基于区块链和联邦学习的边缘计算隐私保护方法

方晨[1]，郭渊博[1]，王一丰[1]，胡永进[1]，马佳利[1]，张晗[2]，胡阳阳[3]
（1. 信息工程大学密码工程学院，河南 郑州 450001；2. 郑州大学网络空间安全学院，河南 郑州 450003；
3. 加利福尼亚大学河滨分校，河滨 CA92521）

摘 要：针对边缘计算的数据隐私性、计算结果正确性和数据处理过程可审计性等需求，提出了一种基于区块链和联邦学习的边缘计算隐私保护方法，不需要可信环境和特殊硬件设施即可在网络边缘处联合多设备实现安全可靠的协同训练。利用区块链赋予边缘计算防篡改和抗单点故障攻击等特性，并在共识协议中融入梯度验证和激励机制，鼓励更多的本地设备诚实地向联邦学习贡献算力和数据。对于联邦学习共享模型参数导致的潜在隐私泄露问题，设计自适应差分隐私机制保护参数隐私的同时减小噪声对模型准确性的影响，并通过时刻统计精确追踪训练过程中的隐私损失。实验结果表明，所提方法能够抵抗 30%的中毒攻击，并且能以较高的模型准确率实现隐私保护，适用于对安全性和准确性要求较高的边缘计算场景。

关键词：联邦学习；边缘计算；区块链；中毒攻击；隐私保护
中图分类号：TP301
文献标识码：A
DOI: 10.11959/j.issn.1000-436x.2021190

Edge computing privacy protection method based on blockchain and federated learning

FANG Chen[1], GUO Yuanbo[1], WANG Yifeng[1], HU Yongjin[1], MA Jiali[1], ZHANG Han[2], HU Yangyang[3]
1. Department of Cryptogram Engineering, Information Engineering University, Zhengzhou 450001, China
2. School of Cyberspace Security, Zhengzhou University, Zhengzhou 450003, China
3. University of California, Riverside, Riverside CA92521, USA

Abstract: Aiming at the needs of edge computing for data privacy, the correctness of calculation results and the auditability of data processing, a privacy protection method for edge computing based on blockchain and federated learning was proposed, which can realize collaborative training with multiple devices at the edge of the network without a trusted environment and special hardware facilities. The blockchain was used to endow the edge computing with features such as tamper-proof and resistance to single-point-of-failure attacks, and the gradient verification and incentive mechanism were incorporated into the consensus protocol to encourage more local devices to honestly contribute computing power and data to the federated learning. For the potential privacy leakage problems caused by sharing model parameters, an adaptive differential privacy mechanism was designed to protect parameter privacy while reducing the impact of noise on the model accuracy, and moments accountant was used to accurately track the privacy loss during the training process. Experimental results show that the proposed method can resist 30% of poisoning attacks, and can achieve privacy protection with high model accuracy, and is suitable for edge computing scenarios that require high level of security and accuracy.

Keywords: federated learning, edge computing, blockchain, poisoning attack, privacy preservation

1 引言

边缘计算是一种将计算、存储资源从云平台迁移到网络边缘的分布式服务架构，它由多个位于云服务器和本地设备间的边缘节点协同完成数据分析任务。由于其更靠近本地设备，因此能够提供时

收稿日期：2021–06–15；**修回日期**：2021–09–15
基金项目：国家自然科学基金资助项目（No.61501515, No.61601515）
Foundation Item: The National Natural Science Foundation of China (No.61501515, No.61601515)

延更小的服务，如自动驾驶、虚拟现实、智慧城市等[1]。但是由于边缘节点通常位于不可信环境中，也面临各种安全和隐私威胁。如本地设备可能添加投毒样本或者将低质量数据发送给边缘节点，边缘节点可能推测本地设备的数据隐私，或者篡改计算结果来破坏协议的执行。因此设计边缘计算隐私保护的新方法需要考虑数据隐私性、计算结果正确性和数据处理过程可审计性 3 个方面。

联邦学习[2]作为一种新型的分布式机器学习框架，可以联合多个本地设备在仅共享模型参数的前提下协同训练机器学习模型，能够有效避免本地设备向边缘节点直接传输数据造成的隐私泄露问题。而区块链作为一种分布式账本，以透明的方式记录数据处理过程，且具有去中心化、可追溯以及难以篡改等一系列特性[3]，可以满足边缘计算的可审计性需求。它与联邦学习相结合，可以代替中央服务器执行模型参数聚合，避免单点故障攻击问题。鉴于以上优点，近两年陆续有学者基于区块链和联邦学习对边缘计算的隐私保护展开研究。

Kim 等[4]基于区块链框架提出了一种应用于设备端的联邦学习方法，将每轮迭代的本地梯度经过验证和共识后存储在区块中，并分析了端到端时延和最优的区块生成速率。Qu 等[5]通过结合区块链和联邦学习，为工业 4.0 中的认知计算技术开发了一种去中心化数据平台，解决数据孤岛和激励机制的问题。Wang 等[6]提出了支持异构模型的区块链联邦学习系统，并设计了线下和线上 2 种挖掘方法抵抗拜占庭攻击。但是上述方法均使用工作量证明（PoW, proof of work）作为共识算法，高强度的计算消耗使其难以适用于计算资源有限且宝贵的边缘计算。为此，Lu 等[7]采用轻量级的委托权益证明（DPoS, delegated proof of stake）作为共识算法，并针对车联网中数据共享的安全需求和效率提出了混合区块链结构。上述方法均将模型参数作为交易记录存储在区块链中，这虽然保证了训练过程的可审计性，但是一旦攻击者获取区块链内容，依然可以发起最新的模型提取攻击和模型逆向攻击，从模型参数中推断出训练数据信息。为了进一步提高隐私安全性，Qu 等[8]设计了一种基于数字签名和加密协议的混合身份机制，以防止攻击者窃取区块链中存储的数据信息。但是当联邦学习迭代次数过多时，这种机制将消耗大量的计算开销，难以部署于本地设备中。Zhao 等[9]为了保护家居场景中用户的隐私数据，在卷积层提取的特征中加入差分隐私噪声后再上传至区块链。Lu 等[10]和 Qi 等[11]将本地差分隐私技术应用于区块链联邦学习中，通过在原始数据上添加噪声扰动以保护工业互联网和智慧交通领域的数据隐私。但是在带噪数据上训练得到的联邦学习模型普遍存在准确性较低的问题。另外，如果部分参与训练的设备的数据集质量过低或者被攻击者发起中毒攻击，则其上传的模型参数将导致联邦学习偏离正常的训练方向，这将给边缘计算应用带来极大的安全隐患。Liu 等[12]在执行模型聚合前利用包含验证数据集的智能合约自动评估设备上传的更新，以检测是否存在中毒攻击。Short 等[13]基于验证数据集测试加入设备上传的参数后模型准确性是否有所提升，进而筛选出可靠的更新。但是这 2 种方法均需假设提前拥有一个与训练数据集同分布的验证测试集，这会增加许多敏感信息领域如医疗等的隐私泄露风险。

综上所述，当前在边缘计算中应用区块链和联邦学习方法存在以下几个问题。

1) 区块链账本的公开透明性虽然保证了联邦训练的可审计性，但是其以明文形式存储的模型参数会被攻击者利用推测本地设备的数据隐私。

2) 本地设备的数据集中一旦存在投毒样本就会威胁联邦学习的正确性。

3) 本地设备的资源有限性要求区块链与联邦学习结合后的效率需要进一步提高。虽然上述文献针对其中个别问题提出了解决方案，但均存在不足。

为此，本文提出了一种基于区块链和联邦学习的边缘计算隐私保护方法，可以在互不信任的本地设备间构建一个安全可靠的智能边缘计算框架。不需要任何可信的中央服务器，多个分布式设备即可实现高效安全的协同训练。主要贡献有以下几点。

1) 设计了一个基于区块链的联邦学习框架，不仅使联邦学习具备防篡改和抗单点故障特性，还提供了激励机制鼓励更多设备参与联邦训练。

2) 提出了一种自适应差分隐私机制，保护参数隐私的同时可根据训练进度自适应调整裁剪阈值，缓解噪声对模型准确性的负面影响。

3) 设计了梯度验证机制，不仅可以防止恶意设备获取额外奖励，还能够检测一定比例的中毒攻击，确保联邦学习更加安全。

2 相关基础知识

2.1 区块链

区块链作为一种去中心化、难以篡改的数字账本，能够在无信任环境下以安全可验证的方式构建分类账，在物联网、大数据、云计算和边缘计算等领域得到了广泛的应用。在区块链中，所有参与节点都可以进行事务的验证和转发，并通过共识算法维护全网一致的分类账，账本中的每个区块记录一系列事务和前一个区块的散列值，从而将当前区块链接到前一个区块。

共识算法是区块链技术的核心。工作量证明是比特币网络使用的共识算法，它要求网络中的每个节点都计算特定的哈希散列值。哈希散列值满足一定条件的节点得到生成新区块的权利。新区块通过验证后会广播给网络中的所有节点以保持账本的一致性。但是这种共识机制会浪费大量的计算资源，因此以太坊提出权益证明（PoS, proof of stake），节点利用持币数以及持有的时间来竞争生成新区块的权利，相比之下避免了不必要的资源浪费，但仍面临易分叉和扩展性的问题。委托权益证明在 PoS 的基础上进行了改进，由节点投票选举出特定数目的代理节点负责区块的生成和验证，因此在牺牲部分去中心化特性的情况下加快了区块的确认速度。拜占庭容错算法（BFT, byzantine fault tolerance）来源于拜占庭将军问题，是考虑在有恶意节点的情况下达成共识。它要求所有节点之间两两通信，因此节点数量不能太多，可扩展性较弱。最新提出的 Algorand 协议[14]是一个采用纯 PoS 共识的公链项目，其结合密码抽签技术和改进的拜占庭共识协议，能够实现快速的交易确认，并且用户数量可无限扩展，被宣称能解决区块链中“可扩展性、安全性和去中心化”的三角难题。其中，1) 可扩展性：Algorand 采用可验证随机函数（VRF, verifiable random function）选出若干个验证者，无论网络中有多少用户，每生成一个新区块只需要在少数验证者上进行验证，具有较高的吞吐量（TPS, transactions per second）。2) 安全性：只有当区块生产者和验证者确定自己被选中并广播相应的证明信息时才会被披露，攻击者无法提前预测，即使发起攻击也无法阻止新区块在网络中传播。3) 去中心化：Algorand 在每一轮中都重新随机选取区块生产者和验证者，具有较好的去中心化性。

由于区块链天然的泛中心分布式可信机制，为构建更加安全的边缘智能计算框架提供了新的思路，可以有效解决本地设备协作时面临的网络安全攻击问题。

2.2 联邦学习

在分布式场景中，传统的机器学习算法要求用户将数据上传至数据中心再进行训练。然而，数据中可能包含隐私信息，部分用户不愿意共享其数据，这就造成了严重的数据孤岛现象，阻碍了机器学习进一步的发展。为了解决这一问题，谷歌于 2016 年提出一种新的分布式机器学习框架——联邦学习，用于在移动终端与服务器间建立共享模型，从而在终端数据不出本地的情况下实现数据“可用不可见”。在该框架下，每个分布式终端基于本地数据集训练机器学习模型，然后将模型参数发送给中央服务器。服务器聚合所有上传的参数后得到全局模型，下发给各个终端，用以更新它们的本地模型。假设联邦学习系统中有 K 个终端，每个终端持有包含 $n_i=\left|\mathrm{DB}_i\right|$ 个样本的本地数据集 $\mathrm{DB}_i(1\leqslant i\leqslant K)$，则中央服务器的损失函数为

$$f(w)=\sum_{i=1}^{K}\frac{n_i}{n}F_i(w) \tag{1}$$

其中，$n=\sum_{i=1}^{K}n_i$ 是所有终端数据量总和，$F_i(w)=\frac{1}{n_i}\sum_{j\in\mathrm{DB}_i}f_j(w)$ 是第 i 个终端的本地损失函数，$f_j(w)=l(x_j,y_j,w)$ 是样本 (x_j,y_j) 对模型 w 造成的损失。联邦学习通常采用随机梯度下降算法以最小化损失函数，直至达到指定的迭代次数或模型准确率。

2.3 差分隐私

差分隐私是一种严格可证明的数学框架，其基本思想是通过对函数的输入或输出结果添加精心设计的噪声，使数据集中任意单个记录的修改都不会对输出结果造成显著的影响，因此攻击者不能通过分析输出结果来推测数据集中的隐私信息。相关定义如下。

定义 1[15] (ε,δ)-差分隐私。令 $A:D\to R$ 为随机算法，D 和 D' 是最多有一条记录不同的 2 个数据集，$O\in R$ 为算法 A 的输出，若算法 A 满足

$$\Pr[A(D)=O]\leqslant e^{\varepsilon}\Pr[A(D')=O]+\delta \tag{2}$$

则称 A 满足 (ε,δ)-差分隐私。其中，ε 为差分隐私

预算，该值越小说明隐私保护程度越高，但同时对于算法 A 的精度损失越大；δ 表示允许违背严格差分隐私的概率，一般值较小。

定义 2[15]　敏感度。对于任意的查询函数 $f:D\to \boldsymbol{R}^d$，D 为输入数据集，$\boldsymbol{R}^d$ 为函数输出的 d 维向量，则函数 f 的敏感度为

$$\Delta f=\max_{D,D'}\left\|f(D)-f(D')\right\|_p \tag{3}$$

其中，D 和 D' 为最多相差一条记录的相邻数据集，$\|\bullet\|_p$ 表示 L_p 范数。敏感度反映了查询函数 f 在一对相邻数据集上输出结果的最大变化范围。敏感度越小，则实现差分隐私时需要向输出结果添加的噪声就越少。

定义 3[15]　高斯机制。若使用 L_2 范数计算函数 f 的敏感度，则可以通过向函数 f 的输出添加高斯噪声来实现 (ε,δ)-差分隐私，如式(4)所示。

$$A(D)=f(D)+N(0,(\Delta f\sigma)^2\boldsymbol{I}) \tag{4}$$

其中，高斯噪声是满足均值为 0、协方差为 $(\Delta f\sigma)^2\boldsymbol{I}$ 的高斯分布，$\boldsymbol{I}$ 为单位矩阵。

差分隐私满足以下特性。

1) 后处理性。若一个算法的输出结果满足差分隐私，则在这个结果上进行的任何操作都不会造成额外的隐私损失。

2) 序列化组合原理。差分隐私算法的序列化组合依然满足差分隐私性质。

3　方案设计

3.1　系统威胁

本节给出在边缘计算中应用联邦学习面临的安全威胁。

威胁 1　潜在隐私泄露。虽然联邦学习只传输模型参数而不传输原始数据，但是最新的隐私攻击[16]表明通过利用模型参数依然可以推测出本地设备数据的部分隐私信息。

威胁 2　中毒攻击。恶意设备可以通过篡改原始数据或者提交错误的本地梯度来破坏联邦学习的正确性。

威胁 3　单点故障攻击。中央服务器一旦被攻击者瘫痪，则整个联邦学习训练就会失败。

下面介绍本文方案中常用的术语和符号。

本地设备。部署在网络边缘的本地设备，如工业物联网中的传感器、智慧城市中的摄像机、车联网中的汽车等，拥有有限的本地数据集和计算能力，希望在保护数据隐私的前提下和其他设备通过联邦学习构建一个更准确的机器学习模型，以提供更加智能的服务。

矿工。即边缘节点，通常配备了一定的计算资源和通信资源，如工业物联网中的边缘服务器、移动通信网中的基站、车联网中的路边单元等。提供区块链中的验证、共识等服务，并由此获取相应的代币作为收益。

事务。即区块链节点间交互的数据记录，比如比特币中事务记录的是资金转移。在本文中，事务记录的是模型的梯度以及相关训练信息。

协同训练。所有设备以相同的初始化参数为起点，共同迭代训练同一个深度学习模型。在每轮迭代中，设备将本地训练得到的模型更新上传给区块链，然后由区块链完成模型聚合和共识，得到的新区块由设备下载以更新本地模型，接着进行下一轮训练。

代币。本区块链中的资产，主要用于激励设备和矿工参加训练。当设备的更新被验证为合法、矿工参与验证或生成新区块时，都能够获取一定数量的代币作为奖励。这种设置已经在很多基于模型定价的场景中[17-18]进行应用。例如，在车联网场景中[19]，汽车积极参与联邦训练以获取代币奖励，路边单元提供有偿的区块链服务以增加自己收益。与现有工作不同的是，本文给代币设置一个有效期，即经过一定轮数的训练后，代币即失效。这将用于后面的共识机制中防止财富过度累积。由于本文使用 Algorand 作为共识协议，因此为了确保安全性，假设恶意代币（即被恶意矿工持有）的数量不超过 1/3[14]。

3.2　系统架构

如图 1 所示，假设本系统由 K 个本地设备和若干个边缘节点充当的矿工组成，其中，本地设备可以是汽车、手机或者摄像头等具备部分计算能力的智能终端，拥有包含 n_i $(1\leqslant i\leqslant K)$个样本的本地数据集。其一轮完整的训练流程可概括如下。

步骤 1　所有矿工和设备向任务发布者申请注册，其中，设备注册信息中含有其本地数据集大小。任务发布者为它们分配用于签名的公钥和私钥，根据训练任务创建创世块（即区块链中第一个区块）并通过安全链路分发给所有本地设备和矿工以执行模型初始化。创世块主要包含以下信息：1) 模型初始化参数 w_0 和总训练轮数 T；2) 所有矿工和设备用于签名的公钥；3) 所有设备的本地数据集大小

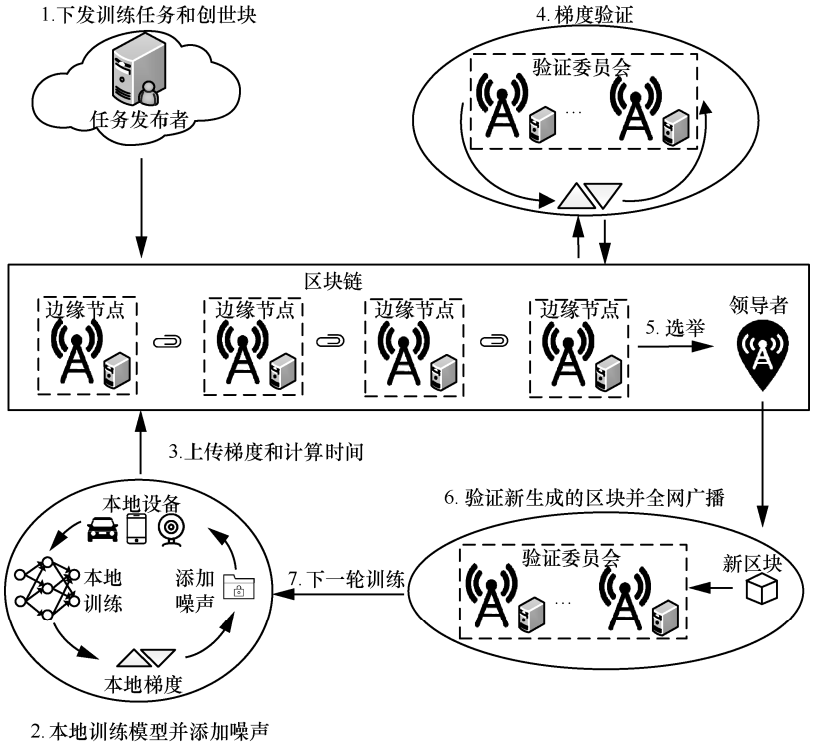

图 1　系统架构

n_i (1≤i≤K)；4) 所有设备和矿工的初始代币数量；5) 代币抵押和奖励函数；6) 随机数种子 seed_0，后续每轮训练都会根据前一轮训练的随机种子 seed_{t-1} 生成 seed_t，主要用于保证共识阶段选举领导者时的随机性（见 3.3.3 节）。本文假设创世块中的信息是可靠且不能被攻击者篡改的，这里的任务发布者仅仅起到一个引导训练过程的作用，可由可信权威代替。

步骤 2　设备在本地数据集上训练机器学习模型，迭代 n_i 次后在得到的梯度上添加差分隐私噪声（详细介绍见 3.3.1 节），以应对威胁 1。

步骤 3　设备将带噪梯度、本地运算时间以及数字签名，以区块链事务的形式上传给关联的矿工。本文假设本地运算时间是可信的，可利用 Intel SGX 可信硬件技术下的消耗时间证明机制[20]实现。

步骤 4　矿工收到数据后，首先验证签名的合法性，以防止攻击者对数据进行篡改。若签名合法，则验证梯度的可靠性，并组成验证委员会检测是否存在恶意更新（详细介绍见 3.3.2 节），以应对威胁 2。

步骤 5　基于随机种子和代币数量从矿工中选举领导者，负责计算全局梯度并生成新区块（详细介绍见 3.3.3 节）。

步骤 6　验证委员会对新区块的合法性进行验证，并广播通过验证的区块，同步全网的账本（详细介绍见 3.3.3 节），以应对威胁 3。

步骤 7　设备从其关联的矿工处下载新区块，从中获取全局梯度来更新本地模型，并从步骤 2 开始下一轮训练，直至模型收敛或达到最大训练轮数。

本文使用的主要符号如表 1 所示。

表 1　　**主要符号**

符号	定义
$g_{i,t}$	第 t 轮训练时设备 i 的本地梯度
$\widetilde{g}_{i,t}$	第 t 轮训练时设备 i 的带噪梯度
$\tilde{g}_t$	第 t 轮训练的全局梯度
C_t	第 t 轮训练的梯度裁剪阈值
G	先验阈值
n_i	设备 i 的本地数据集大小
$T^t_{\{\text{local},i\}}$	第 t 轮训练时设备 i 的本地运算时间
T	算法总的训练轮数
K	设备总数量
seed_i	第 t 轮训练时共识协议中的随机种子

3.3　方案组件

本文方案主要由 3 个关键部分实现基于联邦学

习和区块链的隐私保护方法，即自适应差分隐私机制、验证和激励机制以及共识协议。下面分别对其进行详细介绍。

3.3.1　自适应差分隐私机制

所有设备在本地数据集上训练得到模型梯度，将其上传给矿工之前，需对梯度做隐私保护处理以应对威胁 1。为此，文献[21]和文献[22]分别提出利用门限 Paillier 加密算法和 Shamir 秘密共享算法来保护本地梯度，但均存在计算开销过大的问题；相比之下，差分隐私技术计算量小，更适用于资源受限的边缘计算设备。文献[11]利用本地差分隐私技术在原始训练数据上添加噪声以保护隐私，但会造成较大的模型精度损失。文献[23]利用全局阈值 C 裁剪梯度后添加高斯噪声以保护隐私，但未说明阈值 C 的选取依据。C 值对于深度学习模型来说至关重要：C 值过大会添加过量噪声，C 值过小会过度裁剪梯度，二者都会造成模型精度严重受损。文献[24]令 C 值取所有设备梯度范数的中位数，但要求服务器获取所有设备的明文梯度，依然面临威胁 1 的挑战。为此，本文借鉴 RMSProp 优化算法的思想，提出一种适用于本地设备的自适应差分隐私机制，可根据训练过程灵活调整裁剪阈值，以减小噪声对模型精度的负面影响。

RMSProp 优化算法作为梯度下降算法的一种优化，主要通过调整步长来加快收敛速度。其迭代更新计算式为

$$\begin{aligned}&\mathrm{E}[g^2]_t \leftarrow (1-\gamma)\mathrm{E}[g^2]_{t-1}+\gamma(g_t)^2\\&\theta_t \leftarrow \theta_{t-1}-\eta\frac{g_t}{\sqrt{\mathrm{E}[g^2]_t+\varepsilon_0}}\end{aligned} \tag{5}$$

其中，θ_t 代表第 t 轮训练时的模型参数，g_t 代表模型梯度，η 是学习速率，ε_0 为了确保除数不为零，一般定为 10^{-8}，$\mathrm{E}[g^2]_{t-1}$ 用于估计历史梯度的累积平方。鉴于优化过程的连续性和渐进性，历史梯度通常可用于估计当前梯度的值[25]。因此，RMSProp 优化算法中的 $\mathrm{E}[g^2]_{t-1}$ 可以看作当前梯度的先验知识。

已有算法[26]令阈值 $C\approx\|\tilde{g}_t\|_2$ 来实现近似最优裁剪效果，而依据 3.2 节中的训练流程，本文算法中设备在上传梯度前无法获取当前训练轮次的全局梯度。因此本文借鉴 RMSProp 优化算法中的思想，利用先验知识 $\mathrm{E}[\tilde{g}^2]_{t-1}$ 预测本轮的全局梯度 $\tilde{g}_t$，并将其作为本轮的裁剪阈值 C_t，即 $C_t=\beta\sqrt{\mathrm{E}[\tilde{g}^2]_{t-1}}$，其中，$\beta$ 为本地裁剪因子，先验知识 $\mathrm{E}[\tilde{g}^2]_{t-1}$ 的计算式为

$$\begin{aligned}&\mathrm{E}[\tilde{g}^2]_0=\vec{0}\\&\mathrm{E}[\tilde{g}^2]_{t-1}\leftarrow(1-\gamma)\mathrm{E}[\tilde{g}^2]_{t-2}+\gamma(\tilde{g}_{t-1})^2\end{aligned} \tag{6}$$

注意，在第一轮训练时先验知识 $\mathrm{E}[\tilde{g}^2]_0=0$，会导致 $C_1=\beta\sqrt{\mathrm{E}[\tilde{g}^2]_0}=0$，不能用于梯度裁剪。因此，另设一个先验阈值 G：当训练初期梯度的先验知识不足时（即 $\mathrm{E}[\tilde{g}^2]_{t-1}<G$），令梯度裁剪阈值取固定值 C；当训练不断进行直到先验知识满足 $\mathrm{E}[\tilde{g}^2]_{t-1}>G$ 时，令梯度裁剪阈值取 $C_t=\beta\sqrt{\mathrm{E}[\tilde{g}^2]_{t-1}}$。

综上所述，在第 t 轮训练中，设备 i $(1\leqslant i\leqslant K)$ 在本地端裁剪梯度 $g_{i,t}$ 并添加噪声的过程可表示为

$$\begin{aligned}&\bar{g}_{i,t}=\frac{g_{i,t}}{\max\left(1,\dfrac{\|g_{i,t}\|_2}{C_t}\right)}+N(0,C_t^2\sigma^2)\\&\text{where } C_t=\begin{cases}C, & \mathrm{E}[\tilde{g}^2]_{t-1}<G\\ \beta\sqrt{\mathrm{E}[\tilde{g}^2]_{t-1}}, & \mathrm{E}[\tilde{g}^2]_{t-1}>G\end{cases}\end{aligned} \tag{7}$$

由式(7)可知，随着模型不断收敛，本地裁剪阈值 C_t 会随着 $\sqrt{\mathrm{E}[\tilde{g}^2]_{t-1}}$ 的减小而减小，将使添加在梯度上的噪声 $\xi\sim N(0,(C_t\sigma)^2\boldsymbol{I})$ 也越来越小，有助于模型在训练后期收敛。

3.3.2　验证和激励机制

由于本地设备收集的数据中可能包含用户的隐私信息，且训练模型需要消耗计算资源，因此部分设备不愿意参与联邦训练，甚至会出现部分恶意的设备上传虚假参数误导联邦训练等。为了吸引更多的设备参与训练并诚实地执行计算任务，本文利用 Multi-KRUM 算法[27]来检测中毒攻击，并根据区块链的特点设计了激励机制。其中，Multi-KRUM 算法可以解决参与分布式梯度下降算法中的 R 个设备间存在 f 个拜占庭设备（需满足 $2f+2<R$）的问题，恰好与联邦学习的分布式框架相吻合。其核心思想是“少数服从多数”，即取那些与大多数向量的平方距离之和较小的向量作为合法向量。具体过程如下。

如 3.2 节中的训练流程步骤 3～步骤 4 所述，当矿工收到其关联设备上传的数据后，首先验证签名的合法性来确保数据传输过程中不被篡改。然后判断本地运算时间 $T^t_{\{\mathrm{local},i\}}$ 是否与该设备的本地数据

集大小 n_i 成正比，以验证梯度的可靠性，并将可靠的梯度放入事务池中。接着采用可验证随机函数（VRF, verifiable random function）[14]从矿工中选出验证委员会，通过 Multi-KRUM 算法过滤事务池中可能由中毒攻击产生的恶意更新。主要步骤如下。

步骤 1 假设 R 为事务池中梯度的总数量，f 为拜占庭梯度的数量。将每个梯度与其最近的 $R-f-2$ 个梯度的欧氏距离相加，作为该梯度的质量得分。

$$s(i,t)=\sum_{i\to j}\left\|\bar{g}_{i,t}-\bar{g}_{j,t}\right\| \tag{8}$$

其中，$i\to j$ 表示 $\bar{g}_{j,t}$ 属于离 $\bar{g}_{i,t}$ 最近的 $R-f-2$ 个梯度之一。

步骤 2 选择质量得分最低的 $R-f$ 个梯度作为合法更新，并对其进行签名，同时删除其余的梯度。

针对区块链中的设备和矿工，分别设计了 2 种不同形式的激励：数据奖励和挖矿奖励。其中，1) 数据奖励用于激励本地设备向联邦学习贡献更多的数据集：在设备向矿工上传数据前，先缴纳一定数量的代币作为押金。若设备的梯度被验证为合法更新，由矿工退还设备的押金，并且分发一定数量的代币作为数据奖励，代币数量与该设备的本地数据集大小 n_i 成正比。为了防止恶意设备通过伪造数据集大小来获取更多的奖励，令设备将梯度与本地运算时间一同上传给矿工，通过比较数据集大小与该运算时间来验证可靠性；若设备的梯度被验证为恶意更新，则扣除该设备缴纳的押金，作为惩罚。当该设备的代币数量归零时，将其加入黑名单不允许参与训练。2) 挖矿奖励用于激励矿工从更多的设备中收集数据并参与区块链验证与共识环节：当矿工完成梯度验证或生成新区块时，区块链向其分发一定数量的代币作为挖矿奖励，代币数量与矿工相关联的设备的数据集总量成正比，即 $\sum_{i=1}^{N_{m_j}} n_i$，其中，N_{m_j} 代表与矿工 m_j 相关联的设备数量。

3.3.3 共识协议

共识协议对于区块链来说至关重要。PoW 通过让所有矿工计算随机哈希值来争夺记账权，已被文献[4-6]采用作为共识协议，但是其存在浪费计算资源、共识效率慢、吞吐量低的问题。Algorand 协议基于 PoS 随机选择区块生产者以及验证者，具有较高的共识效率，且可以通过引入可验证随机函数、种子参数等抵抗 DDoS 攻击、女巫攻击等，具有较高的安全性，更加适用于计算资源有限、面临更多复杂攻击的边缘计算场景。文献[9]已将 Algorand 协议应用于智能家居场景，但是其在共识协议中未设计激励机制。本文将矿工设定为工业物联网中的边缘服务器、移动通信网中的基站、车联网中的路边单元等，他们在提供区块链服务时需要消耗一定的计算、存储、通信等开销，因此，为了维持矿工持续性提供区块链服务的积极性，本文在原有 Algorand 协议的基础上增加了相应的代币奖励机制来激励矿工维护区块链。协议主要包含 3 个步骤。

步骤 1 领导者选举。在每一轮训练中，利用 Algorand 协议中的加密抽签算法从持有合法更新的矿工中随机选举出领导者，主要包含以下 2 个函数。

$$\begin{aligned}&\text{Sortition}(\text{sk},\text{seed}_t,\tau,\text{role}=\text{miner},w,W)\to\\&\langle\text{hash},\text{proof},j\rangle\\&\text{VerifySort}(\text{pk},\text{hash},\text{proof},\text{seed}_t,\tau,\text{role}=\\&\text{miner},w,W)\to j\end{aligned} \tag{9}$$

其中，sk 和 pk 分别是矿工的私钥和公钥，seed_t 是第 t 轮训练的随机种子：$\text{seed}_t=H(\text{seed}_{t-1}\|t)$，$H$ 为哈希函数。将每个代币看成是一个子用户，τ 为系统期望选择子用户的数量，W 为所有矿工的代币数量总和，则任意一个子用户被选择的概率为 $p=\tau/W$。对于拥有 w 个代币的矿工，它首先将自己的私钥 sk 和本轮训练的种子 seed_t 作为 VRF 的输入数据，得到散列值 hash 和证明 proof。然后将区间 [0,1)划分为 $w+1$ 个连续子区间，若 $\text{hash}/2^{\text{hashlen}}$ 满足

$$\text{hash}/2^{\text{hashlen}}\in\left[\sum_{k=0}^{j}\binom{w}{k}p^k(1-p)^{w-k},\sum_{k=0}^{j+1}\binom{w}{k}p^k(1-p)^{w-k}\right)$$

其中，hashlen 代表 hash 的长度，说明该矿工有 j 个子用户被选择，这也代表该矿工的优先级。可见矿工被选举为领导者的概率与其持有的代币数量 w 成正比。为了避免财富累积，本共识算法中的 w 只计算在有效期内的代币。通过上述过程，拥有最高优先级的矿工被选举为本轮训练的领导者，其他矿工可以通过证明 proof 对其优先级进行验证。

领导者从事务池中获取所有合法更新，并通过联邦平均算法计算全局梯度 $\tilde{g}_t$，如式(10)所示。

$$\tilde{g}_t=\sum_{i=1}^{K'}\frac{n_i}{n}\bar{g}_{i,t} \tag{10}$$

其中，K' 为合法更新的总数，n_i 为第 $i(1\leqslant i\leqslant K')$ 个更新所对应的样本量，$n=\sum_{i=1}^{K'}n_i$ 是所有合法更新所

对应的总样本量。

然后领导者生成这一轮训练的区块，如图 2 所示。除了包含用于链接前一个区块的哈希值以外，还包含该轮的全局梯度、所有合法更新及其签名，以及用于下一轮领导者选举的随机种子 seed_{t+1} 等。

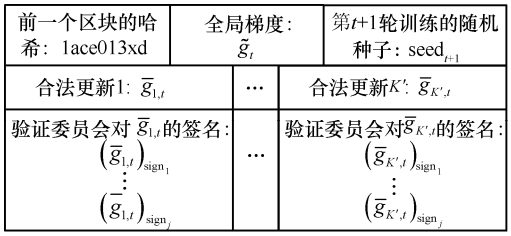

图 2　第 t 轮训练生成的区块

步骤 2　委员会验证。验证委员会对生成的新区块进行验证，主要检查其中包含的梯度更新签名是否合法，以及全局梯度计算是否正确等。只有当超过 2/3 的委员验证通过时，该区块才被认定为有效，相应的领导者和验证者从区块链中获取一定数量的代币作为挖矿奖励；否则，生成一个空区块。

步骤 3　邻居广播。委员会中的每个验证者执行 Gossip 协议[28]向邻居广播新区块，同步全网的账本。

3.4　隐私性分析

在给定隐私预算的情况下，如何计算算法在训练过程中的隐私损失十分关键。本文基于 Abadi 等[23]提出的时刻统计来计算隐私损失。相关定义如下。

定义 4[23]　隐私损失。令 $A: D \to R$ 为随机算法，D 和 D' 为相邻数据集，A 在输出 $O \in R$ 处的隐私损失为

$$c(O, A, D, D') \triangleq \log \frac{\Pr[A(D) = O]}{\Pr[A(D') = O]} \tag{11}$$

定义 5[23]　时刻统计。算法 A 在 λ 时刻的时刻统计为

$$\alpha(\lambda) \triangleq \max_{D,D'} \log \mathrm{E}_{O\sim A(D)}[\exp(\lambda c(O, A, D, D'))] \tag{12}$$

定理 1[23]（组合性）　若算法 A 由一系列子算法 A_1, A_2,…, A_k 组成，则对于任一时刻 λ，算法 A 的时刻统计上界为所有子算法 A_1, A_2,…, A_k 的时刻统计之和。

$$\alpha_A(\lambda) \leqslant \sum_{i=1}^{k} \alpha_{A_i}(\lambda) \tag{13}$$

定理 2[23]（尾界限）　对于任意 $\varepsilon > 0$，若式(14)成立，算法 A 满足 (ε, δ)-差分隐私。

$$\delta = \min_{\lambda} \exp(\alpha_A(\lambda) - \lambda\varepsilon) \tag{14}$$

基于定理 1，本文联邦学习算法的隐私损失与设备端总数和全局训练轮数成正比。假设设备数量为 K，全局训练轮数为 T，算法总的时刻统计为 $\alpha(\lambda)$，第 t 轮训练时设备 $i(1 \leqslant i \leqslant K)$ 的时刻统计为 $\alpha_{i,t}(\lambda)$，则根据定理 1 中的组合性，有

$$\alpha(\lambda) \leqslant \sum_{t=1}^{T} \sum_{i=1}^{K} \alpha_{i,t}(\lambda) \tag{15}$$

其中，$\alpha_{i,t}(\lambda)$ 主要体现在设备在裁剪后的梯度上添加高斯噪声 $\xi \sim N(0, (C_t\sigma)^2 \boldsymbol{I})$，如式(7)所示。$\alpha_{i,t}(\lambda)$ 的计算过程如下[23]。

令 μ_0 为高斯分布 $N(0, (C_t\sigma)^2)$ 的概率密度函数 $\mu_0(x) = \dfrac{1}{\sqrt{2\pi}\sigma C_t} \mathrm{e}^{-\frac{x^2}{2(\sigma C_t)^2}}$，$\mu_1$ 为高斯分布 $N(1, (C_t\sigma)^2)$ 的概率密度函数 $\mu_1(x) = \dfrac{1}{\sqrt{2\pi}\sigma C_t} \mathrm{e}^{-\frac{(x-1)^2}{2(\sigma C_t)^2}}$，$\mu$ 为混合 μ_0 和 μ_1 的高斯分布 $\mu = (1-q)\mu_0 + q\mu_1$，其中，$q$ 为设备在本地训练时的抽样概率，则 $\alpha_{i,t}(\lambda) = \log \max(E_1, E_2)$，其中，$E_1 = \mathrm{E}_{x\sim\mu_0}[(\mu_0(x)/\mu(x))^{\lambda}]$, $E_2 = \mathrm{E}_{x\sim\mu}[(\mu(x)/\mu_0(x))^{\lambda}]$。

由于所有设备在本地添加的噪声 $\xi \sim N(0, (C_t\sigma)^2 \boldsymbol{I})$ 是一样的，因此所有设备的 $\alpha_{i,t}(\lambda)$ 也是一样的。在计算得到总的时刻统计 $\alpha(\lambda)$ 后，利用定理 2 得到算法满足 $(\varepsilon, \delta = \min_{\lambda} \exp(\alpha(\lambda) - \lambda\varepsilon))$-差分隐私的形式。算法在实际运行过程中，整数时刻 λ 的取值范围通常为 $0 \leqslant \lambda \leqslant 100$。

4　实验过程及结果分析

实验在 Ubuntu 18.04 系统下进行，硬件配置为 Intel i7-8700K CPU, GTX 1080T GPU, 16 GB RAM。使用 Go 语言来处理方案中涉及区块链的部分，使用 Pytorch 1.4.0 训练深度学习模型和添加差分隐私噪声，并通过 go-python v1.0 库搭建 Python 和 Go 的接口。网络结构采用卷积神经网络（CNN, conventional neural network），由 2 个 5×5 的卷积层、一个全连接层和一个 softmax 输出层组成。模型中的权重初始化为从正太分布 $N(0, 0.022)$采样的随机值，并将偏差初始化为 0。实验数据集采用 MNIST

和 CIFAR10，这 2 个数据集可代表本地设备所收集的复杂度中等的数据，也被大量基于边缘计算场景的联邦学习算法[5-7,9]作为测试数据使用。其中，MNIST 是一个包含 60 000 个训练样本和 10 000 个测试样本的手写数据集，每个样本是一个 28×28 的灰度图像，标签为 0～9；CIFAR10 是一个包含 50 000 个训练样本和 10 000 个测试样本的图像数据集，每个样本是一个 32×32 的 RGB 图像，标签包含“飞机”“狗”“汽车”等 10 类普适物体。实验中令 RMSProp 优化算法中的 $\gamma=0.1,\eta=0.002,\varepsilon_0=10^{-6}$，自适应差分隐私中的 $G=10^{-6},\beta=1.2$，$\sigma=4$，$\delta=10^{-4}$。在 MNIST 数据集上初始裁剪阈值 C=4，隐私预算 $\varepsilon=2$；在 CIFAR10 数据集上 C=3，$\varepsilon=4$。为了模拟联邦学习的分布式环境，假设系统中有 20 个本地设备，并将实验数据集随机均匀划分为 20 份分给每个设备作为本地数据集。设备在本地训练批次大小为 64，通过使用 pickle 模块，将梯度参数转换为字节流进行传输，默认采用 64 bit 的精度。

4.1 隐私预算消耗

为了衡量本算法中自适应差分隐私机制在减少隐私预算消耗方面的作用，采用文献[24]中的差分隐私联邦学习算法（DPFL）作对比，即在 MNIST 和 CIFAR10 数据集上分别将裁剪阈值固定为 C=4 和 C=3，记录 2 种算法到达指定准确率时所消耗的隐私预算，如表 2 所示，其中，ε_{D} 和 ε_{A} 分别代表 DPFL 和本文算法所消耗的隐私预算。

表 2 本文算法和 DPFL 所消耗的隐私预算

数据集	准确率	δ	ε_{D}	ε_{A}	减少率	平均值
MNIST	94%	10^{-4}	2.12	1.64	22.6%	37%
	96%		3.43	1.96	42.9%	
	97%		5.15	2.78	46.0%	
CIFAR10	68%	10^{-4}	4.39	3.28	25.3%	29%
	70%		6.05	4.11	32.1%	
	72%		8.77	6.08	30.7%	

由表 2 可知，当准确率相同时，本文算法在 MNIST 和 CIFAR10 数据集上比 DPFL 平均减小了 37%和 29%的隐私预算，由此证明了本文算法通过自适应差分隐私机制有效减少了隐私预算的消耗。由于隐私预算越大，隐私保护程度越低，为了在模型准确率和隐私保护之间取得平衡，本文算法在 MNIST 数据集上令 $\varepsilon=2$，在 CIFAR10 数据集上令 $\varepsilon=4$。

4.2 算法的准确率

为了衡量差分隐私机制对于算法准确性的影响，给定相同的隐私预算，将本文算法与 DPFL 在准确率上进行对比。同时采用原始联邦学习算法作为比较基准。结果如图 3 所示。

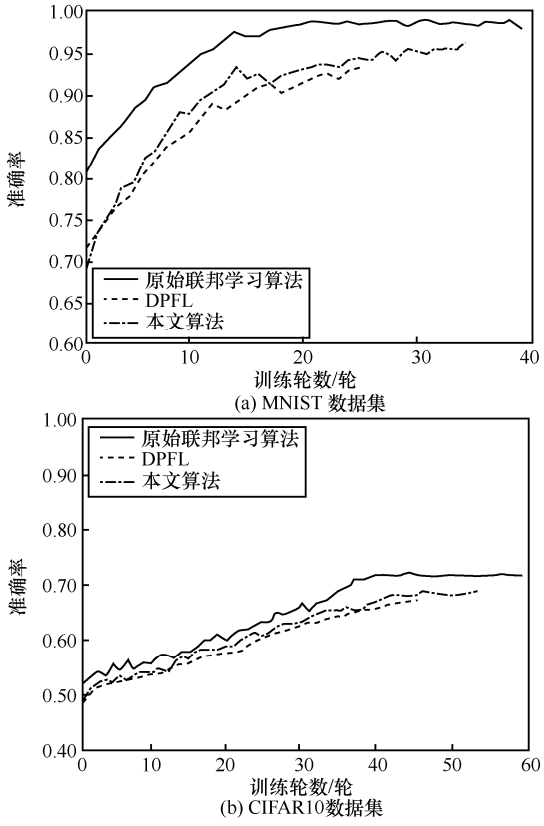

图 3 3 种算法的准确率对比

根据图 3(a)可知，在 MNIST 数据集上，原始联邦学习算法取得 98.8%的准确率，而由于隐私预算 $\varepsilon=2$ 的限制，本文算法训练至 35 轮时停止，准确率达到 96.3%，DPFL 算法训练至 26 轮时停止，准确率达到 93.7%。如图 3(b)所示，在 CIFAR10 数据集上，原始联邦学习算法取得 72%的准确率，而由于隐私预算 $\varepsilon=4$ 的限制，本文算法训练至 54 轮时停止，准确率达到 69.2%，DPFL 训练至 46 轮时停止，准确率达到 67.8%。

由此可见，通过自适应差分隐私机制，本文算法在相同的隐私预算下能够训练更多轮次，达到更高的准确率，仅略低于原始联邦学习算法。因此本文算法适用于对精度要求高、需要隐私保护的应用场景。

4.3 吞吐量和运行时间

系统吞吐量 TPS 是评估区块链性能的重要因

素，即区块链每秒处理的事务数。由于本文将区块链与联邦学习相结合应用于边缘计算场景，则一个设备向区块链上传的模型梯度等信息代表一个事务，事务在区块链中的处理流程包括梯度验证和共识 2 个阶段。统计在不同的设备数量（即不同的事务数量）下，每一轮训练中梯度验证和共识 2 个阶段分别消耗的平均时间，如图 4 所示。其中梯度验证阶段对应于 3.2 节训练流程中的步骤 4，共识阶段对应于步骤 5～步骤 6。

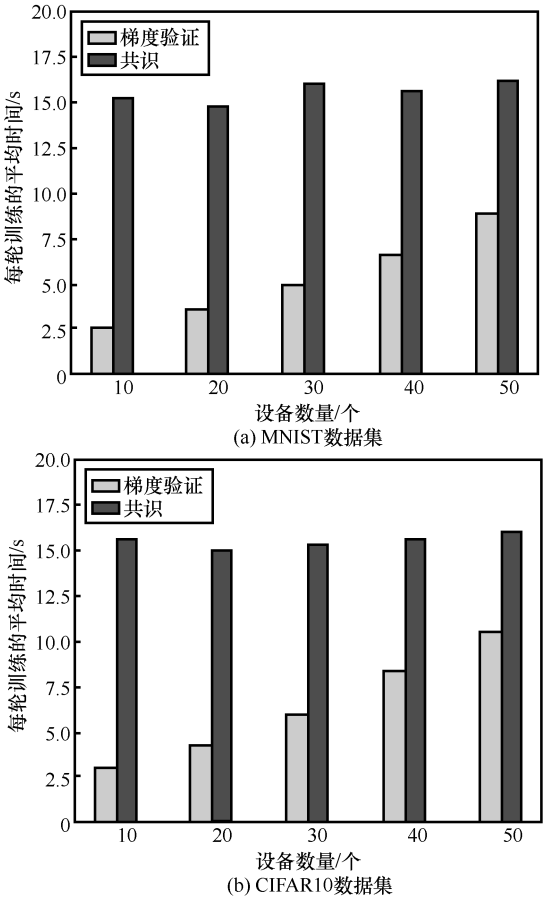

图 4　梯度验证和共识阶段的运行时间

由图 4 可知，梯度验证的时间小于共识阶段的时间，这是因为共识阶段需要执行领导者选举、联邦平均以及委员会验证等操作，需要较大的计算开销。但是梯度验证的运行时间随着设备数量的增加而增加，这是由 Multi-KRUM 算法的计算复杂度所决定的。

因此，为了更加直观地反映在共识协议中融入梯度验证后对于区块链 TPS 的影响，计算在不同的设备数量下，未加入梯度验证的 TPS 和加入梯度验证后的 TPS。具体地，未加入梯度验证的 TPS 的计算式为 $\mathrm{TPS}_1=\dfrac{\text{设备数量（事务数量）}}{\text{共识时间}}$，加入梯度验证后的 TPS 的计算式为 $\mathrm{TPS}_2=\dfrac{\text{设备数量（事务数量）}}{\text{梯度验证时间+共识时间}}$，结果如表 3 所示。可以看出，梯度验证机制在一定程度上降低了区块链的 TPS，且随着设备数量的增加，对于 TPS 的影响越大。说明梯度验证机制以牺牲部分 TPS 为代价来强化边缘计算的安全性，但是当设备小于一定数量时，TPS 减少率依然在一个可接受的范围内。如设备数量小于 50 时，TPS 减少率小于 40%。

表 3　梯度验证机制对于区块链 TPS 的影响

设备数量（事务数量）/个	MNIST 数据集			CIFAR10 数据集		
	TPS_1	TPS_2	减少率	TPS_1	TPS_2	减少率
10	0.66	0.56	15.2%	0.65	0.54	16.9%
20	1.36	1.10	19.1%	1.32	1.03	22.0%
30	1.88	1.44	23.4%	1.96	1.42	27.6%
40	2.58	1.82	29.5%	2.53	1.67	34.0%
50	3.09	2.00	35.3%	3.13	1.89	39.6%

为了进一步探讨区块链与联邦学习结合后对算法运行效率的影响，将本文算法与原始联邦学习算法[2]在运行时间上进行对比，结果如图 5 所示，其中，本文算法的训练曲线在隐私预算消耗完毕时截止，原始联邦学习算法的训练曲线在算法收敛时截止。

由图 5 可知，当模型收敛时，对于 MNIST 数据集，本文算法的运行时间约为原始联邦学习算法的 3.4 倍，分别为 1 088 s 和 323 s；对于 CIFAR10 数据集，本文算法的运行时间约为原始联邦学习算法的 2.2 倍，分别为 1 825 s 和 820 s。可见区块链中的共识和验证机制会增加算法的运行时间，但同时为边缘计算提供了更高的安全性和稳定性。因此，本文算法适用于对安全性要求较高的边缘计算场景。

4.4　抵抗中毒攻击能力

为了测试本方法抵抗中毒攻击的能力，采用文献[29]中的标签翻转攻击生成投毒样本，即更改训练样本的标签并保持样本特征不变，然后将投毒样本分配给指定的攻击者。具体地，对于 MNIST 数据集，将样本中的源标签“1”改为目标标签“8”；对于 CIFAR10 数据集，将样本中的源标签“狗”改为目标标签“马”。为了消除其他标签的影响，仅使用带有目标和源标签的样本训练二进制分类器，

并从测试数据集中随机选择 500 个带有源标签的样本测试攻击成功率，即样本的源标签被预测为目标标签所占的比例。

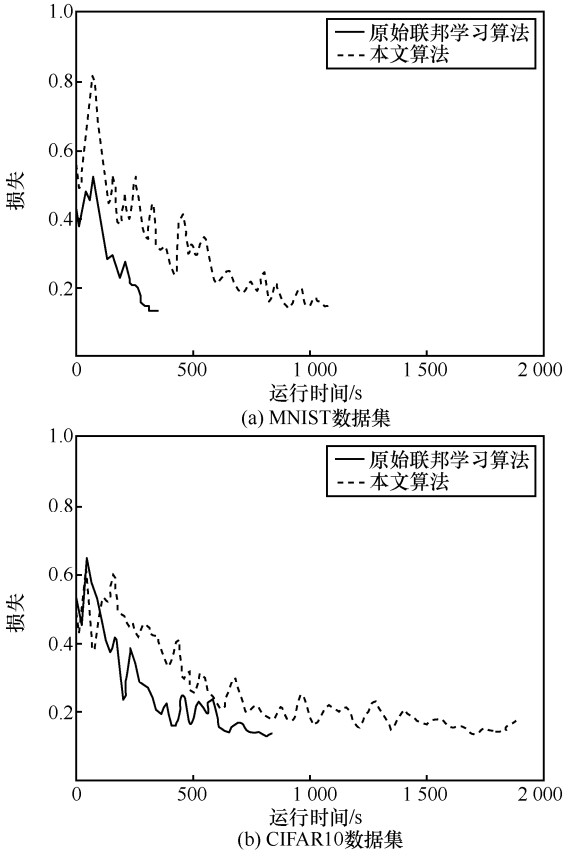

图 5　本文算法与原始联邦学习算法的运行时间对比

首先将投毒样本的比例分为设置为 30%、40%和 50%，运行 20 次实验，取平均值，并与原始的联邦学习算法[2]进行对比，如图 6 所示。

由图 6 可知，由于隐私预算的限制，本文算法在 MNIST 和 CIFAR10 数据集上迭代至一定轮数时停止。当投毒样本为 30%时，本文算法在迭代后期能够逐渐收敛至接近于无投毒样本的原始联邦学习。但是当投毒样本为 40%和 50%时，本文算法难以收敛。因此可认为本文算法能够抵抗 30%的中毒攻击。

图 7 进一步展示了 30%的投毒样本对于原始联邦学习和本文算法的攻击成功率。可见，由于原始联邦学习无法检测中毒攻击，导致攻击成功率几乎一直大于 50%。而本文算法的攻击成功率在迭代后期逐渐降至 10%以下。这是因为本文算法在 3.3.2 节的激励机制中规定，设备一旦被检测出中毒攻击就会被扣除一定数量的代币，且当代币数量归零时不

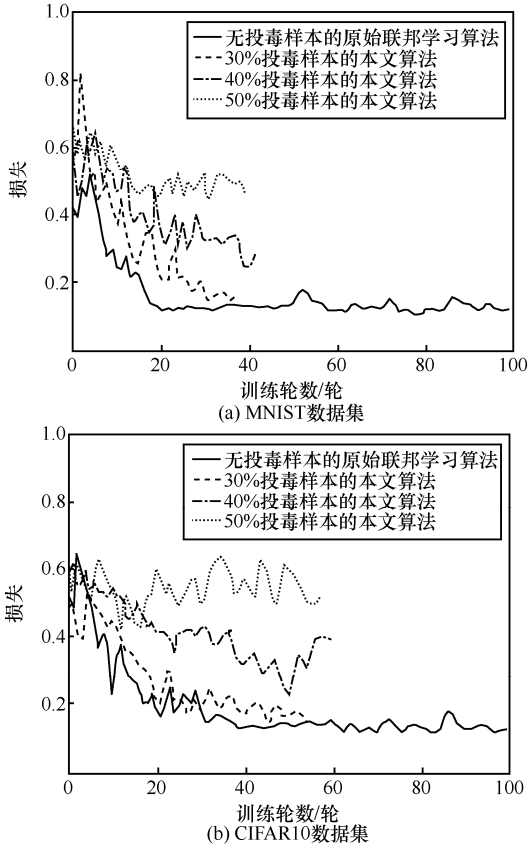

图 6　不同比例中毒攻击下本文算法与原始联邦学习算法对比

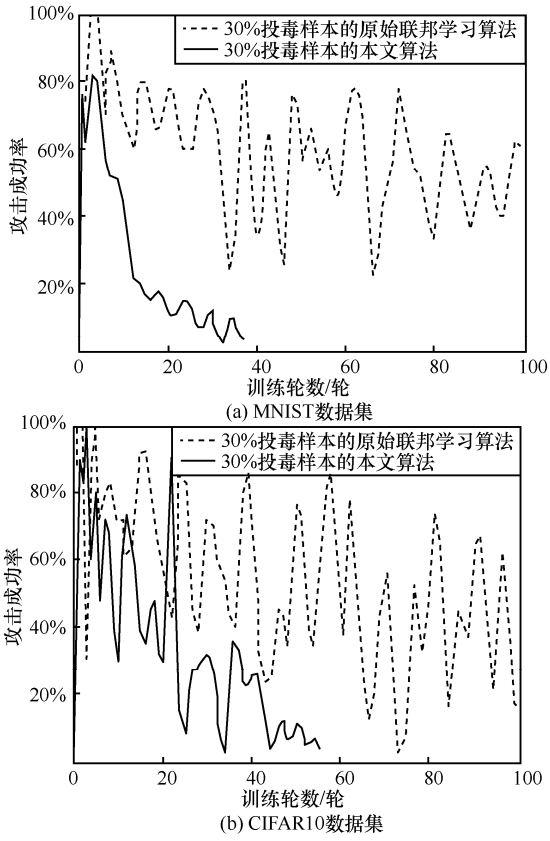

图 7　30%的投毒样本对于本文算法与原始联邦学习算法的攻击成功率

允许参与训练。实验数据表明，本文算法进入迭代后期时，在 MNIST 和 CIFAR10 数据集上分别有 4 个和 5 个设备被禁止参与训练，因此本文算法有效降低了攻击成功率。

5　结束语

本文通过结合区块链和联邦学习提出了一种应用于边缘计算的隐私保护方法。利用联邦学习为多设备建立协同训练平台，引入区块链实现训练过程的去中心化和可审计性。针对攻击者对本地设备发起的中毒攻击，设计梯度验证算法检测恶意更新，并通过激励机制鼓励更多设备加入联邦学习。针对网络边缘处潜在的隐私泄露问题，设计自适应差分隐私机制保护参数隐私并减小噪声对模型准确性的影响。在 MNIST 和 CIFAR10 数据集上进行实验，与原始联邦学习和基于差分隐私的联邦学习进行对比，表明本文算法能以较高的准确性实现隐私保护和抗中毒攻击能力，且无须依赖可信环境和特殊硬件设施。下一步将考虑设计效率更高的梯度验证算法和共识协议，以应用于时延更小的边缘计算场景。

参考文献：

[1] 周俊, 沈华杰, 林中允, 等. 边缘计算隐私保护研究进展[J]. 计算机研究与发展, 2020, 57(10): 2027-2051.
ZHOU J, SHEN H J, LIN Z Y, et al. Research advances on privacy preserving in edge computing[J]. Journal of Computer Research and Development, 2020, 57(10): 2027-2051.

[2] MCMAHAN H B, MOORE E, RAMAGE D, et al. Communication-efficient learning of deep networks from decentralized data[J]. arXiv Preprint, arXiv: 1602.05629, 2016.

[3] 曾诗钦, 霍如, 黄韬, 等. 区块链技术研究综述：原理、进展与应用[J]. 通信学报, 2020, 41(1): 134-151.
ZENG S Q, HUO R, HUANG T, et al. Survey of blockchain: principle, progress and application[J]. Journal on Communications, 2020, 41(1): 134-151.

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

[5] QU Y Y, POKHREL S R, GARG S, et al. A blockchained federated learning framework for cognitive computing in industry 4.0 networks[J]. IEEE Transactions on Industrial Informatics, 2021, 17(4): 2964-2973.

[6] WANG Q L, GUO Y F, WANG X F, et al. AI at the edge: blockchain-empowered secure multiparty learning with heterogeneous models[J]. IEEE Internet of Things Journal, 2020, 7(10): 9600-9610.

[7] LU Y L, HUANG X H, ZHANG K, et al. Blockchain empowered asynchronous federated learning for secure data sharing in Internet of vehicles[J]. IEEE Transactions on Vehicular Technology, 2020, 69(4): 4298-4311.

[8] QU Y Y, GAO L X, LUAN T H, et al. Decentralized privacy using blockchain-enabled federated learning in fog computing[J]. IEEE Internet of Things Journal, 2020, 7(6): 5171-5183.

[9] ZHAO Y, ZHAO J, JIANG L S, et al. Privacy-preserving blockchain-based federated learning for IoT devices[J]. IEEE Internet of Things Journal, 2021, 8(3): 1817-1829.

[10] LU Y L, HUANG X H, DAI Y Y, et al. Blockchain and federated learning for privacy-preserved data sharing in industrial IoT[J]. IEEE Transactions on Industrial Informatics, 2020, 16(6): 4177-4186.

[11] QI Y H, HOSSAIN M S, NIE J T, et al. Privacy-preserving blockchain-based federated learning for traffic flow prediction[J]. Future Generation Computer Systems, 2021, 117: 328-337.

[12] LIU Y, PENG J L, KANG J W, et al. A secure federated learning framework for 5G networks[J]. IEEE Wireless Communications, 2020, 27(4): 24-31.

[13] SHORT A R, LELIGOU H C, PAPOUTSIDAKIS M, et al. Using blockchain technologies to improve security in federated learning systems[C]//Proceedings of 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC). Piscataway: IEEE Press, 2020: 1183-1188.

[14] GILAD Y, HEMO R, MICALI S, et al. Algorand: scaling Byzantine agreements for cryptocurrencies[C]//Proceedings of the 26th Symposium on Operating Systems Principles. New York: ACM Press, 2017: 51-68.

[15] DWORK C, ROTH A. The algorithmic foundations of differential privacy[J]. Foundations and Trends® in Theoretical Computer Science, 2013, 9(3/4): 211-407.

[16] FREDRIKSON M, JHA S, RISTENPART T. Model inversion attacks that exploit confidence information and basic countermeasures[C]// Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2015: 1322-1333.

[17] CHEN L J, KOUTRIS P, KUMAR A. Model-based pricing for machine learning in a data marketplace[J]. arXiv Preprint, arXiv: 1805.11450, 2018.

[18] KURTULMUS A B, DANIEL K. Trustless machine learning contracts; evaluating and exchanging machine learning models on the ethereum blockchain[J]. arXiv Preprint, arXiv: 1802.10185, 2018.

[19] LI C L, FU Y C, YU F R, et al. Vehicle position correction: a vehicular blockchain networks-based GPS error sharing framework[J]. IEEE Transactions on Intelligent Transportation Systems, 2020, 22(2): 898-912.

[20] CHEN L, XU L, SHAH N, et al. On security analysis of proof-of-elapsed-time (PoET)[C]//Proceedings of International Symposium on Stabilization, Safety, and Security of Distributed Systems. Berlin: Springer International Publishing, 2017: 282-297.

[21] WENG J S, WENG J, ZHANG J L, et al. DeepChain: auditable and privacy-preserving deep learning with blockchain-based incentive[J]. IEEE Transactions on Dependable and Secure Computing, 2021, 18(5): 2438-2455.

[22] SHAYAN M, FUNG C, YOON C J M, et al. Biscotti: a ledger for private and secure peer-to-peer machine learning[J]. arXiv Preprint, arXiv: 1811.09904, 2018.

[23] ABADI M, CHU A, GOODFELLOW I, et al. Deep learning with differential privacy[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2016: 308-318.

[24] GEYER R C, KLEIN T, NABI M. Differentially private federated learning: a client level perspective[J]. arXiv Preprint, arXiv: 1712.07557, 2017.

[25] FANG C, GUO Y B, HU Y J, et al. Privacy-preserving and communication-efficient federated learning in Internet of Things[J]. Computers & Security, 2021, 103: 102199.

[26] XU C G, REN J, ZHANG D Y, et al. GANobfuscator: mitigating information leakage under GAN via differential privacy[J]. IEEE Transactions on Information Forensics and Security, 2019, 14(9): 2358-2371.

[27] BLANCHARD P, MHAMDI E M E, GUERRAOUI R, et al. Machine learning with adversaries: byzantine tolerant gradient descent[C]//Proceedings of the 31st International Conference on Neural Information Processing Systems. New York: Curran Associates Inc.. 2017: 118-128.

[28] DEMERS A, GREENE D, HAUSER C, et al. Epidemic algorithms for replicated database maintenance[C]//Proceedings of the 6th annual ACM Symposium on Principles of distributed computing. New York: ACM Press, 1987: 1-12.

[29] HUANG L, JOSEPH A D, NELSON B, et al. Adversarial machine learning[C]//Proceedings of the 4th ACM workshop on Security and artificial intelligence. New York: ACM Press, 2011: 43-58.

[作者简介]

方晨（1993− ），男，安徽宿松人，信息工程大学博士生，主要研究方向为机器学习隐私安全。

郭渊博（1975− ），男，陕西周至人，博士，信息工程大学教授、博士生导师，主要研究方向为大数据安全、态势感知。

王一丰（1994− ），男，江苏泰兴人，信息工程大学博士生，主要研究方向为深度学习、网络安全。

胡永进（1981− ），男，山东潍坊人，信息工程大学讲师，主要研究方向为大数据安全、态势感知。

马佳利（1996− ），男，河北邢台人，信息工程大学博士生，主要研究方向为数字孪生、机器学习。

张晗（1985− ），女，河南项城人，郑州大学讲师，主要研究方向为机器学习、自然语言处理。

胡阳阳（1990− ），男，江苏南京人，加利福尼亚大学河滨分校博士生，主要研究方向为机器学习。