# 多模态威胁感知驱动的边缘控制器动态防御系统研究

郎丁凡
杭州字节信息技术有限公司　浙江　杭州　310000

**摘　要：**随着边缘计算在各领域广泛应用，其安全问题愈发凸显。本研究聚焦多模态威胁感知驱动的边缘控制器动态防御系统，旨在提升边缘计算环境的安全性与稳定性。通过融合多模态感知技术，如流量监测、行为分析等，确定关键感知指标并进行传感器选型，运用高效数据融合算法整合多源数据，精准识别潜在威胁。同时，依据防御策略制定原则，采用动态端口切换、伪装服务等技术实现动态防御，并构建科学的防御效果评估方法。经实验室模拟验证与实际场景应用测试，系统有效提升了边缘计算系统抵御各类威胁的能力，降低安全风险，为边缘计算安全防护提供了创新性解决方案。

**关键词：**多模态威胁感知；边缘控制器；动态防御；数据融合

## 1 引言

在数字化转型加速的当下，边缘计算凭借其靠近数据源、低延迟、本地化处理等特性，在工业制造、智能交通、医疗等众多领域广泛应用，成为支撑新型应用和服务的关键技术。然而，边缘计算节点分布广泛、资源受限且常暴露于复杂网络环境，面临着恶意攻击、数据泄露、非法访问等诸多安全威胁。传统静态防御手段难以应对动态变化的威胁，无法满足边缘计算场景对安全的严苛要求。多模态威胁感知与动态防御技术的融合为解决上述问题提供了新途径。多模态感知可从多维度收集信息，全面洞察潜在威胁；动态防御则能依据威胁变化灵活调整防御策略，主动抵御攻击。因此，开展多模态威胁感知驱动的边缘控制器动态防御系统研究，对保障边缘计算安全、推动其可持续发展意义重大。

## 2 相关技术理论基础

### 2.1 多模态感知技术原理

多模态感知技术融合多种类型的信息采集方式，对目标系统进行全方位监测。以网络流量监测为例，通过分析数据包的大小、频率、协议类型等，可洞察网络连接的异常活动，像端口扫描、分布式拒绝服务攻击的早期迹象都能被捕捉。行为分析则聚焦系统中实体的操作行为，无论是用户的登录、数据访问，还是进程的创建、资源调用，正常行为模式一旦被偏离，就可能暗示着威胁。此外，还包括对硬件状态、环境参数的感知。不同模态的数据各有优势与局限，而融合这些数据，能消除单一模态的不确定性，实现更精准的威胁探测，为后续的防御决策提供坚实的数据基础。

### 2.2 边缘计算架构与特性

边缘计算架构打破传统云计算集中式处理的模式，在靠近数据源或用户端的网络边缘侧，如智能设备、基站、边缘服务器等，进行数据的计算、存储与处理。这种架构具备低延迟特性，例如在自动驾驶场景中，车辆产生的大量传感器数据能在本地边缘节点迅速处理，及时做出驾驶决策，避免因数据回传云端处理造成的时间延误，保障行车安全。同时，边缘计算还能降低网络带宽压力，本地处理大量非关键数据，仅将关键信息上传至云端，缓解网络拥堵[1]。并且，其分布式的部署方式，增强了系统的可靠性与可扩展性，个别边缘节点故障不影响整体运行，也便于根据业务需求灵活增减节点，适配不同规模的应用场景。如图一所示：

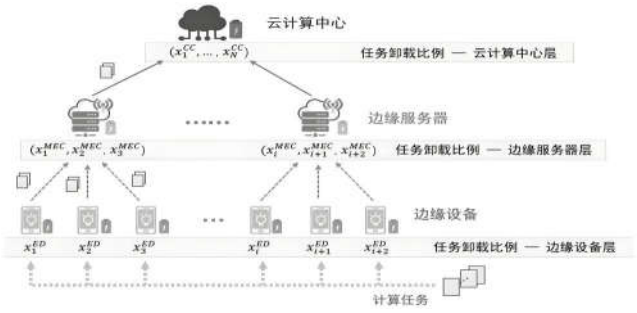


**图1 边缘计算结构架构图**

### 2.3 动态防御理论

动态防御理论摒弃传统静态防御被动等待攻击的模式，主动出击，通过不断改变系统的网络配置、服务状态等，增加攻击者的攻击难度与成本。比如，采用动态IP地址变换技术，定期或在检测到异常时更换系统的IP地址，使攻击者难以锁定目标，之前扫描到的漏洞信息也因IP变更而失效。伪装服务也是常见手段，模拟虚假服务端口，诱导攻击者访问，消耗其资源并及时告警。动态防御还会根据实时的威胁情报，动态调整防御策略，从

多层次、多角度构建防御体系。相较于传统防御，它能更好地适应复杂多变的网络攻击环境，变被动挨打为主动防御，有效降低系统遭受攻击的风险，提升整体安全防护能力[2]。

## 3 多模态威胁感知模块设计与实现

### 3.1 感知指标确定与传感器选型

明确多模态威胁感知指标是模块设计的基础。网络流量层面，确定流入流出带宽、连接数峰值、异常流量占比等指标，监测网络活动。系统行为方面，关注进程创建频率、文件读写异常次数、系统资源使用率突变等，察觉内部异常。

依据指标特性选型传感器。监测网络流量时，采用能线速监测、精确解析流量信息的高精度传感器；监测系统行为，选用可嵌入操作系统内核、实时捕获操作且对性能影响小的轻量级系统探针，确保全面、准确收集威胁感知数据，同时不干扰边缘计算正常运行。

### 3.2 多模态数据融合算法

多模态数据来源、格式与维度不同，需有效融合算法整合。先采用特征级融合算法，从网络流量、系统行为等原始数据中提取特征，拼接成高维特征集。

再利用基于深度学习的多模态神经网络进行融合。将特征集输入网络，通过隐藏层挖掘数据潜在关联，借助大量标注样本训练优化，判断数据是否存在威胁[3]。

为提升效率与鲁棒性，引入注意力机制，使模型自动聚焦关键数据特征，增强对重要信息的敏感度。该方法有效解决数据冲突与冗余问题，大幅提高威胁识别的准确率。

### 3.3 威胁识别与预警机制

构建威胁识别模型是该环节的核心。利用训练好的多模态数据融合模型，对实时融合数据进行分析判断。当模型输出结果超过预设的威胁阈值时，判定为存在安全威胁。

预警机制则确保及时通知管理人员。一旦威胁被识别，系统立即启动预警流程，通过多种渠道发出警报。一方面，在边缘控制器本地界面显示醒目的警告信息，直观呈现威胁类型、发生时间与位置等关键信息；另一方面，向远程管理中心发送预警消息，支持短信、邮件推送，以便管理人员及时响应。同时，系统自动记录威胁相关数据，包括威胁发生前后的多模态感知数据，为后续安全事件分析与溯源提供依据，实现对安全威胁的快速发现、及时预警与有效记录，保障边缘计算环境安全。

## 4 边缘控制器动态防御策略设计

### 4.1 防御策略制定原则

防御策略制定需紧密围绕威胁类型与系统资源状况。面对不同类型的威胁，如DDoS攻击、恶意软件入侵，要采取针对性措施。对于DDoS攻击，重点在于流量清洗与带宽限制；恶意软件入侵则需强化文件检测与隔离机制。同时，考虑边缘控制器资源有限，策略应避免过度占用计算、存储和网络资源，防止影响正常业务运行。比如，在检测算法选择上，优先采用轻量级、高效的算法，平衡安全防护与系统性能。此外，还需遵循及时性原则，当威胁出现时，能迅速触发相应策略，最大程度降低损失；持续性原则也不可或缺，确保防御策略能随威胁的发展和变化持续生效，保障系统长期安全稳定[4]。

### 4.2 动态防御技术实现

动态防御技术通过不断改变系统配置和运行状态，迷惑攻击者，增加攻击难度。IP地址动态变换是常见手段，利用特定算法按一定周期随机更换边缘控制器的IP地址，使攻击者难以锁定目标，中断其攻击连接。端口动态切换则根据业务需求和安全状况，动态开放或关闭端口，减少端口暴露时间，降低被扫描和攻击的风险。伪装服务技术同样关键，通过模拟虚假服务，诱导攻击者访问，收集其攻击特征和行为模式，同时保护真实服务不受侵害。在实现这些技术时，要确保与边缘计算环境的兼容性，通过开发适配边缘控制器硬件和软件环境的工具和模块，保障动态防御技术稳定运行。

### 4.3 防御效果评估方法

构建科学的防御效果评估方法对衡量系统安全性至关重要。从攻击检测率、误报率、漏报率等维度入手，攻击检测率反映系统准确识别攻击的能力，通过统计检测到的真实攻击次数与实际发生攻击次数的比例来计算。误报率体现系统错误报警的情况，计算误报次数与总报警次数的比例，误报率过高会干扰安全运维人员判断。漏报率则衡量系统未能检测到攻击的概率，漏报会使系统面临潜在风险。除这些指标外，还需评估系统性能影响，如防御策略执行后，边缘控制器的计算延迟、吞吐量变化等。采用模拟攻击测试、实际场景监测等方式，定期收集数据，运用数据分析工具进行深入分析，为防御策略优化提供依据。

## 5 系统集成与验证

### 5.1 系统集成方案设计

系统集成旨在将多模态威胁感知模块、边缘控制器动态防御模块与边缘计算基础设施有机融合。首先，梳理各模块间的数据交互关系和接口需求，设计统一的数据格式与通信协议，确保感知数据能顺畅传输至防御模块，防御指令也能准确下达至边缘计算节点。考虑到

边缘计算环境的多样性，采用模块化、可扩展的架构设计，使系统能适配不同硬件设备和网络拓扑[5]。针对资源受限的边缘节点，优化系统部署方案，合理分配计算、存储和网络资源，避免资源过载。同时，建立系统监控与管理平台，实时掌握各模块运行状态，便于集中管理与维护，保障系统稳定运行。

5.2 实验室模拟验证

实验室模拟验证为系统上线前的关键测试环节。模拟多种复杂网络环境，如不同带宽、延迟和丢包率的网络，以及包含常见攻击手段（如DDoS攻击、SQL注入等）的恶意网络场景。在模拟环境中部署系统，对多模态威胁感知模块进行测试，验证其能否准确捕获各类威胁信号，评估数据融合算法的准确性和时效性。针对动态防御模块，检验防御策略能否及时响应威胁，验证防御技术的有效性，如动态IP地址变换是否成功规避攻击，伪装服务是否能迷惑攻击者。记录测试过程中的各项指标，如威胁检测率、误报率、防御响应时间等，与预期目标对比分析，查找系统存在的漏洞和不足，为后续优化提供依据。

5.3 实际场景应用测试

实际场景应用测试是对系统实战能力的检验。选取工业互联网、智能安防等典型边缘计算应用场景，在真实业务环境中部署系统。持续监测系统运行状况，收集实际产生的威胁数据和业务性能指标。观察系统在应对真实威胁时的表现，例如在工业生产场景中，面对针对设备控制指令的篡改攻击，系统能否及时感知并采取有效防御措施，保障生产安全。根据实际测试结果，进一步优化系统参数和策略。针对实际场景中发现的新问题，如与现有业务系统兼容性问题、特定场景下的性能瓶颈等，进行针对性改进，不断完善系统，使其更好地适应复杂多变的实际应用环境。

## 6 结语

本研究成功构建多模态威胁感知驱动的边缘控制器动态防御系统，融合多模态感知技术与动态防御策略，有效提升边缘计算安全防护能力。通过确定感知指标、设计融合算法精准识别威胁，基于原则制定策略并实现动态防御技术，经模拟验证与实际测试，系统性能良好。然而，研究仍存不足。面对新型复杂攻击，威胁识别准确性和防御及时性有待提升；系统在大规模边缘节点部署时，资源优化配置需进一步研究。未来，可引入人工智能技术优化算法，探索更高效资源管理策略，持续完善系统，为边缘计算安全提供更有力支持，推动其在各领域安全稳定应用。

## 参考文献

[1]李小明, 张悦. 多模态数据融合技术在网络安全态势感知中的应用[J]. 信息安全学报, 2023, 38(4): 23-32.

[2]赵强, 刘慧. 边缘计算安全架构与关键技术研究[J]. 计算机工程与应用, 2022, 58(18): 1-8.

[3]王芳, 陈宇. 动态防御技术在工业互联网安全中的应用与挑战[J]. 工业安全与环保, 2021, 47(9): 45-49.

[4]刘阳, 孙宇. 基于人工智能的网络威胁检测算法优化研究[J]. 智能系统学报, 2024, 19(3): 567-575.

[5]张峰, 王丽. 边缘计算环境下的资源调度与安全协同策略[J]. 通信学报, 2023, 44(7): 112-122.