一种基于合同理论的可激励联邦学习模型

王 鑫*①④⑤ 李美庆② 王黎明② 余 芸③ 杨 漾③ 孙凌云④⑤

①(浙江工业大学计算机科学与技术学院 杭州 310023)

②(西安电子科技大学计算机科学与技术学院 西安 710071)

③(南方电网数字电网研究院有限公司 广州 510663)

④(浙江大学南方电网人工智能创新联合研究中心 杭州 310058)

⑤(浙江大学计算机科学与技术学院 杭州 310058)

摘 要：针对目前较少研究去中心化联邦学习中的激励机制设计，且已有联邦学习激励机制较少以全局模型效果为出发点的现状，该文为去中心化联邦学习加入了基于合同理论的联邦学习激励机制，提出一种新的可激励的联邦学习模型。使用区块链与星际文件系统(IPFS)取代传统联邦学习的中央服务器，用于模型参数存储与分发，在此基础上使用一个合同发布者来负责合同的制定和发布，各个联邦学习参与方结合本地数据质量选择签订合同。每轮本地训练结束后合同发布者将对各个本地训练模型进行评估，若满足签订合同时约定的奖励发放条件则发放相应的奖励，同时全局模型的聚合也基于奖励结果进行模型参数的聚合。通过在MNIST数据集以及行业用电量数据集上进行实验验证，相比于传统联邦学习，加入激励机制后的联邦学习训练得到的全局模型效果更优，同时去中心化的结构也提高了联邦学习的鲁棒性。

关键词：联邦学习；激励机制；合同理论；去中心化；电力大数据

中图分类号：TP181 **文献标识码**：A **文章编号**：1009-5896(2023)03-0874-10

DOI: 10.11999/JEIT221081

An Incentivized Federated Learning Model Based on Contract Theory

WANG Xin①④⑤ LI Meiqing② WANG Liming② YU Yun③

YANG Yang③ SUN Lingyun④⑤

①(*College of Computer Science and Technology, Zhejiang University of Technology, Hangzhou* 310023, *China*)

②(*College of Computer Science and Technology, Xidian University, Xi'an* 710071, *China*)

③(*Digital Grid Research Institute Co. Ltd, China Southern Power Grid, Guangzhou* 510663, *China*)

④(*Zhejiang University-China Southern Power Grid Joint Research Centre on AI, Hangzhou* 310058, *China*)

⑤(*College of Computer Science and Technology, Zhejiang University, Hangzhou* 310058, *China*)

Abstract: In view of the fact that there is rare research on the incentive mechanism design in decentralized federated learning, and the existing incentive mechanisms for federated learning are seldom based on the global model effect, an incentive mechanism based on contract theory, is added into decentralized federated learning and a new incentivized federated learning model is proposed. A blockchain and an InterPlanetary File System (IPFS) are used to replace the central server of traditional federated learning for model parameter storage and distribution, based on which a contract publisher is responsible for contract formulation and distribution, and each federated learning participant chooses to sign a contract based on its local data quality. The contract publisher evaluates each local training model after each round of local training and issues a reward based on the agreed-upon conditions in the contract. The global model aggregation also aggregates model parameters based on the reward results. Experimental validation on the MNIST dataset and industry electricity consumption dataset show that the proposed incentivized federated learning model outperforms traditional federated learning and its decentralized structure improves its robustness.

Key words: Federated learning; Incentive mechanism; Contract theory; Decentralization; Power big data

收稿日期：2022-08-16；改回日期：2023-03-02；网络出版：2023-03-03

*通信作者： 王鑫 xinw@zjut.edu.cn

基金项目：国家重点研发计划 (2020YFB0906000, 2020YFB0906004)

Foundation Items: The National Key Research and Development Program of China(2020YFB0906000, 2020YFB0906004)

1　引言

大数据时代，数据隐私问题备受关注，然而传统的模型训练需要将数据收集到一起，这无疑增加了数据隐私泄露的风险。2016年Google提出了联邦学习这一概念[1]。然而传统联邦学习基于一个无私贡献的假设，即数据所有方都愿意无条件地参与到联邦学习训练，提供高质量的数据进行训练。而实际情况下，训练需要耗费一定的资源[2]，模型参数的传输也会产生通信开销[3,4]。在没有合理奖励情况时，理性的数据所有方将不愿意参与到联邦学习训练中。故在传统联邦学习中加入合理的激励机制十分重要。

本文选用经济学中的合同理论，合同的制定参考了Tian等人[5]的理论推导，结合区块链、星际文件系统(InterPlanetary File System, IPFS)等技术来取代传统联邦学习的中央服务器从而达到去中心化的效果，具体设计实现了一种基于合同理论的可激励联邦学习模型。本文的贡献主要有以下4点：

(1)由于参与方数据质量与训练的全局模型效果息息相关，本文在合同制定时将数据质量纳入考虑，使用了数据量和移动距离(Earth Mover's Distance, EMD)两个指标来衡量数据质量。让各个参与方获得合理的奖励基础上，基于奖励结果来聚合，提高联邦学习训练的模型效果。其中合同的制定与求解采用已有方法，数据质量的衡量是本文新的结合。

(2)多数联邦学习激励机制研究偏重于理论推导，具体模型设计实现较少，本文则设计了一个具体的可激励联邦学习模型，并完成了软件系统实现。

(3)在本文设计的面向去中心化联邦学习激励机制中基于区块链的联邦学习去中心化思想之前已有，加入IPFS与运行在区块链上的智能合约共同管理模型参数是本文创新，且未见有将基于合同理论的激励机制用于去中心化联邦学习的文献。

(4)目前采用非独立同分布(Non-Independent and Identically Distributed, Non-IID)的数据进行实验的研究工作较少，进行回归类型实验的研究工作更少[6]。本文则在Non-IID数据上进行实验，分别对分类问题与回归问题进行了全局模型训练。

2　相关工作

文献[6,7]已对现有联邦学习激励机制的研究工作进行了全面的文献综述，本节则聚焦于是否引入经济学模型、是否作用于去中心化联邦学习上2个角度对联邦学习激励机制的研究现状进行总结与分析。

文献[8]提出了一个分布式的、公平和保护隐私的深度学习(Fair and Privacy-Preserving Deep Learning, FPPDL)框架，每个参与者都会收到与其表现相匹配的不同版本的联邦学习模型，从而发现并隔离低贡献方，促进高贡献方的参与。但由于参与方会收到不同版本的联邦训练模型，可能会降低参与方的积极度。文献[9]设计了一种激励机制，参与方频繁提供更新就可以获得更多回报，而不断更新的全局模型将吸引更多参与方。但仅凭提供更新的次数来发放奖励并不可靠，这可能导致参与方为获取奖励，恶意多次提交模型参数，影响正常训练。文献[10]提出了一个深度学习框架DeepChain，这是一个具有激励机制的合作训练框架，鼓励各方共同参与深度学习模型训练，并共享训练中获取的局部梯度信息。但提出的协议需要以加密的方式选择一个节点去创建由委员会验证的块，而选择一个诚实的委员会有一定难度，而且随机算法接近于完全随机，这在实践中会有一些问题。文献[11]提出FLChain来建立一个去中心化的、公众可审计的、鲁棒的、可信任和具有激励功能的联邦生态系统，其中的激励机制可使诚实的参与方根据其贡献从全局模型中获得公平合理的收益。但其实现繁杂，贡献评估与激励策略有待细化，且系统的加解密耗费大量的时间成本。文献[12]是按照联邦学习数据参与方的贡献度对其进行奖励分配，其中贡献度由训练效果评估与训练成本相乘得到。本文则引入了合同理论，在每轮训练之前，合同发布者根据参与方制定不同类型的合同，各个参与方根据自身情况选择签订。当参与方的训练效果达到合同预定的模型标准线，即发放奖励。激励计算的整体流程与文献[12]有较大不同，特别是省去了文献[12]中每轮初始评估指标的计算。并且本文的全局模型聚合是基于奖励结果进行的，与文献[12]相比，在模型训练效果上有一定提升。

联邦学习参与方往往有着不同的目标，如收入(或效用)最大化、成本最小化和系统性能提升等。参与方之间的互动是复杂的，上述几项研究在设计联邦学习激励机制时并未将这些经济影响纳入考虑。因此联邦学习激励机制设计可考虑将经济学模型引入，例如博弈论、拍卖理论、合同理论等，目前已有一些相关研究[13]，此处不再分类阐述，接下来详细地介绍基于合同理论的激励机制研究。

合同理论是用来解决联邦学习中信息不对称问题的一种方法，目前已经有一些基于合同理论设计联邦学习激励机制的研究工作[14–23]。但这些文献在合同设计时，较少从模型训练效果角度进行设计，例如，文献[14]从耗费的时间这一个维度对服务器

成本、利润建模。文献[15–17]主要从参与方获利角度进行研究讨论。文献[18]是从计算、通信和隐私成本角度建模。文献[19]从中央服务器成本角度进行讨论。文献[20]设计合同时仅考虑了数据量大小。文献[21]设计激励机制侧重模型所有者的任务偏好，激励参与方按照偏好进行训练。文献[23]旨在考虑无人机子区域分配问题，通过最优合同的自我揭示特性，使得最优无人机与子区域有效地匹配。本文则是从更直接的模型训练效果角度，将数据质量纳入讨论，进行联邦学习激励机制设计并实现；现有的基于合同理论的联邦学习相关研究均在传统的中心化结构的联邦学习上进行，例如文献[14–23]，这些文献研究侧重激励机制设计，但忽略了联邦学习中心化结构鲁棒性差的不足，传统联邦学习的中央服务器瘫痪则影响整个联邦学习过程，训练参数也面临丢失的风险。本文则在去中心化的联邦学习结构基础上将基于合同理论的激励机制加入，实现了一个可激励的联邦学习模型，在不影响激励过程的前提下，也提升了传统联邦学习的鲁棒性；现有相关研究实验部分大多对分类问题进行讨论，例如文献[14,18,20,22]。一些研究对实验问题类型没有提及，例如文献[15–17,19,21,23]，其中文献[16,17,19,21,23]的实验部分为仿真实验，而且并非所有研究实验部分均采用了Non-IID数据，例如文献[20]。

以上研究是在传统中心化结构的联邦学习上进行激励机制设计的，目前也有将激励机制与去中心化联邦学习结合的研究，文献[6]搜集并筛选出40篇将激励机制与去中心化联邦学习结合的现有文献，并对这些研究进行了分析。但其中未见基于合同理论设计激励机制并与去中心化联邦学习结合的研究。而且在所综述的研究中，实验部分采用Non-IID数据的研究数目较少，进行回归问题实验的研究更少。本文研究将基于合同理论的激励机制与去中心化联邦学习结构结合，实现了一个可激励的联邦学习模型，同时实验部分使用Non-IID数据，分别在分类问题和回归问题上进行了实验。

3 基于合同理论的可激励联邦学习模型

3.1 合同理论

合同理论是一门以合同为核心，以博弈论为方法，研究激励、信息和经济制度的正式理论[24]。合同理论将机制设计作为主要研究特色，具体研究委托代理关系中的信息和激励问题。为便于理解，以雇员雇主这类常见的委托代理关系为例。合同理论主要研究雇员与雇主之间的互动。当员工努力投入工作，其绩效会有所提高，雇主也更加满意[24]。

在合同理论中，通过设计包含有所需绩效与对应奖励的合同来有效激励员工[25]。设计合同时，目标是最大化雇主的收益或效用。通常，表示出雇主收益或效用的目标函数，在两个约束之下，最大化该目标函数，进而求得合同解。其中这两个约束分别是个体理性(Individual Rationality, IR)和激励相容性(Incentive Compatibility, IC)。IR即雇员有积极性选择签订合同来获取报酬；IC即雇员在选择签订某种合同时的预期报酬(或效用)大于等于选择签订其他类型合同的预期报酬(或效用)。在联邦学习中，类似于雇主的委托人为全局模型训练者，类似于雇员的代理人为各联邦学习参与方。

3.2 基于合同理论的激励机制

联邦学习中，各个参与方本地的数据质量是不同的，本文基于合同理论为参与方制定不同类型的合同，合同中说明了奖励数目，获得奖励的条件是本地训练的模型效果达到合同预设的标准。不同类型的合同奖励数目与获得奖励的条件均不同，获奖励条件越高，奖励数目越大。各个参与方在联邦学习每轮开始时根据自身数据质量等情况量力而行，选择合适类型的合同进行签订。

合同的制定参考了文献[5]中的方法，文献[5]从提升全局模型效果角度进行合同设计，引入数据质量与计算工作量，详细叙述如下：对于联邦学习的若干个参与方，数据质量类型按照升序排列为$\theta_1 \le \cdots \le \theta_i \le \cdots \le \theta_n$。对于每一轮联邦学习，制定一个合同集$\Phi = \{\phi_i = (f_i, R_i) | i \in \{1,2,\cdots,n\}\}$，合同集中包含为$n$类参与方制定的$n$个合同，每一个合同中的$f$是参与方签订合同需缴纳的注册费(不予退回)，$R$是参与方可获得的奖励，当参与方本地训练模型的测试效果满足合同预设的标准M_i时，可获得该奖励，否则，奖励不能获得。参与方的效用为$U_i = \theta_i e_i R_i - f_i - (c/2){e_i}^2$，其中$e_i$为第$i$类参与方的训练意愿，$c$代表给定训练任务环境中的单位成本；全局的效用为$U_s = \sum_{i=1}^{n} \beta_i (f_i + \theta_i e_i (G(M_i) - R_i))$，其中，参与方的类型分布为$\{\beta_i\}, i \in \{1,2,\cdots,n\}$，$\sum_{i=1}^{n} \beta_i = 1$，$G(M_i)$代表类型为$i$的参与方上传本地模型给全局带来的收入。合同的优化问题可以表示为

$$\left.\begin{aligned} &\max \sum_{i=1}^{n} \beta_i (f_i + \theta_i e_i (G(M_i) - R_i)) \\ &\text{s.t.} \\ &(\text{IR}) U_i = \theta_i e_i R_i - f_i - \frac{c}{2} {e_i}^2 \ge 0 \\ &(\text{IC}) \theta_i e_i R_i - f_i - \frac{c}{2} {e_i}^2 \ge \theta_i e_i^j R_j - f_j - \frac{c}{2} (e_i^j)^2, \\ &\forall j \ne i, i, j \in \{1,2,\cdots,n\} \end{aligned}\right\} \tag{1}$$

其中，e_i^j表示数据质量类型为θ_i的参与方选择合同(f_j, R_j)后的联邦学习努力程度。

第1个约束为IR，即保证每一个参与方的效用非负，第2个约束为IC，即确保每一个参与方选择与自己相符的合同类型来实现效用最大，也即选择其他合同类型没有选择与自己相符的合同类型达到的效用高。

根据文献[5]中的推导，得出最优的合同解为

$$\begin{aligned} &R_i = G(M_i), \forall i \in \{1,2,\cdots,n\} \\ &f_1 = \frac{1}{2c}(\theta_1 R_1)^2 \\ &f_i = \frac{1}{2c}(\theta_i R_i)^2 - \frac{1}{2c}(\theta_i R_{i-1})^2 + f_{i-1}, \forall i \in \{2,3,\cdots,n\} \end{aligned} \tag{2}$$

参与联邦学习的若干个参与方，数据质量类型已按升序排列：$\theta_1 \le \cdots \le \theta_i \le \cdots \le \theta_n$。参与方$i$拥有的数据质量越好，上传本地模型给全局带来的收入$G(M)$越大。从最优合同解式(2)可以看出，当$G(M)$越大时，合同中对应的奖励设置$R$也增大，即有$R_i > R_{i-1}(i \in \{2,3,\cdots,n\})$，那么$f_i > f_{i-1}(i \in \{2,3,\cdots,n\})$；当合同中奖励$R$越大时，与之对应的注册费$f$也会增加，结合实际情况解释是：若参与方签订具有较高奖励的合同，当本地模型训练效果未达到发放奖励的条件，按照约定注册费不予退回时，注册费较高符合激励相容约束。

其中数据质量θ如何计算文献[5]并未提及，可根据具体的应用场景进行衡量。如本文实验部分的基于MNIST数据集的分类实验，采用与数据量大小成正比的方法衡量各个参与方数据质量；本文的基于行业用电量数据的回归实验，引入了EMD这一指标，EMD表示各个参与方数据与全局数据的分布差异程度，某个参与方的 EMD值越小代表参与方与整体数据偏移程度越小，那么该参与方数据质量越好，故使用1减去某参与方的EMD值(每个参与方的EMD值已进行线性归一化)表示该参与方的数据质量。数据质量可看作联邦学习开始前各个参与方自主计算并自主报告的，因为合同的设计计算需要依据数据质量，而参与方只有选择为其设计的合同类型才能保证获利最大，因此各个参与方没有必要瞒报数据质量。

3.3　可激励联邦学习模型

传统的联邦学习为中心化结构，所有参与方将本地训练的模型参数上传到中央服务器，由中央服务器完成模型参数的聚合与全局模型参数(聚合后的模型参数)的下发。当中央服务器发生故障时，整个联邦学习过程便会瘫痪，中央服务器中的模型参数也可能面临丢失，鲁棒性较差。本文结合区块链、智能合约、IPFS等设计实现了一个去中心化的联邦学习框架，在此基础上，将基于合同理论的激励机制加入到去中心化联邦学习中，形成本文所述的基于合同理论的可激励联邦学习模型。尽管已经有一些在去中心化联邦学习上的激励机制的研究工作，但尚未见有研究在去中心化联邦学习上加入基于合同理论的激励机制。接下来将详细阐述基于合同理论的可激励联邦学习模型。

首先将区块链、IPFS等与联邦学习结合，取代传统联邦学习的中央服务器，进而实现去中心化的联邦学习。模型参数由区块链上的智能合约与IPFS进行管理，各个参与方在本地完成模型参数聚合，以此替换掉传统联邦学习的中央服务器，实现去中心化。基于上述去中心化联邦学习，将激励机制与之结合，引入一个合同发布者，负责每轮联邦学习的合同制定、合同发布、评估各个参与方本地训练模型效果、发放奖励等。具体地，合同发布者根据3.2中的合同最优解结合参与方的数据质量情况计算制定该轮合同集，记录到智能合约中。各个参与方根据自身数据质量来选择尽可能使自己获得奖励的合同类型，缴纳合同中约定的注册费，进行签订，签订情况将记录到智能合约。合同选择签订完成后，各个参与方在本地开始训练，训练后的模型参数由IPFS与运行在区块链上的智能合约进行管理。当所有参与方本地模型参数都上传后，合同发布者获取这些模型参数，利用测试集对各个参与方本地训练模型进行测试，测试完成后，合同发布者从智能合约获取各个参与方签订的合同类型，对比签订合同中奖励发放的预设标准，给通过本地模型测试达到标准的参与方发放所签订合同约定的奖励，记录到智能合约。各个参与方获取所有参与方上传的模型参数，根据每个参与方所获奖励占总奖励数目的比例对各个模型参数进行聚合。如此多次迭代，完成全局模型训练。

为了直观地展示基于合同理论的可激励联邦学习模型训练步骤，绘制了如图1的步骤图：

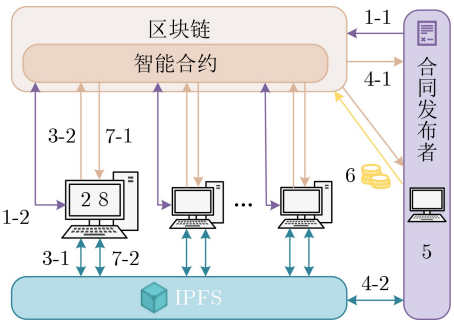

图 1 基于合同理论的可激励联邦学习模型训练步骤图

步骤1-1　合同发布者发布设计的合同集；步骤1-2　不同参与方根据自身情况选择签订合同；

步骤2　参与方本地训练；

步骤3-1　上传模型参数并接收IPFS返回的Hash值；步骤3-2　将模型参数文件Hash值记录到合约；

步骤4-1　合同发布者从智能合约收集Hash值；步骤4-2　通过Hash值从IPFS下载各个模型参数文件；

步骤5　利用测试集对参与方的本地训练模型进行测试；

步骤6　获取签订合同情况，给模型效果达到合同预设标准的参与方发放奖励，记录到智能合约；

步骤7-1　获取多个参与方上传的Hash值；步骤7-2　通过Hash值从IPFS下载多个参与方模型参数；

步骤8　本地完成模型参数聚合；

步骤9　多次重复上述步骤，直至完成全局模型训练。

3.4 可激励联邦学习模型的举例阐述

以电网场景下行业用电量预测为例，选定某个行业(如餐饮行业)，利用现有的多个地区餐饮行业用户的用电量数据进行训练，使用训练模型预测该行业的新加入用户用电情况。该行业不同地区的用户用电量数据可能分布在多个子公司的电力计量系统中，这些用电量数据将参与联邦学习。基于本文模型进行联邦学习，得到最终的全局模型。为方便理解，现假定有3个子公司参与联邦学习。

具体步骤为步骤1-1，合同发布者根据各个子公司(参与方)所拥有的用户用电量数据质量(例如$\theta_1=0.718,\theta_2=0.786,\theta_3=0.794$)为其制定奖励发放的模型标准线以及不同类型的合同，奖励发放的模型标准线定为$M_1=0.038\ 9, M_2=0.039\ 3, M_3=0.039\ 7$，多种类型合同的计算使用2.2节的式(2)最优合同解(计算时$R_i=4\ 000{M_i}^2$, $c=50$)，计算可得合同集为$\Phi=\{(0.221\ 7,6.052\ 8),(0.231\ 2,6.178),(0.241\ 1,6.304\ 4)\}$。合同发布者将合同集与模型标准线等信息保存到智能合约中。步骤1-2，各个参与方根据自身情况选择签订某种合同(合同制定时满足IC，即每个参与方为了效用达到最大会选择与自己相符的合同类型)，例如参与方1选择合同1 (0.221 7, 6.052 8)，参与方2选择合同2 (0.231 2,6.178)等。步骤2，接着各个参与方开始本地训练。步骤3，本地训练的模型参数将由IPFS与智能合约管理。步骤4，所有参与方上传本地模型参数后，合同发布者从IPFS和智能合约获取各个参与方本地训练的模型参数。步骤5，合同发布者利用测试集对各个参与方本地模型进行测试，例如3个参与方的模型效果分别为0.25, 0.27, 0.31。步骤6，合同发布者为模型效果达到合同预设标准的参与方发放奖励，记录到智能合约。此例中3个参与方模型效果均达到所签订合同预定的标准线，分别可获得对应合同中约定的奖励6.052 8, 6.178, 6.304 4。步骤7，最后各个参与方获取多个参与方上传的本地模型参数。步骤8，按照奖励比例(各个参与方所获奖励占总奖励数目的比值)完成模型参数聚合。步骤9，如此多次重复上述步骤，直至完成全局模型的训练。使用训练得到的全局模型，即可预测餐饮行业新加入的用户未来一段时间的用电量趋势。

4 实验与分析

4.1 可激励联邦学习模型的具体实现

具体的技术选型如下：

智能合约：使用Solidity语言编写智能合约，Truffle作为智能合约的开发工具；

区块链：Ganache搭建本地以太坊区块链，用于智能合约的部署与测试；

IPFS：用于模型参数文件的存储；

Python与IPFS交互：使用ipfshttpclient库便于完成参与方与IPFS交互(模型参数文件的上传与下载)；

Python与智能合约交互：使用web3py库完成参与方与智能合约的交互；

模型训练：使用PyTorch框架编写。

利用上述技术选型，实现了上述可激励联邦学习模型，代码链接为https://github.com/yeliauk/DMFL。

4.2 基于MNIST数据集的实验

MNIST数据集中包含0-9的手写数字图像，其中训练集共有60 000张图像和标签，测试集共有10 000张图像和标签。将训练集分为若干部分，用来模拟多个参与方，每个参与方拥有若干张图像和标签，各个参与方的数据分布为Non-IID；合同发布者拥有测试集的10 000张图像和标签，用于评估各个参与方本地训练模型，并将评估得到的各个参与方本地模型准确率与对应预设的准确率标准线进行对比，为通过测试的参与方发放对应的合同奖励。设置了3组实验，所有实验的全局训练轮数为5，参与方epoch为1，batch size为32，学习率为0.01。各组实验的参与方数据设置情况如表1所示。根据最优合同解计算设计的合同情况如表2所示，其中数据质量根据数据数量大小衡量(数据质量与数据数量成正比，此处比例系数设为0.000 1)。

表 1　MNIST数据各组实验参与方数据设置情况表

实验编号	参与方数目	数据不均匀比例	数据数量
1	9	0.8	[1500, 2000, 2500, 3500, 5000, 7000, 9500, 13000, 16000]
2	10	0.8	[1000, 1500, 2000, 2500, 3500, 5000, 6500, 8500, 12000, 17500]
3	10	0.9	[1000, 1500, 2000, 2500, 3500, 5000, 6500, 8500, 12000, 17500]

表 2　MNIST数据各组实验合同设置情况表

实验编号	合同数目	参与方数据质量	模型准确率标准线	合同注册费	合同奖励
1	9	[0.1500, 0.2000, 0.2500, 0.3500, 0.5000, 0.7000, 0.9500, 1.3000, 1.6000]	[0.0075, 0.0100, 0.0125, 0.0175, 0.0250, 0.0350, 0.0475, 0.0650, 0.0800]	[0.00001, 0.00006, 0.00020, 0.00156, 0.01343, 0.10045, 0.61885, 4.06914, 13.53474]	[0.2250, 0.4000, 0.6250, 1.2250, 2.5000, 4.9000, 9.0250, 16.9000, 25.6000]
2	10	[0.1000, 0.1500, 0.2000, 0.2500, 0.3500, 0.5000, 0.6500, 0.8500, 1.2000, 1.7500]	[0.0050, 0.0075, 0.0100, 0.0125, 0.0175, 0.0250, 0.0325, 0.0425, 0.0600, 0.0875]	[0.000001, 0.00001, 0.00005, 0.00019, 0.00155, 0.01342, 0.06243, 0.31061, 2.54491, 24.91741]	[0.1000, 0.2250, 0.4000, 0.6250, 1.2250, 2.5000, 4.2250, 7.2250, 14.4000, 30.6250]
3	10	[0.1000, 0.1500, 0.2000, 0.2500, 0.3500, 0.5000, 0.6500, 0.8500, 1.2000, 1.7500]	[0.0050, 0.0075, 0.0100, 0.0125, 0.0175, 0.0250, 0.0325, 0.0425, 0.0600, 0.0875]	[0.000001, 0.00001, 0.00005, 0.00019, 0.00155, 0.01342, 0.06243, 0.31061, 2.54491, 24.91741]	[0.1000, 0.2250, 0.4000, 0.6250, 1.2250, 2.5000, 4.2250, 7.2250, 14.4000, 30.6250]

为了得知参与方选择不同类型合同时参与方效用的大小情况，以及参与方数目对全局效用大小的影响。首先计算了每组实验各个参与方选择不同类型合同时的参与方效用，为了清晰地展示，选取第2组实验以折线图的形式绘制了参与方选取不同类型合同时的参与方效用(为避免参与方数目过多造成的图中折线混杂，选择性地展示了参与方1, 3, 5, 7, 9的效用)，如图2所示。同时在各个参与方均选择为其设计的合同类型前提下，计算了参与方数目不同时的全局效用，并用柱形图展示，如图3所示。

从图2可以看出，当参与方选择为其设计的合同类型时，如参与方3选择签订类型3的合同，参与方效用达到最高，即满足激励相容性，且此时参与方效用均非负，即满足个体理性。从图3可以看出，当每个参与方均选择为其设计的合同类型时，参与方数目越大，全局的效用越高。

为了显示本文可激励模型对联邦学习全局模型训练效果的提升情况，上述每组实验分别使用本文可激励的联邦学习模型(使用奖励比例聚合)与传统联邦学习方法(聚合算法为FedAvg[1], FedProx[26], SCAFFOLD[27])进行全局模型的训练，对比全局模型准确率，结果如表3所示。

从实验结果可以看出，使用本文的基于合同理论的可激励联邦学习模型可训练得到全局模型，且全局模型的准确率相比于使用传统联邦学习训练得到的全局模型准确率更高，模型效果有一定提升。尤其是当参与方数据质量相差较大时，例如实验3，各个参与方的数字分布极不均匀，数据数量较多的参与方数据质量较好。本实验的数据质量按照与数据数量成正比的关系来衡量，使用本文可激励联邦学习模型训练得到的全局模型效果较为理想。但数据量不是衡量数据质量的唯一标准，衡量数据质量的标准要具体情况具体分析。例如针对MNIST数据集而言，数据质量取决于数据量大小，但是换做其他数据集，数据质量可能就需要增加更多指标

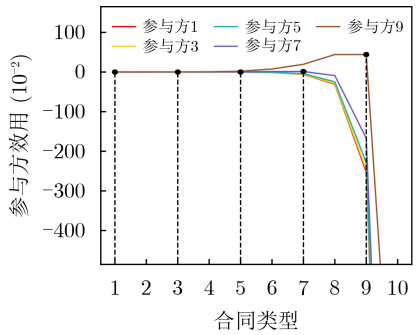

图 2 基于MNIST数据集实验参与方效用展示图

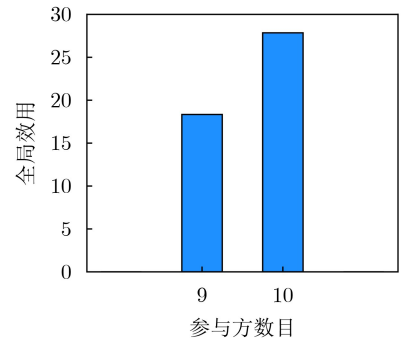

图 3 基于MNIST数据集实验全局效用展示图

项，如覆盖率、信噪比等。然而需要注意的是，本文研究模型只是考量将数据质量作为一个总体指标纳入对模型效果的影响，至于影响数据质量有哪些具体分项指标则不是本文研究重点。使用本文可激励的联邦学习模型，基于奖励比例进行聚合，得到的全局模型效果相较于传统联邦学习方法有了一定的提升。

4.3 基于行业用电量数据的实验

本小节实验数据采用南方电网采集的广州市不同行业不同地区用户的每日用电量数据，时间跨度为2017.1.1-2018.12.10。实验选取行业代码为IC1811的用电量数据，从中选取若干个用户模拟多个参与方，其中每个用户前80%时间段的用电量数据作为参与方的本地训练数据；选取一个用户的用电量数据，将其后20%时间段的数据作为合同发布者用于评估模型的测试数据，即可看作预测该行业未来一段时间的用电量，采用均方根误差(Root Mean Square Error, RMSE)作为模型效果评估的指标，根据评估得到的各个参与方本地模型RMSE与对应合同预设的标准线对比，为通过测试(1-RMSE值大于预设标准线)的参与方发放对应的合同奖励。设置了3组实验，所有实验的全局训练轮数为50，参与方epoch为4，batch size为32，学习率为0.01。每组设置不同的参与方数目，根据最优合同解计算设计的合同情况如表4所示，其中数据质量衡量方法如下：使用EMD表示各个参与方数据与全局数据的分布差异程度，记为d_i，EMD越小，参与方与整体数据偏移程度越小，那么该参与方数据质量越好，故使用$1-d_i$(d_i已进行线性归一化)表示数据质量θ_i。

同4.2节基于MNIST数据集的实验，为了得知参与方选择不同类型合同时参与方效用的大小情况，以及参与方数目对全局效用大小的影响。首先计算得到每组实验各个参与方选择不同类型合同时的参与方效用。为了清晰地展示，选取第1组实验以折线图的形式绘制了参与方选取不同类型合同时的参与方效用(为避免图中折线混杂，选择性地展示参与方1, 3, 5, 7, 9的效用)，如图4所示。同时在各个参与方均选择为其设计的合同类型前提下，计算了参与方数目不同时的全局效用，并用柱形图展示，如图5所示。

从图4、图5可看出同4.2节的结论：当参与方选择为其设计的合同类型时，参与方效用达到最高，即满足激励相容性，且此时参与方效用均非负，即满足个体理性。当每个参与方均选择为其设计的合同类型时，参与方数目越大，全局的效用越高。

为了显示本文模型对联邦学习全局模型训练效果的提升情况，上述每组实验分别使用本文可激励的联邦学习模型(使用奖励比例聚合)与传统联邦学习方法(聚合算法为FedAvg, FedProx, SCAFFOLD)进行全局模型的训练，对比全局模型的RMSE，结果如表5所示。

从实验结果可以看出，使用本文的基于合同理论的可激励联邦学习模型可训练得到全局模型，且

表 3 MNIST数据各组实验结果对照表

实验编号	传统联邦学习(FedAvg聚合)全局模型准确率	传统联邦学习(FedProx聚合)全局模型准确率	传统联邦学习(SCAFFOLD聚合)全局模型准确率	本文可激励联邦学习(奖励比例聚合)全局模型准确率
1	0.8945	0.8958	0.8971	0.9031
2	0.8933	0.8961	0.8973	0.9003
3	0.7790	0.7831 0.7905	0.7905	0.8022

表 4 行业用电量数据各组实验合同设置情况表

实验编号	合同数目	参与方数据质量	模型测试标准线	合同注册费	合同奖励
1	9	[0.7766, 0.7855, 0.7944, 0.8055, 0.8251, 0.8757, 0.8967, 0.9297, 0.9386]	[0.0388, 0.0393, 0.0397, 0.0403, 0.0413, 0.0438, 0.0448, 0.0465, 0.0469]	[0.2187, 0.2305, 0.2405, 0.2564, 0.2860, 0.3806, 0.4253, 0.5148, 0.5378]	[6.0218, 6.1780, 6.3044, 6.4964, 6.8228, 7.6738, 8.0282, 8.6490, 8.7984]
2	50	[0.5074, 0.5076, 0.5206, 0.6992, 0.7312, 0.7550, 0.7812, 0.8709, 0.8723, 0.8750, ···]	[0.0254, 0.0254, 0.0260, 0.0350, 0.0366, 0.0378, 0.0391, 0.0435, 0.0436, 0.0438, ···]	[0.0171, 0.0171, 0.0189, 0.1005, 0.1256, 0.1481, 0.1770, 0.3279, 0.3319, 0.3401, ···]	[2.5806, 2.5806, 2.7040, 4.9000, 5.3582, 5.7154, 6.1152, 7.5690, 7.6038, 7.6738, ···]
3	100	[0.5460, 0.5460, 0.6424, 0.7820, 0.7881, 0.8711, 0.8749, 0.8860, 0.8971, 0.9042, ···]	[0.0273, 0.0273, 0.0321, 0.0391, 0.0394, 0.0436, 0.0437, 0.0443, 0.0449, 0.0452, ···]	[0.0265, 0.0265, 0.0599, 0.1847, 0.1919, 0.3381, 0.3422, 0.3679, 0.3953, 0.4097, ···]	[2.9812, 2.9812, 4.1216, 6.1152, 6.2094, 7.6038, 7.6388, 7.8500, 8.0640, 8.1722, ···]

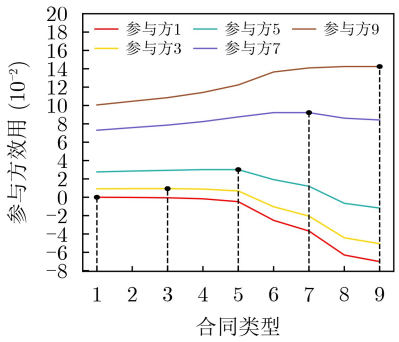

图 4 基于行业用电量数据实验参与方效用展示图

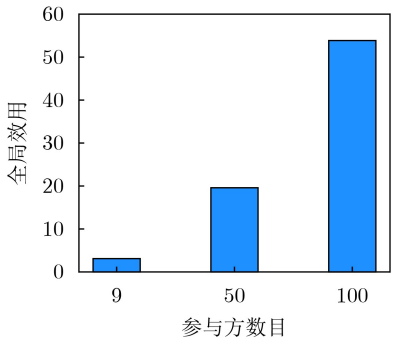

图 5 基于行业用电量数据实验全局效用展示图

表 5　行业用电量数据各组实验设置与结果对照表

实验编号	参与方数目	传统联邦学习(FedAvg聚合)全局模型RMSE	传统联邦学习(FedProx聚合)全局模型RMSE	传统联邦学习(SCAFFOLD聚合)全局模型RMSE	本文可激励联邦学习(奖励比例聚合)全局模型RMSE
1	9	0.143608	0.140512	0.139842	0.135423
2	50	0.135517	0.135411	0.135375	0.135252
3	100	0.135652	0.135508	0.135419	0.135396

全局模型的RMSE相比于使用传统联邦学习(聚合算法为FedAvg)训练得到的全局模型的RMSE更小，模型效果得到提升。可以发现，参与方数目较多时(如实验3，参与方数目为100时)，奖励比例聚合得到的全局模型RMSE与FedAvg方法聚合得到的全局模型RMSE相近。其原因为当参与方数目较大时，其中会有一些数据质量较差的参与方，而本文可激励联邦学习模型会为所有参与方制定合同，这些数据质量较差的参与方本地训练模型通过测试获得的奖励较少，即使这些模型参数在聚合过程中被采纳的权重较小，但仍占据一定比例。同时，参与方数目较大时，使用上述两种聚合方法聚合各个参与方模型参数时，分配给每个参与方的聚合权重都较小，这样对于某个参与方，两种聚合方法为其分配的聚合权重相差很小，最终两种聚合方法得到的全局模型效果相近。这就是当参与方数目较多时，使用本文的基于合同理论的可激励联邦学习模型训练得到的全局模型相较于使用传统联邦学习(聚合算法为FedAvg)训练得到的全局模型，效果有提升，但提升有限的原因。

4.4　实验总结

首先介绍了本文基于合同理论的可激励联邦学习模型的具体实现各模块的技术选型。接着分别使用MNIST数据集和行业用电量数据集进行实验，基于本文的基于合同理论的可激励联邦学习模型进行训练，各个参与方每轮达到签订合同约定的目标时可得到相应奖励，最终训练得到的全局模型在测试集上的表现均好于传统联邦学习方法训练得到的全局模型。尤其是当参与方的数据质量相差较大时，本文可激励联邦学习模型训练得到的全局模型相较于传统联邦学习方法效果提升较明显。当参与方数目较多时，提升效果有一定局限，但最终全局模型表现仍较好，未来可对该点进一步优化。因此，使用本文的基于合同理论的可激励联邦学习模型可训练得到全局模型，各个参与方能得到签订合同约定的与自身数据质量相匹配的奖励，且最终全局模型效果优于传统联邦学习方法训练得到的全局模型效果。

5　结束语

针对目前较少在去中心化联邦学习上研究激励机制设计且已有联邦学习激励机制较少以全局模型效果为出发点的现状，本文提出了一种基于合同理论的可激励联邦学习模型，在去中心化联邦学习结构基础上引入基于合同理论的激励机制，合同发布者为联邦学习参与方制定合同，合同的制定需满足IR与IC。各联邦学习参与方选择签订合同发布者发放的合同，并开始联邦学习训练，当各参与方本地模型满足合同预设的条件时，即可得到合同约定的奖励，且每轮全局模型参数的聚合使用每个参与方的奖励比例作为每个参与方模型参数的权重。通过在两个数据集上进行实验，结果表明本文基于合同理论的可激励联邦学习模型能完成全局模型训练任务，各个参与方可得到相应的奖励，与传统联邦学习方法相比，本文方法得到的全局模型效果更优。

参 考 文 献

[1]　MCMAHAN H B, MOORE E, RAMAGE D, *et al*.

Communication-efficient learning of deep networks from decentralized data[C]. The 20th International Conference on Artificial Intelligence and Statistics, Fort Lauderdale, USA, 2017: 1273–1282.

[2] TRAN N H, BAO Wei, ZOMAYA A, *et al*. Federated learning over wireless networks: Optimization model design and analysis[C]. IEEE INFOCOM 2019 - IEEE Conference on Computer Communications, Paris, France, 2019: 1387–1395. doi: 10.1109/INFOCOM.2019.8737464.

[3] YAN Zhigang, LI Dong, YU Xianhua, *et al*. Latency-efficient wireless federated learning with quantization and scheduling[J]. *IEEE Communications Letters*, 2022, 26(11): 2621–2625. doi: 10.1109/LCOMM.2022.3199490.

[4] KONEČNÝ J, MCMAHAN H B, YU F X, *et al*. Federated learning: Strategies for improving communication efficiency[EB/OL]. https://arxiv.org/abs/1610.05492, 2017.

[5] TIAN Mengmeng, CHEN Yuxin, LIU Yuan, *et al*. A contract theory based incentive mechanism for federated learning[C/OL]. International Workshop on Federated and Transfer Learning for Data Sparsity and Confidentiality in Conjunction with IJCAI 2021 (FTL-IJCAI'21), 2021.

[6] WITT L, HEYER M, TOYODA K, *et al*. Decentral and incentivized federated learning frameworks: A systematic literature review[J]. *IEEE Internet of Things Journal*, 2023, 10(4): 3642–3663. doi: 10.1109/JIOT.2022.3231363.

[7] ZHAN Yufeng, ZHANG Jie, HONG Zicong, *et al*. A survey of incentive mechanism design for federated learning[J]. *IEEE Transactions on Emerging Topics in Computing*, 2022, 10(2): 1035–1044. doi: 10.1109/TETC.2021.3063517.

[8] LYU Lingjuan, YU Jiangshan, NANDAKUMAR K, *et al*. Towards fair and privacy-preserving federated deep models[J]. *IEEE Transactions on Parallel and Distributed Systems*, 2020, 31(11): 2524–2541. doi: 10.1109/TPDS.2020.2996273.

[9] LI Yuzheng, CHEN Chuan, LIU Nan, *et al*. A blockchain-based decentralized federated learning framework with committee consensus[J]. *IEEE Network*, 2021, 35(1): 234–241. doi: 10.1109/MNET.011.2000263.

[10] WENG Jiasi, WENG Jian, ZHANG Jilian, *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. doi: 10.1109/TDSC.2019.2952332.

[11] BAO Xianglin, SU Cheng, XIONG Yan, *et al*. FLChain: A blockchain for auditable federated learning with trust and incentive[C]. 2019 5th International Conference on Big Data Computing and Communications (BIGCOM), Qingdao, China, 2019: 151–159. doi: 10.1109/BIGCOM.2019.00030.

[12] 王鑫, 周泽宝, 余芸, 等. 一种面向电能量数据的联邦学习可靠性激励机制[J]. 计算机科学, 2022, 49(3): 31–38. doi: 10.11896/jsjkx.210700195.

WANG Xin, ZHOU Zebao, YU Yun, *et al*. Reliable incentive mechanism for federated learning of electric metering data[J]. *Computer Science*, 2022, 49(3): 31–38. doi: 10.11896/jsjkx.210700195.

[13] TU Xuezhen, ZHU Kun, LUONG N C, *et al*. Incentive mechanisms for federated learning: From economic and game theoretic perspective[J]. *IEEE Transactions on Cognitive Communications and Networking*, 2022, 8(3): 1566–1593. doi: 10.1109/TCCN.2022.3177522.

[14] KANG Jiawen, XIONG Zehui, 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): 10700–10714. doi: 10.1109/JIOT.2019.2940820.

[15] LIM W Y B, XIONG Zehui, MIAO Chunyan, *et al*. Hierarchical incentive mechanism design for federated machine learning in mobile networks[J]. *IEEE Internet of Things Journal*, 2020, 7(10): 9575–9588. doi: 10.1109/JIOT.2020.2985694.

[16] LIM W Y B, GARG S, XIONG Zehui, *et al*. Dynamic contract design for federated learning in smart healthcare applications[J]. *IEEE Internet of Things Journal*, 2021, 8(23): 16853–16862. doi: 10.1109/JIOT.2020.3033806.

[17] LE T H T, TRAN N H, TUN Y K, *et al*. An incentive mechanism for federated learning in wireless cellular networks: An auction approach[J]. *IEEE Transactions on Wireless Communications*, 2021, 20(8): 4874–4887. doi: 10.1109/TWC.2021.3062708.

[18] WU Maoqiang, YE Dongdong, DING Jiahao, *et al*. Incentivizing differentially private federated learning: A multidimensional contract approach[J]. *IEEE Internet of Things Journal*, 2021, 8(13): 10639–10651. doi: 10.1109/JIOT.2021.3050163.

[19] DING Ningning, FANG Zhixuan, and HUANG Jianwei. Optimal contract design for efficient federated learning with multi-dimensional private information[J]. *IEEE Journal on Selected Areas in Communications*, 2021, 39(1): 186–200. doi: 10.1109/JSAC.2020.3036944.

[20] WANG Yuntao, SU Zhou, LUAN T H, *et al*. Federated learning with fair incentives and robust aggregation for UAV-aided crowdsensing[J]. *IEEE Transactions on Network Science and Engineering*, 2022, 9(5): 3179–3196. doi: 10.1109/TNSE.2021.3138928.

[21] LIM W Y B, XIONG Zehui, KANG Jiawen, *et al*. When information freshness meets service latency in federated learning: A task-aware incentive scheme for smart industries[J]. *IEEE Transactions on Industrial Informatics*,

2022, 18(1): 457–466. doi: 10.1109/TII.2020.3046028.

[22] YE Dongdong, HUANG Xumin, WU Yuan, *et al*. Incentivizing semisupervised vehicular federated learning: A multidimensional contract approach with bounded rationality[J]. *IEEE Internet of Things Journal*, 2022, 9(19): 18573–18588. doi: 10.1109/JIOT.2022.3161551.

[23] LIM W Y B, HUANG Jianqiang, XIONG Zehui, *et al*. Towards federated learning in UAV-enabled internet of vehicles: A multi-dimensional contract-matching approach[J]. *IEEE Transactions on Intelligent Transportation Systems*, 2021, 22(8): 5140–5154. doi: 10.1109/TITS.2021.3056341.

[24] 帕特里克·博尔顿, 马赛厄斯·德瓦特里庞, 费方域, 蒋士成, 郑育家, 等译. 合同理论[M]. 上海: 格致出版社, 2008: 1–6.
BOLTON P, DEWATRIPONT M, FEI Fangyu, JIANG Shicheng, ZHENG Yujia, *et al*. translation. Contract Theory[M]. Shanghai: Truth & Wisdom Press, 2008: 1–6.

[25] ZHANG Yanru, PAN Miao, SONG Lingyang, *et al*. A survey of contract theory-based incentive mechanism design in wireless networks[J]. *IEEE Wireless Communications*, 2017, 24(3): 80–85. doi: 10.1109/MWC.2017.1500371WC.

[26] LI Tian, SAHU A K, ZAHEER M, *et al*. Federated optimization in heterogeneous networks[C]. Machine Learning and Systems 2, Austin, USA, 2020: 429–450.

[27] KARIMIREDDY S P, KALE S, MOHRI M, *et al*. SCAFFOLD: Stochastic controlled averaging for federated learning[C/OL]. The 37th International Conference on Machine Learning, 2020: 5132–5143.

王　鑫：男，副教授，硕士生导师，研究方向为数字孪生、智能电网、联邦学习等.

李美庆：女，硕士生，研究方向为联邦学习、智能电网等.

王黎明：男，副教授，研究方向为人工智能机器诊疗技术、工业智能视觉检测、航天系统软件关键技术.

余　芸：女，硕士，副高级工程师，研究方向为数字电网信息系统软件架构.

杨　漾：女，博士，高级经理，研究方向为数字电网信息系统软件架构.

孙凌云：男，博士，教授，博士生导师，研究方向为人工智能、设计智能、信息与交互设计.

责任编辑：马秀强