文章类型：论文|刊号（ISSN）：2972-4236(P) / 2972-4244(O)

基于 AI Agent 协同的边缘物联网设备入侵检测机制

高偲
广州软件学院
DOI:10.32629/acair.v3i4.17935

[摘　要] 在物联网不断扩展应用的情况下,网络安全风险也越来越严重。入侵检测技术属于物联网安全体系的重要组成,对识别恶意行为、抵御潜在威胁起到了非常重要的作用。本文提出了一种以AI Agent协同为基础的边缘物联网设备入侵检测机制,利用多层次的数据特征提取、异常检测判断、Agent协同决策聚合来实现对边缘设备网络行为的实时监测和威胁识别；系统采用分层架构处理数据、优化Agent间的通信共享信息、动态入侵检测流程加强对于异常行为的响应能力,提高边缘物联网设备整体安全防护效率和智能化水平,给物联网安全防护提供可扩展、实时、协同高效的解决方案。
[关键词] 边缘物联网；AI Agent协同；入侵检测
中图分类号：TN934.85　文献标识码：A

Intrusion detection mechanism for edge IoT devices based on AI Agent collaboration

Cai Gao
GUANGZHOU UNIVERSITY OF SOFTWARE

[Abstract] With the continuous expansion and application of the Internet of Things, network security risks are becoming increasingly serious. Intrusion detection technology is an important component of the Internet of Things security system, playing a crucial role in identifying malicious behavior and resisting potential threats. This article proposes an edge IoT device intrusion detection mechanism based on AI Agent collaboration, which utilizes multi-level data feature extraction, anomaly detection and judgment, and Agent collaborative decision aggregation to achieve real-time monitoring and threat recognition of edge device network behavior; The system adopts a layered architecture to process data, optimize communication and information sharing between agents, and strengthen the response capability to abnormal behavior through dynamic intrusion detection processes. It improves the overall security protection efficiency and intelligence level of edge IoT devices, providing scalable, real-time, collaborative and efficient solutions for IoT security protection.
[Key words] Edge Internet of Things; AI Agent Collaboration; Intrusion Detection

引言

物联网(Internet of Things,简称IoT)技术的迅猛发展与广泛使用,使人们的生活、工作方式发生了很大的改变。但是,由于IoT设备的种类繁多、异构性强、部署环境复杂多变,它所面临的安全风险和挑战也日益突出。近几年来,由于物联网的恶意攻击和入侵事件时有发生,对物联网系统的正常运转以及数据安全造成了严重威胁。为了提高边缘IoT设备的安全防护能力,AI Agent协同机制渐渐引起人们的注意,它利用各个智能Agent在边缘设备之间做信息感知、共享、协作决策,从而达到对异常行为的快速识别和响应。该种协同方式可以充分利用分布式计算资源,提高入侵检测的实时性、准确性。

1 边缘物联网设备与入侵检测的定义与特点

1.1边缘物联网设备的定义与特点

边缘物联网设备是指在网络边缘部署,可以独立处理数据并与中心服务器协同工作的智能终端或者节点,其主要目的就是把计算、存储和分析的能力下沉到数据源头,从而减轻中心服务器的负载、降低延迟、提高系统响应速度。此类设备一般为边缘网关、智能传感器、微型处理器、嵌入式终端,具备异构性强、分布广、实时性高、自适应能力突出的特点。它们不仅可以对采集到的海量数据进行初步的处理和筛选,而且可以对本地分析做出快速的决策,并在工业自动化、智慧交通、智能家居、医疗监测等场景中起到重要的作用。边缘物联网设备依靠分布式计算和协同机制,提升了系统可扩展性以及鲁棒性,使得整个IoT生态系统在碰到复杂环境或者突发事件的时候,依然可以保持高效稳定的运转。

1.2入侵检测的定义与特点

入侵检测就是对网络流量、设备行为、系统日志等多源信息进行实时监测、分析、评价,从而识别非法访问、异常行为、潜在攻击的一种安全防护技术。其主要特点涵盖实时性、智能化、自适应性：实时性是指能够迅速捕捉到异常事件并作出及时的反应；智能化是指使用机器学习或者AI算法来识别和预测行为模式；自适应性是指系统能够根据网络环境及威胁的演变来调整检测策略。入侵检测不仅要即时发现攻击,还要对复杂的、隐蔽的威胁进行长期监控和趋势分析。随着IoT环境规模的增大、设备种类的增多以及边缘计算的出现,入侵检测技术要具有高可扩展性、协同决策能力和低资源消耗等特点,保证物联网系统的安全稳定。

2 基于AI Agent协同的边缘物联网设备入侵检测方法

2.1数据特征提取方法

物联网边缘设备异常检测当中,特征提取属于多源观测建模的重要部分。在基于AI Agent协同的机制里,每一个Agent都可以独立地对来自传感器、网关、终端设备的流量模式、设备状态、协议交互特征等多方面数据进行采集和分析。经过本地预处理和降维之后,Agent不仅可以去掉冗余信息,还能找出潜在的行为模式和异常信号;然后再借助跨Agent的信息共享以及特征融合,形成全局感知的高维特征空间。该方法重视分布式处理和协同优化,既考虑实时性又考虑准确性。

2.2异常检测判别方法

异常检测判别是用提取出的特征对设备行为进行智能分析、分类的主要步骤。AI Agent使用机器学习、深度学习、强化学习等算法,从历史行为模式中学习正常和异常的分布特征,并用动态阈值或者概率模型进行实时判断。各个Agent独立完成初步判断,再通过协同通信对判别结果进行校正和优化,从而降低误报率和漏报率。此方法既可以识别出多种攻击类型,包括DoS攻击、恶意访问、数据篡改等,还可以适应设备数量增加和网络拓扑变化的情况。

2.3协同决策聚合方法

协同决策聚合是把各个Agent的检测结果整合为全局决策的关键步骤。每一个Agent依据自身的观测以及判别结果来形成局部的决策信息,然后借助通信协议同附近的Agent展开交流。系统利用加权投票、置信度评价或者图神经网络聚合的方法,把多源决策融合成最终的入侵判定,以此来充分发挥分布式智慧的作用,从而达到对异常行为进行全局感知和精确识别的目的。协同决策聚合可以动态调整Agent的权重和决策策略,使边缘物联网设备在复杂、动态的网络环境中仍然能够保持高效的、可靠的入侵检测能力。

3 基于AI Agent协同的边缘物联网入侵检测机制设计

3.1系统总体架构设计,分层处理数据

“万物互联”时代产生的海量数据使我们不得不面对数据处理的实时性、智能性、安全性与隐私性问题。根据国际数据公司(IDC)分析,到2025年,全球数据总量达到213.56ZB,而目前的集中式处理方式已经不能满足海量数据传输的要求了。边缘计算应运而生,它把计算资源下沉到网络边缘,把数据存储、分析、处理的任务分摊到接近数据源的节点上,从而减少延迟、加快系统响应速度。在此情况下,基于AI Agent协同的边缘物联网入侵检测机制采用三层架构设计,把整个系统分成感知层、边缘处理层和管理控制层。感知层采集设备状态、流量数据、环境信息；边缘处理层用分布式Agent做数据预处理、特征提取、初步异常判断；管理控制层把各个Agent的决策整合起来,形成全局安全策略和响应措施。每一层既独立运行又相互配合,使数据在局部处理和全局监控之间高效流通。在实际的设计过程中,系统架构注重冗余和负载均衡,边缘节点可用动态调度策略分配计算任务,减少单点瓶颈。Agent在各个节点上独立处理本地数据,并对异常行为做初步标注;边缘节点把经过处理的上传到管理控制层,形成全局的威胁感知视图。整个架构既可以对实时数据进行处理,也可以采用分层的方式控制数据的传输频率和粒度。

3.2 Agent协同通信设计,优化信息共享

在复杂的边缘物联网环境下,单个节点的安全判断受到观测范围、计算能力和网络拓扑的局限,而信息孤岛效应会使得威胁识别出现延迟或者误判,进而影响到整个系统的防护能力。因此,以AI Agent协同为基础的通信设计,试图冲破这样的限制,依靠多Agent之间高效的互相交流,达成分布式感知、协同分析以及智能决策。每个Agent在本地完成数据采集、特征提取、异常判断之后,会把重要的特征、局部威胁评分、置信度信息、可执行策略等用安全、低延迟的通信协议与邻近的Agent或者管理控制层共享,从而形成跨节点的全局威胁感知。为保证信息的可靠、实时和容错,在系统中可采用异步消息队列、事件驱动通信、动态路由、优先级调度等技术来保证信息在节点间流动时既高效又安全,并能适应网络波动以及节点负载变化。在实际的应用中,Agent协同通信不仅要保证数据的完整传输,还要结合上下文信息做智能筛选、冗余去重、优先级排序,从而达到最大化信息利用效率、降低带宽消耗、减少延迟的目的。另外,每一个Agent都能够根据自身的计算负载、网络状况、节点状态等来改变自身的通信频率和数据量,并对于接收到的其它Agent的信息加以融合评价。该机制可以在节点异常、网络抖动、部分设备失效的时候保证系统的稳定,依靠集体智慧来提高整个检测的精度。

3.3入侵检测流程设计,强化实时响应

入侵检测流程是保证边缘物联网安全的关键环节,它的目的不仅是发现威胁,还要迅速做出响应并采取有效的防护措施。利用AI Agent协同的设计方法,可把整个流程分成数据采集、特征处理、异常判断、协同聚合和全局响应这五个步骤,从而形成端到端闭环式的安全防护机制。感知层Agent对本地设备状态、通信流量、协议交互、环境参数进行持续采集,经过本地预处理、特征提取、标准化之后,把多源信息转化成可以分析的数据向

量。之后边缘处理层Agent利用机器学习、深度学习、图神经网络等算法进行数据的异常检测,生成局部威胁评分,并结合历史行为模式、上下文信息做动态调整,提高检测的精准度、适应性。各个Agent把局部的判别结果以及置信度通过安全、高效的协同通信机制上传到管理控制层,从而达成跨节点的信息共享与整合。聚合阶段系统用加权投票、置信度融合、策略优化的方式,对多Agent的判别结果做全局评价,得到完整的威胁态势图,实时调整安全策略。根据最后判定,管理控制层可以触发流量限速、策略更新或者报警通知等防护措施,并将反馈信息传给边缘Agent。该流程既加强了实时响应能力,也兼顾了系统自适应性。

4 系统性能分析与应用前景

基于AI Agent协同的边缘物联网入侵检测机制具有明显的优势。首先,分布式处理、协同决策大大减小了单点计算的压力,使得系统在处理海量数据流的时候仍然可以保持高吞吐量；其次,多Agent之间信息共享、动态聚合的策略提高了检测精度、异常识别的可靠性,即使节点出现故障或者网络出现波动,整个系统仍然可以保持稳定运行。另外,边缘节点预处理和本地判别机制降低了中心传输的数据量,提高了带宽利用率。实验结果表明,该机制在多种入侵场景下既可以取得较好的召回率、误报率,也可以根据网络规模和设备数量的增加来灵活地调整Agent的数量和协作策略。

从应用前景来看,基于AI Agent协同的边缘物联网入侵检测机制有广泛的推广价值。其既能适应智慧城市、智能家居、医疗监测等复杂的场景,也可以同云计算、边缘AI、5G网络等新的技术相结合,组成端-边-云三层安全架构。未来,随着IoT设备数量激增与应用场景多样化,该机制可以给实时、智能的安全防护提供支持,还可以根据不同的场景动态调整策略。另外,其分布式、协作式的架构模式为构建可持续、高鲁棒性的物联网安全生态奠定了良好的基础。

5 结语

由于边缘物联网设备的大量应用,所以安全防护的需求越来越强烈。以AI Agent协同为入侵检测机制,依靠多个Agent对数据特征进行提取、对异常做出判断、进行决策聚合,从而达到对边缘设备网络行为的高效监控以及威胁识别的目的。系统采用分层结构来处理数据,并且使用改进的Agent之间的信息交换机制提高信息共享能力,使得入侵检测流程可以即时响应异常事件,进而改善整体安全防护能力。

[参考文献]

[1]郭志林.面向物联网环境的入侵检测与防御系统设计[J].信息记录材料,2025,26(08):205-207.

[2]龚岩.边缘计算在物联网中的应用研究[J].信息记录材料,2025,26(12):158-160.

[3]张婷.基于人工智能的物联网边缘设备异常检测方法研究[J].网络安全和信息化,2025,(11):55-57.

[4]吕正林,段炼,朱龙,等.边云协同环境下智能家居物联网入侵检测方法[J].移动通信,2022,46(05):106-112.

[5]邓淼磊,阚雨培,孙川川,等.基于深度学习的网络入侵检测系统综述[J].计算机应用,2025,45(2):453-466.

[6]方栋梁,刘圃卓,秦川,等.工业控制系统协议安全综述[J].计算机研究与发展,2022,59(5):978-993.

作者简介：

高偲(1980--),男,汉族,湖南衡阳人,助教,硕士研究生,广州软件学院,研究方向：物联网,人工智能。