

Incentive-Aware Federated Learning with Training-Time Model Rewards

摘要

在联邦学习中，激励潜在竞争客户贡献训练资源（例如数据和计算资源）至关重要。现有的激励机制通常在训练后分发货币奖励，但这种方式在实际操作中面临及时性和可行性的挑战。在训练完成后给予奖励可能会导致客户中途放弃合作，而将贡献货币化在实践中也具有一定的难度。为了解决这些问题，我们提出了一种激励感知算法，该算法在每次 FL 迭代中为每个客户提供差异化的训练阶段模型奖励。我们通过理论证明，这种局部设计可以确保客户激励的全局目标。通过理论分析，我们进一步发现了模型奖励中的误差传播问题，并提出了一种随机参考模型恢复策略，从理论上保证所有客户最终都能在极限情况下获得最优模型。我们进行了大量实验，证明了我们方法在激励性能方面优于现有的基线方法。

关键词：联邦学习；激励机制

1 引言

1.1 选题背景

随着人工智能和大数据技术的快速发展，联邦学习因其在数据隐私保护和分布式计算中的突出优势而逐渐成为热门研究领域。在 FL 中，多个分散的客户端（如智能设备或机构）在不共享数据的情况下协同训练模型。这一分布式学习范式不仅提升了数据隐私，还解决了集中化数据收集带来的成本和效率问题。然而，FL 的成功依赖于客户端贡献的高质量资源（例如数据和计算能力）。由于这些资源通常属于独立且可能具有竞争关系的个体或组织，如何激励客户端持续、高效地参与训练成为了 FL 落地应用的关键挑战。

1.2 选题依据

当前主流的激励机制通常在训练结束后对客户端进行货币化奖励。然而，这种方法存在以下问题：

1. 时效性不足：训练完成后的奖励可能无法及时反馈，降低了客户端的参与热情。
2. 可行性受限：在实际应用中，对资源贡献进行货币化定价并非易事，尤其是在跨区域或跨领域的合作中。

3. 协作风险：由于奖励的滞后性，部分客户端可能在训练过程中中途退出，从而影响全局模型的性能和收敛性。

针对上述问题，有必要研究一种能够实时激励客户端参与的机制，同时确保全局训练目标的有效实现。

1.3 选题意义

本研究的意义主要体现在以下几个方面：

1. 理论创新：提出一种差异化的训练阶段模型奖励机制，从理论上证明了这种局部设计能够实现全局激励目标，填补了现有激励机制在实时性和可行性上的不足。
2. 实践推动：通过理论分析发现并解决了模型奖励中的误差传播问题，进一步设计了随机参考模型恢复策略，确保所有客户端最终能获得最优模型。这一创新对 FL 的实际部署具有重要指导意义。
3. 性能提升：通过实验验证，所提出的方法在激励效果方面显著优于现有基线方法，为 FL 领域的激励机制研究提供了新的方向。

总体而言，本研究从理论和实践两个层面为 FL 的激励机制设计提供了新的思路，不仅增强了 FL 的协作效能，还为其在多领域的实际应用奠定了坚实基础。

2 相关工作

2.1 联邦学习激励机制设计

在联邦学习 (FL) 激励机制的设计中，常用的建模工具包括斯塔克尔伯格博弈 (Stackelberg games) [2]、拍卖 (auction) [15] 和契约理论 (contract theory) [7]。这些方法均采用训练后货币激励方案来激励客户端的贡献 [14]。Karimireddy 等人提出了通过噪声模型扰动实现的不同效用的训练后模型奖励。然而，由于客户端在 FL 过程中已经通过模型广播获得了最佳全局模型，这种方法可能不适用于 FL。相比之下，我们的研究直接将激励机制集成到 FL 算法中，采用训练阶段的模型奖励。

2.2 异构性与个性化联邦学习

分布式客户端之间的数据异构性是 FL 中的一个常见挑战 [1]。诸如 FedProx [6] 和 FedNova [11] 等方法通过训练单个共享模型来调整因异构本地数据分布而导致的客户端目标不匹配问题。而个性化联邦学习则为每个客户端生成个性化模型，重点提升其本地测试集的性能 [10]。个性化模型的实现通常通过对共享模型的层或结构进行个性化调整 [9]。与之不同，我们的研究专注于通过优化具有数据异构性的共享全局目标来定制客户端模型奖励。例如，即使一个客户端仅拥有 MNIST 数据集中数字 0-9 的样本，其仍然希望获得一个能够分类所有数字的模型。

2.3 联邦学习中的训练阶段模型激励

CGSV [13] 和 Rank [3] 已经探讨了联邦学习中训练阶段的模型激励。然而，这些启发式方法缺乏理论上的收敛性分析。此外，Rank 方法假设能够访问一个验证集来对本地模型性能进行排名以供聚合，但这一假设在实际中难以实现。CGSV 方法的视角与我们的研究形成了对比：CGSV 对所有客户端的部分模型更新参数值置零，而我们的 IAFL 方法对所有参数值的部分客户端模型更新置零。我们的聚合方法更符合 FL 中部分客户端参与的设置 [6]。此外，CGSV 的本地性能保证无法推广到整个 FL 训练的全局激励目标。

3 本文方法

3.1 本文方法概述

本文提出了一种名为激励感知联邦学习 (IAFL) 的新算法，具体流程如图1该算法通过根据客户端在每轮联邦学习迭代中的贡献，动态地为每个客户端分配差异化的训练时间模型奖励，从而实现对客户端的有效激励。IAFL 通过衡量客户端的本地模型更新质量来调整奖励分配，并从理论上证明了该奖励机制能够在激励公平性和全局收敛性之间实现平衡，确保联邦学习的全局激励目标和渐近收敛特性。

此外，作者发现了联邦学习中的错误传播问题，即低质量本地模型更新可能对高质量模型造成负面影响。为此，提出了一种随机参考模型恢复策略，在每轮迭代中以一定概率为客户端提供恢复模型，从而减缓错误传播，确保所有客户端最终能够获得接近全局最优的模型。

在广泛的实验中，IAFL 在多种异构数据划分条件下均表现出卓越的性能。实验结果表明，IAFL 不仅能显著提高客户端的激励参与度，还能在平均模型性能和激励公平性之间取得更优的平衡，尤其在具有标签分布不平衡等挑战性场景下具有显著优势。本文方法具有以下四个主要贡献：

1. 差异化模型奖励：IAFL 根据客户端贡献分配训练时间模型奖励，动态激励客户端参与，提高联邦学习的有效性。
2. 理论保障：提供严格的理论证明，确保局部奖励策略能够实现客户端激励的全局目标和模型的渐近收敛性。
3. 错误传播问题及解决：针对低贡献客户端引发的错误传播，提出随机参考模型恢复策略，显著提高了全局模型的鲁棒性和性能。
4. 实验验证：大量实验表明，IAFL 在多种异构数据划分条件下，尤其在标签分布不平衡场景中，表现出更高的激励性能和更优的模型质量。

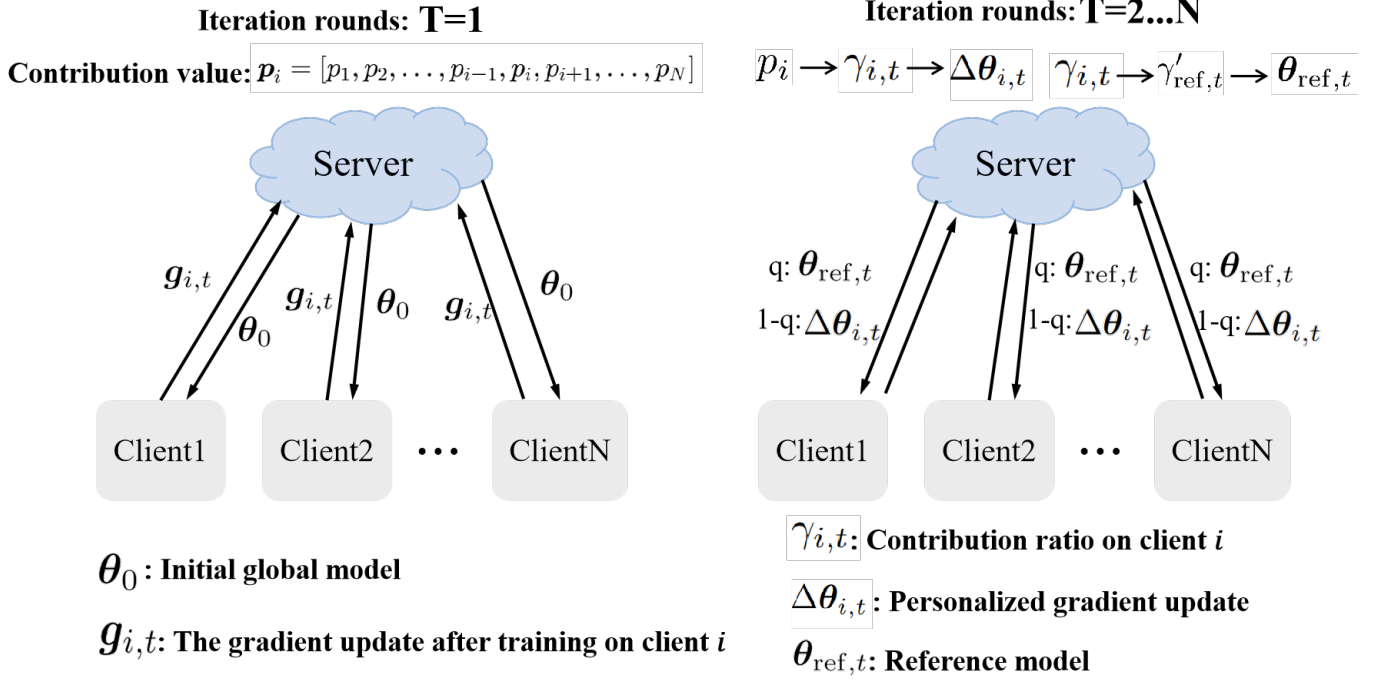


图 1. 流程图

4 激励机制

在联邦学习 (FL) 中, 客户端的参与与贡献程度直接影响全局模型的训练效果。然而, 由于现有标准联邦学习机制的奖励设计较为简单, 所有客户端无论贡献多少都能获得相同的全局模型更新, 导致激励机制的缺失。为了解决这一问题, 本文提出了一种基于贡献的奖励机制, 从理论和实践两方面重新定义了客户端的激励方式。

4.1 奖励机制设计

奖励机制旨在通过贡献向量 $p = [p_1, p_2, \dots, p_N]$ 来计算每个客户端的奖励值 $[M_\nu(p)]_i$ 。传统联邦学习机制下, 全局模型的聚合函数 $h(p_{-i})$ 仅依赖于其他客户端的贡献 p_{-i} , 这意味着客户端的自身贡献 p_i 不会影响其最终获得的奖励。为了解决这一问题, 本文设计了一个新的聚合函数 $\tilde{h}(p_i, p_{-i})$, 使聚合结果同时依赖于客户端的自身贡献和其他客户端的贡献。奖励机制定义如下:

$$[M_\nu(p)]_i = \nu \left(p_i, \left(\min \left\{ \frac{p_i}{p_{\text{ceil}}}, 1 \right\} \right)^{1-\kappa} h(p_{-i}) \right)$$

其中:

- p_i : 客户端 i 的贡献程度, 可通过计算参与率、计算资源投入或其他指标量化。
- p_{ceil} : 贡献上限值, 限制了极端贡献带来的影响。
- $\kappa \in [0, 1]$: 共享系数, 用于调节奖励的公平性。
- $h(p_{-i})$: 表示其他客户端贡献的聚合结果, 可解释为局部模型更新的平均值。

4.1.1 机制的作用

1. 贡献与奖励正相关：奖励机制通过函数设计确保客户端的贡献程度 p_i 与其获得的奖励 $[M_\nu(p)]_i$ 呈正相关关系。即贡献越高的客户端将享受到更优质的奖励。
2. 避免不良均衡：为了防止客户端通过“低贡献”达成均衡（即所有客户端贡献相近但整体贡献不足的情况），本文提出的奖励机制引入了 p_{ceil} 和 κ 的联合设计。一方面，较高的 p_{ceil} 提供了较大的贡献激励空间，另一方面，较大的 κ 提高了低贡献客户端的参与动力。
3. 平衡高低贡献客户端：奖励机制不仅激励高贡献客户端继续投入，还通过调节共享系数 κ 鼓励低贡献客户端提高参与率，从而实现整体效率和公平性的平衡。

4.1.2 激励机制的理论条件

为了保证激励机制的有效性，本文提出了以下两个关键条件：

1. 贡献影响聚合结果

$$\frac{\partial \tilde{h}(p_i, p_{-i})}{\partial p_i} > 0$$

该条件确保客户端自身贡献增加会提高其从其他客户端聚合结果中获益。

2. 聚合结果影响奖励

$$\frac{\partial \nu(p_i, \tilde{h}(p_i, p_{-i}))}{\partial \tilde{h}(p_i, p_{-i})} > 0$$

该条件确保客户端通过提升整体贡献水平可以获得更高奖励。

这两个条件结合，揭示了奖励机制的激励作用，客户端在提升自身贡献的同时，也间接推动了整体模型的优化。

4.1.3 个体理性 (Individual Rationality, IR)

定义：一个奖励机制 $M_\nu(p)$ 满足个体理性 (Individual Rationality, IR)，如果任意客户端 i 的奖励满足：

$$[M_\nu(p)]_i \geq \nu(p_i, h(0)), \quad \forall i, p$$

即客户端至少可以获得与单独训练自身模型相当的奖励。

意义：个体理性条件的满足确保了所有理性客户端均愿意参与联邦学习，因为参与后获得的奖励总是大于或等于其单独工作时的收益。

本文机制的优势：提出的奖励机制在设计上天然满足个体理性条件，确保客户端不仅能够获得相应的奖励，还能因参与联邦学习而提升自身模型的性能。

4.2 随机参考模型恢复策略

受博弈论启发，该论文提出客户端可以聚合的局部模型更新比例应与其在每次 FL 迭代中的贡献相匹配，从而作为局部奖励。因此，客户端接收到的模型不同（每个模型使用特定比例的局部模型更新进行聚合），使得高贡献的客户端获得从更多局部模型更新中聚合的模型。论文证明了这种局部奖励方案确保高贡献的客户端能够获得一个具有更好性能保证的最终模型。然而，观察到来自性能边界的一个不良现象——误差传播：低贡献的客户端可能会恶化每个客户端的模型，因为聚合低质量的模型更新可能会对高质量模型产生不利影响。

在训练时的局部奖励方案确保高贡献的客户端能够获得一个具有更好性能保证的最终模型。进一步地，本文提出了一种随机参考模型恢复策略，以缓解理论上观察到的误差传播问题，并确保随着 $T \rightarrow \infty$ ，客户端模型渐进收敛到全局最优解。为了简化分析，我们考虑了全体客户端参与的情况，结果可以根据 Li 等人（2020d）的方法扩展到部分客户端参与的情形。论文定义了一个诱导奖励率 $\gamma'_{i,t} = \gamma_{i,t} - (\gamma_{i,t} - 1)/N$ ，它表示客户端 i 在 FL 迭代 t 中使用的局部模型更新的比例。

为了确保收敛到全局最优解，论文提出了一种随机恢复策略，该策略以概率 q 将当前参考模型共享给客户端。参考模型可以具有自定义的诱导参考奖励率 γ'_{ref} 。具体而言，参考模型通过聚合局部模型更新 $\{\mathbf{g}_{i,t}\}_{i \in \mathcal{S}_{\text{ref},t}}$ 来训练，其中 $\mathcal{S}_{\text{ref},t}$ 是从 $[N]$ 中随机抽样得到的，使得 $|\mathcal{S}_{\text{ref},t}| = \lceil \gamma'_{\text{ref},t} N \rceil$ 。因此，在每次 FL 迭代中，每个参与的客户端都有一个相等的概率 q 接收到当前的参考模型。以概率 $1 - q$ ，客户端仍然从服务器接收到一个更新，该更新是通过聚合相应比例的局部模型更新得到的。下面算法图概述了该实现过程。如以下定理所示，这种方法可以防止持续的误差传播，并使模型收敛。IAFL 的具体算法流程如图2。

定理 1（改进的界限）。设 $\eta_t = \frac{\beta}{t+\alpha}$ ，对于一个随机恢复率为 q 的情况，客户端模型 $\boldsymbol{\theta}_{i,T}$ 在经过 T 次 FL 迭代后的性能有如下界限：

$$\begin{aligned} \mathbb{E}[F(\boldsymbol{\theta}_{i,T})] - F^* &\leq \frac{L}{2} \left(\prod_{t=1}^T (1 - 2\mu\eta_t\tau) \right) \|\boldsymbol{\theta}_1 - \boldsymbol{\theta}^*\|^2 + \frac{L}{2} \sum_{t=1}^T \eta_t^2 (Q + D_t + E_t) \prod_{l=t+1}^T (1 - 2\mu\eta_l\tau) \\ D_T &= \frac{H_T}{N} \sum_{m=1}^N \sum_{t=1}^T \left(\frac{T+\alpha}{t+\alpha} \right)^2 \left(\frac{1}{\gamma'_{m,t}} + \frac{1}{\gamma'_{\text{ref},t}} - 2 \right) (1-q)^{T-t+1} \\ E_T &= H_T \sum_{t=1}^T \left(\frac{T+\alpha}{t+\alpha} \right)^2 \left(\frac{1}{\gamma'_{i,t}} + \frac{1}{\gamma'_{\text{ref},t}} - 2 \right) (1-q)^{T-t+1}. \end{aligned}$$

命题 1（渐近收敛）。如果 $\frac{1}{\gamma'_{i,t}} = o\left(\frac{t^2}{\log t}\right)$ 对于所有 $i \in [N]$ 以及 $\frac{1}{\gamma'_{\text{ref},t}} = o\left(\frac{t^2}{\log t}\right)$ ，则

$$\lim_{T \rightarrow \infty} \mathbb{E}[F(\boldsymbol{\theta}_{i,T})] - F^* = 0.$$

Algorithm 1: Incentive-Aware Federated Learning

```

1 Initialize  $\theta_{i,0} = \theta_{\text{ref},0} = \theta_0$  and  $g_{i,0} = 0$ ;
2 for  $t = 1$  to  $T$  do
3   Perform Procedure 2 such that
      $\{\Delta\theta_{i,t-1}\}_{i=1}^N, \theta_{\text{ref},t-1} = \text{ServerAgg}(t-1)$ ;
4   foreach client  $i$  do
5     with probability  $q$  do
6       Server shares  $\theta_{\text{ref},t-1}$  with client  $i$ ;
7        $\theta_{i,t} = \theta_{\text{ref},t-1}$ ;
8     else
9       Server shares  $\Delta\theta_{i,t-1}$  with client  $i$ ;
10       $\theta_{i,t} = \theta_{i,t-1} + \Delta\theta_{i,t-1}$ ;
11       $\theta_{i,t}^{\tau+1} = \theta_{i,t} - \eta_t \sum_{j=1}^{\tau} \nabla F_i(\theta_{i,t}^j, \xi_{i,t}^j)$ ;
12      Upload the local update  $g_{i,t} = \theta_{i,t}^{\tau+1} - \theta_{i,t}$ ;

```

Procedure 2: ServerAgg(t)

```

1 foreach client  $i$  do
2   Compute
      $\gamma_{i,t} = \min \left\{ (p_{i,t}/p_{\text{ceil}})^{1-\kappa}, 1 \right\}$ ;
3   Sample  $\mathcal{S}'_{i,t} \subseteq \{j : j \in [N], j \neq i\}$ 
     randomly s.t.
      $|\mathcal{S}'_{i,t}| = \lceil \gamma_{i,t}(N-1) \rceil$ ;
4   Include client  $i$ 's update
      $\mathcal{S}_{i,t} = \{i\} \cup \mathcal{S}'_{i,t}$ ;
5    $\Delta\theta_{i,t} = \frac{1}{|\mathcal{S}_{i,t}|} \sum_{j \in \mathcal{S}_{i,t}} g_{j,t}$ ;
6 Sample  $\mathcal{S}_{\text{ref},t} \subseteq [N]$  randomly such that
      $|\mathcal{S}_{\text{ref},t}| = \lceil \gamma'_{\text{ref},t} N \rceil$ ;
7  $\theta_{\text{ref},t} = \theta_{\text{ref},t-1} + \frac{1}{|\mathcal{S}_{\text{ref},t}|} \sum_{j \in \mathcal{S}_{\text{ref},t}} g_{j,t}$ ;
8 return  $\{\Delta\theta_{i,t}\}_{i=1}^N, \theta_{\text{ref},t}$ 

```

图 2. 算法图

5 复现细节

5.1 与已有开源代码对比

Wu [12] 作者已经完成了代码的开源, 代码地址为 <https://github.com/ZhaoxuanWu/Incentive-Aware-FL>。因此, 在实验过程中, 复现工作不仅仅是简单地搭建作者提供的代码环境并进行训练。我们在复现过程中发现, 尽管作者的模型已经取得了一定的成果, 但仍然存在一些不足之处。为此, 我们提出了一些改进方法, 旨在优化模型的性能, 并通过实验验证了这些改进的有效性。

此外, 作者的开源代码并没有对每个客户端的贡献进行有效的评估。在原始实现中, 客户端的贡献只是根据模型更新的数量进行简单的衡量, 未能全面反映每个客户端的真实贡献。为了弥补这一缺陷, 我们提出了一种新的贡献评估方法, 并将其集成到现有代码中, 以便更加精确地量化客户端在联邦学习中的贡献。这一改进有助于进一步提升联邦学习模型的性能, 并解决了原始模型中因客户端贡献不平衡而可能导致的收敛问题。

通过这些改进, 我们不仅改进了模型的效果, 还提升了实验的可操作性和复现性, 为未来的研究和实践提供了有价值的参考。

5.2 实验环境搭建

本文的所有模拟实验均在搭载 NVIDIA GeForce RTX 3090 GPU 的工作站上使用 PyTorch 进行, 基于两个广泛认可的数据集, MNIST [5] 和 CIFAR-10 [4]。我们使用了两个简单的卷积神经网络 (CNN) 模型, 这些模型包含批归一化层 (batch normalization layers) 来实现 IAFL。每个模型由三个模块组成, 每个模块包括一个卷积层、一个批归一化层和一个 ReLU 激活函数。接着, 我们在模拟中应用了 SGD 优化器、指数衰减学习率调度器和交叉熵损失函数。同时, 我们还探索了 IAFL 在非独立同分布 (non-IID) 场景下的表现, 在该场景中, 客户端异质性通过 Dirichlet 分布被准确建模。

5.3 创新点

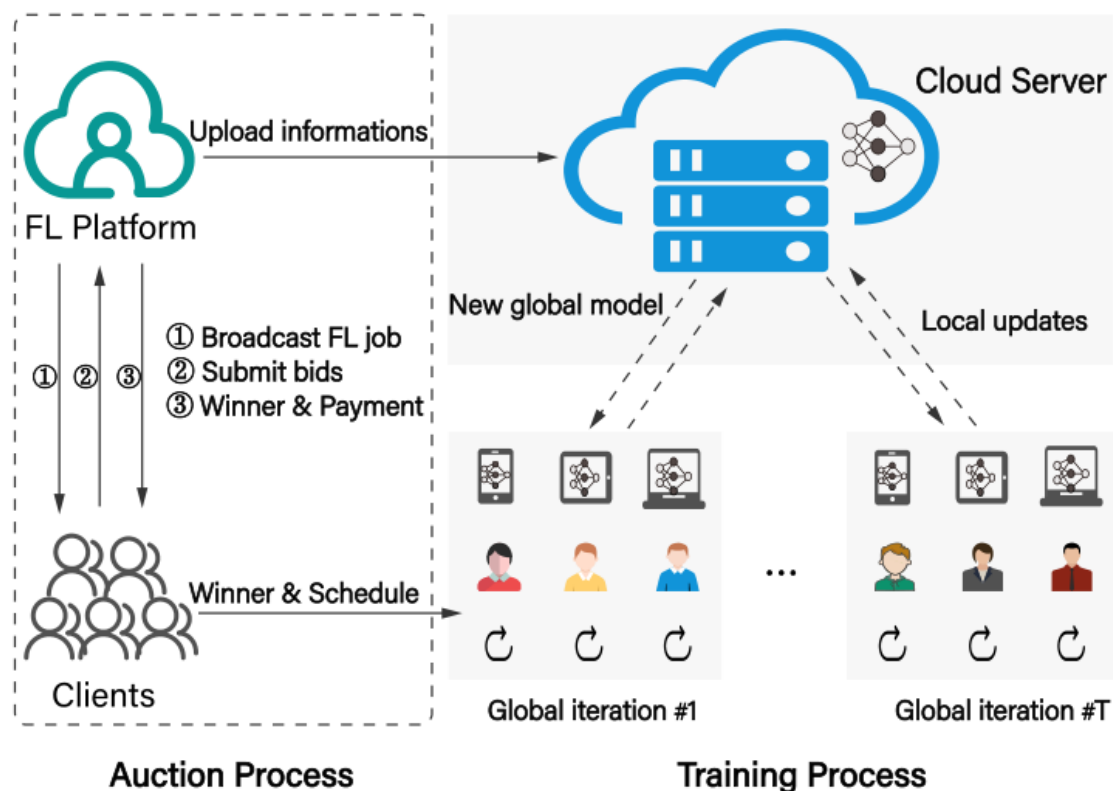


图 3. 反向拍卖和联邦学习框架图

在这篇论文中，使用传统的激励机制来评估客户端参与度并不是十分合理，尤其是在金钱定价问题上，难以找到一个有效的解决方案。通常情况下，金钱激励虽然能在一定程度上吸引客户端的参与，但由于客户端的参与动力和数据质量存在异质性，单纯依赖金钱定价往往无法公平有效地衡量每个客户端的贡献，甚至可能导致不公平的资源分配或过度依赖数据质量较高的客户端，进而影响全局模型的性能。更新后的联邦框架如图3。

本文的创新之处在于引入了反向拍卖框架作为激励机制，使得每个客户端的参与定价由客户端自身来设定，而非由服务器强制规定。在这个框架下，服务器端通过客户端提交的投标（即每个客户端为自己的参与设置的价格）以及客户端的数据量大小来评估其贡献。反向拍卖的核心优势在于，它能够引导客户端根据自身的利益设定参与价格，同时服务器能够通过竞标的方式获取最具成本效益的参与者，从而优化参与客户端的选择。

为了确保这一机制的有效性，在支付阶段，服务器采用二价拍卖（Second-Price Auction）模型进行支付决策。具体而言，二价拍卖确保了每个客户端的个人理性和真实性，因为客户端在设置投标时不需要担心自己最终的支付金额会高于其真实价值。通过这一机制，客户端可以放心地按照其真实的参与意愿和数据质量设置价格，而服务器则可以确保支付给每个客户端的报酬反映了其真实的贡献。这种方式不仅提高了激励机制的透明度，还确保了各方的公平性和效益。

在实验中，我们验证了这一反向拍卖激励机制的有效性，发现它能够在客户端参与度和贡献评估方面提供更加合理和灵活的解决方案，尤其在非独立同分布（non-IID）环境下，能

够有效地调节客户端的异质性，并促进全局模型的收敛。通过反向拍卖的方式，服务器能够对客户端的参与进行更加精准的激励和调整，从而提升了联邦学习系统的整体性能。

6 实验结果分析

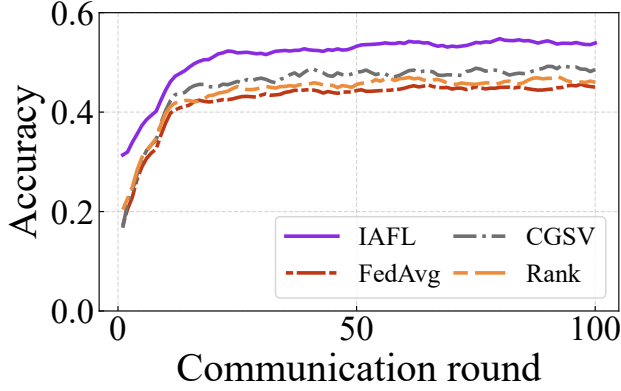


图 4. 在 noniid 下 cifar 数据集实验结果

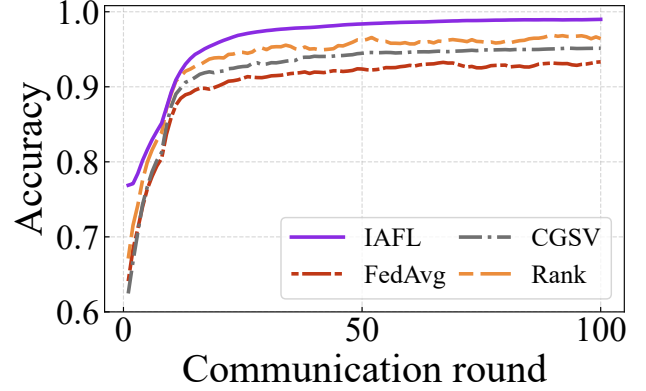


图 5. 在 noniid 下 mnist 数据集实验结果

IAFL [12] 实现遵循算法图。我们设置共享参数 $\kappa = 0$ 和随机恢复概率 $q = 0$ 。我使用客户端拥有的数据量作为它们的贡献 $p_{i,t}$ ，并且这些贡献在每次迭代中保持固定。

标准的 FedAvg [8] 在每次 FL 迭代中将相同的模型返回给所有客户端。在这种情况下，相关性度量 ρ 是未定义的且无法计算的。为了解决这个问题并为每个客户端创建个性化模型，我们考虑了一种简单的修改，允许客户端在 FL 算法结束时进行额外的训练周期。因此，这种变体，称为 FedAvg finetune，作为一个直接的 FL 个性化基准。

CGSV [13] 余弦梯度夏普利值 (CGSV) 根据客户端梯度与所有客户端梯度的平均值之间的余弦相似度评估客户端的贡献。在奖励阶段（即服务器发送相应更新时），CGSV 根据客户端的贡献掩盖（即置零）梯度更新聚合的部分内容。这种掩盖是按层执行的，其中贡献决定了每个模型层梯度更新中被掩盖的参数值比例。

Rank [3] 根据每个客户端在验证数据集上的模型准确度，在每次迭代中对客户端进行奖励。该方法在奖励之前根据验证准确度对客户端进行排名。客户端 i 可以从验证准确度低于其本身的其他客户端聚合模型更新。

在联邦学习过程中，客户端模型的性能直接关系到整体学习任务的效果。一个优秀的客户端模型不仅能够提高其自身的预测准确性，还能促进整体模型性能的提升。因此，为了激励客户端积极参与并持续贡献，必须确保每个客户端都能获得有竞争力的模型训练效果。IAFL（基于反向拍卖的激励机制）正是通过这种方式成功激励了客户端，确保它们不仅能在自己的数据上获得高准确度，同时也能在协作过程中通过参与联邦学习而受益。

为了验证 IAFL 的有效性，我们通过对比基准方法，评估了客户端模型的测试准确度。根据实验结果（如图4和5所示），IAFL 在几乎所有实验设置中均表现出了优于其他方法的性能。这表明，IAFL 通过合理的激励机制，使得客户端能够更积极地参与训练，且最终模型的表现也更为优异。IAFL 不仅在客户端的平均准确度上超越了其他方法，更在最优准确度上取得了显著的提升。这一结果进一步验证了 IAFL 在利用去中心化的数据和模型参数优化方面的优势，能够有效地从每个客户端的独特数据中提取有价值的信息，从而实现全局模型的性能提

升。这种去中心化的数据利用方式是 IAFL 相比其他方法的一个突出特点，也是其在实际应用中具有潜力的重要原因之一。

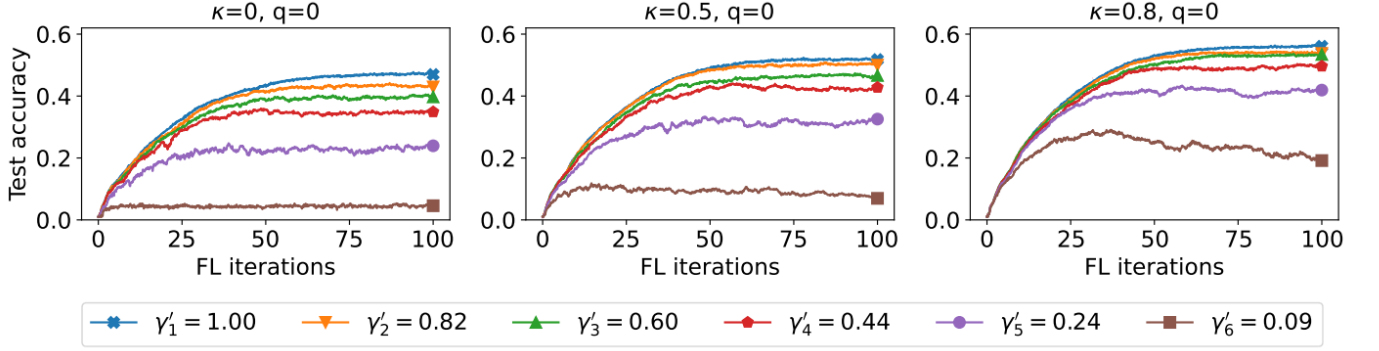


图 6. 共享系数与固定随机恢复率的影响图

共享系数 $\kappa \in [0, 1]$ 决定了 IAFL 中共享的程度，并反映了模型性能与客户端激励之间的实际权衡。较大的 κ 值意味着模型的共享程度增大，客户端之间的模型更加公平和一致，且能够提升客户端模型的整体性能。然而，这种增加的共享可能会影响到高贡献客户端的激励。具体来说，高贡献客户端收到的模型将更接近于低贡献客户端的模型，这可能导致其激励效应下降。通过图6中的实验结果，我们可以看到在不同的 κ 值下，6 个客户端的模型性能变化。较大的 κ 能够更好地融合本地模型的更新信息，进而提高模型的总体准确率。然而，这也导致了客户端之间的模型性能差异减小，从而减少了通过 ρ 所衡量的激励效果，特别是对于那些贡献较高的客户端。对于收敛性，贡献较少的客户端将收敛到较差的模型，这些模型远离全局最优解。

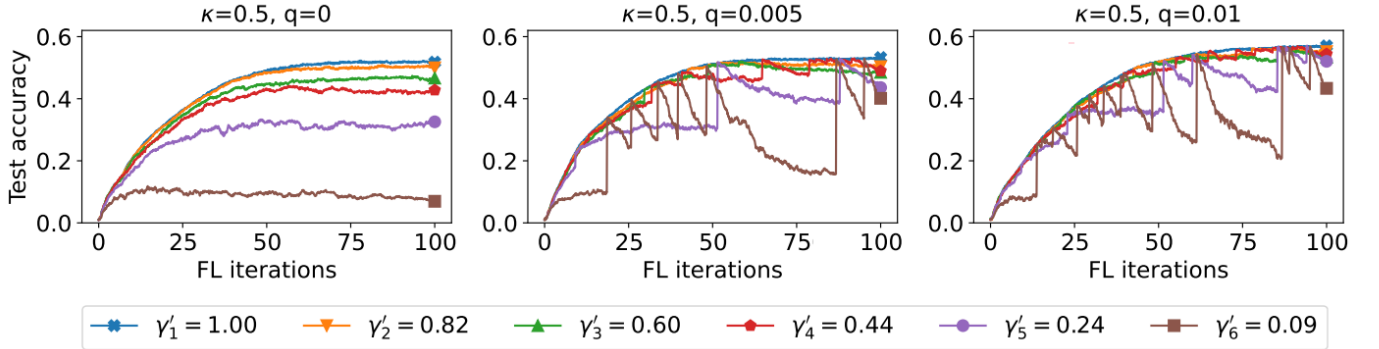


图 7. 固定共享系数下随机恢复率的影响图

在 IAFL 中，随机恢复机制不仅帮助确保客户端模型能够逐步收敛到全局最优解，同时也引入了一定的灵活性，使得每个客户端都有机会被恢复为参考模型，从而避免了由于客户端个体差异过大导致的收敛问题。具体而言，每个客户端在每次 FL 迭代中都有相同的概率 q 被选择为恢复为参考模型，参考模型的更新通常是选择当前迭代中奖励最大的模型（即 λ_i, t' 最大）。这种做法有效促进了模型的收敛，并且避免了在某些客户端未能及时更新的情况下全局模型的性能下降。

参考模型的更新频率和恢复概率 q 在实践中会影响整个模型训练的性能。在图7中，可以看出，随机恢复机制在客户端激励性能和客户端模型的测试准确度之间形成了一种平衡关系。

当 q 较小时（例如 $q = 0.01$ ），可以观察到更高的测试准确率，同时保持相对较高的激励性能。这种设置能够保证在有限的 FL 迭代次数内，客户端不仅能够持续优化自身模型，还能保持较好的激励水平。

关于搭便车行为的处理，IAFL 通过为不同的客户端提供差异化的奖励来应对这一问题。搭便车者指的是那些贡献较小的客户端，它们在训练过程中未能对全局模型做出显著的贡献，因此无法获得相应的奖励。图7中标识出客户端 6，其贡献远小于其他客户端，因此被视为搭便车者。在这种情况下，当 $q = 0$ 时，搭便车者在 $\kappa = 0$ 时仅能达到 4.6% 的准确率，而在 $\kappa = 0.8$ 时，准确率为 19.2%。这表明，尽管搭便车者模型的更新较少，但通过恢复机制可以帮助其获得一定程度的改善。

当引入随机恢复后，搭便车者可以在延迟的时间点获得一个较好的恢复奖励，这意味着其模型有机会被提升。然而，尽管恢复奖励能够带来一时的改善，由于搭便车者每次 FL 迭代中都没有贡献有效的模型更新，其表现最终仍会继续恶化。这种现象反映了 IAFL 系统在激励设计上的一个重要特点，即低贡献客户端的模型始终会因其持续的低更新而无法达到全局最优解。

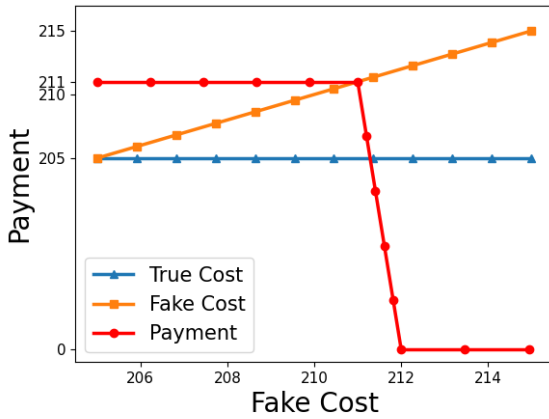


图 8. 赢家真实性

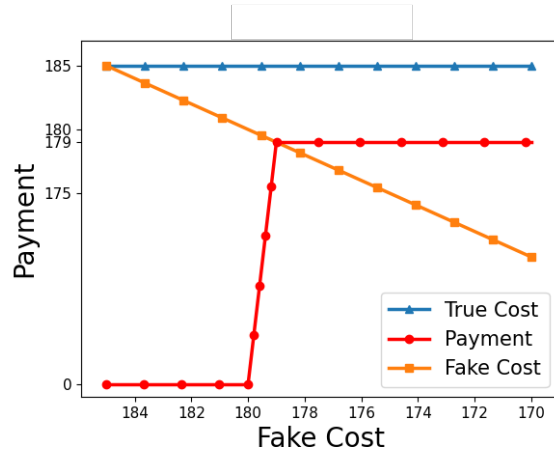


图 9. 输家真实性

在拍卖中，真实性是指每个客户在出价时使用真实成本，以最大化其效益。即当客户以真实成本出价时，其效益最大化。这种诚实性在拍卖中是非常重要的，因为它确保了拍卖的公平性和有效性。只有当所有参与者都表现诚实时，拍卖才能达到最优结果，确保资源的合理分配。尤其是在联邦学习激励机制的设计中，诚实性能够促进每个客户端按照自己的真实贡献参与训练，从而帮助系统高效地进行优化。

二价拍卖（Second-Price Auction）是一种常见的拍卖机制，其核心特点是获胜者并不会支付自己出价的金额，而是支付第二高的出价。这种机制的关键优势在于它鼓励参与者在出价时保持诚实，因为他们知道如果出价超过了他们的真实价值，最终的支付金额将会是第二高的出价，而不是他们的出价本身。因此，二价拍卖能够激励参与者报告其真实的意愿出价，从而提高了拍卖的效率。

二价拍卖的一个典型应用场景是在分布式学习中，其中各个节点（即客户端）为其计算资源和数据贡献出价。通过这种方式，二价拍卖能够有效地分配奖励，并最大程度地降低系统中的搭便车行为，使得各个参与者的贡献能够被准确地反映在奖励机制中。与此同时，二价拍卖也能够帮助降低由于不诚实出价所带来的效率损失，确保系统的高效运作和公平竞争。

如图8所示，我们观察到随着声明的出价增加，获胜者持续被选择，并且 IAFL 支付逐渐增加，直到达到最大值。然而，当出价超过临界值 211 时，获胜者不再被选择，意味着不再支付任何奖励。因此，客户端不会增加其出价，因为这样可能会导致客户端不被选中。如图9所示，我们发现当出价低于 179 时，输家将被选中。然而，客户端将获得负利润，意味着支付无法充分补偿其实际成本。因此，客户端没有动机不真实地提交其成本。

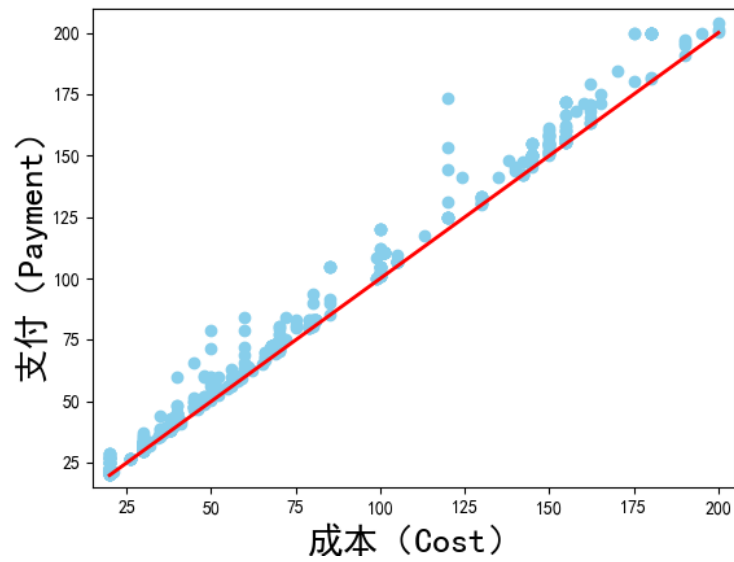


图 10. 个人理性

个人理性是拍卖机制中的一个重要特性，指的是每个参与者在拍卖过程中能够获得非负的效益。具体来说，个人理性要求每个客户的支付金额必须至少等于其参与拍卖的成本，否则客户可能会选择退出拍卖。换句话说，个人理性确保了客户在参与拍卖时，不会因成本超过支付金额而遭受损失，从而保证了客户的参与动机。

如图10所示，我们通过将客户端的（成本，支付）作为二维坐标系中的（x，y）点进行展示。在图中，所有的蓝色点都位于 $y = x$ 这条红线上方，表示所有客户端的成本都小于或等于其所获得的支付金额。这表明，每个客户端都能获得不低于其成本的支付，因此满足了个人理性条件。通过这种方式，我们能够证明该拍卖机制在理论上实现了个人理性，从而确保了参与者的利益不受损失，鼓励更多的客户端参与拍卖和合作。个人理性不仅仅是一个技术要求，也是拍卖机制中最基本的原则之一。在实际的拍卖设计中，确保个人理性有助于提升客户的参与度，并使拍卖系统能够在长期运行中保持稳定性和可靠性。如果一个拍卖机制无法保证个人理性，那么可能会导致客户的退出或虚假参与，最终影响系统的整体效能。

7 总结与展望

本文研究了在联邦学习（Federated Learning, FL）中引入激励机制和随机恢复机制的有效性。首先，分析了联邦学习中的客户端激励问题，提出了一种基于拍卖的激励机制（FPIN），旨在通过合理的支付设计，确保客户端根据其贡献参与模型训练，同时避免搭便车行为。通过引入客户端贡献奖励机制和参考模型恢复机制，实现了高效的客户端激励，并解决了由于不同客户端训练质量差异带来的收敛性问题。

在理论层面，论文展示了如何在联邦学习中通过拍卖机制保证客户端的真诚性和个人理性，确保每个客户端的支付不低于其成本，从而最大化客户的效益。在随机恢复机制方面，本文通过调整恢复概率，提供了一种在不同客户端之间平衡激励和模型准确度的解决方案。通过实验证明，合理选择恢复概率能够有效提升模型的测试准确度，同时保持较高的激励水平，确保了系统的稳定性和高效性。

尽管论文在联邦学习的激励机制方面取得了一定的成果，但仍有许多值得进一步研究和改进的地方。首先，关于客户端之间的异质性，尤其是在数据分布和计算能力方面，未来可以深入探讨如何通过优化激励机制进一步提升低贡献客户端的参与度。其次，随机恢复机制的优化也可以作为未来研究的一个方向，探索更加精细的恢复策略，例如动态调整恢复概率、使用不同类型的参考模型等，以进一步提升系统的收敛速度和全局模型的质量。

另外，尽管论文主要集中在激励机制的设计与优化，但联邦学习中的其他问题，如数据隐私保护、通信效率优化等，也亟待进一步探索。在未来的研究中，可以结合多种技术，如差分隐私、加密技术等，以提升联邦学习在安全性和隐私保护方面的能力。此外，随着联邦学习在实际应用中的逐渐推广，如何将这些机制与实际场景相结合，并处理大规模、多样化的客户端参与问题，也是未来研究的重要方向。

参考文献

- [1] Daoyuan Chen, Dawei Gao, Weirui Kuang, Yaliang Li, and Bolin Ding. pfl-bench: A comprehensive benchmark for personalized federated learning. *Advances in Neural Information Processing Systems*, 35:9344–9360, 2022.
- [2] Latif U Khan, Shashi Raj Pandey, Nguyen H Tran, Walid Saad, Zhu Han, Minh NH Nguyen, and Choong Seon Hong. Federated learning for edge networks: Resource optimization and incentive mechanism. *IEEE Communications Magazine*, 58(10):88–93, 2020.
- [3] Shuyu Kong, You Li, and Hai Zhou. Incentivizing federated learning. *arXiv e-prints*, pages arXiv–2205, 2022.
- [4] Alex Krizhevsky, Geoffrey Hinton, et al. Learning multiple layers of features from tiny images. 2009.
- [5] Yann LeCun, Bernhard Boser, John Denker, Donnie Henderson, Richard Howard, Wayne Hubbard, and Lawrence Jackel. Handwritten digit recognition with a back-propagation network. *Advances in neural information processing systems*, 2, 1989.
- [6] Tian Li, Anit Kumar Sahu, Manzil Zaheer, Maziar Sanjabi, Ameet Talwalkar, and Virginia Smith. Federated optimization in heterogeneous networks. *Proceedings of Machine learning and systems*, 2:429–450, 2020.
- [7] Yuan Liu, Mengmeng Tian, Yuxin Chen, Zehui Xiong, Cyril Leung, and Chunyan Miao. A contract theory based incentive mechanism for federated learning. In *Federated and Transfer Learning*, pages 117–137. Springer, 2022.

- [8] Brendan McMahan, Eider Moore, Daniel Ramage, Seth Hampson, and Blaise Agüera y Arcas. Communication-efficient learning of deep networks from decentralized data. In *Artificial intelligence and statistics*, pages 1273–1282. PMLR, 2017.
- [9] Krishna Pillutla, Kshitiz Malik, Abdel-Rahman Mohamed, Mike Rabbat, Maziar Sanjabi, and Lin Xiao. Federated learning with partial model personalization. In *International Conference on Machine Learning*, pages 17716–17758. PMLR, 2022.
- [10] Alysia Ziying Tan, Han Yu, Lizhen Cui, and Qiang Yang. Towards personalized federated learning. *IEEE transactions on neural networks and learning systems*, 34(12):9587–9603, 2022.
- [11] Jianyu Wang, Qinghua Liu, Hao Liang, Gauri Joshi, and H Vincent Poor. Tackling the objective inconsistency problem in heterogeneous federated optimization. *Advances in neural information processing systems*, 33:7611–7623, 2020.
- [12] Zhaoxuan Wu, Mohammad Mohammadi Amiri, Ramesh Raskar, and Bryan Kian Hsiang Low. Incentive-aware federated learning with training-time model rewards. In *The Twelfth International Conference on Learning Representations*, 2024.
- [13] Xinyi Xu and Lingjuan Lyu. A reputation mechanism is all you need: Collaborative fairness and adversarial robustness in federated learning. *arXiv preprint arXiv:2011.10464*, 2020.
- [14] Yufeng Zhan, Peng Li, Zhihao Qu, Deze Zeng, and Song Guo. A learning-based incentive mechanism for federated learning. *IEEE Internet of Things Journal*, 7(7):6360–6368, 2020.
- [15] Jingwen Zhang, Yuezhou Wu, and Rong Pan. Incentive mechanism for horizontal federated learning based on reputation and reverse auction. In *Proceedings of the Web Conference 2021*, pages 947–956, 2021.