Heat Behind the Meter:
A Hidden Threat of Thermal Attacks in Edge Colocation Data Centers

仪表背后的热量：边缘托管数据中心面临的潜在热攻击威胁

汇报人: 陈立伟 M202173809

CONTENTS

01

边缘托管数据中心的概念

What is Edge Colocation Data Centers?

边缘托管数据中心的概念

边缘计算

边缘计算处于物理实体和工业连接之间，在靠近物或数据源头的一侧，采用网络、计算、存储、应用核心能力为一体的开放平台，就近提供最近端服务。它可以为增强现实和自动驾驶等延迟高敏感应用实现超低延迟。

边缘托管数据中心

边缘计算的兴起刺激了多租户边缘托管数据中心的蓬勃发展。
边缘托管是一种建在分布式位置上的小规模共享主机托管数据中心，主要用于托管处理延迟高敏感工作负载的服务器。在这种小型数据中心里，运营商负责为租户提供电力供应与冷却系统以容纳租户自己的物理服务器。

边缘托管与云平台的区别

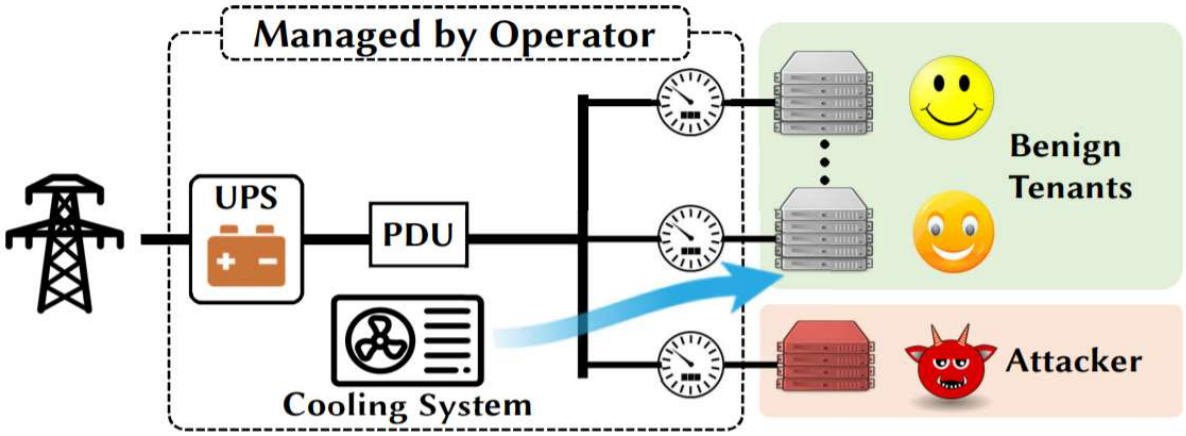
用户向云平台运营商租借共享的云资源，比如弹性计算服务，但是真实的物理服务器对用户完全透明，由运营商维护。
而边缘托管运营商提供的是非IT基础设施支持，即电力和冷却系统，租户要将自己的物理服务器架在边缘托管数据中心的机架上。

02

威胁模型与热攻击策略

Threat Model and Thermal Attack Strategies

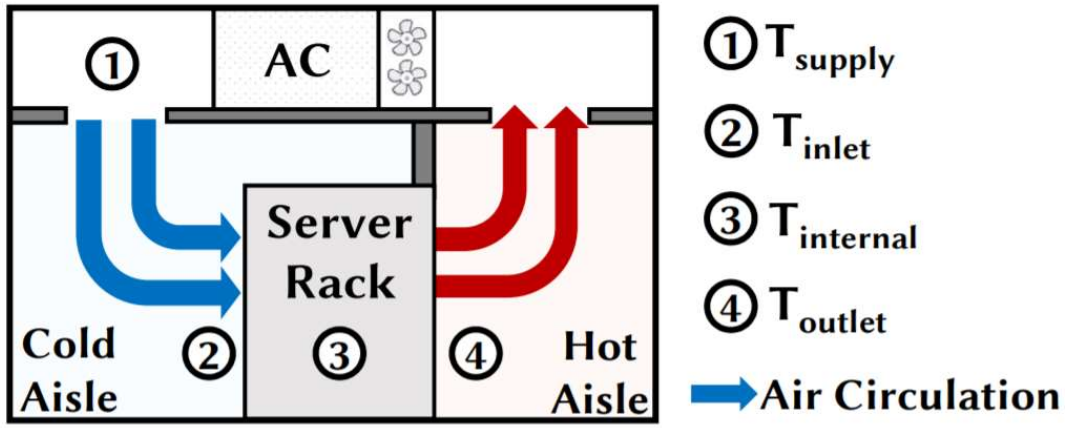
威胁模型与热攻击策略 - 电力供应架构



边缘托管数据中心通常使用树形电源层次架构，总功率容量一般为几千瓦到几十千瓦范围内，由多个租户共享。

接入的市电首先通过不间断电源(UPS)进入数据中心，尔后，受UPS保护的电力进入配电单元(PDU)，该单元负责将电力分配给其下游服务器。

威胁模型与热攻击策略 - 冷却系统架构



边缘托管的典型冷却系统架构如左图所示，一般会采用体积较小的机房空调，并实施冷热通道封闭以防止热空气与冷空气混合。

数据中心有四种不同的温度概念：送风温度 T_{supply}、服务器入口温度 T_{inlet}（即冷空气进入服务器的温度）、服务器内部温度 $T_{internal}$（例如 CPU 温度）和服务器出口温度 T_{outlet}（即离开服务器的热空气的温度）。

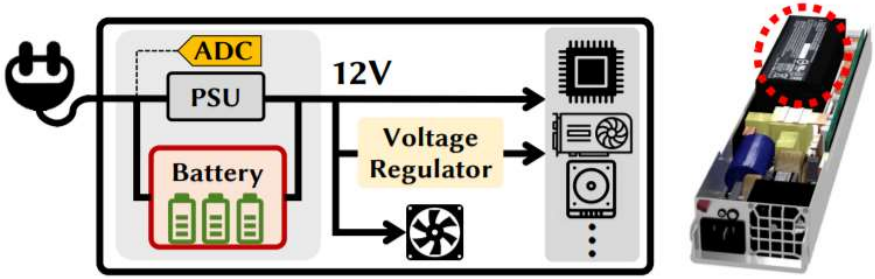
安装了隔热装置后，所有服务器的入口温度几乎与送风温度相同。 因此，送风温度和服务器入口温度是最低的基线，其升高将导致服务器内部和出口温度升高。

威胁模型与热攻击策略 - 热攻击威胁模型

攻击者在边缘托管中安置自己的物理服务器，与其他良性租户共享电力和冷却基础设施。但是，攻击者使用的是内置了电池单元的服务器电源，这种内置电池单元可以为服务器提供额外功率支持，而运营商的用来监控数据中心的功率表和电量表无法探测到攻击者的实际服务器功率和冷却负载。

具体而言，攻击者从运营商那订阅了C_a的功率容量，然后一直保持其电力消耗在订阅功率之下以满足运营商的要求。接着，攻击者利用内置电池单元放电以产生大量额外的热量，向整个数据中心注入超出其功率容量的额外冷却负载。如果攻击者在数据中心总负载临近阈值的情况下发起热攻击，那么极容易**影响其他租户的服务器性能**甚至导致**数据中心因持续高热而宕机。**

其他类型的攻击比如网络DDoS、服务器自爆等方式不在攻击者的考量范围里。



威胁模型与热攻击策略 - 热攻击策略

一次性攻击 One-shot attack

通过增加服务器入口温度T_{inlet}，使其超过安全温度限制（比如45℃）造成系统中断，可以跨多个边缘托管进行协调，实现广域服务中断。即使它是一次性攻击，造成的损害也会很大，尤其是对安全性要求较高的延迟敏感应用，比如边缘辅助驾驶。

重复攻击 Repeated attacks

重复攻击的目标不是以激进的产热策略使托管宕机，而是通过触发边缘托管的热紧急情况和冷却负载上限，使数据中心启动应急措施以降低温度。在很长的一段时间内，重复攻击将会频繁地降低其他良性租户的延迟敏感应用的性能，同时会损害数据中心冷却系统的长期可用性。

由于该策略烈度较低，且攻击时机与攻击持续时间的选择都较为复杂，受实际环境影响很大，需要利用计算流体力学(CFD)和强化学习(RL)对该策略进行实地实时建模。

03

使用强化学习建模重复攻击策略

Using Q-learning to model the repeated attack policy

使用强化学习建模重复攻击策略 - Markov决策过程

将一次性攻击视作是重复攻击的一种特殊情况，即攻击者对良性租户的负载设置了足够高的阈值，并在此之上耗尽内置单元的所有电池能量进行攻击。

因此，论文作者研究了一种通用的前瞻性重复攻击策略:“**Foresighted**”，并将其表述为离散时间Markov决策过程(MDP)。将时间线分为等距时隙后，MDP如右图所示。

其中，元组(s, a, s')表示给定动作a，系统状态将从s演变至s'。
系统状态(System state)包含两个子状态，分别是电池剩余量b和攻击者估计的良性用户负载状态u(利用电压估计其他用户的负载)。

动作a包括三种可能，①给内置电池充电②启动热攻击③待机(伪装正常工作负载)。

MDP的目标是找到一个最优策略$\pi^*: S \to A$，使折扣奖励函数$\sum_{k=0}^{\infty} \gamma^k R(s_k, a_k, s_{k+1})$最大化。

- System state: $s = (b, u) \in \mathcal{S}$
- Action: $a(s) \in \mathcal{A}(s)$
- State transition probabilities: $P(s, a, s')$
- Reward function: $R(s, a, s')$
- Discount factor: $\gamma \in (0, 1)$

使用强化学习建模重复攻击策略 - Q-learning建模

强化学习可以有效地帮助攻击者的代理在未知环境中找到最佳动作。

边缘托管的冷却负载状态对于攻击者而言是外生不可控的，但是电池状态却是完全可控的。因此可以引入批量Q学习进行建模。

具体而言，引入一个中间态$\tilde{s}_k$，则有两个状态转换过程：

①从s_k到$\tilde{s}_k$: 根据攻击者采取的动作去更新电池状态

②从$\tilde{s}_k$到s_{k+1}: 观察边缘托管的负载情况去更新冷却需求状态

对于每个时隙k，其批量Q学习原理如右所示。观察到系统状态s_k后，攻击者根据状态-动作矩阵$Q(s_k, a_k)$、状态后值$V(\tilde{s}_k(s_k, a))$按照公式(3)作出动作a。然后，基于攻击者的该动作能够获得后置状态s_k，并根据攻击者观察到的服务器入口温度及奖励函数获得奖励R_k。最后，利用对电压侧通道的冷却状态估计可以获得下一个状态s_{k+1}。据此，Q、C、V中3个矩阵可以随方程递归更新，且公式(5)(6)(7)将会使学习过程收敛得更快。

$$a_k \leftarrow \arg \max_{a \in \mathcal{A}(s_k)} [Q(s_k, a) + \theta V(\tilde{s}_k(s_k, a))] \quad (3)$$

$$\tilde{s}_k(s_k, a_k) \leftarrow f(s_k, a_k) \quad (4)$$

$$Q(s_k, a_k) \leftarrow (1-\delta) Q(s_k, a_k) + \delta R(s_k, a_k, s_{k+1}) \quad (5)$$

$$C(s_k) = \max_a [Q(s_k, a) + \gamma V(\tilde{s}_k)] \quad (6)$$

$$V(\tilde{s}_k) = (1-\delta) V(\tilde{s}_k) + \delta C(s_{k+1}) \quad (7)$$

04

小集群模拟实验

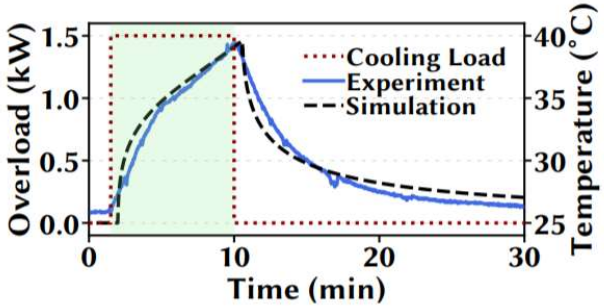
Small cluster simulation experiment

小集群模拟实验 - 实验参数设置

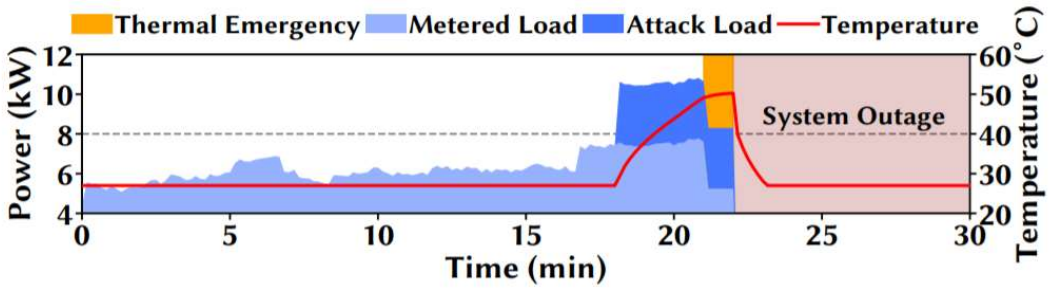
Parameter	Value
Data Center Capacity	8 kW
Number of Tenants	4
Number of Servers	40
Number of Server Racks	2
Attacker's Capacity (c_a)	0.8 kW
Attacker's Total Battery Capacity ($\bar{B}$)	0.2 kWh
Attack Thermal Load from Battery	1 kW
Charging Rate of the Battery	0.2 kW
Temperature Threshold for Emergency (T_{th})	32°C
Q-learning Discount Factor (γ)	0.99
Q-learning Learning Rate ($\delta(t)$)	$1/t^{0.85}$

基于完善的计算流体力学分析方法，可以模拟边缘托管的热力动态。通过在14台服务器的小集群边缘托管原型上进行真实实验可以评估前述提出的模拟模型。左表是相关实验参数设置。

攻击者通过CFD分析获得数据中心的热分布模型，下图展示了CFD分析与实际负载的动态曲线，可以看到热分布模型和实际的温度传感器读数表现出了非常相似的动态曲线。



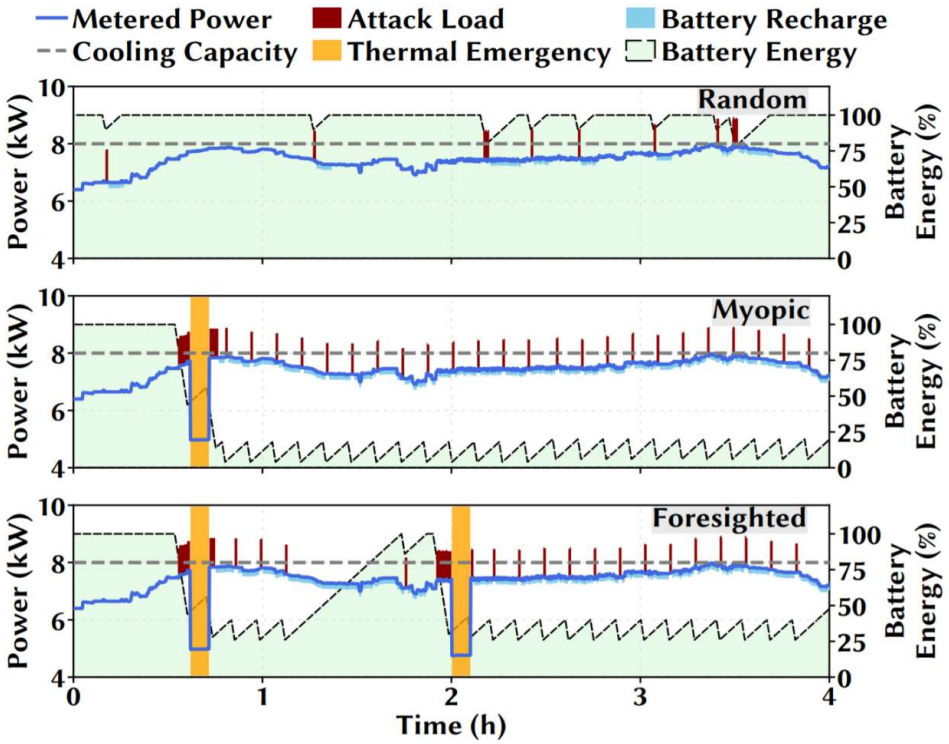
小集群模拟实验 - One-shot attack simulation



攻击者在第18分钟左右注入了3KW的强烈攻击负载，使服务器入口温度迅速上升。在第21分钟时，触发边缘托管的热紧急措施使其将总的计量负载限制在5KW以下。

尽管数据中心及时作出了应对，高强度的工作负载仍然保持服务器入口温度超过45℃的安全阈值，最终导致系统中断。这与其他的正交研究一致：在冷却系统故障的情况下，入口温度会迅速升高。如果这样的一次性攻击跨越多个托管进行协调进攻，将会使相应的服务中断并造成重大损失。

小集群模拟实验 - Repeated attacks simulation



利用总功率和冷却负载相对较高的4小时快照可以说明不同的重复攻击策略如何触发热紧急情况，如左图所示。

Random攻击策略无法触发任何热紧急情况。

Myopic策略利用检测到的良性租户负载阈值发动热攻击，但是在造成了第一次热紧急情况后，内置电池单元未经过足够充电而负载一直在阈值之上，则该策略会不停地发动热攻击但却因为电池容量耗尽而做无用功。

Foresighted策略在触发第一次热紧急情况后，不会像Myopic那样发起一系列失败的短期攻击。它会等待电池能量充沛(即电池状态满足要求)后再次发动热攻击以触发第二次热紧急情况。这正说明了强化学习让其可以考虑行为对未来状态的影响，以最大限度地提高长期收益。

05

防御机制

Defense Machanism

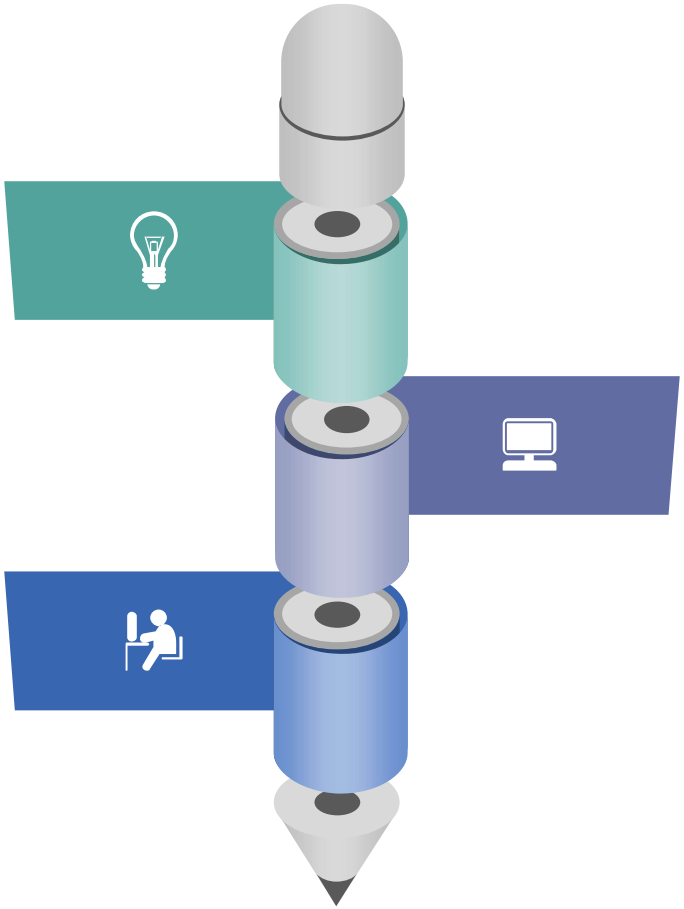
防御机制 - 预防潜在热攻击

基础设施弹性

加强边缘托管的物理基础设施以处理热过载

可以部署额外冗余冷却系统、降低服务器入口温度阈值

但是会提高设施成本



严格进场检查

- 对租户的服务器采用严格背调，检测并移除集成的内置电池单元
- 进行现场功率负载测试，确保服务器真正的功率与租户的订阅容量一致

物理侧信道扰动

- 攻击者需要利用物理侧信道探测环境信息，运营商可以通过添加噪声到电力网络中以混淆攻击者的感知
- 禁止租户服务器上部分传感器的使用

防御机制 – 检测热攻击


检测隐藏冷却负载
发动热攻击时，相同功率读数会导致不同的冷却负载和服务器出入口温度
使用异常检测算法可以检测由于热攻击引起的不规则热环境
识别热攻击
当系统中断或出现热紧急情况后，利用高级算法监控长期温度SLA指标以尽早检测热攻击的存在性
改进边缘托管监控
可以使用麦克风阵列和热成像仪，精确定位高风扇转速的过热服务器，以追查被注入的额外冷却负载的来源

Thanks.

陈立伟 M202173809

2021.12.24