计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.210700195

一种面向电能量数据的联邦学习可靠性激励机制

王　鑫[1,3,4]　周泽宝[1]　余　芸[2]　陈禹旭[2]　任昊文[2]　蒋一波[1]　孙凌云[3,4]
1 浙江工业大学计算机科学与技术学院　杭州 310023
2 中国南方电网数字电网研究院有限公司　广州 510663
3 浙江大学南方电网人工智能创新联合研究中心　杭州 310058
4 浙江大学计算机科学与技术学院　杭州 310058

摘　要　联邦学习解决了数据安全日益受到重视条件下的数据互用难题,但是传统联邦学习缺少鼓励和吸引数据拥有方参与到联邦学习中的激励机制,联邦学习审核机制的缺失给恶意节点进行破坏攻击提供了可能性。针对这个问题,文中提出基于区块链技术的面向电能量数据的可靠的联邦学习激励机制。该方法从对数据参与方的训练参与进行奖励和对数据参与方的数据可靠性进行评估两方面入手,设计算法对数据参与方的训练效果进行评估,从训练效果和训练成本等角度来确定数据参与方的贡献度,并根据贡献度来对参与方进行奖励,同时针对数据参与方的可靠性建立声望模型,根据训练效果对数据参与方的声望进行更新,藉此实现对数据参与方的可靠性评估。基于联邦学习开源框架和真实电能量数据进行算例分析,所得结果验证了所提方法的有效性。

关键词:电力计量;联邦学习;区块链;激励机制;可靠性;声望模型
中图法分类号　TP391

Reliable Incentive Mechanism for Federated Learning of Electric Metering Data

WANG Xin[1,3,4],ZHOU Ze-bao[1],YU Yun[2],CHEN Yu-xu[2],REN Hao-wen[2],JIANG Yi-bo[1] and SUN Ling-yun[3,4]
1 College of Computer Science and Technology,Zhejiang University of Technology,Hangzhou 310023,China
2 Digital Grid Research Institute Co. Ltd.,China Southern Power Grid,Guangzhou 510663,China
3 Zhejiang University-China Southern Power Grid Joint Research Centre on AI,Hangzhou 310058,China
4 College of Computer Science and Technology,Zhejiang University,Hangzhou 310058,China

Abstract　Federated learning has solved the problem of data interoperability under the premise of satisfying user privacy protection and data security. However,traditional federated learning lacks an incentive mechanism to encourage and attract data owners to participate in federated learning. Meanwhile,the lack of a federated learning audit mechanism provides the possibility for malicious nodes to conduct sabotage attacks. In response to this problem,this paper proposes a reliable federated learning incentive mechanism for electric metering data based on blockchain technology. This method starts from two aspects:rewarding data participants for training participation and evaluating data reliability for all of them. We design an algorithm to evaluate the training effect of data participants. The contribution of data participants is determined from the perspective of training effect and training cost,and the participants are rewarded according to the contribution. At the same time,a reputation model is established for the reliability of the data participants,and the reputation of the data participants is updated according to the training effect,so as to achieve the reliability assessment for data participants. Based on the open-source framework of federated learning and real electric metering data,a case study is carried out,and the obtained results verify the effectiveness of our method.

Keywords　Electricity metering,Federated learning,Blockchain,Incentive mechanism,Reliability,Reputation model

大数据人工智能将是未来智能电网的核心。若要在电网领域实现各类电能计量数据的分析和智能化应用,除了需要高效的机器学习算法,还需要类型广、体量大、维度高的电力系统大数据资源。分布式机器学习能够基于大规模数据量和计算能力,提高数据分析计算的能力和速度[1]。目前电网公司已经在电网系统配置了相关技术,不断收集和整合来自数百万台智能传感器的数据,并在一定程度上实现了自主学习大型数据集中的模式并分析了存在的异常现象,但是现阶段数据的使用还局限于区域内。区域内数据集中模式虽然能够较好地反映区域电力系统的运行特征,但具有较强的区域

到稿日期:2021-07-19　返修日期:2021-08-16
基金项目:国家重点研发计划(2020YFB0906004)
This work was supported by the National Key R&D Program of China (2020YFB0906004).
通信作者:王鑫(xinw@zjut.edu.cn)

特征，无法统一表征整个地区甚至全网的运行特征。造成此问题的主要原因为各电力部门采集的数据具有保密性，分享数据需要经过繁琐的手续且需要花费高昂的传输成本，并且可能会造成自身隐私数据的泄露甚至对自身数据系统造成破坏，因此大规模跨地区使用数据非常困难，电力系统内部的数据孤岛问题亟待解决。

联邦学习是解决数据孤岛问题的新兴技术，由 Google 团队于 2016 年首先提出[2]。联邦学习定义了一种新的分布式机器学习框架，在此框架下通过设计虚拟模型来解决不同数据拥有方在不交换数据的情况下进行协作的问题，能有效帮助多个机构在满足用户隐私保护、数据安全和政府法规的要求下，进行数据使用和机器学习建模[3]。将联邦学习引入电力系统能够有效解决电力系统内部存在的数据孤岛问题，Zheng 等[4]针对电力计量系统的数据特征和应用场景，提出了一种面向电力计量系统的联邦学习框架。他们的研究工作很好地解决了电力计量领域本地数据的隐私保护问题，但是其采用的联邦学习框架缺少鼓励和吸引数据拥有方参与到电能量联邦学习中的激励机制，与此同时，审核机制的缺失也给恶意破坏节点提供了攻击联邦学习过程的机会。

目前针对联邦学习的激励机制和审核机制已有一些研究工作。Liao 等[5]提出了一套应用于点对点(Peer-to-peer，P2P)网络的社会规范准则模型，通过博弈收益分析给出了一种能够有效激励节点协作和抑制节点搭便车行为的激励策略。本文参考了 Liao 等的思路，对激励方法进行了优化。Li 等[6]提出了一种包括身份认证、传感数据上传、星际文件系统(Inter-Planetary File System，IPFS)存储、区块链上传、访问验证 5 个部分的可信存储机制，构建电能量数据星际存储联盟链(Interplanetary Storage Consortium Blockchain，ISCB)，利用区块链实现身份认证、密钥分配、权限管理和共识算法，并通过 IPFS 实现数据上传和访问，实现了电能量数据的区块链扩容存储和防篡改。Bao 等[7]针对传统联邦学习缺少吸引数据参与方的激励机制和审核机制，错误的数据可能对模型造成极大破坏的问题，提出了 FLChain 系统，引入了区块链技术、梯度加密和解密共享技术，组建去中心化的、可审计的、可追踪的、具有信任机制和激励机制的联邦学习生态系统，并且 FLChain 提供了一个经过良好测试的联邦学习市场系统供数据参与方利用数据盈利，一定程度上解决了传统联邦学习框架缺少激励机制的问题。Short 等[8]提出使用区块链技术改善联邦学习系统的安全性，通过区块链加密传输联邦学习过程中的各类信息，虽然能够实现联邦学习中信息的安全和可追溯，但是区块链的计算开销非常大。Ismael 等[9]提出的解决方案通过使用企业运营体系(Enterprise Operation System，EOS)区块链和 IPFS 系统设计新的联邦学习工作框架和工作流程，结合类抽样验证错误方案，对梯度上传进行验证和奖励，保证了数据的安全性，同时根据数据集大小判定参与节点的贡献值大小，实现了联邦学习框架的数据安全性和有效激励。该研究使用区块链存储激励相关信息的方案给予了本文一定启发。Toyoda 等[10]为联邦学习引入重复竞争机制，新一轮的数据参与方能够使用上一轮数据参与方训练后的模型数据，并根据自身的使用效果对上一轮数据参与方的训练效果进行投票，由此决定上一轮数据参与方的奖励所得，重复竞争机制的引入很好地保证了数据的有效性，同时能够促使拥有高质量数据的数据节点参与到联邦学习中，但是重复竞争机制给节点私下串通以获得高额奖励提供了可能。Weng 等[11]提出的 DeepChain 方案利用协同加密技术，引入惩罚机制，通过正确性验证和超时检查等手段一定程度上解决了联邦学习的吸引力和安全性问题。DeepChain 方案的惩罚机制在本文数据审核中有所借鉴。Han 等[12]提出的联邦学习激励方法(Federated Learning Incentivizer，FLI)方案以上下文感知的方式在联邦学习数据节点之间动态地划分给定的奖励预算，通过共同最大化集体效用和最小化数据节点之间的不平等，来实现奖励分配的公平、公正和高效，以期达到激励机制对数据节点的吸引效果。本文参考了其根据数据节点贡献进行奖励分配的思路。Kang 等[13]定义了一个主观逻辑模型，该模型将交互产生的直接声誉意见和来自其他任务发布者的间接声誉意见集成到一个用于工作者选择的综合声誉意见中，通过引入多权重主观逻辑模型和契约理论来实现用户可靠性的维护。Tang[14]在贝叶斯博弈模型中引入 TFT(Tit for Tat)策略，提出一种节点激励机制改进的 TFT 策略，以对网络中的自私节点进行有效激励。Zhou 等[15]将显性时空关联的用户激励问题转化为集合覆盖问题并利用贪心算法对其进行求解，同时结合显性时空关联算法和马尔可夫模型求解隐性时空关联的用户激励问题。本文参考 Kang 等的方法定义了一个声望模型，在使用声望表征用户可靠性的同时，从声望计算和更新入手简化流程并降低计算消耗。

Bao 等的 FLChian 使用区块链技术组建了联邦学习市场系统，针对参与激励和用户审核进行了优化，信任机制和激励机制相结合有非常好的效果，但实现繁琐且不适用于电力系统；Short 等使用区块链记录了联邦学习过程中的各类信息，这能够保证相关信息的公开和可追溯，但也给系统带来了很大的存储和计算开销；Toyoda 等先使用联邦学习资源再对资源进行评价的方案和 Kang 等的主观逻辑模型方案能够对联邦学习的成果进行比较合理的评价，但引入过多的主观因素使计算变得繁琐且给作弊提供了机会。本文基于上述分析提出了一种面向电能量数据的联邦学习可靠性激励机制，为传统面向电力计量系统的联邦学习框架引入激励机制，在保证联邦学习正常工作的情况下实现对数据拥有方的有效可激励，并保证数据参与节点的可靠性。本文的贡献主要有以下 3 点：1)引入模型评估指标作为联邦学习效果评估的依据，并根据评估结果对参与方数据进行可靠性判断，统筹计算成本等其他因素进行参与方贡献度计算，保证了激励机制和审核机制在不同类型联邦学习中的通用性；2)引入声望模型描述数据节点的可靠性，并设计了新的声望模型计算方案，数据节点的声望计算与其历史可靠性评估结果直接相关，通过声望实现对数据节点的审核和筛选，并且节点每次参与联邦学习都会对其本身的声望产生影响；3)针对电力计量系统的特点设计了独特的区块链，引入权威证明(Proof of Authority，PoA)共识机制，简化区块结构，降低电能量节点使用区块链的计算成本，并使用区块链实现联邦学习激励机制和声望模型相关数据的存储。

本文第 1 节对所提出的面向电能量数据的联邦学习可靠性激励机制的整体流程和模块设计进行了整体介绍；第 2 节

对激励机制中 4 个核心模块进行了详细介绍；第 3 节根据本文方法的流程，结合联邦学习（Federated AI Technology Enabler，FATE）开源框架，使用电能量数据设计算例实验对本文方法进行有效性验证；最后总结全文。

1　整体介绍

Zheng 等[4]提出了面向电力计量系统的联邦学习框架的整体架构，该框架允许各参与公司在本地保留自己所在管辖区域内采集到的原始用户数据，且这些本地数据之间存在数据壁垒隔绝。本文为面向电力计量系统的联邦学习框架引入了基于区块链技术的可靠性激励机制，设计了实现激励机制的总体流程以及激励机制和声望模型的详细算法，其中激励机制和声望模型的数据存储由区块链技术保障，联邦学习任务调度和联邦模型聚合使用联邦学习开源框架 FATE[16]实现。

本文联邦学习可靠性激励机制的整体工作流程如图 1 所示。在联邦学习过程中，数据需求方首先根据自身需求发布联邦学习任务；各数据节点根据自身数据提交任务参与申请；数据需求方接收各个数据节点的参与请求，在请求期结束后，爬取候选数据节点在区块链中的相关记录并完成候选数据节点的声望计算；根据各候选节点的声望值选择参与联邦学习的数据节点；确定数据参与节点后，调度数据需求方和各数据参与方进行联邦学习；数据需求方收集各数据参与方的训练结果，进行训练效果评估和贡献度计算，以及进一步的数据参与方奖励分配（用于激励机制实现）和可靠性评估（用于审核机制实现）；利用区块链技术对相应的奖励信息和可靠性评估信息进行存储。

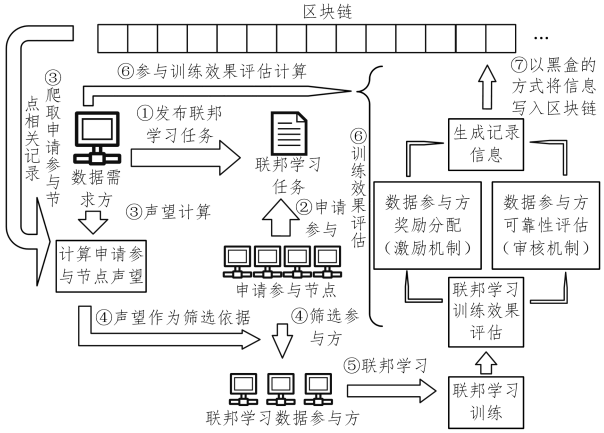

图 1　可靠的联邦学习激励机制的整体流程

Fig. 1　Overall workflow of reliable incentive mechanism for federated learning

联邦学习需要在训练过程中进行参数交换，其目的是将各个参与者的中间训练参数进行汇总融合并分发回去，以让各个参与者更新自己的本地模型，这就需要联邦学习协调模块。联邦学习协调模块如图 2 所示，其由训练调度模块、激励机制模块、声望模型模块和区块链模块 4 部分构成。其中，训练调度模块负责指导数据节点之间的数据交换和使用区块链记录相关信息；激励机制模块负责各参与数据节点的贡献度计算和对相应数据节点的奖励；声望模型模块负责各数据节点的可靠性管理和对优质数据源的筛选；区块链模块负责对相应的激励信息和声望信息进行去中心化的存储。

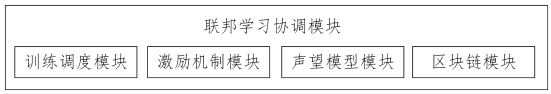

图 2　联邦学习协调模块

Fig. 2　Coordination module for federated learning

2　可靠激励机制模块设计

2.1　模型训练调度模块

联邦学习训练调度模块融合了联邦学习开源框架协调调度计算资源的功能，同时负责激励机制中其他模块的协调调用，具体有：1）将初始模型分发给各数据参与方；2）在各数据参与方利用本地数据对模型进行训练后，收集各参与方的回传信息并进行验证；3）调用激励机制模块和声望模型模块，对各个数据参与节点进行贡献度计算和可靠性计算，并对联邦模型进行聚合；4）调用区块链模块进行奖励分配信息和可靠性评估信息的存储。

在声望模型模块完成数据节点声望计算并选择参与联邦学习的数据节点后（见图 3），第①步训练调度模块负责将电能量数据需求节点的初始模型的全局模型参数 W 同对齐特征信息一同加密并分发给各参与电能量数据节点（子公司）。此时训练调度机制工作已经完成，各参与节点根据收到的模型信息部署本地模型并进行第②步，利用本地电能量数据对本地模型（即初始联邦模型的本地备份 M_{init}）进行训练，M_{train} 是参与数据节点使用本地数据对模型 M_{init} 进行训练后的结果。在电能量数据参与节点训练完成后，训练调度模块进行第③步，提取参与节点训练模型 M_{train} 的全局模型参数 W，将训练得到的模型信息同其他用于激励机制实现的辅助信息一同发送至电能量数据需求节点。

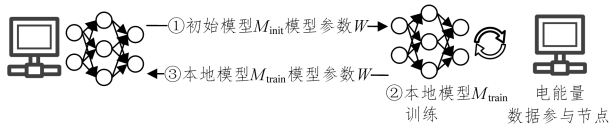

图 3　训练调度过程

Fig. 3　Process of training scheduling

训练调度模块收集各电能量数据参与节点发送的信息并对信息进行验证，验证通过后解析信息，将模型信息传入激励机制模块和声望模型模块并进行调用，以进行进一步的贡献度和可靠性计算，详细计算过程将在激励机制模块和声望模型模块部分进行介绍。在激励机制模块和声望模型模块分别完成对各数据参与节点的奖励计算和可靠性评估计算后，训练调度模块将调用区块链模块对相应的奖励信息和可靠性评估信息进行去中心化存储。

2.2　激励机制模块

激励机制模块对本文提出的可靠的联邦学习激励机制十分重要，该模块在联邦学习过程中主要负责两个方面，即数据参与方的贡献度计算和奖励分配，模块工作流程如图 4 所示。

在经典联邦学习框架中，各用户都是用各自的本地数据对同一个联邦模型进行训练，即都是优化同一个模型，因此本文选择对同一初始模型的优化结果作为联邦学习数据参与方的训练评估结果。

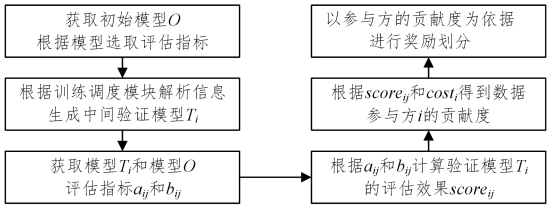

图 4 激励机制模块的工作流程

Fig. 4 Workflow of incentive mechanism module

在训练调度模块对各个节点发送的第 j 次训练数据进行验证之后，验证通过后的数据将作为参数调用激励机制模块，激励机制模块使用节点 i 发送数据中的梯度数据生成中间验证模型 T_i，同时获取本轮次训练调度模块分发的初始模型 O，并根据模型的类型选取适合的评估指标，如分类模型 F1-score 指标、回归模型的 R2-score 指标等，当然也可以自行定义。指标值越大，模型的精度就越高，鲁棒性也越好。在初始模型、中间验证模型以及评估指标都确定后，获取训练模型 T_i 和初始模型 O 的评估指标值 a_{ij} 和 b_{ij}，a_{ij} 和 b_{ij} 的数量关系将作为对数据参与方 i 的训练评估结果 $score_{ij}$ 的依据。

$$score_{ij}=\begin{cases}-1, & a_{ij}<b_{ij}\\ \dfrac{a_{ij}-b_{ij}}{b_{ij}+e^{-10}}, & a_{ij}\geqslant b_{ij}\end{cases} \tag{1}$$

已知在第 j 次训练中，数据节点 i 使用的初始模型 O 的评估指标为 b_{ij}，模型 O 在节点 i 使用本地数据进行训练后，如果模型效果变好，那么其评估指标应该大于 b_{ij}，即中间验证模型 T_i 的评估指标 a_{ij} 应大于初始模型评估指标 b_{ij}，反之亦然。因此，当 $a_{ij}<b_{ij}$ 时，数据节点 i 利用本地数据对模型进行训练的效果极差，此时应该对数据参与方 i 打低分，即 $score_{ij}=-1$；当 $a_{ij}\geqslant b_{ij}$ 时，数据节点 i 利用本地数据对模型进行训练后模型将得到优化。式(1)为了防止表达式出现除以 0 的情况，在表达式分母中加上了一个很小的正数。为了让同一轮次不同数据参与方的评估更加公平，本文利用初始模型 O 的评估指标进行标准化，即评估结果等于评估指标提升值/初始评估指标。

为了有效地鼓励和吸引数据拥有方使用更多数据参与联邦学习，公平公正的奖励机制是有利的技术支撑，而为了对参与方进行公平的激励，需要合理的奖励分配依据。本文按照联邦学习数据参与方的贡献度对其进行奖励分配。贡献度的大小不仅取决于数据参与方的训练结果评估，还应该与参与方的训练成本相关，数据参与方 i 在第 j 次训练中的贡献度 con_{ij} 应该由训练效果评估 $score_{ij}$ 和训练成本 $cost_{ij}$ 相乘得到。研究[9]表明，用户 i 使用本地资源 D_i 对模型进行训练时，所产生的训练成本 $cost_{ij}$ 与用户 i 的数据集大小 n_{ij} 成线性关系，k 为两者之间的相关系数，即：

$$cost_{ij}=k\times n_{ij} \tag{2}$$

进而，数据参与方 i 的贡献度为：

$$con_{ij}=cost_{ij}\times score_{ij} \tag{3}$$

根据数据节点提供的数据规模和数据整体质量对数据节点的贡献度进行计算评估，有利于吸引更大规模、更高质量的数据参与到联邦学习中。

针对数据参与方的奖励方法主要考虑在针对联邦学习数据参与方进行奖励时，应当综合考虑平等、边际收益和边际损失的博弈，对数据参与方进行奖励分配。由数据参与方的贡献计算方法得到的各方贡献为分配依据，按照收益分配方法进行奖励的分配，以保证公平性，同时提高数据拥有方参与联邦学习的热情。在各个数据参与方的贡献度都计算完成后，需要对各方进行公正合理的奖励分配。Han 等[12]基于博弈理论以及贡献公平性、期望损失分配公平性和期望公平性三大标准提出的 FLI 方案，证明了按劳分配原则在联邦学习过程中的可行性，因此本文在进行奖励分配时也秉持公平的按劳分配原则，按照各数据参与方的贡献对其进行奖励。W 表示该轮次所有数据参与方的贡献度之和，R 表示数据需求方提供的奖励总额，N 表示通过验证并且 con_{ij} 大于 0 的数据节点数量，则该次训练中各数据参与方 i 应得奖励 r_i 为：

$$r_i=\frac{con_{ij}}{W}R \tag{4}$$

其中，贡献度之和 W 为：

$$W=\sum_{i=1}^{N}con_{ij} \tag{5}$$

2.3 声望模型模块

面向电能量数据联邦学习的声望模型的引入旨在解决联邦学习的可靠性问题，防止恶意节点对联邦学习的攻击造成严重的后果。为实现这一目的，声望模型模块起着举足轻重的作用。本文设计的声望模型为每一个数据节点都维护一个声望值，数据节点的声望值直接反映了其可靠性程度，数据需求方可以根据声望值筛选合适可靠的数据节点作为参与方参与自己组织的联邦学习。本文中，数据节点的声望值不仅考虑了数据节点的历史参与训练的可靠性得分记录，还考虑了可靠性得分记录数据的时间跨度(最近的可靠性得分记录在计算节点声望值的过程中具有更高的权重)和可靠性得分记录给出对象(自身给出的可靠性得分记录在计算节点声望的过程中具有更高的权重)。本文使用区块链技术来实现各电能量数据节点可靠性评估信息的公开记录，保证了可靠性信息的可追溯性和不可篡改性，同时保存的信息也作为实现声望模型的凭证。

在联邦学习框架中，数据需求方发布联邦学习任务后，各数据节点可以根据任务需求和自身的数据特点提交联邦学习参与申请。数据需求方在收到各数据节点的申请后，可以根据区块链中记录的历史信息计算各申请参加的数据节点的声望值，具体流程如图 5 所示。

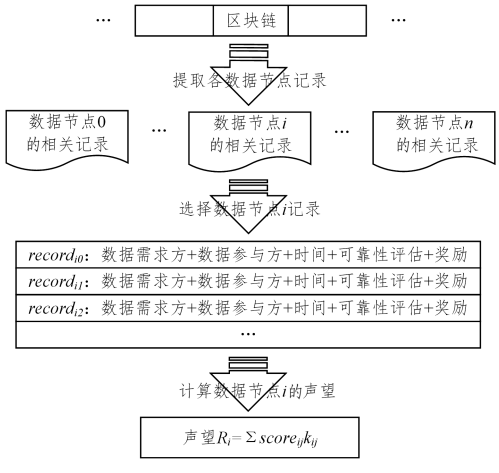

图 5 数据节点的声望计算方法

Fig. 5 Calculation method of data node's reputation

声望模型模块首先查找区块链，提取链中申请参与当前联邦学习的数据节点的所有历史记录，并按照数据节点对提取的记录进行分组。对于数据节点 i 的相关记录集合 S（集合大小为 N），每一条记录 $record_{ij}$ 表示数据节点 i 第 j 次训练的相关信息，包括数据需求方 $guest_{ij}$、数据节点（数据参与方）$host_{ij}$、记录时间 $time_{ij}$、可靠性评估结果 $score_{ij}$ 以及用于进行激励的奖励和参与方收款地址，数据节点 i 的声望 R_i 的计算式为：

$$R_i=\sum_{j=0}^{N} score_{ij} * k_{ij} \tag{6}$$

其中，k_{ij} 表示数据节点 i 的各可靠性评估结果 $score_{ij}$ 的权重，对于某条历史记录，l 表示计算系数，如果记录中的数据需求方为此次联邦学习任务的数据需求方 $guest$ 本身，那么该条记录将具有更高的权重 $weight(weight>1)$，最终权重 k_{ij} 由对应的数据需求方 $guest_{ij}$ 和记录时间跨度 $span_{ij}$（$span_{ij}=NOW-time_{ij}$，单位为天）共同决定，数据节点 i 只有时间跨度阈值 $threshold_{\text{span}}$ 内的可靠性记录才会被用于数据节点的声望计算，即 $k_{ij}=weight(guest_{ij},span_{ij})$，具体表示为：

$$k_{ij}=\begin{cases}0, & span_{ij}>threshold_{\text{span}}\\ \dfrac{l}{span_{ij}+1}, & guest_{ij}\neq guest\\ \dfrac{weight*l}{span_{ij}+1}, & guest_{ij}=guest\end{cases} \tag{7}$$

本文结合电网实际应用场景，经过灵敏度分析后确定在 l 设为 1、$threshold_{\text{span}}$ 设为 100、$weight$ 设为 1.5 的情况下能得到较好的效果。

在本文的联邦学习框架设计中，可靠性评估用训练评估 $score_{ij}$ 表示，因为训练效果好的模型训练往往代表着参与模型训练的数据也更加可靠。在各个申请参与联邦学习的数据节点的声望值计算都完成后，数据需求方可以根据各候选节点的声望值选择合适的数据节点参与联邦学习训练。

数据节点每一次参与联邦学习训练的经历都将影响节点本身的声望，基于上述提到的数据节点声望值的计算方法，本文提供的方法通过使用区块链记录数据节点每一次参与联邦学习任务的可靠性评估结果，以实现对数据节点声望值的更新。数据节点声望值的更新流程如图 6 所示。

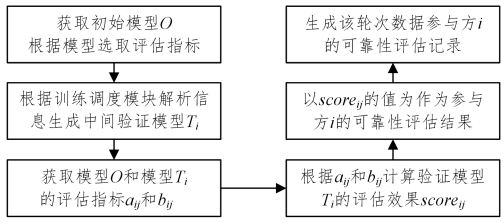

图 6　数据节点声望更新工作的流程

Fig. 6　Workflow of node's reputation updating

可靠性评估过程与第 2 节的训练结果评估过程类似，训练调度模块对各个节点发送的数据进行验证，验证通过后的数据将作为参数调用声望模型模块，声望模型模块使用节点 i 发送数据中的梯度数据生成中间验证模型 T_i，同时获取本轮次训练调度模块分发的初始模型 O，并根据模型的类型选取适合的评估指标。在初始模型、中间验证模型以及评估指标都确定以后，从中间验证模型 T_i 获取评估指标值 a_{ij}，并从初始模型 O 获取评估指标值 b_{ij}，a_{ij} 和 b_{ij} 的数量关系，并将其作为对数据参与方 i 的训练评估结果 $score_{ij}$ 的依据。

$$score_{ij}=\begin{cases}-1, & a_{ij}<b_{ij}\\ \dfrac{a_{ij}-b_{ij}}{b_{ij}+e^{-10}}, & a_{ij}\geqslant b_{ij}\end{cases} \tag{8}$$

因为训练效果好的模型训练往往代表着参与模型训练的数据也更加可靠，所以本文选择使用训练评估结果 $score_{ij}$ 代替此次联邦学习任务中的数据可靠性评估结果。

2.4　区块链模块设计

为了更高效地将面向电能量数据的联邦学习与区块链相结合，本文针对实际应用场景设计了简单高效的区块链结构。该区块链的独特之处在于：1）针对电力计量系统应用场景的共识机制；2）能够减少计算量的区块头设计；3）针对声望模型设计的区块体格式。整体区块链设计如图 7 所示。

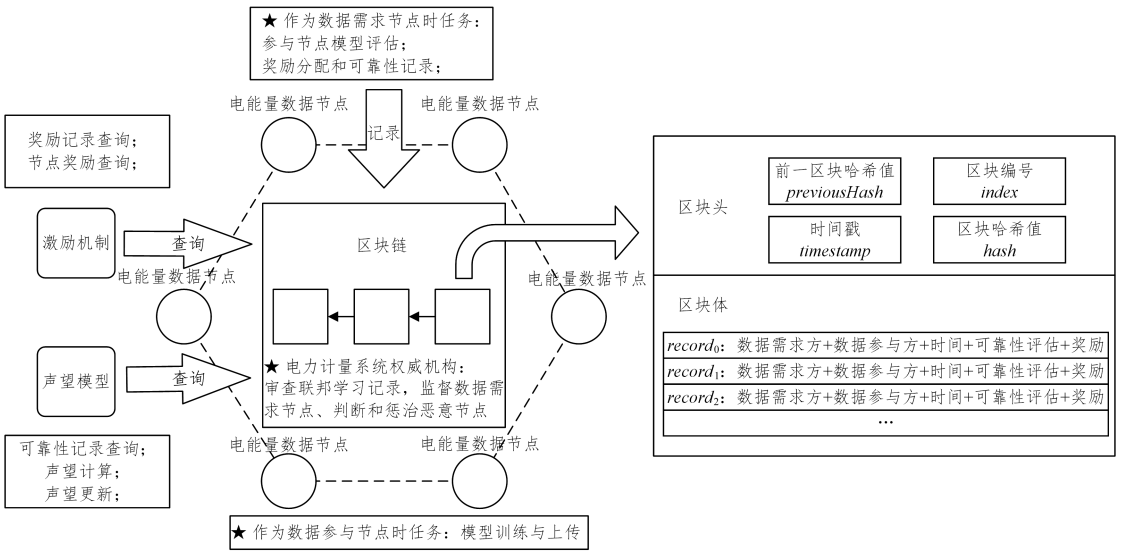

图 7　区块链设计

Fig. 7　Design of blockchain

区块链采用类似 PoA 区块生成机制的共识机制[17]，相比工作量证明(Proof of Work，PoW)区块生成机制，PoA 区块生成机制能够保证各数据节点专注于联邦学习过程本身而不是将算力分散以进行区块打包(挖矿)[18]，有效地减小了区块生成过程中的计算消耗。在面向电能量数据领域的联邦学习框架中，相对固定且封闭的数据节点受电力系统权威机构管控节制，能够保证各数据节点进行正确且合规的区块操作，这为 PoA 机制的实现提供了良好的条件。因此，在联邦学习过程中，当电能量数据节点作为数据参与节点时，不需要对区块链进行相关操作；当其作为数据需求节点时，同时承担作为生成区块的权威节点的任务，负责对相关信息进行区块打包和上传，进而将奖励分配信息和可靠性记录信息记录在区块链中。电力计量系统权威机构作为监督和监察机构，能够审查联邦学习的相关记录，监督数据需求节点区块生成过程中的公平性和正确性，同时判断和惩治恶意节点。

本文设计的区块链从需求出发，删除了传统区块链区块中的冗余属性，在保证功能实现的前提下减小了生成区块的性能开销。区块链中的区块数据如图 7 中左侧区块结构所示，区块头负责记录该区块的基础信息，由 *index*，*previousHash*，*timestamp* 和 *hash* 组成，其中 *index* 表示当前区块的块号，*previousHash* 表示上一个区块的哈希值，用于串联区块成链，*timestamp* 时间戳记录区块生成时间，*hash* 表示当前区块的哈希值，根据区块信息利用 SHA256 加密算法[19]计算得到的加密值为：

$$hash = sha256(index, previousHash, timestamp, data) \tag{9}$$

区块体 *data* 负责记录区块存放的信息数据，针对激励机制和声望模型的算法实现对数据格式的设计和优化。具体为以 json 数组格式记录的电能量数据需求方(guest)、数据参与节点(host)、时间(time)、数据参与方训练模型的可靠性评估结果(score)以及参与方参与联邦学习所获得的奖励(reward)。

3 算例分析

为验证本文方法的有效性，本文基于南方电网某计量中心提供的样本数据、联邦学习开源框架和上述区块链结构进行仿真实验，并对实验结果进行了分析。

3.1 算例说明

本文为模拟所设计的算法在面向电能量数据的联邦学习中的作用效果，基于样本电网数据，使用联邦学习开源框架和区块链进行仿真实验。在仿真过程中，为了模拟真实电力计量系统的联邦学习过程，设置多个数据节点代表不同的电能量数据节点(子公司)，并将原始数据集切分成大小相似的若干个数据集，随机分给各数据节点，同时为各数据节点预设一些可靠性评估记录，以期赋予各数据节点相对均匀的声望值。为了验证基于声望模型的审核机制对恶意数据节点的筛除作用，实验设置了对照组进行对比，预先人为选择几个数据节点，为其设定一些不良的可靠性记录，人为修改其所拥有的数据集的数据，使其模拟能够被声望模型侦测到的恶意节点。实验使用本文方法进行联邦学习，并将其作为实验组，同时使用这些模拟的恶意节点作为对照组进行对照实验。实验预先将上述模拟数据节点在 FATE 联邦学习开源框架和区块链中进行设置。

本节从两个算例的结果出发，分析验证本文方法的有效性。为验证本文算法在不同类型的任务中的有效性，本文使用算例 1 的数据集训练分类模型，使用算例 2 的数据集训练回归模型。

算例 1　家庭用电数据集。该数据集共有 10000 个样本数据，每个样本数据具有 8 维特征并带有 1 个 0-1 标签表示该样本的城乡属性，标签与实际情况相符且近似平均分布，数据随机分发给各模拟数据节点。算例 1 基于家庭用电数据集，使用 FATE 和 SecureBoost 算法[20]进行联邦学习，模拟 3 个电能量数据节点使用本地数据训练分类树模型，并聚合形成分类树联邦模型。训练完成后，使用分类树联邦模型，根据家庭用电数据特征预测家庭城乡属性，并对模型效果进行评估。

算例 2　用电量数据集。该数据集共有 26496 个样本数据，每个样本数据具有 7 维特征并带有 1 个标签，标签值连续且符合实际用电量的分布情况。算例基于某数据采集点用电量数据，使用 FATE 和深度神经网络进行联邦学习。模拟 3 个数据节点使用本地数据训练神经网络，并将其聚合形成神经网络联邦模型并训练完成后，使用神经网络模型，根据各项环境数据指标对用电量进行预测，并对模型预测精度进行分析。

实验为模拟联邦学习场景，首先确定联邦学习任务数据需求方节点，使用数据需求方拥有的数据构建初始模型，并发布联邦学习任务；其次各数据节点计算自身的声望，数据需求方择优参与联邦学习任务；再次使用 FATE 框架，数据需求方和数据参与方利用各自拥有的数据进行本地模型训练并聚合生成联邦模型，同时分别利用各数据参与方的数据进行训练，生成中间验证模型；然后比较中间验证模型参数和初始模型的效果，按照激励机制算法生成奖励计划；最后人工引入恶意节点，使用恶意节点作为数据参与方参与联邦学习训练，聚合生成被恶意影响的联邦模型，通过对照实验验证基于声望模型的审核机制的有效性。

上述实验均在阿里云安装有 64 位 CentOS7.2 系统的 4vCPU/8GiB 的 EOS 云服务器环境下进行。

3.2 激励机制可行性验证

在对激励机制的可行性进行验证之前，首先根据本文提出的联邦学习数据参与方激励方法，计算各电能量数据参与节点的训练效果评估和贡献度计算结果，算例 1 和算例 2 的一组结果如表 1 和表 2 所列。其中，初始模型指数据需求方进行联邦学习前的模型，Id=10000 表示 Id 标识为 10000 的数据节点使用本地数据在初始模型的基础上进行训练得到的模型，聚合模型指 FATE 使用各数据参与节点使用本地数据训练得到的模型聚合形成的模型。

表 1　节点家庭城乡属性分类模型训练效果评估及贡献度

Table 1　Training effect and contribution of node's family urban-rural attribute classification model

模型	*AUC*	训练效果评估	贡献度
初始模型	0.7881	—	—
Id=10000	0.87032	0.10433	20.866
Id=10001	0.9277	0.17713	35.426
Id=10002	0.84107	0.06721	13.442
聚合模型	0.996058	—	—

表 2　节点采集点用电量预测模型训练效果评估及贡献度

Table 2　Training effect and contribution of power consumption prediction model

模型	*R2 score*	训练效果评估	贡献度
初始模型	0.18077	—	—
Id=10000	0.22103	0.22271	44.09658
Id=10001	0.24391	0.34928	69.50672
Id=10002	0.21502	0.18947	37.32559
聚合模型	0.31569	—	—

表 1 列出了某轮基于家庭用电数据进行城乡属性分类模型的联邦学习训练的过程数据，该联邦学习任务以分类模型经典评估指标接受者操作特性曲线（Receiver Operating Characteristic Curve，ROC 曲线）下方的面积（Area Under Curve，AUC）作为模型训练效果的评估依据，根据各数据参与节点中间验证模型的 *AUC* 来计算各节点的训练效果评估结果，进一步根据训练效果和训练成本确定各节点的贡献度。从表中的数据可以看出，各参与方的数据都能对原始模型起到优化的效果，聚合模型的效果最优，训练效果评估和贡献度与 *AUC* 直接相关。

表 2 列出了某轮基于数据采集点用电量数据进行用电量预测模型的联邦学习训练的数据，该联邦学习任务以回归模型经典评估指标 *R2-score* 为模型训练效果的评估依据，根据各数据参与节点中间验证模型的 *R2-score* 来计算各节点的训练效果评估结果，进一步根据训练效果和训练成本确定各节点的贡献度。实验结果与算例 1 一致。

上述实验结果证明了本文提出的激励机制实现方案在算法上是可行的。Hou 等[21]论证了 Stackelberg 博弈模型在信息对称的情况下对用户激励的有效性；Kang 等[13]论证了契约理论模型在信息对称的情况下能够实现联邦学习中任务发布者和数据参与方两者之间的效用最大化，在数据需求方设置总奖励需要考虑信息比率（Information Ratio，IR）和信息系数（Information Coefficient，IC）约束的前提下，实现了数据参与节点效用的最大化。本文通过区块链实现的信息对称的激励博弈模型与 Kang 等所述的契约理论模型相似，数据参与节点只有选择与自己数据类型相匹配的联邦学习任务才能实现自身的最大效用，这就解释了 IC 约束；同时，每个参与节点在选择其数据类型对应的联邦学习任务时，可以获得非负效用，验证了 IR 约束，说明本文提出的激励方案也具有较高的可行性。

3.3　声望模型效果评估

表 3 和表 4 分别列出了算例 1、算例 2 引入对照组作为基准进行对照实验后，对各自训练得到的模型进行评估测试的对照效果。实验通过是否有恶意节点参与联邦学习的训练过程，模拟了声望模型的筛选机制是否发挥作用，同时根据实验结果分析了声望模型防治恶意节点的效果。其中，M_{normal} 和 $M_{\text{malicious}}$ 分别表示利用声望模型筛除恶意数据后进行联邦学习得到的联邦模型和模拟传统框架下无声望模型筛选训练得到的联邦模型。

表 3　城乡分类模型恶意数据影响结果对照

Table 3　Comparison of malicious data's influence on urban-rural classification model

模型	*AUC*	*Precision*	*Recall*	*F1 Score*
M_{normal}	0.996058	1	0.831933	0.966387
$M_{\text{malicious}}$	0.922554	0.923913	0.714286	0.901639

表 4　用电量预测模型恶意数据影响结果对照

Table 4　Comparison of malicious data's influence on power consumption prediction model

模型	*MAE*	*MSE*	*R2 score*
M_{normal}	13.10338	188.37013	0.71569
$M_{\text{malicious}}$	19.72471	241.67551	0.55183

表 3 列出了使用家庭用电数据进行模型训练后得到的城乡分类模型的对照效果，选用 ROC 曲线面积 *AUC*、查准率 *Precision*、召回率 *Recall* 和 F 系数 *F1-score* 指标对训练得到的分类树模型效果进行评价。从表中可以看出，正常的联邦学习 M_{normal} 的各个误差指标均优于作为对比基准的被恶意节点影响的模型 $M_{\text{malicious}}$。*AUC*，*Precision*，*Recall* 以及 *F1-score* 分别提高了 7.96%，8.24%，16.47% 和 7.18%。M_{normal} 相比 $M_{\text{malicious}}$ 具有更好的模型分类精度，表明了在算例 1 中，声望模型的筛除机制很好地起到了防止恶意数据破坏联邦学习的效果。

同样地，表 4 列出了使用某数据采集点用电量数据进行模型训练后得到的用电量预测模型的对照效果，选用平均绝对误差（Mean Absolute Error，MAE）、均方误差（Mean Square Error，MSE）和 R 系数 *R2-score* 指标对训练得到的神经网络模型预测效果进行评价。从表中可以看出，正常的联邦学习 M_{normal} 的各个误差指标均优于作为对比基准的被恶意节点影响的模型 $M_{\text{malicious}}$。*MAE* 和 *MSE* 分别降低了 33.57% 和 22.06%，*R2-score* 提高了 29.69%，M_{normal} 相比 $M_{\text{malicious}}$ 具有更好的预测精度，表明了在算例 2 中，声望模型的筛除机制也很好地起到了防止恶意数据破坏联邦学习的效果。

通过上述两组对照实验不难发现，恶意节点的数据能够明显影响联邦模型的能力，破坏联邦学习的效果，而声望模型的引入能够有效地筛除恶意节点，阻止恶意数据参与到联邦学习中，防止其对联邦学习任务造成不利影响。表 3 和表 4 的实验结果共同表明，无论是在分类任务还是在回归任务中，声望模型的筛除作用都能够有效地保护联邦学习，防止恶意数据破坏联邦学习，证明了基于声望模型审核机制的有效性和适用性。本文算法在筛除恶意数据、提高联邦学习可靠性方面起到了积极作用。

结束语　针对传统面向电力计量系统的联邦学习框架缺少激励机制和节点审核的问题，本文提出了一种面向电能量数据的联邦学习可靠性激励机制。所提方法在传统联邦学习流程的基础上，引入了声望模型对联邦学习参与节点进行

筛选，同时依据模型评估指标对各电能量数据参与节点的训练模型进行训练效果评估，根据训练效果和训练成本计算得到贡献度，并根据各节点贡献度对其进行奖励分配。此外，还根据训练评估效果对节点数据进行可靠性评估，形成节点可靠性记录，并针对可靠性记录设计声望模型以实现对数据节点的审核和筛选。通过算法推演和实验论证发现，对数据参与节点进行奖励，能够有效地鼓励和吸引数据拥有节点参与到联邦学习中，从而为联邦学习提供更多的数据来源，缓解数据紧张问题；此外，声望模型能够有效地筛除恶意节点，防止恶意数据破坏联邦学习，提高通过联邦学习得到的模型的精度和效果。

参 考 文 献

[1] SHU N, LIU B, LIN W W, et al. Survey of Distributed Machine Learning Platforms and Algorithms [J]. Computer Science, 2019, 46(3): 9-18.

[2] MCMAHAN H B, MOORE E, RAMAGE D, et al. Communication-Efficient Learning of Deep Networks from Decentralized Data[C]// AISTATS. 2017: 1273-1282.

[3] YANG Q. AI and Data Privacy Protection: the Way to Federated Learning[J]. Journal of Information Security Research, 2019, 5(11): 961-965.

[4] ZHENG K H, XIAO Y, WANG X, et al. A Federated Learning Framework for Electricity Metering System[J]. Proceedings of The CSEE, 2020, 40(S1): 122-133.

[5] LIAO X K, WANG L S. Research on Incentive Mechanism Based on Social Norms and Boycott [J]. Computer Science, 2014, 41(4): 28-30, 35.

[6] LI J, WU S Q, ZHANG S L, et al. Trusted Storage Mechanism of Distributed Electric Energy Data Based on Blockchain [J]. Chinese Journal of Network and Information Security, 2020, 6(2): 87-95.

[7] BAO X L, SU C, XIONG Y, et al. FLChain: A Blockchain for Auditable Federated Learning with Trust and Incentive[C]// BigCom. 2019: 151-159.

[8] SHORT A R, LELIGOU H C, PAPOUTSIDAKIS M, et al. Using Blockchain Technologies to Improve Security in Federated Learning Systems[C]// 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC). IEEE, 2020.

[9] ISMAEL M, SREYA F, ABDELHAKIM S H. Record and Reward Federated Learning Contributions with Blockchain[C]// CyberC. 2019: 50-57.

[10] TOYODA K, ZHANG A N. Mechanism Design for An Incentive-aware Blockchain-enabled Federated Learning Platform [C]// BigData. 2019: 395-403.

[11] WENG J S, WENG J, LI M, 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.

[12] HAN Y, LIU Z L, LIU Y, et al. A Fairness-aware Incentive Scheme for Federated Learning[C]// AIES. 2020: 393-399.

[13] KANG J W, XIONG Z H, NIYATO D, et al. Incentive Mechanism for Reliable Federated Learning: A Joint Optimization Approach to Combining Reputation and Contract Theory[J]. IEEE Internet Things of Journal. 2019, 6(6): 10700-10714.

[14] TANG J. Nodes Incentive Strategy Based on Bayesian Game in Ad Hoc Networks[J]. Computer Engineering, 2019, 45(8): 152-158, 164.

[15] ZHOU Q, LI P, NIE L. User Incentive Mechanism Based on Spatial-Temporal Correlation for Crowd Sensing[J]. Computer Engineering, 2021, 47(3): 227-236.

[16] YANG Q, LIU Y, CHENG Y, et al. Federated Learing[M]. Beijing: Publishing House of Electronics Industry, 2020: 11-16.

[17] GUO S T, WANG R J, ZHANG F L. Summary of Principle and Application of Blockchain[J]. Computer Science, 2021, 48(2): 271-281.

[18] YUAN Y, NI X C, ZENG S, et al. The Development Status and Prospects of Blockchain Consensus Algorithms[J]. Acta Automatica Sinica, 2018, 44(11): 2011-2022.

[19] CHENG L, WANG W G. Research on Bitcoin Mining Optimization Based on SHA256 Hash Algorithm[J]. Information Technology and Informatization, 2015, 10(1): 158-159.

[20] CHENG K W, FAN T, JIN Y L, et al. SecureBoost: A Lossless Federated Learning Framework[J]. arXiv: 1901.08755, 2021.

[21] HOU Z W, CHEN H, LI Y H. Branka Vucetic: Incentive Mechanism Design for Wireless Energy Harvesting-Based Internet of Things[J]. IEEE Internet of Things Journal, 2018, 5(4): 2620-2632.

WANG Xin, born in 1984, Ph.D, associate professor, master supervisor, is a member of China Computer Federation. His main research interests include machine learning, big data analysis and federated learning.

（责任编辑：喻藜）