

基于信誉评估机制和区块链的移动网络联邦学习方案

杨明¹, 胡学先¹, 张启慧¹, 魏江宏¹, 刘文芬²

(1. 信息工程大学, 河南 郑州 450001;

2. 桂林电子科技大学, 广西 桂林 541004)

摘 要: 联邦学习是一种新兴的分布式机器学习技术, 通过将训练任务下放到用户端, 仅将训练得到的模型参数发送给服务端, 整个过程并不需要参与方直接共享数据, 从而很大程度上规避了隐私问题。然而, 这种学习模式中移动用户间没有预先建立信任关系, 用户之间进行合作训练时会存在安全隐患。针对上述问题, 提出一种基于信誉评估机制和区块链的移动网络联邦学习方案, 该方案允许服务端利用主观逻辑模型对参与训练的移动用户进行信誉评估, 并且基于区块链智能合约技术为其提供可信的信誉意见共享环境和动态访问策略接口。理论和实验分析结果表明, 此方案可以使服务端选择可靠的用户进行训练, 同时能够实现更公平和有效的信誉计算, 提高联邦学习的准确性。

关键词: 移动网络; 联邦学习; 区块链; 信誉管理

中图分类号: TP399

文献标识码: A

DOI: 10.11959/j.issn.2096-109x.2021083

Federated learning scheme for mobile network based on reputation evaluation mechanism and blockchain

YANG Ming¹, HU Xuexian¹, ZHANG Qihui¹, WEI Jianghong¹, LIU Wenfen²

1. Strategic Support Force Information Engineering University, Zhengzhou 450001, China

2. Guilin University of Electronic Technology, Guilin 541004, China

Abstract: Federated learning is a new distributed machine learning technology, where training tasks are deployed on user side and training model parameters are sent to the server side. In the whole process, participants do not need to share their own data directly, which greatly avoids privacy issues. However, the trust relationship between mobile users in the learning model has not been established in advance, there is hidden safety when users perform

收稿日期: 2021-01-19; 修回日期: 2021-03-30

通信作者: 杨明, imbtym@163.com

基金项目: 国家自然科学基金(62172433, 62172434, 61862011, 61872449); 广西密码学与信息安全重点实验室研究课题(GCIS201704)

Foundation Items: The National Natural Science Foundation of China (62172433, 62171434, 61862011, 61872449), Guangxi Key Laboratory of Cryptography and Information Security (GCIS201704)

论文引用格式: 杨明, 胡学先, 张启慧, 等. 基于信誉评估机制和区块链的移动网络联邦学习方案[J]. 网络与信息安全学报, 2021, 7(5): 99-112.

YANG M, HU X X, ZHANG Q H, et al. Federated learning scheme for mobile network based on reputation evaluation mechanism and blockchain[J]. Chinese Journal of Network and Information Security, 2021, 7(5): 99-112.

cooperative train with each other. In view of the above problems, a federated learning scheme for mobile network based on reputation evaluation mechanism and blockchain was proposed. The scheme allowed the server side to use subjective logic models to evaluate the reputation of participating mobile users and provided them with credible reputation opinions sharing environment and dynamic access strategy interface based on the technique of smart contract of blockchain. Theoretical and experimental analysis results show that the scheme can enable the server side to select reliable users for training. And it can achieve more fair and effective reputation calculations, which improves the accuracy of federated learning.

Keywords: mobile network, federated learning, blockchain, reputation management

1 引言

随着嵌入式系统和网络技术的加速发展,具有计算、感知和无线通信能力的传感器以及由其构成的移动网络已经逐步进入人们的生活^[1]。基于这些传感器收集的数据,通过在移动设备终端部署机器学习模型,可以极大地提高移动服务的质量,如疾病预测^[2]和自动驾驶路径规划^[3]等。然而,传统的端到端学习需要将训练数据上传到云服务器或者数据中心进行集中处理,这不仅会带来过高的通信和存储成本,而且会使移动用户面临隐私泄露的风险^[4]。因此,如何在保证用户隐私的前提下,充分发挥机器学习等人工智能方法的潜力是一项意义深远而又亟待解决的问题。

联邦学习^[5-7]作为一种新兴的分布式隐私保护机器学习训练模型得到越来越多的重视,其系统结构如图 1 所示。在每次迭代过程中,参数服务器将模型训练任务部署到终端设备,后者不需要上传原始数据,而是在本地根据自己的私有数据训练机器学习模型,然后由前者聚合更新来自不同设备的模型参数。参数服务器和终端设备不断重复上述过程,直到模型参数达到预定的精度^[8]。目前,联邦学习技术已经在一些移动网络中有所应用。谷歌^[9]将联邦学习技术应用到 Pixel 和安卓等智能手机中,在保护用户数据隐私的情况下提升自然语言处理模型的准确率。通过让车辆在本地训练预测模型,Uber 推出的应用 UberEats 采用联邦学习的方式利用实时交通信息估计送餐时间,以提高个性化服务的水平^[10]。为协作训练诊断模型以确定最佳治疗方法,多家医院可以通过医学 AI 应用框架 NVIDIA Clara 将联邦学习任务部署到各个医疗设备,而无须集中收集患者的敏感信息。

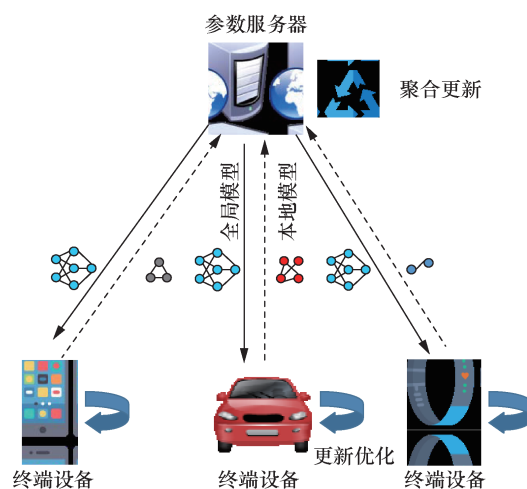


图 1 联邦学习系统结构
Figure 1 Architecture for a federated learning system

联邦学习技术虽然在移动网络中有广阔的应用前景,但由于其本身处在发展的初级阶段,仍然面临严峻的挑战。一方面是参与方的互信问题,即联邦学习中的参与用户来自不同的组织或个体,彼此之间缺少信任,如果没有公开公正的可信平台,参与用户不愿意参加模型训练^[11-12]。另一方面是参与方提供的参数缺乏验证,即一些参与用户本地收集的数据质量与其他参与方相比差距过大,训练的模型会直接影响整体模型的质量,此外,恶意的参与用户甚至还会提供虚假的参数破坏学习过程^[13],从而对其他参与方产生不利影响。因此,将联邦学习应用到移动网络的同时需要重点设计一种可靠的信誉评估管理机制,使移动用户之间既能互相信任对方,又能获得高质量的模型参数。

近年来,区块链技术以其独有的去中心化、不易篡改和可追溯等特性为解决上述问题提供了思路。一些研究人员开始将联邦学习和区块链技术相结合来实现移动网络中的数据共享。文献[14]

设计了基于改进的 DPoS 共识的区块链车联网数据共享模型, 引入主观逻辑模型以实现安全高效的信誉管理。Rehman 等^[15]提出了基于区块链的细粒度信誉感知的概念, 确保移动边缘计算的参与方能够进行可信的联合训练。Fedcoin^[16]从博弈论的角度出发, 由共识网络的矿工节点通过采用沙普利法精确计算各参与方所做的贡献, 使各参与方能够公平分配联邦学习获得的利润。

现有的移动网络联邦学习研究中缺乏对参与各方信誉的评估和管理, 无法为用户提供互信的协作训练平台。本文以此为出发点, 利用主观逻辑模型计算参与方的信誉值, 然后将每次训练后各个参与方的信誉值存储到不可更改的区块中, 以供其他用户使用。同时, 为了对用户上传的信誉意见进行评价和管理, 本文采用信誉评估机制和区块链技术相结合的模式, 将模糊层次分析 (FAHP, fuzzy analytic hierarchy process) 法集成到智能合约中, 为用户提供可调节的信誉意见访问控制策略。只有信誉值超过一定阈值的用户才可以访问链上资源, 从而有效降低了用户的恶意行为, 激励更多用户共享高质量的信誉意见。实验表明, 本文的方案可以显著降低恶意数据拥有方参与联邦学习的可能性, 提高模型的准确率。

2 预备知识

2.1 区块链的基本概念

区块链是由区块按时间顺序串联起来的链式结构, 每个区块包含区块头和区块体两部分^[17-18], 其存储结构如图2所示。以比特币为例^[19], 区块头存储了版本号、前一个区块的哈希值 (父哈希)、时间戳、Merkle 根、难度值和一个随机数, 区块体由交易信息构成, 所有的交易以 Merkle 树的结构存储。其中, 哈希指针能唯一标识区块并将各个区块相连接, 使得区块中的每条数据可以追溯

到源头, 时间戳则保证了区块的有序性。同时利用 Merkle 树, 可以单独下载一个分支对部分数据校验, 实现高效的交易验证。

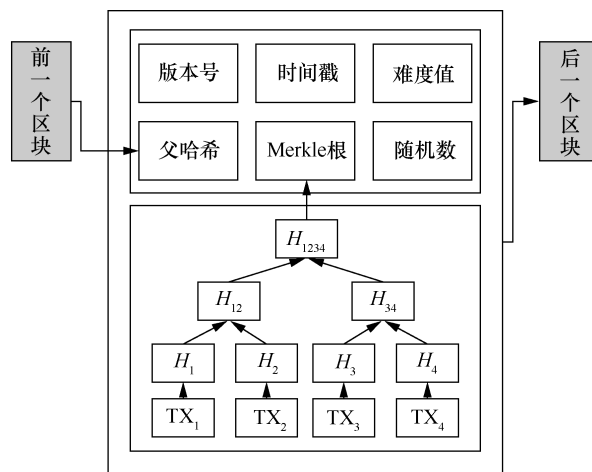


图2 区块结构

Figure 2 The structure of blocks

依据账本权限准入机制的不同, 区块链可以划分为公有链、私有链和联盟链^[20], 如表1所示。公有链没有权限设定, 任何人都可以随时加入网络, 链上数据对全网公开, 由全体网络节点共同维护, 被认为是完全去中心化的分布式账本, 如比特币、以太坊等。私有链建立在一套身份认证与权限设置的机制上, 对参与节点的状态有更多的控制权, 账本记录不对外开放, 仅在组织内部使用, 如企业的财务审计、供应链管理等。介于前两者之间, 联盟链采用混合的组网机制, 网络中的节点只有部分控制权, 信息对多个组织构成的联盟成员开放, 通常应用于企业合作, 如银行间的结算、企业间物流管理等。

本文面向移动网络提出的联邦学习方案, 具有以下3个特点: 一是参与方的种类确定, 由拥有各种终端设备的移动用户组成; 二是训练得到的模型参数涉及用户的隐私, 不会随便对外公开; 三是需要较高的交易速度, 要求节点之间能够较

表1 区块链分类
Table 1 Classification of blockchain

区块链分类	参与者	记账人	组织程度	激励机制	承载能力	典型场景
公有链	任何人自由进出	所有参与者	去中心化	需要	3~20 笔/秒	金融、存证
私有链	个体或者公司内部	自定义	多中心化	可选	1 000~20 万笔/秒	审计、发行
联盟链	联盟成员	联盟成员协商决定	多中心化	可选	1 000~1 万笔/秒	支付、公益

快达成共识,对参与方的信誉实现高效管理。基于上述特点,本文采用联盟链作为底层区块链。

2.2 智能合约

智能合约是一套以数字形式定义的承诺,该承诺控制着数字资产流转,并包含了合约参与者约定的权利和义务,合约是由计算机系统自动执行^[21]。智能合约中的内容以数据化的形式写入区块链中,由区块链技术的特性保障存储、读取、执行^[22]。智能合约的自动化和可编程特性使封装分布式区块链系统中各节点的复杂行为得以实现,这促进了区块链技术在各类分布式系统中的应用。

智能合约中的数据主要分为 storage 和 memory 两种类型。前者也可称为合约的状态变量,会永久存储在区块链中,后者则是临时变量,交易处理完成后会被清空。因此,在编写合约时要为永久存储的数据定义 storage 类型变量,而不仅仅是处理交易逻辑。

3 方案设计

本文提出一种基于信誉评估机制和区块链的移动网络联邦学习方案。首先,介绍系统的架构和 workflows;然后,分别为任务发布方和数据拥有方设计了具体的信誉意见共享激励机制和信誉评估机制。

3.1 系统架构

本节介绍的系统架构主要包括系统模型和敌手模型两个部分。

3.1.1 系统模型

基于联盟链的移动网络联邦学习系统主要由移动设备、数据拥有方、任务发布方和区块链服务平台 4 个部分组成,如图 3 所示。

1) 移动设备主要由各种移动网络中的物联网设备组成,包括智能手机、可穿戴设备、车辆传感器和家用电器等。移动设备是执行联邦学习任务的基础设施,不仅可以从应用程序生成各种用户数据,而且可以收集大量传感数据。

2) 数据拥有方是收集、存储和处理数据的实体。数据拥有方负责收集来自移动设备的数据,并存储在本地的数据库中。在模型训练期间,首先,每个数据拥有方根据任务发布方的全局模型

参数和训练数据本地生成局部模型参数。然后,所有数据拥有方将各自的局部模型参数发送给任务发布方,以便更新下一轮的全局模型。接着,数据拥有方重复训练过程,直到全局模型的精度达到预定的期望值。

3) 任务发布方主要由各种需要模型的物联网设备和机构组成,如无人驾驶汽车、家政服务机器人、医疗机构和安监部门等。任务发布方负责公开联邦学习任务的规范,如应用程序类型、设备类型、训练数据的类型与格式、学习模型的类型和计算要求等,并根据实际情况选择合适的数据拥有方。同时,任务发布方需要评估数据拥有方的局部模型质量,根据他们的评估结果生成信誉意见索引,然后制定相关的合约策略,并将信誉意见索引和合约策略一起上传到区块链服务平台,以供其他任务发布方在联邦学习中选择信誉较好的数据拥有方。

4) 区块链服务平台是存储信誉意见索引和合约策略的第三方平台,由一组具有足够计算和存储资源的矿工维护。矿工通过共识算法进行验证后,将接收到的信誉意见索引存储到数据块中。由于区块链可追溯和防篡改的性质,当数据拥有方发送低质量的局部模型时,数据块中相关信息可以作为持久且透明的证据。任务发布方将直接信誉意见与其他任务发布方的最新信誉意见进行集成,生成数据拥有方的综合信誉值,将其作为在联邦学习过程中选择可靠数据拥有方的重要指标。此外,任务发布方通过区块链中预先定义的访问控制策略,确保信誉意见的安全共享,其他任务发布方对信誉意见的访问都将保存在区块链中。

3.1.2 敌手模型

由于移动网络体系结构的开放性和复杂性,参与用户在合作训练时存在着巨大的安全隐患。例如,数据拥有方通过不可靠的无线通信信道传输数据,导致遭受恶意攻击,从而影响数据的可用性。针对面向移动网络的联邦学习可能产生的安全问题,本文着重考虑投毒攻击和合谋攻击。投毒攻击是指在本地训练过程中,恶意的数据提供方通过攻击训练数据集来操纵模型预测的结果。投毒攻击主要有两种方式:数据投毒(对训

练集中的样本进行污染,如添加错误的标签或有偏差的数据,降低数据的质量)和模型投毒(改变模型参数的变化方向,如发送错误的参数,减慢模型的收敛速度)。合谋攻击是指任务发布方和某个数据拥有方进行主动合作,在对数据拥有方的模型质量进行评估时,生成不符合实际的信誉意见(如对低质量的模型按高质量的模型处理),故意误导其他任务发布方选择特定的数据拥有方。这两种攻击都会对全局模型的准确性产生负

面影响,降低诚实参与方的积极性。

3.2 系统工作流程

基于联盟链的移动网络联邦学习系统如图3所示。系统可以借助区块链服务平台为任务发布方选择信誉较高的数据拥有方进行模型训练,具体描述如下。

步骤1 任务发布阶段。任务发布方将联邦学习任务的规范广播到全网,满足要求的数据拥有方将数据集信息的摘要发送给任务发布方,该

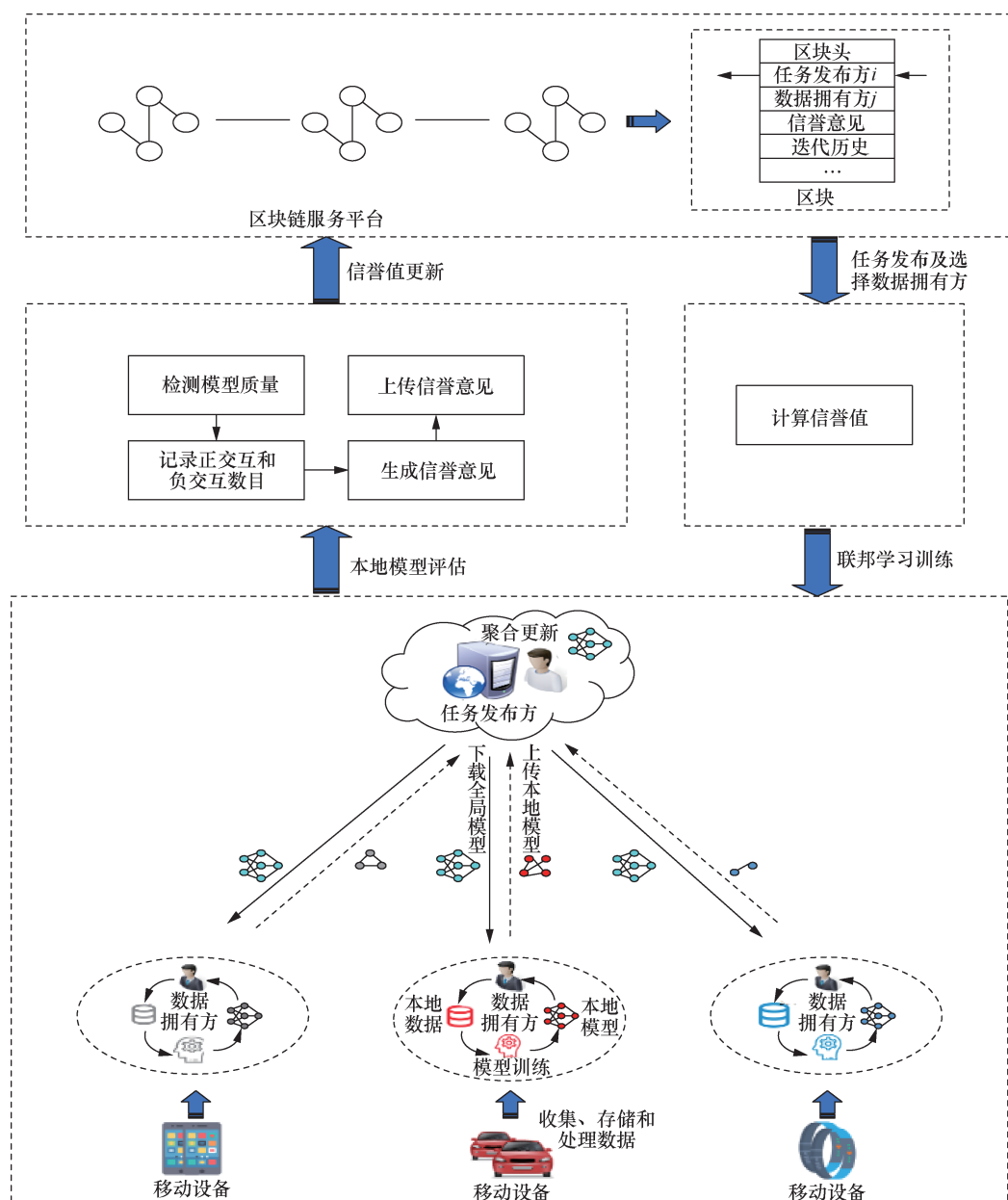


图3 基于联盟链的移动网络联邦学习系统

Figure 3 The system of federated learning for mobile network based on a consortium blockchain

数据拥有方成为模型训练的候选人。

步骤 2 数据拥有方选择阶段。为了获得高质量的全局模型，在训练模型前，任务发布方需要预先从区块链服务平台下载候选数据拥有方最近一段时间的信誉意见。基于区块链和联邦学习的移动网络中含有两种类型的信誉意见：直接信誉意见和间接信誉意见。任务发布方通过融合这两种意见对每个数据拥有方做出综合评价，选择信誉值较高的数据拥有方参与联邦学习的任务。

步骤 3 模型训练评估阶段。任务发布方向参与训练的数据拥有方发送初始化后的全局模型参数。数据拥有方收到参数后，在本地依据所持有的数据，通过随机梯度下降算法，寻找局部模型参数，使损失函数最小化，并将更新的模型参数上传到任务发布方。为了识别进行投毒攻击的数据拥有方，任务发布方需要执行一些投毒攻击检测方案。RONI (reject on negative influence) 和 FoolsGold 分别是针对数据独立同分布 (IID) 和非 IID 场景下的攻击检测方案。通过这两种方案，任务发布方可以拒绝接受恶意数据拥有方的局部模型参数，并按照文献[23]的方法计算其他局部模型参数的平均值。在每次迭代过程中，进行投毒攻击的数据拥有方将会被记录下来，任务发布方依此为其生成本地信誉意见。

步骤 4 信誉值更新阶段。首先依据历史记录对数据拥有方生成直接信誉意见后，这些意见被当作交易由任务发布方签名后上传到区块链服务平台。然后，矿工验证信誉意见的有效性，并执行实用拜占庭容错 (PBFT, practical Byzantine fault tolerance) 共识算法将其上链。至此，信誉值的更新工作完成，所有的任务发布方都可以通过查询区块链上的信誉意见选择表现良好的数据

拥有方以完成联邦学习任务。

3.3 信誉意见共享激励机制

为了对任务发布方上传信誉意见的行为进行监督，激励更多任务发布方提供高质量的信誉意见，本文设计了一种信誉意见共享激励机制。该激励机制主要分为两部分：基于智能合约的信誉意见管理和任务发布方信誉的评价。前者将信誉评估机制集成到智能合约中，为任务发布方提供可调节的共享策略；后者提出了计算信誉值的具体方法，为任务发布方调节共享策略提供依据。本节首先介绍基于智能合约的信誉意见管理，对任务发布方信誉的评价将在下一节进行介绍。

在本文的方案中，智能合约负责所有的交易逻辑处理，包括用户节点注册、信誉意见共享、信誉意见访问和信誉意见更新 4 种交易。其中，节点注册交易负责登记用户身份，只有在区块链中注册的任务发布方才能进行信誉意见的共享、访问和更新。智能合约状态变量保留了永久性存储在区块链中的数据，为任务发布方的身份验证、信誉意见的共享及任务发布方信誉值计算提供数据支撑。智能合约函数用于处理合约的内部逻辑，实现请求和更新等功能。智能合约状态变量说明和智能合约函数说明分别如表 2 和表 3 所示。

(1) 用户身份注册

任务发布方将真实身份 ID、身份证明 V_{id} 、注册地址 address 和公钥 pk 等信息发送给区块链服务平台上的审计节点，申请将信息登记到区块链中。在该过程中，审计节点验证任务发布方的身份信息，身份验证成功后调用合约接口 `node_register()` 将任务发布方的信息写入区块链，同时将信息更新到审计节点变量 `audit_node`。任务发布方注册成功后就能够上传和下载有关数据

表 2 智能合约状态变量说明
Table 2 Description of smart contract variables

名称	说明
address_pk	任务发布方公钥 pk 与地址的对应关系
audit_node	审计节点结构，记录审计节点个数等内容
reos_share	由信誉意见的索引 url 的 hash 值映射到结构体 reos_sharing，记录了任务发布方共享的信誉意见的具体信息
url_pk	由信誉意见的索引 url 的 hash 值映射到 pk，记录了 url 与任务发布方 pk_p 的对应关系
url_whitelist	由信誉意见的索引 url 的 hash 值映射到白名单结构体 pk_whitelist，记录任务发布方为共享的 url 设置的白名单成员的相关信息

表3 智能合约函数说明
Table 3 Description of smart contract functions

名称	说明
node_register()	用于登记通过身份验证的任务发布方，仅审计节点可以调用
contribute_reo()	用于任务发布方共享信誉意见，该函数将信誉意见的 url、hash 值等重要信息记录到变量 url_share 中
set_url_pk()	将信誉意见的 url 与任务发布者的公钥 pk_p 的关系记录到 url_pk 中
verify_pk()	变量 address_pk 验证用户是否通过审计节点的验证
request_reo()	请求方访问信誉意见的接口
remove_whitelist()	任务发布方设置白名单的接口，将指定的用户从白名单中删除

拥有方的信誉意见。注册过程如算法1所示。

算法1 节点注册算法

输入 ID, V_{ID} , address, pk

1) 任务发布方发送 ID、 V_{ID} 、address 和 pk 给

审计节点

2) 审计节点验证任务发布方身份信息

3) 调用合约函数 node_register(pk,address,role)

4) 更新 address_pk[address]

5) 将任务发布方信息加入变量 audit_node 中

(2) 信誉意见共享

联邦学习任务结束后，任务发布方生成本地信誉意见 reo，并且用随机产生的对称密钥 smk 加密 $[reo]_{smk}$ 。任务发布方将 $[reo]_{smk}$ 上传到云端，云端返回信誉意见的存储索引 url。任务发布方使用公钥 pk_p 加密 smk 获得 $[smk]_{pk_p}$ ，然后调用接口函数 contribute_reo() 创建共享交易 REO_TXID。合约内部执行函数 verify_pk()，检测任务发布方的身份注册信息，验证通过后将信誉意见相关信息存入变量 reo_share[url_hash] 中，该变量指向 reo_sharing 结构体。同时合约调用内部函数 set_url_pk() 将 url 与任务发布方公钥 pk_p 的对应关系记录到变量 url_pk[url_hash] 中。之后合约为该信誉意见初始化白名单 url_whitelist[url_hash]，将任务发布方的信息及解密 $[smk]_{pk_p}$ 的私钥存入白名单所指向的 pk_whitelist 中。随后，任务发布方调用合约给白名单添加成员，允许其他信誉较高的任务发布方访问信誉意见。本文方案基于移动网络中只有少数任务发布方是恶意的这个假设，在共享过程中，单个任务发布方生成本地意见后进行修改对数据拥有方的信誉值几乎没有影响，因为所提方案会根据数据拥有方的历史交互

记录和其他多个任务发布方的间接信誉意见，结合熵的理论定义自适应权重，对数据拥有方进行综合的信誉评估，从而使信誉评估客观准确。信誉意见共享如算法2所示。

算法2 信誉意见共享算法

输入 url, url_hash, address, $[smk]_{pk_p}$, pk_p

1) 任务发布方调用合约函数 contribute_reo(url, url_hash, address, $[smk]_{pk_p}$, pk_p)

2) if verify_pk(address, pk_p) = true

3) 合约将信誉意见信息存入 reo_share[url_hash] 变量中

4) 合约调用内部函数 set_url_pk(url_hash, pk_p) 将信誉意见与任务发布方的关系记录到变量 url_pk[url_hash] 中

5) 合约初始化信誉意见的白名单，将任务发布方的信息加入白名单 url_whitelist[url_hash] 中

6) 合约查询已经注册的其他任务发布方，分别将它们加入白名单中

7) return REO_TXID

8) else

9) return default

10) end

(2) 信誉意见访问

任务发布方在每次进行联邦学习前，执行信誉意见访问算法请求得到其他任务发布方的信息意见，以选择可靠的数据拥有方。请求方输入被访问任务发布方的公钥 pk_p 及信誉意见索引路径哈希 url_hash、自己的公钥 pk_p ，调用函数 request_smk() 后，合约验证请求方的身份，如果验证成功，合约会判断请求方是否在被访问任务发布方的白名单中，如果存在就会更新请求方的

访问时间,并返回加密密钥 $[smk]_{pk_r}$,请求方用私钥就可以解密得到对称密钥;否则视为请求方在被访问任务发布方的本地信誉较低,任务发布方拒绝访问,访问失败。此外,在访问链上相应资源时,还需要由区块链服务平台上的审计节点进行身份认证。如果非白名单中的任务发布方通过与白名单中的任务方合谋得到对称密钥,不在白名单的任务发布方在认证时不会被通过,从而无法获取信誉意见 reo 。信誉意见的访问如算法 3 所示。

算法 3 信誉意见访问算法

输入 $pk_p, url_hash, pk_r, address$

- 1) 请求方调用合约函数 $request_smk(pk_p, url_hash, pk_r)$
- 2) if $verify_pk(address, pk_r) = fakery$
- 3) return $fakery$
- 4) if $url_whitelist[url_hash][is_white]$
[pk_r]= true
- 5) pk_r 的访问时间戳 $timestamp$ 更新
- 6) return $Request_TXID, [smk]_{pk_r}$
- 7) else
- 8) return $default$
- 9) end if
- 10) end if
- (3) 信誉意见更新

请求方会在本地对其他任务发布方的信誉意见进行评估,若某一任务发布方信誉较低的次数超过设定的阈值,请求方就会调用函数 $update_smk_remove()$,将该任务发布方从自己的白名单中移除。信誉意见的更新如算法 4 所示。

算法 4 信誉意见的更新

输入 $pk_p, url_hash, pk_r, address$

- 1) 请求方调用合约函数 $update_smk_remove(pk_p, url_hash, pk_r)$
- 2) if $verify_pk(address, pk_r) = fakery$
- 3) return $fakery$
- 4) 记录 pk_r 的更新时间戳
- 5) 调用合约函数 $remove_whitelist(url_hash, pk_p)$ 将任务发布方从白名单中移除
- 6) return $Remove_TXID$

7) end if

3.4 信誉评估机制

本节给出计算任务发布方和数据拥有方信誉值的具体方法。

3.4.1 对任务发布方的信誉评估

任务发布方会根据其他任务发布方的信誉意见在本地对其进行信誉评估,从而调用信誉意见共享算法调整信誉意见共享策略。被评价任务发布方提供的信誉意见越可靠,信誉值就越高,可访问的信誉意见资源就越多。任务发布方的信誉并不能从单一特性进行评估,本文采用模糊层次分析法^[24-25]对任务发布方的信誉进行评估。先将任务发布方的信誉分为 n 个特性,再把每个特性分为若干个特征类型,将任务发布方行为信誉评估问题转化为简单明确的信誉特征加权求和问题。FAHP 计算任务发布方信誉值的过程分为以下 4 个步骤。

步骤 1 将信誉分为 3 层,如图 4 所示。为了不给区块链造成负担,任务发布方会在本地分析其他任务发布方的信誉意见并依据区块链网络中交易情况,从而确定被评价任务发布方的行为特征。

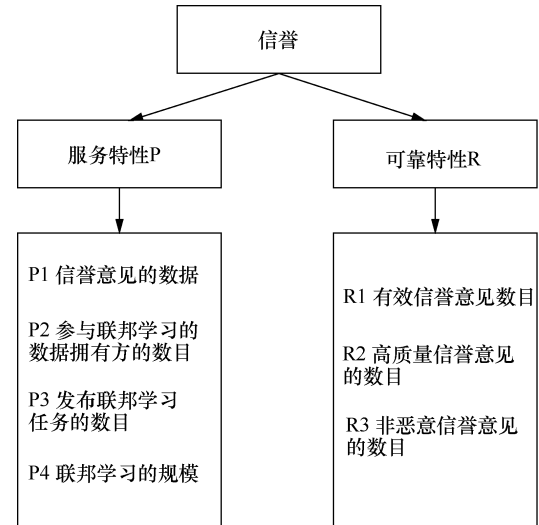


图 4 任务发布方行为特征分类

Figure 4 Classification of task publisher behavior characteristics

步骤 2 建立行为特征矩阵 $C = [c_{ij}]_{n \times m}$, n 为特性个数, m 为特性中行为特征个数的最大值,不够的项用零补充。为了便于计算和评估任务发布方行为,需要对矩阵 C 进行归一化处理,将其规范为 $[0,1]$ 的特征矩阵 $E = [e_{ij}]_{n \times m}$, 将同一特性

下的特征按重要性做二元对比, 获得初始判断矩阵 $\mathbf{EQ} = [eq_{ij}]_{m \times m}$ 。以服务特性为例, 特征个数为4, 特征矩阵 $\mathbf{E}_p = [e_1, e_2, e_3, e_4]$, 利用式(1)获得初始判断矩阵 $\mathbf{EQ}_p$ 。

$$eq_{ij} = \begin{cases} 0, & e_i < e_j \\ 0.5, & e_i = e_j \\ 1, & e_i > e_j \end{cases} \quad (1)$$

然后, 通过式(2)将初始判断矩阵转化为模糊判断一致矩阵 $\mathbf{Q}_p = [q_{ij}]_{m \times m}$ 。

$$\begin{cases} q_{ij} = \frac{q_i - q_j}{2m} + 0.5 \\ q_i = \sum_{k=1}^m eq_{ik} \end{cases} \quad (2)$$

步骤3 使用式(3)计算服务特性下个特征的特征权重向量, 从而得到 $\mathbf{w}_p = [w_{p1}, w_{p2}, w_{p3}, w_{p4}]$, 对于可靠特性, 同样利用式(1)~式(3)得到可靠特性 R 的特征权重向量 $\mathbf{w}_R = [w_{R1}, w_{R2}, w_{R3}]$ 和特性权重向量 $\mathbf{W}_f = [w_p, w_R]$ 。

$$w_{pi} = \frac{\sum_{k=1}^m q_{ik} - 0.5}{m(m-1)/2} \quad (3)$$

步骤4 由特征矩阵 $\mathbf{E} = [e_{ij}]_{n \times m}$, 权重矩阵 $\mathbf{W} = (w_{ij})_{n \times m}$, 根据 $\mathbf{E} \times \mathbf{W}^T$ 得到的矩阵对角线上的值就是任务发布方的特性评估值矩阵 $\mathbf{F} = (f_1, f_2, \dots, f_n)$, 最后, 任务发布方的信誉值表示为

$$T = 1 - \mathbf{F} \times \mathbf{W}_f^T = 1 - \sum_{i=1}^n f_i w_i \quad (4)$$

3.4.2 对数据拥有方的信誉评估

在移动网络中, 有效和准确的信誉计算方法会激励更多数据拥有方提供高质量的模型参数。本文在主观逻辑的基础上, 采用贝叶斯理论消除训练过程中的不确定交互, 根据数据拥有方的历史交互记录和其他多个任务发布方的间接信誉意见, 结合熵的理论定义自适应权重, 制定了一个综合的信誉评估方案。下面从信誉计算涉及的相关定义和评估方法进行详细阐述。

定义1 (交互) 数据拥有方从任务发布方下

载全局模型参数, 并根据本地数据迭代训练上传一次参数的过程被称为一次交互。其中, 通过任务方投毒攻击检测方案的为正交互, 否则为负交互。当数据拥有方未上传任何参数时, 即代表出现了不确定交互。

定义2 (历史交互) 历史交互是在 Δt 时间内任务发布方对数据拥有方交互记录的集合 $t = \{s, f\}$, 其中, s 和 f 分别为正交互的数目和负交互的数目。

本文在计算数据拥有方信誉值时采用了3种信誉评估的方法, 分别为直接信誉评估、间接信誉评估和综合信誉评估。

(1) 直接信誉评估

根据主观逻辑的概念, 将任务发布方 i 在 Δt 时间内对数据拥有方 j 的信誉评价表示为一个三元组的形式 $\Upsilon_{i \rightarrow j} = \{b_{i \rightarrow j}, d_{i \rightarrow j}, u_{i \rightarrow j}\}$ 。 $b_{i \rightarrow j}$ 是相信数据拥有方 j 服务质量的真实概率, $d_{i \rightarrow j}$ 是认为数据拥有方服务是低质的概率, $u_{i \rightarrow j}$ 表示对数据拥有方 j 服务质量的不确定性。其中 $b_{i \rightarrow j}$, $d_{i \rightarrow j}$, $u_{i \rightarrow j} \in (0, 1)$, 并满足以下要求

$$b_{i \rightarrow j} + d_{i \rightarrow j} + u_{i \rightarrow j} = 1 \quad (5)$$

进一步, 基于主观逻辑的本地模型^[14,26]和定义2, 可以得到:

$$\begin{cases} b_{i \rightarrow j} = (1 - u_{i \rightarrow j}) \frac{s_{i \rightarrow j}}{s_{i \rightarrow j} + f_{i \rightarrow j}} \\ d_{i \rightarrow j} = (1 - u_{i \rightarrow j}) \frac{f_{i \rightarrow j}}{s_{i \rightarrow j} + f_{i \rightarrow j}} \\ u_{i \rightarrow j} = 1 - q_{i \rightarrow j} \end{cases} \quad (6)$$

其中, $q_{i \rightarrow j}$ 是参数传输成功的概率, 代表着通信质量。为了使信誉评价更精确, 当数据拥有方 j 出现不确定交互时, 本文使用贝叶斯公式预测数据拥有方出现正交互的概率, 即

$$P(H|E) = \frac{P(H)P(E|H)}{P(E)} \quad (7)$$

其中, 将数据拥有方 j 的历史交互 $t_{i \rightarrow j}$ 作为前置条件 E , 出现正交互的行为作为事件 H 。假设事件 E 发生的条件下事件 H 发生的概率服从 Beta 分布, 则数据拥有方 j 的不确定交互行为对信誉

影响的相关系数 $a_{i \rightarrow j}$ 可以用 Beta 分布^[27]的数学期望表示为

$$a_{i \rightarrow j} = \frac{s_{i \rightarrow j} + 1}{s_{i \rightarrow j} + f_{i \rightarrow j} + 2} \quad (8)$$

相关系数 $a_{i \rightarrow j}$ 表示数据拥有方 j 不确定交互时表现为正交互的概率。结合式(6)、式(8)，在一次联邦学习任务中，任务发布方 i 对数据拥有方 j 直接信誉值 $T_{i \rightarrow j}$ 的计算公式为

$$T_{i \rightarrow j} = (1 - u_{i \rightarrow j}) \frac{s_{i \rightarrow j}}{s_{i \rightarrow j} + f_{i \rightarrow j}} + \frac{s_{i \rightarrow j} + 1}{s_{i \rightarrow j} + f_{i \rightarrow j} + 2} u_{i \rightarrow j} \quad (9)$$

为了使评估具有更高的可靠性和可信度，本文考虑了活跃度和实效性两个因素。

① 活跃度。模型的训练过程需要考虑数据拥有方的计算成本和通信成本，其交互数目越多，付出的成本就越高。数据拥有方 j 的活跃度是任务发布方 i 在一定时间窗口与其交互的数目与其他数据拥有方平均交互数目的比率，即

$$I_{i \rightarrow j} = \frac{r_{i \rightarrow j}}{\frac{1}{|S|} \sum_{s \in S} r_{s \rightarrow j}} \quad (10)$$

其中， $r_{i \rightarrow j} = s_{i \rightarrow j} + f_{i \rightarrow j}$ ，表示任务发布方 i 与数据拥有方 j 在一定时间窗口内交互的总数目。本文假设在这个时间窗口与任务发布方交互的数据拥有方的集合为 S 。结合式(6)、式(9)和式(10)，信誉值 $T_{i \rightarrow j}$ 的计算公式可以进一步调整为

$$T_{i \rightarrow j} = \left(q_{i \rightarrow j} \frac{s_{i \rightarrow j}}{s_{i \rightarrow j} + f_{i \rightarrow j}} + u_{i \rightarrow j} \frac{s_{i \rightarrow j} + 1}{s_{i \rightarrow j} + f_{i \rightarrow j} + 2} \right) I_{i \rightarrow j} \quad (11)$$

调整后的信誉值与活跃度相关，这不仅能反映当前数据拥有方自身的交互情况，也能反映它在所有交互情况下所占的比例。

② 时效性。历史交互是任务发布方和数据拥有方在 Δt 时间内交互记录的集合，因此对数据拥有方的信誉评价随时间动态变化。一般来说，最新的历史交互要比过去的历史交互影响大，对信誉值计算有更多的参考价值。为了准确及时反映信誉评价的时效性，本文用 ε 表示最新历史交互的权重， σ 表示过去历史交互的权重， $\varepsilon + \sigma = 1$ ，

$\varepsilon > \sigma$ 且 $\varepsilon, \sigma \in (0, 1)$ 。具体 ε 的大小可以根据交互情况和历史经验获得。据此，信誉值的更新公式表示为

$$T_{i \rightarrow j}^{\text{new}} = \varepsilon T_{i \rightarrow j}^{\text{near}} + \sigma T_{i \rightarrow j}^{\text{old}} \quad (12)$$

其中， $T_{i \rightarrow j}^{\text{old}}$ 是旧的信誉值， $T_{i \rightarrow j}^{\text{near}}$ 是最近一次的信誉值， $T_{i \rightarrow j}^{\text{new}}$ 是更新后的信誉值。

(2) 间接信誉评估

与社交网络相似，移动网络中的每个任务发布方在评估数据拥有方的信誉值时，会间接参考其他任务发布方对当前数据拥有方的信誉评估。间接信誉值 $T_{k \rightarrow j}^{\text{rec}}$ 是其他任务发布方 k 对数据拥有方 j 评估的直接信誉值，是任务发布方 i 通过查询区块链得到的。

考虑到其他任务发布方可能与一些数据拥有方串谋欺骗，因此间接信誉值并不都是可信的。本文引入信息熵的概念给不同的间接信誉值分配权重，可有效改善主观分配权重带来的问题，增强模型适应性。根据式(13)，计算信誉值 $T_{k \rightarrow j}^{\text{rec}}$ 的熵。

$$H(T_{k \rightarrow j}^{\text{rec}}) = -T_{k \rightarrow j}^{\text{rec}} \text{lb} T_{k \rightarrow j}^{\text{rec}} - (1 - T_{k \rightarrow j}^{\text{rec}}) \text{lb}(1 - T_{k \rightarrow j}^{\text{rec}}) \quad (13)$$

信息熵能够反映间接信誉值之间的差异程度，即各间接信誉值偏离整体间接信誉值集合的程度。一些任务发布方可能为了利益对数据拥有方做出不切实际的信誉评价，造成信誉值的计算过高或者过低，信息熵将这种行为识别出来，使其信誉值在整体间接信誉评价中占有很小的比例，从而使间接评估客观准确。通常，间接信誉值之间的差异化程度越小，对数据拥有方的间接评估就越客观，因此，可以利用式(14)计算各间接信誉值 $T_{k \rightarrow j}^{\text{rec}}$ 的权重。

$$\omega_k = \frac{1 - \frac{H(T_{k \rightarrow j}^{\text{rec}})}{\text{lb} T_{k \rightarrow j}^{\text{rec}}}}{\sum_{k=1}^n \left[1 - \frac{H(T_{k \rightarrow j}^{\text{rec}})}{\text{lb} T_{k \rightarrow j}^{\text{rec}}} \right]} \quad (14)$$

其中， n 表示间接信誉值的个数。最后，全局的间接信誉评估值 $T_{i \rightarrow j}^{\text{rec}}$ 为

$$T_{i \rightarrow j}^{\text{rec}} = \sum_{k=1}^n \omega_k T_{k \rightarrow j}^{\text{rec}} \quad (15)$$

(3) 综合信誉评估

任务发布方 i 的综合信誉评估方法是将直接信誉值 $T_{i \rightarrow j}$ 和全局间接信誉值 $T_{i \rightarrow j}^{\text{rec}}$ 进行合成，从而得到数据拥有方 j 的综合信誉值，使评估过程全面准确。合成的方法是利用两者所提供信息的效用值，即根据两种评估方法之间的差异程度对信誉值的权重进行修正，因此，综合信誉值 $T_{i \rightarrow j}^{\text{final}}$ 由式(16)计算。

$$T_{i \rightarrow j}^{\text{final}} = \theta_d T_{i \rightarrow j} + \theta_r T_{i \rightarrow j}^{\text{rec}} \quad (16)$$

其中， θ_d 和 θ_r 分别是直接信誉值 $T_{i \rightarrow j}$ 和间接信誉值 $T_{i \rightarrow j}^{\text{rec}}$ 的自适应权重， $H(T_{i \rightarrow j})$ 和 $H(T_{i \rightarrow j}^{\text{rec}})$ 分别是 $T_{i \rightarrow j}$ 和 $T_{i \rightarrow j}^{\text{rec}}$ 的信息熵。

$$H(T_{i \rightarrow j}) = -T_{i \rightarrow j} \text{lb} T_{i \rightarrow j} - (1 - T_{i \rightarrow j}) \text{lb}(1 - T_{i \rightarrow j}) \quad (17)$$

$$H(T_{i \rightarrow j}^{\text{rec}}) = -T_{i \rightarrow j}^{\text{rec}} \text{lb} T_{i \rightarrow j}^{\text{rec}} - (1 - T_{i \rightarrow j}^{\text{rec}}) \text{lb}(1 - T_{i \rightarrow j}^{\text{rec}}) \quad (18)$$

$$\theta_d = \frac{1 - \frac{H(T_{i \rightarrow j})}{\text{lb} T_{i \rightarrow j}}}{\left[1 - \frac{H(T_{i \rightarrow j})}{\text{lb} T_{i \rightarrow j}} \right] + \left[1 - \frac{H(T_{i \rightarrow j}^{\text{rec}})}{\text{lb} T_{i \rightarrow j}^{\text{rec}}} \right]} \quad (19)$$

$$\theta_r = \frac{1 - \frac{H(T_{i \rightarrow j}^{\text{rec}})}{\text{lb} T_{i \rightarrow j}^{\text{rec}}}}{\left[1 - \frac{H(T_{i \rightarrow j})}{\text{lb} T_{i \rightarrow j}} \right] + \left[1 - \frac{H(T_{i \rightarrow j}^{\text{rec}})}{\text{lb} T_{i \rightarrow j}^{\text{rec}}} \right]} \quad (20)$$

4 系统评估与分析

4.1 安全性分析

本节证明所提出的方案可以有效防止投毒攻击和合谋攻击。

(1) 防止投毒攻击

本文通过检测模型参数和信誉评估两种方法可有效防止投毒攻击。一方面，在模型训练阶段，恶意数据拥有方上传的模型参数由本次的任务发布方进行检测。只有检测成功的模型参数才会用于模型的聚合，从而去除了可以对模型产生负面影响的参数。另一方面，在模型评估阶段，未通过检测的数据拥有方会被记录下来，任务发布方根据记录生成信誉意见并上传到区块链服务平

台。恶意数据拥有方投毒的次数越多，其信誉值越低。任务发布方能够通过查看区块链上的信誉记录选择信誉值较高的数据拥有方参与模型训练，从而降低了恶意数据拥有方投毒的可能。

(2) 防止合谋攻击

为了防止一些任务发布方与数据拥有方进行合谋攻击，必须确保在计算间接信誉评估值时，这些任务发布方的信誉评估占有很小的权重。信息熵可以反映数据拥有方信誉值的无序化程度，也就是各个信誉值偏离整个推荐信誉集合的程度。任务发布方做出的不切实际的信誉评估会被信息熵识别出来，从而保证数据拥有方能够获得客观准确的评价。同时，与任务发布方合谋的数据拥有方作恶一次后，其信誉值会显著下降。只有通过更多的正交互才能提高信誉值。作恶时间段越短，信誉值下降越快，被选中参与联邦学习的可能性就越小。此外，任务发布方之间通过其行为特征互相评价，信誉较低的任务发布方将被大多数用户从白名单中移除，从而无法访问信誉意见资源。

4.2 性能分析

4.2.1 实验设置

为了评估所提出方案的性能，本文基于经典的 Car Evaluation 分类数据集进行了仿真实验。该数据集包括 1 728 个测试实例，6 个测试属性和 4 类标签。本文将数据集随机分配给 10 个数据拥有方，其中包括 3 个恶意数据拥有方，它们会有意修改实例的标签（修改后训练实例数量占本地数据实例数量的百分比表示攻击强度），操纵联邦学习的结果。本文在 Hyperledger Fabric v1.4.0 上建立了信誉区块链系统，共识算法采用实用高效的 PBFT 算法^[14]。

3.4.2 节介绍了任务发布方信誉值的计算方法，使用 FAHP 对任务发布方的行为特征进行划分，其中，服务特性 P 的重要性划分为 $P1 > P2 > P3 = P4$ ，可靠特性 R 的重要性划分为 $R1 = R2 = R3$ ，特性的重要性划分为 $R > P$ 。本文进行了 20 次联邦学习的实验，每次联邦学习任务的最大迭代次数为 50。新历史交互的权重交互 $\varepsilon = 0.6$ ，过去历史交互的权重 $\sigma = 0.4$ 。数据包传输失败的概率为 1%~

40%，且数据拥有方的初始信誉值为 0.5。同时，将本文提出的结合贝叶斯的主观逻辑模型与文献[28]中的多权重主观逻辑模型（multi-weight subjective logic model）进行比较，以分析在不确定交互情况下两种方案对信誉值和联邦学习准确性的影响。

4.2.2 实验结果

图 5 展示了恶意攻击者在不同攻击强度下对联邦学习的影响。可以看出，攻击强度的提高会导致联邦学习准确率的降低。此外，当攻击强度相同时，攻击者越多，联邦学习的准确率就会越低。当攻击强度为 0.9，且存在 3 个攻击者时，联邦学习的准确率仅为 71%，攻击强度为 0.5 且比有一个攻击者的情况低 26%。因此，攻击强度和攻击者数量的提高能够对联邦学习的准确性产生明显的负面影响。

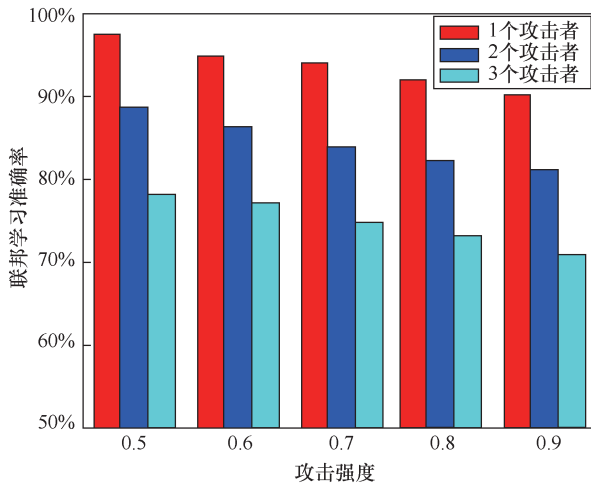


图 5 攻击强度对联邦学习准确率的影响
Figure 5 The impact of attack strength on federated learning accuracy

为了测试恶意攻击者在不同联邦学习任务次数下的信誉变化，本文设定该攻击者在前 8 次和最后 4 次联邦学习任务中不进行攻击，目的是获得较高的信誉值。但在第 9~16 次实验中，会向任务发布方上传恶意的模型参数，实验结果如图 6 所示。在前 8 次实验中，本文方案和文献[28]中的方案对攻击者的信誉值没有很大差异，其信誉值总体是增加的，中间出现的波动主要是由于受到了通信质量的影响。当攻击者采取攻击行为时，其信誉值显著下降，且本文的方案比文献[28]方案信誉值下降更快。在整个攻击期间，信誉值从

0.87 下降到 0.66，下降了 0.21。在之后的实验中，本文方案攻击者的信誉值已有所增加，但文献[28]方案的信誉值仍在降低。图 7 展示了信誉值阈值对联邦学习准确率的影响。如果计算后的数据拥有方信誉值低于给定的信誉阈值，则该数据拥有方被视为不可靠的参与方。

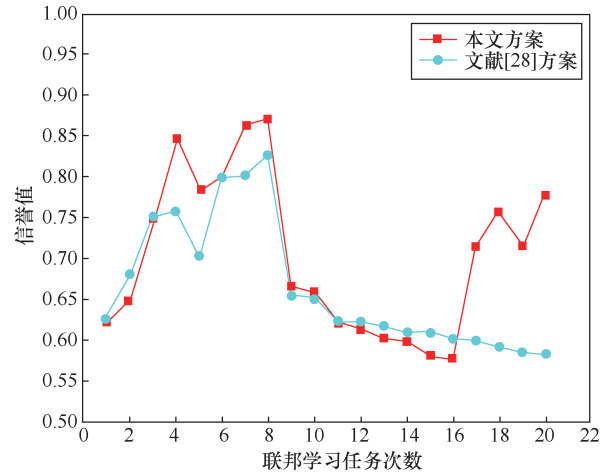


图 6 一个攻击者在不同联邦学习任务次数下的信誉值变化
Figure 6 The reputation value of an attacker under different number of federated learning task

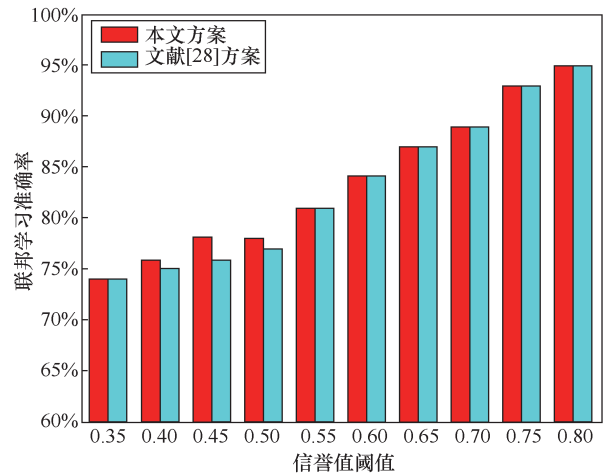


图 7 信誉值阈值对联邦学习准确率的影响
Figure 7 The impact of reputation value thresholds on federated learning accuracy

从图 7 中可以看出，随着信誉值阈值的增加，联邦学习的准确率也会增加。当信誉值范围为 0.35 到 0.5 时，文献[28]方案中的准确率比本文方案的准确率低，但当信誉值阈值不小于 0.55 时，文献[28]方案的性能与本文相同。这是由于本文在计算信誉值时采用贝叶斯公式，计算了数据拥有方在传输失败时的信誉值，更多地考虑了节点

正交互的影响,而文献[28]忽略了这种情况,这会导致部分表现良好的数据拥有方信誉值偏低,被选择参与联邦学习的概率降低,从而降低参与方的积极性。当信誉值阈值高于0.55时,任务发布方更容易检测恶意的数据拥有方,两种方案都会选择信誉较高的数据拥有方,因此联邦学习的准确率没有差别。

综上,本文的方案可以实现更准确和公平的信誉计算,从而能够使任务发布方选择更可靠的数据拥有方。

5 结束语

本文提出了一种基于信誉评估机制和区块链的移动网络联邦学习方案。为了选择可靠的数据拥有方参与模型训练,引入了基于信誉的选择方法,并采用主观逻辑模型和贝叶斯模型,根据数据拥有方的交互历史和间接信誉评估计算其信誉值。通过将信誉评估机制和访问策略集成到智能合约中,任务发布方对数据拥有方做出的信誉意见被存储到联盟链中。实验分析表明,本文的方案可以选择更多的信誉较高的数据拥有方参与训练,提高联邦学习的准确率。此外,数据拥有方的数量和联邦学习算法的选取与信誉值的计算密切相关,如何动态地调节信誉值阈值的大小,将恶意数据拥有方的负面影响降到最低,是本文下一步的研究方向。

参考文献:

- [1] LUETH K L. State of the IoT 2018: number of IoT devices now at 7B—Market accelerating[J]. IoT Analytics, 2018, 8.
- [2] PRYSS R, REICHERT M, HERRMANN J, et al. Mobile crowd sensing in clinical and psychological trials: a case study[C]//Proceedings of International Symposium on Computer-Based Medical Systems. 2015: 23-24.
- [3] 王仁生, 吴天昊, 张琳, 等. 基于区块链的智能网联车队协同轨迹预测系统[J]. 网络与信息安全学报, 2020, 6(3): 78-87.
WANG R S, WU T H, ZHANG L, et al. Cooperative trajectory prediction system for intelligent and automated connected convoy based on blockchain[J]. Chinese Journal of Network and Information Security, 2020, 6(3): 78-87.
- [4] ZHU X, LI H, YU Y. Blockchain-based privacy preserving deep learning[C]//Proceedings of International Conference on Information Security and Cryptology. 2018: 370-383.
- [5] MCMAHAN B, MOORE E, RAMAGE D, et al. Communication-efficient learning of deep networks from decentralized data[C]//Proceedings of Artificial Intelligence and Statistics. 2017: 1273-1282.
- [6] BONAWITZ K, EICHNER H, GRIESKAMP W, et al. Towards federated learning at scale: system design[J]. arXiv preprint arXiv:1902.01046, 2019.
- [7] YANG Q, LIU Y, CHEN T, et al. Federated machine learning: Concept and applications[J]. ACM Transactions on Intelligent Systems and Technology, 2019, 10(2): 1-19.
- [8] ANH T T, LUONG N C, NIYATO D, et al. Efficient training management for mobile crowd-machine learning: a deep reinforcement learning approach[J]. IEEE Wireless Communications Letters, 2019, 8(5): 1345-1348.
- [9] HARD A, RAO K, MATHEWS R, et al. Federated learning for mobile keyboard prediction[J]. arXiv preprint arXiv:1811.03604, 2018.
- [10] LIANG L, YE H, LI G Y. Toward intelligent vehicular networks: a machine learning framework[J]. IEEE Internet of Things Journal, 2018, 6(1): 124-135.
- [11] TRAN N H, BAO W, ZOMAYA A, et al. Federated learning over wireless networks: optimization model design and analysis[C]//Proceedings of IEEE INFOCOM 2019—IEEE Conference on Computer Communications. 2019: 1387-1395.
- [12] LI Y, COURCOUBETIS C, DUAN L. Recommending paths: Follow or not follow[C]//Proceedings of IEEE INFOCOM 2019—IEEE Conference on Computer Communications. 2019: 928-936.
- [13] FUNG C, YOON C J M, BESCHASTNIKH I. Mitigating sybils in federated learning poisoning[J]. arXiv preprint arXiv:1808.04866, 2018.
- [14] KANG J, XIONG Z, NIYATO D, et al. Toward secure blockchain-enabled Internet of Vehicles: Optimizing consensus management using reputation and contract theory[J]. IEEE Transactions on Vehicular Technology, 2019, 68(3): 2906-2920.
- [15] REHMAN M H, SALAH K, DAMIANI E, et al. Towards blockchain-based reputation-aware federated learning[C]//Proceedings of IEEE INFOCOM 2020—IEEE Conference on Computer Communications Workshops. 2020: 183-188.
- [16] LIU Y, AI Z, SUN S, et al. Fedcoin: A peer-to-peer payment system for federated learning[M]//Federated Learning. Springer, Cham, 2020: 125-138.
- [17] WU L, MENG K, XU S, et al. Democratic centralism: A hybrid blockchain architecture and its applications in energy internet[C]//Proceedings of 2017 IEEE International Conference on Energy Internet (ICEI). IEEE, 2017: 176-181.
- [18] LIND J, NAOR O, EYAL I, et al. Teechain: reducing storage costs on the blockchain with offline payment channels[C]//Proceedings of the 11th ACM International Systems and Storage Conference. 2018: 125-125.
- [19] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[R]. Manubot, 2019.
- [20] BENJI M, SINDHU M. A study on the Corda and Ripple blockchain platforms[C]//Proceedings of Advances in Intelligent Systems and Computing. 2019: 179-187.
- [21] BOGNER A, CHANSON M, MEEUW A. A decentralised sharing app running a smart contract on the ethereum blockchain[C]//Proceedings of the 6th International Conference on the Internet of Things. 2016: 177-178.
- [22] 孟博, 刘加兵, 刘琴, 等. 智能合约安全综述[J]. 网络与信息安

全学报, 2020, 6(3): 1-13.

MENG B, LIU J B, LIU Q, et al. Survey of smart contract security[J]. Chinese Journal of Network and Information Security, 2020, 6(3): 1-13.

- [23] BENJI M, SINDHU M. A study on the Corda and Ripple blockchain platforms[M]//Advances in Big Data and Cloud Computing. Springer, Singapore, 2019: 179-187.

- [24] 张凯, 潘晓中. 云计算下基于用户行为信任的访问控制模型[J]. 计算机应用, 2014, 34(4): 1051-1054.

ZHANG K, PAN X Z. Access control model based on user behavior trust in cloud computing[J]. Journal of Computer Applications, 2014, 34(4): 1051-1054

- [25] 王海勇, 潘启青, 郭凯璇. 基于区块链和用户信用度的访问控制模型[J]. 计算机应用, 2020, 40(6): 1674-1679.

WANG H Y, PAN Q Q, GUO K X. Access control model based on blockchain and user credit[J]. Journal of Computer Applications, 2020, 40(6): 1674-1679

- [26] HUANG X, YU R, KANG J, et al. Software defined networking for energy harvesting internet of things[J]. IEEE Internet of Things Journal, 2018, 5(3): 1389-1399.

- [27] XIONG L, LIU L. Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities[J]. IEEE Transactions on Knowledge and Data Engineering, 2004, 16(7): 843-857.

- [28] KANG J, XIONG Z, NIYATO D, et al. Reliable federated learning for mobile networks[J]. IEEE Wireless Communications, 2020, 27(2): 72-80.

[作者简介]



杨明（1994-），男，内蒙古包头人，信息工程大学硕士生，主要研究方向为大数据安全、区块链技术。



胡学先（1982-），男，湖北红安人，博士，信息工程大学副教授，主要研究方向为安全协议、大数据安全。



张启慧（1983-），女，安徽阜阳人，博士，信息工程大学讲师，主要研究方向为安全协议、大数据安全。



魏江宏（1987-），男，甘肃定西人，博士，信息工程大学讲师，主要研究方向为属性基密码、大数据安全。



刘文芬（1965-），女，湖北安陆人，桂林电子科技大学教授、博士生导师，主要研究方向为网络通信、信息安全。