计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.220500272

联邦学习激励机制研究综述

梁文雅[1]　刘　波[1]　林伟伟[2,3]　严远超[1]
1 华南师范大学计算机学院　广州 510631
2 华南理工大学计算机科学与工程学院　广州 510640
3 鹏程实验室　广东 深圳 518066
(1799871545@qq.com)

摘　要　联邦学习(Federated Learning,FL)以多方数据参与为驱动,参与方与中央服务器通过不断交换模型参数,而不是直接上传原始数据的方式来实现数据共享和隐私保护。在实际的应用中,FL全局模型的精确性依赖于多个稳定且高质量的客户端参与,但客户端之间数据质量不平衡的问题会导致在训练过程中客户端处于不公平地位甚至直接不参与训练。因此,如何激励客户端积极可靠地参与到FL中,是保证FL被广泛推广和应用的关键。文中主要介绍了在FL中激励机制的必要性,并根据激励机制在FL训练过程中存在的子问题将现有研究分为面向贡献测量、面向客户选择、面向支付分配以及面向多子问题优化的激励机制。对现有的激励方案进行分析和对比,并在此基础上总结激励机制在发展中存在的挑战,探索FL激励机制未来的研究方向。

关键词:联邦学习;激励机制;贡献测量;客户选择;支付分配
中图法分类号　TP181;TP309

Survey of Incentive Mechanism for Federated Learning

LIANG Wen-ya[1],LIU Bo[1],LIN Wei-wei[2,3] and YAN Yuan-chao[1]
1 School of Computer Science,South China Normal University,Guangzhou 510631,China
2 School of Computer Science and Engineering,South China University of Technology,Guangzhou 510640,China
3 Pengcheng Laboratory,Shenzhen,Guangdong 518066,China

Abstract　Federated Learning(FL) is driven by multi-party data participation,where participants and central servers continuously exchange model parameters rather than directly upload raw data to achieve data sharing and privacy protection. In practical applications,the accuracy of the FL global model relies on multiple stable and high-quality clients participating,but there is an imbalance in the data quality of participating clients,which can lead to the client being in an unfair position in the training process or not participating in training. Therefore,how to motivate clients to participate in federated learning actively and reliably is the key,which ensuring that FL is widely promoted and applied. This paper mainly introduces the necessity of incentive mechanisms in FL and divides the existing research into incentive mechanisms based on contribution measurement,client selection,payment allocation and multiple sub-problems optimization according to the sub-problems of incentive mechanisms in the FL training process,analyzes and compares existing incentive schemes,and summarizes the challenges in the development of incentive mechanisms on this basis,and explores the future research direction of FL incentive mechanisms.

Keywords　Federated learning,Incentive mechanism,Contribution measurement,Client selection,Payment allocation

1　引言

随着数字化技术进入高速发展期,新一代的人工智能和大数据等技术为传统行业智能化转型发展带来了新的机遇[1]。例如,以铸造、船舶以及汽车等行业为典型的制造行业已由传统制造模式升级为数据驱动下的智能制造模式。在数据成为生产要素并发挥着愈加重要作用的今天,数据共享及隐私安全迎来了新的挑战。传统的数据共享方式是用户将

到稿日期:2022-05-29　**返修日期**:2022-08-05
基金项目:广东省重点领域研发计划项目(2021B0101420002);国家自然科学基金面上项目(62002078,61872084);广州市开发区国际合作项目(2020GH10);鹏城实验室重大任务项目(PCL2021A09)
This work was supported by the Key Research and Development Program of Guangdong Province(2021B0101420002),General Project of National Natural Science Foundation of China(62002078,61872084),Guangzhou Development Zone International Cooperation Project(2020GH10) and Major Key Project of PCL(PCL2021A09).
通信作者:刘波(liugubin530@126.com);林伟伟(linww@scut.edu.cn)

数据上传至一台高算力的云服务器上，然后进行集中训练。这种数据共享方式需要消耗大量的通信资源，且会导致数据流向不可控和数据泄露等问题。此外，我国的《数据安全法》和欧盟的《通用数据保护条例》(General Data Protection Regulation，GDRP[2])等相关规定的出台以及用户对隐私数据保护意识的觉醒，使得各部门对隐私安全的要求比以前更加严格，隐私安全和数据共享之间存在着不可协调的矛盾。

为了解决上述问题，谷歌在 2016 年首次提出了联邦学习理论[3]。作为机器学习的新兴范式，FL 为用户数据共享提供了新颖的解决方案。数据持有者直接进行模型训练，不需要将其原始数据传输到第三方服务器，就能得到一个更优化的模型[4]，这为多个数据持有者之间的数据共享提供了解决方案，确保了隐私安全，打破了数据孤岛[5]的桎梏，充分挖掘了隐私数据中的潜在价值。目前联邦学习已经初步应用于医学成像[6]、智能家居[7]以及计算机视觉[8]等领域。

目前，FL 的研究主要集中在异质性[9]、联邦模型优化等方面，以提高模型效率、确保模型有效性[10]和保证隐私安全[11]。然而，这些研究都会假设一个乐观的前提，即所有的参与方都会无条件参与到联邦学习中，但这在实际应用中并不存在。在模型训练和上传参数到服务器的过程中，客户端需要消耗大量的计算资源和通信资源，如果没有一定的激励机制，这些客户端可能不愿意参与 FL。此外，联邦学习模型训练涉及多方参与，参与的客户端之间数据质量的不平衡性会导致某些客户端处于不公平地位。因此，FL 需要通过一个公平的激励机制，给予客户端合理的奖励，鼓励不同的客户端贡献私人数据并积极参与到 FL 中。

在最近 3 年内，FL 的综述文献研究主要集中在联邦学习的隐私安全、应用和其他(如通信开销、激励机制等)3 个方面，分别占 43.7%，31.25%，25%[12]。其中，关于激励机制的综述文献占比较小，激励机制的发展正处于起始阶段。但激励机制对 FL 的推广和应用起着关键的作用，是 FL 工业化必不可少的一个环节，因此对激励机制进行综述研究是非常有必要的。Zhan 等[13]根据在 FL 激励机制实施过程中出现的问题，提出了基于驱动的方式来划分激励机制，但这种分类方式对于一些使用自定义的激励方案无法进行归类。Zeng 等[14]根据激励机制所用的技术，如博弈论、拍卖理论以及契约理论等，提出基于所用技术的方式划分激励机制，但这种分类方式无法一一列举所有激励方案所用的技术。本文从 FL 系统架构的训练过程出发，根据激励机制在此过程中存在的子问题，创造性地提出了面向子问题的激励机制分类方式，对 FL 激励机制的现有方案进行了分析和总结。

本文第 2 节概述了联邦学习和激励机制；第 3 节从面向贡献测量、面向客户选择、面向支付分配以及面向多子问题优化的激励机制 4 个方面对 FL 激励机制的研究现状进行了分析和总结；第 4 节总结了 FL 激励机制研究当前存在的挑战，并探索了未来的研究方向；最后总结全文。

2 研究背景

2.1 联邦学习概述

联邦学习又叫联邦机器学习、联合学习或联盟学习，是一种新型的分布式机器学习框架。其思想是在满足数据隐私安全和相关政府规定的前提下，在不需要共享原始数据的情况下，允许多个数据拥有者通过迭代更新参数模型来协作训练共享模型，其系统架构如图 1 所示。

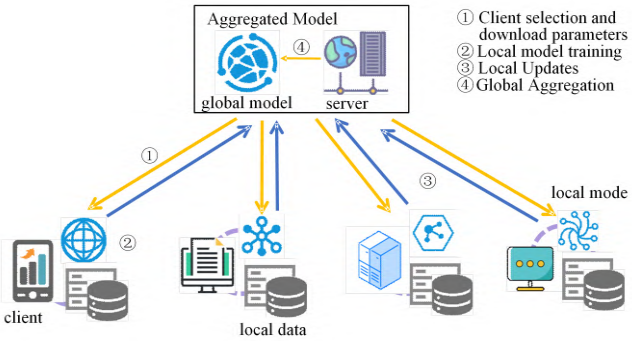

图 1 联邦学习系统架构

Fig. 1 System architecture of FL

具体来说，FL 的训练过程可以分为以下 5 个步骤。

(1)初始化：服务器根据训练任务随机对全局模型参数进行预训练，并选择符合条件的客户端，将初始的模型参数分发给选定的客户端。

(2)本地训练：选定的客户端使用本地数据集及收到的全局模型参数更新本地模型参数。

(3)本地上传：将更新的参数上传到服务器。

(4)全局聚合：服务器接收各个客户端更新上传的参数并进行聚合。

(5)模型更新：将最新的全局模型参数和奖励分发给最新选定的客户端。

重复步骤(2)－步骤(5)，直到全局模型达到一定的要求，即达到预设的性能指标或达到预设的时间。

2.2 激励机制概述

激励机制指通过特定的方法与管理体系，将员工对组织及工作的承诺最大化的过程[13]。大多数激励机制是为了激励高质量的客户端参与到模型训练中，使资源消耗(如通信和计算成本等)最小化，模型性能(如模型精度和训练速度等)最大化。

设 $N=\{0,1,\cdots,N-1\}$ 表示 N 个客户端，客户端 i 的成本由资源向量 $\boldsymbol{q}_i$ 和对应的权重向量 $\boldsymbol{\theta}_i$ 表示的多维向量共同决定。当 $\boldsymbol{q}_i=\vec{0}$ 时表示客户端 i 未参与联邦训练。客户端 i 的利润函数表示为：

$$\pi_i=p_i-c_i(\boldsymbol{q}_i,\boldsymbol{\theta}_i) \tag{1}$$

其中，p_i 是 N_i 从全局模型中获得的奖励，$c_i(\cdot)$ 是客户端 i 的成本函数。

服务器的利润函数表示为：

$$\pi=U(Q)-\sum p_i \tag{2}$$

其中，$U(\cdot)$ 是效用函数，Q 为 $(\boldsymbol{q}_0,\boldsymbol{q}_1,\cdots,\boldsymbol{q}_{N-1})$。

激励机制的目的是找到 Q 的最优解，以最大化客户端和服务器的利润函数[14]。在边缘计算和群智感知等领域，激励机制使用博弈论验证能否达到纳什均衡来研究是否能找到 Q 的最优解。纳什均衡指任意客户端 i 在其他客户端策略不变的情况下，单方面改变自己的策略，这并不会提高自身的利润。也就是说，当达到纳什均衡时，客户端 i 满足：

$$\pi_i(q_i^{NE}, q_{-i}^{NE}) \geqslant \pi_i(q_i, q_{-i}^{NE}) \tag{3}$$

其中，$q_{-i}^{NE}=\{q_0^{NE},\cdots,q_{i-1}^{NE},q_{i+1}^{NE},\cdots,q_{N-1}^{NE}\}$，$q_i \in S_i$ 是客户端 i 的一个策略。

当服务器和所有客户端处于纳什均衡状态时，$\{q_0^{NE}, q_1^{NE},\cdots,q_{N-1}^{NE}\}$ 为 Q 的最优解。除了纳什均衡外，激励机制还可以采用其他方式，如 Blum 等[15]证明了存在自定义的稳定且无嫉妒的均衡，在保持客户端的样本收集负担较低的基础上找到 FL 的最优解；Zhang 等[16]使用贝叶斯博弈优化模型训练策略，来求解贝叶斯均衡以得到最优解。

2.3 联邦学习的激励机制

在 FL 激励机制中，服务器会根据成本和贡献水平来确定参与训练的客户端。首先，服务器会选择一组符合条件的客户端进行初始化训练，训练结束后根据贡献水平进行收益分配。在新一轮的训练开始之前，客户端会根据收益水平调整自己的资源策略。客户端可以随时选择加入、离开或是留在 FL 中[17]。若客户端首次参与 FL，服务器会随机分配一个初始参数。若客户端选择退出 FL，则服务器会对其行为做出一定惩罚。选择参与 FL 的客户端会调整自己的资源策略进行多轮博弈，直至达到均衡状态。本节从 FL 训练过程中存在的子问题出发，探讨如何激励客户端积极参与 FL。FL 激励机制包括贡献测量、客户选择和支付分配 3 个子问题[12]，如图 2 所示。

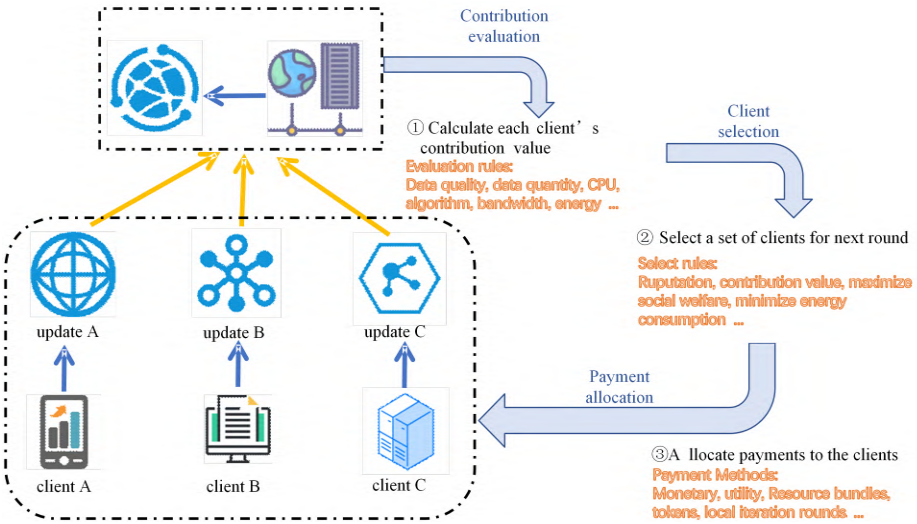

图 2 联邦学习激励机制的子问题

Fig. 2 Sub-problem of incentive mechanism in FL

贡献测量是根据资源的效用来量化每个客户端对全局模型的贡献水平。最简单的测量方法是根据客户端贡献的数据量的大小来进行测量。但是，在 FL 中，模型精度和数据量大小并不是正比关系，客户端的贡献值的大小由数据量、数据质量、机器学习算法和 CPU 资源等多个因素决定；客户选择指选择一组高质量的客户端加入联邦训练。在 FL 中，客户选择不仅要考虑资源最优化，还要考虑经济因素，实现客户端对全局模型贡献最大化，成本最小化；支付分配是根据收益分配方式来决定选定客户端的支付方式和收益大小，激励客户端长期稳定地参与 FL。

3 联邦学习激励机制的研究现状

现有 FL 激励机制的研究大都集中于优化 FL 激励机制中的某个子问题或者多个子问题，从而提升联邦训练的性能。本节将从面向贡献测量的激励机制、面向客户选择的激励机制、面向支付分配的激励机制以及面向多子问题优化的激励机制 4 个方面对现有的 FL 激励机制方案进行详细阐述。

3.1 面向贡献测量的激励机制

参与方加入 FL 需要付出一定的计算资源和通信资源，因此参与方往往不会在没有得到一定补偿的情况下加入 FL。一个合理的贡献测量标准可以使联邦系统的效用达到最大，且进一步激励更多的高质量用户加入 FL。面向贡献测量的激励机制大体可以分为单维度贡献测量和多维度贡献测量两种。

单维度贡献度测量指在测量的过程中，把对全局模型影响最大的某个因素（如计算资源、通信资源、数据量、数据质量等）作为利润函数的变量。Kang 等[18]为了解决 FL 任务发布者和用户之间的信息不对称的问题，提出了基于契约理论的单维度贡献测量方法。对于用户来说，计算资源贡献越多，局部模型训练就越快，就可以从 FL 系统中得到更高的回报；Zhan 等[19]将服务器的总奖励和边缘节点的总收益建模为一个 Stackelberg 博弈，求解纳什均衡以得到最优解，同时使用基于深度强化学习算法来动态调整激励策略，以优化各方利润。但是，该方案假设了边缘节点训练数据质量相同且独立同分布，边缘节点的总收益由参与方的数据量单个维度决定，这在现实的 FL 环境中几乎是不可能的。

影响全局模型精确度的多个因素共同决定用户的贡献水平。相比单维度贡献测量，多维度贡献测量更加公平[20-23]。单个因素与全局模型的准确性之间不存在明确的线性关系，单独使用数据量或者数据质量度量用户的贡献是不合理的。在机器学习中，基于 Shapley 值的测量方法经常被用于评估数据对模型的性能。现有的 Shapley 值评估方案应用于 FL 的多维度贡献测量会带来额外的计算量，未被广泛使用。基于 Shapley 值的概念，Song 等[20]定义了用户的贡献指数，通过本地数据集、机器学习算法和测试集等因素量化了数据提供者在水平 FL 任务中的贡献。该方法只需在训练过程中

记录中间结果，不涉及额外的模型训练；但 Zhang 等[21]指出，在某些学习场景中（如使用不同的机器学习算法、参与方的 Shapley 值为负数等）使用基于 Shapley 值的激励机制是不公平的，甚至会导致参与方退出 FL。因此，该方案提出了一种分层公平联邦学习框架 HFFL，通过公开可验证的多维因素，如数据质量、数据量、数据收集成本等，把所有参与的客户端分为多个不同的贡献水平，从而实现各方之间的公平性。Nishio 等[22]提出了一种基于逐步贡献计算的轻量化多维度贡献测量方法。该方案把客户端加入 FL 训练时将性能上的增益作为评估客户端贡献的指标，用于评估客户模型在每一轮中改进全局模型的程度。该方案有效减少了流量和计算开销，但是必须满足在每一轮迭代中提升客户端模型性能将提升最终的全局模型性能这一前提。

3.2 面向客户选择的激励机制

客户选择是 FL 中必不可少的一个步骤，选择合格的参与方来参与 FL，使联邦系统的集体效用达到最大化，是联邦优化的一个重要环节。在训练过程中加入激励机制，不仅能够使 FL 达到更好的性能，而且能够避免额外的训练，减少不必要的计算和通信资源消耗。因此，客户选择和激励机制的结合是一个非常有前景的研究方向。

声誉是 FL 客户选择的一个重要指标。声誉间接地反映了客户的可靠性和数据质量，更高声誉的客户端有更大的可能为 FL 任务带来更可靠和更高质量的训练[7,24-26]。声誉的更新规则如图 3 所示，每次任务结束时，服务器根据客户的行为更新客户的声誉，在下一轮迭代开始时，再根据声誉记录选择声誉高的用户参与下一轮训练。

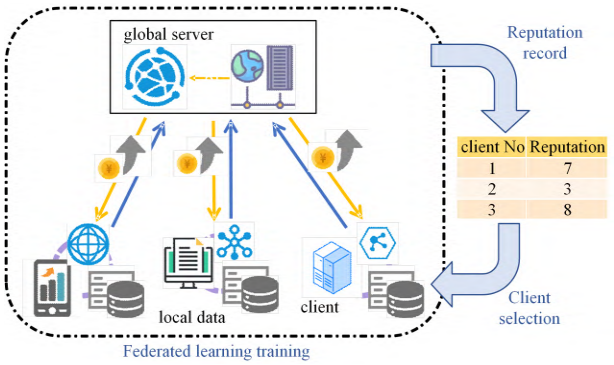

图 3 基于声誉的客户选择

Fig. 3 Selection client by clients' reputation

Zhao 等[7]设计了一个基于区块链的 FL 系统。在该系统中，区块链上的声誉验证器使用 Muti-KRUM 算法来计算信誉并评估不满意的更新，验证器接受一个客户端的更新，该客户端的声誉就加 1，否则就减 1。他们还在物联网设备中实现了 FL 系统，并利用该系统帮助家电制造商训练了一个基于客户数据的机器学习模型；对于资源受限的 FL，Zhang 等[24]提出了一种基于声誉和反向拍卖理论的 FL 激励机制。任务发布者发布任务，通过客户端的竞价和声誉来选择具有良好数据质量的客户端。客户端进行联邦训练后，任务发布者会测量每个客户端的贡献和声誉再更新声誉和支付奖励。

客户选择的目的是效用最大化。在 FL 中，效用最大化主要依靠优化不同客户之间动态的资源分配问题[27-32]。Hu 等[27]采用博弈论将 FL 中的服务器和用户效用最大化问题建模为两阶段的 Stackelberg 博弈。该方案通过求解 Stackelberg 均衡推导出服务器和用户的最佳策略，从而选择最有可能提供可靠隐私数据的用户进行补偿。Le 等[28]将基站和移动用户之间的交互建模为拍卖博弈，基站为拍卖方，移动用户为卖方，移动用户根据能参与 FL 的最小能耗成本提交投标。为了确定拍卖的赢家和实现社会福利最大化，该方案通过推导出博弈的近似解来确定移动用户赢得投标所需能耗成本的最小值。该方案可以保证真实性、个体合理性和效率 3 种经济特性，所获得的社会福利是固定价格机制的 5 倍；Khan 等[29]将边缘网络中的基站（BS）和用户设备（UEs）建模为一个领导者（BS）和多个追随者（UEs）的 Stackelberg 博弈。首先，BS 发布其效用函数，UEs 响应该函数并选择它们各自的局部迭代策略；然后 BS 评估 UEs 的响应以调整奖励率；最后不断重复上述过程，直到达到 Stackelberg 均衡后由 BS 选择一组自愿加入 FL 的 UEs。用被选择的设备训练全局模型的训练产出的成本最小。

3.3 面向支付分配的激励机制

支付分配是根据收益分配方式来决定选定的客户端的收益方式和收益量。在 FL 激励机制中，不同的收益分配方式有利于激励拥有高质量数据的参与者持续参与到联邦学习中。Hu 等[27]为了激励具有私有数据的用户参与到联邦任务中，让服务器根据用户的隐私预算为其提供金钱奖励，以补偿其在联邦训练过程中产生的隐私损失。在该方案中，拥有更大隐私预算的用户将得到更高的奖励，从而促进拥有隐私数据的用户贡献其数据并参与到 FL 中；在一些方案[17,33]中，客户端选择了金钱补偿用户的损失。Song 等[20]并未选择金钱激励方案，而是选择奖励学习模型或者资源包。这样有利于高质量的用户一直持续参与到 FL 中，而不是得到金钱补偿后就退出 FL。

在 FL 中，客户端参与模型训练时需要先承担一部分成本。因为模型的训练和商业化需要时间，所以联邦服务器偿还客户端会存在一定的延迟。为了解决这一问题，Yu 等[34]通过在客户端之间动态分配给定的预算和实时计算分配收益来实现客户端之间的公平。该方案缩短了服务器和客户端之间的延迟时间，实现了最大化集体效用，最小化了用户之间的不公平性。该方案相比其他方案对高质量的用户更具有吸引力，更有利于激励用户长期参与到 FL 中。但是，该方案只关注用户的收益分配，没有使用合理的方式来量化用户的贡献，无法估计用户加入 FL 所需的成本。

3.4 基于多子问题优化的激励机制

在 FL 激励机制中，一些研究同时解决多个子问题，而不是仅仅着重于某个子问题。FL 激励机制的 3 个子问题是相互依赖的，一个激励方案可能涉及多个子问题[35-39]。Liu 等[35]提出了一个基于区块链的点对点支付系统 FedCoin。该系统在每个矿工分别计算用户的近似 Shapley 值后，选择最接近所有矿工平均值的矿工为赢家。赢家生成一个新的块并根据在区块链中 Shapley 值的记录支付奖励；Zeng 等[36]提出了一个基于多维采购拍卖的激励机制方案 FMore。在该方案中，服务器先广播评分规则进行客户选择。客户端收到带有

评分规则的投标请求时，会根据自身资源决定是否投标。客户端提交投标书后，服务器根据排序分数大小选择 K 个赢家，并使用单价拍卖执行支付分配。FMore 鼓励更多高质量的客户端以低成本参与联邦训练，最终提升了联邦学习的性能。Zhang 等[37]建立了一种容易下降且难以提高的声誉机制。工人通过反向拍卖竞价任务，任务发布者根据单位声誉投标价格的大小来选择赢家。然后，该方案在有限的预算下根据绩效分配规则来支付赢家的奖励。Han 等[38]提出了一个标记化激励机制。标记是用于支付客户端数据和资源消耗服务的一种手段。该方案使用新的指标(如标记减少率和效用提高率)来测量客户端的贡献率，整个过程是在模型训练中实时完成的，不需要额外的训练开销。该方案利用历史准确性记录和随机探索法来选择高性能的客户端，并根据设定的指标将标记同时奖励给服务器和参与者，以吸引高质量的客户端持续参与 FL。这些方案涉及 3 个子问题中的多个子问题，以更加全面的方式来实现激励机制，这将成为激励方案设计未来的发展趋势。

3.5 联邦学习激励机制的比较

本节对 FL 激励机制的子问题优化的各种方案进行了对比。根据研究的子问题类型、使用技术、实现方法，从模型的性能、隐私安全、计算资源、通信资源、模型复杂度等方面进行对比分析。表 1 列出了 FL 激励机制方案的对比。

表 1 联邦学习激励机制分析比较

Table 1 Analysis and comparsion of incentive mechanism for federated learning

文献	子问题	关键技术	方法描述	优缺点
[18]	贡献测量、支付分配	契约理论	签署契约合同对数据质量进行分级，向不同数据质量级别提供不同的资源包	根据用户数据质量和类型给予奖励，解决了任务发布者和用户之间信息不对称的问题。但是，贡献测量因素单一，隐私安全无法保证
[20]	贡献测量、支付分配	定义贡献指数(CI)	量化了数据提供者的贡献，记录训练过程中的中间结果，并使用这些结果近似计算贡献指数	不需要额外的训练成本就能合理分配利润、有效逼近准确的贡献指数。但是该方案只适用于横向联邦学习
[21]	贡献测量	分层公平联邦学习框架	把所有参与方分为多个不同的贡献水平，并根据贡献水平来确定各参与方的奖励	根据用户贡献分配奖励，灵活性高。但是，训练时间较长，未考虑终端的异构性
[23]	贡献测量	实时贡献测量方法 FedCM	定义了各参与方的影响，综合考虑前一轮和当前轮次，基于注意力聚合得到各参与方的贡献率	实时计算测量各参与方的贡献水平。但是，无法保证隐私安全，且需要额外的计算资源
[24]	客户选择	声誉+反向拍卖+区块链	将声誉保存在区块链中，服务器结合用户声誉和投标价格来选择和支付用户	智能选择可靠用户，模型精度较高，保证隐私安全。但是，模型复杂度较高，计算复杂，只适用于横向联邦学习
[27]	客户选择、支付分配	博弈论+差分隐私	以差分隐私为特征量化隐私损失，并补偿其隐私泄露的成本	激励私人数据用户参与 FL，实现集体效用最大化，但通信成本和计算成本高
[28]	客户选择	拍卖机制	提出一种原始-对偶贪婪算法来解决选择赢家和基于临界值支付的 NP 难问题	最小化能耗成本，最大化用户效用，计算复杂度较低，但无法保证隐私安全
[29]	客户选择	Stackelberg 博弈	选择一组自愿加入模型训练的用户设备协作训练全局模型，以获得最小的训练成本	策略性设置本地迭代的次数，最大化用户效用，模型精度较高，但本地迭代次数多，受 CPU 功率限制
[34]	支付分配	收益共享方案 FLI	以上下文感知的方式动态划分给定的预算，最大化集体效益	具有实时性，减少偿还用户的延迟，保证公平性，但训练时间长，计算复杂
[36]	贡献测量、客户选择、支付分配	多维激励框架 FMore	提出一个基于 K 个赢家的多维采购拍卖激励机制，用于最大化预期利润	模型轻量级且具有兼容性、模型性能好、有效减少训练轮次，但没有考虑外部和内部攻击，增加了额外成本
[37]	贡献测量、客户选择、支付分配	声誉+拍卖机制	设计合理的贡献测量方法建立声誉，通过综合声誉和投标价格选择用户和分配奖励	保证隐私安全，灵活性较高，模型精度高，但模型复杂度高，计算和通信成本高

4 研究展望

FL 作为连接数据孤岛的桥梁，在满足数据隐私安全和监管要求的前提下，客户端可以使用本地模型参与使服务器获得高质量的模型。如何激励高质量的用户持续参与 FL，是保证 FL 被广泛推广和应用的关键。目前，FL 激励机制的研究仍处于起步阶段，贡献测量的合理性、激励机制使用的复杂的技术所带来的昂贵的计算成本、提升 FL 的模型性能以及保证激励机制的安全性等仍是 FL 激励机制尚未解决的问题。本文通过对相关研究进行分析与总结，提出了以下未来可能的研究方向。

(1)贡献测量方法。在 FL 中，参与者提供的资源和模型都是由多个因素共同决定的，单维度量的贡献测量方法不适用于 FL 场景，过于单一或者主观的测量方案都比较容易受到恶意评分者的影响。一个合理的贡献测量方案是激励机制成功的基石。未来的研究需要进一步考虑使用全面且可调整的贡献测量算法。Wang 等[40]利用删除方法来计算水平 FL 的数据样本影响函数，使用 Shapley 值来计算垂直 FL 的数据特征，提供了公平可靠的贡献测量方法；Liu 等[35]提出了一种基于 Shapley 值的 PoSap 共识协议，用于计算每个用户的贡献值，并使用区块链保证了隐私安全。但是，这些方案未考虑可能出现贡献值为负数和恶意用户使用有毒数据训练模型等情况带来的负面影响。同时，在训练过程中用户的资源(如 CPU、内存等)使用状态也是衡量贡献测量的一个重要标准。

(2)计算成本。现阶段的 FL 激励机制大多会使用区块链、Shapley 值、拍卖机制、强化学习以及自定义算法等复杂的技术，这会带来巨大的计算成本和通信开销。这对于资源受限的客户端是非常不友好的，资源受限的用户不愿意付出昂贵的代价执行激励机制。因此，FL 的激励方案应该是轻量级的。Zhang 等[41]将知识系数矩阵参数化，将知识系数矩阵和

模型参数沿着梯度下降交替更新,从而量化每个用户的贡献,不需要额外的训练来进行贡献测量;Song 等[20]通过记录训练过程中的中间结果来近似计算贡献指数。虽然这些方法能有效减少计算成本,但是需要消耗额外的存储资源。未来的研究应该平衡资源消耗和训练收益之间的关系,以最小的能耗达到最大的集体效用。

(3)模型性能。FL 激励机制旨在通过激励更多的高质量客户端加入 FL,以低成本实现高性能的 FL。如果激励机制激励了更多的用户参与 FL,但没有提升甚至降低了 FL 的性能,设计的激励机制就没有意义。Le 等[42]采用随机拍卖机制解决在选择赢家和确定奖励率时出现的 NP 难问题,以最小化社会成本。该方案保证了模型的性能,但模型复杂度高,不能有效平衡通信成本和模型性能。Han 等[38]提出的标记化激励机制在不需要额外训练成本的情况下激励了更多客户端加入 FL,提高了模型的准确性。未来的研究应实现多目标和多功能激励,既要合理分配用户的奖励,也要平衡模型性能和计算成本。

(4)隐私安全。在 FL 系统中,参与方容易受到恶意攻击。例如,客户端将有毒的数据注入训练数据或者直接上传有毒模型,导致产生不正确的梯度模型,从而误导 FL 的全局模型训练,严重影响 FL 的系统性能。区块链作为保证隐私安全的常用技术,也被用于 FL 激励机制的设计中[43]。区块链保证了用户数据不可篡改,但是会带来一定的学习延迟。未来的研究应设计低延迟的共识算法,在保证安全性的同时最大化模型性能。Tahanian 等[44]提出了一个基于博弈论的鲁棒联邦平均算法 GFA,用于检测和丢弃用户提供的坏更新。该系统通过迭代的方式来获得每次用户更新的可信度和最终模型的鲁棒估计,服务器可以通过选择忽略某些用户来避免受到攻击。通过激励机制选择高可靠的用户,从而避免恶意攻击,是一个非常有前景的研究方向。

结束语 联邦学习是一种新兴的机器学习范式,使用用户的数据实现分布式学习,既保证了数据隐私安全,又实现了较优的模型性能,这是未来分布式机器学习的发展趋势。有效的激励机制能够吸引高质量用户积极参与 FL,是 FL 推广和应用的关键环节。本文对联邦学习的激励机制做了深入的调查和分析,根据激励机制在 FL 训练过程中存在的子问题,重点阐述了面向贡献测量、面向客户选择、面向支付分配以及面向多子问题优化的激励机制,分析并对比当前主流的 FL 激励机制,探索了 FL 激励机制当下存在的挑战和未来可能的研究方向。

参 考 文 献

[1] LECUN Y,BENGIO Y,HINTON G. Deep learning[J]. Nature,2015,521(7553):436-444.

[2] LIM W Y B,LUONG N C,HOANG D T,et al. Federated learning in mobile edge networks: A comprehensive survey[J]. IEEE Communications Surveys & Tutorials,2020,22(3):2031-2063.

[3] MCMAHAN B,MOORE E,RAMAGE D,et al. Communication-efficient learning of deep networks from decentralized data[C]// Artificial Intelligence and Statistics. PMLR,2017:1273-1282.

[4] 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,2021,33(3):536-550.

[5] MEHMOOD A,NATGUNANATHAN I,XIANG Y,et al. Protection of big data privacy[J]. IEEE Access,2016,4:1821-1834.

[6] LUNDERVOLD A S,LUNDERVOLD A. An overview of deep learning in medical imaging focusing on MRI[J]. Zeitschrift fur Medizinische Physik,2019,29(2):102-127.

[7] ZHAO Y,ZHAO J,JIANG L,et al. Privacy-preserving blockchain-based federated learning for IoT devices[J]. IEEE Internet of Things Journal,2020,8(3):1817-1829.

[8] AHMED L,AHMAD K,SAID N,et al. Active Learning Based Federated Learning for Waste and Natural Disaster Image Classification[J]. IEEE Access,2020,8:208518-208531.

[9] LI T,SAHU A K,ZAHEER M,et al. Federated optimization in heterogeneous networks[J]. Proceedings of Machine Learning and Systems,2020,2:429-450.

[10] LIU J,WANG J H,RONG C,et al. FedPA:An adaptively partial model aggregation strategy in Federated Learning[J]. Computer Networks,2021,199:108468.

[11] BONAWITZ K,IVANOV V,KREUTER B,et al. Practical secure aggregation for privacy-preserving machine learning[C]// Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. 2017:1175-1191.

[12] LI S B,YANG L,LI C J,et al. Overview of Federated Learning:Technology,Applications and Future[J]. Computer Integrated Manufacturing System,2022,28(7):2119-2138.

[13] ZHAN Y,ZHANG J,HONG Z,et al. A survey of incentive mechanism design for federated learning[J]. IEEE Transactions on Emerging Topics in Computing,2022,10(2):1035-1044.

[14] ZENG R,ZENG C,WANG X,et al. A Comprehensive Survey of Incentive Mechanism for Federated Learning[J]. arXiv:2106.15406,2021.

[15] BLUM A,HAGHTALAB N,PHILLIPS R L,et al. One for one,or all for all:Equilibria and optimality of collaboration in federated learning[C]// International Conference on Machine Learning. PMLR,2021:1005-1014.

[16] ZHANG X N,ZHU J M,GAO S,et al. Federal learning incentive mechanism based on blockchain and Bayesian game[J]. Chinese Science:Information Science,2022,52(6):971-991.

[17] NG K L,CHEN Z,LIU Z,et al. A multi-player game for studying federated learning incentive schemes[C]// Proceedings of the Twenty-Ninth International Conference on International Joint Conferences on Artificial Intelligence. 2021:5279-5281.

[18] KANG J,XIONG Z,NIYATO D,et al. Incentive design for efficient federated learning in mobile networks:A contract theoryapproach[C]//2019 IEEE VTS Asia Pacific Wireless Communications Symposium(APWCS). IEEE,2019:1-5.

[19] ZHAN Y,LI P,QU Z,et al. A learning-based incentive mechanism for federated learning[J]. IEEE Internet of Things Journal,2020,7(7):6360-6368.

[20] SONG T, TONG Y, WEI S. Profit allocation for federated learning[C]// 2019 IEEE International Conference on Big Data(Big Data). IEEE, 2019: 2577-2586.
[21] ZHANG J, LI C, ROBLES-KELLY A, et al. Hierarchically fair federated learning[J]. arXiv: 2004. 10386, 2020.
[22] NISHIO T, SHINKUMAR, MANDAYAM N B. Estimation of individual device contributions for incentivizing federated learning[C]// 2020 IEEE Globecom Workshops. IEEE, 2020: 1-6.
[23] YAN B, LIU B, WANG L, et al. Fedcm: A real-time contribution measurement method for participants in federated learning[C]// 2021 International Joint Conference on Neural Networks(IJCNN). IEEE, 2021: 1-8.
[24] ZHANG J, WU Y, PAN R. Incentive mechanism for horizontal federated learning based on reputation and reverse auction[C]// Proceedings of the Web Conference 2021. 2021: 947-956.
[25] TANG M, WONG V W S. An incentive mechanism for cross-silo federated learning: A public goods perspective[C]// IEEE INFOCOM 2021-IEEE Conference on Computer Communications. IEEE, 2021: 1-10.
[26] 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.
[27] HU R, GONG Y. Trading data for learning: Incentive mechanism for on-device federatedlearning[C]// GLOBECOM 2020—2020 IEEE Global Communications Conference. IEEE, 2020: 1-6.
[28] 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.
[29] KHAN L U, PANDEY S R, TRAN N H, et al. Federated learning for edge networks: Resource optimization and incentive mechanism[J]. IEEE Communications Magazine, 2020, 58(10): 88-93.
[30] PANDEY S R, TRAN N H, BENNIS M, et al. A crowdsourcing framework for on-device federated learning[J]. IEEE Transactions on Wireless Communications, 2020, 19(5): 3241-3256.
[31] CONG M, YU H, WENG X, et al. A vcg-based fair incentive mechanism for federated learning[J]. arXiv: 2008. 06680, 2020.
[32] LEE J, KIM D, NIYATO D. A Novel Joint Dataset and Incentive Management Mechanism for Federated Learning Over MEC [J]. IEEE Access, 2022, 10: 30026-30038.
[33] PANDEY S R, TRAN N H, BENNIS M, et al. Incentivize to build: A crowdsourcing framework for federated learning[C]// 2019 IEEE Global Communications Conference(GLOBECOM). IEEE, 2019: 1-6.
[34] YU H, LIU Z, LIU Y, et al. A sustainable incentive scheme for federated learning[J]. IEEE Intelligent Systems, 2020, 35(4): 58-69.
[35] LIU Y, AI Z, SUN S, et al. Fedcoin: A peer-to-peer payment system for federated learning[M]// Federated Learning. Cham: Springer, 2020: 125-138.
[36] ZENG R, ZHANG S, WANG J, et al. Fmore: An incentive scheme of multi-dimensional auction for federated learning in mec[C]// 2020 IEEE 40th International Conference on Distributed Computing Systems(ICDCS). IEEE, 2020: 278-288.
[37] ZHANG J, WU Y, PAN R. Auction-Based Ex-Post-Payment Incentive Mechanism Design for Horizontal Federated Learning with Reputation and Contribution Measurement [J]. arXiv: 2201. 02410, 2022.
[38] HAN J, KHAN A F, ZAWAD S, et al. Tokenized Incentive for Federated Learning[C]// Proceedings of the Federated Learning Workshop at the Association for the Advancement of Artificial Intelligence(AAAI) Conference. 2022.
[39] WANG Z, HU Q, LI R, et al. Incentive Mechanism Design for Joint Resource Allocation in Blockchain-based Federated Learning[J]. arXiv: 2202. 10938, 2022.
[40] WANG G, DANG C X, ZHOU Z. Measure contribution of participants in federated learning[C]// 2019 IEEE International Conference on Big Data(Big Data). IEEE, 2019: 2597-2604.
[41] ZHANG J, GUO S, MA X, et al. Parameterized Knowledge Transfer for Personalized Federated Learning[J]. Advances in Neural Information Processing Systems, 2021, 34: 10092-10104.
[42] LE T H T, TRAN N H, TUN Y K, et al. Auction based incentive design for efficient federated learning in cellular wireless networks[C]// 2020 IEEE Wireless Communications and Networking Conference(WCNC). IEEE, 2020: 1-6.
[43] GAO L, LI L, CHEN Y, et al. FGFL: A blockchain-based fair incentive governor for Federated Learning[J]. Journal of Parallel and Distributed Computing, 2022, 163: 283-299.
[44] TAHANIAN E, AMOUEI M, FATEH H, et al. A game-theoretic approach for robust federated learning[J]. International Journal of Engineering, 2021, 34(4): 832-842.

LIANG Wen-ya, born in 1997, postgraduate. Her main research interests include federated learning and incentive mechanism.

LIU Bo, born in 1968, Ph.D, professor, is a member of China Computer Federation. His main research interests include cloud computing, big data technology and distributed security technology.

LIN Wei-wei, born in 1980, Ph.D, professor, is a member of China Computer Federation. His main research interests include cloud computing, big data technology and AI application technology.

（责任编辑：喻藜）