

面向多租户的关键虚拟机动态迁移方法研究

赵硕¹, 季新生¹, 程国振¹, 毛宇星²

(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: 提出一种面向多租户的关键虚拟机动态迁移方法。首先, 根据租户对虚拟机的安全需求设定关键虚拟机的比例, 减少虚拟机动态迁移的数量; 然后, 通过虚拟机之间共存时间约束条件最大化降低虚拟机动态迁移的频率; 最后, 以最小化迁移开销作为虚拟机迁移的目标函数, 进一步降低虚拟机迁移带来的开销。实验表明, 与现有的防御方法相比, 该方法在有效防御侧信道攻击的前提下, 能够减少对网络服务性能的影响, 降低虚拟机迁移的成本, 更加适用于大规模的网络场景。

关键词: 侧信道攻击; 关键虚拟机; 动态迁移; 迁移算法; 迁移开销

中图分类号: TP302

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2017.00191

Research on dynamic migration of critical virtual machines for multi-tenancy

ZHAO Shuo¹, JI Xin-sheng¹, CHENG Guo-zhen¹, MAO Yu-xing²

(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: A dynamic migration method of critical virtual machines for multi-tenancy was proposed. Firstly, the tenants can set ratio of critical virtual machines according to tenant's security requirements, then the dynamic migration frequency of virtual machines were maximized by the coexistence time constraints between virtual machines, finally the migration cost was minimized as an object function for the virtual machines migrated to further reduce the migration cost. Simulation experiments demonstrate that the proposed approach can reduce the impact on the performance of network services and the cost of virtual machines migration, and is more suitable for large-scale network scenarios under the premise of effective defense side-channel attacks.

Key words: side-channel attacks, critical virtual machines, dynamic migration, migration algorithm, migration cost

1 引言

云计算技术^[1-3]是目前产业界和学术界研究

的一个热点话题, 它提供了一种新型共享基础设施的方法, 租户可以通过互联网分享虚拟化的资源, 极大扩展了互联网服务提供的种类和范围。

收稿日期: 2017-06-25; 修回日期: 2017-08-03。通信作者: 赵硕, zshuo2016@126.com

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); 信息工程大学新兴方向培育基金资助项目 (No.2016610708); 国家重点研发计划项目 (No.2016YFB0800100, No.2016YFB0800101); 河南省科技攻关计划项目 (No.172102210615); 国家自然科学基金资助项目 (No.61602509)

Foundation Items: The Foundation for Innovative Research Groups of the National Natural Science Foundation of China (No.61521003), The Emerging Direction Nurturing Foundation in Information Engineering University (No.2016610708), The National Key R&D Program of China (No.2016YFB0800100, No.2016YFB0800101), The Science and Technology Research Project of Henan Province (No.172102210615), The National Science Foundation for Distinguished Young Scholars of China (No.61602509)

云计算作为一种大规模的资源共享模型,需要超大规模的数据中心建设,对数据中心网络提出了新的要求。网络虚拟化(NV, network virtualization)^[4~7]为满足这些要求提供了一条有效的途径,其主要思想是将数据中心网络划分为多个虚拟网(VN, virtual network),各个VN共享相同的底层物理网络资源(SN, substrate network),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。网络虚拟化虽然大大提高了数据中心网络的灵活性、应用的多样性、资源的利用率,能够最大程度地满足租户的需求,但多个虚拟网共享相同底层物理资源也带来了新的安全威胁^[8~13]。其中,侧信道攻击^[8,11~13]是造成当前云计算与数据中心环境下多租户间信息泄露的安全威胁之一。攻击者通过放置恶意虚拟机与目标虚拟机共存相同的物理主机上,然后通过侧信道窃取目标虚拟机中的隐私信息。

目前,防御侧信道攻击的研究主要分为2种思想。一种思想^[14~16]是根据具体的侧信道攻击机制修改物理主机的软硬件。该类方法可以有效地防御特定类型的侧信道攻击,但无法防御不同类型的和未知类型的侧信道攻击。另一种思想^[17~20]是在不修改物理主机的软硬件前提下,通过虚拟机的映射、迁移策略主动地防御侧信道攻击。该类方法能够防御不同类型的和未知类型的侧信道攻击,也不需要修改物理主机的软硬件,但受制于对网络服务性能影响大、防御成本高的问题,难以适用于大规模的网络场景。

针对现有防御方法存在的局限性,借鉴文献[20]提出的侧信道攻击的信息泄露模型,本文提出一种面向多租户的关键虚拟机动态迁移方法,主要贡献如下。

1) 根据租户的安全需求设定关键虚拟机的比例,有针对性地对虚拟机进行主动的动态迁移,减少虚拟机迁移的数量。

2) 通过虚拟机之间共存时间约束条件来最大化降低虚拟机动态迁移的频率。

3) 以最小化迁移开销作为虚拟机迁移的目标函数,进一步降低虚拟机迁移的成本。

4) 定义了风险系数作为侧信道攻击防御效果的评价指标。

2 相关工作

在云计算与数据中心环境下,通过虚拟化技术能够对不同租户的虚拟机之间进行逻辑隔离,以此保证虚拟机(VM, virtual machine)功能的独立性和信息的安全性,但恶意虚拟机仍然可以通过侧信道窃取共存在相同物理主机上其他虚拟机的隐私信息。有关研究表明^[8,12,21],利用虚拟机之间的侧信道窃取租户的隐私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识别攻击目标^[8],也可以从共享信息中得知攻击目标的应用^[22]和操作系统^[23]。文献[12]表明,利用侧信道攻击,可以在2~3 min恢复高级加密标准(AES, advanced encryption standard)密钥。

目前,防御侧信道攻击的研究主要分为2种思想。第一种思想^[14~16]是根据具体的侧信道攻击机制修改物理主机的软硬件。文献[14]提出为了防御基于时间的侧信道攻击,可以通过隐藏程序运行的时间和改变程序暴露的时间进行防御;文献[15]表明,通过在操作系统层内保护的进程中加入噪音来防御基于操作系统层的侧信道攻击。文献[16]提出采用跨多个虚拟机的分区加密来防御针对应用层的侧信道攻击。第二种思想^[17~20]是在不修改物理主机的软硬件前提下,通过虚拟机的映射、迁移策略主动地防御侧信道攻击。文献[17]提出建立灵活的迁移架构,在保证网络健全的情况下对虚拟节点进行迁移,能够减缓侧信道攻击带来的威胁,但虚拟机迁移没有目的性,会带来较大的迁移开销。文献[17]根据虚拟机的安全需求设计了一种安全感知的虚拟网映射架构,一定程度上提高了虚拟机信息的安全性,但使虚拟网络映射成功率出现较大幅度的下降,对网络服务的性能影响较大。文献[19]提出采用混合的虚拟机放置策略,增加恶意虚拟机与目标虚拟机共存的难度,提高了攻击者的攻击成本。但对侧信道攻击的防御不够彻底,防御效果有限。文献[20]提出通过周期性地对虚拟机进行动态迁移来降低虚拟机之间共存的时间,能够较彻底地防御侧信道攻击,但虚拟机数量过多会导致迁移开销成本过高,难以适应于大规模的网络场景。

3 问题描述

3.1 网络模型

1) 数据中心网络

数据中心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。对于本文，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。

2) 虚拟网请求

虚拟网请求是不断到达的。虚拟网请求的集合模型表示为 $G^v = \{G_1^v, G_2^v, \dots, G_k^v\}$ ，其中 $k=1, 2, \dots, n$ 。第 i 个虚拟网请求可以表示为 $G_i^v = (N_i^v, L_i^v, Arrvial_i^v, Dur_i^v)$ 。类似地， N_i^v 、 L_i^v 分别表示虚拟网 G_i^v 中虚拟机和虚拟链路的集合， $Arrvial_i^v$ 表示虚拟网 G_i^v 的到达时刻， Dur_i^v 表示虚拟网 G_i^v 持续的生存时间。对于每一个虚拟机 $n_i^v \in N_i^v$ ，对应有一个虚拟机资源需求 $C(n_i^v)$ ，表示该虚拟机所需的物理资源。每条链路 $l_i^v \in L_i^v$ 对应一个链路资源需求 $B(l_i^v)$ ，表示该虚拟链路所需的带宽资源。

3) 虚拟网映射

基于上述描述，定义虚拟网映射 M 为一组虚拟网请求的映射集合， $M = \{M_1, M_2, \dots, M_i, \dots\}$ ，其中， M_i 表示将虚拟网请求的拓扑 G_i^v 映射到数

据中心网络拓扑 G^s 上，即 $M_i: G_i^v \rightarrow G_i^s(N_i^s, L_i^s)$ ，其中 $N_i^s \subseteq N^s$ ，表示数据中心网络 G^s 中的物理主机子集，是虚拟网 G_i^v 的虚拟机的映射对象； $L_i^s \subseteq L^s$ ，表示数据中心网络 G^s 中的链路子集，是虚拟网 G_i^v 的虚拟链路的映射对象。 N_i^s 和 L_i^s 都必须满足对应虚拟机和虚拟链路的资源需求。虚拟网映射可以分为虚拟机映射和虚拟链路映射这 2 个阶段。图 1 给出了虚拟网映射实例，其中右半部分表示一个数据中心网络实例，物理主机边的方框中数值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 $B(l^s)$ ，左半部分是 2 个虚拟网请求实例。

3.2 侧信道攻击问题描述

在云计算和数据中心环境中，攻击者通过放置恶意虚拟机达到与目标虚拟机共存在相同物理主机上的目的，然后利用侧信道窃取目标虚拟机中的隐私信息^[19]。如图 2 所示，攻击者通过构建虚拟网 G_1^v 使部分恶意虚拟机能够与虚拟网 G_2^v 中的目标虚拟机共存在相同的物理主机上，进而对目标虚拟机发动侧信道攻击。

攻击者发动侧信道攻击主要分为 4 个步骤。

① 攻击者通过启动大量恶意虚拟机或根据探测到的网络信息有选择地启动恶意虚拟机，使部分恶意虚拟机能够与目标虚拟机共存在同一个物理主机上。

② 目标虚拟机在工作时对共享的物理资源（CPU cache、网络队列）产生影响。

③ 恶意虚拟机通过共享的物理资源对共有的目标虚拟机进行评估和测量。

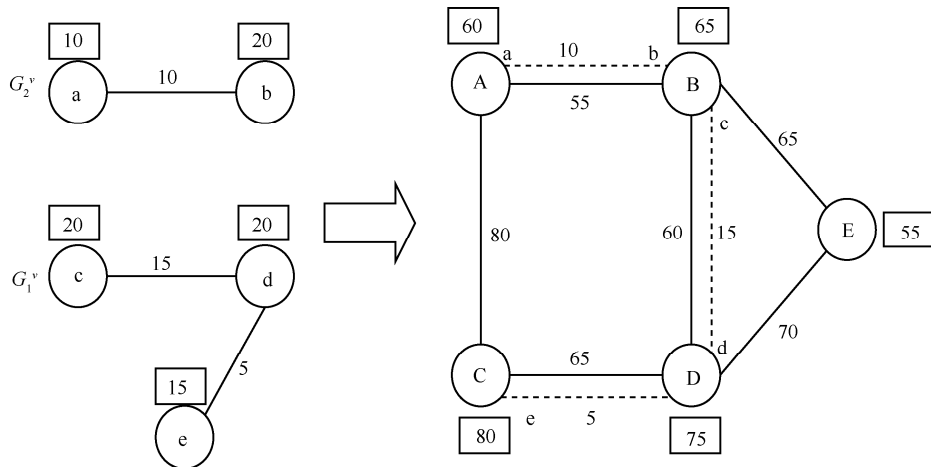


图1 虚拟网映射实例

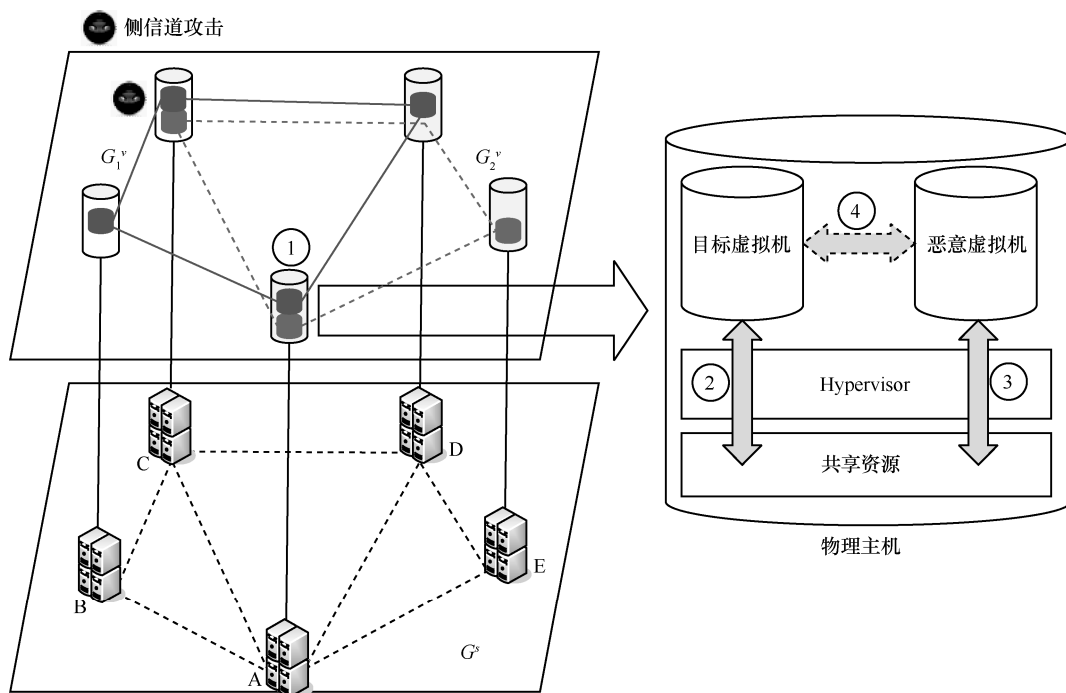


图 2 侧信道攻击模型

④ 恶意虚拟机根据评估和测量的结果,建立与目标虚拟机的隐蔽信道,窃取目标虚拟机的隐私信息。

由文献[20]知,攻击者若想通过侧信道成功窃取目标虚拟机中的隐私信息,必须保证恶意虚拟机与目标虚拟机共存一定的时间。因此,虚拟机中隐私信息的安全主要取决于如下几个因素,如表 1 所示。

表 1	安全影响因素
符号	含义
K	信息泄露速率
Γ	共存的时间间隔数量
ε	最小的时间间隔

其中,信息泄露速率 K 的值和目标虚拟机的 CPU 需求资源的大小有关。目标虚拟机的 CPU 需求资源越大,对共享的物理资源产生的影响越多,则恶意虚拟机能够评估和测量的信息越多,通过侧信道窃取信息的速率越快,目标虚拟机的信息泄露速率越快。

因此,要想成功防御侧信道攻击,保证虚拟机隐私信息的安全,需要满足式(1)。

$$K\Gamma\varepsilon \leq I \quad (1)$$

其中, I 表示信息被成功窃取的最小信息量。

4 面向多租户的关键虚拟机动态迁移方法

由式(1)知,可以通过周期性地对虚拟机进行动态迁移,减少虚拟机之间共存的时间,来改变式(1)中 Γ 的大小,以此保证目标虚拟机中的隐私信息不被恶意虚拟机成功窃取。但是,随着网络规模的增大,虚拟机数量的增多,如果对所有的虚拟机都进行周期性的动态迁移,将造成虚拟机迁移成本过大,迁移算法收敛时间过长,导致该方法难以适应大规模的网络场景。因此,本文提出一种面向多租户的关键虚拟机动态迁移方法。一方面,根据租户对虚拟机的安全需求设定关键虚拟机的比例,以此减少虚拟机迁移的数量,降低虚拟机迁移的开销成本和算法的收敛时间;另一方面,在保证虚拟机信息安全性的前提下,最大化降低虚拟机动态迁移的频率,进一步降低虚拟机的迁移开销成本。本节对本文所提方法进行具体的描述。

4.1 关键虚拟机的设定

由 3.2 节知,虚拟机的 CPU 需求资源越大,信息泄露速率 K 的值越大,该虚拟机的隐私信息被攻击者成功窃取的风险越大,另外,由于部分虚拟机中不含有隐私信息或重要的信息,不需要对该部分虚拟机进行动态迁移保护。因此,可以

将虚拟机内是否含有隐私信息和虚拟机 CPU 值的大小作为关键虚拟机设定的标准。在虚拟网请求到达时,先对该虚拟网中的所有虚拟机按照 CPU 值的大小进行降序排列,即虚拟机的 CPU 值越大,则该虚拟机的序号越小。

云服务提供商为租户提供一个自定义的关键虚拟机比例设定接口,如图3所示。租户可以通过该接口自定义虚拟网中关键虚拟机所占的比例。例如,若租户选择30%的关键虚拟机比例,则虚拟机 CPU 值大小排名在该虚拟网中前30%的虚拟机将被设定为关键虚拟机。

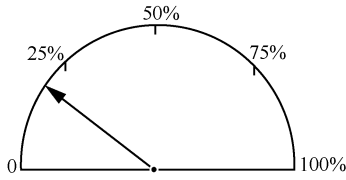


图3 关键虚拟机比例设定接口

关键虚拟机设定步骤如下。

步骤1 虚拟机安全需求判断。虚拟网请求到达时,若该虚拟网中的虚拟机存在安全需求且租户有指定要进行保护的虚拟机,则进行步骤2;若有安全需求但没有指定保护的虚拟机,则进行步骤3;若无安全需求,则直接进行虚拟网映射。

步骤2 指定关键虚拟机。租户根据虚拟机中含有信息的重要程度,直接指定需要进行保护的虚拟机,则该指定的虚拟机被标记为关键虚拟机,若还需要设定关键虚拟机的比例,则进行步骤3;若不需要继续设定关键虚拟机的比例,则直接进行虚拟网映射。

步骤3 设定关键虚拟机比例。首先将租户指定的关键虚拟机从虚拟机集合中去除,然后对剩余虚拟机按照 CPU 值的大小进行排序。租户根据自身虚拟网中对虚拟机的安全需求,通过自定义的关键虚拟机比例接口对关键虚拟机的比例进行设定,则指定的虚拟机和比例范围内的虚拟机均被标记为关键虚拟机,然后进行虚拟网映射。

4.2 关键虚拟机的动态迁移方法

1) 迁移策略

由式(1)知,要想保证虚拟机隐私信息的安全性,必须使虚拟机动态迁移的时间间隔数值 Γ 不能超过共存时间阈值 $\Gamma_{\text{阈值}}$, 即

$$\Gamma \leq \Gamma_{\text{阈值}} = \frac{I}{K\varepsilon} \quad (2)$$

综上所述,本文提出方法的迁移策略为:① 有针对性地对虚拟机进行迁移。仅对带有关键虚拟机标记的虚拟机进行迁移,减少动态迁移虚拟机的数量;② 最大化降低虚拟机迁移的频率。以共存时间阈值 $\Gamma_{\text{阈值}}$ 作为虚拟机动态迁移的时间间隔,降低虚拟机动态迁移的频率。

2) 重映射策略

关键虚拟机的动态迁移必将导致与之相关的虚拟链路的迁移,则对虚拟机进行重映射时必须同时满足虚拟机和虚拟链路的重映射约束条件。该方法的映射策略为:① 满足相关约束条件,进行虚拟机重映射时,需要满足资源约束、唯一性约束、虚拟链路流约束等条件;② 最小化迁移开销,以最小化迁移开销作为重映射的目标函数,降低虚拟机迁移带来的迁移开销。

5 关键虚拟机的动态迁移模型

5.1 变量说明

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

② $\beta(l_i^v, l^s)$: 0~1 变量,当虚拟链路 l_i^v 映射到物理链路 l^s 上, $\beta(l_i^v, l^s)$ 为1, 否则为0。

③ $\alpha'(n_i^v, n^s)$: 0~1 变量,当虚拟机 n_i^v 在 t 时刻映射到物理主机 n^s 上, $\alpha'(n_i^v, n^s)$ 为1, 否则为0。

④ $\beta'(l_i^v, l^s)$: 0~1 变量,当虚拟链路 l_i^v 在 t 时刻映射到物理链路 l^s 上, $\beta'(l_i^v, l^s)$ 为1, 否则为0。

5.2 约束条件

为了确保关键虚拟机的隐私信息不被攻击者成功窃取,对不同虚拟网的虚拟机之间共享物理主机的时间进行约束,即虚拟机之间共存时间约束:虚拟网 G_i^v 中的虚拟机 n_i^v 和虚拟网 G_j^v 中的虚拟机 n_j^v 共存的时间间隔数量不能超过时间间隔数量阈值。

① 虚拟机之间共存时间约束

$$\sum_{\lambda=1}^{\Gamma} \sum_{n^s \in N^s} \alpha^{\lambda\varepsilon}(n_i^v, n^s) \alpha^{\lambda\varepsilon}(n_j^v, n^s) \leq \Gamma_{\text{阈值}}, \quad (3)$$

$$i \neq j, n_i^v \in N_i^v, n_j^v \in N_j^v$$

其中, ε 为最小的时间间隔, $\lambda=1,2,\dots,\Gamma$ 。 $\lambda\varepsilon$ 代表不同的时刻,是时间 t 的离散表示形式。

当不同虚拟网的虚拟机之间共存时间达到共存时间间隔阈值时，需要对其中一个虚拟机进行迁移。虚拟机的迁移必将导致与之相关的虚拟链路的迁移，因此对虚拟机进行重映射时需要同时满足虚拟机重映射约束和虚拟链路重映射约束。

② 重映射资源约束

$$\sum_{G_i^v \in G^v} \sum_{n_i^v \in N_i^v} C(n_i^v) \alpha(n_i^v, n^s) \leq C(n^s), \forall n^s \in N^s \quad (4)$$

$$\sum_{G_i^v \in G^v} \sum_{l_i^v \in L_i^v} B(l_i^v) \beta(l_i^v, l^s) \leq B(l^s), \forall l^s \in L^s \quad (5)$$

③ 重映射唯一性约束

$$\sum_{n^s \in N^s} \alpha(n_i^v, n^s) = 1, \forall n_i^v \in N_i^v, \forall i \in [1, k] \quad (6)$$

$$\sum_{n_i^v \in N_i^v} \alpha(n_i^v, n^s) \leq 1, \forall n^s \in N^s, G_i^v \in G^v \quad (7)$$

④ 重映射流约束

$$\sum_{t \in N^s} \beta(l_{i,(m,n)}^v, l_{(s,t)}^s) - \sum_{t \in N^s} \beta(l_{i,(m,n)}^v, l_{(t,s)}^s) = 0, \quad \forall i \in [1, k], s \in N^s \setminus \{n_m^s, n_n^s\} \quad (8)$$

$$\min \left(\chi \sum_{G_i^v \in G^v} \sum_{n_i^v \in N_i^v} C(n_i^v) \alpha^t(n_i^v, n^s) (1 - \alpha^{t+\Gamma_{\text{阈值}}}(n_i^v, n^s)) + \phi \sum_{G_i^v \in G^v} \sum_{l_i^v \in L_i^v} B(l_i^v) \beta^t(l_i^v, l^s) (1 - \beta^{t+\Gamma_{\text{阈值}}}(l_i^v, l^s)) \right), \quad \forall n^s \in N^s, l^s \in L^s \quad (11)$$

其中， χ 和 ϕ 分别表示虚拟机和虚拟链路的单位资源迁移开销。 $\alpha^t(n_i^v, n^s) (1 - \alpha^{t+\Gamma_{\text{阈值}}}(n_i^v, n^s))$ 表示在 $\Gamma_{\text{阈值}}$ 时间间隔后，虚拟机是否在同一物理主机上，同理， $\beta^t(l_i^v, l^s) (1 - \beta^{t+\Gamma_{\text{阈值}}}(l_i^v, l^s))$ 表示在 $\Gamma_{\text{阈值}}$ 时间间隔后，虚拟链路是否在同一物理链路上。式(11)的第一项表示迁移虚拟机带来的开销，第二项表示迁移虚拟链路带来的开销。

5.4 评价指标

为了比较不同防御方法对侧信道攻击的防御效果，本文定义了风险虚拟机和风险系数作为衡量防御侧信道攻击效果的指标，从而对防御侧信道攻击的效果有一个定量的评估。

由式(1)知，若要成功防御侧信道攻击，保证虚拟机中隐私信息的安全，虚拟机之间共存的时间不能超过共存时间阈值，否则虚拟机中的隐私信息有被恶意攻击者成功窃取的风险。若超过共存时间阈值的虚拟机数量越多，则该网络环境中虚拟机的隐私信息被成功窃取的风险越大，虚拟机内信息的安全性越低。

$$\sum_{t \in N^s} \beta(l_{i,(m,n)}^v, l_{(n_m^s, t)}^s) - \sum_{t \in N^s} \beta(l_{i,(m,n)}^v, l_{(t, n_n^s)}^s) = 1, \forall i \in [1, k] \quad (9)$$

$$\sum_{t \in N^s} \beta(l_{i,(m,n)}^v, l_{(n_n^s, t)}^s) - \sum_{t \in N^s} \beta(l_{i,(m,n)}^v, l_{(t, n_m^s)}^s) = -1, \forall i \in [1, k] \quad (10)$$

其中， $l_{i,(m,n)}^v$ 表示源虚拟机和目的虚拟机分别为 m 和 n 的虚拟链路， n_m^s 表示虚拟机 m 所在的物理主机。

式(4)和式(5)表示保证物理主机和物理链路的资源能够满足其承载上的虚拟机和虚拟链路的资源需求；式(6)表示一个虚拟机只能完整地映射到一个物理主机上，式(7)表示同一虚拟网的2个虚拟机不能映射到同一物理主机上；式(8)~式(10)表示虚拟链路重映射的流约束。

5.3 目标函数

为降低虚拟机迁移带来的迁移开销，本文将最小化迁移开销作为重映射的目标函数。

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。

定义1 风险虚拟机

若虚拟网 G_i^v 中的虚拟机 n_i^v 和虚拟网 G_j^v 中的虚拟机 n_j^v 共存的时间间隔数量大于共存时间间隔数量阈值，则虚拟机 n_i^v 、 n_j^v 中含有关键虚拟机标记的虚拟机被定义为风险虚拟机。根据式(3)，风险虚拟机的集合 P_{risk} 为

$$P_{\text{risk}} = \{n_i^v \in N_i^v, n_j^v \in N_j^v, \forall i, j \in [1, k], \quad i \neq j \mid \sum_{\lambda=1}^{\Gamma} \sum_{n^s \in N^s} \alpha^{\lambda \epsilon}(n_i^v, n^s) \alpha^{\lambda \epsilon}(n_j^v, n^s) > \Gamma_{\text{阈值}}\} \cap P_{\text{all_key}} \quad (12)$$

其中， $P_{\text{all_key}}$ 为该数据中心网络上映射的所有关键虚拟机的集合。

定义2 风险系数

风险虚拟机的数量占总关键虚拟机数量的比例，即为风险系数。

$$\rho = \begin{cases} \frac{|P_{\text{risk}}|}{|P_{\text{all_key}}|}, & |P_{\text{all_key}}| > 0 \\ 0, & |P_{\text{all_key}}| = 0 \end{cases} \quad (13)$$

由式(12)和式(13)可知,风险系数 ρ 的值可以直接反映防御侧信道攻击的效果。风险系数 ρ 越大,则网络环境中的风险虚拟机数量越多,即存在侧信道攻击风险的虚拟机数量越多,因此网络环境的安全状况越差,防御侧信道攻击的效果越差。同理,风险系数 ρ 越小,防御侧信道攻击的效果越好。

6 关键虚拟机动态迁移算法

本文以式(3)~式(10)为约束条件,以最小化迁移开销作为重映射目标函数,设计关键虚拟机动态迁移算法,具体算法流程如图4所示。

1) 判断物理主机上是否映射有 2 个及以上不同虚拟网的虚拟机,若有,则进行步骤 2); 否则进行步骤 7)。

2) 判断映射的虚拟机中是否含有关键虚拟机,若无,则进行步骤 7), 否则进行步骤 3)。

3) 判断不同虚拟网的虚拟机之间的共存时间是否达到共存时间阈值,若达到,则进行步骤 4), 否则进行步骤 7)。

4) 首先将达到共存时间阈值的 2 个虚拟机

的计数器都归 0, 然后对含有关键虚拟机标记的虚拟机进行迁移,若都属于关键虚拟机,则选取 CPU 值小的虚拟机进行迁移,以减小虚拟机迁移对整个网络的影响,进行步骤 5)。

5) 搜索同时满足虚拟机和虚拟链路重映射约束条件的物理主机,将满足条件的物理主机放入集合 $P_{migrate}^s$ 中,进行步骤 6)。

6) 选取集合 $P_{migrate}^s$ 中产生迁移开销最小的物理主机作为重映射的目标物理主机,映射完成后更新底层物理资源,进行步骤 7)。

7) 是否遍历完数据中心网络中的所有物理主机,若是,则该周期内虚拟机迁移完成;否则,对下一个物理主机进行检查,进行步骤 1)。

7 仿真实验

7.1 实验设置

本文实验在 Intel Core i7-4790 CPU 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数据中心网络拓扑,关键虚拟机动态迁移算法采用 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 100 个物

```

1) for all  $n^s \in N^s$  do //对于数据中心网络中的所有物理主机进行检查
2)   if  $\sum_{G_i^s \in G^s} \sum_{n_i^v \in N_i^v} \alpha(n_i^v, n_j^s) \geq 2 \quad \forall n^s \in N^s$  then //物理主机  $n_j^s$  上是否映射有 2 个以上不同虚拟网的虚拟机
3)     if  $P_{n_j^s}^v \cap P_{all\_key} \neq \emptyset$  then //映射在物理主机  $n_j^s$  上的虚拟机是否有关键虚拟机
4)        $P_{n_j^s}^{v\_key}.counter++$  //有, 则对物理主机  $n_j^s$  上的关键虚拟机进行计时
5)     if  $\sum_{i=1}^r \sum_{n_i^v \in N^s} \alpha^{ic}(n_i^v, n^s) \alpha^{ic}(n_j^v, n^s) > \Gamma_{\text{阈值}} \quad i \neq j, n_i^v \in N_j^v, n_j^v \in N_j^v$  then //不同虚拟网的虚拟机  $n_i^v$ 、 $n_j^v$  之间是否
        达到共存时间阈值 (其中  $n_i^v$ 、 $n_j^v$  中至少需要含有一个关键虚拟机)
6)        $n_i^v.counter = 0, n_j^v.counter = 0$  //此时将虚拟机  $n_i^v$ 、 $n_j^v$  计时器都归 0
7)        $n_{migrate}^v = \min\_CPU\{\{n_i^v, n_j^v\} \cap P_{all\_key}\}$  //选择关键虚拟机为待迁虚拟链路, 若都是关键虚拟机, 则选择
        CPU 值小的作为待迁虚拟机
8)       if  $(RES[migrate\_nodes] == true) \& \& (RES[migrate\_links] == true)$  then //物理主机是否满足虚拟机和虚
        拟链路重映射约束条件
9)          $P_{migrate}^s = \{n_{migrate\ 1}^s, n_{migrate\ 2}^s, \dots, n_{migrate\ n}^s\}$  //满足映射条件的物理主机放在集合  $P_{migrate}^s$  中
10)         $n_{migrate\_embedding}^s = \min\_migrate.cost(P_{migrate}^s)$  //选择带来迁移开销最小的物理主机作为关键虚拟机重映
        射的物理主机
11)        Embedded, update physical resources. //映射完成, 更新底层物理资源
12)      end if
13)    end if
14)  end if
15) end if
16) end for

```

图4 关键虚拟机动态迁移算法

理节点, 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[5,20]和[5,15]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。

本文对文献[20]的虚拟机动态迁移方法和本文方法进行实验对比。为了方便描述, 将本文方法和文献[20]方法分别用 CVMM (critical virtual machines migrated) 和 VMM (virtual machines migrated) 表示, 其中 VMM 方法采取的是对全部虚拟机进行周期性的动态迁移。

7.2 实验结果

本节实验通过虚拟网络映射成功率、迁移算法收敛时间、迁移开销和侧信道攻击防御效果这 4 个方面, 对 CVMM 方法和 VMM 方法进行性能对比分析。

1) 虚拟网络映射成功率

图 5 表示虚拟机的动态迁移分别用 CVMM 方法和 VMM 方法对虚拟网络映射成功率的影响。从图中可以看出, 使用 CVMM 方法的虚拟网络映射成功率要高于使用 VMM 方法的虚拟网络映射成功率, 而且关键虚拟机设定的比例越低, 对虚拟网络映射成功率的影响越小。该结果产生的原因有 2 个: ① 虚拟机迁移后重映射会导致底层物理资源利用率出现一定程度上的下降, 而且虚拟机迁移的数量越多, 对底层物理资源的利用率的影响越大, 则对虚拟网络映射成功率的影响越大, 而 CVMM 方法仅对带有关键虚拟机标记的虚拟机进行动态迁移, 减少了虚拟机动态迁移的数量, 所以, CVMM 方法比 VMM 方法对虚拟网络映射成功率影响小, 虚拟网络映射成功率高;

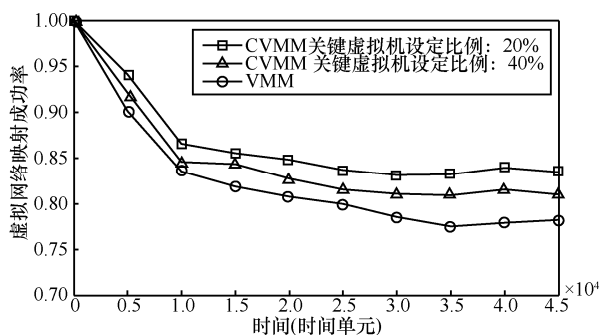


图5 虚拟网络映射成功率

② CVMM 方法在算法设计上考虑到虚拟机迁移和重映射时对底层物理资源的影响, 所以能使底层物理资源相较于 VMM 算法能承载更多的虚拟网请求。因此, CVMM 方法比 VMM 方法对虚拟网络映射成功率的影响小。

2) 迁移算法收敛时间

图 6 描述了 CVMM 方法和 VMM 方法在迁移算法收敛时间方面的对比。本实验将虚拟机迁移间隔周期数值设置为 2 000 个时间单元。一次完整的虚拟机迁移等于从检查物理主机上的虚拟机之间的共存时间间隔开始到该次检查中达到共存时间阈值的虚拟机全部重映射完成为止。当采用 CVMM 方法、关键虚拟机设定比例为 20% 时, 虚拟机迁移算法的收敛时间平均为 56 个时间单元; 当采用 CVMM 方法、关键虚拟机设定比例为 40% 时, 虚拟机迁移算法的收敛时间平均为 301 个时间单元; 当采用 VMM 方法时, 虚拟机迁移算法的收敛时间平均为 1 046 个时间单元。显然, 相较于 VMM 方法, CVMM 方法大大降低了虚拟机迁移算法的收敛时间。由于 CVMM 方法通过设定关键虚拟机的比例, 根据虚拟机的安全需求, 仅对关键虚拟机进行动态迁移, 减少了虚拟机动态迁移的数量, 因此大大降低了虚拟机迁移算法的收敛时间。

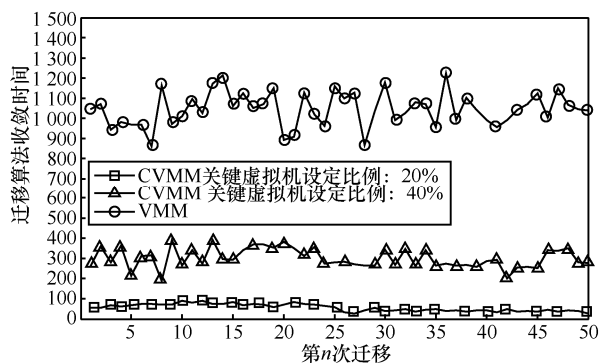


图6 虚拟机迁移算法的收敛时间

3) 迁移开销

图 7 表示 CVMM 方法和 VMM 方法在迁移开销总和方面的对比。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。其中, 虚拟机单位资源迁移开销 χ 和虚拟链路的单位资源迁移开销 ϕ 分别设置为 3 个单位开销和 1 个单位开销。从图 6 中可以直观地看出, 使用 VMM 方法的虚拟机动态迁移开销总和要

远远大于 CVMM, 而且有较快的增长速度。从实验数据中得到, 当使用 CVMM 方法, 关键虚拟机比例为 20% 时, 每 500 个时间单元产生 29 个单位开销; 当使用 CVMM 方法, 关键虚拟机比例为 40% 时, 每 500 个时间单元产生 76 个单位开销; 当使用 VMM 方法时, 每 500 个时间单元产生 180 个单位开销。CVMM 方法使迁移开销降低的原因主要有 2 个: ① 仅对有安全需求的关键虚拟机进行迁移, 减少了虚拟机迁移的数量; ② CVMM 方法将最小化迁移开销作为虚拟机迁移的目标函数, 在进行虚拟机动态迁移过程中也一定程度上降低了迁移开销。因此, 使用 CVMM 方法可以大大减少虚拟机迁移带来的迁移开销。

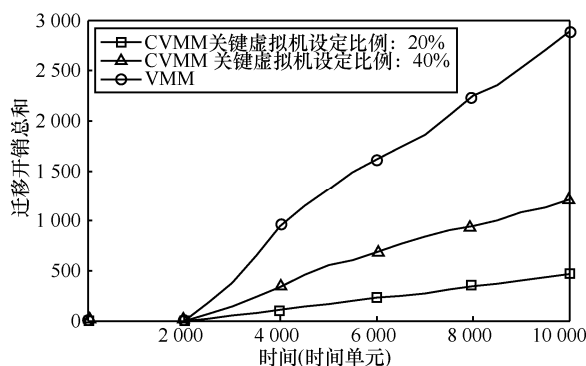


图7 虚拟机动态迁移开销

4) 侧信道攻击防御效果

图8表示 CVMM 方法和 VMM 方法在侧信道攻击防御效果方面的影响。其中, 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, 纵坐标表示租户隐私信息被成功窃取的风险系数。首先, 根据实验计算得到迁移一个虚拟机的平均迁移开销为 8.35 个单位开销, 然后由图6得到每 500 个时间单元内待迁虚拟机的数量, 最后根据每 500 个时间单元内开销预算的大小得到风险虚拟机的数量, 从而得到风险虚拟机占总待迁虚拟机的比例, 即风险系数 ρ 。因此, 在开销预算有限的情况下, 单位时间需要的迁移开销越少, 能够进行迁移的虚拟机数量越多, 风险虚拟机的数量越少, 风险系数 ρ 越小, 侧信道攻击防御效果越好。例如, 当云服务提供商每 500 单位时间提供的迁移开销预算为 20 个单位开销时, VMM 方法的风险系数 ρ 为 0.89; 关键虚拟机比例为 40% 的 CVMM 方法的风险系

数为 0.74; 关键虚拟机比例为 20% 的 CVMM 方法的风险系数为 0.31, 因此 CVMM 方法的侧信道攻击防御效果较好, 且关键虚拟机比例越低, 防御效果越好。另外, 当风险系数 ρ 为 0 时, 则表示采用的方法使所有的虚拟机都可以成功地防御侧信道攻击。当预算开销等于或大于 29 时, 关键虚拟机比例为 20% 的 CVMM 方法的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; 当预算开销等于或大于 79 时, 关键虚拟机比例为 40% 的 CVMM 方法的风险虚拟机的比例达到 0, 可以使所有虚拟机成功地防御侧信道攻击; 当预算开销等于或大于 180 时, VMM 方法的风险虚拟机的比例达到 0, 可以使所有虚拟机成功地防御侧信道攻击。因此, 当单位时间内的开销预算有限时, CVMM 方法相较于 VMM 方法, 可以使风险系数更小, 能更加有效地防御侧信道攻击; 当单位时间提供的开销预算足够大时, VMM 和 CVMM 方法都可以使所有的虚拟机成功地防御侧信道攻击。

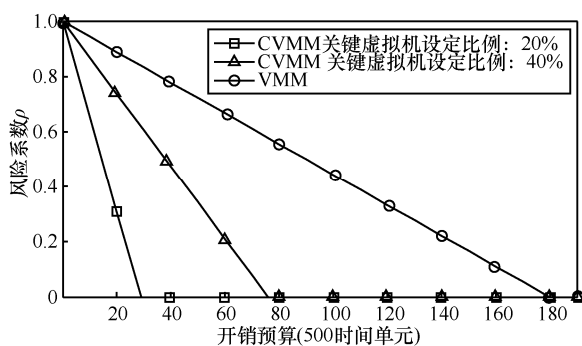


图8 侧信道攻击防御效果

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, 提出了一种面向多租户的关键虚拟机动态迁移方法, 以最小化迁移开销为目标建立了关键虚拟机迁移模型, 设计了关键虚拟机迁移算法, 并进行仿真实验。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, 该方法在有效防御侧信道攻击的前提下, 能够降低对虚拟网络映射成功率的影响, 大大降低虚拟机迁移算法的收敛时间,

从而降低对网络服务性能的影响, 同时降低虚拟机迁移带来的开销。另外, 在单位时间内提供的开销预算有限的情况下, 本文方法能够更加有效地防御侧信道攻击。因此, 本文方法更适用于大规模网络场景。

参考文献:

- [1] ZHANG Q, CHENG L, BOUTABA R. Cloud computing: state-of-the-art and research challenges[J]. Journal of Internet Services and Applications, 2010, 1(1):7-18.
- [2] BUTT S, SRIVASTAVA A, GANAPATHY V. Self-service cloud computing[C]//ACM Conference on Computer and Communications Security. 2015:253-264.
- [3] JAIN R, PAUL S. Network virtualization and software defined networking for cloud computing: a survey[J]. IEEE Communications Magazine, 2013, 51(11):24-31.
- [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] CHOWDHURY N M M K, BOUTABA R. A survey of network virtualization[J]. Computer Networks, 2010, 54(5): 862-876.
- [6] 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.
- [7] 余涛, 毕军, 吴建平. 未来互联网虚拟化研究[J]. 计算机研究与发展, 2015, 52(9):2069-2082.
YU T, BI J, WU J P, et al. Research on the virtualization of future internet[J]. Journal of Computer Research and Development, 2015, 52(9): 2069-2082.
- [8] 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, CCS 2009, Chicago, Illinois, USA, November. 2009: 199-212.
- [9] 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. 2015:729-737.
- [10] 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.
ZHANG Y Q, WANG X F, LIU X F, et al. Survey on cloud computing security[J]. Journal of Software, 2016, 27(6): 1328- 1348.
- [11] WU Z, XU Z, WANG H. Whispers in the Hyper-space: high-speed covert channel attacks in the cloud[C]//USENIX Security symposium. 2012: 159-173.
- [12] 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. 2015:591-604.
- [13] ZHANG Y, LI M, BAI K, et al. Incentive compatible moving target defense against vm-colocation attacks in clouds[C]//IFIP International Information Security Conference. 2012: 388-399.
- [14] LI P, GAO D, REITER M K. Stopwatch: a cloud architecture for timing channel mitigation[J]. ACM Transactions on Information and System Security (TISSEC), 2014, 17(2): 1-28.
- [15] 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.
- [16] PATTUK E, KANTARCIOGLU M, LIN Z, et al. Preventing cryptographic key leakage in cloud virtual machines[C]//The 23rd USENIX Security Symposium (USENIX Security 14). 2014: 703-718.
- [17] GILLANI F, AL-SHAER E, LO S, et al. Agile virtualized infrastructure to proactively defend against cyber attacks[C]//Computer Communications. 2015:729-737.
- [18] WANG Y, CHAU P, CHEN F. A framework for security-aware virtual network embedding[C]//2015 24th International Conference on Computer Communication and Networks (ICCCN). 2015: 1-7.
- [19] HAN Y, ALPCAN T, CHAN J, et al. Security games for virtual machine allocation in cloud computing[C]//International Conference on Decision and Game Theory for Security. 2013:99-118.
- [20] 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. 2015: 1595-1606.
- [21] LIU F, YAROM Y, GE Q, et al. Last-level cache side-channel attacks are practical[C]// 2015 IEEE Symposium on Security and Privacy (SP). 2015: 605-622.
- [22] SUZAKI K, IJIMA K, YAGI T, et al. Memory deduplication as a threat to the guest OS[C]//The Fourth European Workshop on System Security. 2011: 1-6.
- [23] OWENS R, WANG W. Non-interactive OS fingerprinting through memory de-duplication technique in virtual machines[C]// 2011 IEEE 30th International Performance Computing and Communications Conference (IPCCC). 2011: 1-8.

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。

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。

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。

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。