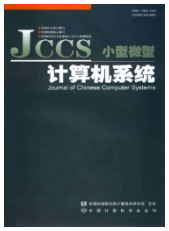

小型微型计算机系统
Journal of Chinese Computer Systems
ISSN 1000-1220,CN 21-1106/TP

《小型微型计算机系统》网络首发论文

题目：面向联邦学习激励优化的演化博弈模型
作者：孙跃杰，赵国生，廖祎玮
收稿日期：2022-09-16
网络首发日期：2023-02-07
引用格式：孙跃杰，赵国生，廖祎玮．面向联邦学习激励优化的演化博弈模型[J/OL]．小型微型计算机系统.
https://kns.cnki.net/kcms/detail//21.1106.TP.20230206.1826.009.html

面向联邦学习激励优化的演化博弈模型

孙跃杰[1]，赵国生[1]✉，廖祎玮[1]

（1 哈尔滨师范大学 计算机科学与信息工程学院 ，哈尔滨 150025）

E-mail：1021420440@qq.com

摘 要：针对联邦学习中参与者虚报训练成本导致激励不匹配的现象，提出了面向联邦学习激励优化的演化博弈模型。首先在联邦学习系统中建立了联邦参与者-联邦组织者演化博弈模型，设计模型质量评估算法对参与者提交的模型进行质量评估，去除低质量模型的同时量化参与者训练成本。然后结合信誉度指标提出优化的激励分配方法，通过求解演化博弈的稳定策略得到不同初始状态下的最优收益策略。最后仿真实验表明参与者激励收益方面，与平均分配法和个体收益分享法相比诚实参与者的收益提升了 70%和 57.4%，虚报参与者收益降低了 65%和 69.5%，策略选择方面，所提模型能合理选择收益策略。

关键词：联邦学习；演化博弈；激励机制；复制动态方程

中图分类号：TP391　　**文献标识码：**A

An Evolutionary Game Model for Federated Learning Incentive Optimization

SUN Yue-jie[1], ZHAO Guo-sheng[1]✉, LIAO Yi-wei[1]

(1 School of Computer Science and Information Engineering, Harbin Normal University, Harbin 150025,China)

Abstract: In response to the phenomenon of incentive mismatch caused by participants' misreporting of training costs in federal learning, an evolutionary game model for incentive optimization of federal learning is proposed. Firstly, the federated participant-federal organizer evolutionary game model is established in the federated learning system, and the model quality evaluation algorithm is designed to evaluate the quality of the models submitted by the participants and quantify the training cost of the participants while removing the low-quality models. Then the optimal incentive allocation method is proposed by combining the credibility index, and the optimal payoff strategy under different initial states is obtained by solving the stable strategy of the evolutionary game. The final simulation experiments show that in terms of participant incentive gains, the gains of honest participants are improved by 70% and 57.4% compared with the average allocation method and the individual gain sharing method, and the gains of misrepresented participants are reduced by 65% and 69.5%. In terms of strategy selection, the proposed model can reasonably select the gain strategy.

Key words: Federated learning; Evolutionary games; Incentive mechanisms; Replication dynamic equations

1　引言

深度学习技术蓬勃发展至今，能否获取足够的高质量样本数据是制约其发展速度的重要因素之一。由于数据安全、竞争关系等因素，获取数据过程中出现了严重的数据孤岛问题，并且在数据的集中过程中还存在数据泄漏的风险。因此联邦学习（Federated Learning,FL）作为新兴的分布式机器学习范式应运而生[1]。它使得各个参与方可以在不泄露底层数据的前提下共同建立模型，适用于训练数据涉及敏感信息以及数据量过大无法集中收集的情况。然而，当客户参与联邦学习时，会不可避免的消耗他们的设备资源，同时客户也承担着一定的安全风险，因此对联邦学习激励机制的研究一直是当下的热点。

收稿日期：2022-09-16 收修改稿日期：2022-10-12　基金项目：国家自然科学基金项目（61202458，61403109）资助；黑龙江省自然科学基金（LH2020F034）资助；哈尔滨市科技创新研究基金项目（2016RAQXJ036）资助. 作者简介：**孙跃杰**，男，1999 年生，硕士研究生，研究方向为联邦学习和网络与信息安全；**赵国生**（通讯作者），男，1977 年生，博士，教授，CCF 高级会员，研究方向为认知网络和可信计算；**廖祎玮**，女，1968 年生，硕士，副教授，研究方向为认知网络和可信计算.

区别于博弈论的一次直接达到纳什均衡，演化博弈论的行为主体在演化过程中会动态修正自己的行为，在多次博弈之后达到均衡。据此而建立的联邦学习激励机制更切合实际并且更加有助于联邦的长期稳定发展。

本文将演化博弈中的“适者生存”的基本思想运用到联邦学习当中，将演化稳定策略（Evolutionary Stabilization Strategies, ESS）与复制动态方程（Copy Dynamic Equations, CDE）相结合，提出了一种演化均衡的联邦学习激励机制（Evolutionary Balanced Federated Learning Incentive Mechanism, EBFLIM）。本文的主要贡献如下：

1. 通过模型质量评估算法评估联邦参与者提交模型的质量同时量化其训练成本，并对低质量模型提交进行筛除，以提升联邦任务的完成效果。

2. 提出了一种演化均衡的联邦学习激励机制 EBFLIM，克服了联邦学习中参与者虚报训练成本造成的激励不匹配问题，实现了对联邦学习激励机制的优化。

本文其余部分组织如下：第二章总结与联邦学习激励机制和演化博弈论相关的研究工作；第三章提出面向联邦学习激励优化的演化博弈模型；第四章针对本文提出的优化方法进行仿真实验；第五章对本文进行总结并交代下一步工作。

2 相关工作

2.1 联邦激励机制

为了联邦激励能够更合理的覆盖参与者的资源消耗，吸引更多高质量数据用户加入联邦，已有很多学者投入了联邦学习激励机制的研究。Tang 等人[2]针对组织异质性和公共产品特性提出了社会福利最大化问题，并提出了一种针对 cross-silo FL 的激励机制，同时提出了一种分布式算法，使组织能够在不知道彼此的估值和成本的情况下最大化社会福利。Yu 等人[3]为了解决训练成本和激励之间暂时不匹配的问题，提出了联邦激励机制，通过上下文感知的方式将给定的预算进行动态划分，最大化集体效用，同时最小化数据所有者之间的不平等。Ding 等人[4]针对 non-IID 数据进行了最优契约设计。契约规定了每一个类型用户参与联邦学习能够获得的奖励并且会给到服务器更偏好的用户类型更高的奖励，从而达到激励相对高效、低成本用户参与联邦学习的目的。Bai 等人[5]首先构建众包系统的激励模型。其次，结合反向拍卖和 VCG 拍卖的概念，提出了一种基于拍卖的激励机制。Sun 等人[6]首先考虑了空地网络的动态数字孪生和联合学习，其次基于 Stackelberg 博弈设计联邦学习的激励机制。此外，考虑到不同的数字孪生偏差和网络动态，设计了一个动态激励方案，以自适应地调整最佳客户的选择及其参与程度。Richardson 等人[7]考虑联邦参与者因冗余数据获得奖励的搭便车现象，提出了基于影响力的激励方案保证激励预算与联邦模型价值成比例有界，防止联邦被迫支付多余奖励。杜等人[8]提出了以在线双边拍卖机制为基础的 ODAM-DS 算法。基于最优停止理论，帮助边缘服务器在适当的时间选择移动设备，最小化移动设备的平均能耗。 Hu 等人[9]首先，将数据质量和数据量相结合，构建了特定指标下的联邦学习激励机制模型。然后，对基于服务器平台和数据岛的效用函数构建的激励机制模型进行了两阶段的 Stackelberg 博弈分析。最后，导出两阶段博弈的最优均衡解，确定平台服务器和数据岛的最优策略。从等人[10-11]建立了一个关于 FL 激励机制设计的推理研究框架，提出了 FML 激励机制设计问题的精确定义，基于不同的设置和目标提供了一个清单，供实践者在没有深入博弈论知识的情况下选择合适的激励机制。同时在文献[11]中基于 VCG 提出了一种联邦激励机制，使社会剩余最大化，并使联邦的不公平最小化。

2.2 演化博弈论

博弈论作为解决双方或多方收益问题的重要手段应用于各种环境，基于博弈论的联邦学习激励机制的研究近年来也非常火热。Hasan 等人[12]使用享乐博弈将联邦的交互建模为稳定的联盟划分问题。解决了是否存在确保纳什稳定联盟分区的享乐博弈的问题，并分析了纳什稳定集的非空条件。丁等人[13]针对以数据为中心的开放信息系统，基于演化博弈构建了面向隐私保护的多参与者访问控制演化博弈模型。Byde 等人[14] 描述了一种基于演化的评估拍卖机制的方法，并将其应用于包括标准第一价格和第二价格密封投标拍卖在内的机制空间，对拍卖理论进行了扩展。王等人[15]介绍并给出了混合均匀有限人口中随机演化动力学问题与确定复制方程的相互转化关系。同时介绍了无标度、小世界等复杂网络上演化博弈的研究结论。全等人[16]通过利用一个广义适应度相关的 Moran 过程，研究了一个有限规模的良好混合种群中的对称 2×2 博弈的演化模型，给出了博弈的进化稳定策略，并将其结果与无限种群中复制者动力学进行了比较。王等人[17]综述了网络群体行为和随机演化博弈模型与分析方法等方面的研究工作。针对以上方面的若干研究方法进行总结，并探讨了通过随机演化博弈进行网络群体行为研究的可行性。

由于联邦参与者虚报成本而造成激励不匹配的问题会导致集体利益受到损害，但现有的联邦学习激励机制缺乏对激励不匹配问题的重视。

因此本文在考虑了信息不对称因素的同时，构建演化博弈模型，设计了更符合实际应用场景的联邦学习激励机制。

3 面向联邦学习激励优化的演化博弈模型

本节提出一种面向联邦学习激励优化的演化博弈模型。首先在联邦学习系统中建立联邦参与者-联邦组织者演化博弈模型（Federal Participant-Federal Organizer Evolutionary Game Model,FPFOEGM），然后通过对联邦参与者提交的模型进行质量评估来过滤低质量模型，同时结合联邦参与者的信誉度指标设计联邦激励策略，最后通过求解复制动态方程得到演化稳定策略。

3.1 模型假设

基于客户-服务器架构构建的联邦学习系统模型如图 1 所示。考虑当前有 n 个联邦参与者表示为 $P=\{p_1,p_2,\cdots,p_n\}$。有模型使用者向联邦发送任务请求并将自己获得收益的一部分下发给联邦用于激励联邦参与者。为了能够对模型进行质量评估和筛选，同时量化参与者训练成本，在联邦中加入具有一定计算能力的联邦组织者，组织者接收参与者提交的模型进行筛选后将符合条件的模型上传至参数服务器进行整合，并作为协调方在激励预算允许的范围内对参与者进行激励。

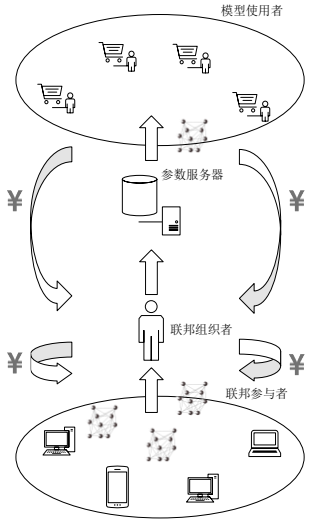

图 1 基于客户-服务器架构的联邦学习模型

Fig.1 Federated learning model based on client-server architecture

本文在 FPFOEGM 模型中设置以下假设条件：

1. 博弈参与者均具有有限理性。联邦参与者通过选择合适的模型提交策略获得收益；联邦组织者通过选择适当的激励策略获得收益。

2. 博弈双方的策略选择随着博弈进行发生动态变化。

3. 联邦组织者的博弈收益即为联邦的收益。

3.2 模型构建

FPFOEGM 模型可以用一个三元组进行表示，$\mathrm{FPFOEGM}=\{M,S,U\}$。

1. $M=(N_p,N_o)$ 表示演化博弈参与者，N_p 为联邦参与者，N_o 为联邦组织者。

2. $S=(S_p,S_o)$ 表示联邦参与者和联邦组织者的策略空间，其中 $S_p=\{S_{p1},S_{p2},\cdots,S_{pn}\}$ 为联邦参与者的策略集，$S_o=\{S_{o1},S_{o2},\cdots,S_{om}\}$ 为联邦组织者的策略集。

3. $U=(U_p,U_o)$ 表示博弈双方收益函数集合，U_p 为联邦参与者的收益函数，U_o 为联邦组织者的收益函数。

在演化博弈模型中，联邦参与者和联邦组织者均有多个博弈策略可选择，并且双方选择同一个策略的概率会随着博弈进行发生变化，因此双方的策略选取是一个动态过程。

3.3 基于演化博弈的联邦学习激励优化方法

本节对联邦参与者提交模型的质量进行了评估并且针对联邦中的成本虚报现象设定信誉度指标。提出了一种基于演化博弈的联邦学习激励优化方法。

3.3.1 模型质量评估

将模型质量评估加入 FPFOEGM 模型，量化模型训练成本的同时去除低质量的模型提交。当联邦参与者接收到来自模型使用者发布的任务时，将从参数服务器中下载模型数据并使用本地数据进行训练，提交训练好的模型表示为 $M=\{m_1,m_2,\cdots,m_n\}$，有 m 个评估模型质量的指标 $A=\{a_1,a_2,\cdots,a_m\}$，$G=g_{ij}$ 表示联邦参与者提交的训练模型 m_i 在指标 a_j 上的评估值。模型质量的评估与测试集的测试结果密切相关，因此基于混淆矩阵将模型质量评价指标总结为准确率（a_1）、精确率（a_2）、召回率（a_3）三种。

由于以上评估指标均与模型质量成正相关，因此可以通过式（1）对指标进行归一化处理，并以此为依据去除低质量模型。

$$\alpha_{ij}=\begin{cases}0, g_{ij}<\beta_j^{\min}\\ \dfrac{g_{ij}-\beta_j^{\min}}{\beta_j^{\max}-\beta_j^{\min}}, \beta_j^{\min}\le g_{ij}\le\beta_j^{\max}\end{cases} \tag{1}$$

其中的 $\beta_j^{\min}$ 和 $\beta_j^{\max}$ 表示 a_j 的下限和上限，提交模型 i 在每种指标下的评估值序列记为 $\{\alpha_{i1},\alpha_{i2},\cdots,\alpha_{im}\}$。

使用公式（2）计算提交模型 m_i 最小的评估值 $\alpha_i^{\min}$ 并依此判断其合理性。

$$\alpha_i^{\min}=\min\{\alpha_{ij}\} \tag{2}$$

如果 $\alpha_i^{\min}=0$ 那么该联邦参与者提交的模型就被视为低质量模型并被去除。

针对模型使用者对模型性能的不同需求，引入权重 ω_j，使模型质量评估结果更加符合实际情况。通过式（3）对参与者 p_i 第 k 次提交模型的质量进行评估，便于联邦组织者进行激励策略选择。

$$C_i^k=\sqrt{\sum_{j=1}^{m}\left(\omega_j\times\alpha_{ij}\right)^2}, i=1,2,\ldots,n, k=1,2,\ldots \tag{3}$$

模型质量评估算法如表 1 所示。

表 1 模型质量评估算法

Table 1 Model quality assessment algorithm

算法 1. 模型质量评估算法

输入：用户训练并提交的模型。

输出：模型质量评估结果。

步骤1. 确定模型质量评估指标 a_j；

步骤2. 确定评估指标权重 ω_j；

步骤3. 用相同测试集对用户提交的模型进行测试，得到 g_{ij}；

步骤4. $FOR\ i=1,2,\cdots,n\ \ j=1,2,\cdots,m$；//对模型质量评估数值进行归一化处理，得到模型 i 在每种指标下的评估值序列

步骤5. $\alpha_{ij}=\begin{cases}0, g_{ij}<\beta_j^{\min}\\ \dfrac{g_{ij}-\beta_j^{\min}}{\beta_j^{\max}-\beta_j^{\min}}, \beta_j^{\min}\le g_{ij}\le\beta_j^{\max}\end{cases}$；

步骤6. $\alpha_i^{\min}=\min\{\alpha_{ij}\}$；//计算每种评估指标下的最小评估值

步骤7. $IF\ \ \alpha_i^{\min}=0$；//根据指标最小值判断模型是否为低质量模型，并筛选

步骤8. *END IF*

步骤9. $C_i^k=\sqrt{\sum_{j=1}^{m}\left(\omega_j\times\alpha_{ij}\right)^2},i=1,2,\ldots,n,k=1,2,\ldots$； //对提交的数据模型质量进行评估

步骤 10. *END FOR*

3.3.2 信誉度评估

在联邦学习中，每个参与者追求个体利益最大化时，存在虚报训练成本的情况，即上报联邦的成本与提交模型的质量不匹配，这会导致集体利益受到损害甚至造成合作失败。因此在对联邦参与者提交的模型进行质量评估后，针对虚报成本现象进行信誉度评估。

一般情况下，联邦学习中的联邦参与者的训练成本与其提交的模型质量成正比，因此本文假设其真实训练成本与模型质量在数值上相等。在联邦学习中，联邦参与者上报的成本超出真实成本越多，其信誉度越低，反之信誉度则越高。

联邦参与者 p_i 在第 k 次提交模型后的信誉度 Q_i^k 如式（4）所示：

$$Q_i^k=\frac{\sum_{l=1}^{k}q_i^l}{k} \tag{4}$$

输入参数 q_i^l 如式（5）所示：

$$q_i^l=\begin{cases}1, & D_i^l=0\\ \dfrac{1}{1+\dfrac{D_i^l}{\overline{D^l}}}, & D_i^l\neq 0\end{cases} \tag{5}$$

其中，D_i^l为参与者 p_i 第 l 次提交模型时的成本虚报量，$\overline{D^l}$为参与者第 l 次提交的平均成本虚报量。如式（6）所示：

$$\begin{cases}D_i^l=R_i^l-C_i^l\\ \overline{D^l}=\dfrac{\sum_{i=1}^{n}D_i^l}{n}\end{cases} \tag{6}$$

其中 R_i^l 表示参与者 p_i 第 l 次的上报成本，通过式（5）计算 q_i^l 然后利用式（4）对信誉度进行计算，实现了对联邦参与者信誉度的评估，信誉度评估算法如表 2 所示。

表 2 信誉度评估算法

Table 2 Reputation evaluation algorithms

算法 2. 信誉度评估算法

输入：联邦参与者上报的成本和模型质量评估结果。

输出：参与者信誉度。

步骤1. *FOR* $l=1,2,\cdots,k\ \ i=1,2,\cdots,n$； //结合参与者上报成本和模型质量评估结果对参与者信誉度进行评估

步骤2. $\begin{cases}D_i^l=R_i^l-C_i^l\\ \overline{D^l}=\dfrac{\sum_{i=1}^{n}D_i^l}{n}\end{cases}$； //求得参与者 i 第 l 次提交的成本虚报量和整体平均虚报量

步骤3. $q_i^l=\begin{cases}1, & D_i^l=0\\ \dfrac{1}{1+\dfrac{D_i^l}{\overline{D^l}}}, & D_i^l\neq 0\end{cases}$；// 量化参与者的信誉度指标

步骤4. $Q_i^k=\dfrac{\sum_{l=1}^{k}q_i^l}{k}$；// 计算 k 次提交之后参与者的信誉度

步骤5. *END FOR*

3.3.3 激励分配方法

在对联邦参与者提交模型的质量及其信誉度进行评估的基础上，设计激励策略削弱联邦参与者虚报训练成本的欲望提高联邦整体效用。

本文将激励分配过程分为两部分，第一部分为依据联邦参与者上报训练成本占比进行初次激励分配，第二部分为结合参与者信誉度扣除虚报参与者一定比例的激励收益用于对诚实上报训练成本的参与者进行二次激励分配，两次分配后参与者得到本轮最终激励收益。令 $PT=\{p_{t1},p_{t2},\cdots,p_{tv}\}$ 为诚实参与者集合，$PF=\{p_{f1},p_{f2},\cdots,p_{fw}\}$ 为虚报参与者集合，其中 $v+w=n$。设联邦第 k 轮提交的激励总预算为 B_k，联邦参与者 p_i 通过初次分配获得的激励收益 E_{i1}^k 如式（7）所示：

$$E_{i1}^k=B_k\times u_{i1}^k \tag{7}$$

其中 u_{i1}^k 为参与者 p_i 初次分配的份额占比，如式（8）所示：

$$u_{i1}^k=\frac{R_i^k}{\sum_{i=1}^{n}R_i^k} \tag{8}$$

若 $p_i\in PF$ 即 p_i 为虚报训练成本的参与者，其初次激励收益还需根据其信誉度进行调整且不能参与二次激励分配。则其最终收益 E_i^k 如式（9）所示：

$$E_i^k=E_{i1}^k\times Q_i^k \tag{9}$$

则虚报参与者 p_i 被扣除并用于对诚实参与者进行二次激励的收益量为 $E_{i1}^k\times(1-Q_i^k)$，记所有虚报参与者被扣除收益的总和为 θ。

若 $p_i\in PT$ 即 p_i 为诚实上报训练成本的参与者，则可同其他诚实参与者根据训练成本比重进行二次激励分配，二次分配获得的收益 E_{i2}^k 如式（10）所示：

$$E_{i2}^k=u_{i2}^k\times\theta \tag{10}$$

其中 u_{i2}^k 为 p_i 二次分配的份额占比，则此时参与者获得的最终激励收益如式（11）所示：

$$E_i^k=E_{i1}^k+E_{i2}^k \tag{11}$$

综上可得：

$$\begin{cases}E_i^k=E_{i1}^k\times Q_i^k, & p_i\in PF\\ E_i^k=E_{i1}^k+E_{i2}^k, & p_i\in PT\end{cases} \tag{12}$$

激励分配算法如表 3 所示。

表 3 激励分配算法

Table 3 Incentive allocation algorithm

算法 3. 激励分配算法

输入：参与者提交模型质量评估结果和信誉度评估结果

输出：激励分配结果

步骤1. 根据信誉度评估结果将参与者划分为 PT 和 PF；

步骤2. 确定联邦激励总预算 B_k；

步骤3. $FOR\ i=1,2,\cdots,n$ //计算参与者初次分配获得的激励收益

步骤4. $u_{i1}^k=\dfrac{R_i^k}{\sum_{i=1}^{n}R_i^k}$；//计算参与者 i 初次分配的激励份额占比

步骤5. $E_{i1}^k=B_k\times u_{i1}^k$；//计算参与者 i 初次分配得到的激励

步骤6. $IF\ \ p_i\in PF$ //计算虚报参与者激励收益

步骤7. $E_i^k=E_{i1}^k\times Q_i^k$；//虚报参与者最终激励收益

步骤8. $\theta=\sum_{i=1}^{n}E_{i1}^k\times(1-Q_i^k)$ //用于二次分配的激励总和

步骤9. $END\ IF$；

步骤10. $END\ FOR$；

步骤11. $FOR\ i=1,2,\cdots,n$；//对诚实参与者进行二次激励分配

步骤12. $IF\ \ p_i\in PT$；

步骤13. $E_{i2}^k=u_{i2}^k\times\theta$；//二次分配获得的收益

步骤14. $E_i^k=E_{i1}^k+E_{i2}^k$；//诚实参与者最终收益

步骤15. $END\ IF$；

步骤 16. $END\ FOR$；

3.4 收益矩阵分析

在 FPFOEGM 中，考虑到联邦参与者虚报训练成本的情况引入了联邦组织者，联邦参与者为 P，联邦组织者为 O。构建联邦参与者的策略集$\{PS_1,PS_2\}$，PS_1表示诚实即上报成本等于真实训练成本、PS_2表示虚报，即上报成本大于真实训练成本;构建联邦组织者的策略集$\{OS_1,OS_2\}$，OS_1表示使用模型，OS_2表示不使用模型。一般情况下，联邦给予联邦参与者的激励可以覆盖其训练成本。

下面分析博弈过程中参与者的收益情况，参与者在不同策略下的收益情况如表 4 所示。

表 4 参与者和组织者的收益矩阵

Table 4 Benefit matrix of participants and organizers

O / P	使用(OS_1)	不使用(OS_2)
诚实(PS_1)	(s_1-c_1,e_1-s_1)	$(-c_1,0)$
虚报 (PS_2)	(s_2-c_2,e_2-s_2)	$(-c_2,0)$

其中c_1、c_2分别为联邦参与者选择诚实策略和虚报策略时，其真实训练成本。s为来自联邦的激励收益，e_1、e_2为联邦使用模型获得的收益。

基于上述收益矩阵，设x为 P 中采用策略PS_1的参与者所占比例，y为 O 中采用策略OS_1的组织者所占比例。则联邦参与者如实上报成本和虚报成本下的期望收益如式（13）所示：

$$\begin{cases}U_{p1}=y(s_1-c_1)+(1-y)(-c_1)\\U_{p2}=y(s_2-c_2)+(1-y)(-c_2)\end{cases}\tag{13}$$

联邦参与者的平均收益如式（14）所示:

$$\overline{U_p}=xU_{p1}+(1-x)U_{p2}\tag{14}$$

由此可得联邦参与者的复制动态方程如式（15）所示：

$$\begin{aligned}F_1(x)=\frac{dx}{dt}&=x\left(U_{p1}-\overline{U_p}\right)=x(1-x)\left(U_{p1}-U_{p2}\right)\\&=x(1-x)\left[y\left(s_1-s_2\right)+c_2-c_1\right]\end{aligned}\tag{15}$$

同理，联邦组织者使用模型和不使用模型的期望收益如式（16）所示：

$$\begin{cases}U_{o1}=x\left(e_1-s_1\right)+(1-x)\left(e_2-s_2\right)\\U_{o2}=0\end{cases}\tag{16}$$

联邦组织者的平均收益如式（17）所示：

$$\overline{U_o}=yU_{o1}+(1-y)U_{o2}\tag{17}$$

则联邦组织者的复制动态方程如式（18）所示：

$$\begin{aligned}F_2(y)=\frac{dy}{dt}&=y\left(U_{o1}-\overline{U_o}\right)=y(1-y)\left(U_{o1}-U_{o2}\right)\\&=y(1-y)\left[x\left(s_2-s_1+e_1-e_2\right)+e_2-s_2\right]\end{aligned}\tag{18}$$

3.5 演化稳定策略

基于联邦参与者与联邦组织者的复制动态方程，对EBFLIM模型的演化稳定策略的求解过程如下:

1. 计算复制动态方程的稳定解

建立复制动态方程组 $E=\begin{bmatrix}F_1(x)\\F_2(y)\end{bmatrix}=0$，通过计算方程组$E$求得稳定解为：$E_1=[0\ 0]^\top$，$E_2=[0\ 1]^\top$，$E_3=[1\ 0]^\top$，$E_4=[1\ 1]^\top$，$E_5=\begin{bmatrix}x^*\\y^*\end{bmatrix}=\begin{bmatrix}\dfrac{s_2-e_2}{s_2-s_1+e_1-e_2}&\dfrac{c_1-c_2}{s_1-s_2}\end{bmatrix}^\top$。其中，$E_1=[0\ 0]^\top$ 表示联邦参与者选择策略P_{s2}，联邦组织者选择O_{s2}；$E_2=[0\ 1]^\top$ 表示联邦参与者选择策略P_{s2}，联邦组织者选择O_{s1}；$E_3=[1\ 0]^\top$ 表示联邦参与者选择策略P_{s1}，联邦组织者选择O_{s2}；$E_4=[1\ 1]^\top$，表示联邦参与者选择策略P_{s1}，联邦组织者选择O_{s1}；$E_5=\begin{bmatrix}x^*\\y^*\end{bmatrix}=\begin{bmatrix}\dfrac{s_2-e_2}{s_2-s_1+e_1-e_2}&\dfrac{c_1-c_2}{s_1-s_2}\end{bmatrix}^\top$ 表示联邦参与者以混合概率$\left(\dfrac{s_2-e_2}{s_2-s_1+e_1-e_2},1-\dfrac{s_2-e_2}{s_2-s_1+e_1-e_2}\right)$选择策略$\{P_{s1},P_{s2}\}$，联邦组织者以混合概率$\left(\dfrac{c_1-c_2}{s_1-s_2},1-\dfrac{c_1-c_2}{s_1-s_2}\right)$选择策略$\{O_{s1},O_{s2}\}$。

2. 演化稳定性分析

1）联邦参与者上报成本策略的演化博弈分析

对联邦参与者的复制动态方程进行分析，当 $y=\frac{c_1-c_2}{s_1-s_2}$ 时，$F_1(x)$ 始终为 0，所有 x 水平都是稳定状态；如果 $y\neq\frac{c_1-c_2}{s_1-s_2}$，则 $x^*=0$ 和 $x^*=1$ 是两个稳定状态。其中 $y>\frac{c_1-c_2}{s_1-s_2}$，$x^*=0$ 是 ESS，此时，联邦参与者倾向于选择虚报策略；$y<\frac{c_1-c_2}{s_1-s_2}$ 时，$x^*=1$ 是 ESS，此时，联邦参与者倾向于选择诚实策略。三种情况下 x 的动态趋势图如图 2 所示。

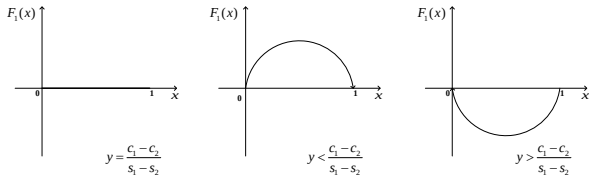

图 2 联邦参与者复制动态相位图

Fig.2 Replication dynamic phase diagram of federated participants

2）联邦组织者策略的演化博弈分析

对联邦组织者的复制动态方程进行分析，当 $x=\frac{s_2-e_2}{s_2-s_1+e_1-e_2}$ 时，$F_2(y)$ 始终为 0，所有 y 水平都是稳定状态；如果 $x\neq\frac{s_2-e_2}{s_2-s_1+e_1-e_2}$，则 $y^*=0$ 和 $y^*=1$ 是两个稳定状态。其中 $x>\frac{s_2-e_2}{s_2-s_1+e_1-e_2}$，$y^*=1$ 是 ESS，此时，联邦组织者倾向于选择使用策略；$x<\frac{s_2-e_2}{s_2-s_1+e_1-e_2}$ 时，$y^*=0$ 是 ESS，此时，联邦组织者倾向于选择不使用策略。三种情况下 y 的动态趋势图如图 3 所示。

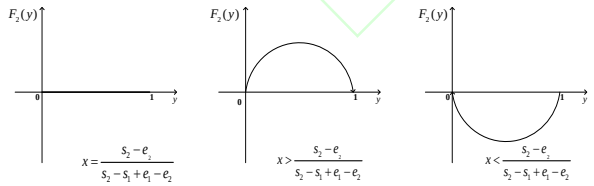

图 3 联邦组织者复制动态相位图

Fig.3 The replication dynamic phase diagram of the federation organizer

3）联邦参与者与联邦组织者的博弈演化稳定策略

演化稳定策略指如果绝大多数个体选择演化稳定策略，那么小部分的突变个体就无法入侵到这个群体[18]。根据上述演化稳定均衡解，构建雅可比矩阵，求出行列式与迹。雅可比矩阵构建如式（19）所示：

$$J=\begin{pmatrix}(1-2x)\left[y(s_1-s_2)+(c_2-c_1)\right] & x(1-x)(s_1-s_2)\\ y(1-y)(s_2-s_1+e_1-e_2) & (1-2y)\left[x(s_2-s_1+e_1-e_2)+(e_2-s_2)\right]\end{pmatrix} \quad (19)$$

根据雅可比矩阵计算其行列式和迹，结果如式（20）和式子（21）所示：

$$DetJ=(1-2x)[y(s_1-s_2)+(c_2-c_1)](1-2y)[x(s_2-s_1+e_1-e_2)+(e_2-s_2)]-x(1-x)(s_1-s_2)y(1-y)(s_2-s_1+e_1-e_2) \quad (20)$$

$$TrJ=(1-2x)[y(s_1-s_2)+(c_2-c_1)]+(1-2y)[x(s_2-s_1+e_1-e_2)+(e_2-s_2)] \quad (21)$$

在EBFLIM模型中，选择虚报策略的联邦参与者的实际训练成本较低，所以 $c_1>c_2$ 在基于模型质量以及联邦参与者信誉度的联邦激励机制的作用下，联邦参与者和联邦组织者的收益满足以下条件：$s_1-c_1>s_2-c_2, e_1-s_1>e_2-s_2$。

利用雅可比矩阵判断是否为演化稳定策略，若局部平衡点对应矩阵的行列式 *DerJ* 大于零，且迹 *TrJ* 小于零，则为 ESS；若 *DerJ* 大于零，且迹 *TrJ* 大于零，则为不稳定解；若 *DerJ* 小于零，且迹 *TrJ* 为任意值，则为鞍点。

基于以上条件局部均衡点稳定性分析如表 5 所示。

表 5 局部均衡点稳定性分析

Table 5 Stability analysis of local equilibrium point

局部均衡点	*DetJ*	*TrJ*	均衡结果
E_1（0，0）	-	不确定	鞍点
E_2（1，0）	-	不确定	鞍点
E_3（0，1）	+	+	不稳定点
E_4（1，1）	+	-	ESS
E_5（x^*，y^*）	+	0	中心点

4 仿真实验

4.1 仿真设置

本文使用经典 MNIST 手写数据集进行实验仿真。为了真实还原联邦学习系统环境，将训练图例按照随机比例分配给 10 名联邦参与者以模拟参与者持有不同训练资源的情形，并从中随机选取 5 名有意虚报训练成本的参与者。本实验在 Windows 系统下通过 Matlab 平台搭建 GoogLeNet 执行手写数字识别训练任务以模仿参与者训练模型的过程。具体参数设置如表 6 所示。

表 6 训练参数设置

Table 6 Training parameter setting

参数名称	数值
训练集总数/个	60000
测试集总数/个	10000
验证集占比	30%
训练轮次/轮	30
随机翻转/度	[-90,90]
随机缩放/倍	[1,2]
验证频率	70次迭代
学习率	0.001

4.2 实验结果分析

首先对参与者提交模型的质量及参与者信誉度进行评估，在 EBFLIM 中，联邦参与者提交高质量的模型可以得到更多的激励收益，同时也会提升联邦的总体效用。十名联邦参与者使用各自持有的数据对模型进行训练，之后用

相同的测试集对他们训练好的模型进行测试，测试准确率如图 4 所示。

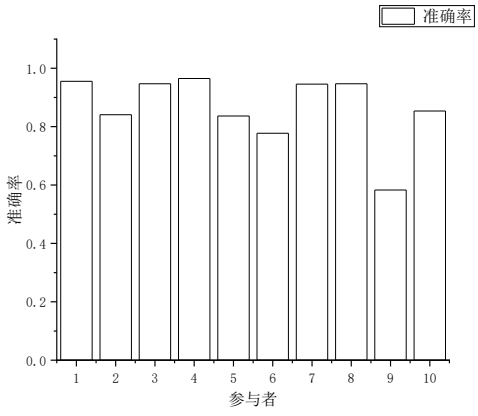

图 4 测试准确率

Fig.4 Test accuracy

通过对测试结果进一步分析可以得到十个模型对应的混淆矩阵，通过公式（22）计算 *Precision* 和 *Recall* 。

$$\begin{cases} Precision = \dfrac{TP}{TP + FP} \\ Recall = \dfrac{TP}{TP + FN} \end{cases} \tag{22}$$

其中 *TP* 表示是正类并且被判定为正类的实例， *FP* 表示实际为负类但被判定为正类的实例， *FN* 表示本为正类但被判定为负类的实例。

每个模型识别不同类别测试样例的精确率与召回率应被分以不同的权重，在仿真实验过程中，为了简化实验过程，将不同分类的权重均设置为 1，则进一步处理后，不同模型对应的精确率与召回率如图 5 所示：

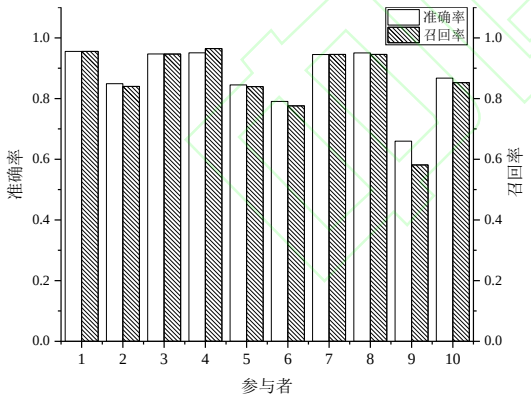

图 5 处理后的精确率与召回率

Fig.5 Precision and recall after processing

利用以上实验测得的模型性能评估指标结合 4.3 节中的模型质量评估算法即可度量联邦参与者提交模型的质量。设期望值下限 $\beta_j^{\min} = 0.6$，期望值上限 $\beta_j^{\max} = 1$，评估指标 a_1, a_2, a_3 对应的权重 $\omega_1, \omega_2, \omega_3$ 由 rand 函数随机生成，根据以上信息评估参与者 P_i 的信誉度，参与者上传模型质量 C 、上报训练成本 R 以及参与者信誉度评估结果 Q 如表 7 所示（结果保留两位小数，×表示未通过模型质量筛选）。

表 7 参与者的模型质量、上报成本和信誉度

Table 7 Model quality, reporting cost, and creditworthiness of participants

P	C	R	Q
P_1	0.89	0.89	1
P_2	0.61	0.91	0.25
P_3	0.83	0.83	1
P_4	0.91	0.91	1
P_5	0.6	0.8	0.33
P_6	0.45	0.85	0.2
P_7	0.86	0.95	0.5
P_8	0.87	0.87	1
P_9	×	×	×
P_{10}	0.64	0.64	1

由表 7 数据可知，参与者 9 因未能通过模型质量筛选而被移出联邦，在本实验设置的条件下，对使用模型评估算法前后两种状态下的联邦学习系统引入 FedAvg 框架[19]进行参数聚合得到两个训练模型，用相同测试集对两个模型进行测试，输出相应的混淆矩阵，测试结果表明，在参与者 9 持有数据占比仅为 0.3%的情况下，经过模型质量筛选后聚合得到的模型的精度仍比未经过筛选得到的模型提高了 0.01%。在联邦学习实际应用的过程中，该方法对联邦模型精度的提升效果会随着数据量以及联邦参与者数量的增加而更加显著。

平均分配方法是平等收益分享的一种，在这种方法中第 k 轮可用收益预算 B_k 被均等的分配给所有 n 个参与者，因此参与者 i 第 k 轮的收益 E_i^k 如式（23）所示：

$$E_i^k = \frac{1}{n} B_k \tag{23}$$

在个体收益分享法中，参与者 i 对集合体做出的边际收益被用于计算他能得到的收益分成如式（24）所示：

$$E_i^k = v(\{i\}) B_k \tag{24}$$

其中 $v(X)$ 表示评估集合体效用的函数。

使用三种不同的激励分配方法，联邦参与者的激励收益情况如图 6 所示。

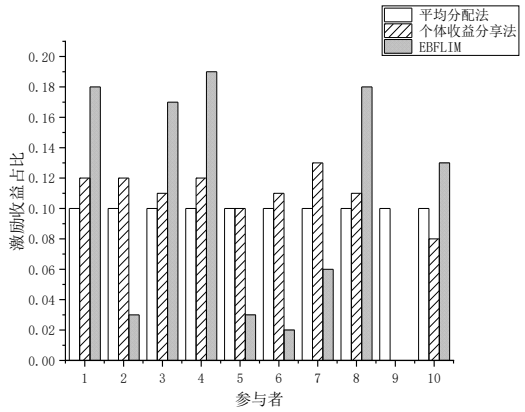

图 6 不同分配方法下参与者的收益

Fig.6 The benefits of participants under different distribution methods

EBFLIM 在进行激励分配时，综合考虑了参与者虚报

成本的现象，降低虚报参与者的激励收益，同时提高诚实上报训练成本的参与者的激励收益。如图 6 所示，利用平均分配法和个体收益分享法均会导致部分诚实上报训练成本的参与者的收益占比小于或等于部分真实训练成本较低的虚报者，而 EBFLIM 对虚报者的激励收益进行了削减并将其二次分配给诚实上报成本的参与者，与平均分配法和个体收益分享法相比诚实参与者的收益提升了 70%和 57.4%，虚报参与者收益降低了 65%和 69.5%，达到了提高联邦参与者积极性，减少虚报现象的目的。

进一步分析联邦参与者与联邦组织者的演化过程和模型中最优策略的选取问题。[*x*,*y*]初值分别取[0.2,0.8]，[0.4,0.6]，[0.6,0.4]， [0.8,0.2]，图 7 展示了在激励机制的作用下博弈双方的动态演化的过程，可见不同初始状态的策略选择经过演化最终会达到一定的稳定状态并且该状态可以使参与者与联邦均获得最佳收益。

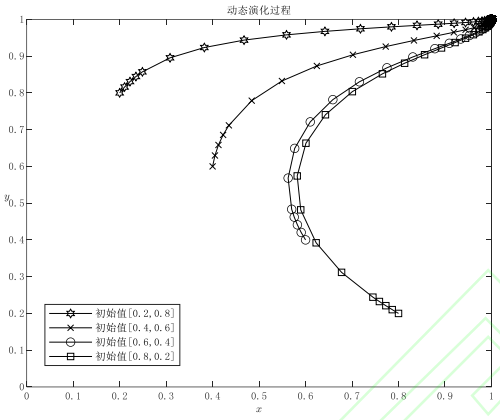

图 7 不同初始状态的动态演化过程

Fig.7 Dynamic evolution process of different initial states

5 结束语

本文提出了面向联邦学习激励优化的演化博弈模型，分析评价表明，优化后的联邦学习激励方法能够有效的限制联邦中虚报成本的参与者的收益，降低其虚报成本的动力，同时在不同初始情况下参与者与联邦均能选取使双方收益最优的策略，提高了联邦的整体效益。下一步的工作首先是将其它导致联邦学习激励不匹配的因素融合进来，以适用于更多样的情形。其次是尝试对所提激励优化方法进行应用。

References：

[1] Yang Q,Liu Y,Chen T,et al.Federated machine learning: Concept and applications[J].ACM Transactions on Intelligent Systems and Technology (TIST),2019,10(2):1-19.

[2] Tang M,Wong V W.An incentive mechanism for cross-silo federated learning:a public goods perspective[C]// IEEE Conference on Computer Communications(IEEE INFOCOM 2021),2021:1-10.

[3] Yu H,Liu Z,Liu Y,et al.A sustainable incentive scheme for federated learning[J].A Sustainable Incentive Scheme for Federated Learning,2020,35(4):58-69.

[4] Ding N,Fang Z,Huang J.Optimal contract design for efficient federated learning with multi-dimensional private information[J].IEEE Journal on Selected Areas in Communications,2020,39(1):186-200.

[5] Bai L,Hu F,Jiao C,et al.A fair incentive mechanism in federated learning[C]//2nd International Conference on Big Data Economy and Information Management (BDEIM),2021:396-399.

[6] Sun W,Xu N,Wang L,et al.Dynamic digital twin and federated learning with incentives for air-ground networks[J].IEEE Transactions on Network Science and Engineering, 2020,9(1):321-333.

[7] Richardson A,Filos-Ratsikas A,Faltings B.Budget-bounded incentives for federated learning[M].Federated Learning,Switzerland:Springer,Cham,2020:176-188.

[8] Du Hui,Li Zhuo,Chen Xin.Incentive mechanism for hierarchical federated learning based on online double auction[J].Computer Science,2022,49(3):23-30.

[9] Hu P,Gu H,Qi J,et al.Design of two-stage federal learning incentive mechanism under specific indicators[C]//2nd International Conference on Big Data Economy and Information Management (BDEIM),2021:475-478.

[10] Cong M,Yu H,Weng X,et al. A game-theoretic framework for incentive mechanism design in federated learning[M].Federated Learning.Switzerland:Springer, Cham, 2020:205-222.

[11] Cong M,Yu H,Weng X,et al.A VCG-based fair incentive mechanism for federated learning[J].arXiv preprint arXiv:2008.06680,2020,doi:10.48550/arXiv.2008.06680.

[12] Hasan C.Incentive mechanism design for federated learning: hedonic game approach[J].arXiv preprint arXiv:2101.09673,2021,doi:10.48550/arXiv.2101.09673.

[13] Ding Hong-fa,Peng Chang-gen,Tian You-liang,et al.Privacy risk adaptive access control model via evolutionary game [J].Journal on Communications,2019,40(12):9-20.

[14] Byde A.Applying evolutionary game theory to auction mechanism design[C]//IEEE International Conference on E-Commerce(CEC 2003),2003:347-354.

[15] Wang Long,Fu Feng,Chen Xiao-jie,et al.Evolutionary games on complex networks[J].CAAI Transactions on Intelligent Systems,2007,2(2):1-10.

[16] Quan Ji,Wang Xian-jia.Evolutionary games in a generalized Moran process with arbitrary selection strength and mutation[J].Chinese Physics B,2011,20(3):25-30.

[17] Wang Yuan-zhuo,Yu Jian-ye,Qiu Wen,et al.Evolutionary game model and analysis methods for network group

behavior[J].Chinese Journal of Computers,2015,38(2):282-300.

[18] Smith J,Price G R.The logic of animal conflict[J].Nature, 1973,246(5427):15-18.

[19] Mcmahan H B,Moore E,Ramage D,et al.Communication-efficient learning of deep networks from decentralized data[C]//International Conference on Artificial Intelligence and Statistics(AISTATS),2017:1273-1282.

附中文参考文献：

[8] 杜 辉,李 卓,陈 昕.基于在线双边拍卖的分层联邦学习激励机制[J].计算机科学,2022,49(3):23-30.

[13] 丁红发,彭长根,田有亮,等.基于演化博弈的隐私风险自适应访问控制模型[J].通信学报,2019,40(12):9-20.

[15] 王 龙,伏 锋,陈小杰,等.复杂网络上的演化博弈[J].智能系统学报,2007,2(2):1-10.

[17] 王元卓,于建业,邱 雯,等.网络群体行为的演化博弈模型与分析方法[J].计算机学报,2015,38(2):282-300.