DOI:10.3969/j.issn.1003-5060.2024.11.008

联邦学习中基于 Chebyshev 定理的模型性能感知逆向拍卖

罗　丰，王　琦，王青山
(合肥工业大学 数学学院,安徽 合肥　230601)

摘　要:文章研究多服务器、多客户端联邦学习(federated learning,FL)场景中的激励机制,并将任务分配和定价问题建模为多个逆向拍卖问题。根据切比雪夫(Chebyshev)定理对客户端每一轮的本地模型性能进行评估,并进一步利用指数衰减函数评估其本地模型的总体性能;设计基于本地模型性能的逆向拍卖(local model performance based reverse auction,LPRA)算法解决任务分配和定价问题以激励更多高性能的客户端参与,并从理论上证明 LPRA 算法满足个体理性、真实性和计算高效性;通过仿真实验验证 LPRA 算法的有效性。

关键词:联邦学习(FL);激励机制;切比雪夫定理;逆向拍卖;个体理性
中图分类号:TP183　　**文献标志码**:A　　**文章编号**:1003-5060(2024)11-1486-07

Model performance-aware reverse auction based on Chebyshev's theorem in federated learning

LUO Feng,　WANG Qi,　WANG Qingshan
(School of Mathematics, Hefei University of Technology, Hefei 230601, China)

Abstract: This paper studies the incentive mechanism in a multi-server, multi-client federated learning (FL) scenario and models the task allocation and pricing as multiple reverse auction problem. Firstly, local model performance of clients is evaluated in each round according to Chebyshev's theorem, and exponential decay function is used to evaluate the historical performance of clients. Then, a local model performance based reverse auction (LPRA) algorithm is designed to solve the task allocation and pricing problems with the goal of maximizing the overall performance of clients participating in FL. Through theoretical analysis, it is confirmed that LPRA algorithm satisfies individual rationality, truthfulness and computational efficiency. Finally, the effectiveness of the LPRA algorithm is verified by simulated experiments.

Key words: federated learning(FL); incentive mechanism; Chebyshev's theorem; reverse auction; individual rationality

0　引　　言

随着物联网(internet of things,IoT)技术快速发展,全球已有近 70 亿台 IoT 设备和 30 亿部智能手机[1],它们每时每刻都在产生海量数据,这些数据成为神经网络[2]发展的重要支柱。传统的神经网络模型训练要求客户端将本地数据传输到云端进行统一训练,但随着数据规模的增加,将所有数据上传会产生大量的通信成本,同时也导致用户隐私的泄漏。为了解决上述问题,一种新型

收稿日期:2023-03-30;**修回日期**:2023-09-10
基金项目:安徽省自然科学基金资助项目(2208085MF165)
作者简介:罗　丰(1997—),男,安徽安庆人,合肥工业大学硕士生;
王　琦(1975—),女,安徽合肥人,博士,合肥工业大学副教授,硕士生导师,通信作者,E-mail:wangq@hfut.edu.cn;
王青山(1975—),男,安徽合肥人,博士,合肥工业大学教授,博士生导师.

的分布式训练框架即联邦学习（federated learning，FL）[3]被引入。在 FL 中，全局模型由服务器下发到本地客户端，客户端利用本地数据进行模型迭代训练，并将训练后的模型参数发送给中心服务器进行全局聚合。上述过程重复多次直至达到所需的全局模型精度。相比传统的集中式训练，FL 不需要客户端上传本地数据，而只需要上传训练后的模型参数，大大减少了通信开销，并且有效降低了客户端隐私泄露的风险。与此同时，对于一些实时性要求高的 FL 任务，如自动驾驶导航、路况检测等，客户端既作为训练的参与者，同时也是模型的受益者，模型在本地能实现更短的推理延迟。

虽然 FL 具有以上优点，但要部署一个真实、高效的 FL 框架依然面临以下两大挑战：① 由于 FL 的隐私保护，通常很难对客户端的性能进行真实、有效的评估，这导致低性能的客户端会降低全局模型训练的效率和质量；② 客户端贡献本地数据和计算资源参与 FL 任务，如果没有合适的补偿，那么客户端可能拒绝参与 FL 任务。因此设计真实有效的激励机制来吸引更多高性能的客户端参与 FL 任务是一个亟需解决的问题。目前，已经存在一些关于联邦学习激励机制的研究，主要有拍卖理论[4-6]、合约理论[7-9]和博弈论[10-12]。文献[4]认为全局模型的迭代次数是由所有参与者的本地模型精度决定的，在此基础上运用采购拍卖理论设计了 A_{FL} 拍卖框架，目标使社会成本最小化；文献[9]考虑客户端的信息新鲜度和服务延迟的权衡，并提出了一种基于合约理论的任务感知激励机制，根据客户端的数据更新成本设计奖励；文献[13]将客户端的历史信誉度作为其可靠性的衡量指标，并将信誉度与合约理论相结合设计了有效的激励机制，激励具有高质量数据和高信誉度的客户端参与 FL 任务。

与以往工作不同的是，本文根据 Chebyshev 定理将客户端的本地模型损失作为本地模型性能评估指标，并利用指数衰减函数评估其总体模型性能。同时，FL 任务的分配和定价问题被建模为多个逆向拍卖问题，以最大化本地模型性能为目标，该问题被证明是一个 NP-hard 问题，本文进一步设计了基于本地模型性能的逆向拍卖（local model performance based reverse auction，LPRA）算法，LPRA 算法在满足个体理性、真实性和计算高效性的同时能有效提高全局模型的收敛速度和精度。

1　系统综述

本文研究包含多个服务器、多个客户端和 1 个中间基站的联邦学习模型。设服务器集合为 $S=\{s_1,s_2,\cdots,s_M\}$，M 表示服务器数目；客户端集合为 $C=\{c_1,c_2,\cdots,c_N\}$，N 表示客户端数目。当 $M=3$、$N=8$ 时，系统模型如图 1 所示。在拍卖开始时，每个服务器都会向基站发布 1 个 FL 任务，基站作为拍卖商会为每个 FL 任务选择多个客户端参与，并决定最终的拍卖价格。然后客户端对各自分配的 FL 任务进行本地模型训练，步骤⑤～步骤⑧表示 1 轮本地模型迭代，通常为了达到所需的全局模型精度，每一次 FL 任务的步骤⑤～步骤⑧会重复执行多轮。在所有 FL 任务完成后，基站会向参与 FL 任务的客户端支付最终报酬，并开启下一次拍卖。

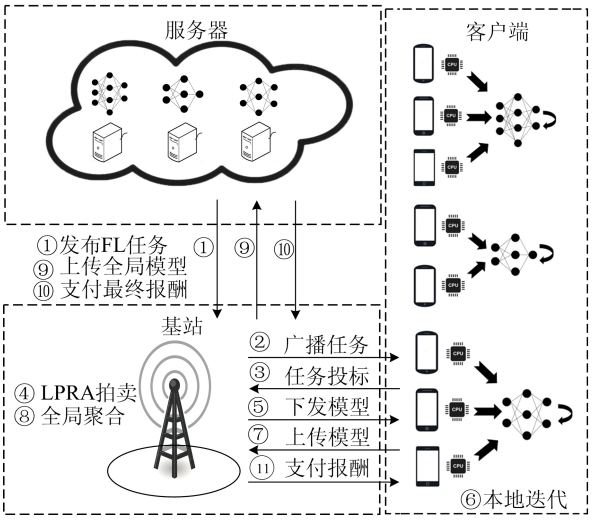


图 1　系统模型

1.1　本地模型性能评估

假设客户端 $c_i(i\in[1,N])$ 参与服务器 $s_j(j\in[1,M])$ 的 FL 任务，在第 t 轮本地迭代时，c_i 接收到的全局模型参数记为 ω_j^t。c_i 利用本地数据进行模型更新，更新后的本地模型参数记为 $\omega_{i,j}^{t+1}$。本地模型更新的目标是最小化其损失函数 $L(\omega_{i,j}^t)$，即

$$\omega_{i,j}^t=\arg\min L(\omega_{i,j}^t) \tag{1}$$

$$L(\omega_{i,j}^t)=(1/|D_i|)\sum_{h\in D_i}f_h(\omega_{i,j}^t) \tag{2}$$

其中：$f_h(\omega_{i,j}^t)$ 为客户端 c_i 的样本 h 在第 t 轮的损失函数；$|D_i|$ 为 c_i 的数据集 D_i 的样本数目。

在本地模型第 t 轮迭代完成后，客户端将本地模型参数发送给基站进行全局模型聚合，聚合后第 $(t+1)$ 轮的全局模型参数 ω_j^{t+1} 为：

$$\omega_j^{t+1}=(1/\mid D_j\mid)\sum_{c_i\in C_j}\mid D_j\mid\omega_{i,j}^t \tag{3}$$

其中:$|D_j|$为参与 s_j 模型训练的所有客户端的数据量总和;C_j 为参与服务器 s_j 本次任务的客户端集合。从式(3)可以看出,全局模型参数是所有参与训练的客户端按其贡献数据量的加权平均。全局聚合的目标是最小化全局模型的损失函数值,第 $t+1$ 轮全局聚合的损失函数 $L(\omega_j^{t+1})$定义为:

$$L(\omega_j^{t+1})=(1/\mid C_j\mid)\sum_{c_i\in C_j}L(\omega_{i,j}^t) \tag{4}$$

其中,$|C_j|$为参与 s_j 模型训练的客户端数目。基站收集到来自不同客户端的本地模型损失是一串未知分布的序列,其均值和标准差分别记为 μ、σ,根据式(4)可以得到 $\mu=L(\omega_j^{t+1})$。由切比雪夫定理可知,至少有 75%和 89%的客户端的本地损失分别位于全局损失的 2σ 和 3σ 范围以内。本文以 2σ 为阈值,将第 t 轮本地迭代中客户端 c_i 对服务器 s_j 全局模型的正反馈$\alpha_{i,j}^t$定义为:

$$\alpha_{i,j}^t=\begin{cases}1, & L(\omega_{i,j}^t)-L(\omega_j^{t+1})\leqslant 2\sigma;\\ 0, & L(\omega_{i,j}^t)-L(\omega_j^{t+1})>2\sigma\end{cases} \tag{5}$$

其中,$\alpha_{i,j}^t$为二进制变量。当本地损失小于全局损失,或者即使大于全局损失但差值在 2σ 以内时,认为在此轮本地迭代中客户端对全局模型起到促进作用,令 $\alpha_{i,j}^t=1$;否则,认为客户端的本地模型对全局模型起到抑制作用,令 $\alpha_{i,j}^t=0$。同时,将第 t 轮本地迭代中客户端 c_i 对服务器 s_j 全局模型的负反馈$\beta_{i,j}^t$定义为:

$$\beta_{i,j}^t=1-\alpha_{i,j}^t \tag{6}$$

通过收集每一轮本地迭代中客户端对全局模型的影响,可以得到在第 T 次 FL 任务中客户端正负反馈次数分别为:

$$\alpha_{i,j}^T=\sum_{t\in T_{i,j}^+}\alpha_{i,j}^t \tag{7}$$

$$\beta_{i,j}^T=\sum_{t\in T_{i,j}^-}\beta_{i,j}^t \tag{8}$$

其中,$T_{i,j}^+$、$T_{i,j}^-$分别表示正、负反馈的迭代轮集合。基于主观逻辑模型[13]可以得到:

$$\begin{cases}b_{i,j}^T=(1-u_{i,j}^T)\alpha_{i,j}^T/(\alpha_{i,j}^T+\beta_{i,j}^T),\\ d_{i,j}^T=(1-u_{i,j}^T)\beta_{i,j}^T/(\alpha_{i,j}^T+\beta_{i,j}^T),\\ u_{i,j}^T=1-q_{i,j}^T\end{cases} \tag{9}$$

其中,$u_{i,j}^T$表示在迭代过程中的不确定性,它与通信质量 $q_{i,j}^T$相关[14]。进一步将客户端 c_i 在第T 次拍卖中参与(唯一参与)服务器 s_jFL 任务的本地模型性能 p_i^T 定义为:

$$p_i^T=b_{i,j}^T+\theta u_{i,j}^T \tag{10}$$

其中,$\theta\in[0,1]$为超参数,表示不确定性对性能评估的影响。若 c_i 在发布的第 T 次 FL 任务中不参与任何任务,则 $p_i^T=0$。

在 FL 训练中,客户端的性能通常是不稳定的,对于时间间隔越短的历史信息被认为更具有参考价值,因此本文利用指数衰减函数来评估客户端在前 T 次 FL 中总体本地模型性能。具体来说,客户端 c_i 的总体本地模型性能 p_i 定义为:

$$p_i=\Big(\sum_{s=1}^{T}\rho^{T-s}p_i^s\Big)\Big/\Big(\sum_{s=1}^{T}\rho^{T-s}\Big) \tag{11}$$

其中,$\rho\in[0,1]$为损失因子,ρ 值决定客户端历史训练信息随时间衰减的程度。

本文假设不同服务器发布的 FL 任务是相近的,如不同的短视频运营商会共同需要移动设备为其训练用户的视频浏览偏好模型,其所需训练的网络模型是相似的。这意味着客户端为不同服务器执行 FL 任务的历史记录都能够用来评估其整体的本地模型性能。

1.2 激励机制设计

本文将客户端 $c_i(i\in[1,N])$在历史 FL 任务中本地模型性能 p_i 作为当前轮客户端本地模型训练性能的预测。进一步根据客户端和服务器的报价,设计基于逆向拍卖的激励算法来解决 FL 任务分配和定价问题,目的是激励更多高性能本地模型的客户端参与 FL 任务。

将多服务器、多客户端 FL 场景下的任务分配和定价问题公式化为:

$$\max\sum_{s_j\in S}\sum_{c_i\in C_j}p_i \tag{12}$$

$$\text{s.t.}\quad b_{i,j}'\geqslant b_{i,j},c_i\in C_j,s_j\in S \tag{13}$$

$$\sum_{c_i\in C_j}b_{i,j}'=b_j'\leqslant b_j,c_i\in C_j,s_j\in S \tag{14}$$

$$\sum_{j=1}^{M}x_{i,j}\leqslant 1,i\in[1,N] \tag{15}$$

$$x_{i,j}\in\{0,1\},i\in[1,N],j\in[1,M] \tag{16}$$

其中,C_j 表示参与服务器 s_jFL 任务的客户端集合。式(12)表示优化的目标是最大化参与 FL 任务的所有客户端的本地模型性能。式(13)、式(14)分别表示参与 FL 的客户端 c_i 获得的报酬 $b_{i,j}'$不低于其投标价格 $b_{i,j}$,服务器的最后支付 b_j'不高于其投标价格 b_j,式(13)、式(14)共同满足激励机制设计的个体理性要求。式(15)表示每一个客户端最多只能参与 1 个服务器的 FL 任务,其中 $x_{i,j}$为二进制变量。式(16)中,当 $x_{i,j}=1$ 时表示客户端 c_i 参与服务器 s_j 的 FL 任务;反之,$x_{i,j}=0$表示不参加。

上述优化问题实际上是一个多背包问题,将

客户端获得的报酬 $b_{i,j}'$ 等价于物品的质量；各服务器的支付报酬 b_j 等价于各背包的最大承重；每个客户端的本地模型性能等价于物品的价值，最大化所有参与 FL 客户端的本地模型性能等价于所有背包的物品价值总和最大化。多背包问题已经被证明是一个 NP-hard 问题，无法在多项式时间内找出上述问题的最优解。因此本文设计基于本地模型性能的启发式逆向拍卖算法进行求解。

输入：服务器的投标集合 $B^S=\{b_j \mid j\in[1,M]\}$；客户端的投标集合 $B^C=\{b_{i,j} \mid i\in[1,N],j\in[1,M]\}$；客户端的本地模型性能集合 $p=\{p_i \mid i\in[1,N]\}$。

输出：各服务器的实际支付集合 $B=\{b_j' \mid j\in[1,M]\}$，客户端获得的报酬矩阵 $\boldsymbol{L}=(b_{i,j})_{N\times M}$。

1. 初始化 $b_{i,j}'\leftarrow 0(i\in[1,N],j\in[1,M])$；$x_{i,j}\leftarrow 0$；$\boldsymbol{L}\leftarrow \boldsymbol{0}$；$B\leftarrow 0$
2. 将服务器的投标价格按降序排序得 $\hat{B}^S=\{b_{j_1},\cdots,b_{j_M}\}$
3. l 从 1 到 M：
4. 　假设有 h 个客户端对服务器 S_{j_l} 投标，对每个客户端计算 $p_{i_z,j_l}/b_{i_z,j_l}(z\in[1,h])$ 并降序排序：$\{p_{i_1,j_1}/b_{i_1,j_1},\cdots,p_{i_h,j_h}/b_{i_h,j_h}:\}$
5. 　k 从 2 到 h：
6. 　　$b_{j_l}'=\sum_{s=1}^{k-1}[p_{i_s,j_l}(b_{i_k,j_l}/p_{i_k,j_l})]$
7. 　　如果 $b_{j_l}'>b_{j_l}$：
8. 　　取前$(k-2)$个客户端作为拍卖赢家
　　s 从 1 到$(k-2)$：
9. 　　计算中标客户端报酬：$b_{i_s,j_l}'=p_{i_s,j_l}\cdot(b_{i_{k-1},j_l}/p_{i_{k-1},j_l})$
10. 　　计算服务器最终支付：$b_{j_l}'=b_{j_l}'+b_{i_s,j_l}'$
11. 　　$x_{i_s,j_l}\leftarrow 1$
12. 　　中标的客户端不会再中其他标：
　　$b_{i_s,q}\leftarrow 0,q\in[1,M]$且 $q\neq j_l$
13. 　终止循环
14. 返回 $\boldsymbol{L}$、B

LPRA 算法优先为投标价格高的服务器(第 2 行)分配客户端(第 3～13 行)。计算每个投标客户端的性价比 $p_{i_z,j_l}/b_{i_z,j_l}(z\in[1,h])$，并优先选择性价比高的客户端。记第 k 个客户端为第 1 个不中标的客户端，计算前 $k-1$ 个客户端的总预算(第 6 行)，若超过服务器投标价格，则取前$(k-2)$个客户端中标，再分别计算中标客户端的最终报酬(第 9 行)和服务器的最终支付(第 10 行)，最后将中标客户端的其他投标变成 0(第 12 行)。需要注意的是，客户端本地模型性能的更新发生在每次 FL 任务完成之后。

2　理论分析

本节从理论上证明所设计的 LPRA 算法满足参与者的个体理性、拍卖的真实性和计算高效性。

定理 1　LPRA 算法满足客户端和服务器的个体理性。

证明　个体理性是指拍卖的参与者在拍卖中获得的收益非负。客户端和服务器作为理性的个体，只有当其收益非负时才会自愿参与 FL 任务。特别地，对于中标客户端，其最终获得的报酬须不低于其投标价格；对于服务器，其最终支付的报酬须不高于其投标价格。

对于客户端 $c_{i_s}(i_s\in[1,N])$。若 c_{i_s} 不中标，则其获得的报酬和训练成本均为 0，满足其个体理性；若 c_{i_s} 中标，且 $x_{i_s,j_l}=1$，则根据 LPAR 算法的第 4 行可得：

$$\frac{p_{i_s,j_l}}{b_{i_s,j_l}}\geqslant\frac{p_{i_k,j_l}}{b_{i_k,j_l}} \tag{17}$$

$$b_{i_s,j_l}\leqslant p_{i_s,j_l}(b_{i_k,j_l}/p_{i_k,j_l}) \tag{18}$$

根据 LPRA 算法的第 9 行可得：

$$b_{i_s,j_l}\leqslant p_{i_s,j_l}(b_{i_{k-1},j_l}/p_{i_{k-1},j_l})=b_{i_s,j_l}' \tag{19}$$

由式(19)可知，中标客户端 c_{i_s} 获得的最终报酬 b_{i_s,j_l}' 不低于其投标价格 b_{i_s,j_l}。因此 LPRA 算法满足客户端的个体理性。

对于服务器 $s_{j_l}(j_l\in[1,M])$，根据算法的第 6、第 7 行可得：

$$b_{j_l}'=\sum_{s=1}^{k-1}[p_{i_s,j_l}(b_{i_k,j_l}/p_{i_k,j_l})]>b_{j_l} \tag{20}$$

此时 k 值刚好使得 $b_{j_l}>b_{j_l}'$。根据算法第 8～13 行，取前$(k-2)$个客户端作为拍卖赢家，得到：

$$b_{j_l}'=\sum_{s=1}^{k-2}[p_{i_s,j_l}(b_{i_{k-1},j_l}/p_{i_{k-1},j_l})]\leqslant b_{j_l} \tag{21}$$

由式(21)可知，服务器 s_{j_l} 的最终支付 b_{j_l}' 不高于其投标价格 b_{j_l}。因此 LPRA 算法满足服务器的个体理性。

定理 2　LPRA 算法满足真实性。

证明　真实性是指在拍卖中客户端不能通过提交虚假的投标报价来提高所获得的报酬。假设客户端 $c_{i_s}(i_s\in[1,N])$ 对服务器 $s_{j_l}(j_l\in[1,M])$ 的真实投标价格为 b_{i_s,j_l}(b_{i_s,j_l} 可以认为是 c_{i_s} 的成本价或者最低接受价格)，虚假投标价格为 $\tilde{b}_{i_s,j_l}$，且虚假投标获得的报酬为 $\tilde{b}_{i_s,j_l}'$。此时，分为如下 4 种情况：

1) 若 b_{i_s,j_l} 不中标，$\tilde{b}_{i_s,j_l}$ 不中标，则有 $b_{i_s,j_l}'=$

$\tilde{b}_{i_s,j_l}'=0$。

2) 若 b_{i_s,j_l} 中标，$\tilde{b}_{i_s,j_l}$ 不中标，则有 $b_{i_s,j_l}'=p_{i_s,j_l}(b_{i_{k-1},j_l}/p_{i_{k-1},j_l})>\tilde{b}_{i_k,j_l}'=0$。

3) 若 b_{i_s,j_l} 中标，$\tilde{b}_{i_s,j_l}$ 中标，根据算法第 9 行，中标客户端获得的报酬与其投标价格无关，则有 $b_{i_s,j_l}'=p_{i_s,j_l}(b_{i_{k-1},j_l}/p_{i_{k-1},j_l})=\tilde{b}_{i_s,j_l}'$。

4) 若 b_{i_s,j_l} 不中标，$\tilde{b}_{i_s,j_l}$ 中标，则有 $\tilde{b}_{i_s,j_l}<b_{i_s,j_l}$；当投标价格为 $\tilde{b}_{i_s,j_l}$ 时，c_{i_s} 获得的报酬为 $\tilde{b}_{i_s,j_l}=p_{i_s,j_l}(b_{i_{k-1},j_l}/p_{i_{k-1},j_l})$，不高于其成本 b_{i_s,j_l}，客户端的实际收益非正，不满足其个体理性。因此，这种情况不成立。

综上所述，LPRA 算法满足真实性。

定理 3 LPRA 算法满足计算高效性，且计算复杂度为 $O(M^2N^2)$。

证明 计算高效性是指所设计的拍卖算法是轻量级的，即计算时间复杂度为多项式级的。在 LPRA 算法中，主循环(第 3～第 13 行)一共执行 M 次，第 2 重循环(第 5～第 13 行)为选择中标客户端最多执行 N 次，第 3 重循环(第 8～第 12 行)为每一个中标客户端定价最多执行 N 次，将中标客户端的其他投标设为(第 12 行)最多执行 M 次。因此，LPRA 算法的计算复杂度为 $O(M^2N^2)$，满足算法的计算高效性。

3 实验验证

本节对所设计的 LPRA 算法的性能进行实验验证。FL 仿真系统采用 Pytorch 3.6.2 环境搭建，各参数的设置见表 1 所列。FL 训练的模型采用 MLP 网络，训练的数据集采用 MNIST，M、N 分别为服务器和客户端的数目，投标价格 b_j、$b_{i,j}$ 均服从均匀分布 U。为了能够筛选更多高性能的客户端参与 FL 任务以验证 LPRA 算法的有效性，实验中客户端的数目 N 是设置充足的。

表 1 实验参数设置

实验	M	N	b_j	$b_{i,j}$
1	4	100	$U(40,50)$	$U(2,5)$
2	2	30	$U(20,30)$	$U(2,5)$

首先，实验 1 验证了所设计的 LPRA 算法满足个体理性和真实性。中标客户端的投标价格和最终报酬的比较如图 2 所示，所有服务器的投标价格和最终支付价格的比较如图 3 所示。从图 2、图 3 分别可以看出，每一个中标客户端获得的最终报酬都高于其投标价格，每一个服务器的最终支付价格都低于其投标价格。因此，LPRA 算法满足客户端和服务器的个体理性。

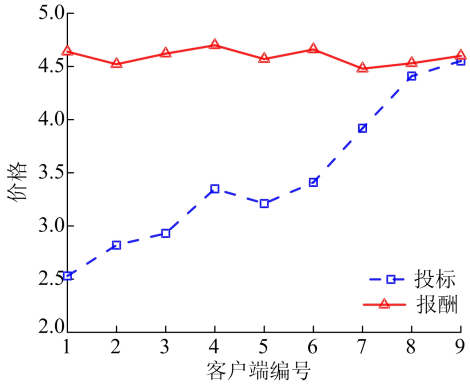


图 2 中标客户端的投标价格与最终报酬比较

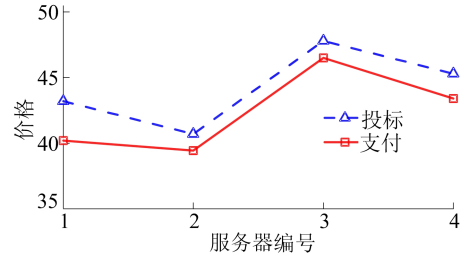


图 3 各服务器的投标价格与最终支付价格比较

其次，实验 1 还验证所设计 LPRA 算法满足客户端投标的真实性。客户端在不同投标价格下获得的最终报酬如图 4 所示。

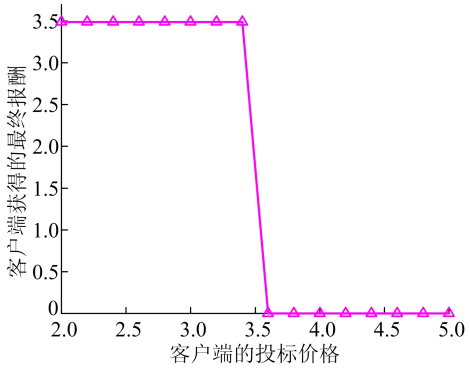


图 4 客户端获得的最终报酬随其投标价格变化

从图 4 可以看出，随着客户端的投标价格增加，其拍卖获得的报酬首先为一定值，而当投标价格超过某个值时，其获得的报酬均变为 0。原因如下：根据 LPRA 算法，当投标价格较低时，客户端均能中标，且获得的报酬与其投标价格无关，而当投标价格超过某个值时，客户端将不会中标，其获得的报酬为 0。因此客户端只有提供真实的投标价格才能使其获得的报酬最大化。

实验 2 首先将所设计的 LPRA 算法与其他 3 种算法进行比较。

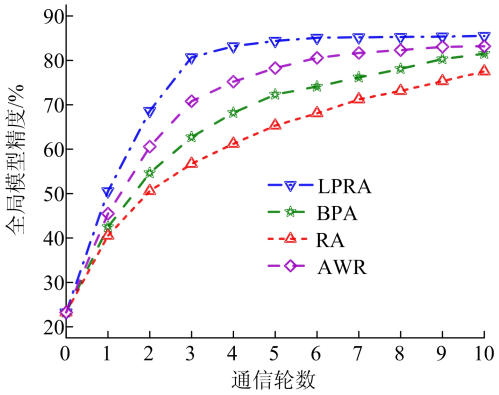
1）随机分配（RA）。在服务器预算内，随机分配客户端参与其 FL 任务，并以客户端的投标价格作为最终报酬价格。

2）按投标价格分配（BPA）。在服务器预算内，优先选择投标价格低的客户端分配 FL 任务，并以客户端的投标价格作为最终报酬价格。

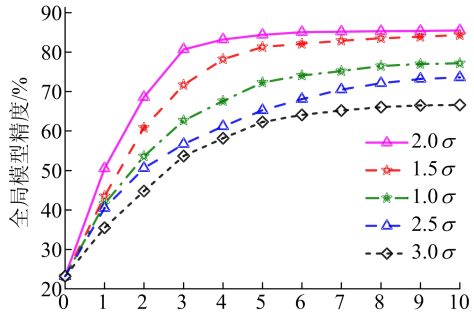
3）拍卖赢家选择算法（AWR）。文献[15]假设所有客户端都会诚实地提供数据量大小、计算资源以及需求等信息，中央控制器据此计算每个参与者的获胜分数 R_{win} 以确定中标客户端和最终报酬 R_{rwd}。

不同分配算法下全局模型精度比较如图 5a 所示。从图 5a 可以看出，随着客户端与服务器通信轮数（即本地模型训练和全局聚合次数）的增加，4 种分配算法下的全局模型精度在不断提升，其中，LPRA 算法下的全局模型收敛速度最快，且在 5 轮通信后基本收敛，而 AWR、BPA 和 RA 算法下全局模型收敛较慢。原因是 LPRA 算法会优先选择本地模型性能高的客户端参与 FL 任务，高质量的本地模型能加快全局模型的速度，同时提高全局模型精度。AWR 没有考虑客户端的本地模型性能以及历史性能，不能充分选择更优质的客户端参与 FL 任务，且 AWR 默认客户端都是诚实的，而实际上客户端可以提供虚假的信息以换取更高回报。BPA 可以选择比 RA 更多的客户端参与 FL 任务，训练数据量的增加会让 BPA 比 RA 收敛速度略快一些，但 BPA 和 RA 并不能筛选客户端，低性能的本地模型会抑制全局模型的收敛。因此，所提出的 LPRA 算法能激励更多高性能的本地客户端参与 FL 任务。

实验 2 还比较了式(5)中不同阈值下的全局模型精度，如图 5b 所示。从图 5b 可以看出：当阈值设置为 2.0σ 时，全局模型性能最高；即模型收敛最快且精度最高，当阈值设置为 1.5σ 时，全局模型性能略低于 2.0σ 时的效果；当阈值设置为 1.0σ、2.5σ、3.0σ 时，全局模型性能进一步降低。原因如下：当阈值设置较大时，如 2.5σ、3.0σ 等，会有更多低性能的本地迭代被认为是正反馈，在拍卖中这些客户端会更有可能中标，低性能的客户端参与 FL 任务最终导致全局模型性能的降低；当阈值设置较小时，如 1.0σ、1.5σ 等，会导致更少的客户端本地迭代被认为是正反馈，无法筛选出高性能的本地模型也不利于全局模型性能的提升。因此，本文通过实验发现当阈值取为 2.0σ 时，全局模型的性能达到最大化。



(a) 不同分配算法



(b) 不同阈值

图 5　不同分配算法、不同阈值下全局模型精度比较

4　结　　论

本文研究在多服务器、多客户端参与的 FL 场景中的激励机制，并将任务分配和定价问题建模为多个逆向拍卖问题。首先根据切比雪夫定理对客户端每一轮的本地模型性能进行评估，并进一步利用指数衰减函数对其总体性能进行评估；然后根据评估结果以及双方的投标价格设计基于逆向拍卖的 LPRA 算法，目标使得参与 FL 任务的客户端的本地模型性能最大化。本文从理论上证明 LPRA 算法满足个体理性、真实性以及计算高效性；最后通过仿真实验验证 LPRA 算法的高效性。

[参　考　文　献]

[1] LUETH K. State of the IoT 2018：number of IoT devices now at 7B-market accelerating [EB/OL]. [2023-02-20]. https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/.

[2] LECUN Y, BENGIO Y, HINTON G. Deep learning[J]. Na-

ture,2015,521(7553):436-444.

[3] 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.

[4] ZHOU R,PANG J,WANG Z,et al. A truthful procurement auction for incentivizing heterogeneous clients in federated learning[C]//2021 IEEE 41st International Conference on Distributed Computing Systems (ICDCS). [S. l.]:IEEE,2021:183-193.

[5] CHENG Z,LIWANG M,XIA X,et al. Auction-promoted trading for multiple federated learning services in UAV-aided networks[J]. IEEE Transactions on Vehicular Technology,2022,71(10):10960-10974.

[6] MAI T,YAO H,XU J,et al. Automatic double-auction mechanism for federated learning service market in internet of things[J]. IEEE Transactions on Network Science and Engineering,2022,9(5):3123-3135.

[7] LIM W Y B,XIONG Z,MIAO C,et al. Hierarchical incentive mechanism design for federated machine learning in mobile networks[J]. IEEE Internet of Things Journal,2020,7(10):9575-9588.

[8] YE D,YU R,PAN M,et al. Federated learning in vehicular edge computing:a selective model aggregation approach[J]. IEEE Access,2020,8:23920-23935.

[9] LIM W Y B,XIONG Z,KANG J,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.

[10] FENG S,NIYATO D,WANG P,et al. Joint service pricing and cooperative relay communication for federated learning [C]//2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber,Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). [S. l.]:IEEE,2019:815-820.

[11] SARIKAYA Y,ERCETIN O. Motivating workers in federated learning:a stackelberg game perspective[J]. IEEE Networking Letters,2020,2(1):23-27.

[12] LIM W Y B,NG J S,XIONG Z,et al. Decentralized edge intelligence: a dynamic resource allocation framework for hierarchical federated learning[J]. IEEE Transactions on Parallel and Distributed Systems,2022,33(3):536-550.

[13] KANG J,XIONG Z,NIYATO D,et al. Incentive mechanism for reliable federated learning: a joint optimization approach to combining reputation and contract theory[J]. IEEE Internet of Things Journal,2019,6(6):10700-10714.

[14] CHEN M,POOR H V,SAAD W,et al. Performance optimization of federated learning over mobile wireless networks[C]//2020 IEEE 21st International Workshop on Signal Processing Advances in Wireless Communications (SPAWC). [S. l.]:IEEE,2020:1-5.

[15] SEO E,NIYATO D,ELMROTH E. Auction-based federated learning using software-defined networking for resource efficiency[C]//2021 17th International Conference on Network and Service Management (CNSM). [S. l.]:IEEE,2021:42-48.

(责任编辑 张 锴)

(上接第 1485 页)

[8] 周雪莹,张文超,胡志毅,等. 基于深度学习的量子比特噪声谱解析[J]. 量子光学学报,2022,28(3):200-207.

[9] DENG L,YU D. Deep learning:methods and applications [J]. Foundations and Trends® in Signal Processing,2013,7(3/4):197-387.

[10] HE F,LIU T,TAO D. Why resnet works? residuals generalize[J]. IEEE Transactions on Neural Networks and Learning Systems,2020,31(12):5349-5362.

[11] HOSNY K M,KASSEM M A,FOUAD M M. Classification of skin lesions into seven classes using transfer learning with AlexNet[J]. Journal of Digital Imaging,2020,33(5):1325-1334.

[12] TAMMINA S. Transfer learning using vgg-16 with deep convolutional neural network for classifying images[J]. International Journal of Scientific and Research Publications (IJSRP),2019,9(10):143-150.

[13] GONZALEZ R C. Deep convolutional neural networks [Lecture Notes][J]. IEEE Signal Processing Magazine,2018,35(6):79-87.

[14] ZHAN Q. Cylindrical vector beams: from mathematical concepts to applications[J]. Advances in Optics and Photonics,2009,1(1):1-57.

[15] JAIS I K M,ISMAIL A R,NISA S Q. Adam optimization algorithm for wide and deep neural network[J]. Knowledge Engineering and Data Science,2019,2(1):41-46.

(责任编辑 张 锴)