基于博弈优化边缘学习的物联网入侵检测研究

梁浩然[1]，伍军[1]，赵程程[1,2]，李建华[1]
（1. 上海交通大学，上海 200240；2. 室兰工业大学，日本 室兰 050-8585）

摘　要：随着 5G 的商用和 6G 开始布局，海量物联网设备正在加速接入互联网，为新一代信息物理融合系统提供决策数据。物联网设备的高度异构及分布式特性使得物联网面临复杂威胁，这些威胁可使信息物理融合系统的关键决策失效。传统技术难以在保护节点隐私的前提下进行入侵检测且容易形成单点故障，同时缺乏协同入侵检测激励机制。因此，基于博弈优化边缘学习，研究了面向物联网的入侵检测系统。基于联邦学习在网络边缘构建了分布式隐私保护物联网入侵检测框架。在此基础上，基于多主多从博弈优化边缘学习过程，激励可信的入侵检测服务器及边缘设备参与边缘联邦学习。仿真实验证明了所提出的联网入侵检测系统的安全性和有效性。

关键词：物联网；边缘学习；博弈论；入侵检测
中图分类号：TN915.08
文献标识码：A
doi: 10.11959/j.issn.2096-3750.2021.00226

Leveraging edge learning and game theory for intrusion detection in Internet of things

LIANG Haoran[1], WU Jun[1], ZHAO Chengcheng[1,2], LI Jianhua[1]
1. Shanghai Jiao Tong University, Shanghai 200240, China
2. Muroran Institute of Technology, Muroran 050-8585, Japan

Abstract: With the commercialization of 5G and the development of 6G, more and more Internet of things (IoT) devices are linked to the novel cyber-physical system (CPS) to support intelligent decision making. However, the highly decentralized and heterogeneous IoT devices face potential threats that may mislead the CPS. Traditional intrusion detection solutions cannot protect the privacy of IoT devices, and they have to deal with the single point of failure, which prevents these solutions from being deploying in IoT scenarios. The edge learning and game theory based intrusion detection for IoT was proposed. Firstly, an edge learning based intrusion detection framework was proposed to detect potential threats in IoT. Moreover, a multi-leader multi-follower game was employed to motivate trusted parameter servers and edge devices to participate in the edge learning process. Experiments and evaluations show the security and effectiveness of the proposed intrusion detection framework.

Key words: Internet of things, edge learning, game theory, intrusion detection

1　引言

近年来，以低时延、超大网络容量为特征的 5G 极大促进了物联网的发展[1]。通过连接泛在异构传感器、工控设备、家用电器等物理实体，物联网可以在视觉、听觉、嗅觉、触觉等层面对真实物理世界进行感知。并且通过连接物理世界与信息世界，物联网可以为信息物理融合系统提供丰富的智慧决策数据。越来越多的智慧边缘设备在 5G 的助推下接入互联网，以万物互联互通为愿景的物联网正

收稿日期：2021−01−07；**修回日期：**2021−02−09
通信作者：伍军，junwuhn@sjtu.edu.cn
基金项目：国家自然科学基金资助项目（No.U20B2048，No.61972255）
Foundation Items: The National Natural Science Foundation of China (No.U20B2048, No.61972255)

在通过电子医疗、智能制造、智慧城市、数字家庭等领域发力重构渗透现代生活[2-3]。物联网正在从方方面面改变人们的生活。

高度分布式、泛在互联的物联网设备不仅能延展信息物理融合系统的感知能力，还能连接物理世界与信息世界。这使得攻击者可以通过网络攻击物联网设备对现实物理世界进行破坏，全球数以亿计的物联网设备成为了攻击者的新目标。即攻击者不仅可以通过入侵物联网设备获取用户的生产、生活隐私数据，还可能通过控制物联网设备对国家电网、核设施等关键基础设施进行破坏。例如，2010 年，攻击者通过入侵伊朗铀浓缩工厂的控制器干扰其离心机的正常运行，损坏了近千台离心机，使得伊朗被迫推迟其核计划。2015 年，攻击者通过入侵乌克兰电力系统的断路器，强制电网断电，造成了乌克兰大停电事件。2016 年，世界领先的内容分发网络（CDN, content delivery network）服务商 Akamai 称攻击者利用 Spike DDoS 工具包结合物联网设备构成的僵尸网络发起了规模为 517 Gbit/s 的 DDoS 攻击。2017 年，Jason Staggs 博士公布了面向风力发电机的入侵方案，该方案可造成风力发电机中涡轮机瘫痪，并对风力电厂进行恶意勒索。2019 年，亚马逊旗下 Ring 摄像头被攻击者大规模入侵，造成用户生活隐私泄露。

随着海量物联网设备伴随 5G 接入互联网，面向物联网设备的攻击也开始呈现爆发式增长。工业界和学术界正投入更多努力进行物联网入侵检测研究，以对潜在威胁进行感知。异构分布式的物联网设备不仅为信息物理融合系统提供了去中心的控制、感知能力，更为物联网自身的入侵检测带来了巨大挑战。具体来说，目前有关物联网入侵检测的研究主要涵盖两种模式：以物联网设备为中心的入侵检测研究和以协作为中心的入侵检测研究。在以物联网设备为中心的入侵检测研究中，研究者侧重于分析物联网设备的潜在威胁，并结合统计分析和机器学习等技术设计面向某种具体攻击手段等的入侵检测算法。例如，Sedjelmaci 等[4]根据物联网中拒绝服务（DoS, denial of service）攻击行为、虚假信息交换攻击行为、虚假警报生成攻击行为进行规则建模，并在此基础上提出了一种轻量级的、基于规则的入侵检测算法 ELIDV，该算法具有高检测率、低假阳率的特性。然而，以物联网设备为中心的入侵检测研究中的威胁感知模型往往基于某个物联网设备中的入侵样本建模、训练而来，其入侵检测能力具有局限性，无法精确感知在其他同类物联网设备中出现过的入侵方法，因此，以物联网设备为中心的入侵检测难以感知物联网中的潜在复杂威胁。近年来，物联网设备在边缘节点（如网关等）的协助下可实现高度的互联互通。因此，以协作为中心的入侵检测成为了研究者们的研究热点。例如，在 Albers 等[5]的研究中，多个物联网设备可构成社区，且各物联网节点中的本地入侵检测系统可通过交换简单网络管理协议（SNMP, simple network management protocol）数据进行协作，以提高社区中各本地入侵检测系统的检测能力。虽然利用社区中的物联网节点进行相互协作可以扩充各物联网节点本地入侵检测系统的训练样本、增强本地入侵检测系统感知潜在未知威胁的能力，但是由于物联网节点构成的社区中入侵样本数量受限且社区中通过点对点通信模式交换入侵样本的方式过于缓慢，以物联网节点间协作为中心的入侵检测方案难以应对物联网中海量的潜在威胁。研究者们将目光投向了具有海量数据处理能力的云计算技术。利用云计算，各物联网设备中的样本可以上传至云中心，并利用云中心强大的计算能力结合机器学习技术构建机器学习模型[6]。

虽然基于云计算的机器学习算法可以通过收集海量物联网设备入侵样本训练出具有泛在检测能力的入侵检测模型，但是，3 个因素阻碍了这类入侵检测系统的发展。首先，海量物联网设备数据上传处理需要占用大量计算、通信、存储资源，云中心难以高效处理这些数据。其次，物联网设备的入侵样本包含大量隐私信息，对隐私信息的保护需求阻碍了物联网设备参与入侵检测模型训练。最后，有关物联网的入侵检测模型统一在单一的云中心进行训练容易形成单点故障，当云中心被攻击者控制时，物联网设备将难以获得有效的入侵检测模型。

联邦学习是一种新型边缘学习技术。联邦学习能够在不泄露设备隐私的前提下联合多个设备进行分布式边缘训练以获取机器学习模型。边缘计算技术的兴起使得网关等可信边缘节点可以在管理物联网设备的同时为云中心进行数据预处理，因此，云计算、边缘计算及联邦学习的结合有潜力在保护物联网设备隐私的条件下训练出面向物联网的可靠入侵检测模型。虽然联邦学习可以在保护物联网设备隐私的前提下训练有效的入侵检测模型，

但是传统静态联邦学习中只有一个参数服务器通过聚合各边缘设备的本地入侵检测模型生成面向物联网的全局入侵检测模型，存在单点故障威胁。为了在保护物联网设备隐私与消除单点故障的前提下，为物联网训练可靠的入侵检测模型，本文提出基于博弈优化边缘学习的物联网入侵检测。具体来说，所提出的物联网入侵检测框架同时利用多个云中心充当边缘学习参数聚合服务器，以消除基于云计算的入侵检测方案所面临的单点故障威胁。同时，本文对边缘学习中入侵检测服务器与边缘设备的效用进行建模，通过博弈论激励可信系统实体参与构建分布式物联网入侵检测系统。本文的创新点总结如下：

1) 本文提出了基于博弈优化边缘学习的物联网入侵检测框架，利用边缘智能为网络边缘的高分布式物联网提供威胁感知能力；

2) 本文构建了基于联邦学习的入侵检测机制，在消除单点故障及保护物联网设备隐私的基础上为物联网协同训练入侵检测模型；

3) 本文面向联邦学习建立了多主多从博弈模型，通过动态调整入侵样本定价策略及入侵样本分配策略，激励可信边缘设备及入侵检测服务器参与入侵检测模型分布式训练过程。

2　国内外研究现状与分析

2.1　物联网入侵检测技术

在以物联网设备为中心的入侵研究中，学者们综合利用机器学习等技术在物联网设备本地部署入侵检测装置。文献[7]提出智能车间的数据协作共享机制，并利用协作共享获得的车流速度、车辆密度等数据对女巫攻击及错误警报生成攻击进行统计分析，实验表明新提出的数据协作共享机制可以实现对女巫攻击及错误警报生成攻击进行低开销感知。文献[8]利用报文通信周期间隔对智能车状态进行分析建模，并通过观测报文通信周期间隔异常感知智能车所面临的潜在威胁，但是该模型无法感知攻击者对报文的修改行为。文献[9]面向 DoS 攻击、指令注入攻击与恶意软件 3 种威胁提出了基于循环神经网络与长短期记忆网络的智能车联网威胁感知机制，同时还提出了一种基于云计算的计算资源迁移模型，以在云计算中心完成对智能车威胁的感知。为感知恶意智能车的 Bus-Off 攻击，文献[10]通过提取智能车电子控制单元分布在时域和频域的 60 种信号对电子控制单元进行识别，并利用支持向量机（SVM, support vector machine）和径向基核函数构造可识别正常电子控制单元的分类器，该分类器基于分类分值对电子控制单元进行分类，如果分类分值低于目标阈值则判定该电子控制单元为恶意电子控制单元。然而这种威胁感知方法只能识别面向物理层的攻击，无法感知来自应用层的威胁。文献[11]将控制器域网（CAN, controller area network）数据帧中的 CAN ID 转换为图像，同时利用生成对抗网络构建基于图像判别的智能车威胁感知模型，该模型能够准确识别 DoS 攻击、Fuzzy 攻击以及 Gear 攻击，但是对于正常故障引发的 CAN ID 分布异常容易误判为智能车遭遇潜在威胁。文献[12]针对智能车联网威胁感知计算资源不对称问题，提出基于车辆边缘计算的低时延威胁感知机制，利用周边可信车辆协同计算进行威胁感知智能决策，解决本地计算资源不足与云计算时延较高的难题。文献[13]提出一种可以感知重放攻击和 Fuzzy 攻击的威胁感知模型，该模型使用了 Bloom 过滤器来节省威胁感知所需的存储资源。然而，以物联网设备为中心的入侵检测样本获取具有较强的局限性，难以应对物联网泛在复杂威胁。文献[14]为智能车提出了一种基于博弈论的威胁感知算法，新提出的算法可以预测被监控的车辆是否会遭遇 DoS 攻击。针对 CAN ID 的独特熵特征，文献[15]首次提出了基于熵的面向智能车联网威胁感知模型，该模型对 DoS 攻击敏感，但是无法识别数量较少的恶意消息注入。现有的基于机器学习的物联网入侵检测方案需要大量的标记数据才能完成模型更新，文献[16]面向物联网提出一种基于伪标签与迁移学习的入侵检测机制，在拥有少量标记数据的情况下实现对新型攻击的感知。车内网络 CAN 总线具有协同车内电子控制单元的作用，缺乏安全防护机制的 CAN 总线容易受到攻击者的入侵进而影响车辆行驶安全，文献[17]基于循环卷积神经网络提出了面向车内 CAN 总线的入侵检测机制，提升了车内电子控制单元协同安全。

为了扩充入侵检测样本获取的途径，研究者们将目光转向了以协作为中心的入侵检测。具体来说，以协作为中心的物联网入侵检测研究侧重于构建物联网设备间的协作方案以促进物联网设备间的入侵样本交流。文献[18]提出了一种基于层次化的入侵检测方案，在该方案中，系统中的节点将自

身收集的入侵样本逐层传递到更上层的系统节点中，越靠近顶层的系统节点拥有的入侵样本越多，进而可以利用顶层系统节点生成具有感知复杂攻击能力的入侵检测模型。文献[19]提出基于 mobile agent 的入侵检测方案，其中每个 mobile agent 具有感知、决策等不同的功能，该方案中的系统节点可以依据自身资源状况运行具有不同功能的 mobile agent，同时根据系统节点间的相互协作来完成入侵检测。文献[9]提出一种基于云计算的安全方案，该方案利用边缘计算节点收集、预处理物联网设备中的入侵样本，同时利用边缘计算节点将处理后的入侵检测样本上传至云中心，并由云中心根据这些入侵样本训练具有泛在检测能力的入侵检测模型。协作式入侵检测虽然能解决以物联网设备为中心的入侵检测难以应对的复杂入侵检测的问题，但是协作式入侵检测往往需要传播物联网设备中的入侵检测样本，而物联网设备往往由于隐私保护的需求不愿意共享传播这些高度敏感的入侵检测样本。因此，如何面向物联网构建入侵检测系统仍然是一个开放性问题。

2.2 边缘学习与博弈论

随着边缘设备计算资源的提升，越来越多的机器学习算法被部署于边缘设备上，以低时延的方式在网络边缘提供智能服务。联邦学习是一种新型的边缘学习模型，近来，几种激励机制已被提出，激励联邦学习客户端参加耗费资源的学习任务。文献[20]将 Stackelberg 博弈与深度强化学习相结合，以改善联邦学习客户端提供的数据集大小，其中联邦学习系统中的参数服务器可以生成没有任何先验信息的最佳策略来给各联邦学习客户端数据集进行定价。文献[21]提出了一种基于信誉的可靠联邦学习，并利用契约理论激励具有高质量数据集的移动设备参与联邦学习过程。联邦学习的质量不仅受本地学习数据的影响，还受学习客户端数量的影响。文献[22]提出了一种激励机制，以确保有足够的合格联邦学习客户端为无线学习任务提供服务。以上关于联邦学习的激励机制主要集中应对一个参数服务器与多个联邦学习客户端的情况，无法直接应用于多个参数服务器与多个联邦学习客户端构成的边缘学习系统。

3 物联网威胁挑战与入侵检测模型

3.1 物联网安全威胁分析

物联网主要通过传感器对现实物理世界进行感知，并通过网络层将感知的数据传递给应用层以进一步分析处理指导现实世界的生产、生活。因此，物联网的攻击面通常包括感知层攻击面、网络层攻击面及应用层攻击面。感知层攻击面包含物理破坏、无线电干扰等攻击方式。网络层攻击面包括中间人攻击、DoS 攻击等攻击方式。应用层则面临恶意软件欺诈等攻击方式。因此，面向物联网的入侵检测来协助物联网设备感知复杂潜在威胁成为当前的研究热点。

联邦学习是一种新型边缘学习技术。联邦学习能够在不泄露设备隐私的前提下联合多个设备进行分布式边缘学习获取机器学习模型。因此，联邦学习有潜力在保护物联网设备隐私的条件下，允许入侵检测服务商通过向多个物联网设备购买边缘学习服务来训练出可靠的入侵检测模型。虽然经典静态联邦学习能保护边缘设备隐私，但是联邦学习仍面临单点故障威胁，受攻击者操控的参数聚合服务器将使得各物联网设备获取无效的入侵检测模型，进而使物联网设备失去对潜在威胁的感知能力。

3.2 物联网分布式入侵检测系统模型

物联网设备面临震网病毒等潜在异构威胁。本文所提出的物联网分布式入侵检测系统包含多个入侵检测服务器和多个物联网设备。首先，物联网分布式入侵检测系统模型如图 1 所示，边缘设备负责从物联网设备收集入侵样本，并针对入侵检测服务器的定价为不同入侵检测服务器配置不同的入侵样本分配策略。其次，在所提出的物联网分布式入侵检测系统模型中，入侵检测服务器负责入侵检测模型聚合、入侵样本定价、入侵检测模型管理及入侵检测模型分发等。入侵检测服务器可通过对入侵样本进行定价来衡量不同机器学习数据集的价值[23]。入侵样本定价是指入侵检测服务器对某边缘设备中的入侵样本进行价值评估，并定义该边缘设备中入侵检测样本的价格。具体来说，入侵检测服务器通过聚合边缘设备训练的局域物联网入侵检测模型来构建全局物联网入侵检测模型。且入侵检测服务器还能充分利用迁移学习等技术优化边缘联邦学习效率，如入侵检测服务器可针对利用边缘联邦学习对预训练模型进行微调以缩减边缘联邦学习所需轮数，加快获取全局入侵检测模型的速度。在本文提出的物联网分布式入侵检测系统中，多个入侵检测服务器之间从高可信边缘设备获取入侵样本，这些入侵检测服务器通过提高入侵检测

样本定价促使边缘设备参与自己组建的边缘联邦学习过程。同时，各个边缘设备也希望为更可信的入侵检测服务器分配更多的入侵样本以保证及时收到报酬。本文所提出的入侵检测系统不仅能利用边缘联邦学习在保护物联网设备隐私的前提下构建全局的物联网入侵检测模型，还能避免单个入侵检测服务器被入侵者攻击而形成单点故障。

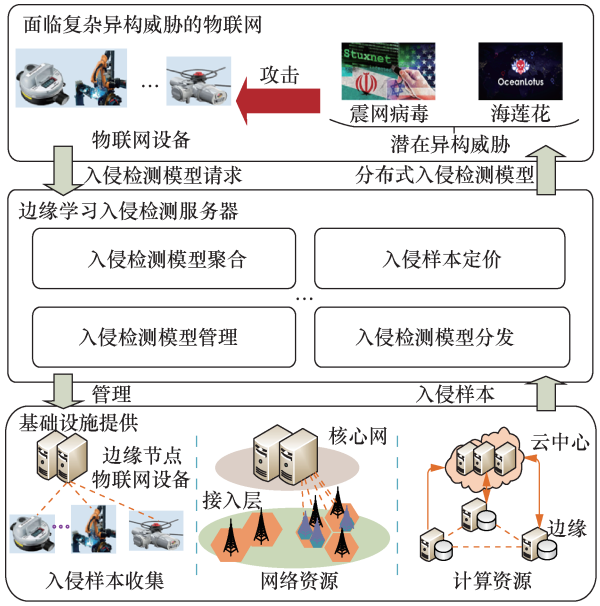

图 1　物联网分布式入侵检测系统模型

4　基于博弈优化边缘学习的物联网入侵检测机制

4.1　入侵检测整体框架设计

博弈优化边缘学习入侵检测框架包括物联网设备层、博弈优化边缘学习层、入侵检测服务层及应用层。物联网设备层由物联网设备及边缘设备构成，边缘设备负责从物联网设备处收集入侵样本，为不同入侵检测服务器制定不同的入侵样本分配策略，并为不同入侵检测服务器训练局域物联网入侵检测模型。入侵检测服务层由各个入侵检测服务器构成，该层与物联网设备层通过博弈优化边缘学习层连接，通过入侵检测服务器构建边缘联邦学习系统，入侵检测服务器对各个边缘设备入侵样本进行定价并对边缘联邦学习系统内各个边缘设备的局域物联网入侵检测模型进行聚合以形成全局入侵检测模型。而应用层利用入侵检测服务器提供的接口，为物联网提供异构入侵检测应用。近年来，博弈论被广泛应用于优化网络边缘资源编排。博弈优化边缘学习层通过博弈论模型为各入侵检测服务器及边缘设备效用进行建模，激励可信的入侵检测服务器及边缘设备参与边缘学习。其中，入侵检测服务器通过对边缘样本进行定价、边缘设备通过为入侵检测服务器配置入侵样本分配策略来提升自身的效用。本文主要符号及其含义如表 1 所示。

表 1　　主要符号及定义

符号	定义
N	入侵检测服务器数量
M	边缘设备数量
$d_{m,n}$	边缘设备 m 分配给入侵检测服务器 n 的入侵样本数量
$p_{m,n}$	入侵检测服务器 n 对边缘设备 m 中入侵样本的定价
f_m	边缘设备 m 的计算资源
ε_m	边缘设备 m 的模型训练精度
$B_{n\_\max}$	入侵检测服务器 n 的最高支出
$d_{m\_\max}$	边缘设备 m 能提供的最大入侵样本数据量

4.2　基于博弈优化边缘联邦学习的入侵检测机制

多主多从联邦学习入侵检测由多个入侵服务器及多个边缘设备构成，利用多主多从博弈对边缘联邦学习过程进行建模。具体来说，首先将边缘客户端建模为多主多从博弈中的跟随者。其次，将入侵检测服务器建模为多主多从博弈中的领导者。领导者通过对入侵样本进行定价最大化自己的效用，同时跟随者根据领导者的定价决定对应的入侵样本分配策略来最大化自己的效用。

4.2.1　边缘设备入侵检测模型的多主多从训练效用建模

在边缘学习过程中，数据量与所获得入侵检测准确率之间的关系呈边际效用递减关系，即入侵检测模型准确率的提升会随着所入侵样本数据量的增长而逐步放缓。假设边缘设备 m 销售给入侵检测服务器 n 的入侵检测样本数量为 $d_{m,n}$，则入侵检测服务器 n 通过购买边缘设备 m 上入侵检测样本所能获得的入侵检测模型准确率可建模为 $1-\beta\cdot \mathrm{e}^{-\gamma_m d_{m,n}}$，$\beta$ 与 γ_m 为关于入侵检测模型准确率的影响因子[20]。

联邦学习边缘设备的时间消耗与计算资源 f_m（CPU 时钟频率）、本地训练要求的精度 ε_m 之间的关系为

$$T_{m,n}(d_{m,n})=\log\left(\frac{1}{\varepsilon_m}\right)\frac{d_{m,n}}{f_m} \tag{1}$$

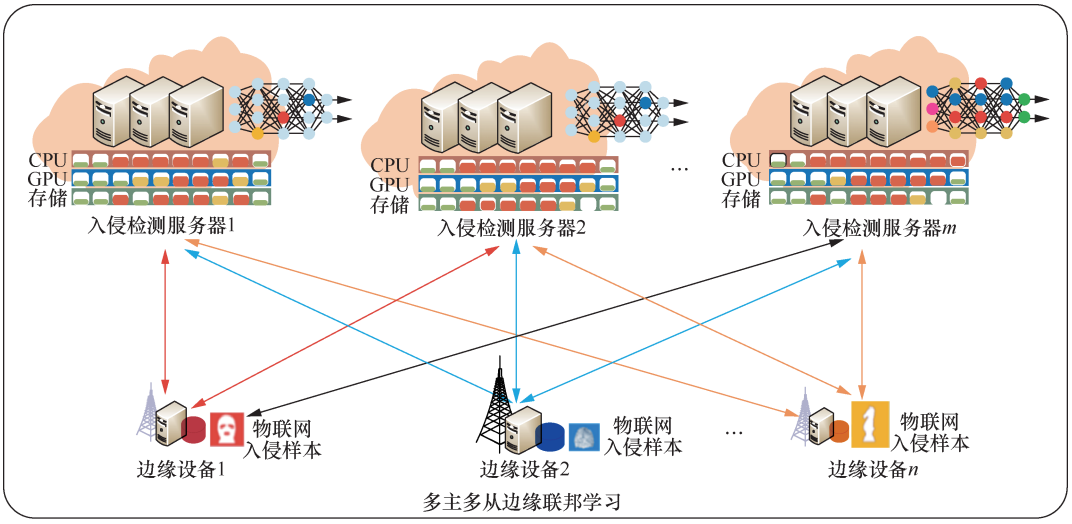

图 2　基于多主多从边缘联邦学习的物联网入侵检测

基于多主多从边缘联邦学习的物联网入侵检测如图 2 所示。

边缘设备的目标为销售更多入侵检测样本，同时降低边缘设备训练模型产生时延对自身利益的负面影响。因此，边缘设备的效用函数可建模为

$$\max U_m(\boldsymbol{d}_m)=\sum_{j=1}^{N}\left(\left(1-\beta\cdot \mathrm{e}^{-\gamma_m d_{m,j}}\right)\cdot p_{m,j}\cdot\omega_j\right)-\sum_{j=1}^{N}\left(\mu_j\cdot\log\left(\frac{1}{\varepsilon_m}\right)\frac{d_{m,j}}{f_m}\right)$$

$$\text{s.t.}\forall j\in N, d_{m,j}\geqslant 0, \sum_{j=1}^{N} d_{m,j}=D_{m\_\max} \tag{2}$$

其中，ω_j 为入侵检测服务器 j 所带来收益的影响因子。此处，ω_j 可以为入侵检测服务器可信度，ω_j 越大说明该服务器越能按时为客户端提供边缘服务器付费，进而放大该入侵检测服务器所产生收益对客户端效用的影响。因此，式(2)第 1 项表示设备 m 为不同的入侵检测服务器提供入侵样本将对自身效用产生不同影响。其中，$\mu_j\geqslant 0$ 为入侵检测服务器 j 相关影响因子。此处，μ_j 可以为与入侵检测服务器可信度成反比的数。μ_j 越大表明该入侵检测服务器越可能不及时对学习服务进行付款，进而放大为该入侵检测服务器进行边缘学习所产生时延对边缘学习客户端的负面影响。因此，式(2)第 2 项表示设备 m 为不同的入侵检测服务器进行模型训练所产生时间消耗对自身效用产生的不同影响。由于服务规模限制入侵检测服务器 n 业务规模动态变化，其需要购买的入侵检测样本总量需要满足 $\sum_{i=1}^{M}\tau_n d_{i,n}=d_{n\_\max}$，$\tau_n$ 表征与业务规模有关的正数。约束条件表明边缘设备由于其总入侵样本数据量有限，因此，最多能共享 $D_{m\_\max}$ 数量的入侵样本数据，同时边缘设备销售的入侵样本数量应大于或等于 0。

4.2.2　服务器端入侵检测的多主多从模型训练效用建模

入侵检测服务器 n 应对入侵样本积极出价，并且在保证尽量低的支出情况下，聚合边缘设备模型参数来获得尽量高的模型精度提升。因此，入侵检测服务器 n 的效用函数可定义为

$$\max U_n(\boldsymbol{p}_n)=\left(1-\beta\cdot \mathrm{e}^{-\alpha_n\sum_{i=1}^{M}\gamma_i d_{i,n}}\right)+\phi_n\cdot\left(\frac{\sum_{i=1}^{M}p_{i,n}}{\sum_{i=1}^{M}\sum_{j=1}^{N}p_{i,j}}\right)-\sum_{i=1}^{M}\sigma_i\cdot\left(1-\beta\cdot \mathrm{e}^{-\gamma_n d_{i,n}}\right)\cdot p_{i,n}$$

$$\text{s.t.}\forall i\in M, p_{i,n}\geqslant 0, \sum_{i=1}^{M} p_{i,n}=B_{n\_\max} \tag{3}$$

其中，$\alpha_n\geqslant 0$ 为所得模型精度影响因子，表示入侵检测服务器无法对所购买的入侵样本进行完全利用。因此，式(3)第 1 项表示入侵检测服务器 n 聚合不同边缘设备获得的入侵检测模型精度提升对自身效用产生的影响。$\phi_n\geqslant 0$ 是关于入侵检测服务器定价高低程度的影响因子，它的值越大，表明该入侵检测服务器将比其他入侵检测服务器更愿意定出更高的价格以争取获得更多入侵样本。因此，式(3)第 2 项表示入侵检测服务器定价积极程度对

自身效用产生的影响。入侵检测服务器对某个边缘设备 i 的支出受 σ_i 影响，$\sigma_i \geqslant 0$ 越大，入侵检测服务器认为针对边缘设备 i 的支出对效用具有更大的负面影响。具体来说，σ_i 可以是与边缘设备 i 可信度成反比的数。因此，式(3)第 3 项表示支出对入侵检测服务器 n 效用的影响。由于边缘客户端数据采集难度不同，边缘设备 m 需要获取的总收益需满足 $\sum_{j=1}^{N}\varsigma_m p_{m,j} = b_{m\_\max}$，$\varsigma_m$ 是反映数据收集难度的正数。其中，约束条件表示入侵检测服务器必须对边缘设备提供的入侵样本提供最低定价为 0，同时入侵检测服务器的总体预算在所有边缘学习客户端都有最佳训练效果时的出价不能高于 $B_{n\_\max}$。

4.3　多主多从边缘入侵检测最优策略训练

4.3.1　交替方向乘子法

假设一个系统中有一个领导者和 N 个跟随者，x_j 是领导者为跟随者 j 提供服务的成本，而领导者的效用函数记为 $B(x_j)$，则领导者的目标是最大化其效用函数，可表示为

$$\max B(x_j) = \sum_{j=1}^{N} b(x_j)$$

$$\text{s.t.} \sum_{j=1}^{N} C_j x_j = D \tag{4}$$

其中，$b(x_j)$ 是关于 x_j 的严格凹函数，x_j 是实数且是一个标量的变量，而 C_j 和 D 这两个固定值都是实数构成的标量。如此，假设当前是第 $k+1$ 次迭代，则领导者可根据如下规则更新 x_j 的值

$$x_j(k+1) = \operatorname{argmax}\left(B\left(x_j\right)\right) + \sum_{j=1}^{N}\lambda_j(t)C_j x_j + \frac{\rho}{2}\sum_{j=1}^{N}\left\|C_j x_j - D\right\|_2^2 \tag{5}$$

其中，λ_j 是对偶变量，其更新规则为

$$\lambda_j(k+1) = \lambda_j(k) + \rho\left(\sum_{j=1}^{N}\lambda_j(t)C_j x_j - D\right) \tag{6}$$

4.3.2　基于交替方向乘子法的入侵检测策略求解

对于多主多从联邦学习过程，入侵检测策略的求解过程通过内循环和外循环两个阶段反复迭代完成。具体来说，外循环阶段，入侵检测服务器为边缘设备制定入侵样本定价策略，使得自身效用达到最大。在内循环阶段，各边缘设备依据各入侵检测服务器制定的入侵样本定价策略，给出使自身效用最大的入侵样本分配策略。经过外循环、内循环反复迭代，可得到相应的入侵检测策略，该过程可由式(7)表述。

$$\begin{aligned}
&\max U_n(\boldsymbol{p}_n) = \left(1-\beta\cdot \mathrm{e}^{-\alpha_n\sum_{i=1}^{M}\gamma_i d_{i,n}}\right) + \phi_n\cdot\left(\frac{\sum_{i=1}^{M} p_{i,n}}{\sum_{i=1}^{M}\sum_{j=1}^{N} p_{i,j}}\right) - \\
&\sum_{i=1}^{M}\sigma_i\cdot\left(1-\beta\cdot\mathrm{e}^{-\gamma_n d_{i,n}}\right)\cdot p_{i,n} \\
&\text{s.t.}\begin{cases}
\forall i\in M, p_{i,n}\geqslant 0, \sum_{i=1}^{M} p_{i,n} = B_{n_\max} \\
\boldsymbol{d}_m = \arg\max U_m(\boldsymbol{d}_m) \\
\forall j\in N, d_{m,j}\geqslant 0, \sum_{j=1}^{N} d_{m,j} = D_{m_\max}
\end{cases}
\end{aligned} \tag{7}$$

如式(7)所示，入侵检测服务器在优化自身效用函数的过程中，需要同时考虑自身的约束条件及边缘设备的约束条件。对于边缘设备来说也是如此。因此，中心化的优化策略难以应用于这类复杂的优化问题。交替方向乘子法（ADMM, alternating direction method of multipliers）是一种分布式优化方法，ADMM 可以将复杂的优化问题分布式分解成多个子问题，在每个子问题中求解一个变量，同时保持其他变量不变。且 ADMM 具有快速收敛的特性，因此，ADMM 适用于优化多主多从边缘学习过程。

策略求解过程通过内循环和外循环两个阶段反复迭代完成。具体来说，通过内循环优化各个边缘设备的效用，同时通过外循环优化各个入侵检测服务器的效用。并最终获得边缘设备及入侵检测服务器在限制条件内有关的最佳入侵样本分配策略和入侵样本定价策略。

在内循环阶段，边缘设备根据各个入侵检测服务器的定价策略，选择最优数量的入侵样本为特定的入侵检测服务器进行训练。对边缘设备的效用函数 $U_m(\boldsymbol{d}_m)$ 求二阶导数为

$$\frac{\partial U_m(\boldsymbol{d}_m)}{\partial d_{m,j}} = \gamma_m\beta s_m \mathrm{e}^{-\gamma_m d_{m,j}} p_{m,j} - \mu_j\cdot\log\left(\frac{1}{\varepsilon_m}\right)\frac{1}{f_m} \tag{8}$$

$$\frac{\partial^2 U_m(\boldsymbol{d}_m)}{\partial^2 d_{m,j}} = -\gamma_m^2\beta\,\mathrm{e}^{-\gamma_m d_{m,j}}\ p_{m,j} < 0 \tag{9}$$

由此可知，边缘设备的效用函数$U_m(\boldsymbol{d}_m)$中各个子问题的二阶导数小于零，可以利用 ADMM 进行优化[24]。边缘设备的优化问题求解过程如下，假设外循环的系数是q，内循环的系数是t，则边缘设备贡献数据量的更新计算式为

$$d_{m,*}^{(q)}(t+1)=\operatorname{argmax}\left(U_m(\boldsymbol{d}_m)\right)+\sum_{j=1}^{N}\lambda_j^{(q)}\left(d_{m,j}\right)+\psi \quad (10)$$

其中，$\psi=\frac{\rho}{2}\sum_{j=1}^{N}\left\|\sum_{i=1}^{m-1}\left(\tau_j d_{i,j}^{(q)}(t+1)\right)+\tau_j d_{m,j}+\sum_{i=m+1}^{M}\left(\tau_j d_{i,j}^{(q)}(t)\right)-d_{j\_\max}\right\|_2^2$，$\rho$是惩罚因子。

拉格朗日系数$\lambda_m^{(q)}$的更新计算式为

$$\lambda_j^{(q)}(t+1)=\lambda_j^{(q)}(t)+\rho\left(\sum_{i=1}^{M}\left(\tau_j d_{i,j}^{(q)}(t+1)\right)-d_{j\_\max}\right) \quad (11)$$

可利用交替乘子法对内循环进行更新，以得到在各入侵检测服务器给定入侵样本价格的情况下，各边缘设备的最佳入侵样本贡献策略。

在外循环阶段，边缘设备根据各个入侵检测服务器的入侵样本分配策略为每个边缘设备选择最优的入侵样本定价策略。

对入侵检测服务器效用函数求二阶导数为

$$\frac{\partial U_n(\boldsymbol{p}_n)}{\partial p_{i,n}}=\phi_n\left(\frac{1}{\sum_{i=1}^{M}\sum_{j=1}^{N}p_{i,j}}-\frac{\sum_{i=1}^{M}p_{i,n}}{\left(\sum_{i=1}^{M}\sum_{j=1}^{N}p_{i,j}\right)^2}\right)-\sigma_i\cdot\left(1-\beta\cdot\mathrm{e}^{-\gamma_i s_i d_{i,n}}\right) \quad (12)$$

$$\frac{\partial^2 U_n(\boldsymbol{p}_n)}{\partial^2 p_{i,n}}=\phi_n\left(\frac{2\sum_{i=1}^{M}p_{i,n}-2\sum_{i=1}^{M}\sum_{j=1}^{N}p_{i,j}}{\left(\sum_{i=1}^{M}\sum_{j=1}^{N}p_{i,j}\right)^3}\right)<0 \quad (13)$$

由此可知，$U_n(\boldsymbol{p}_n)$中各个子问题的二阶导数小于零，因此，外循环阶段可以利用 ADMM 对其进行优化求解。在外循环阶段，各入侵检测服务器可根据自身设定的入侵样本定价策略预测各边缘设备的入侵样本分配策略$\boldsymbol{d}_m$。依据所预测的入侵样本分配策略$\boldsymbol{d}_m$，各入侵检测服务器可通过优化自身的效用函数来获得最佳入侵样本定价策略为

$$p_{n,m}^{(q)}(t+1)=\operatorname{argmax}\left(U_n(\boldsymbol{p}_n)\right) \quad (14)$$

如此，各入侵检测服务器可将定价策略$p_{n,m}^{(q+1)}$广播给各边缘设备，如此开始进入第$q+1$次外循环。假设ν是各入侵检测服务器设定的阈值，当外循环满足式(15)时，外循环结束。

$$\left\|\sum_{j=1}^{N}U_n\left(p_n^{(q)}\right)-\sum_{j=1}^{N}U_n\left(p_n^{(q-1)}\right)\right\|\leqslant\nu \quad (15)$$

内循环和外循环反复进行，直到外循环中决定的入侵样本价格在某个时间点收敛。以上面向多主多从博弈的 ADMM 可总结如算法 1 所示。

算法 1 面向多主多从博弈的交替方向乘子算法

初始化：各边缘设备初始入侵样本分配策略$\boldsymbol{d}_m^{(0)}$，各入侵检测服务器入侵样本定价策略$\boldsymbol{p}_n^{(0)}$

while$\left(\left\|\sum_{j=1}^{N}U_j\left(p_j^{(q)}\right)-\sum_{j=1}^{N}U_j\left(p_j^{(q-1)}\right)\right\|>\nu\right)$

（内循环）利用交替乘子法在内循环求解各边缘设备针对各入侵检测服务器的最优数据，边缘设备根据入侵检测服务器指定的价格$\boldsymbol{p}_n^{(q)}$来优化自己的效用函数$U_m(\boldsymbol{d}_m^{(0)})$，进而得到最优入侵样本分配策略$\boldsymbol{d}_m^{(q)}$。

（外循环）利用交替乘子法在外循环求解各入侵检测服务器针对各边缘设备入侵样本的最优报价，各入侵检测服务器针对各边缘设备的最优入侵样本分配策略$\boldsymbol{d}_m^{(q)}$，通过优化自身的效用函数$U_n(\boldsymbol{p}_n^{(q)})$进而得到最优入侵样本定价策略$\boldsymbol{p}_n^{(q)}$。

q=q+1

输出：各边缘设备的最优入侵样本分配策略$\boldsymbol{d}_m$，各入侵检测服务器的最优入侵样本定价策略$\boldsymbol{p}_n$

5 仿真与评估

为了评估所构建边缘学习物联网入侵检测框架的有效性，构建了边缘学习入侵检测模型和迁移边缘学习入侵检测模型以感知潜在威胁，它们均由两个长短期记忆（LSTM, long short-term memory）层和一个全连接层组成，其中全连接层将 Sigmoid 设置为激活函数，而 LSTM 层则选择 Sigmoid 和 hard Sigmoid 作为激活函数。同时，将 TensorFlow Federated（TFF）联邦学习框架部署在具有 12 GB RAM、Tesla P100 GPU 和 Intel XEON 2.0 GHz CPU

的云平台上运行，以进行联邦学习实验。为了使所训练的入侵检测模型对多种攻击具有感知能力，将具备22种攻击类型的KDD-Cup 99数据集作为多主多从联邦学习的训练集。训练过程中，不对所需感知的具体攻击类型进行指定，因此，基于博弈优化边缘学习的入侵检测机制不会存在只能感知某种特定威胁的问题。首先，利用边缘学习过程中未使用过的入侵样本来训练一个深度学习模型。然后，在由两个客户端和一个服务器组成的边缘联邦学习系统中，使用联合平均算法对经过训练的深度学习模型进行微调，以得到完整的迁移边缘学习入侵检测模型。此外，为了与迁移边缘学习入侵检测模型进行对比，在同一联邦学习系统上直接进行训练，以得到边缘学习入侵检测模型。由于预训练模型权重已经包含一定入侵检测的知识，因此迁移学习可以加快入侵检测模型的训练。入侵检测模型训练过程准确率与损失函数评估如图 3 所示，边缘联邦学习可利用边缘设备入侵样本构建有效的入侵检测系统，同时微调等迁移学习手段可加速边缘学习训练过程。

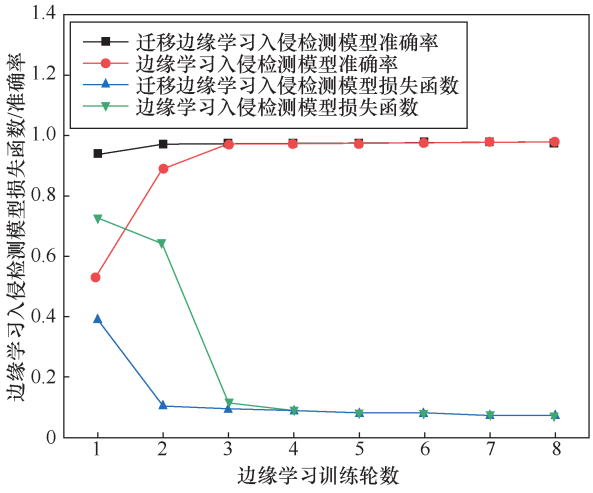

图 3　入侵检测模型训练过程准确率与损失函数评估

为评估多主多从博弈对入侵检测服务器定价策略及边缘设备入侵样本分配策略的影响，构建一个由 2 个入侵检测服务器及 2 个边缘设备构成的多主多从边缘学习入侵检测系统。在这个系统中，假设入侵检测服务器 1 和入侵检测服务器 2 最高预算 $B_{1\_\max}$ 和 $B_{2\_\max}$ 都为 1 000，且影响入侵检测服务器参与定价的因子 ϕ_1 与 ϕ_2 都设为 10^5。入侵检测服务器 1 和入侵检测服务器 2 对所购买入侵样本的影响因子 α_1 与 α_2 设为 0.1。将边缘设备 1 和边缘设备 2 对所贡献入侵样本的影响因子 γ_1、γ_2、β 分别设为 0.1、0.1 与 1。将两个边缘设备所能提供的最大入侵检测样本数据量 $d_{1\_\max}$ 与 $d_{2\_\max}$ 都设置为 1 000。同时将边缘设备的本地训练精度 ε_1 与 ε_2 都设置为 0.01，并在入侵检测服务器可信度相关影响因子 $\mu_1=10^4, \mu_2=1, \omega_1=1, \omega_2=1$、边缘设备可信度影响因子 $\sigma_1=1, \sigma_2=1$ 时，对边缘学习系统进行迭代求解入侵检测服务器的效用值。入侵检测服务器效用函数如图 4 可知，在满足此条件的情况中，两个入侵检测服务器的效用函数随着外循环次数的增加而逐渐收敛，系统达到多主多从博弈均衡状态，入侵检测服务器 1 与入侵检测服务器 2 都得到了在此约束条件下的最优入侵样本定价策略。

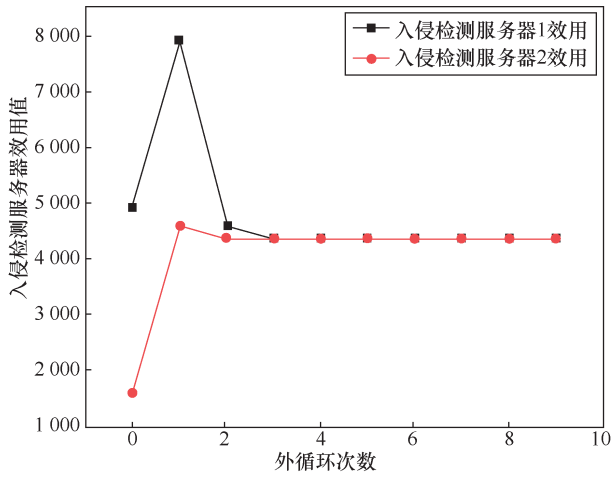

图 4　入侵检测服务器效用函数

为评估入侵检测服务器 1 可信度 ω_1 对其从边缘设备 2 处购买样本数据量的影响，保持图 4 对应设置不变。同时将影响入侵检测服务器参与定价的因子 ϕ_1 与 ϕ_2 都设为 10^2。设置入侵检测服务器可信度影响因子 $\mu_1=1, \mu_2=1, \omega_2=1$，边缘设备可信度相关影响因子 $\sigma_1=0.1, \sigma_2=1$。同时，在此条件下，对边缘学习系统进行多主多从博弈迭代，入侵检测服务器可信度对购买入侵样本的影响如图 5 所示，随着 ω_1 的增长，入侵检测服务器能够从边缘设备 2 购买更多的入侵样本。ω_1 越大说明入侵检测服务器 1 越可信，从入侵检测服务器 1 获取的收益对边缘设备 2 的效用具有更强的正面作用，因此边缘设备 2 愿意分配更多入侵检测样本给入侵检测服务器 1。

为评估边缘设备 2 的影响因子 σ_2 对其从入侵检测服务器 2 所获得入侵样本定价的影响，保

持图 5 对应设置不变。设置入侵检测服务器可信度相关影响因子 $\mu_1=1,\mu_2=1,\omega_1=0.1,\omega_2=1$，边缘设备可信度相关影响因子 $\sigma_1=1$。同时，在此条件下，对由 2 个入侵检测服务器与 2 个边缘设备构成的边缘联邦学习系统进行迭代。边缘设备影响因子对入侵样本定价的影响如图 6 所示，随着 σ_2 的增长，边缘设备 2 从入侵检测服务器 2 获得的入侵样本定价越来越低。这是因为 σ_2 值的增长代表边缘设备 2 变得越来越不可信，入侵检测服务器 2 从边缘设备 2 购买入侵样本对其效用函数的正面作用越来越小，因此，入侵检测服务器 2 对边缘设备 2 入侵样本的定价随着 σ_2 值的增加而减少。

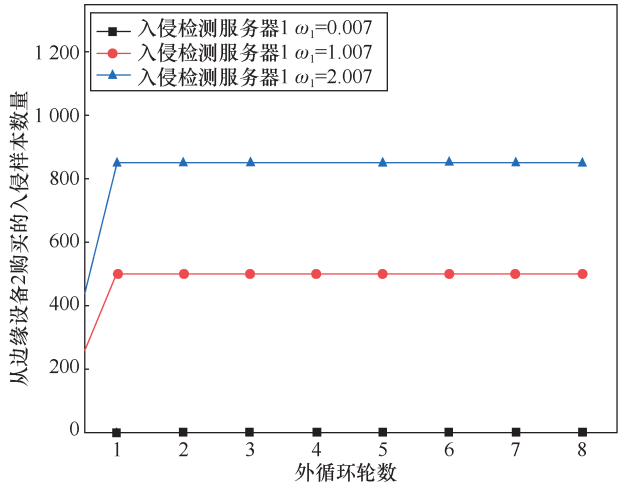

图 5 入侵检测服务器可信度对购买入侵样本的影响

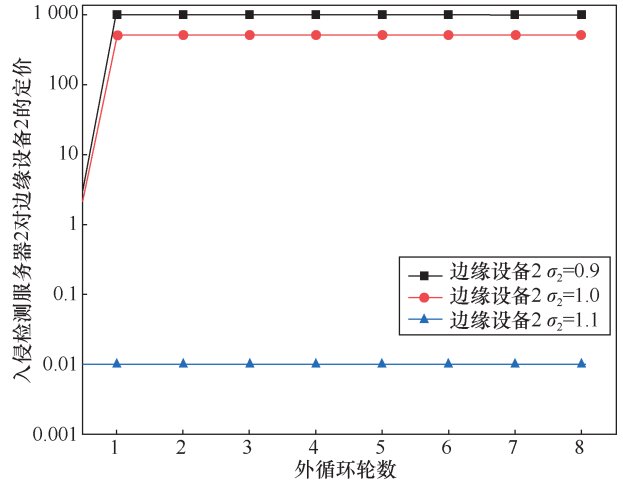

图 6 边缘设备影响因子对入侵样本定价的影响

6 结束语

本文提出了基于博弈优化边缘学习的物联网入侵检测框架，能够利用边缘联邦学习在保护边缘设备隐私的条件下为物联网提供分布式入侵检测服务。同时，本框架利用多主多从博弈优化边缘学习过程，使入侵检测服务器与边缘设备能动态调整入侵检测样本定价策略及物联网入侵样本分配策略来增加自身的效用，进而激励可信的入侵检测服务器及边缘设备参与构建物联网分布式边缘学习入侵检测系统。仿真实验验证了所提出物联网入侵检测框架的安全性及有效性。本文提出的博弈优化边缘学习入侵检测方法能激励入侵检测服务器与边缘设备积极参与边缘联邦学习，在保护节点隐私的前提下提升物联网的安全性。

参考文献：

[1] 尤肖虎, 尹浩, 邬贺铨. 6G 与广域物联网[J]. 物联网学报, 2020, 4(1): 3-11.
YOU X H, YIN H, WU H Q. On 6G and wide-area IoT[J]. Chinese Journal on Internet of Things, 2020, 4(1): 3-11.

[2] 刘怀哲, 高林. 基于移动热点共享的物联网激励机制研究[J]. 物联网学报, 2019, 3(1): 20-29.
LIU H Z, GAO L. Research on incentive mechanism for IoT based on mobile hotspot sharing[J]. Chinese Journal on Internet of Things, 2019, 3(1): 20-29.

[3] 李赞, 廖晓闽, 石嘉, 等. 面向认知物联网的隐蔽通信智能功率控制[J]. 物联网学报, 2020, 4(1): 52-58.
LI Z, LIAO X M, SHI J, et al. Intelligent power control for covert communication in cognitive Internet of Things[J]. Chinese Journal on Internet of Things, 2020, 4(1): 52-58.

[4] SEDJELMACI H, SENOUCI S M, ABU-RGHEFF M A. An efficient and lightweight intrusion detection mechanism for service-oriented vehicular networks[J]. IEEE Internet of Things Journal, 2014, 1(6): 570-577.

[5] ALBERS P, CAMP O, PERCHER J M, et al. Security in ad hoc networks: a general intrusion detection architecture enhancing trust based approaches[C]//Proceedings of the 1st International Workshop on Wireless Information Systems. [S.l.: s.n.], 2002.

[6] CHIEN W C, CHO H H, LAI C F, et al. Intelligent architecture for mobile HetNet in B5G[J]. IEEE Network, 2019, 33(3): 34-41.

[7] ZHANG T, ZHU Q Y. Distributed privacy-preserving collaborative intrusion detection systems for VANETs[J]. IEEE Transactions on Signal and Information Processing Over Networks, 2018, 4(1): 148-161.

[8] SONG H M, KIM H R, KIM H K. Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network[C]//Proceedings of 2016 International Conference on Information Networking (ICOIN). Piscataway: IEEE Press, 2016: 63-68.

[9] LOUKAS G, VUONG T, HEARTFIELD R, et al. Cloud-based cyber-physical intrusion detection for vehicles using deep learning[J]. IEEE Access, 2018(6): 3491-3508.

[10] CHOI W, JOO K, JO H J, et al. VoltageIDS: low-level communication characteristics for automotive intrusion detection system[J]. IEEE Transactions on Information Forensics and Security, 2018, 13(8):

2114-2129.
[11] SEO E, SONG H M, KIM H K. GIDS: GAN based intrusion detection system for in-vehicle network[C]//Proceedings of 2018 16th Annual Conference on Privacy, Security and Trust (PST). Piscataway: IEEE Press, 2018: 1-6.
[12] MOURAD A, TOUT H, WAHAB O A, et al. Ad hoc vehicular fog enabling cooperative low-latency intrusion detection[J]. IEEE Internet of Things Journal, 2021, 8(2): 829-843.
[13] GROZA B, MURVAY P S. Efficient intrusion detection with bloom filtering in controller area networks[J]. IEEE Transactions on Information Forensics and Security, 2019, 14(4): 1037-1051.
[14] MEJRI M N, ACHIR N, HAMDI M. A new security games based reaction algorithm against DOS attacks in VANETs[C]//Proceedings of 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC). Piscataway: IEEE Press, 2016: 837-840.
[15] MÜTER M, ASAJ N. Entropy-based anomaly detection for in-vehicle networks[C]//Proceedings of 2011 IEEE Intelligent Vehicles Symposium (IV). Piscataway: IEEE Press, 2011: 1110-1115.
[16] LI X H, HU Z Y, XU M F, et al. Transfer learning based intrusion detection scheme for Internet of vehicles[J]. Information Sciences, 2021, 547: 119-135.
[17] DELWAR HOSSAIN M, INOUE H, OCHIAI H, et al. An effective in-vehicle CAN bus intrusion detection system using CNN deep learning approach[C]//Proceedings of GLOBECOM 2020 - 2020 IEEE Global Communications Conference. Piscataway: IEEE Press, 2020: 1-6.
[18] STERNE D, BALASUBRAMANYAM P, CARMAN D, et al. A general cooperative intrusion detection architecture for MANETs[C]//Proceedings of 3rd IEEE International Workshop on Information Assurance (IWIA'05). Piscataway: IEEE Press, 2005: 57-70.
[19] KACHIRSKI O, GUHA R. Effective intrusion detection using multiple sensors in wireless ad hoc networks[C]//Proceedings of 36th Annual Hawaii International Conference on System Sciences, 2003. Piscataway: IEEE Press, 2003.
[20] ZHAN Y F, LI P, QU Z H, et al. A learning-based incentive mechanism for federated learning[J]. IEEE Internet of Things Journal, 2020, 7(7): 6360-6368.
[21] KANG J W, XIONG Z H, NIYATO D, et al. Incentive mechanism for reliable federated learning: a joint optimization approach to combining reputation and contract theory[J]. IEEE Internet of Things Journal, 2019, 6(6): 10700-10714.
[22] JIAO Y T, WANG P, NIYATO D, et al. Toward an automated auction framework for wireless federated learning services market[J]. IEEE Transactions on Mobile Computing, 4639, PP(99): 1
[23] LIN X, LI J H, WU J, et al. Making knowledge tradable in edge-AI enabled IoT: a consortium blockchain-based efficient and incentive approach[J]. IEEE Transactions on Industrial Informatics, 2019, 15(12): 6367-6378.
[24] XIONG Z H, KANG J W, NIYATO D, et al. Cloud/edge computing service management in blockchain networks: multi-leader multi-follower game-based ADMM for pricing[J]. IEEE Transactions on Services Computing, 2020, 13(2): 356-367.

[作者简介]

梁浩然（1989− ），男，上海交通大学网络安全技术研究院博士生，主要研究方向为物联网安全、联邦学习等。

伍军（1979− ），男，上海交通大学网络安全技术研究院副院长、教授、博士生导师，主要研究方向为物联网安全、新型网络安全技术、边缘智能、区块链等。

赵程程（1993− ），女，上海交通大学网络安全技术研究院博士生，日本室兰工业大学公派联合培养博士生，主要研究方向为物联网技术、信息中心网络等。

李建华（1965− ），男，上海交通大学网络安全技术研究院院长、教授、博士生导师，主要研究方向为信息内容安全技术、态势感知、工控网络安全等。