文章编号： 1671-7449(2025)03-0291-07　　J. Test Measur. Technol., 2025, 39(3): 291-297.

基于区块链声誉管理的安全公平的联邦学习

范志强[1]，张志才[2*]

（1. 山西大学 物理电子工程学院，山西 太原 030006；2. 海南大学 计算机科学与技术学院，海南 海口 570228）

摘　要： 联邦学习(Federated Learning，FL)作为一种安全的分布式学习框架，可以有效保护参与者的数据隐私，引起了物联网领域的广泛兴趣。然而，传统的FL架构在某种程度上是集中式的，需要一个中央服务器来负责模型的更新和聚合。这种集中式结构容易受到单点攻击，可能导致整个FL系统瘫痪，同时也易受到搭便车者的攻击，从而影响公平性和安全性。为了解决这些问题，提出了一个与传统的集中式管理结构不同的完全分布式结构。通过一个具有不可否认和抗篡改特性的联盟区块链来分散管理来自客户端的本地模型。此外，还在区块链中引入了对于客户端的声誉评估以防范搭便车者的攻击，并根据不同的声誉值给予诚实参与者不同的奖励。实验表明：该方法可以实现较高的公平性，并且可以有效地识别和排除搭便车者。

关键词： 联邦学习；搭便车攻击；区块链；声誉评估

中图分类号： TP181　　**文献标识码：** A　　**doi:** 10.62756/csjs.1671-7449.2025036

引用格式： 范志强，张志才. 基于区块链声誉管理的安全公平的联邦学习[J]. 测试技术学报，2025，39(3)：291-297.

FAN Zhiqiang，ZHANG Zhicai. Secure and fair federated leaning based on blockchain reputation management[J]. Journal of Test and Measurement Technology，2025，39(3)：291-297.

Secure and Fair Federated Leaning Based on Blockchain Reputation Management

FAN Zhiqiang[1]，ZHANG Zhicai[2*]

（1. College of Physics and Electronic Engineering，Shanxi University，Taiyuan 030006，China；
2. School of Computer Science and Technology，Hainan University，Haikou 570228，China）

Abstract： Federated learning (FL)，as a secure distributed learning framework，has attracted widespread interest in the field of the Internet of Things (IoT) because it can effectively protect the data privacy of participants. However，the traditional FL architecture is，to some extent，centralized and requires a central server to be responsible for model updates and aggregation. This centralized structure is susceptible to single-point attacks，which may cause the entire FL system to crash，and is also vulnerable to attacks from free riders，thereby affecting fairness and safety. To address these challenges，a completely distributed structure that is different from traditional centralized management structures is proposed. The local model from clients is decentralized and managed through a consortium blockchain with undeniable and tamper-resistant features. In addition，the reputation evaluation for clients is introduced in the block-chain to prevent attacks from hitchhikers，and honest participants with different rewards are rewarded based on different reputation values. The experiment results show that this method can achieve high fairness and

收稿日期： 2024-07-03

作者简介： 范志强(1999—)，男，硕士生，主要从事联邦学习、算网融合研究。E-mail：202222617007@email.sxu.edu.cn。

***通信作者：** 张志才(1982—)，男，讲师，博士，主要从事人机物系统、分布式机器学习研究。E-mail：zzcai@hainanu.edu.cn。

identify and exclude free riders effectively.

Key words: federated learning; hitchhiking attacks; blockchain; reputation assessment

0 引 言

联邦学习(Federated Learning, FL)是一种协作式机器学习范式，其目标是所有客户端集体训练一个高质量的全局模型，同时训练数据仍然分布在客户端上[1-2]。每个客户端拥有的数据是私有的，不能转移到其他客户端或服务器。因此，每个客户端通过共享其数据的更新而不是共享数据本身来参与FL。这使得FL特别适用于那些数据安全至关重要的领域中的机器学习应用程序，例如医疗领域和车联网等。

FL还有以下优点：由于训练数据集不再被共享，客户端可以保护其训练数据集的隐私；由于训练的模型通常小于训练数据，与在客户端和服务器之间共享数据的情况相比，FL中的通信负载明显减少；没有大型训练数据集或强大计算资源的客户端仍然可以通过使用他们的本地训练数据集和计算资源[3]在FL中集体训练一个全局模型。

在FL中，客户端利用本地计算能力来训练由服务器协调的共享模型，以迭代训练的方式完成学习任务，而不共享任何用户的原始数据[4]。常规FL的标准程序如图1所示：在每次迭代开始时，中央服务器将初始的全局模型分发给选定的用户；所选用户基于所接收的全局模型并行地使用其本地数据执行本地模型训练，然后将本地模型参数上传到中央服务器；中央服务器聚合这些本地模型参数以生成一个新的全局模型，迭代循环到全局模型收敛为止。

然而，传统的集中式FL系统存在以下缺点：1)隐私风险[5]：在传统集中式FL系统中，用户的数据通常需要被集中到一个中心服务器进行模型训练，这可能导致用户数据的隐私泄露。即使采用加密等手段保护数据，仍然存在数据在传输过程中被攻击者窃取的风险。2)单点故障[2]：中心服务器作为唯一的数据聚合和模型更新节点，一旦中心服务器发生故障或遭受攻击，整个系统将无法正常运行。3)搭便车攻击：搭便车攻击是一种被动攻击模式，即参与FL的用户使用服务器发布的全局模型更新本地模型，但拒绝向服务器提供有价值的本地信息。

从中央服务器或者全局的角度考虑，这种搭便车的行为可能会导致以下问题：1)联合训练的模型更容易降低全局模型的准确性；2)搭便车者获得泄漏梯度或局部更新重建个人数据，然后进行模型反演；3)一些搭便车行为会导致不公平的训练，降低诚实参与者的奉献愿望。

并且诚实的客户端更愿意与具有可靠性和公平性的中央服务器合作，所以中央服务器需要建立信任和良好的声誉。因此，如何解决传统集中式FL系统的问题和防御搭便车攻击成为亟待解决的关键问题。

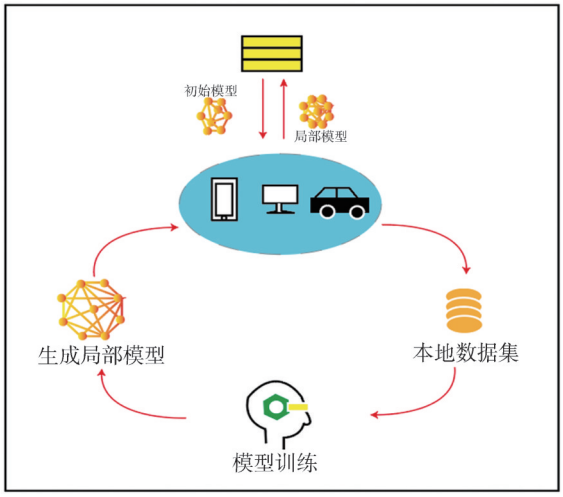

图1 联邦学习过程

Fig. 1 Federated leaning process

为了解决上述问题，本文提出了一个与传统集中式管理结构不同的完全分布式结构。并且，在区块链上引入了关于客户端声誉的计算，并根据不同声誉给予诚实参与者不同的奖励，同时识别和排除搭便车攻击者。此外，利用具有不可否认和抗篡改特性的联盟区块链，以分散的方式管理来自任务发布者的声誉意见。联盟区块链是一种更高效、更实用的区块链技术，具备轻量、高速的共识过程，由预先选择的矿工控制。因其上述优势，联盟区块链特别适用于移动网络中FL的声誉管理。

1 相关工作

1.1 区块链

区块链与FL结合成为当前研究的热点趋势，因为其去中心化框架为学习过程提供了额外的隐

私和安全保障。LÜ 等[6]首次在区块链辅助的去中心化深度学习框架下对联邦学习的公平性进行了调查，设计了一个局部可信度相互评估机制来加强公平性，并开发了一种三层在线式加密方案以保证准确性和隐私性。Aich 等[7]提出了使用 FL 和区块链技术创建一个平台供专业人员访问医疗保健数据的建议，然而文中只提出了体系结构，没有任何关于实现或测试的数据。Kim 等[8]提出了一种区块链 FL（BlockFL，BFL）架构，其中移动设备的本地学习模型更新通过区块链进行交换和验证。本地模型更新是对用户设备上可用的数据样本执行的，并在区块链上以块的形式积累。全局模型更新也由用户设备从最新的块计算，从而建立了设备上 FL 的概念。他们考虑了全局学习模型的可伸缩性、鲁棒性和延迟最小化，最后对延迟的端到端进行了数学分析。Toyoda 等[9]介绍了现有 BFL 研究工作中采用的区块链技术的类别和平台，并对各种 BFL 框架进行了比较。Hou 等[10]对一些流行的 BFL 框架、底层 BFL 基础设施和 BFL 的应用进行了比较和总结。Wahab 等[11]针对 FL 进行了一项全面的调查，其中比较分析涵盖了架构范式、通信效率、激励机制、隐私保护和安全聚合方案等方面，还纳入了对某些 BFL 架构的调查。Nguyen 等[12]探讨了区块链与 FL 的融合，同时考虑了移动边缘计算场景中的通信成本和资源分配。

1.2　搭便车攻击与防御

搭便车攻击是 FL 中普遍存在的基本问题，已被许多学者研究。Lin 等[13]提出了针对 FL 的搭便车攻击的概念，并探讨了攻击者在不需要局部训练数据的情况下构建梯度更新的可能方法。此外，还提出了一种新的模型参数高维异常检测方法（STD-DAGMM），该方法将局部梯度更新矩阵的标准偏差（STD）度量与深度自编码高斯混合模型（Deep Autoencoding Gaussian Mixture Model，DAGMM）相结合，通过更新模型参数特征来检测异常值（搭便车者）。然而，当搭便车车的数量超过 20% 时，检测精度急剧下降。Fraboni 等[14]定义了两种类型的搭便车攻击（表示原始方法）：一种是普通的搭便车攻击，其目标是直接返回到全局模型中，并将每一轮攻击中获得的参数替换为随机数；另一种是伪装的搭便车攻击，其目标是在每一轮获得的全局模型参数中加入随机高斯噪声。Wang 等[15]提出了一种实用的搭便车攻击检测方法，但可能无法完全识别所有的搭便车攻击者，对于高级攻击者，他们可能采取更隐蔽的方式来规避检测随后，Xu 等[16]设计了双重安全保证矩阵分解（Double Security Guaranteed Matrix Factorization，DSGMF）方法，它从客户贡献的角度识别并消除了潜在的搭便车者，从而确保了模型的安全性。

本文通过将区块链与激励机制相结合，利用区块链的分散和防篡改特性，将数据块中的声誉意见作为持久和透明的证据。对于特定的移动设备，任务发布者将其直接声誉意见与最新间接声誉意见整合，从而为移动设备生成综合声誉值。这样可以确保声誉意见的可信度和准确性，并为移动设备提供更加可靠的声誉评估依据。通过可靠的声誉评估，根据不同的声誉给予诚实参与者不同的奖励，并且识别和消除搭便车攻击者。

2　系统模型

本文提出了一个与传统集中式管理结构不同的完全分布式结构，系统模型如图 2 所示，主要利用区块链代替了传统 FL 中的中央服务器，并在区块链上引入了关于客户端声誉值的计算。

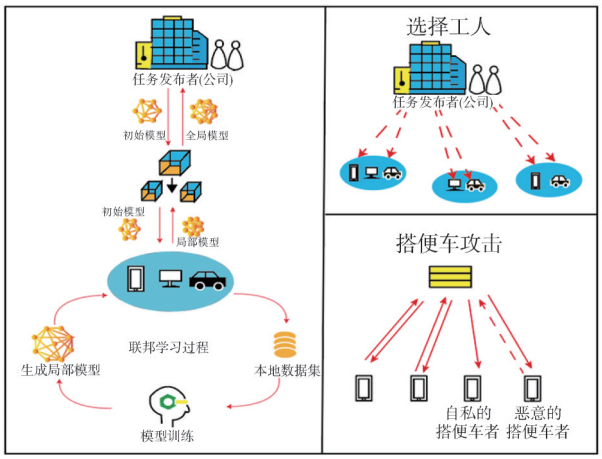

图 2　系统模型

Fig. 2　System model

2.1　传统的联邦学习

在 FL 系统中，各个客户端在中央服务器的协调下进行训练。FedAvg 是一种基于本地模型参数聚合的迭代训练策略。在迭代训练的每一轮，中央服务器将初始的全局模型分发给所有客户端，并汇总本地模型更新，然后，生成一个新的全

局模型。设在一个典型的基于随机梯度下降(Stochastic Gradient Descent, SGD)的训练条件中，有1个中央服务器和n个客户端$C_1, C_2, \cdots, C_n$，每个客户端都有各自的本地私有训练数据集D_i，数据集中训练样本的数量为N_i。在第t轮（t=0, 1, 2, …），中央服务器将当前全局模型$\varpi(t)$分发给各个客户端。客户端C_i以全局模型$\varpi(t)$为初始模型参数进行E轮本地训练，得到本地模型更新B_i并返回到中央服务器。然后，中央服务器将汇总所有本地模型并更新全局模型，如下所示

$$\varpi(t+1)=\varpi(t)+\sum_{i=1}^{n}\frac{N_i}{N}B_i。\tag{1}$$

之后，中央服务器将$\varpi(t+1)$分发给各个客户端进行下一次迭代训练，重复上述过程直到模型收敛。

2.2 联盟区块链

2.2.1 联盟区块链的特点

预先选择的矿工：联盟区块链由一组预先选择的节点（矿工）控制，这些节点通常是已知的、可信的参与者。与公有链（如比特币）相比，联盟区块链的共识机制更为高效，因为不需要进行资源密集型的工作量证明（Proof of Work, PoW）。这种机制可以加快交易处理速度和共识过程。

高效的共识机制：联盟区块链通常使用更轻量级的共识算法，如拜占庭容错算法（BFT）或实用拜占庭容错（PBFT）。这些机制较公有链中的PoW算法更加高效，适合需要快速确认和处理事务的应用场景。

隐私保护：联盟区块链中的交易和智能合约通常仅对参与者开放，这在隐私保护方面优于公有链。在FL场景中，涉及的数据和计算模型可能敏感，联盟区块链可以确保只有授权的参与者能够访问相关信息。

2.2.2 联盟区块链与公有链和私有链的比较

1） 联盟区块链 vs 公有链

效率和速度：公有链（如比特币、以太坊）由于其开放性和去中心化特性，通常需要较高的计算资源和时间来达成共识。这对于需要快速确认和更新的任务（如联邦学习中的声誉管理）可能不够高效。联盟区块链则通过预选的节点和高效的共识算法来提高处理速度和效率。

成本问题：公有链的共识机制（如PoW）消耗大量计算资源，导致高昂的交易费用和能源消耗。联盟区块链因其共识机制较为高效，能显著降低交易费用和系统维护成本。

2） 联盟区块链 vs 私有链

信任和透明性：私有链通常由单一组织控制，虽然保证了更高的控制权和效率，但可能缺乏必要的信任机制。联盟区块链由多个组织共同管理，提供了更多的信任和去中心化特性，相对于私有链来说，具有更高的透明度和可信度。

适用性：在需要多个参与方之间建立信任和共同管理的场景下，联盟区块链比私有链更具优势。FL场景涉及多个独立的客户端和任务发布者，联盟区块链能够有效支持这种合作模式。

3） 应用场景的适配

移动网络中的声誉管理：联盟区块链的轻量级特性和高效共识机制特别适用于资源有限的移动网络环境。在这种环境下，联盟区块链能够提供快速的交易处理和可靠的声誉管理，同时避免了公有链的高成本和私有链的集中化问题。

所以，本文选择联盟区块链来管理FL的客户端声誉是因为它结合了高效的共识机制、隐私保护、适度的去中心化以及适合移动网络的特性。与公有链和私有链相比，联盟区块链在实现声誉管理时提供了更好的效率、透明性和成本效益。

2.2.3 联盟区块链中矿工的职责

对于一个联盟区块链，矿工是预定义的节点。一开始，任务发布者将一个初始模型上传到区块链。客户可以将他们经过本地训练的模型上传到区块链上。由于块大小的限制，本文建议使用星际文件系统（Interplanetary File System, IPFS）作为链外存储。然后，客户只需要将文件的哈希值上传到区块链，同时在本地存储实际数据。当访问区块链时，客户可以获得文件位置的散列。然后，他们可以使用散列来获得实际的点对点文件。矿工负责确认交易和聚合模型。客户将本地训练的模型上传到区块链后，矿工验证上传的模型签名是否有效，检查每一个客户端的局部模型并计算其声誉，这些带有数字签名的声誉意见被记录为“交易”，并上传到声誉区块链的矿工。矿工们将声誉意见放入一个数据块中，并在进行块验证和执行共识方案后，将该块添加到声誉区块链中。在所有客户上传他们训练过的模型后，矿工下载它们并开始聚合模型。然后，选择其中一名矿工作为领导者，将最终的模型上传到区块链。以下将详细解释矿工的工作。

1）矿工将验证上传的文件：当参与者试图将

他的模型上传到区块链时，矿工将检查上传文件的签名。如果签名有效，则矿工确认该文件来自合法参与者，并将该事务放入事务池中。然后，其中一个矿工将生成该块并批准该事务。如果签名无效，矿工应该拒绝事务，因为恶意的客户端有可能使用公钥加密伪造的模型，并将其上传到区块链以攻击FL模型。

2）通过计算欧氏距离来计算每个工人的局部更新梯度与全局更新梯度之间的差异，从而衡量每个工人的贡献度。

3）计算工人的声誉：任务发布者根据资源信息选择合格的工人候选人，然后通过它在FL过程中对全局模型的贡献计算其直接声誉值，最后，任务发布者将其直接声誉意见与历史声誉意见结合起来，生成一个作为每个工人的最终声誉的综合值。

2.3　防御搭便车攻击

对于搭便车者来说，其中可能有3个原因：一是良性的原因，搭便车的客户端没有训练数据和计算资源导致模型更新；二是自私的原因，搭便车的客户端为了避免花费自己的计算资源和通信资源；三是恶意的原因，搭便车的客户端可能旨在窃取全局模型。

2.3.1　客户端的选择

为了防御第一类搭便车者，首先进行客户端的选择来过滤出不合格的客户端并选择高质量的客户端。每个客户端都有不同的感知能力，并有不同类型的数据和计算资源（第二、三类搭便车者都有足够的训练数据和计算资源），例如，移动边缘FL系统通常对网络传输速率很敏感。在这种情况下，具有较高传输速率的客户端更有可能被选择，而那些信道条件持续较差的数据所有者可能永远不会被选择。参考文献[17]，将收集的网络传输速率作为采样率的函数。网络传输速率意味着工人的重要性，即网络传输速率的工人具有更高的重要性，从而可以提高模型的准确性。根据文献[17]中的假设，本文将客户端的数据质量和计算资源作为工人的重要性，工人i的重要性表示为

$$\vartheta_i(h_i)=\frac{\lg(h_i+1)}{\lg 20},\tag{2}$$

式中：h_i表示一个特定工人的数据质量和计算资源，即工人的重要性 。任务发布者选择重要性级别大于ξ的工人，其中ξ为任务发布者要选择的工人的最小重要性阈值级别。ξ值由任务发布者决定，并且是特定于Iot应用程序的。

2.3.2　声誉计算

贡献度测量：高效的FL依赖于具有较高声誉客户端的积极参与。请注意，量化客户端的贡献是区分客户端声誉的关键促成因素。FL过程包括相互协调和动态参与。为了简化动态的长期过程，通过计算每个客户端在参与FL过程中产生的局部更新梯度与全局更新梯度之间的欧式距离d来衡量其贡献。

$$d=sprt\left(sum(x_i-y_i)^2\right)。\tag{3}$$

直接声誉：在6G边缘智能中，边缘服务器会发布多个FL任务。客户有必要综合考虑当前FL任务的长期贡献和历史类似学习任务的贡献，因为在FL中，客户身上的数据会随着时间的推移而不断变化。与此同时，客户始终保持诚实也是不现实的。因此，客户的声誉包括直接声誉和间接声誉。对于客户端j，它在FL任务m中每一轮训练的直接声誉γ_{jm}^t为

$$\varphi_{jm}=1-d,\tag{4}$$

$$\gamma_{jm}=\lambda\varphi_{jm}。\tag{5}$$

间接（历史）声誉：历史声誉值被存储和管理在开放获取的声誉区块链上。声誉区块链是一个公共账本，它将工人的声誉值记录到数据块中。对于每个工人，矿工首先从声誉区块链中下载最新一轮的历史声誉值$\gamma_{jm}^{(t-1)}$。

最终声誉值：在形成客户端j作为最终声誉时，任务发布者不仅考虑直接的声誉意见，还考虑历史的声誉意见，并表示了最终的声誉意见$R_{jm}^{(t)}$为

$$R_{jm}^t=\alpha\gamma_{jm}^t+\beta\gamma_{jm}^{(t-1)},\tag{6}$$

式中：α和β为一个可设置的权重系数，并且$\alpha+\beta=1$。

2.4　激励机制

首先，在区块链设计一个标准的阈值κ，以要求参与者的贡献最少，它也可以用来识别和清除对手，因为他们的贡献通常很低。在每一轮t中，将更新的声誉与κ进行比较，声誉小于κ的参与者将从随后的一轮训练中删除。

聚合模型：在梯度聚合步骤中，采用信誉加权聚合，如下

$$\Delta\omega_g^{(t)}=\sum_{i\in P}R_i^{(t-1)}\Delta\omega_i^{(t)}\times\eta/\|\Delta\omega_i^{(t)}\|,\tag{7}$$

式中：$\Delta\omega_i^{(t)}$为参与者i上传的梯度；η为防止梯度爆炸的归一化系数；P为一组有信誉的客户端，即那些声誉高于预先确定的阈值κ的客户端。

3 实验设置及仿真结果对比

3.1 数据集

在仿真中使用MNIST和Cifar10作为标准的分类基线数据集。MNIST数据集包含28×28个手写数字，共10个类，已成为分类任务中最著名的数据集。Cifar10由10类32×32图像和3个RGB通道组成，由50 000个训练样本和10 000个测试样本组成。在FL的大量研究实验中都利用MNIST和Cifar10作为基线数据集。值得注意的是，MNIST的大小为28×28，而Cifar10为32×32，所以假设FR拥有MNIST，而诚实的客户在FL培训中拥有Cifar10。此外，为了实现模型的平滑训练，需要扩展与Cifar10相同的MNIST张量维数。

3.2 实验设置

3.2.1 联邦学习

模型：本文使用MNIST的2层卷积神经网络（CNN），Cifar10的3层CNN作为FL的基础模型。

参数设置：FL通过SGD优化器进行训练，学习率为0.15，学习速率为0.977，训练轮数为100轮。此外，还考虑了MNIST和Cifar10数据集中两种常见的数据类型，iid和非iid。

3.2.2 搭便车攻击类型

在MNIST上考虑了两种类型的搭便车者：自私的搭便车者和恶意的搭便车者。

3.2.3 超参数

将声誉阈值设置为$\kappa=1/(3N)$，移动平均系数为$\alpha=0.8$，MNIST的梯度归一化常数$\eta=0.5$，Cifar10为0.15，Mr和SST为1。对$\kappa=1/(3N)$的解释是，每个参与者应该至少贡献他们个人比例的1/3，即$1/N$，因为有N个参与者。

3.3 仿真结果

图3为所有客户端训练前30轮每一轮的声誉值，其中包括10名诚实参与者和2名不同类型的搭便车者。可以看出，在训练的第9轮之前搭便车者和诚实参与者的声誉值都在逐步提高，但之后，搭便车者声誉值慢慢下降直到被系统删除。

图4所示为2名搭便车者的声誉值，从图中可以看出，自私的搭便车者在第14轮的训练中被移除出FL系统中，而恶意的搭便车者在第16轮才被移除出，可能是因为恶意搭便车者善于伪装上传的局部更新梯度。

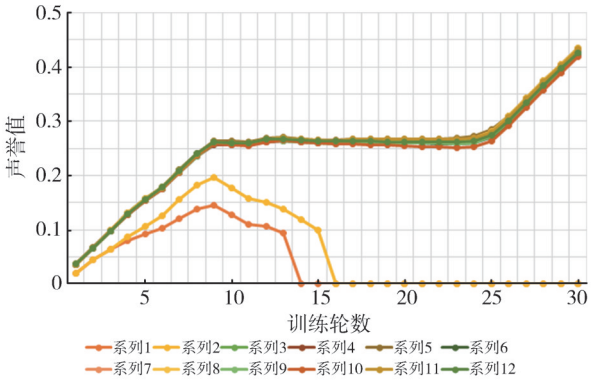

图3 所有客户端训练前30轮的声誉值

Fig. 3 Reputation value for the first 30 rounds of training for all clients

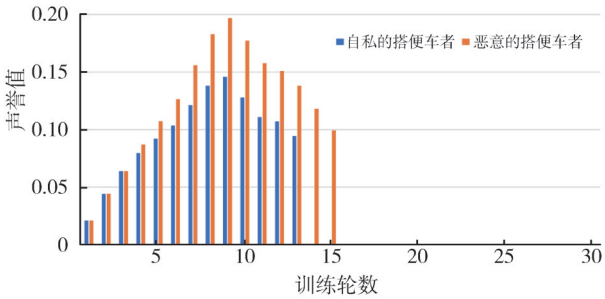

图4 两种搭便车攻击的客户端声誉值

Fig. 4 Client reputation values for two types of free riding attacks

图5为参与者最终局部模型的平均精度。本文方法（B-FFL）性能明显优于其他方法，这可能归因于声誉加权聚合，它可以动态地提高贡献更多的参与者的权重。

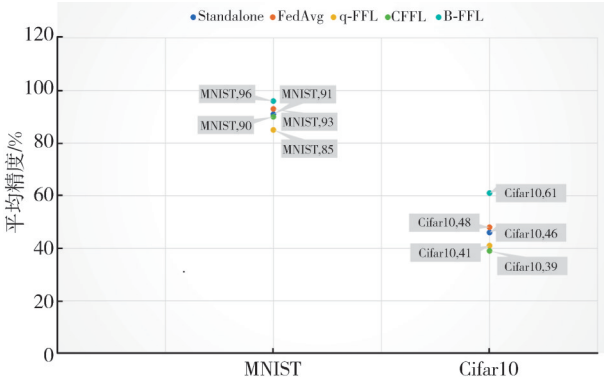

图5 不同聚合模型方法下参与者最终局部模型的平均精度

Fig. 5 The average accuracy of the final local model of participants under different aggregation model methods

从图6可以看出，只有FedAvg和本文方法（B-FFL）表现出持续的鲁棒性。FedAvg之所以

鲁棒，是因为搭便车者的梯度期望为零，因此额外的噪声不会影响渐近无偏性。在其他方法中，Multi-Krum 表现出一定程度的鲁棒性，但会牺牲准确性。FoolsGold 对搭便车者不具备鲁棒性，因为其假设诚实参与者产生的梯度比共同攻击目标函数的对手更随机。对于 Median 方法，诚实梯度可能较小，接近随机噪声梯度，结果使随机噪声梯度被更新到模型中。

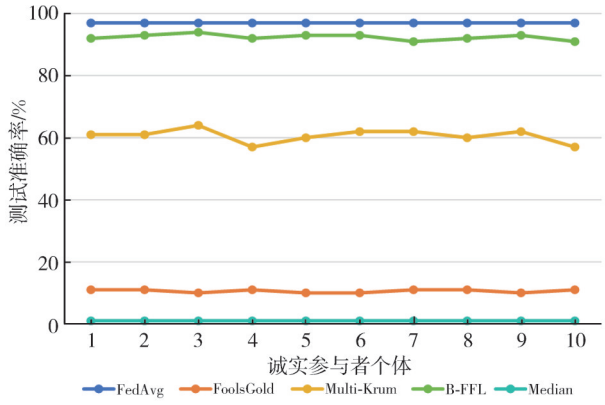

图 6　各个诚实参与者个体的测试准确率

Fig. 6　The testing accuracy of each honest participant individual

4　结　语

本文提出了一个基于联盟区块链的完全分布式 FL 框架来解决传统 FL 中央服务器易受到单点攻击的问题。通过引入声誉评估和参与者上传的局部梯度和聚合的全局梯度之间的欧氏距离，迭代评估每个参与者的贡献来解决 FL 中的搭便车攻击问题。在不同数据集上的大量实验表明，本文方法比 FedAvg 具有更高的精度，并且可以有效识别和排除搭便车者。在未来的工作中，计划探索和理论上形式化潜在的权衡。

参考文献：

[1] ZHANG C, XIE Y, BAI H, et al. A survey on federated learning[J]. Knowledge-Based Systems, 2021, 216: 106775.

[2] KAIROUZ P, MCMAHAN H B, AVENT B, et al. Advances and open problems in federated learning[J]. Foundations and Trends in Machine Learning, 2021, 14(1/2): 1-210.

[3] LI T, SAHU A K, TALWALKAR A, et al. Federated learning: challenges, methods, and future directions[J]. IEEE Signal Processing Magazine, 2020, 37(3): 50-60.

[4] YANG H H, LIU Z, QUEK T Q S, et al. Scheduling policies for federated learning in wireless networks [J]. IEEE Transactions on Communications, 2020, 68(1): 317-333.

[5] BONAWITZ K, IVANOV V, KREUTER B, et al. Practical secure aggregation for privacy-preserving machine learning[C]//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 2017: 1175-1191.

[6] LÜ L, YU J, NANDAKUMAR K, et al. Towards fair and privacy-preserving federated deep models[EB/OL]. Computer Science, 2019. https://arxiv.org/abs/1906.01167v3.

[7] AICH S, SINAI N K, KUMAR S, et al. Protecting personal healthcare record using blockchain & federated learning technologies [C]//2021 23rd International Conference on Advanced Communication Technology (ICACT), 2021: 109-112.

[8] KIM H, PARK J, BENNIS M, et al. Blockchained on-device federated learning[EB/OL]. Computer Science, 2018. arXiv: 1808.03949. https://arxiv.org/abs/1808.03949.

[9] TOYODA K, ZHANG A N. Mechanism design for an incentive-aware blockchain-enabled federated learning platform[C]//2019 IEEE International Conference on Big Data, 2019: 395-403.

[10] HOU D, ZHANG J, MAN K L, et al. A systematic literature review of blockchain-based federated learning: architectures, applications and issues [C]//2021 2nd Information Communication Technologies Conference (ICTC), 2021: 302-307.

[11] ABDEL WAHAB O, MOURAD A, OTROK H, et al. Federated machine learning: survey, multi-level classification, desirable criteria and future directions in communication and networking systems [J]. IEEE Communications Surveys & Tutorials, 2021, 23(2): 1342-1397.

[12] NGUYEN D C, DING M, PHAM Q V, et al. Federated learning meets blockchain in edge computing: opportunities and challenges [C]//IEEE Internet of Things Journal, 2021: 12806-12825.

[13] LIN J, DU M, LIU J. Free-riders in federated learning: attacks and defenses [EB/OL]. Computer Science, 2019. https://arxiv.org/abs/1911.12560v1.

[14] FRABONI Y, VIDAL R, LORENZI M. Free-rider attacks on model aggregation in federated learning [C]//24th International Conference on Artificial Intelligence and Statistics, 2021: 1846-1854.

（下转第 304 页）