文章编号:1671-4598(2024)01-0192-09 DOI:10.16526/j.cnki.11-4762/tp.2024.01.028 中图分类号:TP309.2 文献标识码:A

基于声誉的分布式联邦学习节点选择算法

曲 静,冯云霞
(青岛科技大学 信息科学技术学院,山东 青岛 266061)

摘要:由于隐私泄露的风险越来越大,而采集的数据中通常包含大量隐私信息,使数据的采集者不愿意共享自己的数据,造成“数据孤岛”,联邦学习能够实现数据不离本地的数据共享,但其在多机构数据共享中还存在一些问题,一方面中央服务器集中处理信息造成昂贵的成本,易产生单点故障,另一方面,对于多机构数据共享而言,参与节点中混入恶意节点可能影响训练过程,导致数据隐私泄露,基于上述分析,文章提出了一种将区块链和联邦学习相结合的以实现高效节点选择和通信的新的分布式联邦学习架构,解放中央服务器,实现参与节点直接通信,并在此架构上提出了一种基于信誉的节点选择算法方案(RBLNS),对参与节点进行筛选,保证参与节点的隐私安全;仿真结果表明,RBLNS能够显着提高模型的实验性能。

关键词:分布式学习;区块链;联邦学习;节点选择;声誉值;隐私保护

Reputation-based Learning Nodes Selection Algorithm for Decentralized Federated Learning

QU Jing, FENG Yunxia
(School of Information Science and Technology, Qingdao University of Science and Technology, Qingdao 266061, China)

Abstract: Due to the increasing risk of privacy leakage, the collected data usually contains a large amount of privacy information, data collectors are reluctant to share their private data, which leads to result in "data silos". Federated learning enables data sharing without leaving the local area, but there are still some problems on sharing among multiple data. On the one hand, the centralized processing of central server suffers from expensive cost and single point of failure. On the other hand, for multi-institutional data sharing, model training might be affected by participating nodes mixed with malicious nodes, which leads to data privacy leakage. Therefore, Based on above analysis, a new distributed federated learning architecture is proposed to combine blockchain and federated learning, realize the efficient node selection and communication, and it enables direct communication between participation nodes instead of relying on central server. Based on the proposed architecture, a reputation-based node selection algorithm scheme (RBLNS) is proposed to screen the participating nodes, and ensure the privacy and security of the participating nodes. The experimental results show that the RBLNS significantly improves the test performance of the model.

Keywords: distributed learning; blockchain; federated learning; node selection; reputation value; privacy protection

0 引言

人工智能的飞速发展,机器学习促进了人们的衣食住行到航空航天等各个领域的变革,而这背后也都离不开大数据的支持。当今时代的发展又对机器学习提出了更高的要求,这就需要更多的数据进行训练。但由于数据中往往包含着大量的隐私信息,数据拥有者不愿意共享自己的数据,造成了“数据孤岛”问题。共享数据与隐私保护似乎成了两个相互矛盾的问题。直到物联网技术地快速发展,产生了大量且分散的数据。

谷歌提出的联邦学习[1]找到了解决数据共享与隐私保护之间的矛盾的新思路,联邦学习允许计算节点利用自己的数据集在本地进行训练,最后由中央服务器集中收集并聚合本地模型,避免了直接收集原始数据造成的隐私泄露风险。但传统联邦学习采用中央服务器集中收集、聚合全局模型,默认中央服务器可信,可能会造成隐私泄露风险。另一方面谷歌公司最初提出联邦学习是为了公司内部数据供共享,如果想要将联邦学习推广到开放的网络环境中,参与的计算节点中可能混入影响训练的恶意节点,他们可能发送错误的本地模型参数、攻击其他计算节点造成巨大地隐私泄露风险。所以选择合适的参与节点参与训练了对于模型的训练和隐私安全至关重要。

本文将区块链和联邦学习相结合提出一种分布式联邦学习,并基于此系统提出了一种基于信誉值的分布式节点选择算法。分布式联邦学习在将区块链和联邦学习相结合实现参与节点直接通信,取代了传统联邦学习通过中央服

收稿日期:2023-02-28; **修回日期**:2023-04-11。
基金项目:国家自然科学基金资助项目(61806107;61702135)。
作者简介:曲 静(1998-),女,硕士研究生。
通讯作者:冯云霞(1977-),女,博士,副教授,硕导。
引用格式:曲 静,冯云霞.基于声誉的分布式联邦学习节点选择算法[J].计算机测量与控制,2024,32(1):192-200.

务器转发信息地通讯模式。基于信誉值的分布式节点选择算法采用声誉作为节点可信度的衡量标准，对发布任务的节点以及执行任务的节点都进行筛选，并为此设计了一种基于角色的节点声誉值计算。

1　联邦学习研究现状

为解决传统联邦学习中央服务器带来的问题，文献［2-7］通过加密算法等方式预防联邦学习中的隐私泄露问题，文献［8-13］将区块链与联邦学习结合起来，借用区块链不可篡改等特性，解决此问题。文献［8］中将 C/S 架构下的工作模式移植到区块链系统，每个节点按照顺序循环担任中央服务器，中央服务器不固定，一定程度上可以有效克服单点失效。在文献［9］中提出了 DeepChain，将区块链技术与联邦学习结合起来，它鼓励不信任方参与隐私保护学习、共享梯度和正确更新参数，并最终以双赢的结果完成迭代式深度学习。联邦学习和区块链的结合开始逐渐在实际生活领域广泛研究，2020 年新冠肺炎的爆发，在文献［10］中针对 COVID-19，从不同医院收集少量数据，并使用基于区块链的联合学习训练一个全局深度学习模型用于检测新冠病毒。

为了解决联邦学习的参与者的可信度的问题，节点选择可以分为两个方向：一个是在训练开始之前对参与节点进行选择[14-19]，另一个是在训练过程中对节点上传的本地模型进行有选择地聚合[20-22]。

对于在训练开始之前选择参与节点方向，首先需要确定一个公平的衡量标准来量化节点在训练中的表现，并根据这个标准对节点进行筛选。在文献［14］中通过设置参与者节点上传本地训练模型的截止时间，选择截至时间内上传模型的节点，即计算和通信能力较好的节点，参与训练，以此缩短训练时间。在文献［15］中利用价值函数评估参与节点上传的本地训练结果对整体训练模型的价值，此评估结果为判断节点工作能力好坏的标准，并决定了节点被选择参与下次联邦学习的概率。在文献［16］中引入声誉值作为衡量标准，提出 EigenTrust 算法，利用曾与该节点共同训练的其他节点对该节点的评价计算声誉值，根据节点的行为为其生成声誉意见，并根据收集的声誉意见计算其声誉值，避免了某个节点的片面评价导致声誉值计算错误，从而影响节点的选择。在文献［17］中提出了一种名为 TNA-SL 的基于主观逻辑的参与节点可信度计算方法，从而在参与节点之间建立了信任网络。文献［18］引入不易被篡改的区块链记录声誉意见，保证声誉意见的真实性。文献［19］设计了一个分层信任评估模型，对不同层次的信任指数进行了评估，确定节点的可靠性。

对于训练过程中筛选本地模型聚合方面，主要是由于联邦学习不同于集中式机器学习，它的参与者数据集存在异构性的问题[20]，而 FedAvg 算法随机挑选上传本地模型进行聚合，这可能导致选择的本地模型并不利于了全局模型的收敛。在文献［21］中，为解决参与者数据集异构问题在提出一种名为“FedAdp”的主动加权算法，通过计算收到的本地模型与全局梯度之间的相似度，为本地模型在聚合时设置不同的权重。文献［22］在联邦学习中考虑到数据异构的问题，提出一个概率节点选择框架“FedPNS”，通过计算节点梯度和全局梯度的内积，判断收到的本地模型是否利于全局模型收敛，选择出最有利于全局模型收敛的本地模型子集进行聚合。

在本文，首先将区块链和联邦学习结合，提出一种新的分布式联邦学习，在区块链的架构中实现联邦学习，由任务发布节点代替中央服务器降低单点故障的风险。在此架构的基础上提出了一种基于声誉值的节点选择方法，分别筛选任务执行节点和任务执行节点，引入区块链的共识节点记录声誉意见。为了计算节点的声誉值本文又设计了一种基于角色的节点声誉值计算算法，选择更加适合任务的节点集进行训练。

2　前期准备

在详细阐述节点选择算法之前，本节将介绍本文针对的恶意节点以及系统假设和提出的分布式联邦学习系统模型。

2.1　实验假设

在开放的网络环境中，参与节点混入恶意节点会影响任务的训练，甚至对数据隐私造成威胁[23]。本文重点考虑了主动恶意任务发布节点、被动恶意任务发布节点、主动恶意任务执行节点和被动恶意任务执行节点 4 种类型的万一节点。主动，即恶意节点在任务训练过程中未受到外部干扰主动发起恶意行为；被动，即恶意节点由于外界因素干扰发起恶意行为。主动恶意任务发布节点主动广播虚假任务，恶意分散系统的总算力；而被动恶意任务发布节点被其他节点攻击、控制发布虚假任务，分散系统的总算力。主动恶意任务执行节点故意上传低质量本地模型，甚至故意攻击其他节点，影响全局模型精度甚至造成数据隐私泄露。被动恶意任务执行节点受到自身数据集质量、CPU 计算能力和网络通信条件等外部条件的影响[24]，导致模型不合格或每次迭代的收敛时间受到影响，影响全局模型的训练。

本文假设面向开放的网络环境，如果节点随意加入，会导致系统很高的安全风险，因此本文选择联盟链。所有参与者只有通过身份验证加入联盟链，才有资格发布任务或者参与模型训练，保护参与者的身份隐私。在执行联邦学习过程中节点可能充当两种角色：一种是发布任务的任务执行节点，另一种是执行任务的任务执行节点。而且本文支持节点角色可以动态转换，节点可以担任多角色，即一个联盟链中节点可以在上个任务中担任任务发布节点，在本次任务中担任任务执行节点，甚至一个节点没有任务需求，也不想参与协同训练时也可以申请作为区块链的共识节点，参与共识任务。本文中由任务发布节点充当临时主控节点替代传统联邦学习的中央服务器，且在独立通道 channel 中进行每个联邦学习，让任务发布节点与任务执行

节点的直接通信，而且每个任务独立训练，实现多任务并行训练。联盟链的共识节点在联邦学习训练过程中担任验证节点的角色，负责筛选任务发布节点、根据节点在训练中的行为生成用于计算声誉值的声誉意见存储。联盟链同时维护声誉意见以及联邦学习交易两个账本，既保证联邦学习都记录上链，也能方便快速查找声誉意见。验证节点采用实用拜占庭容错算法（PBFT）达成共识将声誉意见以及行为证据形成区块记录上链。

2.2 分布式联邦学习系统

本文提的分布式联邦学习系统，如图 1，具体运行流程如下：

1）筛选节点。任务发布节点发布任务，验证节点区块链上的声誉意见链上查询节点的声誉值，实现对任务发布节点以及任务执行节点的筛选（节点筛选的详细细节在第 3 章）。

2）联邦学习初始化。联邦学习确定了任务执行节点后，首先为参与训练的节点分配数字证书并设置权限，持有数字证书的参与者可以通过 channel 进行通信，实现多任务并行训练，设置权限，以实现任务执行节点之间无通信无法窃取其他节点上传的本地模型，保证数据隐私安全。

3）联邦学习迭代训练。任务发布节点发送初始全局模型，任务执行节点收到全局模型在本地数据集上训练得到一个本地模型并上传到任务发布节点；然后任务发布节点对本地模型进行筛选（本地模型的具体筛选细节在第 3 章详细介绍），将符合要求的数据集利用联邦平均算法聚合成全局模型。再发送给任务执行节点，进入下一轮的迭代训练，直到最终模型符合任务发布节点的要求，或者迭代次数达到上限，训练结束。

4）生成并存储声誉意见。验证节点根据节点在训练过程中的行为，任务发布节点以及任务执行节点分别生成声誉意见，达成共识，共识认为正确，则记录为可信行为，共识认为错误则记录为不可信行为，否则记录为不确定行为，记录上声誉意见账本。①生成任务发布节点的声誉意见：任务发布节点对任务执行节点进行筛选之后，对任务执行结果的筛选结果达成共识，记录声誉意见；任务发布节点筛选本地模型结束之后，验证节点对筛选结果以及聚合结果达成共识，记录声誉意见。②生成任务发布执行节点的声誉意见：根据任务发布节点的筛选结果，参与聚合的任务执行节点本地模型按照精度利用 softmax 生成一个数值记录在声誉意见中，没参与聚合的任务执行节点记录为 0。

3 基于声誉值的节点选择算法（RBLNS）

在本节中，将介绍基于信誉的节点选择算法，声誉值是根据节点之前行为预测的节点在接下来的行为中可信的概率，声誉值根据区块链中存储的声誉意见进行计算，声誉值计算的详细介绍在第 4 章。由于恶意节点也可能充当任务发布节点发布虚假消息浪费系统整体算力，攻击其他节点，而且本地模型更新的精度决定了最终全局模型的精度，低质量的本地模型更新甚至会拉低全局模型的精度，所以本文对任务执行节点、任务发布节点，根据节点的声誉值在节点之间按照角色横向选择，同时还对上传的本地模型都进行筛选。

3.1 筛选任务发布节点

任务发布节点的筛选在节点广播发布任务请求之后，由验证节点进行筛选，只有通过筛选的节点才有资格组织联邦学习。当有任务需求的联盟链节点广播“任务发布请求”申请发布任务之后，验证节点对发布请求节点进行筛选，具体筛选过程如下：

1）当验证节点收到“任务发布请求”广播，首先检验该节点是否有正在执行的任务，有的话则忽略该“请求”，没有其他任务则进入第二步验证。这是由于当前计算机的

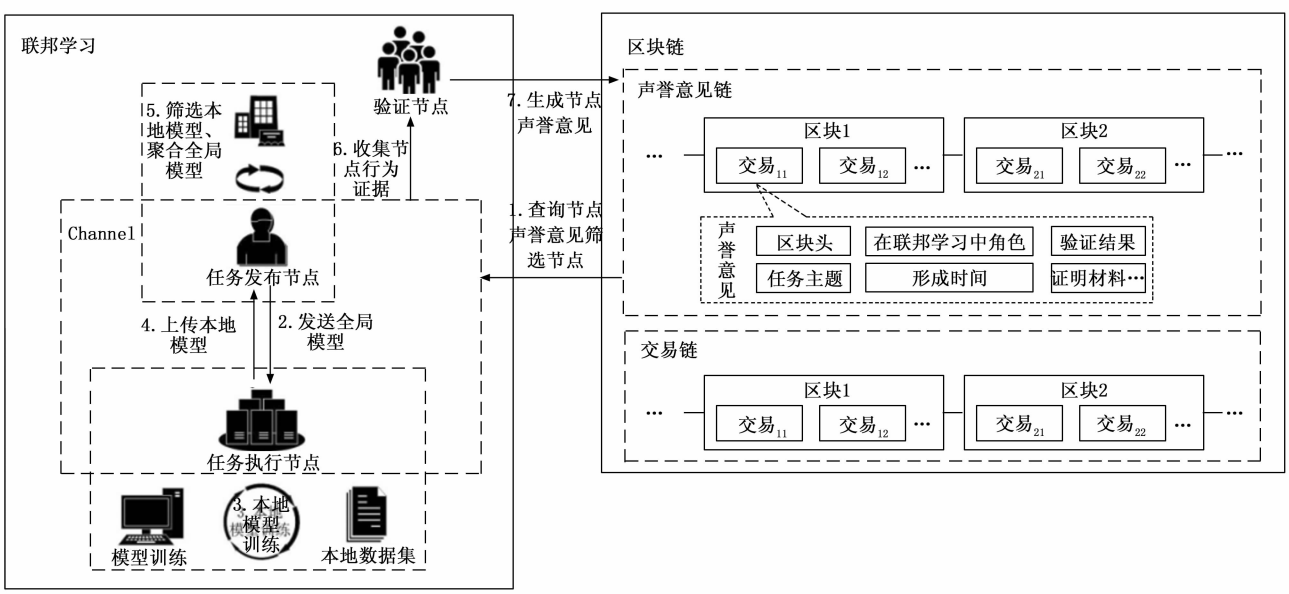

图 1 分布式联邦学习系统架构图

算力可能无法满足同时进行多项训练，而任务发布节点在联邦学习任务中至关重要，一旦任务发布节点的算力被分散将会造成整体训练的延时甚至造成最终模型无法收敛，因此本文中任务发布节点只允许同时至多参与一项任务。以后的发展中节点算力充足则可以省略这一步的筛选。

2）验证节点检验请求发布节点的声誉值。验证节点在联盟链的声誉值账本中查询该节点的声誉意见并计算出该节点的声誉值（声誉值计算的具体细节在第 4 章详细介绍）。如果节点声誉值低于阈值则忽略该“请求”；否则确定该节点为任务发布节点，同时广播带有签名的“任务 T 启动请求”，达成共识记录上链，交易账本更新。

3.2　筛选任务执行节点

任务执行节点接收到任务发布节点发送的“任务发布请求”之后，先在交易账本中查询该任务，查询显示该任务通过验证无误后发送“申请加入任务请求”申请加入任务，否则忽略任务启动请求。随后由任务发布节点对申请协同训练的节点进行筛选。具体步骤如下：

1）节点发送“申请加入任务请求”。联盟链上节点根据任务发布节点发送的“任务启动请求”中的任务要求，满足任务要求的节点自愿发送“申请加入任务请求”，内容包括拥有的数据集大小、种类以及可以验证数据集的证明材料。

2）任务发布节点对申请加入任务的节点进行筛选。任务发布节点收到“申请加入任务请求”后，首先在声誉意见账本中查询该节点作为任务发布节点的声誉意见，然后计算该申请节点的声誉值，如果声誉值不低于阈值，该节点被选为任务执行节点，否则忽略该节点请求。直到任务执行节点数达到任务要求，或者超过截至时间筛选结束。

声誉值低于阈值说明在之前的训练任务中存在恶意行为（主动或者被动）、该节点的数据集不适合当前任务，通过声誉值计算识别选择诚实可信且拥有数据集最合适当前任务的任务执行节点集进行协同训练。

3.3　筛选本地模型

任务执行节点每轮训练上传本地模型到任务执行节点，任务执行节点在训练集上进行测试，筛选出符合条件的本地模型进行聚合，删除低精度模型，以得到高质量的最终模型。具体过程如下：

1）聚合所有收到的本地模型。任务发布节点收到本地模型之后，将所有本地模型聚合成整体模型 M。

2）筛选本地模型。删除其中第一个本地模型聚合成检验模型 m_l，并将检验模型 m_l 与整体模型 M 在测试集上进行测试，如果检验模型 m_l 的精度大于整体模型 M，就淘汰该本地模型。按照上述方式遍历所有本地模型，完成所有本地模型的初步筛选。

3）确定最终参与聚合的本地模型。聚合经过上轮筛选保留下来的本地模型得到检验模型 m_k，将检验模型 m_k 与测试集上进行测试，比较所有检验模型集合与整体模型 M 的精度，选择精度最高的模型作为本轮最终全局模型，而对应的本地模型作为最终参与聚合的本地模型。

4　基于角色的节点声誉值计算模型

为了实现对任务发布节点和任务执行节点的分别筛选，又考虑到任务发布节点和任务执行节点在联邦学习中任务不同，任务发布节点发布任务、筛选本地模型、聚合全局模型，只需筛选行为可靠、设备算力充足的诚实节点，而任务执行节点需要利用自己的数据集在本地进行训练并上传到任务发布节点处，这不仅需要考虑节点的行为以及设备算力，还要考察节点的数据集与当前训练主题的贴合度，因为数据集的类型和质量决定了本地模型的精度，本地模型精度不高也将影响去全局模型的精度。所以为了实现任务发布节点和任务执行节点的分别筛选，本文设计了一种基于角色的节点信誉值计算模型，细化不同节点的声誉计算要素，根据节点角色及节点行为量化节点在训练中的可信度。而一个联盟链中可能储存这一个节点的两种角色的声誉意见。该模型主要包括两部分：节点声誉意见模型和节点声誉值计算算法。

4.1　基于角色的节点声誉意见模型

在联邦学习训练任务中，本文用声誉意见直接记录各节点在任务中表现情况量化生成一条声誉意见，节点声誉意见模型为（$role$，$result$，$time$，$remark$，$sign$，H），其中 $role$ 表示节点在任务中的角色，包括 $publisher$（任务发布节点）和 $worker$（任务执行节点）；$result$ 是节点行为检验结果，任务执行节点的声誉意见记录为数值，任务发布节点记录为：“$true$”、“$false$”和“$uncertainty$”，分别表示可信行为、不可信行为和不确定行为；$time$ 是声誉意见生成时间，$sign$ 是生成声誉意见的验证节点签名，$remark$ 是声誉意见的生成证明材料和任务主题，H 是信誉意见的加密结果。接下来本文将分别详细介绍任务发布节点和任务执行节点的声誉意见。

4.2　节点声誉值计算模型

为了缩短每个任务开始之前计算节点声誉值的时间，本文在每个任务结束后，利用任务内产生的声誉意见生成节点的直接声誉值，节点的声誉意见作为可追溯证据存储在区块链中。下次任务开始之前直接在区块链中检索节点对应角色的直接声誉值来计算声誉值。又考虑到多次以某身份参与联邦学习任务的节点区块链中存储大量对应声誉值，而初次以某种角色参与任务的节点在区块链中没有存储对应直接声誉值，因此本文基于节点参加任务的角色以及该节点以此角色参与任务的次数细化算法，设计了 4 种节点信誉值计算算法：二次任务发布节点声誉值计算算法、首次任务发布节点声誉值计算算法、二次任务执行节点声誉值计算算法、首次任务执行节点声誉值计算算法。其中“二次”和首次分别指该节点多次和首次担任此角色参与任务。首先根据节点的申请判断节点的角色，随后在区块链中查询节点的对应角色的直接声誉值，如果查询到，那么说明节点是“二次”节点，否则节点为“首次”节点，按照对应算法计算声誉值。

接下来将首先介绍直接声誉值计算算法，随后分别详细介绍二次任务发布节点声誉值计算算法、首次任务发布节点声誉值计算算法、二次任务执行节点声誉值计算算法、首次任务执行节点声誉值计算算法。

4.2.1 直接声誉值计算

由于任务发布节点与任务执行节点的声誉意见模型中“*result*”存储类型不同，本文分别计算二者的直接声誉值。具体计算过程如下：

1）任务发布节点直接声誉值计算模，本文综合考虑声誉意见中的可信、不可信和不确定性行为，并通过增加不可信行为的权重，以增加恶意行为的代价，任务发布节点的直接声誉值的具体计算过程如式（1）：

$$\begin{cases} r(publisher)=\lambda N(result[t])-\gamma N(result[f])+ \\ \qquad \zeta N(result[u]), \\ \lambda,\gamma,\zeta\in[0,1], \\ \lambda+\gamma+\zeta=1, \\ \lambda<\gamma, \end{cases} \tag{1}$$

$r(publisher)$ 表示该任务发布节点经过本次训练任务的直接声誉值，$N(result[t])$、$N(result[f])$、$N(result[u])$ 分别表示在联盟链记录的本轮任务中该节点的所有声誉意见中 *result* 记录是“*true*”、“*false*”和“*uncertainty*”的数目，λ,γ,ζ 分别表示 *result* 中可信行为、不可信行为和不确定行为的影响参数。

2）任务执行节点直接声誉值计算模型，即对声誉意见中的数值求平均，具体计算过程如式（2）：

$$r(worker)=\frac{\sum result}{N} \tag{2}$$

$r(worker)$ 表示该任务执行节点经过本次训练任务的直接声誉值，$\sum result$ 表示在联盟链记录的本轮任务中该任务执行节点的所有声誉意见 *result* 中的，N 表示本轮任务中该任务执行节点的所有声誉意见的数目。

任务执行节点和任务发布节点的直接声誉值计算完成后，验证节点将对此计算结果达成的共识，随后该验证节点将本轮任务中所有节点的直接声誉值按照 $r=(role,time,score,remark,H)$ 的格式保存在区块链中，其中 r 表示所记录节点的直接声誉值，*time* 记录为本次任务结束的时间，*score* 表示本次任务中该节点的直接声誉值，*remark* 是备注信息，存储本次任务主题和开始、截止时间。

4.2.2 二次任务发布节点声誉值计算算法

以二次任务发布节点 i 为例，介绍二次任务发布节点声誉值计算模型。当验证节点接收到申请节点发布任务申请之后，首先在联盟链中查询节点 i 作为任务发布节点的直接声誉值，查询到相应直接声誉值，判断节点为二次任务发布节点进行声誉值计算。在二次任务发布节点声誉值计算算法中，考虑到节点和网络的复杂性，随着时间的推移，节点先前行为的可信度逐渐降低，对应的直接声誉值的可参考性也逐渐降低。因此，本文引入时间衰减函数来描述时间对直接声誉值可信度的影响。生成的直接声誉值与当前任务间隔的时间越长，该直接声誉值的可参考性越低，计算最终声誉值时的权重越小，反之该直接声誉值的可参考性越高，计算最终声誉值时的权重越大。所以任务发布节点的最终声誉值如式（3）：

$$\begin{cases} R(publisher_i)= \\ \qquad \dfrac{\sum_{publisher_{i1}\in publisher_i^{all}} T(publisher_i)*r[publisher_i(score)]}{\sum_{publisher_i\in publisher_i^{all}} T(publisher_i)} \\ T(publisher_i)=\beta^{time-r[publisher_i(time)]},\beta\in(0,1) \end{cases} \tag{3}$$

$publisher_i$ 表示节点 i 作为任务发布节点；$R(publisher_i)$ 是节点 i 在本次任务之前计算的作为任务发布节点的声誉值；$T(t_i)$ 是引入的时间衰减函数；$r[publisher_i(score)]$ 是联盟链中储存的节点 i 作为任务发布节点的直接声誉值。β 是时间新鲜度的衰减参数，用于调节时间对于最终声誉值的影响程度；$r[publisher_i(time)]$ 表示查询的节点 i 任务发布节点直接声誉值中记录的时间；$publisher_i^{all}$ 是在联盟链中查询到的节点 i 作为任务发布节点的所有直接声誉值。

4.2.3 首次任务发布节点声誉值计算算法

接下来将以首次任务发布节点 g 为例，介绍首次任务发布节点声誉值计算模型。当验证节点接收到申请节点发布任务申请之后，首先在联盟链中查询节点 g 作为任务发布节点的直接声誉值，查询无果之后，判断节点为首次任务发布节点并令其声誉值等于初始值（任务发布方的信誉值阈值），如式（4）：

$$R(publisher_g)=R_{initial}(publisher) \tag{4}$$

$R(publisher_g)$ 是节点 g 作为任务发布方参与本轮训练的声誉值，$R_{initial}(publisher)$ 是对于任务发布方的信誉阈值。

4.2.4 二次任务执行节点声誉值计算算法

以二次任务执行节点 j 声誉值计算算法为例计算其声誉值。在一个任务中，任务执行节点的主要工作是在本地训练模型并上传训练，本地模型的好坏不仅与节点的行为有关，还与节点的本地数据集有关。所以想要筛选任务执行节点，需要考虑综合考虑其行为及数据集的可靠性。在本文引入余弦函数计算节点直接声誉值记录的任务与当前任务的相似度，相似度直接参与最终信誉值的计算。相似度越大，表示直接信誉值记录的任务与当前任务越接近，节点 j 在直接声誉值所记录的任务对于当前任务的可参考性越大；反之可参考性越小。节点 j 的最终信誉值的计算过程如式（5）：

$$\begin{cases} R(worker_j)=\dfrac{\sum_{worker_j\cdot worker_j^{all}} w(worker_j)*r(worker_j)}{\sum_{d_j\cdot d_j^{all}} w(worker_j)} \\ w(worker_j)=\cos(r[worker_j(type)],type)-a,a\cdot(0,1) \end{cases} \tag{5}$$

其中：$worker_j$ 表示节点 j 作为任务执行节点，$R(worker_j)$ 是任务执行节点 j 的最终声誉值；$w(worker_j)$ 是引入余弦函数计算节点 j 作为任务执行节点的直接声誉值记录的任务主题与当前任务主题的相关度，$\cos(r[worker_j(type)],type)$

是利用余弦函数计算节点 j 的数据类型与任务发布数据类型的相似度，首先将两个数据类型描述转换成两个向量，随后利用余弦函数计算两个向量之间的距离得到两个数据类型描述的相似度；$r(worker_j)$ 是节点 j 区块链中存储的直接声誉值；$r[worker(type)]$ 是的直接声誉值中存储的任务主题；$type$ 是当前任务的主题；α 是熟悉度调节因子；$worker_j^{all}$ 是在联盟链中查询到的节点 j 作为任务执行节点的所有直接声誉值，类似二次任务发布节点声誉值计算算法，本文引入时间衰减函数，用来描述时间对直接声誉值可参考性的影响，式（5）可以改写为：

$$\begin{cases} R(worker_j) = \dfrac{r[worker_j(score)]}{\sum\limits_{d_j \in d_f^{all}} T(worker_j) * w(worker_j)} \\ T(worker_j) = \beta^{time-r[worker_j(time)]}, \beta \in (0,1) \end{cases} \quad (6)$$

$T(worker_j)$ 引入的时间衰减函数，$r[worker_j(time)]$ 表示节点 j 作为任务执行节点的直接声誉值记录中的时间。

4.2.5　首次任务执行节点声誉值计算算法

对于首次任务执行节点参加过训练任务的节点 f，本文结合他的数据集大小、数据类型和其他数据提供者的中值声誉值来计算他的声誉值。如果节点 f 的数据集较大且数据集类型更接近当前任务的主题，则节点 f 的声誉值越高，具体计算如下（7）：

$$\begin{cases} R(worker_f) = w(worker_f) * s(worker_f) + R_{initial}(worker) \\ w(worker_f) = \cos(r[worker_f(type)], type) - \alpha \\ s(worker_f) = \dfrac{S(worker_f) - S}{S_{\min} - S} \\ \alpha \in (0,1) \end{cases} \quad (7)$$

$worker_f$ 指代节点 f 作为任务执行节点；$s(worker_f)$ 是节点 f 的响应中记录的数据集大小；$S_{\min}$ 是所有参加本任务的所有任务执行节点数据集大小的中位数；S 是任务要求的数据集大小；$R_{initial}(worker)$ 是当前任务中任务执行节点的声誉值初始值；$w(worker_f)$ 表示节点 f 的数据集的数据类型与任务规定数据类型的相似情况；$S(worker_f)$ 表示节点 f 数据集大小与任务要求数据集大小的比较情况。

5　结果验证与性能分析

为了验证所提方法的有效性，本文选择两种对比系统进行实验比较。其中一种方法是一个传统声誉值节点选择算法[16]。另一种是方法是利用基于主观逻辑的声誉值计算模型筛选任务执行节点，在计算节点声誉值时参考所有与筛选节点共同训练过的节点对于筛选节点的评价，并引入区块链存储节点的声誉意见[18]，分别简称为 TRM 和 SLM，本文的模型称为 RBLNS。设置了手写数字分类和函数回归两类实验来测试 3 个模型的效果。接下来将介绍实验环境设置并分析分类实验、回归实验的结果。

本文的分布式联邦学习系统建立在 Fabric 平台上，共识算法选择 PBFT，预选 20 个验证节点，平均出块时间为 2 s。实验中的一些参数设置为：$\beta = 0.7$，$\zeta = 0.1$，$\lambda = 0.2$，$S = 20$，$\gamma = 0.7$，$\alpha = \sqrt{2}/2$，$R_{\text{initial}}(t) = R_{\text{initial}}(d) = 0.5$。

联邦学习任务中存在 50 个任务执行节点，其中 10 个节点也担任任务发布节点（8 个可靠的和 2 个不可靠的任务发布节点）。所有任务执行节点的数据集都存储在 IPFS 中，便于检索数据集的大小和类型。

对于手写数字分类实验，本文使用基于卷积神经网络的模型来执行数字识别任务，以评估由 Pytorch 框架实现的节点选择模型。在实验中，使用 MNIST 数据集，该数据集有 60 000 个训练示例和 10 000 个测试示例，广泛用于联邦学习的性能评估实验[24-25]。在 MNIST 训练数据集中，对于诚实的高质量任务执行节点，分配的数据集涵盖所有 10 个类别（0～9），通过为各任务执行节点有差别随机分配每个类别数据的量，模拟诚实任务执行节点的数据集主题与训练任务主题之间的差异；通过为各任务执行节点分配不同数量的数据，模拟诚实任务执行节点的数据集的大小差异。为恶意节点分配少量或缺失某个类别的数据，从而导致上传低质量本地模型。恶意任务发布节点通过发布虚假任务、错误筛选任务执行节点、错误聚合最终结果。

对于回归函数的训练，本文选择了 30 个任务执行节点来共同训练函数 $y = \cos(2\pi x)$，$x \in [0,1]$ 是联邦学习的输入，y 作为输出。其中 25 个诚实可靠的节点，以及 5 个恶意节点。25 个诚实节点有 20～30 个相关训练数据样本，5 个恶意节点中，2 个节点有 10 个相关训练样本，2 个节点有 5 个相关训练样本，1 个数据节点有 20 个不相关训练数据样本。恶意节点的处理与手写数字识别实验一样对应的减少数据集的大小。

5.1　手写数字识别分类实验分析

首先发布任务“识别手写数字 1”，通过调节可信任务执行节点数据集中手写数字 1 的图片比例，来模拟不同任务执行节点数据集的主题与任务要求的相关度不同，例如相关度为 60％意味着 100 张图片中只有 60 张是手写数字 1 的图片。如图 2，可以发现数据集过小或者数据集与任务要求的相似度较低都会影响训练的模型精度。当数据集大小为 200，数据集的任务相关度在 100％时，模型精度为 90.1％，而数据集的任务相关度在 60％时，模型精度仅为 83.2％，大约降低 7 个百分点；同样的当数据集任务相关度在 90％，数据集大小在 1 000 时，精度为 91.7％，而数据集大小在 200 时，精度仅为 89.1％，大约降低了 3 个百分点。由此可以看出，拥有低质量数据集（数据集太小或者与任务相关性低）的恶意节点会生成低质量本地模型，所以对参与任务执行节点进行筛选。

5.1.1　手写数字识别

本节将从手写数字识别结果、恶意节点声誉值变化情况、恶意节点识别能力、聚合模型的准确率 4 个方面对 3 种模型进行比较。

图 3 展示了 RBLNS、SLM、TRM 三种模型对手写数

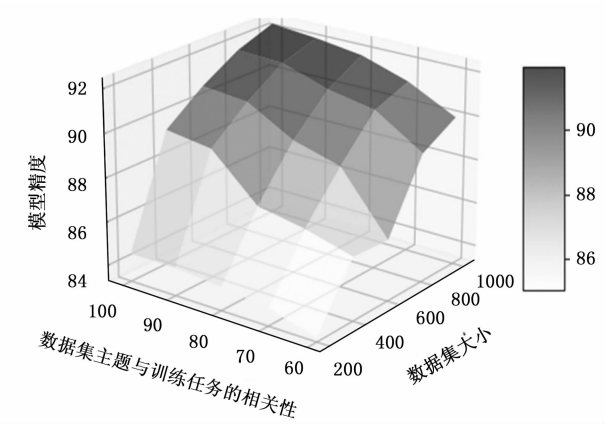

图 2 数据质量对于模型精度的影响

字识别结果。最左边数字是 RBLNS 识别结果，中间数字是 SLM 的识别结果，最右边数字是 TRM 的识别结果。对于总共 20 个手写数字，RBLNS 可以正确识别 18 个数字，而 TRM 和 SLM 可以分别识别 17 个和 16 个。一方面是由于 RBLNS 在筛选任务执行节点时不仅以节点行为为筛选标准，还考虑节点的数据集与当前任务的贴合程度，从而筛选出行为可靠、数据集与任务需求高度相匹配的最佳任务执行节点集合进行训练。另一方面是由于 RBLNS 在联邦学习聚合模型过程中对本地模型进行筛选，通过筛选本地模型再聚合全局模型替代传统联邦学习的随机聚合，从而提高了识别能力。

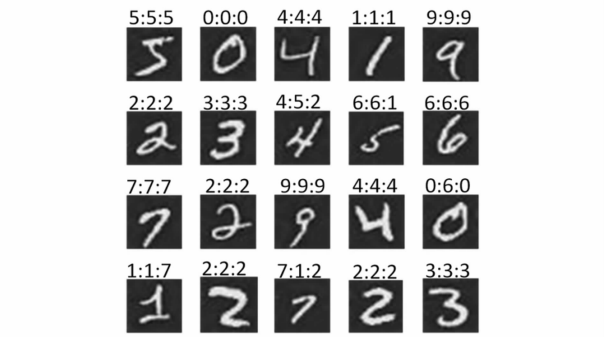

图 3 一个联邦学习识别手写数字的例子

5.1.2 恶意节点声誉值变化情况

在对手写数字分类任务中，为了验证 3 种方法对于二次任务执行节点的筛选情况，假设任务执行节点在执行任务 T 之前至少会执行 6 个任务，且表现诚实可靠。然后恶意节点突然出现异常行为，实验结果如图 4 所示。3 种模型中对于突然出现异常行为的节点声誉值都开始下降。而 RBLNS 在最短时间下降了最大幅度，可以快速识别恶意节点。这是由于 RBLNS 方法中通过对节点上传的本地模型进行验证生成节点声誉意见，恶意任务执行节点一旦行为表现异常，即上传低质量本地模型，验证节点会立即对他生成一个验证结果值为 0 的声誉意见，且本文加大了对于恶意行为的权重，这将导致任务结束之后的直接声誉值很低，又由于考虑了时间对于直接声誉值的影响，短时间内生成的声誉意见在计算最终声誉值的权重较大，所以 RBLSN 在短时间内下降的幅度最大。

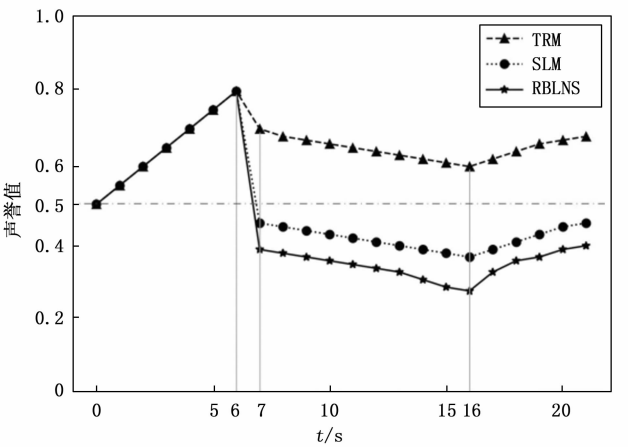

图 4 恶意节点在 3 种模型下声誉值随时间的变化

5.1.3 恶意节点识别能力

本文通过调整恶意节点相互勾结的比例来比较 3 种模型选择节点的能力。实验结果如图 5 所示。实验设置了 4 组具有不同程度勾结的参与节点，勾结程度分别是 0.0、0.1、

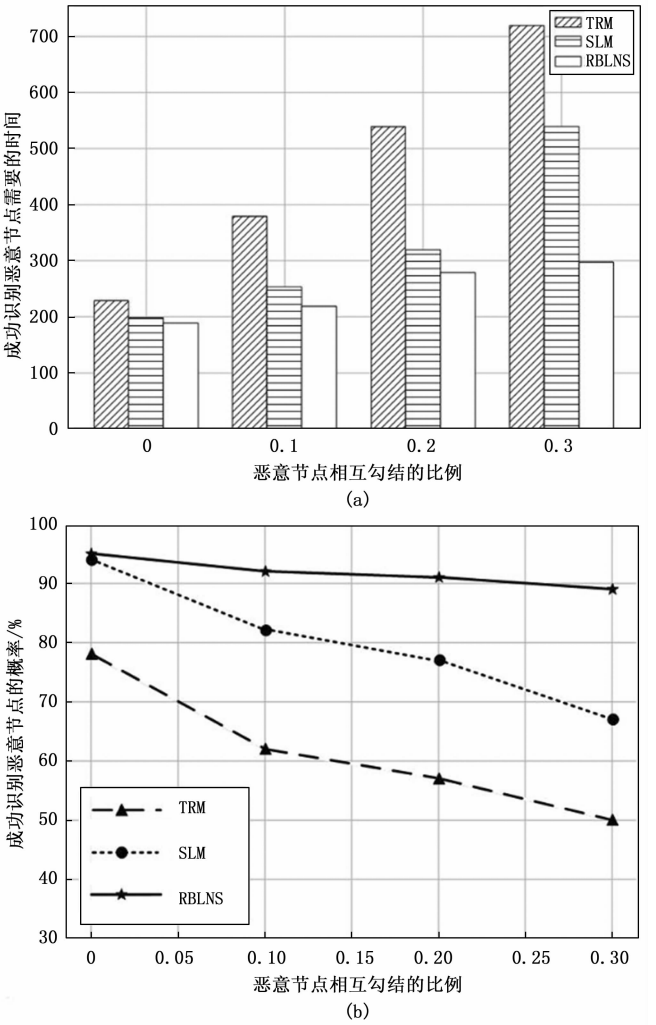

图 5 恶意节点互相勾结情况中 3 种模型的表现

0.2、0.3，0.0 表示节点相互勾结的可能行为 0，而 0.1 表示节点相互勾结的可能性为 10%，0.2 表示节点相互勾结的可能行为 20%，0.3 表示节点相互勾结的可能性为 30%（此时被动恶意节点的数量小于 30%）。

如图 5（a）所示，在恶意节点之间不相互勾结的情况下，所有的方法都能在 300 秒内完全识别恶意节点。然而，当恶意节点之间相互勾结程度增加到 0.2 和 0.3 时，RBLNS 识别时间比其他两种模型都短。因为 RBLNS 的声誉意见由验证节点生成并达成共识记录在区块链中，少数恶意节点相互勾结并不会影响共识结果。然后进一步比较了 3 种模型在不同恶意节点相互勾结情况下将恶意节点识别出来的成功率，从图 5（b）中可以看出，当所有节点相互勾结程度为 0.05～0.15 时，SLM 和 RBLNS 筛选成功率都比较高，但当恶意节点相互勾结率上升为 0.2～0.3 时，SLM 的识别成功率明显降低，RBLNS 成功率仍然比较高。

5.1.4　全局模型精度

图 6 显示了在参与节点中恶意节点比例为 20%的情况下，随着 FL 迭代次数的增加，全局模型精度的变化。从这个图，可以看到随着迭代次数的增加，3 种模型的最终训练精度都有所提高。五角星符号标记了模型成功收敛，与 TRM 和 SLM 相比，RBLNS 的全局模型精度略高于这两个模型，收敛所需的迭代次数也减少。

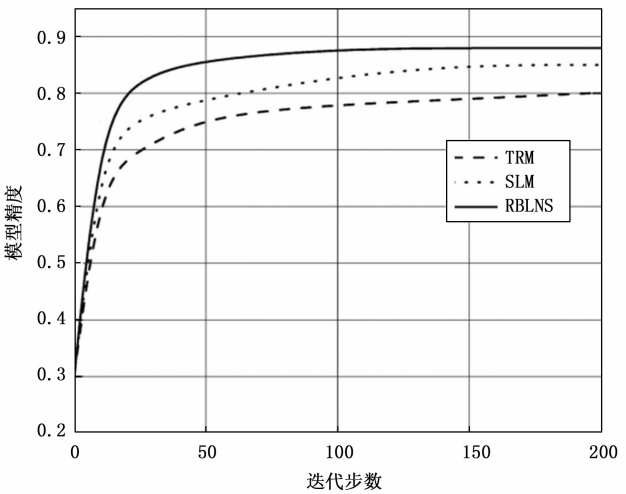

图 6　当恶意节点比例为 20%时，随着迭代次数的变化，模型精度发生的变化

5.2　回归实验分析

在图 7 展示了在拟合回归函数 $y=\cos(2\pi x)$ 的实验中，利用 3 种方法分别训练得到的函数模型随着输入的 x 的变化曲线。可以看到，RBLNS 在最佳拟合函数方面的表现优于 TRM 和 SLM。由于 RBLNS 为任务选择最佳的任务执行节点集进行协同训练，使得每次迭代的拟合效果更好，提高了学习速度。

6　结束语

在本文中，本文提出了分布式联邦学习系统并在此基础上提出基于声誉的学习节点选择算法。本文使用区块链的共识节点生成声誉意见，利用区块链的不易篡改的特性管理声誉意见。在每个任务开始前，利用基于声誉值的节点选择算法，对任务发布节点和任务执行节点分别进行选择。又考虑到任务中节点角色的变化，不同的任务对应不同的角色。针对不同的角色，设计了基于角色的声誉值计算模型，计算任务发布节点以及任务执行节点的声誉值分别计算，也实现首次参与任务的节点与多次参加任务的节点声誉值的分别计算。考虑到不同节点本地模型更新的异构性，而且本地模型的准确性会干扰模型聚合，本文会对收到本地模型筛选后聚合。实验结果表明，该算法能提高训练精度，缩短收敛时间。

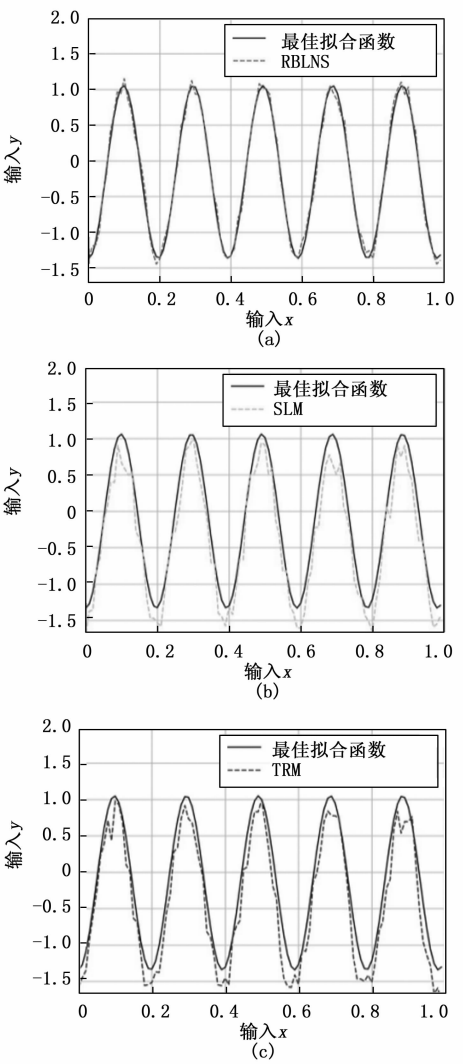

图 7　联邦学习回归函数图例

参考文献：

[1] MCMAHAN B, MOORE E, RAMAGE D, et al. Communication-efficient learning of deep networks from decentralized data [C] //Artificial intelligence and statistics. PMLR, 2017: 1273－82.

[2] 康海燕，冀源蕊. 基于本地化差分隐私的联邦学习方法研究 [J]. 通信学报，2022，43 (10)：94 - 105.
[3] 路宏琳，王利明，杨 婧. 一种新的参数掩盖联邦学习隐私保护方案 [J]. 信息网络安全，2021，(8)：26 - 34.
[4] FEREIDOONI H，MARCHAL S，MIETTINEN M，et al. SAFELearn：secure aggregation for private federated learning [C] //2021 IEEE Security and Privacy Workshops (SPW). IEEE，2021：56 - 62.
[5] MA X，ZHOU Y，WANG L，et al. Privacy-preserving byzantine-robust federated learning [J]. Computer Standards & Interfaces，2022，80：103561.
[6] MOTHUKURI V，PARIZI R M，POURIYEH S，et al. A survey on security and privacy of federated learning [J]. Future Generation Computer Systems，2021，115：619 - 40.
[7] QU Y，GAO L，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 - 83.
[8] KUO T-T，GABRIEL R A，OHNO-MACHADO L. Fair compute loads enabled by blockchain：sharing models by alternating client and server roles [J]. Journal of the American Medical Informatics Association，2019，26 (5)：392 - 403.
[9] WENG J，WENG J，ZHANG J，et al. Deepchain：Auditable and privacy-preserving deep learning with blockchain-based incentive [J]. IEEE Transactions on Dependable and Secure Computing，2019，18 (5)：2438 - 55.
[10] KUMAR R，KHAN A A，KUMAR J，et al. Blockchain-federated-learning and deep learning models for covid-19 detection using ct imaging [J]. IEEE Sensors Journal，2021，21 (14)：16301 - 14.
[11] 方 晨，郭渊博，王一丰，等. 基于区块链和联邦学习的边缘计算隐私保护方法 [J]. 通信学报，2021，42 (11)：28 - 40.
[12] KIM H，PARK J，BENNIS M，et al. Blockchained on-device federated learning [J]. IEEE Communications Letters，2019，24 (6)：1279 - 83.
[13] 朱建明，张沁楠，高 胜，et al. 基于区块链的隐私保护可信联邦学习模型 [J]. 计算机学报，2021.
[14] NISHIO T，YONETANI R. Client selection for federated learning with heterogeneous resources in mobile edge [C] //ICC 2019-2019 IEEE international conference on communications (ICC). IEEE，2019：1 - 7.
[15] CHO Y J，WANG J，JOSHI G. Towards understanding biased client selection in federated learning [C] //International Conference on Artificial Intelligence and Statistics. PMLR，2022：10351 - 75.
[16] KAMVAR S D，SCHLOSSER M T，GARCIA-MOLINA H. The eigentrust algorithm for reputation management in p2p networks [C] //Proceedings of the 12th international conference on World Wide Web. 2003：640 - 51.
[17] JOSANG A，HAYWARD R，POPE S. Trust network analysis with subjective logic [C] //Conference Proceedings of the Twenty-Ninth Australasian Computer Science Conference (ACSW 2006). Australian Computer Society，2006：85 - 94.
[18] KANG J，XIONG Z，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 - 14.
[19] WANG D，YI Y，YAN S，et al. A node trust evaluation method of vehicle-road-cloud collaborative system based on federated learning [J]. Ad Hoc Networks，2023，138：103013.
[20] FALLAH A，MOKHTARI A，OZDAGLAR A. Personalized federated learning with theoretical guarantees：A model-agnostic meta-learning approach [J]. Advances in Neural Information Processing Systems，2020，33：3557 - 68.
[21] WU H，WANG P. Fast-convergent federated learning with adaptive weighting [J]. IEEE Transactions on Cognitive Communications and Networking，2021，7 (4)：1078 - 88.
[22] WU H，WANG P. Node selection toward faster convergence for federated learning on non-iid data [J]. IEEE Transactions on Network Science and Engineering，2022，9 (5)：3099 - 111.
[23] CHEN X，JI J，LUO C，et al. When machine learning meets blockchain：A decentralized，privacy-preserving and secure design [C] //2018 IEEE international conference on big data (big data). IEEE，2018：1178 - 87.
[24] ZHU X，LI H，YU Y. Blockchain-based privacy preserving deep learning [C] //International Conference on Information Security and Cryptology. Springer，2018：370 - 83.
[25] KANE K，BROWNE J C. Using uncertainty in reputation methods to enforce cooperation in ad-hoc networks [C] //Proceedings of the 5th ACM workshop on Wireless security. 2006：105 - 13.

(上接第 191 页)

[15] 陈经锋. 散射宽带通信技术在文昌 13 - 1/2 油田的应用 [D]. 西安：西安电子科技大学，2011.
[16] 方 波. 散射通信调制解调技术研究及中心控制单元的实现 [D]. 西安：西安电子科技大学，2002.
[17] 高 凯，张尔扬. 空时频互相关 MIMO 衰落信道仿真及其性能分析 [J]. 信号处理，2007 (6)：861 - 863.
[18] CHEN D，LIU M，LIU X. A New Algorithm of Deriving Linear Combination for Delayed m-Sequence [C] //Proceedings of 2012 IEEE 11th International Conference on Signal Processing (ICSP 2012). IEEE，2012：1756 - 1760.
[19] 刘 洋，宋汐瑾，肖钧仁. 基于 m 伪随机序列的脉冲响应分析 [J]. 工业控制计算机，2023，36 (1)：78 - 79.
[20] 孟庆萍，周新力，田 伟. 基于 FFT 和长时延自相关函数的频偏估计方法 [J]. 计算机工程与设计，2013，34 (3)：799 - 803.
[21] 董孝东. 基于 FFT 的突发通信载波大频偏估计算法 [J]. 现代电子技术，2013，36 (1)：51 - 53.