数据中心面临的潜在攻击威胁与检测方法综述

陈立伟[1)]

[1)](华中科技大学 计算机科学与技术学院, 湖北 武汉 430070)

摘 要 随着数据中心技术的蓬勃发展，巨大的电力消耗成为了最棘手的问题之一。因此，功率超额订阅也成为了数据中心的一种经济有效的供电方式。然而，功率超额订阅使数据中心更容易遭受恶意攻击。与此同时，由于数据中心的基础设施包括供电架构与冷却系统的升级成本较高，现下的多样化攻击方式对数据中心的安全威胁较大。本文对现有的针对数据中心的攻击方式进行了分类，分析了攻击检测方法及其优缺点，以期为数据中心所面临的安全攻击的检测与识别提供一些技术参考。

关键词 数据中心；电力攻击；热攻击；安全威胁

中图法分类号 TP391 DOI 号 10.11897/SP.J.1016.01.2022.00001

Potential Attack Threats and Detection Methods Facing the Data Centers:A Survey

Chen Liwei[1)]

[1)](School of Computer Science and Technology, HuaZhong University of Science and Technology, WuHan 430070)

Abstract With the rapid development of data center technology, huge power consumption has become one of the most difficult problems. Therefore, power oversubscription has also become a cost-effective power supply method for data centers. However, power oversubscription makes the data center more vulnerable to malicious attacks. At the same time, because the upgrade cost of the data center infrastructure including the power supply structure and cooling system is relatively high, the current diversified attack methods pose a greater threat to the security of the data center. This article classifies the existing attack methods against data centers, analyzes attack detection methods and their advantages and disadvantages, in order to provide some technical references for the detection and identification of security attacks faced by data centers.

Key words Data Center; Power Attack; Thermal Attack; Security Threat

1 引言

随着大数据分析、电子商务、云服务、物联网等无处不在的计算需求的增长，数据中心的能源消耗也增长得越来越快。仅仅截至 2017 年，全球运营的各类数据中心总数已达 860 万余。数据中心数量的快速增长也产生了两个问题：(1) 运营商日益增加的能源消耗。2014 年美国的数据中心总耗电量便占据美国全年总耗电量的 1.8%，到 2020 年底全球数据中心总耗电量已经达到当年世界总耗电量的 8%。(2) 给环境保护带来沉重压力。据全球电子可持续发展倡议组织 (GeSI) 估计，到 2020 年底，数据中心的温室气体排放量将占据整个 IT 产业总排放量的 18%[1]。显然，数据中心能源消耗的大幅增长意味着极高的成本投入与加剧的环境污染。

数据中心容量包括电力容量和冷却容量两部分。电力容量由提供给服务器的受 UPS 保护的功率 (也称为临界功率) 来量化，但不包括其他功耗，比如 UPS 功率损耗和冷却系统产生的功率。由于几乎 100% 的服务器功耗 (风扇功耗除外) 都将转换为热负载 (或称为冷却负载)。因此冷却系统容量通常根据托管的服务器功率容量以确定大小，与电力容量一样以千瓦为单位。数据中心的设计架构可能会在冷却能力方面留下一些余量以处理由于某些服务器产生的热量超出预期而导致的不规则发热点即热紧急情况。在这种情况下，冷却系统的利用率仍然很高，这是因为电力系统的升级成本较为高昂，功率超额订阅已成为现代数据中心处理电力供应以最大限度地利用其现有电力基础设施的一种

收稿日期：2022-01-04；修改日期：2022-01-04 本课题得到沃兹基硕德基金 (No.114514) 资助. 陈立伟, 男, 1999 年生, 硕士, 学生, 非计算机学会 (CCF) 会员，主要研究领域为实时多目标检测、图像合成. E-mail: chen18296276027@gmail.com.
第 1 作者手机号码：18296276027, E-mail: chen18296276027@gmail.com

经济高效的方式。数据中心通过容纳超出其支持能力上限的更多物理服务器以超额分配用户请求的电力容量。当前数据中心租赁行业的平均超额水平已达电力基础设施总用电量的 120%。对于负载分配良好的数据中心而言，功率超额订阅的优势在于其租户服务器极少能够同时达到峰值。但是，一旦多台服务器同时达到所订阅的峰值功耗，就会导致数据中心电源过载进而产生严重后果。诸如 CPU 节流、服务停止等多种技术已被推广以处理功率超额订阅导致的功耗过载，但是这些方法大大降低了依靠这些服务器的应用程序的性能。电力攻击的最终目标是使受害者的供电设施失效，降低或终止相应的供电中断服务器上运行的计算服务，严重影响数据中心的可用性。

除了电力系统之外，数据中心的冷却系统对于服务的正常运行时间也至关重要。如果管理不当，恶意工作负载会产生更多的热量，使服务器暴露在不利的热环境中，从而导致更多热紧急情况[2]。更重要的是，冷却系统已成为最先进的数据中心 (例如微软) 发生的停机事件的主要原因[3][4]。为了满足电力容量限制并避免断电情况出现，运营商通常使用电表以持续监控租户服务器的电源使用情况。同时，电表还被用作测量服务器产生的冷却负载的代理以确保其不违反设计的冷却能力，这是因为几乎 100% 的服务器功率最终会转化为热负载 (或冷却负载)。

数据中心遭受电力攻击或热攻击后会产生严重后果，部分延迟敏感型应用如自动驾驶等依托于部署在分布式位置的大量小型数据中心，如果某个区域内的数据中心因遭受定向打击而导致应用性能下降或系统宕机，将会造成重大损失。

本文主要研究了针对数据中心安全性攻击的不同方法。根据不同的攻击载体和攻击者获取相关环境信息的方式，对这些攻击方式进行分类，并研究了初步的攻击检测与识别方法。通过对数据中心安全攻击的研究，进一步了解数据中心面临的安全威胁，从而构建更加全面有效的防御机制。

2 攻击威胁模型

2.1 基于虚拟机的电力攻击

PaaS(平台即服务) 是一种为用户提供计算平台和解决方案的云计算服务，通常实际的物理服务器对于用户而言完全透明，由运营商进行分配和调度。一些 PaaS 运营商部署了负载平衡机制以防止工作负载暴增和服务器负载不平衡问题。这种负载均衡系统通过监控服务器的系统利用率来动态调度工作负载。但是，负载均衡不能等同于功率均衡，在系统利用率方面运营商很难准确地模拟服务器的功耗。利用 PaaS 的这种特性，攻击者可以从运营商提供的同一机架上的多台服务器上订阅多个虚拟机，在这些虚拟机上运行定制的应用程序 (或称为工作负载)，通过两个攻击阶段显著增加受害者服务器的功耗。

IaaS(基础设施即服务) 是提供 IT 行业基础设施比如电力供应系统与冷却系统等的直接面向物理服务器的一种业务模型。IaaS 显然能够允许攻击者拥有比 PaaS 更多的目标服务器控制权。首先，攻击者可以以很小的成本实例化许多虚拟机并在这些虚拟机上运行任意种类的工作负载。其次，处于便利管理的需要，IaaS 数据中心通常使用一些众所周知的拓扑结构和网络配置策略[5]。攻击者可以通过网络探针推断数据中心的内部结构，并定位数据中心内的目标服务器。基于 IaaS 的数据中心也面临着电力攻击的威胁，攻击者可以通过寄生攻击和虚拟机迁移两种方式在 IaaS 数据中心中发起电力攻击。

SaaS(软件即服务) 平台运营商将应用软件统一部署在自己的服务器上。用户可以根据工作的实际需要，以互联网方式联系运营商订购所需要的应用软件服务，从而获得 SaaS 平台提供的服务。最典型的 SaaS 服务是 Web 服务，与 PaaS 和 IaaS 相比，SaaS 用户对基础物理设施的控制程度要少得多，只能通过运营商提供的接口访问相应应用程序。因此，攻击者只能通过特定的 API 访问其获得的服务。但同时，专门设计的应用程序通常会消耗更多的系统资源，尽管攻击难度大，一旦攻击成功却会产生更大的影响。

2.2 多租户数据中心物理侧信道电力攻击

多租户数据中心提供给用户的是基础电力供应设施和冷却系统，用户要将自己的物理服务器架设在运营商提供的机架上，通过向运营商订阅功率上限以获取基础设施服务。与在公有云中使用虚拟机进行电力攻击[6][7] 相比，多租户数据中心的攻击者需要付出更多成本 (例如购买真实物理服务器) 以发起攻击。在当下的多租户数据中心脆弱管理的大环境下，攻击者可以在其他良性租户的服务器达到负载峰值的情况下故意运行高功率负载，导致更

加频繁的功率容量过载。

Islam 等人[8] 发现恶意攻击者可以通过服务器的热力学侧信道获取其他良性租户的运行时功耗信息。如今，开放式冷却系统广泛应用于多租户数据中心。由于数据中心缺乏一个完整的热容器，环境中积累的热空气可以流动到其他服务器处，并提高其服务器入口温度，从而形成了一种热力学信道。攻击者可以非常轻松地藏匿集成在他们自己的服务器主板上的温度传感器，通过热力学侧信道监控入口温度，从而获取良性租户运行时功耗的使用信息。

但是，上述攻击方式是基于攻击者已知数据中心布局的这一事实。一旦布局发生改变，攻击者需要准确地重新建模数据中心的热循环。除此之外，攻击者通过远程控制自己的服务器产生的额外热量可能需要超过 1 分钟的时间才能够被攻击者部署的温度传感器接收，这使得攻击者估计的其他良性租户的功耗信息存在过时的问题。因此，较为简单的热力学侧信道可能不像攻击者预期的那样可以广泛适用，但是在第 2.4 节中讨论了如何利用强化学习实时学习数据中心热力学环境的变化，可以实现更广泛的热攻击。为了解决简单热力学侧信道的滞后问题，除了强化学习的方式，也有工作[9] 提出可以建立由服务器散热风扇所产生噪声构建的声学侧信道以帮助攻击者在其他良性租户达到功率负载峰值时及时进行电力攻击。由于服务器散热风扇的转速会随着其功耗的增加而增加，产生的噪音也随之增加。利用该特性可以获取服务器散热风扇产生的噪声与服务器功耗之间的相关性，从而使攻击者利用噪声推断良性租户的功耗，并趁机发起电力攻击。

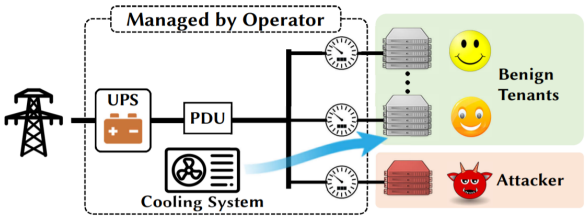

图 1　服务器电压与负载信息密切相关

除了热力学侧信道与声学侧信道，还可以利用电压侧信道去估计其他良性租户从配电单元 (PDU) 中分流的功率，数据中心的电力供应架构如图 1所示。电压侧信道对环境变化具有鲁棒性，而且因为他是有线信号也提供了高精度的测量方法。攻击者只需在其服务器电源单元上安装模数转换器 (ADC)，将 ADC 接入服务器的输入电压即可对 PDU 的电平电压进行采样。电压侧信道的利用原理如图 2所示。由于沿 PDU 共享电源线的电压降，总负载信息包含在电压信号中，同时因为当下的所有服务器都配备功率因数校正 (PFC) 电路，这些电路会产生高频电压纹波，且其幅度与服务器负载密切相关。因此，攻击者可以感知传入的电压信号，提取电压纹波以估计良性租户的负载情况。

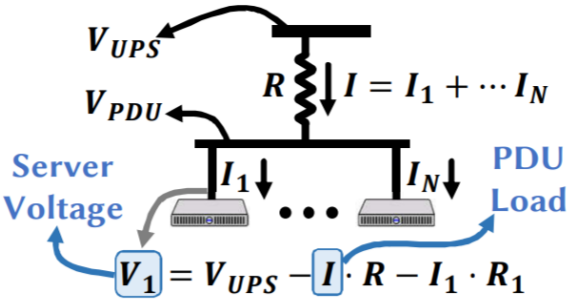

图 2　服务器电压与负载信息密切相关

2.3　DDoS 攻击

DDoS(Distributed Denial of Service, 分布式拒绝服务) 攻击旨在阻止其他合法用户正常访问特定的网络资源。DDoS 攻击正在对那些以互联网为主要方式开展核心业务活动的企业与政府组织构成越来越大的威胁。一次完整的 DDoS 攻击包括攻击者、攻击控制机器、攻击傀儡机器和攻击目标四种参与者，攻击者主机由真正的攻击者进行操作以作为攻击指令的来源，DDoS 原理如图 3所示。在整个攻击过程中，攻击者主机与目标主机并没有产生直接交互，而是利用攻击控制机与攻击傀儡机发起 DDoS 攻击。

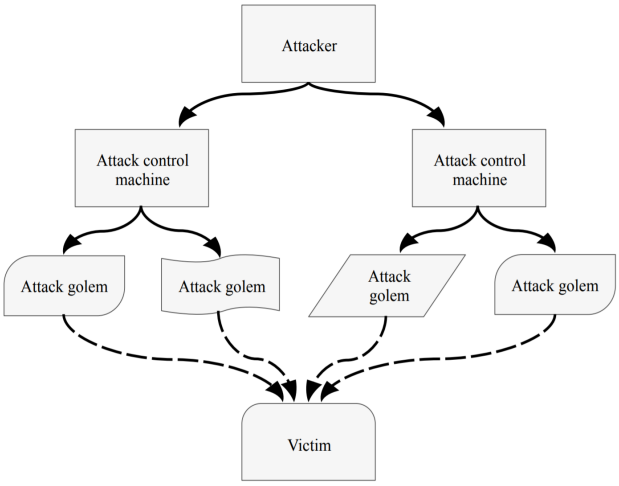

图 3　DDoS 攻击的原理及其参与者

应用级 DDoS 攻击和网络级 DDoS 攻击都是洪泛攻击的一种形式，即通过不断发送服务请求来实现。两者的区别在于，网络级 DDoS 攻击主要利用基层网络协议漏洞，而应用级 DDoS 攻击利用的是诸如 HTTP、FTP、DNS 等较为高级的网络协议栈，客户端与服务端之间会建立正常的网络连接。除此之外，与前者发送大量无意义网络消息不同，应用级 DDoS 攻击向相应协议提供的特殊服务发送具有应用意义的请求消息，比如复杂的数据库嵌套查询请求、大文件图片或视频下载请求等。这些请求无疑会消耗服务器端的大量资源，导致被攻击的目标主机忙于处理攻击请求，无法及时响应其他正常用户的请求。由于应用层网络协议的多样性和复杂性，应用级 DDoS 攻击更难被检测，同时因为高层网络协议可以实现更复杂的功能而导致应用级 DDoS 攻击更具破坏性，对数据中心的网络安全影响更严重。

2.4 基于内置电池单元的热攻击

在多租户数据中心中，租户可以完全控制自己的服务器，但这也引入了潜在的热攻击威胁——即攻击者注入额外的冷却负载以使数据中心的冷却系统过载。由于现在的服务器供应商已经开始以在电源内部集成电池单元的方式为服务器提供更佳的能源效率，攻击者可以利用这种新兴的内置电池单元架构并产生额外的冷却负载 (即热量)，同时不会违反数据中心运营商给予的订阅功率容量，如图 4所示。由于当下数据中心的常见做法是严格监控租户的用电量以及服务器出入口温度，攻击者控制内置电池单元放电以提供额外的电力，这部分额外电力便会转换为热能，从而产生比运营商使用电表测量时更多的热量。

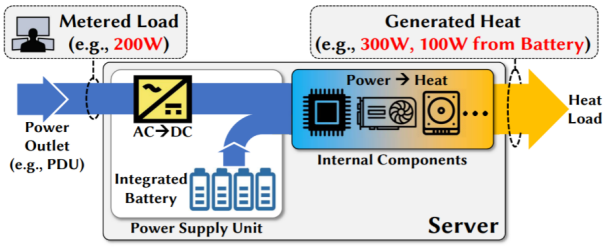

图 4 利用内置电池单元向环境注入额外的冷却负载

仅通过监控服务器出入口温度可能无法及时确定这种额外的冷却负载。因此，攻击者可以注入令运营商难以察觉的额外冷却负载以超过整个数据中心共享的冷却能力，从而引发热紧急情况，进而影响其他良性租户的服务器性能甚至导致数据中心停机。这种电池辅助的热攻击有两种可能策略：(1) 一击必杀型攻击。它旨在持续增加服务器入口温度使其超过安全限制以造成系统中断。它还能够跨多个数据中心进行协调，以实现广域服务中断。(2) 重复攻击。这种攻击方式通过烈度更低的高频热攻击，不断触发热紧急情况和冷却负载上限，在很长一段时间内频繁降低良性租户对延迟敏感型应用程序的性能，将会损害数据中心冷却系统的长期可用性。

但是，这种基于内置电池单元发起热攻击的先决条件是攻击者代理 (即攻击者托管在数据中心的物理服务器) 能够准确估计其所处数据中心的热力学环境情况和其他良性用户的工作负载状况。仅通过简单的电压侧和热力学侧信道等显然无法准确得到环境估计。因此，Shao 等人[10] 提出了一种基于批量 Q-learning 的前瞻性策略，该策略根据电池状态和良性租户的负载动态学习执行重复攻击的最佳时机：只有当良性租户的负载与剩余电池电量同时超过阈值时才会发起热攻击。基于计算流体动力学 (Computational Fluid Dynamics, CFD) 分析和离散时间片 Markov 决策过程，可以对攻击者代理所在数据中心的热力学环境进行建模。

由于数据中心的冷却负载状态对于攻击者而言是外生且不可控的，但是内置电池状态完全可控，可以将电池状态简化为 $b_{k+1}=\min(b_k+e_k,\overline{B})$，其中 e_k 为一个时隙内的充电能力 (取负值时表示放电攻击)，$\overline{B}$ 为电池总能量。引入一个中间状态 $\tilde{s}_k$ 后可以抽象出两个状态转换过程：(1) 从 s_k 到 $\tilde{s}_k$，只更新电池状态，其转换完全由攻击者对内置电池的操作所确定;(2) 从 $\tilde{s}_k$ 到 s_{k+1}，根据攻击者代理的观察去更新冷却需求状态。对于每个时隙 k，批量 Q-learning 的工作原理如下：

$$a_k \leftarrow \arg\max_{a\in\mathcal{A}(s_k)}\left[Q(s_k,a)+\theta V(\tilde{s}_k(s_k,a))\right] \tag{1}$$

$$\tilde{s}_k(s_k,a_k)\leftarrow f(s_k,a_k) \tag{2}$$

$$Q(s_k,a_k)\leftarrow(1-\delta)Q(s_k,a_k)+\delta R(s_k,a_k,s_{k+1}) \tag{3}$$

$$C(s_k)=\max_a\left[Q(s_k,a)+\gamma V(\tilde{s}_k)\right] \tag{4}$$

$$V(\tilde{s}_k)=(1-\delta)V(\tilde{s}_k)+\delta C(s_{k+1}) \tag{5}$$

其中 $\delta\in(0,1)$ 是学习率，当在公式 (2)中设置状态 $\tilde{s}_k(s_k,a)$ 后，仅根据内置电池的充/放电动作更新电池状态。批量 Q-learning 使用了 3 个不同的值矩阵：**状态-动作值** $Q(s_k,a_k)$，**状态后值** $V(\tilde{s}_k)$ 和**正常状态值** $C(s_K)$。首先，在观察到系统状态 s_k 后，攻击者

基于 $Q(s_k, a)$ 和 $V(\tilde{s}_k(s_k, a))$ 根据公式 (1)做出动作 a。接着，基于攻击者观察到的服务器入口温度使用奖励函数获得状态后值 s_k，同时下一个状态 s_{k+1} 是使用电压侧信道估计冷却负载状态获得的。3 个值矩阵可以根据方程递归更新，公式(3)(4)(5)能够使学习过程收敛得更快，攻击者能够迅速学习到发起热攻击的最佳时机。

3　攻击检测与识别方法

3.1　基于攻击特征的检测方法

为了检测并防范攻击者的恶意行为，Jia Bin 等人[11] 提出了一种分布式攻击流量监测模型。该模型主要通过数据采集模块、数据预处理模块、分布式分类检测模块和告警响应模块 4 个部分实现攻击检测与识别。然而，使用机器学习方法去学习电力攻击的统计学特征的缺点是需要进行复杂的人工特征工程。为了提高模型的训练精度和检测精度，基于卷积神经网络的 DDoS 攻击检测方法也应运而生。

总的来说，上述方法可以准确检测攻击行为并识别攻击类型，但其缺点是无法检测到未知攻击且总是落后于新兴的攻击方法，需要加入新攻击方法的特征并不断地迭代训练模型。

3.2　基于异常特征的电力攻击检测方法

前述的基于攻击特征的检测方法只能检测攻击类型已知且攻击消息特征明显的入侵行为，并不适用于未知类型的攻击。Rajesh 等人[12] 提出了一种新的安全系统框架——单类辅助学习环境 (Single Class Assisted Learning Environment, SCALE)，它使用机器学习方法监控并学习数据中心生命周期的可接受特征，以识别异常负载请求。检测到恶意攻击后，抢占控制模块 (Preemption Control Module, PCM) 通过抢占恶意负载的资源以防止电力攻击。PCM 通过监控管理程序的功率管理决策和硬件响应，将数据中心的特征数据提供给机器学习框架。为了降低计算开销并优化特征集，物理主机以集群方式存在，进而特征集就包括每个集群的平均 CPU 利用率、平均功耗、空闲主机数和数据中心总功耗。特征集的选择直接影响可识别的攻击类型。因此，为了检测更加广泛的攻击方式，可以给特征集增加网络带宽利用率、内存利用率等特征。

3.3　基于用户异常行为的 DDoS 攻击检测方法

由于基于网络流量的 DDoS 攻击方式不可避免地会带来流量的异常变化，目前检测 DDoS 攻击的常用方法便是基于异常流量的攻击检测。类似的，可以建立机器学习模型判断数据中心是否受到攻击。Meng 等人[13] 提出了一种基于离散时间马尔科夫链 (DTMC) 算法的用户异常行为检测系统。其核心思想是利用 DTMC 模型提取并比较正常用户的行为特征和需要检测的用户行为特征。如果两者偏差超过设定的阈值，则表明该用户行为异常，应该采取进一步的防御措施。

然而，上述研究中 DTMC 模型的训练数据通常是基于用户在特定网站上访问过的页面来模拟用户行为，一个 Web 页面显然包含许多不同的资源。这种基于用户浏览 Web 页面的数据对用户行为进行建模的方法首先需要将用户从 Web 服务器请求的资源序列映射到 Web 站点上浏览的 Web 页面的实际序列。由于用户的浏览器和服务器上已经缓存的资源不同，不同的用户从 Web 服务器请求资源的顺序可能也会不同，并且不同网页间也可以共享相同资源。因此，映射请求资源序列是一件比较困难的事情。为了解决这一问题，有一项工作[14] 提出了一种基于用户请求资源的异常用户行为检测方法，通过检测用户行为来判断服务器是否受到 DDoS 洪泛攻击。

其具体过程包括两部分：首先从 Web 服务器日志中提取用户浏览行为的实例，每个行为实例代表每个用户在一定的时间间隔内访问该 Web 服务器时所请求的资源。然后利用子空间分析算法——主成分分析 (PCA) 异常检测算法对用户的异常行为实例进行检测，检测出的这些异常行为实例遭受 DDoS 恶意攻击的可能性比较大。

3.4　基于物理信道扰动的热攻击检测方法

第 2.4 节中介绍的基于内置电池单元的热攻击可以通过检测由其引起的不规则热环境而探知。对于基于内置电池单元的热攻击而言，它暴露给数据中心运营商的功率表读数与实际的发热功率不同，会导致同一功率读数下不同的冷却负载状况和服务器出入口温度。对于这部分恶意攻击的额外热量而言，可以使用较为简单的异常检测方法 (比如使用温度传感器和功率表进行交叉读数匹配)，运营商可以检测到由于热攻击可能性而引起的不规则热环境。

另外，如果由于热攻击而导致数据中心系统中断，可以通过彻底排查以检测攻击者的代理。对于重复攻击策略而言，由于其注入的是烈度更低的冷却负载以频繁触发热紧急情况，可能需要采取更复杂的方式以检测重复攻击的存在。而对于开放式气流冷却系统而言，因为其难以进行精确的温度管理，即使不存在热攻击也会偶尔出现热紧急情况。数据中心的运营商通常使用长期温度 SLA(比如服务器入口温度在 99% 以上的时间内都低于安全阈值 27□)，使用类似冷却系统的数据中心可以实施高级算法以监控 SLA 指标并检测出热攻击的存在。

除此之外，也可以在前述提到的电压侧信道和声学侧信道施加扰动以增加攻击者对于攻击时机的不确定性。将干扰噪声添加到电力网络中或者使用供电线的噪声滤波器，可以有效防止攻击者利用电压侧信道探知良性租户的负载情况。此外，多租户数据中心的运营商还可以检查并禁止租户服务器上的异常传感器 (比如麦克风)，以防止攻击者利用其它具有可能性但仍未知的物理侧信道。

4 总结与展望

针对数据中心的攻击方法通常都因其隐蔽性的优势而难以发现。到目前为止，相关的攻击检测技术并不完善，而随着攻击技术的不断发展，各种攻击方式也呈现出了新的特征，更难以被发现并防御。本文首先分析了不同类型的攻击威胁模型，包括虚拟机迁移、物理侧信道、DDoS 洪泛、内置电池单元放电等，然后针对这些攻击方式初步分析了不同的检测方法与预防策略，为数据中心运营商检测和识别恶意攻击者提供了一定的技术参考。

数据中心在未来一段时间内还会保持强劲的发展势头，相应的安全技术也需要持续跟进才能保证数据中心的安全性进而保证基于其上的计算服务与应用程序的可靠性。鉴于深度学习浪潮的涌起，使用鲁棒性较强的机器学习与深度学习方法分析并建模恶意攻击也是一种显而易见的趋势。因此，如何抽象恶意攻击的行为范式并进行针对式预防与检测的研究是该领域在未来一段时间内的主流。

参考文献

[1] ANDERSON D, CADER T, DARBY T, et al. A framework for data center energy productivity[J]. White paper, 2008, 13.

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

[3] INSTITUTE P. 2016 cost of data center outages[R]. https://www.ponemon.org/news-updates/blog/security/2016-cost-of-data-center-outages: Ponemon Institute, 2016.

[4] JONES P. Overheating brings down microsoft data center [R]. https://www.datacenterdynamics.com/news/overheating-brings-down-microsoft-data-center: Datacenter Dynamics, 2013.

[5] RISTENPART T, TROMER E, SHACHAM H, et al. Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds[C]//Proceedings of the ACM Conference on Comp and Communications Security (CCS). 2009.

[6] LI C, WANG Z, HOU X, et al. Power attack defense: Securing battery-backed data centers[C]//Proceedings of the ACM/IEEE 43rd Annual International Symposium on Computer Architecture (ISCA). 2016: 493-505.

[7] XU Z, WANG H, XU Z, et al. Power attack: An increasing threat to data centers[C]//Proceedings of the 2014 Network and Distributed System Symposium (NDSS). 2014.

[8] ISLAM M A, REN S, WIERMAN A. Exploiting a thermal side channel for power attacks in multi-tenant data centers[C]//Proceedings of the ACM SIGSAC Conference on Computer and Communications Security. 2017.

[9] 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[C]//Proceedings of the ACM on Measurement and Analysis of Computing Systems: volume 2. 2018: 1 - 33.

[10] SHAO Z, ISLAM M A, REN S. Heat behind the meter: A hidden threat of thermal attacks in edge colocation data centers[C]//IEEE International Symposium on High-Performance Computer Architecture (HPCA). 2021: 318-331.

[11] BIN J, YAN M, XIANG Z. Ddos attack traffic distributed detection model based on ensemble classifiers[J]. Journal of HuaZhong University of Science and Technology(Natural Science Edition), 2016, 406 (44):1-5+10.

[12] RAJESHJ. S, RAJAMANIKKAM C, CHAKRABORTY K, et al. Securing data center against power attacks[J]. Journal of Hardware and Systems Security, 2019, 3:177-188.

[13] MENG B, ANDI W, JIAN X, et al. Ddos attack detection system based on analysis of users' behaviors for application layer[J]. Proceedings of the 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), 2017, 01:596-599.

[14] NAJAFABADI M M, KHOSHGOFTAAR T M, CALVERT C, et al. User behavior anomaly detection for application layer ddos attacks[C]//Proceedings of the 2017 IEEE International Conference on Information Reuse and Integration (IRI). 2017: 154-161.

Chen Liwei, M.S., student. His research interests include real-time multi-object detection and image synthesis.