基于区块链的分层联邦学习系统

胡荣磊,刘思惠,段晓毅,左珮良,张艳硕
(北京电子科技学院电子与通信工程系,北京 100070)

摘 要: 联邦学习可以在云边端构建一个分布式、安全的计算环境,以适应数据隐私保护和实时性要求高的应用场景. 其作为一种跨设备分布式学习,其中客户端异构及隐私安全是两个关键性的问题. 首先,在客户端数据异构和设备异构的条件下,其响应速度和数据分布均存在较大差异,会导致客户端之间存在滞后问题,对联邦学习的性能造成很大影响;其次,在隐私安全方面,联邦学习仍存在中心服务器遭受单点攻击、客户端不可信以及推理攻击的安全性问题. 本文设计了分层联邦学习系统FATChain来解决以上问题. 首先针对客户端异构的问题,提出一种高效的客户端选择机制,将被选中客户端按响应速度分组,对每组客户端采用基于代表性梯度的聚类采样,保证具有独特数据分布的客户被选中,通过分层桥接的方式将同步和异步训练相结合,降低全局同步带来的压力,并解决了数据异构和设备异构造成的客户端间的滞后问题;同时设计了基于影响力函数的加权聚合算法,通过提高高质量局部模型的聚合权重,解决由于数据异构造成低质量局部模型权重过高而影响全局精度的问题,加速全局模型的收敛,提升了模型训练准确率. 其次针对隐私安全问题,将联邦学习算法与区块链相结合,实现了去中心化,解决单点攻击问题;系统中设置投毒攻击检测模块,在聚合前过滤掉不合格的本地更新,解决投毒攻击问题;利用区块链组网中群组里参与方节点只上传更新而不生成区块的办法,有效预防了恶意参与方造成的推理攻击. 分析表明,本文提出的联邦学习系统很好地实现了各方的隐私安全防护,同时性能相较于同类方案有了很大的提升,具有很好的可扩展性,适用于大规模且对隐私保护要求较高的应用场景.

关键词: 区块链;联邦学习;隐私保护;聚类采样;模型聚合;云边端
基金项目: 中央高校基本科研业务费资金资助(No.3282023017,No.3282024052,No.3282024058)
中图分类号: TN915.08;TP181 **文献标识码:** A **文章编号:** 0372-2112(2025)07-2482-18
电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20241078

Blockchain-Based Hierarchical Federated Learning System

HU Rong-lei, LIU Si-hui, DUAN Xiao-yi, ZUO Pei-liang, ZHANG Yan-shuo
(*Department of Electronics and Information Engineering*, *Beijing Electronic Science and Technology Institute*, *Beijing* 100070, *China*)

Abstract: Federated learning can build a distributed and secure computing environment at the cloud-edge-terminal for application scenarios with high data privacy protection and real-time requirements. As a cross-device distributed learning, client heterogeneity and privacy security are two critical issues. Firstly, under the conditions of client data heterogeneity and device heterogeneity, there are large differences in response speed and data distribution, which can lead to lag between clients and greatly affect the performance of federated learning. Secondly, in terms of privacy security, federated learning still has security problems such as single-point attack on the central server, untrustworthy clients, and inference attacks. In this paper, we designed a hierarchical federated learning system FATChain to solve the above problems. Firstly, for the problem of client heterogeneity, an efficient client selection mechanism is proposed to group the selected clients according to their response speeds, and cluster sampling based on the representative gradient is used for each group of clients to ensure that clients with unique data distributions are selected, and synchronous and asynchronous training are combined through hierarchical bridging, which reduces the pressure caused by global synchronization while solving the problem of data and device heterogeneity. At the same time, a weighted aggregation algorithm based on the influence function is designed to improve the aggregation weight of high-quality local models, to solve the problem that global accuracy is affected by the high weight of low-quality local models due to data heterogeneity, to accelerate the convergence of the global model, and to improve the accuracy of model training. Secondly, to address the privacy and security issues, the federated learning algorithm

收稿日期:2024-12-02;录用日期:2025-03-13;责任编辑:孙瑶

is combined with the blockchain to achieve decentralization and solve the problem of single-point attack. A poisoning attack detection module is set up in the system to filter out the unqualified local updates before aggregation, solving the problem of poisoning attack. And the approach that participant nodes in the blockchain grouping only upload the updates without generating the blocks is utilized, which effectively prevents the inference attack caused by the malicious participant. The analysis shows that the proposed federated learning system well achieves privacy security protection for all parties, while the performance is greatly improved compared to similar schemes with good scalability. And it is suitable for large-scale application scenarios with high requirements for privacy protection.

Key words: blockchain; federated learning; privacy protection; cluster sampling; model aggregation; cloud-edge-terminal

Foundation Item(s): Fundamental Research Funds for the Central Universities (No.3282023017, No.3282024052, No.3282024058)

1 引言

联邦学习(Federated Learning,FL)作为面向分布式数据的机器学习[1]方法,通过在多个设备或者数据中心中进行本地计算和模型更新,实现在不共享原始数据的情况下进行模型训练.联邦学习可以在云边端构建分布式、安全的计算环境,以适应数据隐私保护和实时性要求高的应用场景.但是目前传统的联邦学习仍存在一些问题.

首先在性能方面,目前有两方面需要改进:

(1)联邦学习客户端异构问题[2].不同的客户端之间计算能力和网络资源不同,分布在不同客户端上的训练数据通常也是不均匀的,是非独立同分布的.这种资源和数据的异构,往往会在联邦学习过程中产生落后者,即客户端之间存在滞后.

(2)数据异构导致低质量局部模型权重过高的问题[3].目前联邦学习的每个设备上传的模型参数的权重大多是根据设备上的本地数据量大小进行赋值的,如联邦学习中的联邦平均(Federated Averaging,FedAvg)[4],它通过加权平均来聚合模型参数,将本地模型的参数上传到服务器,服务器计算所有模型参数的平均值,然后将这个平均值广播回所有本地设备.这样的聚合方式忽略了高质量数据及参与方对整个全局模型的贡献,扩大了低质量数据及参与方对全局模型的危害,对全局模型的收敛精度和模型准确率等性能造成影响.

其次在联邦学习隐私安全方面,尽管在传统联邦学习算法中的各个用户在不共享数据的情况下进行分布式训练,对隐私起到了一定的保护作用,但是经研究发现,其在隐私安全保护方面仍然存在很大的漏洞,目前存在以下三方面的问题:

(1)中心聚合服务器不可信问题.传统的联邦学习采用中心服务器进行全局聚合容易遭到单点攻击,Wang等人[5]对中心服务器进行攻击,发现整个联邦学习系统彻底崩溃了.同时恶意的聚合服务器会在聚合时隔离部分局部代理,干预模型的收敛方向,严重损害模型的性能.

(2)局部代理不可信问题.首先恶意局部代理会对联邦学习进行投毒攻击,包括数据投毒攻击[6]和模型投毒攻击[7].Tolpegin等人[8]在训练复杂神经网络时发现,全局模型准确率一直低下的原因在于客户端中存在恶意局部代理进行数据投毒,同时恶意的局部代理还可能向联邦学习其他客户端发起梯度推理攻击.对联邦学习的隐私安全造成了极大危害的还包括特征推理攻击,Carlini等人[9]从递归神经网络中提取用户敏感数据,证明恶意局部代理或攻击者可以从上传至聚合服务器的梯度更新中推理出原始数据的样本标签等隐私信息.

(3)参与方对联邦学习系统的安全性不信任,难以提供高质量数据.

针对联邦学习性能方面存在的问题,我们提出解决思路.在异步分层联邦学习中,根据响应延迟的快慢,将客户端划分为不同的逻辑层,层内同步更新,层间异步更新全局模型,从而缓解了设备异构带来的危害,提升了收敛速度和可扩展性.为解决客户端数据分布不均带来的数据异构问题,采用基于代表性梯度的聚类采样,在不需要所有客户端都参与的基础上,也能更好地体现全局数据的分布特性,在减少通信负担的同时,使模型加速收敛到全局最优解.同时,为了解决数据异构导致低质量局部模型权重过高的问题,我们从模型聚合策略方面进行优化,提出基于影响力函数的加权聚合算法,使高质量局部模型拥有更高的权重,确保达到更平滑、更快速的全局收敛效果.

针对联邦学习安全性的问题,本文利用区块链去中心化的节点网络取代传统联邦学习的中心聚合服务器,可以很好地预防传统联邦学习所遭受的单点攻击,其可溯源、不可篡改的特点有助于建立高效的监督管理机制.另外,利用智能合约自我执行和自我验证,不需要人为干预的特点,能够在保证模型评估的公平性和可靠性的同时,提升联邦学习的安全性.

基于上述的研究思路,本文设计了基于区块链的

分层联邦学习系统 FATChain(Blockchain-based Asynchronous Hierarchical Federated Learning System),主要贡献如下:

(1)设计了一种新的区块链群组框架. 与现有的区块链结合联邦学习方案不同,本方案将异步分层联邦学习算法和区块链群组框架相结合,通过分层桥接同步和异步训练,实现去中心化,解决了传统联邦学习易遭受单点攻击威胁的问题,同时最大限度地减少了客户端异构造成的落后者效应,即客户端之间存在滞后的问题,提高了模型训练的准确度和收敛速度,通过将同步和异步训练相结合的方式提升了该框架的可扩展性.

(2)设计了自适应模型加权聚合算法. 根据模型训练贡献度a和更新频率f所产生的影响力因子来调整模型聚合参数,层内局部聚合时,增加贡献度高的模型在聚合中的占比,同时由于每层更新频率不同,根据层更新全局模式的次数动态调整分配给每个层的相对权重. 该算法可以帮助全局训练更快地收敛,提高联邦学习算法的性能.

(3)提出一种全面高效的客户端选择机制. 根据客户端响应速度进行分组,每组内再根据客户端相似梯度选举出参与每层同步更新的用户,在保持最小的通信代价的基础上,保证更小的节点选择差异性. 该机制保证了那些具有独特数据分布的客户可以被选中,从而实现更平滑、更快速的全局模型收敛效果.

(4)针对传统联邦学习所面临的隐私安全隐患,设计了安全防护体系. 设计模型筛查智能合约,过滤掉不符合条件的局部更新模型,以防止投毒攻击对模型精度造成影响.

(5)将新提出的 FATChain 方案与 FedAsync(Asynchronous Federated optimization)[10]、FedAvg[4]、FedAT(Federated learning system with Asynchronous Tiers)[11]方案进行实验比较分析,证明了其在性能上的优势,并对其收敛性进行证明.

2 相关工作

2.1 联邦学习的隐私保护

联邦学习在理论上能够实现隐私保护前提下的多方共同合作训练模型,但是落地仍旧存在许多问题. 杨庚等人[12]分析了联邦学习现存的隐私安全问题及其使用的隐私保护方法;Melis 等人[13]通过推理攻击,发现恶意局部代理可能会学习到其他局部代理的隐私数据;Song 等人[14]在全局聚合时,隔离部分局部代理上传的模型更新,从而操纵模型收敛方向.

针对以上联邦学习安全问题,国内外已提出一些相应的解决方案. Qiu 等人[15]提出了一种基于同态加密技术来保护训练数据的算法,利用加性同态加密来保护局部和全局模型参数. Sun 等人[16]设计了一个针对客户端投毒攻击的防御模型,提出一种定量估计器,估计了投毒模型对全局模型参数的影响,减轻已经污染了全局模型的投毒攻击. 差分隐私技术也已经被广泛应用于隐私敏感领域,以提高联邦学习算法的安全性. Choudhury 等人[17]利用了基于目标扰动的差分隐私在模型的目标函数中添加噪声,以产生最小的目标扰动,获得一个近似差分. Lang 等人[18]提出联合隐私增强和量化方法,利用基于随机格的矢量化,通过专用的多元隐私保护噪声增强模型增强隐私. Geyer 等人[19]利用客户端差分隐私技术提出了一个联邦优化算法,其算法可以隐藏模型训练期间参与方的模型参数. 此外,还有其他解决方案. Lebrun 等人[20]提出了一种新的隐私保护服务以对抗来自恶意服务器的推理攻击,防止恶意服务器利用更新进行属性推理. 刘飚等人[21]设计了一种拜占庭鲁棒聚合算法,可以有效抵御拜占庭客户端的攻击. 目前的这些隐私保护方案,仍然存在一些问题,无法平衡隐私保护和模型性能之间的关系,例如大多数方案只考虑不可信局部代理造成的安全隐私问题,而忽略了在梯度收集和更新过程中不诚实的行为和恶意的攻击对整个过程造成的损害.

2.2 区块链结合联邦学习

区块链作为一种分布式账本技术,其去中心化、可溯源、防篡改的特点是替换传统联邦学习中心化服务器的有效解决策略. 目前也有一些区块链结合联邦学习的相关方案. Kang 等人[22]提出了一种方案,将联邦学习与区块链相结合,将训练好的模型上传至区块链,并利用区块链的择优算法对模型进行评估过滤,保证了模型的准确度. 但是该方案只是利用区块链的共识算法对其进行审查,最后还是依赖中心服务器进行全局聚合,并未做到去中心化. Majeed 等人[23]提出一种基于公共区块链的联邦学习框架,训练节点和矿工无须验证,直接参与训练. 这种基于公共区块链的联邦学习系统,可能会有恶意节点进行攻击,使得全局模型收敛受损. Li 等人[24]提出一种基于联盟链和联邦学习的框架,方案中联盟链用于节点管理、梯度验证. BLADE-FL(Blockchain Assisted Decentralized Federated Learning)[25]是一个区块链辅助的分布式联邦学习框架,通过对整体架构的设计解决了恶意客户端投毒攻击的问题,但是其存在通信瓶颈的问题.

通过以上分析可知,现有的联邦学习结合区块链的方案,缺乏联邦学习安全和性能之间的平衡,往往只解决安全性问题,而忽略了联邦学习效率、通信瓶颈等性能问题,对于客户端贡献的量化问题也存在一定的忽视,同时在解决安全性问题上未能思考全面,缺少完整的安全防护体系.

2.3 联邦学习客户端异构问题

客户端异构问题是指由于不同的客户端之间计算能力和网络资源的不同,以及分布在不同客户端上的训练数据通常是不均匀的,是非独立同分布的,这种资源和数据的异构往往会在联邦学习过程中产生落后者. 面对此问题,客户端如何与服务器通信成为关键. 目前联邦学习常见的通信方式包括同步通信和异步通信. Li等人[4]提出了FedAvg同步算法,该算法等待所有客户端完成本地更新后再进行聚合,算法扩展性差,当参与训练的客户端数量很多时,大大增加了训练的时间,同时还会浪费计算能力强的设备资源. Bonawitz等人[26]提出直接忽略落后者,但会造成服务器与通信能力强的客户端多次通信,从而造成全局模型过拟合. 为此,又有研究者提出异步的通信方式. Xie等人[10]提出FedAysnc算法,该算法服务器不需要等待所有客户端更新完毕后再聚合,而是只要客户端上传更新,就立刻聚合. 这种方式虽然减少了训练时间,但是这种传输策略使得每个客户端都要与服务器通信,会造成通信瓶颈. Nguyen等人[27]提出了一种半异步联邦学习算法,这个工作中的服务器不是在接收到单个本地训练结果后立即聚合,而是在全局模型聚合之前等待预设的时间,但该算法仍然难以解决通信瓶颈的问题.

3 提出FATChain系统模型

FATChain是去中心化的安全分层联邦学习系统,通过区块链取代联邦学习的中心服务器,将异步分层联邦学习算法和区块链群组框架相结合,通过分群组桥接同步和异步训练. 为了更好地描述系统框架,根据任务不同,将区块链上的节点划分为任务发布节点,参与方节点和验证节点,如图1所示.

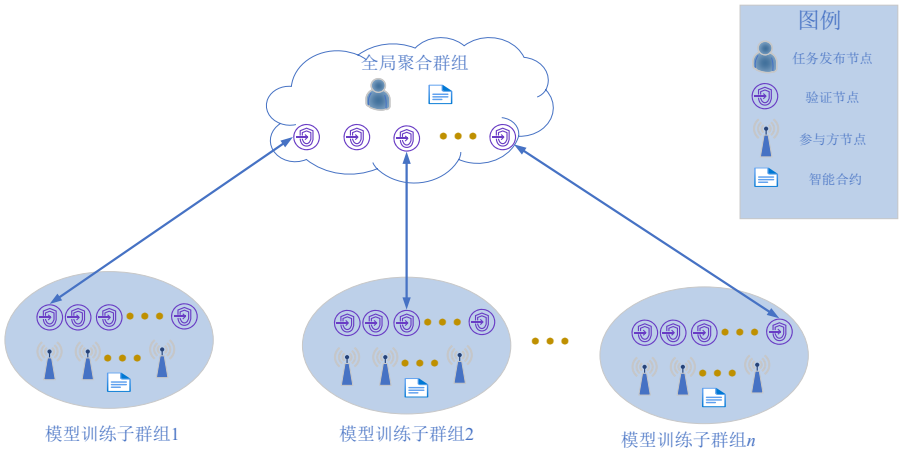

图1　FATChain节点框架示意图

模型训练子群组:根据客户端响应速度,划分成多个模型训练子群组,各子群组内的参与方节点(客户端)采用同步的聚合方式. 每一个模型训练子群组对应分层联邦学习算法中根据客户端响应延迟划分的一个层.

全局聚合群组:由部分客户端构成,该群组负责接收各模型训练子群组上传的局部模型参数,并异步地进行全局模型聚合,并将新的全局模型下发至各模型训练子群组.

参与方节点:与传统分布式深度学习模型中定义的相同实体,具有相似的需求,但由于自身数据量有限,同时受到自身计算能力的限制,无法独立完成整个训练任务. 参与方节点是联邦学习的重要组成部分,主要任务是对模型进行本地训练,并将本地更新上传至区块链.

任务发布节点:根据自身需要,发布一个联邦学习任务(包括模型精度要求、存储、计算能力等),并提供初始模型供参与方节点联合训练,设立激励机制鼓励高效模型训练和优秀的参与者.

验证节点:验证节点(客户端)包括模型训练子群组的验证节点和全局聚合群组的验证节点. 模型聚合子群组的验证节点不参与本地更新,其根据模型筛查合约,利用验证数据集验证参与方节点上传的本地更新是否在规定阈值内,从而避免不可信客户端造成的投毒攻击,当所有本地更新上传完毕后,将本地更新同步地聚合,得到局部聚合模型. 全局聚合群组的验证节点,维护一个全局模型列表,异步地更新各子群组上传的局部模型,获得全局模型.

系统的整体模型及流程如图2所示. 该系统模型的运行步骤如下.

步骤1:根据响应延迟将客户端分为不同群组,包括n个模型训练子群组和1个全局聚合群组.

步骤2:任务发起方发起训练任务,将初始全局模

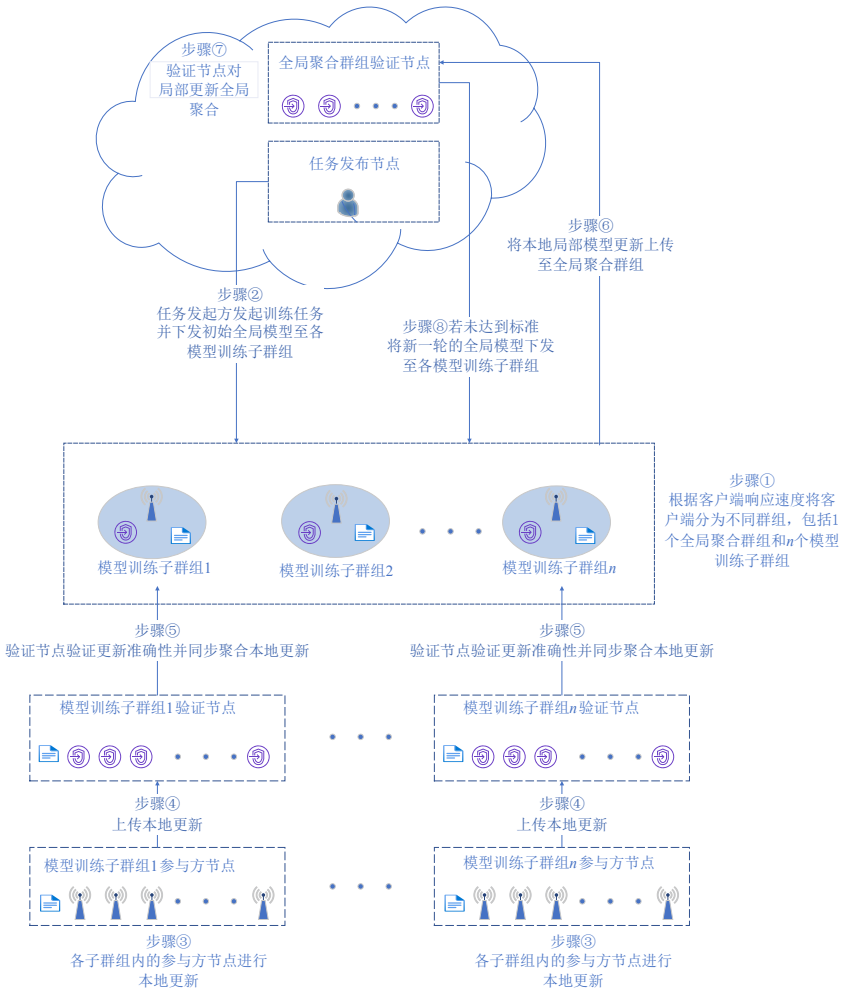

图2 FATChain系统模型及运行流程

型数据上传区块链,下发至各模型训练子群组.

步骤3:各模型训练子群组中依照用户选择算法选择参与局部聚合的参与方节点,被选中的节点从区块链上下载全局模型,并进行本地更新.

步骤4:各模型训练子群组的参与方节点将本地更新上传至子群组验证节点交易池中.

步骤5:各模型训练子群组的验证节点在接收到上传的本地更新后,使用验证数据集对本地更新的可信度进行验证,当所有更新均上传完毕后,验证节点加权聚合所有验证通过的本地更新,获得局部聚合模型.

步骤6:将局部聚合模型打包生成区块,上传至区块链,自动扩散至区块链全局聚合群组.

步骤7:全局聚合群组的验证节点对接收到上传的局部聚合模型更新,异步地进行模型全局聚合.

步骤8:将新一轮生成的全局模型打包生成区块,上传到区块链上.

步骤9:重复上述步骤4~8,直至全局模型达到任务发起方的标准.

根据框架运行流程设计了联邦学习算法,如算法1所示. 此算法将联邦学习训练过程,分为层内同步训练和层间异步训练,采用此分层结构,解决了联邦学习客户端异构和通信瓶颈问题,同时设计用户选择算法,保证具有独特数据分布的客户可以被选中,进一步优化了数据异构的问题. 在聚合步骤上,设计了基于影响力函数的加权聚合算法,提升联邦学习算法的性能. 在安全性上,设置模型投毒攻击检测模块,通过验证节点在局部聚合前对不合格的本地更新进行过滤,避免了联邦学习遭受投毒攻击;设置参与方节点只上传本地更新不打包生成区块,解决了推理攻击的问题. 该算法既提升了联邦学习算法的性能,又具备完善安全体系,保证了联邦学习的隐私安全. 在框架中将算法1以智能合约形式部署到区块链上,利用智能合约自我执行和自我验证而不需要人为干预的特点,能够保证模型评估的公平性和可靠性. 该算法的收敛性证明见6.2节.

FATChain方案能够更好地适应大规模、多场景的应用需求,例如对隐私保护要求较高的医疗领域,在多

家医院合作开发基于电子病历的疾病预测模型时,每家医院作为系统中的客户端,本地存储并预处理自己电子病历数据. 任务发布者初始化并分发全局预测模型至各家医院,各医院利用本地数据在全局模型的基础上进行本地训练,将获得的本地更新上传至区块链网络,区块链上的智能合约自动执行验证、聚合操作,将更新后的全局模型发布到区块链,供所有医院下载进行下一轮训练. 最终,多家医院在无须共享数据的前提下,共同开发出一个高性能疾病预测模型. 该框架不仅满足了医疗领域对患者疾病数据隐私保护的需求,而且其可扩展性能允许多家医院同时参与训练,使框架能够高效整合多源数据,提高预测模型性能. 模型在其他领域也得到应用,比如金融行业中,银行、保险公司间在保护客户数据隐私的基础上联合训练风控模型、欺诈检测模型等;在智能设备与物联网领域,智慧城市中的不同区域或设备协作开发交通管理、能源优化模型等.

算法1　FATChain训练过程

输入:初始全局模型ω^{t_0},全局迭代轮次t,群组更新次数$T_M=0$,所有群组更新次数总和T,根据客户端响应延迟划分为M个群组(层),通过聚类采样选出的参与方节点z_k,$n_k=|D_k|$设备的样本数量,模型投毒检测阈值Y_k,$S(z_k)$客户端的影响因子函数计算

输出:全局模型ω^t

1. 根据客户端响应延迟将客户端划分为M个群组
2. 任务发布节点发布任务至各模型训练子群组,并且每个子群组根据聚类采样选出参与训练的客户端z_k,作为参与方节点
3. FOR $i=1;i\leqslant T$;DO
4. FOR EACH $q\epsilon M$ in parallel DO
5. 参与方节点下载全局模型进行本地训练$\omega_k^{t+1}=\omega_k^t-\nabla h_k(\omega^t)$,并上传至验证节点
6. 验证节点对接收的本地更新进行验证,获得验证准确率a_k
7. IF $a_k\geqslant Y_k$ THEN
8. 计算客户端的影响因子$S(z_k)$
9. 根据影响因子进行加权聚合,得到局部聚合模型$\omega_q^{t+1}=\sum_{k=1}^{m}S(z_k)\cdot\omega_k^{t+1}$
10. 将局部聚合模型上传至全局聚合群组
11. $T_M=T_M+1,t=t+1$
12. END IF
13. END FOR
14. 全局聚合群组的验证节点进行全局聚合获得新一轮的全局聚合模型:$\omega^t=\sum_{l=1}^{M}\frac{T_{(M+1-l)}}{T}\cdot\omega_q$
15. END FOR
16. 输出最终模型ω^t

4　FATChain详细训练方案

本节详细介绍所提出的FATChain方案,表1描述了使用的相关符号.

表1　相关符号说明

符号	说明
M	客户端分层
q_k	聚类采样中每个类的样本数量
m	每层客户抽样数
K	聚类数
T_i	更新次数
∇h_k	梯度
P_k	第k个参与方
ω_q^t	t时刻,q层的局部聚合模型
ω	全局模型

4.1　客户端选择

(1)分层依据

首先确定待分析的性能指标,包括客户端完成训练任务的时间和每个客户端的响应延迟v_i,然后采用轻量级分析器,测量并分析所有参与客户的性能指标;接着分析收集到的性能数据,比较每个客户端的响应延迟;最后基于每个客户端的响应延迟执行客户端分层(群组),根据响应延迟快慢,将客户端分为M层.

(2)基于聚类采样的用户成员选择机制

为了提高联邦学习训练性能,使得全局模型收敛更快速、更平稳,同时减少通信量,本文基于聚类采样[28]为联邦学习过程提供了一个全面、高效的客户端选择机制. 在每层内,利用相似性函数余弦相似度计算本地模型和聚合后形成的全局模型之间的梯度差异,称为代表性梯度,再根据代表性梯度进行聚类采样,选取每层参与同步更新的客户端作为参与方节点. 这种用户选择机制在保持最小通信代价的基础上,保证更小的节点选择差异性. 同时,由于分布是由"代表性梯度"产生的相似数获得的,该方案基于客户端的相似度提升了客户端的代表性,保证了那些具有独特数据分布的客户端可以被选中,从而实现更平滑、更快速的全局模型收敛效果.

算法2以智能合约的形式部署在模型训练子群组中,负责选择每层参与联邦训练的成员,组建联邦社区. 首先,计算每个用户的代表性梯度. 代表性梯度是指用户本地模型和聚合后形成的全局模型之间的差异. 根据代表性梯度,采用Ward层次聚类[28],将客户端聚成K个类,且$K\geqslant m$. 接着,按每个类的样本数量q_k对聚类结果进行降序排序,将前m个类置于前m个分布,剩下的$K-m$个类,按顺序填充至上述m个分布. 然后,以每个分布中客户的样本数量来定义其被选中的概率. 最后,在m个分布中每个分布抽取1个客户,m个训练用户成员即选择完毕. 该算法的无偏性证明见6.1节.

算法2 基于代表性梯度聚类采样的训练用户成员选择算法

输入:客户端样本数量$\{n_i\}_{i=1}^{n}$,客户端代表性梯度$\{G_i\}_{i=1}^{n}$,每层客户端抽样数m,聚类方法Ward,相似性函数:余弦相似度$\mathrm{sim}(G_i,G_j)$

输出:采样概率$r_{k,i}$

1. 获得相似矩阵$\rho,\mathrm{sim}(G_i,G_j)$,用Ward层次聚类从相似矩阵$\rho$估计获得层次聚类$p$
2. 对p进行分割,切割成K组($K\geqslant m$),层次聚类将客户端聚为K个类,得到聚类结果$\{B_k\}_{k=1}^{K}$
3. 定义q_k为每个类的样本总数$q_k=\sum_{i\in B_k}\alpha n_i\leqslant N$($\alpha$为放大系数,$N$为最大样本数量上限)
4. 按每个类的样本数量q_k,对聚类结果$\{B_k\}_{k=1}^{K}$进行降序排列
5. 基于q_k的排序,定义m个分布中的客户端样本数$\{W_k\}_{k=1}^{m}$($\forall k\leqslant m,\forall i\in B_k, r'_{k,i}\leftarrow\alpha n_i$),即将前$m$个聚类置于前$m$个分布
6. 使用其余组$K-m$创建一个集$S=\{\{i,U_i=\alpha n_i\},\forall i\in B_{m+1}\cup B_{m+2}\cup\cdots\cup B_K\}$
7. 开始分配W_k,重复以下操作8~20
8. 在S中选择第一个聚类i,并分配U_i样本
9. 求出$(U_i+q_k)\div N$的商a_i和余数b_i
10. IF $a_i=0$ THEN
11. $r'_{k,i}\leftarrow b_i$,并将i从S中移除
12. ELSE
13. $r'_{k,i}\leftarrow N-q_k$
14. $U_i\leftarrow U_i-r'_{k,i}$
15. IF $U_i=0$
16. REMOVE i FROM S
17. END IF
18. $i\leftarrow i+1$
19. END IF
20. UNITIL $S=\varnothing$
21. 输出采样概率$r_{k,i}=r'_{k,i}\div N$

4.2 本地模型训练

首先介绍每层同步更新时本地模型的训练过程.每一层由上述基于聚类采样的用户选择算法2选择出的m个客户端,定义为$P=\{P_1,P_2,\cdots,P_m\}$,联邦学习的目标是得到一个全局模型ω,使得所有本地参与节点的经验损失函数$h_k(\omega)$最小.传统的联邦学习所有参与本地节点的经验损失函数$F_k(\omega)$表示为

$$F_k(\omega)\overset{\text{def}}{=}\frac{1}{n_k}\sum_{i\in D_k}l_i(x_i,y_i,\omega)\tag{1}$$

其中,D_k表示存储在设备上的样本$(k\in\{1,2,\cdots,m\})$,n_k表示数据样本数,$n_k=|D_k|$,$l_i(x_i,y_i,\omega)$表示单节点本地数据样本$\{x_i,y_i\}$基于全局模型ω的损失函数.

然而,经过研究发现非独立同分布数据以及频繁的局部更新会导致每个客户端倾向于局部最优模型,而不是全局最优模型.为解决此问题,本文在传统联邦学习局部损失函数$F_k(\omega)$中添加约束项,限制局部更新更接近全局模型,从而解决上述问题.改进后的经验损失函数$h_k(\omega)$表示为

$$h_k(\omega)=F_k(\omega)+\frac{\lambda}{2}\left\|\omega_k-\omega\right\|^2\tag{2}$$

每个选定的客户端使用随机梯度下降算法SGD(Stochastic Gradient Descent)用于最小化损失函数,其中梯度的计算公式为

$$\nabla h_k(\omega)=\frac{\partial h_k(\omega)}{\partial m_k}\tag{3}$$

其中,m_k表示客户端P_k的本地训练模型参数.每层选定的客户端使用SGD在自己的数据上执行多个周期,每层再局部聚合,然后将局部聚合更新送至主区块链进行全局聚合更新.

4.3 跨层训练

(1)层内同步训练

各模型训练子群组通过4.1节所述的用户选择机制中所选举出的客户端快速完成本地训练,并迭代多次后,聚合为局部模型,将获得的局部聚合模型上传至全局聚合层(群组).

(2)层间异步训练

全局聚合层维护一个M模型列表$\{\omega_{q_1}^{t},\omega_{q_2}^{t},\cdots,\omega_{q_M}^{t}\}$,如$\omega_{q_m}^{t}$表示的是在$t$时刻,层$m$的局部模型.该列表反映的是每一个时间节点$t$中每一层局部更新的情况,同时全局聚合层的验证节点依据加权聚合智能合约(详情见4.4节),异步地聚合所有层发送的最新更新,形成了全局模型ω.例如,在时间t_1时刻,层1(模型训练子群组1)中的客户端完成同层更新后得到层局部更新模型$\omega_{q_1}^{t_1}$,加权聚合同一时刻其他层的层局部模型$\{\omega_{q_1}^{t_1},\omega_{q_2}^{t_1},\cdots,\omega_{q_M}^{t_1}\}$,得到$t_1$时刻的全局模型$\omega^{t_1}$,并将$\omega^{t_1}$发送至下一个准备就绪层,重复上述操作,直至全局模型达到要求.

如图3所示,t_3时刻层1重新准备就绪,层1接收到全局聚合层上传的全局模型ω^{t_3},层1中的参与方节点下载全局模型ω^{t_3},并进行本地更新,参与节点上传本地更新,层1中的验证节点对本地更新进行同步的加权聚合,得到局部聚合模型$\omega_{q_1}^{t_3}$,再将局部聚合模型发送至全局聚合层,参与异步的模型聚合,一直反复迭代下去.

4.4 加权聚合

传统的联邦学习多采用联邦平均对模型进行聚合,但是这种聚合方式没有考虑到低质量模型对全局模型的影响,更新频率的不同会导致聚合有偏向,因此为了实现无偏、更平衡的训练效果,得到更高质量的数

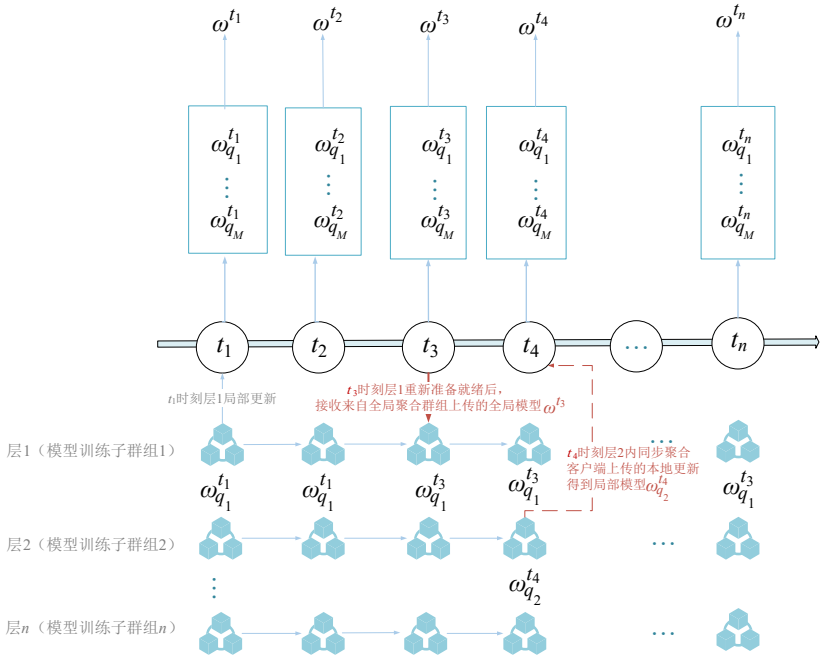

图3　异步分层联邦学习具体步骤

据,本文基于影响力函数[29]提出了自适应模型加权聚合算法,通过影响力函数量化各参与方对全局模型的贡献度,并根据各参与方模型贡献度大小和更新频率来调整模型聚合参数,层内局部聚合时增加贡献度高的模型在聚合中的占比. 同时,由于每层更新频率不同,根据层更新全局模式的次数动态调整分配给每个层的相对权重,帮助全局训练更快地收敛.

(1)层内同步局部聚合

将局部聚合智能合约部署至各模型训练子群组中,局部聚合算法根据参与训练的客户端的影响因子加权聚合层局部模型ω_q^t. 影响因子反映的是由客户端训练的本地模型对局部聚合模型准确率的影响程度,即客户端的贡献量. 贡献量越大在模型聚合时的占比就应当越高,从而提高聚合模型的准确率. 计算影响因子的函数$\mathrm{infl}\left(z_j\right)$为

$$\mathrm{infl}\left(z_j\right)=\sigma_j\frac{n_j}{\sum_{i=1}^{j}n_i}+\rho_j\left(1-\frac{\left|\mathrm{Loss}_j\right|}{\sum_{i=1}^{j}\left|\mathrm{Loss}_i\right|}\right)\tag{4}$$

其中,n_j是表示第j个参与方所包含的数据量,z_j第j个参与方,Loss_j是损失函数在z_j上计算得出的损失值,σ_j和ρ_j分别是参与方所包含的数据量和损失值指标的影响系数. 本文认为参与方所包含数据量相比于损失值指标对全局模型收敛影响更大,因此将σ_j设为0.6,ρ_j设为0.4. 该函数量化了客户端z_j对全局模型性能的影响,为层内加权聚合的权重提供依据. 影响力大的客户端,其局部模型质量更高,分配的权重更大,从而帮助联邦学习更好地解决由数据异构引起的局部模型差异、低质量模型权重过高影响收敛速度和全局模型精度的问题.

模型训练子群组的验证节点根据上述公式计算z_j的影响力,并根据公式$S\left(z_j\right)=\dfrac{\mathrm{infl}\left(z_j\right)}{\sum_{i=1}^{m}\mathrm{infl}\left(z_i\right)}$计算$z_j$的权重,至此$t$时刻$q$层内有$m$个参与方的局部更新模型计算过程可以表示为$\omega_q^t=\sum_{i=1}^{m}S\left(z_j\right)\cdot\omega_j^t$.

(2)层间异步加权聚合

为更新频率较低的、较慢层分配相对较高的权重,以便全局模型不会偏向较快的层,假设有M层,那么到现在为止,每层的更新次数分别是$T_1,T_2,\cdots,T_M$,所有层的更新总数是$T_1+T_2+\cdots+T_M=T$,将跨层异步聚合的全局函数定义为$\omega^t=\sum_{l=1}^{M}\dfrac{T_{(M+1-l)}}{T}\cdot\omega_q$.

5　安全性分析

FATChain系统将联邦学习与区块链相结合,通过智能合约实现任务发布者和联邦学习之间的可信交互,并通过智能合约的有序自动运行,实现联邦学习去中心化,提高联邦学习框架的隐私安全性. 区块链中智能合约的设计主要包括节点分组模块、数据提交模块、验证模块、聚合模块、记录与溯源模块. 智能合约依据客户端响应速度,将参与联邦学习的客户端划分为多

组. 各组更新本地模型并由验证节点经过智能合约的验证模块验证后,局部聚合并打包生成区块上传至区块链上,触发合约的全局聚合操作. 迭代执行上述步骤,直到满足结束条件,由智能合约返回结果. 安全性分析如下.

5.1 抗单点攻击

威胁. 传统的联邦学习依赖中心聚合服务器对模型更新进行全局聚合,然而这是存在安全威胁的. 首先中心聚合服务器一旦遭受单点攻击[30],就会使联邦学习系统无法进行全局聚合,从而影响整个联邦学习系统的进程. 其次,如果中心聚合服务器是恶意的,那么它会根据检测到的用户上传的本地更新,恶意地篡改全局模型,恶意控制全局模型的收敛方向,严重影响联邦学习的最终结果.

安全性分析. 利用区块链去中心化的特点,将区块链和联邦学习系统相结合,用区块链代替中心聚合器,进行联邦学习的局部和全局聚合. 相比于中心聚合器,利用区块链的共识机制,能确保网络中的节点达成一致意见,以确保全局模型的更新是通过共识达成的,而不是由单一实体控制,从而消除了由于中心服务器遭到破坏,整个联邦学习系统进程都会受到很大影响的安全威胁. 同时,在区块链上使用智能合约来规范联邦学习的过程. 智能合约可以定义参与者之间的规则,确保每个节点都按照规定的协议上传和接受模型更新,去中心化的区块链网络使得每个节点都可以参与验证和记录模型更新,增加了系统的透明度和抗攻击性,避免了中心服务器恶意篡改全局模型的安全隐患.

5.2 抗投毒攻击

威胁. 在联邦学习中,投毒攻击包含模型投毒攻击和数据投毒攻击[8,31]. 模型投毒攻击指恶意的局部代理通过改变本地更新模型参数,使学习到的模型满足某些对抗性指标,进而破坏全局模型;数据投毒攻击指通过污染本地训练所用的样本,使得学到的模型对具有特定特征的测试集的分析结果产生偏移,或者做出完全错误的判断. 在这种背景下,如果某个恶意节点篡改或注入有毒样本到其所持有的数据中,或篡改本地模型参数,就会对本地模型训练造成干扰. 当服务器将来自这个恶意节点的更新用于聚合全局模型时,会影响其他正常节点的本地模型训练,对全局模型的训练精度产生负面影响.

安全性分析. 在模型训练子群组中设置验证节点,以模型质量评估为评判依据,验证节点接收到的本地更新经验证后最高的准确率p,当参与方节点上传的本地更新准确率a_k在$Y_k=p(1-k)$以下时,将会被过滤,不参与聚合. 设置超参数阈值k,用以筛掉质量不好的模型和恶意节点投毒的模型:

$$\begin{cases} a_k<p(1-k), \text{不合格局部模型} \\ a_k>p(1-k), \text{合格局部模型} \end{cases}$$

同时,区块链上设有监管,恶意投毒的用户是可溯源并给予处罚的. 通过筛查不合格模型,并对用户的行为进行监管,避免了投毒攻击对联邦学习性能和隐私安全所造成的危害.

5.3 抗推理攻击

威胁. 虽然联邦学习采用梯度代替数据进行共享,但是恶意的参与方仍然可以通过推理反演其他参与方上传的梯度信息,从而得出其他用户的私有数据,对联邦学习用户的隐私安全造成了极大的威胁.

安全性分析. 本文将联邦学习与区块链群组结构相结合,局部聚合群组的参与方节点只上传本地梯度更新,但不打包上传到区块链,只有群组内的验证节点将本地更新局部聚合后才打包上传到区块链,这样参与方是看不到除自身之外其他参与方的梯度更新的,因此可以避免推理攻击,增强联邦学习的安全性.

6 收敛性分析

6.1 聚类采样带来的改进

(1)聚类采样无偏性

假设 1 无偏抽样,$E_{S_t}\left(\omega^t\right)=E_{S_t}\left(\sum_{k\in S_t}\omega_k\left(S_t\right)\cdot\omega_k^t\right)=\sum_{k=1}^{N}p_i\omega_k^t$,其中$\omega_k\left(S_t\right)$是客户端$k$对于客户端子集$S_t$的聚合权重.

首先证明聚类采样是无偏的,总样本中有m种不同分布,用于根据其权重p_i对一个客户端进行采样. 定义$r_{k,i}^t$为客户端i在分布$W_k(t)$中被采样的概率,经过构造有

$$\forall k\in\{1,2,\cdots,m\},\ \sum_{i=1}^{n}r_{k,i}^t=1, r_{k,i}^t\geqslant 0 \tag{5}$$

将假设 1 扩展到m个独立抽样分布$\left\{W_k(t)\right\}_{k=1}^{m}$,得到以下属性:

$$\forall i\in\{1,2,\cdots,n\},\ \sum_{i=1}^{n}r_{k,i}^t=mp_i \tag{6}$$

命题 1 式(5)、式(6)是满足聚类采样是无偏估计的充分条件.

证明 满足式(5)可确保用于聚类采样的m个分布是可行的,当从m个分布$W_k(t)$之一抽取一个客户端时,得到:

$$E_{W_k(t)}=\left[\sum_{j\in W_k(t)}\omega_j\left(W_k(t)\right)\omega_i^t\right]=\sum_{i=1}^{n}r_{k,i}^t\omega_i^t \tag{7}$$

每层的局部模型是由m个分布中选中的客户端聚合形成的,根据期望值的线性关系,由式(7)可得:

$$E_{S_t}\left[\omega^t\right]=\sum_{k=1}^{m}\frac{1}{m}\sum_{i=1}^{n}r_{k,i}^{t}\omega_i^t=\sum_{i=1}^{n}p_i\omega_i^t \tag{8}$$

证毕.

由此可证采用聚类采样可以实现对全部数据的无偏采样.

(2)聚类采样带来的改进

传统的联邦学习在选择参加聚合的客户端时,采用随机采样的方法进行抽取,本节对聚类采样可以降低客户端聚合权重方差并提高客户端代表性进行证明,聚合权重方差越小说明聚合过程越稳定.

首先分析传统随机采样的聚合权重方差. 随机采样中,各客户端的聚合权重等于其样本权重,定义S_{MD}为使用随机采样在第t次迭代中采样客户端子集,在随机抽取的方式中,m个客户端根据伯努利分布$\mathcal{B}(p_i)$被随机抽取,其聚合权重方差可表示为

$$\begin{aligned}\mathrm{Var}_{S_{\mathrm{MD}}}\left[\omega_i\left(S_{\mathrm{MD}}\right)\right]&=\frac{1}{m^2}m\mathrm{Var}\left[\mathcal{B}\left(p_i\right)\right]\\&=\frac{1}{m}p_i\left(1-p_i\right)\end{aligned} \tag{9}$$

分析本文所采用的聚类采样的聚合权重方差. 定义$S_c(t)$为使用聚类采样在第t次迭代中采样客户端子集,其聚合权重方差可表示为

$$\begin{aligned}\mathrm{Var}_{S_C(t)}\left[\omega_i\left(S_C(t)\right)\right]&=\frac{1}{m^2}\sum_{k=1}^{m}\mathrm{Var}\left[\mathcal{B}\left(r_{k,i}^t\right)\right]\\&=\frac{1}{m}p_i\left(1-mp_i\right)\end{aligned} \tag{10}$$

综上所述,$\mathrm{Var}_{S_C(t)}\left[\omega_i\left(S_C(t)\right)\right]\leqslant\mathrm{Var}_{S_{\mathrm{MD}}}\left[\omega_i\left(S_{\mathrm{MD}}\right)\right]$,当且仅当$m=1$时,客户端数据独立同分布相等,由此可证聚类采样可以降低客户端聚合权重方差并提高客户端的代表性.

6.2 FATChain算法收敛性分析

(1)假设

假设2　函数$f(x)$是$L-$smooth平滑的:

$$\text{If }\forall x_1,x_2,$$

$$f\left(x_1\right)-f\left(x_2\right)\leqslant\left(x_1-x_2\right)^{\tau}\nabla f\left(x_2\right)+\frac{L}{2}\left\|x_1-x_2\right\|^2\left(L>0\right) \tag{11}$$

假设3　函数$f(x)$是$\mu-$strongly强凸的:

$$\text{If }\forall x_1,x_2,$$

$$f\left(x_1\right)-f\left(x_2\right)\geqslant\left(x_1-x_2\right)^{\tau}\nabla f\left(x_2\right)+\frac{\mu}{2}\left\|x_1-x_2\right\|^2\left(\mu>0\right) \tag{12}$$

假设4　对于函数$h(\omega)=f(\omega)+\frac{\lambda}{2}\left\|\omega-\omega_0\right\|^2$,$\gamma\in[0,1]$,若$\left\|\nabla h\left(\omega^*\right)\right\|\leqslant\gamma\left\|\nabla h\left(\omega_0\right)\right\|$,则$\omega^*$是$\min_{\omega}h(\omega)$的$\gamma-$不精确解,其中$\nabla h(\omega)=\nabla F(\omega)+\lambda\left(\omega-\omega_0\right)$.

假设5　中心目标$f(\omega)$是有界的,$\min f(\omega)=f\left(\omega_*\right)>-\infty$.

假设6　随机梯度的期望平方范数一致有界:For all t=0, 1, ⋯, T−1,存在一个标量G,使得:

$$E\left\|\nabla F_k\left(\omega_k^t,\varepsilon_k^t\right)\right\|^2\leqslant G^2 \tag{13}$$

假设7　以$\bar{g}_t\left(\omega^t\right)=\sum_{k=1}^{m}S\left(z_k\right)\nabla h_k\left(\omega^t\right)$作为某个层级$m$个客户端的平均梯度,存在$\sigma>0$,使得$\nabla f\left(\omega^t\right)E\left(\bar{g}_t\left(\omega^t\right)\right)\geqslant\sigma\left\|\nabla f\left(\omega^t\right)\right\|^2$,确保局部层$\bar{g}_t\left(\omega^t\right)$的梯度是$\nabla f\left(\omega^t\right)$的估计值,当$\sigma=1$时,$\bar{g}_t\left(\omega^t\right)$的梯度是$\nabla f\left(\omega^t\right)$的无偏估计.

假设8　ε_t^k是从第k个客户端的本地数据中均匀随机采样,每个客户端中,随机梯度方差有界,有

$$\begin{aligned}&\text{For }k=0,1,\cdots,N,\\&E\left\|\nabla F_k\left(\omega_k^t,\varepsilon_k^t\right)-\nabla F_k\left(\omega_k^t\right)\right\|^2\leqslant{\rho_k}^2\end{aligned} \tag{14}$$

定义1　如果函数$f(x)$是$L-$smooth平滑的,则:

$$f\left(x_1\right)-f\left(x_2\right)\leqslant\left\langle\nabla f\left(x_2\right),x_1-x_2\right\rangle+\frac{L}{2}\left\|x_1-x_2\right\|^2 \tag{15}$$

(2)FATChain在非独立同分布数据上理论上收敛到强凸函数的最优解的收敛性证明

定理1　根据假设4本地经验损失函数$h(\omega)$是不精确的,对于层加权聚合模型,$\bar{g}_t\left(\omega^t\right)$是有界的:

$$\mathrm{E}\left\|\bar{g}_t\left(\omega^t\right)\right\|^2\leqslant\gamma^2G^2c^2 \tag{16}$$

其中,c是聚类采样所选出的客户端总数.

证明　设每个局部目标是 γ-不精确的,有

$$\nabla h_k\left(\omega^t\right)=F_k\left(\omega^t\right)+\lambda\left(\omega^t-\omega_0\right) \tag{17}$$

$$\left\|\nabla h_k\left(\omega^t\right)\right\|\leqslant\gamma\left\|\nabla F_k\left(\omega^t\right)\right\| \tag{18}$$

由于$\bar{g}_t\left(\omega^t\right)=\sum_{k=1}^{c}S\left(z_k\right)\nabla h_k\left(\omega^t\right)$,其中$S\left(z_k\right)=\frac{\mathrm{infl}\left(z_k\right)}{\sum_{k=1}^{N}\mathrm{infl}\left(z_k\right)}$,且$S\left(z_k\right)\leqslant1$,所以:

$$\begin{aligned}\left\|\bar{g}_t\left(\omega^t\right)\right\|^2&=\left\|S\left(z_1\right)\nabla\mathrm{h}_1\left(\omega^t\right)+S\left(z_2\right)\nabla h_2\left(\omega^t\right)+\cdots\right.\\&\quad\left.+S\left(z_c\right)\nabla h_c\left(\omega^t\right)\right\|^2\\&\leqslant\left\|\nabla h_1\left(\omega^t\right)+\nabla h_2\left(\omega^t\right)+\cdots+\nabla h_c\left(\omega^t\right)\right\|^2\\&\leqslant m^2\left\|\nabla h_{k^*}\left(\omega^t\right)\right\|^2\left(k^*=\arg\max_k\nabla h_k\left(\omega^t\right)\right)\end{aligned} \tag{19}$$

由式(18)可得:

$$\left\|\bar{g}_t\left(\omega^t\right)\right\|^2\leqslant m^2\gamma^2\left\|\nabla F_{k^*}\left(\omega^t\right)\right\|^2 \tag{20}$$

对式(20)两边取期望,可得:

$$E\left(\bar{g}_t\left(\omega^t\right)\right)^2 \leqslant m^2\gamma^2 E\left(\nabla F_{k^*}\left(\omega^t\right)\right)^2 \leqslant \gamma^2 G^2 c^2$$

证毕.

证明在基于影响力函数的加权聚合条件下,每层局部模型$\bar{g}_t\left(\omega^t\right)$是收敛有界的.

引理1 如果函数$f(x)$是$\mu-$strongly强凸的,根据假设3有

$$2\mu\left(f\left(\omega^t\right)-f\left(\omega_*\right)\right) \leqslant \left\|\nabla f\left(\omega^t\right)\right\|^2 \tag{21}$$

证明 过程参见文献[11].

定理2 当目标函数$f(x)$是$L-$smooth平滑且强凸的,本地经验损失函数$h(\omega)$是不精确的,局部函数$h(\cdot)$是γ-不精确的. 当假设2和假设3成立时,进行T全局更新后,FATchain收敛到全局最优ω_*.

$$E\left[f\left(\omega^T\right)-f(\omega)\right]=\left(1-2\mu \mathrm{B}\eta\sigma\right)^T\left(f\left(\omega^0\right)-f\left(\omega_*\right)\right)+\frac{L}{2}\eta^2\gamma^2B^2G^2c^2 \tag{22}$$

根据定理1在每层加权局部模型有界的条件下,证明定理2的收敛性,其中收敛界限取决于局部约束μ,层间加权参数B,学习率η.

证明 将$\omega^{t+1}=\omega^t-\frac{T_{M+1-m}}{T}\eta\bar{g}_t\left(\omega^t\right)$代入定义1并整理,然后将$B=\frac{T_{M+1-m}}{T}$代入,有

$$f\left(\omega^{t+1}\right)-f\left(\omega^t\right) \leqslant -\nabla f\left(\omega^t\right)^{\top}B\eta\bar{g}_t\left(\omega^t\right)+\frac{L\eta^2}{2}B^2\left\|\bar{g}_t\left(\omega^t\right)\right\|^2 \tag{23}$$

利用定理1,式(23)更新为

$$E\left[f\left(\omega^{t+1}\right)\right]-f\left(\omega^t\right) \leqslant -\nabla f\left(\omega^t\right)^{\top}B\eta E\left[\bar{g}_t\left(\omega^t\right)\right]+\frac{L}{2}\eta^2\gamma^2B^2G^2c^2 \tag{24}$$

利用假设7梯度无偏性有

$$E\left[f\left(\omega^{t+1}\right)\right]-f\left(\omega^t\right) \leqslant -B\eta\sigma\left\|\nabla f\left(\omega^t\right)\right\|^2+\frac{L}{2}\eta^2\gamma^2B^2G^2c^2 \tag{25}$$

利用引理1,有

$$E\left[f\left(\omega^{t+1}\right)\right]-f\left(\omega^t\right) \leqslant -2\mu B\eta\sigma\left(f\left(\omega^t\right)-f\left(\omega_*\right)\right)+\frac{L}{2}\eta^2\gamma^2B^2G^2c^2 \tag{26}$$

通过从两边减去$f\left(\omega_*\right)$并将$f\left(\omega^t\right)$从左向右移动,得到:

$$E\left[f\left(\omega^{t+1}\right)\right]-f\left(\omega_*\right) \leqslant \left(1-2\mu B\eta\sigma\right)\left(f\left(\omega^t\right)-f\left(\omega_*\right)\right)+\frac{L}{2}\eta^2\gamma^2B^2G^2c^2 \tag{27}$$

对式(27)整个取期望,并从两边减去$\frac{L\eta\gamma^2BG^2m^2}{4\mu\sigma}$可得:

$$E\left[f\left(\omega^{t+1}\right)-f\left(\omega_*\right)\right]-\frac{L\eta\gamma^2BG^2c^2}{4\mu\sigma} \leqslant \left(1-2\mu B\eta\sigma\right)\left(E\left[\left(f\left(\omega^t\right)-f\left(\omega_*\right)\right)\right]-\frac{L\eta\gamma^2BG^2c^2}{4\mu\sigma}\right) \tag{28}$$

式(28)左边是公比为$1-2\mu B\eta\sigma$的等比级数,当$t+1=T$时得到式(22). 证毕.

(3)FATChain算法在非独立同分布数据上理论上收敛到非凸函数的全局最优解

定理3 当目标函数$f(x)$是$L-$smooth平滑且非凸的时,本地经验损失函数$h(\omega)$是不精确的,局部函数$h(\cdot)$是γ-不精确的. 当假设1、假设2和假设3成立时,进行全局更新后有:

$$\sum_{t=0}^{T-1}BE\left[\left\|\nabla f\left(\omega_t\right)\right\|^2\right] \leqslant \frac{f\left(\omega^0\right)-f\left(\omega_*\right)}{\eta\sigma}+\frac{L}{2\sigma}T^2\eta\gamma^2BG^2c^2 \tag{29}$$

证明 对式(25)两边取期望,可得:

$$E\left[f\left(\omega^{t+1}\right)\right]-E\left[f\left(\omega^t\right)\right] \leqslant -B\eta\sigma E\left[\left\|\nabla f\left(\omega_t\right)\right\|^2\right]+\frac{L}{2}\eta^2\gamma^2B^2G^2c^2 \tag{30}$$

在全局迭代T上对式(30)求和:

$$E\left[f\left(\omega^{t+1}\right)\right]-f\left(\omega^0\right) \leqslant \sum_{t=0}^{T-1}-B\eta\sigma E\left[\left\|\nabla f\left(\omega_t\right)\right\|^2\right]+\frac{L}{2}T^2\eta^2\gamma^2B^2G^2c^2 \tag{31}$$

由于$\min f\left(\omega^t\right)=f\left(\omega_*\right) \leqslant E\left[f\left(\omega^{t+1}\right)\right]$,因此有:

$$f\left(\omega_*\right) \leqslant f\left(\omega^0\right)-\sum_{t=0}^{T-1}B\eta\sigma E\left[\left\|\nabla f\left(\omega_t\right)\right\|^2\right]+\frac{L}{2}T^2\eta^2\gamma^2B^2G^2c^2 \tag{32}$$

重新整理公式可得式(29). 证毕.

7 性能分析

7.1 仿真场景及参数设置

(1)实验环境

在虚拟机中Ubuntu 18.04.1 LTS搭建联邦学习系统,采用联盟链FISCO BCOS模拟系统中的区块链系统,使用Solidity语言编写智能合约,采用Python SDK实现联邦学习任务与区块链之间的交互,包括访问FISCO BCOS节点的Python API,支持节点部署和调用合约等功能. 学习模型采用Python 3.7.11和Tensorflow2.0.0编写.

(2)数据集

采用MNIST[32]和CIFAR-10[33]数据集. MNIST数据集,包含60 000个示例的训练集和10 000个示例的测试集. 每个示例都是1个28像素×28像素的灰度图像,与10个类别的标签相关联,代表0~9之间的手写数字;CIFAR-10数据集包含60 000张32像素×32像素的彩色图像,分为10个类别,每类有6 000张图像. 其中有50 000张训练图像和10 000张测试图像. 上述两种数据集分别划分为50个客户端,并对数据集进行数据异构设置,数据异构参考文献[34],每次通信的用户数量为25.

(3)学习模型

采用典型的卷积神经网络模型LeNet作为联邦学习系统性能测试任务发布的初始模型来对图像进行分类. 网络框架包括3个卷积层、2个池化层、2个全连接层,其中卷积层的卷积核大小为55,激活函数为ReLU.

(4)联邦学习训练设置

实验设置了FedAvg[4]、FedAsync[10]、FedAT[11]与FATChain进行比较,见表2.

表2　训练设置

参数	取值
学习率	0.001 5
批量大小	64
全局通信轮次epochs	150
局部更新步骤t	10

(5)区块链仿真环境设置

仿真环境设置见表3.

表3　仿真环境设置

参数	取值
任务发布节点数量	1
联邦学习群组	6
每组中的验证节点	3
模型聚合群组中的参与方节点	10
每组通过聚类采样选举的客户端	5

(6)模拟不同性能层

联邦学习的客户端通常是边缘设备,其计算能力和网络连接可能不稳定,简单地分配固定数量的资源不足以反映真实情况. 因此,在整个训练过程中为每个客户端分配一个CPU,并在客户端进行的计算中添加随机延迟. 增加的随机延迟是为了模拟不同级别的落后者效应,这些效应是由现实世界联邦学习设置中较弱的计算能力和间歇性网络连接引起的. 首先将所有客户端平均分为5个部分,然后在每轮中分别为每个部分的客户端随机分配0 s、0~10 s、10~20 s、20~30 s、30~40 s的延迟.

(7)攻击设置

假设在联邦学习训练过程中存在一些控制了部分参与节点的恶意攻击者,攻击者在学习过程中可任意操纵其控制节点上传的本地模型参数,以降低全局模型的收敛速度和收敛精度. 为模拟上述攻击场景,我们设置常见的投毒攻击方式,模拟联邦学习中存在的恶意局部代理. 抗攻击实验中设有25个客户端,其中包含0~15个恶意局部代理,这些恶意局部代理通过向自身训练集中注入中毒数据,具体设置如文献[35],来模拟投毒攻击.

7.2　实验结果分析

(1)全局模型准确率

为了衡量整体框架设计对于全局模型准确性的影响,给定相同的参数设定及实验环境,首先将本文方案与其他联邦学习方案的全局模型准确率.

首先比较FedAvg、FedAsync、FedAT、FATChain这4种算法在MNIST数据集下10~150次模型聚合中的准确率. 如图4所示,可以看出在FATChain方案下全局模型准确率最高,达到了91.68%;FedAvg、FedAsync、FedAT算法下的全局模型准确率分别为88.31%、87.72%、89.25%. FATChain方案较其他方案准确率分别提高了3.68%、4.31%、2.65%. 同时由图4、图5可以看出,FATChain方案下全局模型收敛最快,预测性能最好.

FedAvg、FedAsync、FedAT、FATChain这4种算法在CIFAR-10数据集下的准确率,结果与在MNIST数据集下的结果相似,FATChain方案在模型准确率和收敛速度上得到了较大的提升. 如图6所示,可以看出在FATChain方案下全局模型准确率最高,达到了63.99%;FedAvg、FedAsync、FedAT算法下的全局模型准确率分别为59.62%、58.01%、61.27%.FATChain方案较其他方案准确率分别提高了6.83%、9.35%、4.44%. 同时由图6、图7可以看出,FATChain方案下全局模型收敛最快,预测性能最好.

(2)训练损失对比

为了进一步衡量整体框架的性能,比较FedAvg、FedAsync、FedAT、FATChain4种算法在MNIST、CIFAR-10数据集下的训练损失,由图5、图7可知,本文方案在稳定性和收敛性上具有明显优势.

(3)所有客户端之间测试准确率的平均方差

在联邦学习场景中,考察所有客户端之间测试准确率的平均方差是了解模型性能一致性的重要指标. 平均方差较小意味着客户端间的模型性能相对一致,较大的平均方差则可能暗示模型在不同客户端上的表现差异较大,这是由于不同客户端数据和资源的异构性引起了落后者效应.

表4、表5展示的是4种联邦学习算法在MNIST和CIFAR-10数据集下,每个模型达到收敛后的最佳预测精度Accuracy,以及所有客户端之间测试准确性的平均

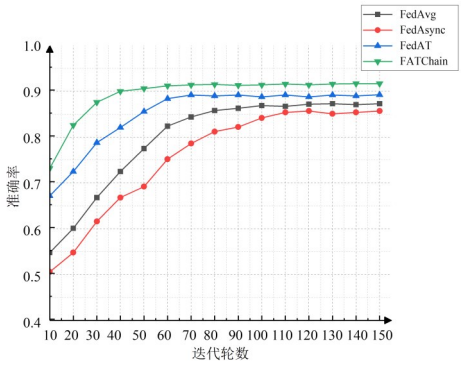

图4 MNIST数据集下4种联邦学习算法准确率对比图

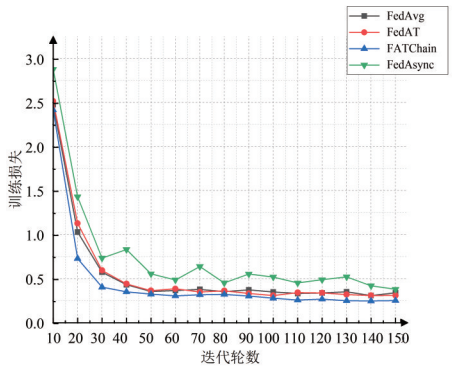

图5 MNIST数据集下4种联邦学习算法训练损失对比图

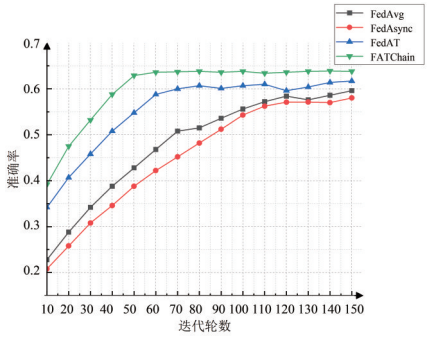

图6 CIFAR-10数据集下4种联邦学习算法准确率对比图

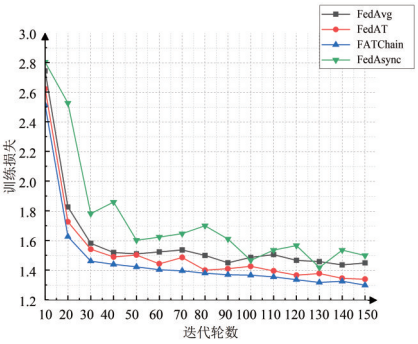

图7 CIFAR-10数据集下4种联邦学习算法训练损失对比图

表4 4种联邦学习算法在MNIST数据集2类非独立同分布上的性能比较

联邦学习算法	Accuracy	Abs.Var.
FedAvg	0.883 1	1.86
FedAsync	0.877 2	2.01
FedAT	0.892 5	1.18
FATChain	0.916 8	1.00

表5 4种联邦学习算法在CIFAR-10数据集2类非独立同分布上的性能比较

联邦学习算法	Accuracy	Abs.Var.
FedAvg	0.596 2	2.03
FedAsync	0.580 1	2.01
FedAT	0.612 7	1.26
FATChain	0.639 9	1.00

方差Abs.Var.,并标准化为FATChain的方差.FATChain在所有实验中始终具有最低的准确度方差.FedAvg、FedAsync观察到明显更高的准确率方差.分析原因,是因为客户端设备的异构产生了落后者效应.由于落后的客户接受的训练比较少,从而造成全局模型的巨大波动.同时客户端数据的非独立同分布也会造成客户端模型性能相差较大,从而导致全局模型的不稳定.而本文在采用异步分层联邦学习算法,减少客户端设备异构造成影响的同时,基于聚类采样的用户选择算法保证了那些具有独特数据分布的客户可以被选中,从而实现更平滑的全局模型收敛.

(4)区块链性能分析

评估区块链模型聚合服务所需要的平均存储开销和时延.如图8、图9所示,实验表明,使用区块链进行存证,并不会给联邦学习带来显著的时间与空间损耗.区块链的引入在提供可信存证与可追溯聚合过程的同时,不会造成系统的性能瓶颈.

(5)聚类采样算法的有效性

在CIFAR-10和MNIST数据集下,对分层联邦学习算法中,采用聚类采样选择每层参与训练的客户端和采用随机抽样选择每层参与训练的客户端,对这两种用户选择方式产生的最佳测试准确率进行对比,如图10、图11所示.实验表明,采用聚类采样算法相较于随机采样拥有更高的模型训练准确率,同时达标目标精度所需时间也更少.聚类采样保证了那些具有独特数据分布的客户可以被选中,提升了联邦学习训练的准确率,并加速了全局模型的收敛.

(6)自适应加权聚合算法对性能的影响

分析基于影响力函数的自适应加权聚合策略对联邦学习性能上的影响.比较联邦学习系统在MNIST和CIFAR-10数据集下,层内是否采用加权聚合算法对模型训练准确率的影响,如图12、图13所示,采用加权聚

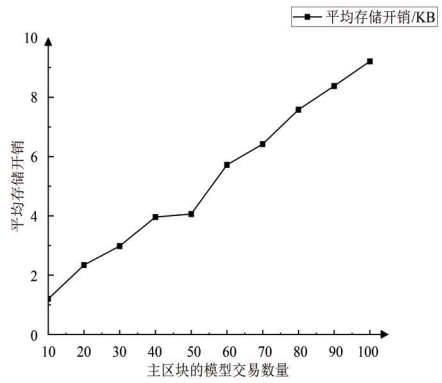

图8　平均存储开销随着区块模型交易数量变化的趋势

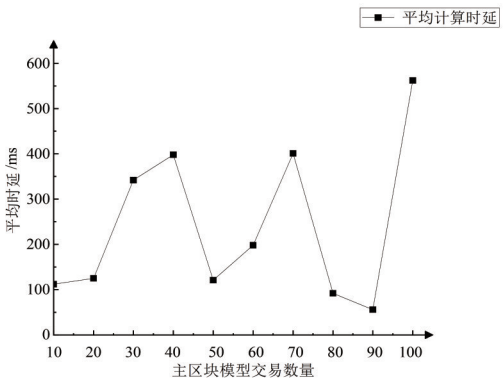

图9　平均时延随着区块模型交易数量变化的趋势

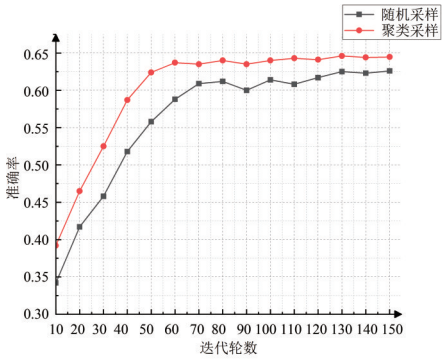

图10　CIFAR-10数据集下采用聚类采样和随机采样准确率比较

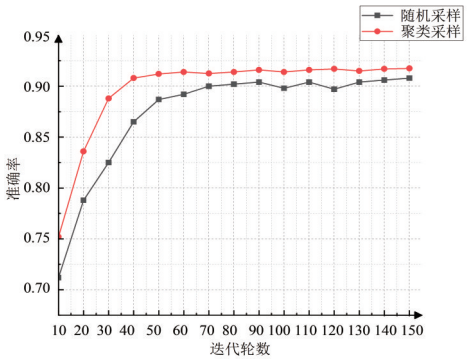

图11　MNIST数据集下采用聚类采样和随机采样准确率比较

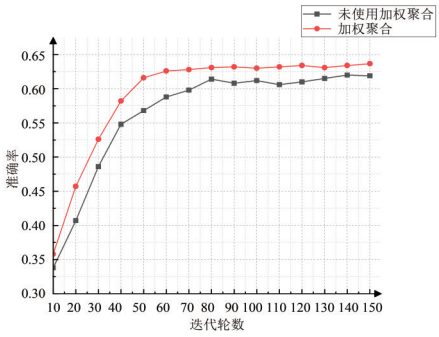

图12　CIFAR-10数据集下加权聚合算法对模型训练的准确率比较

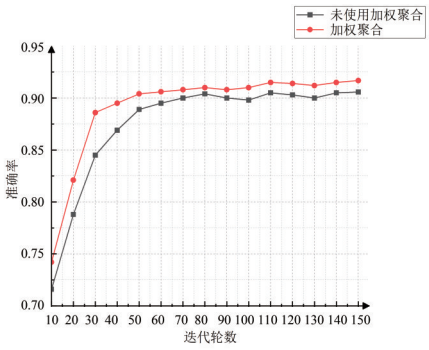

图13　MNIST数据集下加权聚合算法对模型训练的准确率比较

合算法拥有更高的模型训练准确率且收敛得更快. 这是因为数据异构会引起局部模型差异,而传统联邦学习基于数量的加权平均算法,会导致低质量的局部模型权重过高,从而影响收敛速度和全局模型精度的问题. 本文将聚合分为层内局部聚合和层间加权聚合,设计了基于影响力函数的加权聚合算法. 该算法根据模型质量和更新频率所产生的影响力因子来调整模型聚合权重,有助于模型的收敛. 层间根据层更新全局模型的次数动态调整分配给每个层的相对权重,从而帮助全局训练更快地收敛.

(7)抗投毒攻击能力

首先分析验证节点对上传的本地更新模型进行验证时,其阈值设置对全局模型准确率的影响,验证节点接收到的本地更新,经验证后得到最高的准确率p,当准确率在$p(1-k)$以下时,将会被过滤,不参与聚合. 通过实验分析当恶意节点数为3时,k取值为多少时,该框架在MNIST数据集下收敛后的最佳预测精度. 如表6所示,可以看出k值越大,预测精度越高,通常情况下,设置为k=20%.

下面分析FATChain在抗攻击方面的优势. 比较一

表6 验证节点阈值设置

参数	Accuracy
$k=5\%$	0.905 4
$k=10\%$	0.909 7
$k=15\%$	0.913 2
$k=20\%$	0.914 8

般的联邦学习算法FedAvg和本文方案分别在客户端中存在恶意节点的和不存在恶意节点的条件下模型训练的准确度,设置为k=20%,如表7所示.

表7 联邦学习算法抗恶意节点攻击的能力

恶意节点数/个	全局模型准确率	
	FedAvg	FATChain
0	0.883 1	0.916 3
3	0.298 1	0.914 8
6	0.217 5	0.897 9
9	0.199 2	0.908 6
12	0.163 5	0.912 3
15	0.142 4	0.915 1

从表7中可以看出,在恶意节点投毒攻击下,FedAvg基本上完全发散,模型预测精确率一直在降低.在恶意节点为15的情况下,FedAvg准确率下降69.68%,说明投毒对一般联邦学习算法的模型训练的准确率和全局模型的收敛速度及平缓程度影响非常大,这是因为投毒攻击可以通过篡改数据或注入有毒数据影响目标节点的模型精度,从而影响全局模型收敛.而对FATChain的影响较少,这是因为FATChain中,结合区块链去中心化以及通过设置模型过滤智能合约,过滤掉不合格的局部模型,以及利用区块链上的监管机制,可以抑制恶意节点,预防投毒攻击,保证联邦学习模型的性能和隐私安全.

(8)可扩展性分析

下面深入分析FATChain框架的可扩展性.对比在LeNet模型上不同数量客户端在MNIST和CIFAR-10数据集下的模型训练准确率和训练时间,如图14、图15、表8、表9所示.实验结果表明,当客户端数量大幅度增加时,FATChain框架依然能够保持稳定且较高的模型准确率,同时通过与基线算法FedAvg扩展客户端数量对达到目标准确率所需时间相比,反映出相同条件下,FATChain框架具有更高的训练效率,这表明FATChain框架具有很好的可扩展性.这是因为FATChain框架将被选中客户端按响应速度分组,通过分层桥接的方式将同步和异步训练相结合,同时通过聚类采样算法,保证了具有独特数据分布的客户可以被选中,并有效降低全局同步的压力,使得框架可以支持更多的客户端.

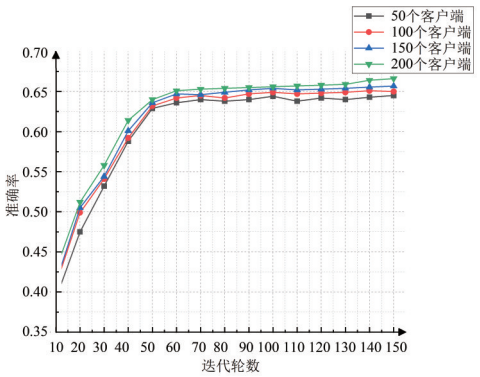

图14 CIFAR-10数据集下不同数量客户端对模型训练的准确率比较

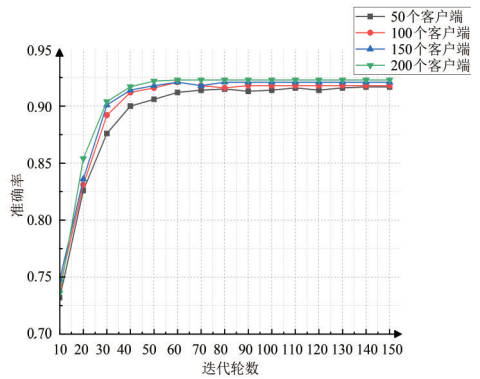

图15 MNIST数据集下不同数量客户端对模型训练的准确率比较

表8 联邦学习算法在CIFAR-10数据集下达到目标精度所需时间对比 单位:s

联邦学习算法	CIFAR-10数据集达到目标准确率(0.45±0.012)所需时间	
	50个客户端	100个客户端
FedAvg	1 021	1 563
FATchain	845	1 014

表9 联邦学习算法在MNIST数据集下达到目标精度所需时间对比 单位:s

联邦学习算法	MNIST数据集达到目标准确率(0.772±0.008)所需时间	
	50个客户端	100个客户端
FedAvg	868	1 384
FATchain	518	752

(9)其他方案对比分析

如表10所示,本文具有相对完善的安全防护体系.本文方案无论在安全性和性能上都相较于其他方案有了很大的提升.

表10　方案对比

方案	区块链技术	去中心化	可溯源	抗单点攻击	抗投毒攻击	推理攻击	抗客户端异构性	抗通信瓶颈
文献[14]	×	×	×	×	√	×	×	×
文献[15]	×	×	×	×	√	√	×	×
文献[22]	√	×	√	×	√	×	×	×
文献[24]	√	√	√	√	×	×	×	×
文献[25]	√	√	√	√	×	×	×	×
本文方案	√	√	√	√	√	√	√	√

8　结论

本文提出了一种基于区块链的高性能、安全的去中心化分层异步联邦学习模型FATChain,该模型与区块链相结合,实现联邦学习的去中心化,解决了单点攻击、投毒攻击、推理攻击的安全性问题;同时采用区块链群组结构,将联邦学习客户端依照响应快慢,分成不同群组,响应速度相似的群组内部同步地进行模型局部更新,响应速度相差较大的不同群组,异步地进行全局更新,使得联邦学习系统最大限度地减少了落后者效应,解决了客户端异构与通信瓶颈的问题. 模型引入聚类采样,选择用于更具有代表性的数据样本的客户端,从而优化数据非独立同分布问题;设计了一种更为全面有效的、基于影响力函数的加权聚合方式,优化了联邦学习的准确率.

然而基于区块链的分层联邦学习模型仍存在一些不足,缺乏鼓励参与方提供高质量数据的激励机制. 在接下来的研究中,将着重设计公平的、高效率的激励机制,以更好地确保联邦学习的效率和隐私安全.

参考文献

[1] MCMAHAN H B, YU F X, RICHTARIK P, et al. Federated learning: Strategies for improving communication efficiency[EB/OL]. (2016-10-18) [2024-12-01]. https://arxiv. org/abs/1610.05492.

[2] RESIZADEH A, MOKHTARI A, HASSANI H, et al. Fedpaq: A communication-efficient federated learning method with periodic averaging and quantization[EB/OL]. (2019-09-28)[2024-12-01]. https://arxiv.org/abs/1909.13014.

[3] CHEN Y J, NING Y, SLAWSKI M, et al. Asynchronous online federated learning for edge devices with non-IID data[C]//2020 IEEE International Conference on Big Data. Piscataway: IEEE, 2020: 15-24.

[4] LI X, HUANG K, YANG W, et al. On the convergence of fedavg on non-iid data[EB/OL]. (2016-10-18)[2024-12-01]. https://arxiv.org/abs/1907.02189.

[5] WANG Z B, SONG M K, ZHANG Z F, et al. Beyond inferring class representatives: User-level privacy leakage from federated learning[C]//IEEE INFOCOM 2019 - IEEE Conference on Computer Communications. New York: ACM, 2019: 2512-2520.

[6] PAPERNOT N, MCDANIEL P, JHA S, et al. The limitations of deep learning in adversarial settings[C]//2016 IEEE European Symposium on Security and Privacy. Piscataway: IEEE, 2016: 372-387.

[7] CAO D, CHANG S, LIN Z J, et al. Understanding distributed poisoning attack in federated learning[C]//2019 IEEE 25th International Conference on Parallel and Distributed Systems. Piscataway: IEEE, 2019: 233-239.

[8] TOLPEGIN V, TRUEX S, GURSOY M E, et al. Data poisoning attacks against federated learning systems[C]//Computer Security-ESORICS 2020. Cham: Springer, 2020: 480-501.

[9] CARLINI N, LIU C, KOS J, et al. The secret sharer: Measuring unintended neural network memorization & extracting secrets[EB/OL]. (2018-02-22)[2024-12-01]. https://arxiv.org/abs/1802.08232.

[10] XIE C, KOYEJO S, GUPTA I, et al. Asynchronous federated optimization[EB/OL]. (2019-03-10) [2024-12-01]. https://arxiv.org/abs/1903.03934.

[11] CHAI Z, CHEN Y J, ANWAR A, et al. FedAT: A high-performance and communication-efficient federated learning system with asynchronous tiers[C]//Proceedings of the International Conference for High Performance Computing, Networking, Storage and Analysis. New York: ACM, 2021: 1-16.

[12] 杨庚, 王周生 . 联邦学习中的隐私保护研究进展[J]. 南京邮电大学学报(自然科学版), 2020, 40(5): 204-214.
YANG G, WANG Z S. Survey on privacy preservation in federated learning[J]. Journal of Nanjing University of Posts and Telecommunications (Natural Science Edition), 2020, 40(5): 204-214. (in Chinese)

[13] MELIS L, SONG C, DE CRISTOFARO E, et al. Inference attacks against collaborative learning[EB/OL]. (2018-03-01)[2024-12-01]. https://www. researchgate. net/publication/325074745_Inference_Attacks_Against_Collaborative_Learning.

[14] SONG C Z, RISTENPART T, SHMATIKOV V. Machine learning models that remember too much[C]//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2017: 587-601.

[15] QIU F Y, YANG H, ZHOU L, et al. Privacy preserving federated learning using CKKS homomorphic encryption[C]// Wireless Algorithms, Systems, and Applications. Cham: Springer, 2022: 427-440.

[16] SUN J, LI A, DIVALENTIN L, et al. Fl-wbc: Enhancing robustness against model poisoning attacks in federated learning from a client perspective[EB/OL]. (2021-10-26)[2024-12-01]. https://arxiv.org/abs/2110.13864.

[17] CHOUDHURY O, GKOULALAS-DIVANIS A, SALONIDIS T, et al. Differential privacy-enabled federated learning for sensitive health data[EB/OL]. (2019-10-07) [2024-12-01]. https://arxiv.org/abs/1910.02578.

[18] LANG N, SOFER E, SHAKED T, et al. Joint privacy enhancement and quantization in federated learning[J]. IEEE Transactions on Signal Processing, 2023, 71: 295-310.

[19] GEYER R C, KLEIN T, NABI M. Differentially private federated learning: A client level perspective[EB/OL]. (2024-03-20) [2024-12-01]. https://arxiv. org/abs/2405.08299.

[20] LEBRUN T, BOUTET A, AALMOES J, et al. MixNN: Protection of federated learning against inference attacks by mixing neural network layers[C]//Proceedings of the 23rd ACM/IFIP International Middleware Conference. New York: ACM, 2022: 135-147.

[21] 刘飚, 张方佼, 王文鑫, 等. 基于矩阵映射的拜占庭鲁棒联邦学习算法[J]. 计算机研究与发展, 2021, 58(11): 2416-2429. LIU B, ZHANG F J, WANG W X, et al. A Byzantine-robust federated learning algorithm based on matrix mapping[J]. Journal of Computer Research and Development, 2021, 58(11): 2416-2429. (in Chinese)

[22] KANG J W, XIONG Z H, JIANG C X, et al. Scalable and communication-efficient decentralized federated edge learning with multi-blockchain framework[C]//Blockchain and Trustworthy Systems. Singapore: Springer, 2020: 152-165.

[23] MAJEED U, HONG C S. FLchain: Federated learning via MEC-enabled blockchain network[C]//2019 20th Asia-Pacific Network Operations and Management Symposium. Piscataway: IEEE, 2019: 1-4.

[24] LI Y Z, CHEN C, LIU N, et al. A blockchain-based decentralized federated learning framework with committee consensus[J]. IEEE Network, 2021, 35(1): 234-241.

[25] MENDIS G J, SABOUNCHI M, WEI J, et al. Blockchain as a service: an autonomous, privacy preserving, decentralized architecture for deep learning[EB/OL]. (2018-07-05)[2024-12-01]. https://www.catalyzex.com/paper/blockchain-as-a-service-an-autonomous-privacy.

[26] BONAWITZ K, EICHNER H, GRIESKAMP W, et al. Towards federated learning at scale: System design[C]// Proceedings of Machine Learning and Systems 1. Cambridge: MLSys, 2019: 374-388.

[27] NGUYEN J, MALIK K, ZHAN H, et al. Federated learning with buffered asynchronous aggregation[C]//International Conference on Artificial Intelligence and Statistics. Cambridge: PMLR, 2022: 3581-3607.

[28] FRABONI Y, VIDAL R, KAMENI L, et al. Clustered sampling: Low-variance and improved representativity for clients selection in federated learning[C]//International Conference on Machine Learning. Cambridge: PMLR, 2021: 3407-3416.

[29] RICHARDSON A, FILOS-RATSIKAS A, FALTINGS B. Rewarding high-quality data via influence functions[EB/OL]. (2019-08-30) [2024-12-01]. https://arxiv. org/abs/1908.11598.

[30] KIM H, PARK J, BENNIS M, et al. Blockchained on-device federated learning[J]. IEEE Communications Letters, 2020, 24(6): 1279-1283.

[31] BHAGOJI A N, CHAKRABORTY S, MITTAL P, et al. Analyzing federated learning through an adversarial lens[C]//International Conference on Machine Learning. Cambridge: PMLR, 2019: 634-643.

[32] DENG L. The MNIST database of handwritten digit images for machine learning research [best of the web[J]. IEEE Signal Processing Magazine, 2012, 29(6): 141-142.

[33] KRIZHEVSKY A. Learning multiple layers of features from tiny images[EB/OL].(2009-04-08)[2024-12-01]. http://www.cs.utoronto.ca/~kriz/learning-features-2009-TR.pdf.

[34] YOSHIDA N, NISHIO T, MORIKURA M, et al. Hybrid-FL for wireless networks: Cooperative learning mechanism using

non-IID data[C]//ICC 2020 - 2020 IEEE International Conference on Communications. Piscataway: IEEE, 2020: 1-7.

[35] FANG M, CAO X, JIA J, et al. Local model poisoning attacks to Byzantine-robust federated learning[C]//Proceedings of the 29th USENIX Conference on Security Symposium. New York: ACM, 2020: 1623-1640.

作者简介

胡荣磊　男,1977年2月出生于河北省衡水景县. 现为北京电子科技学院电子与通信工程系副研究员、硕士生导师. 主要研究方向为保密通信、物联网安全、区块链安全、隐私保护、联邦学习等. 中国电子学会会员编号:E190182822M.

E-mail: huronglei@sina.com

刘思惠　女,2000年8月出生于吉林省吉林市. 现为北京电子科技学院新一代电子信息技术专业硕士研究生. 主要研究方向为联邦学习.

E-mail: lsh15543255168@163.com