计算机科学
COMPUTER SCIENCE

基于PCPEC的数据中心功耗攻击防御策略

欧东阳，张开强，陈圣蕾，蒋从锋，闫龙川

引用本文

欧东阳，张开强，陈圣蕾，蒋从锋，闫龙川基于PCPEC的数据中心功耗攻击防御策略[J]．计算机科学，2022，49(12)：374-380.

OU Dong-yang，ZHANG Kai-qiang，CHEN Sheng-lei，JIANG Cong-feng，YAN Long-chuan. Data Center Power Attack Defense Strategy Based on PCPEC [J]. Computer Science，2022，49(12)：374-380.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.211000065

基于 PCPEC 的数据中心功耗攻击防御策略

欧东阳[1] 张开强[1] 陈圣蕾[1] 蒋从锋[1] 闫龙川[2]
1 杭州电子科技大学计算机学院 杭州 310018
2 国家电网有限公司信息通信分公司 北京 100761
(oudongyang@hdu.edu.cn)

摘 要 当前数据中心广泛应用多租户、容器化、虚拟化等技术进行服务器聚合与资源复用,并通过服务器资源与电力资源的超售(Oversubscription)进一步提高资源利用率。但是,资源与电力超售使得数据中心服务器在尖峰负载(Workload Bursts)时面临功耗过载的威胁。因此,功耗攻击(Power Attack,即电力攻击)通过运行恶意程序来增加服务器设备的功耗,使之达到或超过配电系统功耗极限值,引起服务器故障或断路器跳闸,甚至导致整个数据中心供电系统中断。为了降低数据中心遭受功耗攻击的风险,文中提出了基于性能等价资源配置的功耗封顶方法 PCPEC,该方法利用虚拟机在不同配置下功耗的差异性进行虚拟机配置等效替换,以实现功耗管控。实验结果表明,PCPEC 方法可以使服务器的动态功耗降低 22.2%~29.6%,且大部分虚拟机在进行资源配置替换后性能均呈上升趋势,最大提升了 2.12%,从而有效减小了功耗攻击对数据中心带来的影响。

关键词:虚拟机;数据中心;功耗攻击;功耗封顶;等效替换
中图法分类号 TP391

Data Center Power Attack Defense Strategy Based on PCPEC

OU Dong-yang[1],ZHANG Kai-qiang[1],CHEN Sheng-lei[1],JIANG Cong-feng[1] and YAN Long-chuan[2]
1 School of Computer Science and Technology,Hangzhou Dianzi University,Hangzhou 310018,China
2 Information and Communication Branch of State Grid Corporation of China,Beijing 100761,China

Abstract Currently,due to the wide application of multi-tenancy,containerization,virtualization and power over-subscription in data centers,the possibility of power attack is becoming increasingly higher. The main means of power attack is to run malicious codes to increase the power consumption of servers,storage device and network equipment to exceed the power limit of a distribution system. And it causes server failure or circuit breaker trip,or even the interruption of the power supply system of the data centers. In order to reduce the risk of power attack on data center,this paper proposes a power capping method of performance equivalence configuration(PCPEC). This method takes advantage of the difference of power consumption in different configurations of virtual machines to implement the equivalent replacement of virtual machine configuration. Experiment result shows that PCPEC can reduce the dynamic power consumption of the server by 22.2%~29.6%,and the performance of most virtual machines increases by 2.12% after the replacement of resource configuration,thus effectively reducing the impact of power attack on the data center.

Keywords Virtual machine,Data center,Power attack,Power capping,Equivalent replacement

1 引言

随着云计算产业的高速发展,全球范围内数据中心的规模和数量与日俱增。数据中心是信息系统及信息服务的基础载体,承载着行业客户最核心的价值数据,确保其安全稳定运行至关重要。功耗攻击,指攻击者针对多租户数据中心虚拟机高密度聚集的特点,租用大量的虚拟机并注入恶意代码,耗尽虚拟机所在服务器的计算和存储资源,导致多台服务器同时到达功耗峰值。此时由于电力超额订购技术,数据中心对这种紧急情况的处理空间非常小,攻击者可以轻松破坏服务器的电源限制并使能耗超出机架或断路器供电容量,导致断路器跳闸甚至整个数据中心电力中断[1-3],形成拒绝服务(Denial of Service,DoS)攻击。例如,2017 年 2 月 28 日 09:44—11:35,亚马逊 Amazon S3 遭到恶意的功耗攻击并出现了宕机事件,导致美国众多网站瘫痪,无法提供正常服务[4]。

与传统的网络攻击相比,功耗攻击有以下特点:首先,功耗攻击的目的是引起服务器乃至数据中心的总体功耗增加,进而使相关的电源设施失效,并中断或终止在受害服务器上

到稿日期:2021-10-11 返修日期:2022-05-15
基金项目:国家自然科学基金面上项目"数据中心电力攻击检测技术研究"(61972118)
This work was supported by the National Natural Science Foundation of China(61972118).
通信作者:蒋从锋(cjiang@hdu.edu.cn)

运行的计算服务。其次，在攻击行为模式方面，由于功耗攻击的目的在于长期、持续性损害服务器硬件，其网络流量特征并不明显，难以从正常的客户端连接方面进行甄别，因此很难依赖传统的网络流量挖掘模式或数字指纹等技术对功耗攻击进行检测识别。最后，在对受害主机的影响方面，受攻击的服务器一般呈现出功耗大幅度增加的状态，很难观测到明显的性能降级，直到服务器硬件出现故障或者失效后性能才会有明显的变化。因此，精细化的电力管理策略是识别良性用户和恶意攻击者的基础。

随着多租户、虚拟化和容器化等技术在数据中心大量应用，用户行为越来越复杂，进一步加大了对功耗攻击的防御难度。对于数据中心电力安全问题，在识别功耗攻击之后，本研究提出了一种基于功耗管控的防御策略，通过性能等价资源配置的功耗封顶方法对服务器功耗进行限制，使得服务器的功耗降低到阈值之下，保证服务器正常运行。

2 数据据中心功耗攻击防御策略相关研究

目前电力攻击引起的高功耗是数据中心面临的一个巨大挑战，为了减少它给数据中心带来的一系列影响，许多研究者提出了多种功耗攻击防御方法。在服务器能耗优化方面，Deng 等[5]对新能源数据中心的供电管理、服务质量与可靠性等方面进行了研究。Li 等[6]对绿色数据中心的状态监控、热量建模、热量管理策略以及热量管理评价进行了研究，并提出了绿色数据中心热量管理的总体架构。Song 等[7]对当前混合供电数据中心的能耗优化方法进行了研究，针对资源层、计算层和服务层提出了不同的优化目标。为了降低服务器能耗，Wang 等[8]提出了面向数据中心典型应用的低功耗调度策略，该策略能够有效降低机器学习类负载的能耗。Zhao 等[9]提出了基于模型预测控制的数据中心节能调度算法，该算法通过减少节点之间的热循环来降低数据中心的冷却能耗。然而，部分研究以牺牲服务器性能来降低能耗，如典型的动态电压频率调整(Dynamic Voltage and Frequency Scaling，DVFS)方法。为了研究 DVFS 方法对性能的影响，Li 等[10]构建了基于片上指令与片外指令的量化模型，以预测指定频率下的程序性能。

上述研究均侧重于服务器能耗管理本身，未充分考虑数据中心功耗攻击的安全隐患。为了消除功耗攻击对数据中心的威胁，研究者从不同方面提出了多种防御方法，包括功耗封顶(Power Capping)、服务器整合、虚拟机迁移等。

功耗封顶指将目标服务器的最大功耗限制在指定的功耗阈值范围内，在不同级别的环境下，研究者提出多种功耗封顶技术。Lefurgy 等[11]提出一种服务器级功耗封顶方法，该方法主要利用反馈控制理论来限制服务器的功耗。在机架或者 PDU(Power Distribution Unit)中，服务器的功耗也可通过功耗封顶方法进行限制[12-14]。对于整个数据中心，Wang 等[15]提出一种分级功耗控制方法(Scalable Hierarchical Power Control，SHIP)，在 3 个不同级别，包括机架、PDU 和整个数据中心进行分级功耗封顶。然而，这类功耗封顶方法在实际应用中存在一些不足。首先，其只能对违反功耗预算的情况做出被动响应，不能主动防御。其次，控制周期太长，需要权衡系统响应时间和计算开销后才能确定。

整体而言，采用功耗封顶的方法[11,15-16]的基本思路分别是利用反馈控制理论和分级别功耗封顶方法被动响应，未能对功耗攻击做出主动防御。

3 基于性能等价资源配置的功耗封顶方法

数据中心不断扩展，其中存在的安全漏洞也越来越多，给了恶意攻击者更多的攻击机会，防御数据中心功耗攻击面临着重大挑战。为了减少功耗攻击给数据中心带来的危害，在检测识别到数据中心受到电力攻击并定位到受攻击的服务器或者虚拟机之后，需要对服务器的功耗进行管控。为了能够有效降低服务器的功耗，本研究从功耗控制入手，提出了一种基于性能等价资源配置的功耗封顶方法，并与当前常见的功耗控制方法 DVFS 进行对比，结果表明本文方法在保证服务性能的同时，有效降低了服务器功耗。

虽然峰值功耗在数据中心发生的概率很小，但一旦发生，数据中心无法保证所有服务器能在峰值功耗状态下同时正常运行，整个数据中心都可能出现故障。为了保证更多的服务器能够同时运行，研究人员和云服务提供商通常会限制物理服务器的最大功耗，这种技术称为功耗封顶技术[16-17]。

当服务器的功耗超过阈值时，可以通过两种方法来降低功耗，分别是 DVFS 和 CPU 封顶技术。DVFS 方法[17-19]通过使用动态电压和频率缩放技术在硬件级别上降低服务器的功耗，该方法可以在短时间内迅速降低功耗，然而低频率处理器的性能会受到很大影响。CPU 封顶技术[20-21]通过限制在 CPU 上运行应用程序的时间来降低功耗，其缺点在于可能导致系统吞吐量降低，从而增加系统的请求数量，最终导致系统性能下降。为了解决上述方法带来的性能损失问题，本文提出了一种基于性能等价资源配置的功耗封顶策略(Power Capping of Performance Equivalence Configuration，PCPEC)，该方法能够在不牺牲性能的情况下降低服务器的功耗。结合 PCPEC，数据中心的功耗封顶框架图如图 1 所示。

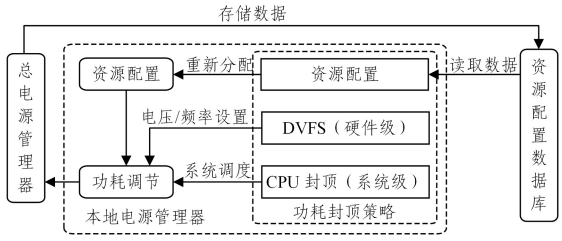


图 1 数据中心功耗封顶框架图

Fig. 1 Power consumption capping framework of data center

功耗封顶框架主要分为 3 部分，分别是总电源管理器、本地电源管理器和资源配置数据库。其中总电源管理器通过任务调度和功耗调节方法来平衡数万台服务器的功率分配。本地电源管理器通过资源配置、DVFS 和 CPU 封顶这 3 种不同级别的功耗封顶策略来进行电源管控，并向总电源管理器报告数据。总电源管理器将多个不同资源配置下的功耗数据存储在资源配置数据库中，通过 PCPEC 替换来降低服务器的功耗。

3.1 基于多级支持向量机的电力攻击检识别

为了准确检测出数据中心服务器或者服务器中的虚拟机是否受到电力攻击，首先需要检测出功耗异常的服务器，本文

利用基于单类支持向量机(Single-Class Support Vector Machine,SC-SVM)策略定位功耗异常的服务器。

SC-SVM 算法的主要思想是获取一个体积最小的球体边界,球体包含所有或者大部分的目标样本。使用 SC-SVM 进行数据分类和异常检测主要分为两个阶段:

(1)训练阶段:假设目标数据集有 n 个数据点,记为 $D=\{x_i \mid 1\leqslant i\leqslant n\}$,对应正常负载在服务器运行的数据。SC-SVM 通过目标数据集创建一个模型,将数据映射到一个特征空间,并建立一个超球体。该超球体将特征空间划分为两个区域,球体内部区域使用代表服务器的正常数据集进行填充,外部区域使用与受攻击的服务器对应的数据填充。

(2)分析阶段:对于任何新的输入样本数据,SC-SVM 都将确定样本是否在超球体内,以识别服务器功耗异常行为。利用 SC-SVM 模型检测功耗异常的服务器的分类算法如算法 1 所示。

算法 1 异常服务器分类算法

输入:数据中心服务器集合 Machine = {Machine_1, Machine_2, …, Machine_m}

输出:异常服务器 Attack_Machine

```
1. for i=0;i+=1 do:
2.   for m in Machine do:
3.     Data1=get(Power, U_CPU);//获得服务器的实时功耗和资源利用率数据
4.     Data2 = calculate(STD_power, STD_cpu, Nor_Mean_power);//获得训练样本数据
5.     train_data=Normalize(Data2);//利用 libSVM 工具归一化数据
6.     for j in length(train_data)/T do://以 T 为时间窗口分别判断每段间隔内的功耗是否异常
7.     res_j=Dis(train_data_j)<R^2? 1:-1;//利用 SC-SVM 方法检测异常服务器
8.     num_attack=length(res_j==-1);//服务器功耗异常的时间段数量
9.     if num_attack>num://若异常时间段的数量大于次数阈值,则判定为异常服务器
10.      Attack_Machine=Attack_Machine+m;//获得功耗异常的服务器集合
11.    end if
12.  end for
13.  end for
14. end for
15. return Attack_Machine;//最终返回受攻击的服务器集合
```

设计脚本以在服务器上运行不同类型的工作负载,得到运行数据之后,对数据进行归一化处理,得到训练样本。之后以 T 作为时间窗口,判断每个时间窗口内计算得到的距离是否大于模型球体半径,若大于则认为该时间段服务器的功耗存在潜在的异常,否则是正常功耗。如果服务器或者虚拟机出现异常的时间段,也就是向量 $\boldsymbol{res}_j$ 中值为 -1 的数量超过次数阈值,则表示该服务器异常,需要做进一步的防御措施。

检测出功耗异常的服务器之后,我们需要对该服务器上运行的虚拟机功耗进行实时预测。虚拟机粒度的实时功耗可见性对于识别恶意功耗攻击和提高服务器能效尤为重要。在攻击检测方面,如果仅考虑单台服务器的功耗或者是单个数据中心的总功耗,那么在攻击者对虚拟机发起攻击时无法定位到具体被攻击的虚拟机,若直接停止被攻击虚拟机所在的服务器,则会严重影响其他任务的运行。在能效优化方面,如果仅考虑虚拟机整合期间物理服务器上的资源利用率,那么部分服务器上整合以后的虚拟机总功耗可能会超过功率限制,并引发功耗封顶机制。

直接通过硬件功耗测量设备来测量虚拟机的功耗是不可行的,需要构建特定的虚拟机功耗预测模型,将物理服务器的功耗测量能力转移给虚拟机进行功耗预测,为最终识别异常虚拟机定位功耗攻击创造条件。本研究中,为了提高功耗预测的准确性,弥补多元线性回归的不足,采用 Vapnik[22] 提出的 ε-SVR 支持向量机回归(Support Vector Regression,SVR)模型来预测虚拟机的功耗。

模型如下:给定 N 个特征向量,每个特征向量具有 n 个元素的 $N\times n$ 数据集 $R=\{(x_{ij}, y_i) \mid i=1,2,\cdots,n; j=1,2,\cdots,N\}$,$x_{ij}$ 表示第 j 个训练特征向量的第 i 个数据样本,y_i 是对应 x_i 的实际值。由于虚拟机的功耗也就是动态功耗资源主要是 CPU、内存和磁盘这 3 部分,故选取 CPU 利用率、内存利用率、磁盘吞吐量和磁盘每秒读写次数(Input/Output Operations Per Second,IOPS)这 4 个特征作为训练模型的输入数据。在 ε-SVR 中,通过将训练数据 R 映射到高维特征空间,形成预测的超平面。该超平面也表示输入数据(自变量)和输出数据(因变量)之间的非线性关系,ε-SVR 函数如下:

$$f(\boldsymbol{x})=W^{\mathrm{T}}\varphi(x)+b \tag{1}$$

其中,$W\in R$ 是特征向量的加权值,b 是超平面的截距,$\boldsymbol{x}$ 是 R 中的输入向量,由影响虚拟机功耗的因素组成,$\varphi(\boldsymbol{x})$ 是将特征向量映射到高维特征空间的映射函数。

在异常服务器上完成运行虚拟机功耗预测之后,再次利用 SC-SVM 分类方法对预测的虚拟机功耗进行分类,识别出功耗异常的虚拟机,最终对定位到的虚拟机进行功耗优化,以减少服务器的整体功耗。

检测过程如下:首先利用 SC-SVM 方法检测出功耗异常的服务器,再利用基于 ε-SVR 的虚拟机功耗预测方法对定位的服务器上的虚拟机进行功耗预测,之后再次利用 SC-SVM 分类方法对预测的虚拟机功耗进行分类,识别出功耗异常的虚拟机,最终对定位的虚拟机进行功耗优化,以减少服务器的整体功耗。具体的实现过程如算法 2 所示。

算法 2 功耗攻击检测识别算法

输入:数据中心服务器集合 Machine = {Machine_1, Machine_2, …, Machine_m}

输出:潜在功耗攻击的虚拟机 res = {$\text{Machine}_i[\text{vm}_x,\cdots,\text{vm}_y]$, …, $\text{Machine}_j[\text{vm}_x,\cdots,\text{vm}_y]$}

```
1. for i=0;i+=1 do:
2.   for m in Machine do:
3.     Attack_Machine = Attack_Machine + Model_SCSVM(data1);//调用算法 1 获得功耗异常服务器集合
4.   end for
5.  for m in Machine do:
6.   if m∈Attack_Machine://若该服务器被判断为是功耗异常服务器
7.     for n in m do:
8.       Data2=get(U_CPU, U_mem, Nor_iops, Nor_thr);//获得虚拟机的实时资源利用率
9.       Power_vm_n=f(Data2);//预测虚拟机功耗
```

```
10.          Data3 = calculate(ST D_power_vm, ST D_cpu_vm,
                 Nor_Mean_power_vm, vm_cpu_temp)
11.      data3=Normalize(Data3);//利用 libSVM 归一化数据
12.      for j in length(data3)/T do:
13.        res2_j=Dis(data3_j)<R^2? 1:-1;
14.       num_attack_vm=length(res2_j==)1);//虚拟机功耗异
          常的时间段
15.      end for
16.       if num_attack_vm>numandvm_cpu_temp>all_cpu_
          temp://若虚拟机功耗异常的时间段数量大于阈值，虚拟
          机 CPU 核心的温度高于所有 CPU 核心的平均温度
17.         res=res+{vm_n};//将检测到的受攻击虚拟机放在 res
            集合中
18.       end if
19.     end for
20.   end if
21.   end for
22. end for
23. return res;//最终返回受攻击的虚拟机集合
```

首先，对于输入的服务器集合，调用算法 1 异常服务器分类算法对服务器进行分类，以得到功耗异常的服务器集合。之后遍历该集合中的每一个服务器，获取服务器中虚拟机的资源利用率和 CPU 核心温度并利用 ε-SVR 方法对虚拟机功耗进行估计。接下来计算虚拟机功耗和 CPU 利用率的标准差以及平均功耗，并利用开源工具 libSVM[23] 进行归一化处理，将其作为模型的输入数据。然后根据虚拟机功耗异常的时间段数量和虚拟机 CPU 核心温度这两个指标来判断当前虚拟机是否为受害虚拟机，若异常的时间段数量大于阈值并且虚拟机的 CPU 核心平均温度高于服务器所有 CPU 核心的平均温度，则将对应的虚拟机视为受攻击服务器，反之则不是。最后将潜在遭受功耗攻击的虚拟机放入结果集合中，以进行后续的防御操作。

3.2 基于等效替换的功耗封顶方法

PCPEC 策略的主要思想是利用虚拟机在不同资源配置下功耗的差异性以及性能的相似性。图 2 给出了多个虚拟机在不同 CPU 和内存配置下运行 DA(Data Analytics)工作负载的功耗和性能的分布图。图中每个星点代表一种资源配置，可以看出，在不同的配置下，虚拟机的性能与功耗都各不相同。在较小的性能变化范围内，如在图中的椭圆框内，虚拟机的功耗有明显的变化，变化值高达 5 W。由此可知虚拟机在不同资源配置下可以有明显的功耗差值但性能却相似，利用这一特点，可通过性能等效替换在不损失性能的情况下降低服务器的功耗。

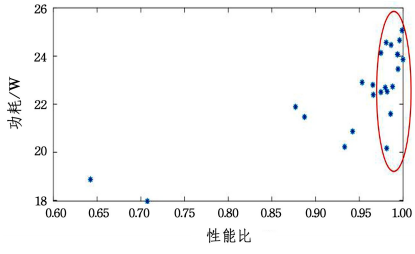


图 2 不同资源配置下虚拟机功耗与性能分布

Fig. 2 VM power consumption and performance distribution with different resource configurations

首先定义一组度量标准，假设当前的资源配置属于等价区域 $EA=[ea_1,ea_2,\cdots,ea_n]$，$ea_i$ 是虚拟机 i 的等价区域，等价区域定义为性能比大于 0.9 的资源配置集合。服务器的资源配置集合表示为 $EC(EA,VM)$，其中 $EC(ea_i,vm_i)$ 表示服务器上第 i 个虚拟机的资源配置集合。

例如，虚拟机 1 和虚拟机 2 的 PCPEC 分别是 $\{conf_1,conf_2\}$ 和 $\{conf_3,conf_4\}$，则服务器的虚拟机配置为 $\{conf_1,conf_3\}$，$\{conf_1,conf_4\}$，$\{conf_2,conf_3\}$，$\{conf_2,conf_4\}$。PCPEC 的目标函数就是要获得性能最高、功耗最低的虚拟机配置，计算式如下：

$$\max \frac{Perfor\_conf}{Power\_conf} \tag{2}$$

$$Perfor\_conf=\frac{\min t}{t\_conf} \tag{3}$$

$$\text{s.t.}\begin{cases} conf\in EC(EA,VM) \\ \sum Power\_conf<thr \\ r_i\_conf<R_i,i=1,2,\cdots,n \end{cases} \tag{4}$$

其中，$conf$ 是虚拟机的配置；$Perfor\_conf$ 表示虚拟机配置为 $conf$ 时的性能，当虚拟机配置为资源配置集合中的一种时，其计算公式为最短的运行时间与当前配置的运行时间的比值；$Power\_conf$ 表示虚拟机配置为 $conf$ 时的功耗，通过上一节中介绍的预测方法进行估算得到；thr 表示服务器的功耗阈值；r_i_conf 表示第 i 个虚拟机分配的资源，R_i 是第 i 个虚拟机的资源上限。

采用 PCPEC 算法进行服务器功耗限制时，首先需要获取每个虚拟机的资源配置集合信息。在实际环境中，等价区域通常是根据性能比的范围要求来确定，若性能比过小，虽然服务器的功耗得到了一定程度的降低，但性能也受到了较大影响，这不符合 PCPEC 方法的思想。因此在收集资源配置集合信息时通过设定性能比的范围来排除不符合的资源配置，属于此范围的所有配置被视为性能等价。在确定资源配置集合信息之后，对集合中的配置根据功耗降低容量和性能损失值的比值进行优先级排序，比值越大，优先级越高。为了量化这一特性，用一个度量值 W_{ij} 来表示，计算式如下：

$$W_{ij}=\begin{cases} \dfrac{\Delta Power_{ij}}{|\Delta Perfor|_{ij}}=\dfrac{Power_i\_conf-Power_j\_conf}{|Perfor_i\_conf-Perfor_j\_conf|}, \\ \qquad Power>0 \\ 0, \qquad Power\leqslant 0 \end{cases} \tag{5}$$

其中，$\Delta Power_{ij}$ 和 $|\Delta Perfor|_{ij}$ 分别是虚拟机 i 与虚拟机 j 在不同资源配置下的功耗差值和性能差值。当功耗差值大于 0 时，说明在替换配置之后功耗有所下降，可以实现服务器的功耗封顶；当功耗差值小于或等于 0 时，说明配置的替换方案不可行。根据度量值 W_{ij} 的大小，利用贪婪策略寻找出功耗降低最多而性能损失最少的配置。

贪心选择策略分为两部分：第一步，建立优先级队列 Q，根据虚拟机的功耗降低能力 W_{ij} 的大小对其进行排序，并把相应的配置和 W_{ij} 值放入 Q 中。为了确保 Q 中的配置满足资源约束的条件，在计算 W_{ij} 之前先过滤掉不满足条件的配置，例如虚拟机最大的 CPU 核数是 30，而目前设置的 CPU 核数是 35。第二步用试错法调整虚拟机的资源配置，这样做的目的是，虽然在第一步中 Q 的配置都满足了资源限制，但是随着

配置的不断替换，服务器以及虚拟机剩余的资源容量也在变化，故可能在迭代过程中又出现违反资源限制的条件。因此，通过从 Q 中选择一个配置来替换当前配置，若替换的配置不违反资源限制，则将其放入候选集合中，重复此过程，直到服务器的功耗低于阈值。基于性能等价资源配置的功耗封顶算法如算法 3 所示。

算法 3 功耗封顶算法

输入：资源配置集合，虚拟机资源配置 conf

输出：候选资源配置集合 Cand_conf

```
1. Cand_conf={};
2. Power_server=get_Power(conf_1,conf_2,…,conf_n);//在多个不同配置的虚拟机下获取服务器的功耗
3. Data=get(U_CPU,U_mem,Nor_iops,Nor_thr);//获得虚拟机的实时资源利用率数据
4. Power_vm=f(Data);//预测虚拟机功耗
5. PEPEC=get_PECPEC();//从 PEPEC 集合中获取虚拟机的资源配置
6. Q=BuildQueue(Cand_conf,PEPEC);//建立优先级队列
7. Q=Q.sort(W);//根据虚拟机的功耗降低能力进行优先级排序
8. if Power_server>P_Thr do:
9.    Cand_conf=Pop(Q);
10. if Res_limit(conf)do://满足服务器和虚拟机的资源限制
11.    Update(Cand_conf,conf);
12.    Update(Power_vm);
13.   end if
14. end if
15. return Cand_conf;//返回最终的候选资源配置集合
```

3.3 等效资源配置结果评估

本研究在一台如表 1 所列的配置的服务器上进行实验。服务器带有一个 Intel(R) Xeon(R) Gold 6230 CPU 80 核超线程处理器，并配备了 173 GB RAM 以及大小为 480GB 的 SSD 硬盘，服务器的 CPU 驱动设置为 userspace 模式。为了评估 PCPEC 资源配置替换的优势，在实验服务器上部署了 3 个虚拟机来隔离资源。在虚拟机启动之后，使用 CPU 热插拔限制虚拟机的资源，使其只能使用固定的 CPU 核数。

表 1 实验服务器规格

Table 1 Experimental server configuration

组件	型号
操作系统	CentOS Linux release 7.6.1810(Core)
CPU 型号	Intel(R) Xeon(R) Gold 6230 CPU @ 2.10GHz
CPU 核数	80
内存	Hynix DDR4 HMA82GR7AFR4N-VK 173GB
磁盘	1*480GB SSD

除此之外，使用 libvirt 工具来控制虚拟机的内存使用容量，并选取 CloudSuite 基准套件中的 DA(Data Analytics)，IMA(In-Memory Analytics)和 DS(Data Serving)这 3 个不同类型的工作负载进行实验。

之后，通过设置 8 组实验共 24 种不同的资源配置来获取资源配置集合信息，具体资源分配如表 2 所列。为了区分 CPU 核数和内存对服务器和虚拟机的功耗以及性能的影响，特设置前 4 组为内存大小相同情况下的实验，后 4 组为内存大小不一致的实验，通过设置不同的配置并进行对比实验，探索 CPU 和内存对虚拟机运行不同类型工作负载时的影响。

表 2 虚拟机资源配置

Table 2 VM resource configuration

资源	配置#1		配置#2		配置#3		配置#4		配置#5		配置#6		配置#7		配置#8	
	CPU	内存/GB	CPU	内存/GB	CPU	内存/GB	CPU	内存/GB	CPU	内存/GB	CPU	内存/GB	CPU	内存/GB	CPU	内存/GB
vm1	2	10	3	10	8	10	15	10	4	15	5	15	9	15	20	15
vm2	4	10	5	10	9	10	20	10	6	20	7	20	10	20	25	20
vm3	6	10	7	10	10	10	25	10	2	25	3	25	8	25	15	25

首先，在表 2 中的 24 种不同虚拟机资源配置下进行不同工作负载的运行实验，通过基于多级支持向量机的检测算法，得到虚拟机在不同资源配置下运行多种类型负载的功耗以及性能指标。3 种工作负载下虚拟机的功耗差值和性能差值分布如图 3 所示，其中红色箱型图为 3 种负载下虚拟机的功耗差值分布，蓝色箱型图为 3 种负载下虚拟机的性能差值分布，虚拟机的性能由式(3)计算得到。

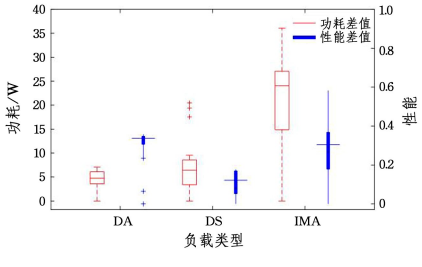


图 3 不同工作负载等效区间的功耗和性能分布(电子版为彩图)

Fig. 3 Power consumption and performance distribution in the equivalent interval of different workloads

从图 3 可以看出，虚拟机功耗差值因负载类型而异，不同类型的工作负载在不同虚拟机资源配置下虚拟机功耗和性能呈现出较大差异，DA 和 DS 在不同资源配置下的虚拟机功耗差值在 5W 左右，而 IMA 负载的功耗差值则超过了 20W，出现如此差距的原因在于 IMA 是 CPU 密集型负载，对于虚拟机 CPU 核数的变化更敏感，故呈现出较大的功耗差异和性能差异。在得到资源配置集合信息之后，利用 PCPEC 算法实现等效性能下服务器功耗的优化。

从资源配置集合中选取虚拟机功耗最大的 3 个资源配置，分别计算这 3 个配置替换为集合中其他资源配置的度量值，从中选出度量值最大的一个配置进行替换，功耗最大的虚拟机优先进行配置替换，直到服务器的功耗低于阈值。这里将阈值设置为服务器功耗峰值的 80%，因为该服务器的最佳利用率为 80%，利用率超过 80%则视为该服务器过载，此时的服务器功耗也极有可能超出设定的功耗阈值。

3 个负载的虚拟机资源配置替换结果如表 3 所列。DA 和 DS 通过 3 个虚拟机的配置替换后服务器的功耗优化到了阈值之下，动态功耗分别由 73.2 W 和 137.9 W 降至 57 W 和

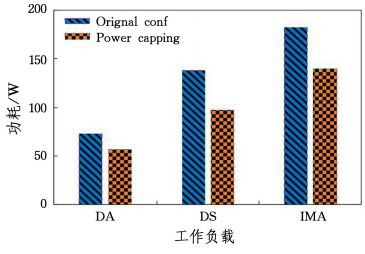
97.1 W，分别降低了 22.2%和 29.6%；IMA 通过两个虚拟机的配置替换后服务器的功耗优化到了阈值之下，动态功耗由 182.2 W 变为 140.3 W，降低了 23%。

表 3 3 个负载虚拟机配置替换结果

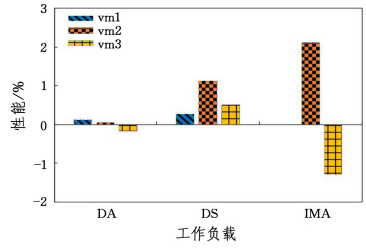
Table 3 Configuration replacement results of three load virtual machines

	DA		DS		IMA	
	替换前配置	替换后配置	替换前配置	替换后配置	替换前配置	替换后配置
vm1	25|20G	8|25G	2|10G	2|25G	10|20G	—
vm2	15|25G	7|20G	4|10G	5|10G	25|20G	20|15G
vm3	25|10G	6|10G	6|10G	25|10G	25|10G	9|10G
动态功耗/W	73.2	57	137.9	97.1	182.2	140.3

配置替换后虚拟机功耗差值和性能差值分布图如图 4 所示，其中图 4(a)给出了利用 PCPEC 方法前后服务器的动态功耗，图 4(b)给出了虚拟机配置替换后的性能变化分布，可以看到，只有 DA 和 IMA 的 vm3 在经过资源配置替换后性能下降了 0.17%和 1.29%，而其他虚拟机的替换性能均有不同幅度的上升，替换性能最大上升了 2.12%，这对于虚拟机以及服务器来说是一个极大的优化，在保证性能相当甚至上升的情况下降低服务器的功耗，使其处在安全状态。



(a)功耗降低分布



(b)性能变化分布

图 4 虚拟机配置替换功耗降低值与性能变化分布

Fig. 4 Virtual machine configuration replacement power consumption reduction value vs. performance change distribution

为了进一步验证 PCPEC 方法的有效性，将其与其他节能方法(本文采用最常见的方法 DVFS)进行对比实验。DVFS 是通过调整服务器 CPU 核的频率大小来动态降低服务器功耗的一种常用的节能方法，利用 CPUFreq 系统来动态调整 CPU 核的最大频率，并使用默认的功耗管理策略，以达到降低服务器功耗的效果。

本文选取 IMA 负载进行功耗封顶和 DVFS 的对比实验，实验结果如图 5 所示，蓝色曲线为原始配置和 CPU 频率下服务器动态功耗分布，橙色曲线和绿色曲线分别是使用 DVFS 和功耗封顶算法后服务器动态功耗分布。

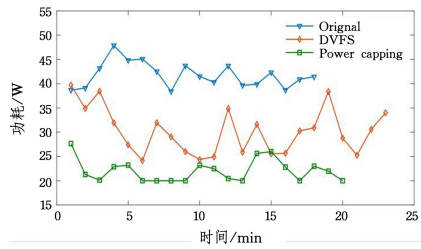


图 5 功耗封顶和 DVFS 算法下服务器动态功耗对比(电子版为彩图)

Fig. 5 Comparison of server dynamic power consumption under power capping and DVFS algorithm

为了使可视化图形分布更明显，特选取以分为单位的时间间隔。可以看到，在功耗方面，本文提出的功耗封顶算法降低的功耗明显比 DVFS 方法多，两者相比平均功耗降低了 27.1%，将近 8W，而通过将 CPU 频率降低 500 MHz，原始的服务动态功耗降低了近 9 W。在性能方面，功耗封顶算法实现的服务器性能比 DVFS 好，前者运行 IMA 的时间为1 148 s，后者为 1 393 s，DVFS 方法使服务器的性能降低了 17.6%，这是因为 DVFS 是通过降低服务器的 CPU 频率来降低服务器功耗，而功耗封顶则是利用资源配置集合进行等效替代。

综上所述，PCPEC 方法可以在不牺牲服务器性能的同时有效降低服务器功耗，使其保持在服务器阈值范围内，有效防御功耗攻击，且与 DVFS 算法相比，提升了用户的使用体验。

结束语 本文研究了针对数据中心功耗攻击的防御策略，主要从功耗控制和负载均衡这两方面来降低数据中心整体的功耗，以应对恶意攻击。首先在功耗控制方面，采用基于性能等价资源配置的功耗封顶方法(PCPEC)来实现对恶意攻击的防御。PCPEC 的核心思想是利用虚拟机不同配置下功耗的差异性，在性能相似的配置下，虚拟机的功耗会出现不同程度的差别。在服务器的功耗超过设定的阈值时，对虚拟机进行性能等价资源配置替换，使得服务器的功耗降低到阈值之下，保证服务器正常运行。实验结果表明，PCPEC 可以使虚拟机在运行不同类型的负载下，其所在服务器的功耗都降低到阈值之下，功耗降低范围在 22.2%～29.6%，且大部分虚拟机在进行资源配置替换后其性能均出现上升趋势，性能最大增加了 2.12%。除此之外，在与 DVFS 的对比实验中，结果显示 PCPEC 方法下服务器的动态功耗最小，与初始服务器的动态功耗相比降低了 52.9%，而与 PCPEC 相比，DVFS 服务器的性能则是降低了 17.6%。实验证明，PCPEC 方法可以降低服务器的整体功耗，以减少功耗攻击带来的影响。

功耗攻击是一种破坏力极强的行为，本文的攻击检测受实验设备所限，没有真实云服务环境中大规模服务器集群，且无法模拟大规模功耗攻击的场景，而是通过注入一些 CPU 密集型的素数程序来进行恶意攻击模拟。因此，在之后的工作中可以进一步完善实验环境，使其更接近真实的恶意攻击场景。考虑到容器技术的快速发展，当前有大量的工作负载容器化部署在多租户容器云平台，未来我们将围绕容器功耗预测和功耗攻击检测展开研究。

参 考 文 献

[1] ISLAM M A，YANG L，RANGANATH K，et al. Why some like

it loud: timing power attacks in multi-tenant data centers using an acoustic side channel [J]. ACM on Measurement and Analysis of Computing Systems, 2018, 2(1): 1-33.

[2] LI C, WANG Z, HOU X, et al. Power attack defense: securing battery-backed data centers [J]. ACM Computer Architecture News, 2016, 44(3): 493-505.

[3] GAO X, XU Z, WANG H, et al. Reduced cooling redundancy: a new security vulnerability in a hot data center [C]// Network and Distributed System Security Symposium(NDSS). 2018.

[4] Summary of the Amazon S3 service disruption in the northern Virginia region [EB/OL]. [2020-03-07]. https://aws.amazon.com/cn/message/41926/.

[5] DENG W, LIU F M, JIN H, et al. New energy application in cloud computing data center: research status and trend [J]. Chinese Journal of Computers, 2013, 36(3): 582-598.

[6] LI X, JIANG X H, WU Z H, et al. Research on heat management method of green data center [J]. Chinese Journal of Computers, 2015, 38(10): 1976-1996.

[7] SONG J, SUN Z Z, LIU H, et al. Research progress on energy consumption optimization of hybrid power supply data center [J]. Chinese Journal of Computers, 2018, 41(12): 2670-2688.

[8] WANG Z G, YI H, ZHANG W H. Data center energy consumption optimization method based on machine learning characteristics [J]. Journal of Software, 2014, 25(7): 1432-1447.

[9] ZHAO X G, HU Q P, DING L, et al. Data center energy-saving scheduling algorithm based on model predictive control [J]. Journal of Software, 2017, 28(2): 429-442.

[10] LI D H, ZHAO J C, CUI H M, et al. Design of DVFS impact model on program performance in data center [J]. Journal of Software, 2017, 28(4): 845-859.

[11] LEFURGY C, WANG X, WARE M. Power capping: A prelude to power shifting [J]. Cluster Computing, 2008, 11(2): 182-194.

[12] RAGHAVENDRA R, RANGANATHAN P, TALWAR V, et al. No "power" struggles: Coordinated multi-level power management for the data center [C]// Proceedings of the 13th International Conference on Architectural Support for Programming Languages and Operating Systems. Seattle: ASPLOS, 2008: 48-59.

[13] RANGANATHAN P, LEECH P, IRWIN D, et al. Ensemble-level power management for dense blade servers [J]. ACM SIGARCH Computer Architecture News, 2006, 34(2): 66-77.

[14] WANG X, CHEN M. Cluster-level feedback power control for performance optimization [C]// 2008 IEEE 14th International Symposium on High Performance Computer Architecture. Salt Lake City: IEEE, 2008: 101-110.

[15] WANG X, CHEN M, LEFURGY C, et al. SHIP: Scalable hierarchical power control for large-scale data centers [C]// 2009 18th International Conference on Parallel Architectures and Compilation Techniques. Raleigh: IEEE, 2009: 91-100.

[16] RANGANATHAN P, LEECH P, IRWIN D, et al. Ensemble-level power management for dense blade servers [J]. ACM SIGARCH Computer Architecture News, 2006, 34(2): 66-77.

[17] FAN X, WEBER W D, BARROSO L A. Power provisioning for a warehouse-sized computer [J]. ACM SIGARCH Computer Architecture News, 2007, 35(2): 12-22.

[18] ARROBA P, MOYA J M, AYALA J L, et al. Dynamic Voltage and Frequency Scaling-aware dynamic consolidation of virtual machines for energy efficient cloud data centers [J]. Concurrency and Computation: Practice and Experience, 2017, 29(10): e4067.

[19] KUEHN P J, MASHALY M. DVFS-power management and performance engineering of data center server clusters [C]// 2019 15th Annual Conference on Wireless On-demand Network Systems and Services(WONS). Wengen: IEEE, 2019: 91-98.

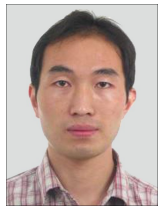
[20] LIM H, KANSAL A, LIU J. Power budgeting for virtualized data centers [C]// 2011 USENIX Annual Technical Conference (USENIX ATC'11). 2011: 59-63.

[21] GUITART J. Toward sustainable data centers: A comprehensive energy management strategy [J]. Computing, 2017, 99(6): 597-614.

[22] VAPNIK V. The nature of statistical learning theory[M]. Springer Science & Business Media, 2012: 201-205.

[23] CHANG C C, LIN C J. LIBSVM: A library for support vector machines [J]. ACM Transactions on Intelligent Systems and Technology(TIST), 2011, 2(3): 1-27.

OU Dong-yang, born in 1980, Ph.D candidate. His main research interests include edge computing and cloud computing.



JIANG Cong-feng, born in 1980, Ph.D, professor, is a member of China Computer Federation. His main research interests include edge computing, system optimization, performance evaluation and distributed system benchmarking.

(责任编辑:何杨)