communications (INFOCOM). IEEE, 2015: 729-737.

作者简介：

赵硕（1993-），男，河南安阳人，国家数字交换系统工程技术中心硕士生，主要研究方向为虚拟网安全、软件定义网络等。

季新生（1968-），男，江苏南通人，国家数字交换系统工程技术中心教授、博士生导师，主要研究方向为网络空间安全、拟态安全等。

毛宇星（1989-），男，河北唐山人，解放军理工大学博士生，主要研究方向为网络空间安全、软件定义网络等。

程国振（1986-），男，山东定陶人，国家数字交换系统工程技术中心助理研究员，主要研究方向为网络空间安全、软件定义网络等。

扈红超（1982-），男，河南商丘人，国家数字交换系统工程技术中心副研究员，主要研究方向为网络空间安全、云数据中心等。