软件学报 ISSN 1000-9825, CODEN RUXUEW
2024,35(12):5725−5740 [doi: 10.13328/j.cnki.jos.007085] [CSTR: 32375.14.jos.007085]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

跨设备联邦学习中的客户端选择算法*

张瑞麟[1], 杜晋华[1], 尹 浩[2]

[1](清华大学 计算机科学与技术系, 北京 100084)

[2](清华大学 北京信息科学与技术国家研究中心, 北京 100084)

通信作者: 尹浩, E-mail: h-yin@mail.tsinghua.edu.cn

摘 要: 联邦学习是一种新型的分布式机器学习范式, 它在满足用户隐私和数据保密性要求的前提下, 充分利用众多分散客户端的计算能力及其本地数据联合训练机器学习模型. 在跨设备联邦学习场景下, 客户端通常由数千甚至万级别的移动设备或端侧设备组成, 由于通信和计算成本的限制, 聚合服务器在每个训练轮次中仅选择少量客户端加入训练. 几种被广泛应用的联邦优化算法均采用完全随机的客户端选择算法, 但这被证明有着很大的优化空间. 近年来, 如何高效可靠地从海量异构客户端中选择合适的集合参与训练, 以优化联邦学习协议的资源消耗和模型性能被广泛研究, 但仍没有文献对这一关键问题进行综合调研. 需要对跨设备联邦学习的客户端选择算法研究进行全面调研. 具体地, 形式化描述客户端选择问题, 然后给出对选择算法的分类并逐一深入讨论分析. 最后, 讨论客户端选择算法的一些未来研究方向.

关键词: 跨设备联邦学习; 客户端选择; 组合优化; 效用理论

中图法分类号: TP303

中文引用格式: 张瑞麟, 杜晋华, 尹浩. 跨设备联邦学习中的客户端选择算法. 软件学报, 2024, 35(12): 5725–5740. http://www.jos.org.cn/1000-9825/7085.htm

英文引用格式: Zhang RL, Du JH, Yin H. Client Selection Algorithm in Cross-device Federated Learning. Ruan Jian Xue Bao/Journal of Software, 2024, 35(12): 5725–5740 (in Chinese). http://www.jos.org.cn/1000-9825/7085.htm

Client Selection Algorithm in Cross-device Federated Learning

ZHANG Rui-Lin[1], DU Jin-Hua[1], YIN Hao[2]

[1](Department of Computer Science and Technology, Tsinghua University, Beijing100084, China)

[2](Beijing National Research Center for Information Science and Technology, Tsinghua University, Beijing100084, China)

Abstract: As a new type of distributed machine learning paradigm, federated learning makes full use of the computing power of many distributed clients and their local data to jointly train a machine learning model under the premise of meeting user privacy and data confidentiality requirements. In cross-device federated learning scenarios, the client usually consists of thousands or even tens of thousands of mobile devices or terminal devices. Due to the limitations of communication and computing costs, the aggregation server only selects few clients for the training during each round of training. Meanwhile, several widely employed federated optimization algorithms adopt a completely random client selection algorithm, which has been proven to have a huge optimization space. In recent years, how to efficiently and reliably select a suitable set from massive heterogeneous clients to participate in training and thus optimize the resource consumption and model performance of federated learning protocols has been extensively studied, but there is still no comprehensive investigation on the key issue. Therefore, this study conducts a comprehensive survey of client selection algorithms for cross-device federated learning. Specifically, it provides a formal description of the client selection problem, then gives the classification of selection algorithms, and discusses and analyzes the algorithms one by one. Finally, some future research directions for client selection algorithms are explored.

Key words: cross-device federated learning; client selection; combinatorial optimization; utility theory

* 基金项目: 国家重点研发计划 (2022YFB2702801); 国家自然科学基金 (92067206, 61972222, 62102217)
收稿时间: 2023-02-22; 修改时间: 2023-09-08; 采用时间: 2023-10-26; jos 在线出版时间: 2024-03-20
CNKI 网络首发时间: 2024-03-23

1 引 言

随着移动互联网和物联网等技术的飞速发展, 使用分布式的、碎片化的数据进行联合机器学习的需求变得越来越迫切. 传统的数据中心分布式机器学习要求将所有原始训练数据汇聚到中央服务器或数据中心, 然后在机器集群上使用 GPU 等并行计算硬件训练机器学习模型[1−3]. 这种方式严重侵犯了数据拥有者的隐私[4], 并且在通信资源受限的环境下, 传输原始数据十分低效, 这大幅度地阻碍了人工智能技术的实用化. 针对上述问题, 谷歌于 2016 年提出了联邦学习 (federated learning, FL), 一种隐私保护的分布式机器学习范式[5]. 典型的联邦学习系统由中央聚合服务器作为协调器, 使用众多分散客户端的本地数据训练联合机器学习模型. 客户端在本地独立地更新模型, 并且通过加密的方式向聚合服务器仅传输必要的中间结果 (模型参数或迭代梯度) 而不是原始数据. 联邦学习无需客户端上交原始数据, 从而保证了数据拥有者的隐私安全. 同时, 联邦学习通过充分利用分散的终端设备算力进行并行计算和使用最小化的中间结果来同步训练提升了分布式机器学习的效率[6].

在应用最为广泛的跨设备 (cross-device) 联邦学习场景下, 客户端通常由数千甚至万级别的异构终端设备 (例如手机、摄像头、智能汽车) 组成, 并且存在大量资源受限制的个体[7]. 由于网络通信、本地计算成本和设备活跃时间等因素的限制[8], 聚合服务器在每个训练轮次中只能选择少量客户端参与联合训练, 即使文献 [5] 的相关实验证明当每轮次参与训练的客户端数据无法覆盖所有的数据分布时, 选择更多的客户端参与训练可以加速联合模型的收敛速度. 因此, 联邦学习协议的一个核心流程就是在每个训练轮次开始之前筛选出参与本轮训练的客户端集合, 简称为“客户端选择”. 几种被广泛应用的联邦优化算法 (FedAvg[5]、FedProx[9]、FedYoGi[10]) 都采用了随机的客户端选择算法, 这是合理的, 因为传统的联邦学习不收集客户端的任何特征信息. 这种完全随机的无偏客户端选择算法得到了理论的收敛证明[9], 但同时也被证明有着很大的优化空间[11]. 近年来, 众多文献致力于研究更复杂的客户端选择算法, 以优化联邦学习的资源消耗 (通信和计算成本) 和联合模型性能 (模型精度和训练速度). 这些研究遵循着统一的思路: 将聚合服务器对于客户端的特征信息从无状态转变为有状态, 并使用这些特征信息计算候选客户端集合的效用值, 以选择拥有最优 (或次优) 效用值的客户端集合. 这引发了一系列新的挑战, 例如如何设计与最终优化目标强相关的效用函数, 如何高效收集海量异构客户端的实时特征信息等.

随着联邦学习被广泛研究和应用 (如谷歌 Gboard 输入法[12]、iPhone 的自动语音识别功能[13]), 众多相关综述文章被发表, 它们几乎涵盖联邦学习的所有关键问题及延伸领域, 如文献 [4,6,7] 概述了联邦学习的通用概念和应用挑战, 文献 [14,15] 概述了联邦学习的激励机制, 文献 [16] 描述了数据隐私和安全性方面的问题, 文献 [17] 描述了联邦学习公平性相关的解决方案, 文献 [18] 总结了联邦学习的开源框架. 但尚未有一篇文章从客户端选择算法这一关键问题出发, 进行深入分析、讨论和总结. 本文旨在综述 2017–2022 年关于联邦学习客户端选择算法的研究文献以填补这个空白. 具体地, 本文的贡献可以描述如下.

(1) 我们给出了客户端选择问题的形式化描述, 包括通用假设、问题抽象和现存挑战 (第 2 节).

(2) 通过对现有研究文献的总结, 我们根据定义客户端集合效用函数所使用的主要特征信息的不同, 将客户端选择算法划分为 3 类, 即基于数据效用、基于资源效用和基于数据与资源效用. 我们对每一类算法进行了深入分析和讨论, 并对其代表性工作进行了总结与对比 (第 3 节).

(3) 我们列出了几个关于客户端选择算法的未来研究方向. 对于每一个方向, 我们总结了现有文献中的不足并进行了深入讨论 (第 4 节).

2 联邦学习客户端选择算法概述

本节的目的是给出联邦学习中的客户端选择算法 (后续简称“选择算法”) 的形式化描述和讨论. 为了更好地理解这个问题, 我们必须先明确选择算法的研究目标和通用假设. 关于联邦学习的基础概念和算法工作流程, 我们建议读者阅读文献 [5−7].

2.1 客户端选择算法的研究目标

和传统的分布式机器学习相比, 联邦学习的客户端 (数据源) 通常拥有强异构性, 具体体现如下.

(1) 数据异构性: 客户端的私有数据一般来源于特定的用户个体或区域内的用户群体, 这导致了客户端私有数据之间通常是非独立同分布的, 且私有数据量相差巨大[19].

(2) 资源异构性: 不同客户端可提供的用于联邦学习任务的系统资源 (例如计算能力、网络带宽等) 相差巨大, 并且存在大量资源受限的个体[20].

客户端强异构性是区别联邦学习和数据中心分布式机器学习的关键特性. 异构性给联邦学习带来了一系列新的挑战, 最显著的是劣质者和掉队者问题[21−23]. 劣质者是指拥有低质量数据 (如持有大量错误标签样本) 的客户端, 聚合劣质者提交的本地模型参数会减缓联邦训练的收敛, 并降低联合模型的精度. 掉队者是指在同步联邦学习协议中, 因网络分区或资源受限等原因, 某一客户端回传本地模型参数的时间远远落后于其余客户端, 大幅度降低了整体联邦训练的效率.

选择算法是缓解客户端异构性问题的有效方案. 聚合服务器通过合理的选择在开始训练前尽可能地避开劣质者和掉队者, 从而提升联邦训练的收敛速度和联合模型的精度. 相比于其他异构性问题解决方案[21,24,25], 选择算法具有诸多优点, 例如, 不改变联邦学习的同步协议模型 (使得联邦学习仍能够与众多基于同步假设的隐私保护方法[26−28]结合)、不盲目地浪费系统资源 (例如因避免掉队者而超额选择客户端, 增加计算和通信成本[24])、对本地更新和本地模型参数回传等核心流程是非侵入性的, 因此可以选择性地与其他优化方法 (如参数压缩[29]、梯度压缩[30]、限制本地更新模型发散[31]、混合精度本地更新[32]) 结合.

2.2 客户端选择算法的通用假设

在具体描述选择算法流程之前, 了解该问题的研究边界是有必要的. 基于现有的大量文献研究, 我们总结出选择算法研究的通用假设.

(1) 跨设备场景而不是跨孤岛 (cross-silo) 场景: 通常, 在跨孤岛联邦学习[33]场景下, 客户端均为具有优质计算资源和数据 (同质化) 的稳定参与者, 一般采用全量参与模型训练的方式进行[34], 无需客户端选择算法.

(2) 完全发掘设备数据的价值需要多轮迭代: 对于所有设备的本地数据价值都可以在一轮次的训练中被完全发掘的场景, 已经参与过训练的客户端没有必要被再次选择. 客户端的特征信息将完全失效, 并且重复选择部分客户端可能造成联合模型的有偏和过拟合. 此时随机选择算法 (或者无放回的随机选择算法) 将是相当好的方案, 比如基于多项分布的 MD 客户端选择算法和在其基础上改进的基于聚类的 clustered sampling 算法, 都满足无偏采样的假设, 这意味着每次迭代的全局模型的期望是无偏的, 因此保证了客户端在期望中得到适当的表示[35]. 注意不能简单地增加客户端的本地训练时期 (epoch) 以符合上述场景, 因为这将严重影响联合模型的精度[5].

(3) 节点都是诚实可信的志愿者: 聚合服务器和客户端都被假定为诚实可信的志愿者, 即系统中不存在拜占庭节点[36]对系统发起恶意攻击 (如使用对抗生成网络生成虚假的私有数据[37]). 在隐私保护的前提下, 客户端志愿提供真实的全量私有数据用于联合训练, 不会主动提供虚假信息以干扰聚合服务器的决策. 聚合服务器对客户端的选择是完全客观无偏见的. 但需要注意的是, 节点仍可能存在故障性容错 (例如网络分区, 长时间垃圾回收造成进程无响应等)[38].

(4) 联邦学习任务对客户端的数据和资源是独占的: 客户端的系统资源和数据几乎完全由当前的联邦学习任务进程独占, 即探测到的特征信息在本轮次持续时间内几乎无波动[39], 本地更新过程中私有数据不发生改变[40].

上述假设基于对大量现有相关研究进行分析与总结. 部分假设是隐式甚至无感知的, 或者根据算法的设计细节推断而来. 在具体的研究中, 上述假设不一定完全成立, 例如文献 [41] 基于区块链上数据的不可篡改和可追溯的特性, 采用分布式的多方验证模式提供对恶意客户端的筛查和惩罚机制, 从而降低了假设 (3) 的要求.

2.3 客户端选择算法的形式化描述与分类

图 1 概括了融入了选择算法的联邦学习协议的通用流程. 我们定义 K^t 为轮次 t 中可供选择的客户端集合, 其大小为 $K=|K^t|$. 聚合服务器每轮次仅选择 m 个客户端参与训练, 其中 $m=\lceil K\times p\rceil$, $p\in(0.0,1.0]$. 在轮次 t 初始, 聚合服务器向客户端集合 B^t 发送特征收集请求, 其中 $m\leqslant|B^t|\leqslant K$ (①). 所有收到特征收集请求的客户端 C_i 将回复自身实时的多维度特征信息 R_i^t, 例如可用网络带宽、处理器资源、本地数据量 (②). 对于任意客户端集合 A^t, 聚合

服务器使用客户端实时特征 R_i^t 及历史特征 H_i 定义集合的效用函数 (utility function), 公式为 $Util(A^t)=u(R_i^t,H_i),\ i\in A^t$. 针对特定的效用函数, 聚合服务器使用不同的筛选策略选择出本轮次参与训练的集合 S^t. 在绝大部分研究中, 筛选策略可以被抽象成一个组合优化问题, S^t 则是该问题的最优 (或次优) 解. 如表 1 所示, 绝大多数筛选策略的优化目标可以被抽象总结为两类 (③).

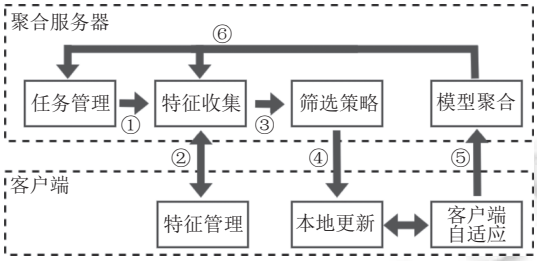

图 1 带有客户端选择算法的联邦学习协议

表 1 筛选策略优化目标分类

筛选策略优化目标	数学描述	核心思想	最大计算复杂度
最大化效用值	$\begin{cases} S^t\triangleq\max Util(A^t) \\ \text{s.t.}\ \begin{cases} \lvert A^t\rvert=m \\ A^t\subset K^t \end{cases} \end{cases}$	选择一定数目的客户端参与训练, 最大化客户端集合效用值	$O\left(\binom{K}{m}\right)$
最大化客户端数量	$\begin{cases} S^t\triangleq\max\lvert A^t\rvert \\ \text{s.t.}\ \begin{cases} \lvert A^t\rvert\leqslant K \\ A^t\subset K^t \\ Util(A^t)\geqslant u^t \end{cases} \end{cases}$	在最小效用阈值 u^t 的限制下, 尽可能多地选择客户端	$O(2^K)$

客户端筛选完成后, 聚合服务器向 S^t 中的所有客户端发送上一轮次的联合模型 $\bar{w}^{t-1}$. 客户端 C_i 使用本地数据, 基于特定的优化算法 (如随机梯度下降[42]) 更新联合模型为局部模型 w_i^t (④). 现有部分研究[43,44]在客户端侧本地模型训练的前后添加额外策略或流程, 我们将其归纳命名为“客户端自适应”. 最后, 聚合服务器收集所有的局部模型参数, 通过聚合算法 (如按数据量作为权重[5]) 得到新的联合模型 $\bar{w}^t=Aggregate(w_i^t),\ i\in S^t$ (⑤). 通常, 聚合服务器根据聚合结果更新客户端的历史特征信息 H_i, 并使用新的联合模型 $\bar{w}^t$ 进行 $t+1$ 轮次的训练 (⑥). 上述单轮次训练流程将持续被重复直到联合模型的评价指标达到预先设定的目标.

相较于传统联邦学习协议, 选择算法在其流程中附加了特征收集 (包括客户端侧特征管理), 筛选策略和客户端自适应这 3 个新环节.

● 特征收集. 采集和管理客户端的特征信息. 根据客户端特征信息反映客户端状态的实时性强弱, 我们将其分类为实时特征 R_i^t 和历史特征 H_i. R_i^t 主要反映在本轮次持续事件内, 客户端的强实时性特征信息, 例如可用网络带宽[45]. H_i 主要反映客户端的弱时变性特征信息, 如在历史任务的贡献和可靠性. 筛选策略通常综合考量二者以预测客户端在当前训练轮次中的效用[46,47].

● 筛选策略. 根据客户端特征信息, 基于特定筛选策略, 选择本轮次参与训练的客户端集合. 首先, 聚合服务器根据最终的优化指标 (如更高的训练效率或更少的全局通信) 设计收集的特征信息种类, 再基于特征设计客户端集合的效用函数 u[48], 即 $Util(A^t)=u(R_i^t,H_i),\ i\in A^t$. 部分研究拥有非常直观的效用函数, 例如 FedCS[38]直接使用客户端集合的轮次物理训练时间估计值作为集合效用. 但由于模型本地更新和聚合过程的可解释性差, 有时很难精确地量化描述特征信息与最终优化目标之间的关系[49]. 因此, 部分研究采用神经网络模型作为效用函数 u, 但因为离线训练的模型无法很好地适应动态的联邦学习场景, 部分研究引入强化学习方法来持续迭代更新网络模型[50].

基于对现有研究中使用的客户端特征信息的分析, 我们进一步将客户端集合效用函数描述为:

$$Util(A^t)=u(Util_D(A^t),Util_R(A^t))=u(u_D(R_i^t,H_i),u_R(R_i^t,H_i)),\ i\in A^t \tag{1}$$

其中, $Util_D(A^t)$ 为 A^t 的数据效用, 它对应着“数据质量”概念, 主要映射客户端之间的数据异构性信息, 选择高数据效用的客户端集合能提升联邦学习的训练效率, 即减少达到指定模型精度所需要的训练轮次数目. $Util_R(A^t)$ 为 A^t 的资源效用, 它对应“节点系统性能”指标, 用于描述客户端的资源异构性信息, 选择高资源效用的客户端集合能提升联邦训练的速度, 即每个轮次消耗的物理时间更短.

通过上述分析, 我们发现聚合服务器用以计算效用函数的特征信息可以被归纳为数据特征和资源特征两类. 因此, 根据定义客户端效用函数时对数据效用和资源效用的不同程度考量, 我们将现有的客户端选择算法归纳为 4 类, 详见表 2.

表 2 客户端选择算法分类及代表性工作

名称	效用函数	效用函数意义	代表性工作
随机选择	常量函数	不考虑数据效用和资源效用, 认为所有客户端集合效用完全相同	FedAvg[5]、FedProx[9]、FedOpt[10]
基于数据效用	$Util_D(A^t)$	仅考虑数据效用	Power-of-choice[51]、Favor[40]、AFL[52]
基于资源效用	$Util_R(A^t)$	仅考虑资源效用	FedCS[39]、FedMCCS[53]、TiFL[54]
基于数据与资源效用	$u(Util_D(A^t), Util_R(A^t))$	联合考虑数据效用和资源效用	Oort[55]、PyramidFL[43]、文献[56]

图 2 更为清晰地展示了 4 类选择算法的不同. 筛选策略问题的任一可行解 S^t_{fea} 可以映射到<资源效用, 数据效用>二维平面上的一个点, 这样的抽象将筛选策略转变为了求解双目标优化问题. 图 2 中使用黑色虚线连接了该问题的所有帕累托最优解, 即无法找到一个可行解在两个目标维度上均优于帕累托最优解. 选择算法因效用函数的不同在平面上拥有不同的最优效用方向或曲线, 因此对应不同的最优解 S^t_{opt} (红色标出). 随机算法以常量作为效用函数, 因此其最优效用方向与平面垂直, 即任一可行解都是最优解. 基于数据效用和基于资源效用的选择算法分别取帕累托最优解集的两个极端值做最优解, 因为它们仅考虑单维度上效用最大化. 对于基于数据与资源效用的选择算法, 需要根据其效用函数表达形式确认最优解的选取, 但容易发现, 当效用函数被描述为数据效用和资源效用的线性组合时, 即 $\alpha \times Util_D(A^t) + (1-\alpha) \times Util_R(A^t)$, 其最优解属于帕累托最优解集, 并且通常能够在单维度效用损失可接受的情况下达成数据效用与资源效用的均衡. 我们将在第 3 节对上述各类选择算法进行更详细地分析、讨论和总结.

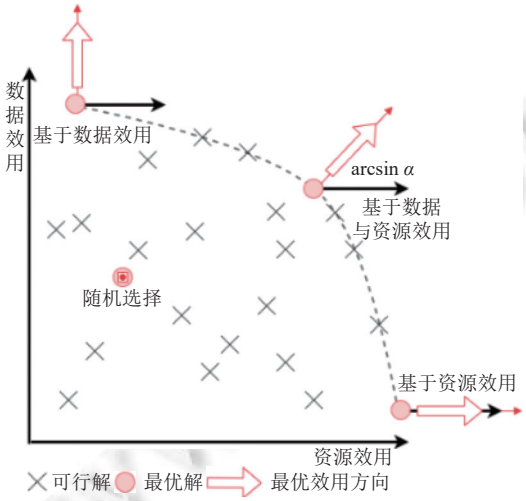

图 2 客户端选择算法分类对最优解的影响

● 客户端自适应. 基于对现有研究的分析, 我们发现诸多选择算法研究在客户端侧本地更新前后设计了相似的策略或流程以进一步收集特征信息并指导聚合服务器的决策, 我们将其归纳命名为客户端自适应. 一方面, 位于客户端侧的自适应策略能够更稳定高效地获取到本地特征, 特别是那些不能被共享的隐私信息和本地更新过程的

中间结果, 因此能够更好地量化客户端的效用. 另一方面, 聚合服务器端的筛选策略仅利用了被选择者和未被选择者的异构性信息, 而客户端自适应进一步探索了被选择者之间的异构性信息, 因此提供更细粒度的筛选. 例如文献 [43] 使客户端根据自身的资源排名状况自适应地调节本地更新时期, 以此来减少同步协议中因客户端资源差异的木桶效应所带来的时间浪费, 文献 [44,57] 旨在客户端自适应感知本地新模型的隐含的梯度信息量, 在梯度信息量低于阈值 (本地数据分布和全局数据分布相关性较差) 时, 放弃上传本地更新结果, 从而降低联邦学习系统的网络通信量.

2.4 客户端选择算法的现存挑战与解决方案

选择算法大幅度地扩展了基础的联邦学习协议, 但这些扩展进一步扩大了联邦学习所面临的部分传统挑战 (如客户端异构性、隐私泄露等), 并且引入了许多新的潜在问题[58,59]. 我们总结了目前选择算法研究主要面临的 4 个主要挑战, 即可扩展性挑战、公平性挑战、隐私安全性挑战和异常数据鲁棒性挑战.

● 可扩展性挑战. 选择具有最优效用值的客户端集合通常需要收集全部客户端的实时精确多维度特征信息, 并采用遍历所有可能的客户端集合 (或采用相同复杂度的算法) 以搜索全局最优选择. 这将给联邦学习协议引入大量额外开销, 具体包括一次面向所有客户端的特征收集请求广播、 K 次多维度特征采集和表 1 中列出的筛选策略最大计算开销. 在实际的联邦学习系统中, 特别是在资源受限的跨设备场景中, 引入大量附加通信和计算的优化方案是不可行的[11], 但现有部分选择算法研究忽略了这个问题, 这大大降低了选择算法的可扩展性, 阻碍了联邦学习的实用化进程.

目前很多研究已经注意到可扩展性挑战并尝试解决它. 一部分研究仅收集少量客户端的特征信息或使用陈旧的特征信息来计算效用, 以此来降低特征收集环节的开销, 例如文献 [51] 基于多臂老虎机[60]的思想设计了“探索-利用 (exploration-exploitation)”算法, 使选择算法的通信开销保持在可接受范围内, 同时很好地平衡了选择已知节点和探索未知节点的冲突. 另一部分研究针对筛选策略设计快速近似算法选择次优的客户端集合, 以达到可扩展性与效用最大化的均衡. 例如文献 [39] 使用基于贪心策略的启发式算法来解决背包约束下的子模函数最大化问题, 将筛选策略由 NP-hard 问题转变为多项式时间可解问题. 文献 [49] 通过引入一个带注意力机制的编码器-解码器[61]网络模型, 使聚合服务器可以做出顺序决策, 大大降低了筛选策略的整体搜索空间.

● 公平性挑战. 公平联邦学习 (fairness-aware FL) 已经成为近期研究的一个热点, 它旨在更多考虑客户端的利益和公平待遇, 以提升客户端参与联邦学习任务的积极性[62−64]. 以最大化聚合服务器利益为目标的客户端选择算法通常面临着公平性问题, 例如选择倾斜, 即高效用的客户端持续被选择, 而低效用的客户端可能永远无法参与训练. 选择倾斜使得客户端遭受不公平待遇, 很少被选择的客户端无法使用联合模型泛化映射出本地数据分布, 因此降低了维护联邦学习生态的意愿[65]. 对部分客户端的过度采样也使得联合模型偏向部分数据, 从而损害联合模型的精度[11].

部分研究尝试在有偏的客户端选择中提供公平性保证. 例如, 文献 [66,67] 基于李雅普诺夫优化算法, 在客户端选择过程中引入了一个长期约束, 并保证每个客户端的平均参与率不低于一个预期的值. 文献 [68] 提出了一种具有公平约束的基于声誉的客户端选择算法, 声誉根据客户端历史训练任务表现计算. 公平约束用以控制声誉和被选择次数的权衡, 以限制声誉良好但已多次参与训练的客户端持续被选择. 文献 [69] 使用杰恩指数 (Jain's index)[70]量化定义了客户端选择中的公平性指标, 并在选择算法的设计中提供了高公平性指标的保证. 但值得注意的是, 增强选择算法的公平性并不是要保证每个客户端拥有相同的概率被选择, 客户端异构性仍是我们要考虑的主要因素.

● 隐私安全性挑战. 虽然我们没有限定聚合服务器收集的特征信息种类, 但这并不代表客户端志愿提供所有特征信息, 特别是原始数据或本地数据分布等隐私信息, 这违反了联邦学习的初衷. 同样地, 聚合服务器也不应该向客户端泄露除联合模型外的隐私信息, 如验证集数据. 但为了收集更清晰的特征信息以达到更优的选择效果, 部分研究降低了隐私保护级别. 例如, 文献 [71] 规定聚合服务器需要分享一部分验证集数据作为微型验证集, 客户端在本地更新过程后使用微型验证集来评估局部模型性能, 并通过淘汰性能阈值以下的客户端来压缩通信. 文献 [72] 根据客户端上传的梯度信息反推本地数据的分布, 以实现选择算法对数据分布的全覆盖. 对于梯度信息的反推可能会泄露本地数据的额外隐私信息[73], 这违反了一些场景下的隐私保护规定.

● 异常数据鲁棒性挑战. 虽然我们已经假定了客户端不存在主观恶意的攻击行为, 但并不意味着所有客户端的本地数据都是准确无误的. 例如, 在监督学习任务中, 客户端可能遭受系统外节点的投毒攻击[74]从而拥有完全错误的数据标签. 选择算法的设计应适当考虑到异常数据的存在, 避免聚合异常梯度造成联合模型发散或精度损失.

目前, 已有研究注意到异常数据的影响, 并改进选择算法以增强其鲁棒性. 例如, 文献 [55] 在每轮次的选择中直接抛弃了拥有阈值 (例如数据效用 95% 分位数值) 以上数据效用的客户端, 但这是一种“悲观”的算法, 即假定异常数据总是存在, 很有可能淘汰了真正有价值的优质客户端个体. 文献 [56] 结合了基于契约理论的激励机制, 提交异常模型参数的个体将拥有更低的声誉, 后续聚合服务器将参考声誉信息鉴别异常数据源.

3 联邦学习客户端选择算法分类讨论

3.1 基于数据效用

基于数据效用的选择算法利用本地数据的统计特征信息来计算客户端集合的效用, 并通过效用映射数据质量这一抽象概念, 以最优化联合模型的训练效率 (达到特定准确率所需要的训练轮次)[51]或压缩通信量[71]. 通过对现有研究的总结, 其效用函数可以被总结为:

$$Util(A^t)=Util_D(A^t)=u(|\mathcal{D}_i|,\mathcal{L}\left(\bar{w}^{t-1},\mathcal{D}_i\right),Diverse(\mathcal{D}_i)),\ i\in A^t \tag{2}$$

其中, $\mathcal{D}_i$ 是客户端 i 的本地数据集, $|\mathcal{D}_i|$ 即代表本地数据样本数量. 文献 [5] 的实验证明越多的样本数量对应轮次中更多的本地迭代次数并加速了联合模型的收敛, 因此 $|\mathcal{D}_i|$ 与 $Util(A^t)$ 通常正相关. $|\mathcal{D}_i|$ 的采集被认为是极低开销的, 因为在绝大多数的持久化数据存储设施中都拥有类似“行号”的数据结构直接记录总样本数量. 并且由于联邦学习任务的独占性假设, $|\mathcal{D}_i|$ 的值可以在首个训练轮次开始前被单独收集, 不附加任何后续通信.

$\mathcal{L}(\bar{w}^{t-1},\mathcal{D}_i)$ 代表本地数据在上一轮次联合模型 $\bar{w}^{t-1}$ 上的损失函数值 (例如 L2 范数损失函数值). 损失函数衡量了模型预测结果与真实数据标签的差异程度, 损失函数值越大, 说明模型越无法反映本地数据的真实分布情况[75]. 在传统集中式机器学习中, 通过有偏地使用损失函数值大的数据样本来提升模型收敛速度已被充分研究[76−78]. 针对联邦学习场景, 文献 [11] 理论证明了有偏选择损失函数值大的客户端参与训练同样能够提升联合模型的收敛速度, 并基于此提出了损失函数感知的客户端选择算法 power-of-choice. 不同于数据量特征, 损失函数值的计算需要所有数据样本都经过模型进行前向传播计算, 并且上一轮次的计算结果不能复用. 因此, 收集全量客户端的实时损失函数值 $\mathcal{L}(\bar{w}^{t-1},\mathcal{D}_i),\ i\in K^t$ 是不现实的. 目前的很多研究旨在压缩损失函数值采集过程中的计算和通信代价, 它们的方法可以被概括为样本抽样、客户端抽样和使用旧的损失函数这 3 种. 样本抽样即仅抽样少量数据计算损失函数值以减小前向传播的计算次数[71], 即 $\mathcal{L}(\bar{w}^{t-1},d_i),d_i\subset\mathcal{D}_i,\ i\in K^t$. 客户端抽样即每轮次仅计算少量客户端的损失函数值以此来减少通信量. 例如文献 [79] 设计了基于多臂老虎机思想的算法达到了探索-利用的均衡[80], 将每轮次的通信量限制在可容忍范围, 同时又能在已探索的集合内选择次优客户端集合来加速收敛. 使用旧的损失函数即客户端的损失函数值仅在被选择的下一轮次才被更新, 否则使用历史的值代替[52], 即当 $i\notin S^t$, $\mathcal{L}_i^{t+1}=\mathcal{L}_i^t$. 但 UCB-CS[69]证明了持续使用历史损失函数值可能会造成联合模型发散, 因此使用一个本地更新中计算得到的历史损失函数积累值来代替 $\mathcal{L}(\bar{w}^{t-1},\mathcal{D}_i)$, 这种方法使得效用值可以随着本地更新过程被计算从而不附加额外的通信, 并且很好地解决了使用历史损失函数值的模型发散问题.

$Diverse(\mathcal{D}_i)$ 代表的是数据多样性. 许多客户端实质上提供了相似的冗余梯度信息, 传输和计算这些冗余信息造成了资源的浪费, 也降低了训练效率. 数据的多样性即本地数据分布对整体数据分布的映射程度. 客户端集合的数据多样性越强, 其聚合模型更接近使用所有客户端参与训练得到的模型, 数据多样性越弱, 聚合模型就更偏离整体数据分布. 目前许多研究使用数据多样性定义效用, 例如 DivFL[81], 它将选择最大化数据多样性集合的问题抽象为一个具有基数约束的子模函数最大化问题[82], 并借由贪心算法实现了这个 NP-hard 问题的多项式时间近似算法[83]. 同时, 从分布式优化的角度出发, DivFL 通过在非独立同分布数据、部分设备参与和本地更新的实际假设下的收敛性行为分析, 充分说明数据多样性给联邦学习带来的增益, 包括提高训练的效率与公平性. 文献 [75] 将客户端多样性量化为本地数据包含的标签类别数量, 并通过实验证明了在部分场景下, 当本地数据包

含的类别数量越多, 其本地模型和聚合模型的误差越小. Favor[40]基于深度双 Q 网络 (DDQN), 通过局部模型参数拟合本地数据分布, 根据模型准确率设定激励, 从而提升联邦学习的训练效率, 这本质上也是以数据多样性为目标的筛选策略.

3.2 基于资源效用

我们将资源定义为客户端为联邦学习任务提供的除本地数据之外的用于保证运行时环境的物理要素, 如处理器资源、网络带宽、设备能耗, 物理位置等. 基于资源效用选择客户端集合通常是为了避开掉队者并防止因聚合服务器长时间同步阻塞导致轮次失败, 以此来优化训练轮次的物理时耗. 目前, 大部分基于资源效用的选择算法研究被限制在移动边缘网络甚至单个蜂窝网络内部的场景. 因为在这些场景下, 设备受制于能源、通信等资源要素的情况最为突出, 并且由于网络资源的静态性, 集合效用可以被更好地被建模.

FedCS[39]探讨了单个蜂窝网络中 (基站作为聚合服务器, 客户端分布在同一小区内部) 的客户端选择问题, 每轮次开始前, 基站通过广播收集所有客户端的资源特征并基于此估算客户端的模型上传下载时间和训练时间. 聚合服务器以最大期望训练时间作为阈值, 在轮次总时间不超过阈值的情况下尽可能多地选择客户端. 在此基础上, FedMCCS[53]基于线性回归模型, 使用 CPU 频率、内存、电量等特征, 预测某个客户端在阈值内能否完成任务, 以此将训练时间不达标的客户端排除在选择之外.

在无线联邦学习场景下, 持续选择尽可能多的客户端没有考虑到对设备能量的巨大消耗, 并且忽略了多轮选择决策之间的关联性. 文献 [84] 关注了上述问题, 并证明了在早期轮次选择较少的客户端, 后期轮次选择更多的客户端可以在相同训练时间下实现更高的模型精度和更低的训练损失, 并提出了在长期视角下的客户端选择算法 OCEAN. 同样基于此观点, 文献 [85] 提出了 ELASTIC 选择算法, 旨在自适应地选择客户端和管理共有资源, 以达成客户端总体能量消耗和轮次训练时间消耗的均衡.

另一些研究工作以选择固定数目的客户端为目标展开, 例如 FMore[45]基于多属性拍卖博弈, 在每轮次收集客户端的资源信息和期望利润, 从聚合服务器效益最大化的角度实现了客户端选择. TiFL[54]利用一个前置的测试训练任务将客户端划分为不同的层, 每一层中的客户端被认为是资源同质化的, 因为它们在测试任务中提供了相近的本地更新时间. 在每轮次选择中, TiFL 根据自适应算法的控制选择某一层, 然后在层中进行随机选择得到最终的客户端集合.

此外, 部分研究不以严格限制或尽最大可能选择客户端数目出发, 如文献 [86] 允许任何数量的参与客户端 (预算 $m<n$, n 为客户端数量的上限), 通过重要性采样来优化客户端的选择, 以减少通信开销并提高联邦学习的效率. 这扩展了文献 [87] 的理论结果, 后者只适用于 $m=1$ 的情况. 重要性采样方法在优化中已经被广泛研究, 特别是在凸优化和深度学习的环境下. 文献 [86] 中也提到了多种采样方法应用于联邦学习客户端选择场景的途径, 包括基于梯度范数的采样、基于历史损失的采样等.

3.3 基于数据与资源效用

基于数据效用的选择算法偏向于选择高质量数据源, 但被选择的客户端很可能受到物理资源的限制成为联合训练中的掉队者. 基于资源效用的选择算法更偏向于选择拥有丰富计算和网络资源的客户端, 但忽视了其本地数据的质量. 在实际的客户端集群中, 高质量数据和优质系统资源往往不具有强相关性, 这为我们综合考量数据效用和资源效用以构建联合优化算法提供了契机.

部分研究已经开始注意到上述问题并且使用资源特征和数据质量特征联合定义客户端的效用以均衡训练效率和时间消耗. 例如, Oort[55]使用数据量和本地数据损失函数值作为效用函数主体, 而资源特征被抽象为“预期训练时间”指标并以一个惩罚系数的形式与效用函数主体相乘. 因此, 高效用客户端代表着同时具有高质量的数据和优质的训练资源. PyramidFL[43]完善了 Oort 算法, 利用了被选中的客户端之间的差异性, 增加了客户端自适应方案, 即客户端以被选择集合中最长的预期训练时间为参考, 尽可能多地在本地训练更多的时期. 在训练完成后, 客户端根据对本地模型效果 (损失函数值) 的判定, 自适应地抛弃部分模型参数以减少联邦学习系统的通信量. Scout 算法[88]进一步利用了客户端之间的相关性, 将客户端集合而不是个体视为效用函数计算的最小元, 并以此

为基础设计了新的效用评估指标和快速计算算法, 较好地达到了联邦训练效率和物理耗时的均衡, 提升了联合模型的最终准确率等指标.

上述工作使用实时性的资源特征和数据特征联合构建效用函数, 后续筛选策略等步骤和其余两种选择算法并无区别. 另一部分研究提供了完全不同的思路, 例如 FedCCPS[72]利用本地更新的梯度信息反推本地数据分布, 根据数据分布相似度对客户端进行聚类, 并基于 CPU 频率、设备传输功率等资源特征建立延迟感知模型以预测客户端的本地更新时间. 在每轮次选择时, FedCCPS 在每个聚类中选择本地更新时间最短的一个客户端组成集合, 从而使每轮次选择的客户端集合覆盖所有的数据分布且没有冗余, 以此达到训练效率和模型精度的联合优化. 文献 [56] 旨在使用陈旧的特征信息融合计算声誉值 (效用函数) 来评估客户端的可靠性和可信性. 任务结束后, 聚合服务器基于客户端的资源消耗、本地模型精度等特征, 更新存储在区块链中的客户端声誉. 后续任务的聚合服务器通过区块链上公开透明的声誉信息进行客户端选择. 这种方法将特征收集请求嵌入聚合更新过程, 大幅度降低了通信成本. 但使用陈旧的特征作为效用降低了选择算法的准确性, 并且声誉完全由聚合服务器给出太过主观. Refiner[41]通过使用分布式的验证者在每轮次训练后投票给出声誉信息的方法, 缓解了上述问题.

相比于仅考虑单维度效用最大化的基于数据效用和基于资源效用两类选择算法, 基于数据与资源效用的选择算法往往能够在双维度效用损失都可接受的情况下, 达成训练效率和物理时耗的联合优化与均衡. 同时, 因为在设计中兼顾了高质量数据和优质系统资源, 此类算法通常能更好地解决选择算法研究面临的 4 大挑战. 但同时, 基于数据与资源效用的选择算法大幅度地提高了效用定义、特征收集和筛选策略求解等步骤的复杂性, 并引发了一系列新型挑战, 例如在训练过程中自适应调整联合效用函数形式.

3.4 各类算法代表性工作总结与对比

最后, 我们将各类选择算法的代表性研究工作陈列在表 3, 并对其主要设计进行清晰的陈列对比.

表 3 4 类客户端选择算法代表性工作总结与对比

分类	具体研究工作	特征收集	优化目标	筛选策略 (算法)	客户端自适应	可扩展性	公平性	隐私安全性	异常值鲁棒性
随机选择	FedAvg[5]	无	无	随机选择	无	√	√	√	×
基于数据效用	Power-of-choice ($\pi_{\text{pow-}d}$)[51]	本地损失函数值	最大化效用值	按效用值排序	无	×	×	√	×
	Favor[40]	本地数据分布 (本地模型参数)	最大化效用值	深度双Q网络 (DDQN)	无	√	×	√	×
	AFL[52]	本地效用值	最大化效用值	将效用值换算成被选择概率	客户端侧使用本地更新结果评估效用值	√	√	√	√
	AUCTION[49]	数据量、本地损失函数值、预期收益等	最大化客户端数量 (阈值: 轮次总花费)	编码器-解码器模型 (encoder-decoder)	无	√	×	√	×
	UCB-CS[69]	本地损失函数值	最大化效用值	置信区间上界算法 (UCB)	无	√	√	√	×
	DCS[71]	无	最小化通信成本	按期望价值阈值过滤	客户端使用全局验证集计算本地更新模型价值, 低价值模型不参与本轮次全局聚合	√	×	×	√
基于资源效用	FedCS[39]	本地更新时间、模型传输时间	最大化客户端数量 (阈值: 轮次总时间)	背包约束下的子模函数最大化问题 (贪心算法近似解)	无	×	×	√	×

表 3 4 类客户端选择算法代表性工作总结与对比 (续)

分类	具体研究工作	特征收集	优化目标	筛选策略 (算法)	客户端自适应	可扩展性	公平性	隐私安全性	异常值鲁棒性
基于资源效用	FedMCCS[53]	处理器、内存、设备能量等	最大化客户端数量 (阈值: 轮次总时间)	背包约束下的双层最大化优化问题 (贪心算法近似解)	无	×	×	√	×
	FMore[45]	处理器、网络带宽、计算算力、预期收益	最大化效用值	多属性拍卖博弈	无	×	×	√	√
	TiFL[54]	本地更新时间	最大化效用值	自适应层选择, 层内随机选择	无	√	√	√	×
	OCEAN[84]	无线信道状态、设备能量等	最大化长期效用值	李雅普诺夫优化算法	无	×	×	√	×
基于数据与资源效用	Oort[55]	数据量、本地损失函数值、本地更新时间	最大化效用值	探索-利用算法 (exploration-exploitation)	无	√	√	√	√
	PyramidFL[43]	数据量、本地损失函数值、本地更新时间	最大化效用值	探索-利用算法 (exploration-exploitation)	客户端根据期望轮次时间调整本地更新周期; 根据重要度排名丢弃部分模型参数	√	√	√	√
	FedCCPS[72]	处理器、网络带宽、模型参数大小、本地数据分布 (本地模型参数)等	最小化轮次时间	K均值聚类算法 (K-means)+二分法+按本地更新时间排序	无	√	×	√	×
	文献[56]	本地数据分布、数据量、历史模型准确率、本地更新时间等	最大化效用值	按效用值 (声誉)排序	无	√	×	×	√
	CACS[89]	无线信道状态、本地损失函数值	最大化效用值	背包约束下的子模函数最大化问题 (贪心算法近似解)	无	√	×	√	×

4 未来研究方向

考虑客户端相关性的强可解释集合效用函数. 虽然在本文的描述中, 效用函数的计算总是以客户端集合为最小元而不是个体, 但事实上目前的绝大部分研究简单地将客户端集合效用定义为集合内所有个体效用的和, 即 $Util(A^t)=\sum_{i\in A^t}Util(i)$. 这是不准确的, 因为客户端之间并非完全独立不相关, 以个体效用累加和估计集合效用的方法缺少对个体间相关性的考量, 例如网络并发情况下的整体模型参数传输时间不等同于个体单独占用信道时的传输时间的和, 在差异很大的数据分布上各自具有高精确度的模型聚合后可能会造成断崖式的精度损失[5]. 使用神经网络定义集合效用的方法虽然能将个体相关性隐藏在复杂的连接关系与网络权值中, 但缺乏可解释性. 因此, 考虑客户端个体之间的相关性, 设计强可解释的集合效用函数是目前选择算法研究的一个有潜力的方向.

通用场景下拜占庭容错的选择算法. 集群中不存在拜占庭节点是目前大部分选择算法的前提假设之一. 但实用化的联邦学习不得不考虑该问题, 特别是对于存在多方主体协作和利益分配的情况. 目前, 一些选择算法的研究已经考虑了这个问题, 并通过设计基于博弈理论的激励机制, 如契约理论[55], 解决了这个问题. 这些研究证明了其设计的激励模型具有相容性, 即客户端无法通过说谎 (例如提供虚假的特征) 获取更高的利益. 但这些研究都局限

于一个假想的商业模式: 联邦学习任务由一个存在模型训练需求但缺乏训练数据的节点 (聚合服务器作为其代理) 主动发起, 众多客户端仅靠出售本地数据价值从发起方获取收益, 而不是期望使用联合模型获取任何后续收益 (如对用户提供商业化服务). 这样的假想是不全面的, 因为联邦学习的一个重要作用就是在对等的服务方之间使用分散的数据构建共用的联合模型, 这将带来完全不同的敌手模型和安全性假设. 针对通用化场景设计拜占庭容错的选择算法是一个有挑战性的研究方向.

专用联邦学习资源调度服务提供商. 现有的大部分研究中, 特征收集和筛选策略等流程均由特定任务的聚合服务器独立完成. 这是合理的, 因为选择算法以最大化聚合服务器利益为目标, 那么聚合服务器承受额外的网络通信和计算开销无可厚非. 但在传统的主从架构分布式系统中, 越来越多的设计希望将状态管理 (特征收集) 和任务调度 (筛选策略) 功能从主节点分离出来, 交由独立的资源调度器或服务提供商集中化实现和管理, 例如 YARN[90]、Omiga[91]、HyperService[92]等, 以实现平台系统的高性能和可扩展. 在目前的选择算法研究中, 已经出现了这个趋势, 例如 Oort[55]被抽象成独立的软件开发套件 (software development kit, SDK) 并对外提供统一的服务接口. 更进一步, 未来可以形成专用的联邦学习资源调度云服务提供商. 如图 3 所示, 联邦学习资源调度云服务提供商对所有的任务发起方开放状态管理、任务调度等服务接口并收取费用, 以此大幅度降低任务发起方的门槛并提供更安全、高效、稳定的选择算法服务. 同时, 云服务提供商能够成为持久的有信誉的联邦学习平台, 以快速建立起模型需求者和数据源之间的连接, 营造良好的联邦学习生态.

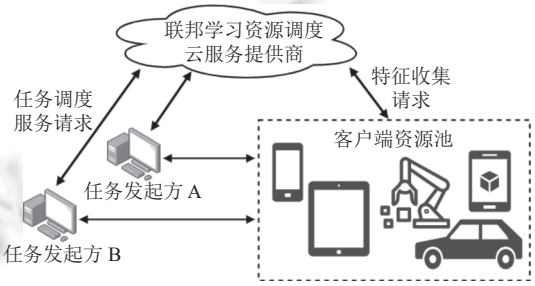

图 3 专用联邦学习资源调度服务提供商

5 结 论

对于跨设备场景下的联邦学习, 如何高效、稳定、可靠地从海量强异构客户端中选择合适的客户端集合参与每轮次的联合训练, 即客户端选择算法, 近年来得到广泛研究. 本文对客户端选择算法研究进行了详细的调研、分析、讨论和总结, 以填补该研究领域综述性文章的空白.

首先, 本文系统化地描述了客户端选择算法的研究目标, 即通过解决客户端数据异构性和资源异构性问题以优化联邦学习的资源消耗和模型性能. 然后, 本文提炼了客户端选择算法研究的通用假设, 具体包括跨设备场景、需要多轮迭代完全挖掘本地数据价值、节点是诚实的志愿者和联邦学习任务对客户端资源和数据的独占性. 在研究的目标和边界清晰后, 我们形式化描述了嵌入选择算法的联邦学习协议的完整生命周期. 特别地, 本文创新性地将绝大部分研究的筛选策略利用效用理论统一建模, 并将选择客户端集合的过程抽象为一个组合优化问题. 进一步地, 本文总结了目前选择算法研究所面临的 4 大挑战, 即可扩展性挑战、公平性挑战、隐私安全性挑战和异常数据鲁棒性挑战, 并概述了现有研究的解决方案.

根据建模客户端集合效用函数时所使用特征信息的不同, 本文将客户端选择算法分为随机选择、基于数据效用、基于资源效用和基于数据与资源联合效用这 4 类, 并对每种算法进行了深入分析和讨论, 最后汇集和对比各类算法的代表性工作. 简单来说, 随机选择算法不收集任何客户端特征信息以指导选择, 在绝大部分场景下拥有极大的可优化空间. 基于数据效用和基于资源效用两类选择算法分别倾向于最优化训练效率和物理时耗, 当客户端集群中高质量数据和强系统资源相关性弱时, 可能会造成另一指标的巨大损失. 基于数据与资源的选择算法通过

基于数据和资源效用联合建模的效用函数实现了双目标的联合优化和均衡, 并且往往能够更好地解决选择算法面临的 4 大挑战, 但同时也大幅提升了算法的复杂性.

最后, 本文讨论了关于选择算法的一些有前景的研究方向, 包括考虑客户端相关性的强可解释集合效用函数、通用场景下拜占庭容错的选择算法和构建专用的联邦学习资源调度服务提供商.

值得注意的是, 本文在联邦学习客户端选择算法的探索和实验中取得了一定的进展, 但还存在一些值得进一步探讨的空白和不足之处. 一方面, 虽然我们的方法考虑了客户端采样的有效性, 但没有从无偏估计角度深入探讨客户端采样算法. 无偏估计在保证模型更新期望的准确性方面起着关键作用, 是实现准确和可靠模型的基础. 另一方面, 本文未充分考虑重要性采样在优化客户端选择过程中的作用. 重要性采样通过权重分配优先选择对模型更新有更大贡献的客户端, 从而加速模型收敛并提高最终性能. 加之, 从分布式优化的视角, 本文综述的各个客户端采样策略虽然减轻了通信开销, 但仍有改进空间, 以更好平衡计算和通信的需求, 并进一步提高联邦学习的效率和性能. 未来的工作将集中在这些方面, 以填补有关空白, 并进一步完善和优化客户端采样算法在联邦学习中的应用.

References:

[1] Li M, Andersen DG, Smola A, Yu K. Communication efficient distributed machine learning with the parameter server. In: Proc. of the 27th Int'l Conf. on Neural Information Processing Systems. Montreal: MIT Press, 2014. 19–27.

[2] Kraska T, Talwalkar A, Duchi JC, Griffith R, Franklin MJ, Jordan MI. MLbase: A distributed machine-learning system. In: Proc. of the 6th Biennial Conf. on Innovative Data Systems Research. Asilomar: www.cidrdb.org, 2013.

[3] Patarasuk P, Yuan X. Bandwidth optimal all-reduce algorithms for clusters of workstations. Journal of Parallel and Distributed Computing, 2009, 69(2): 117–124. [doi: 10.1016/j.jpdc.2008.09.002]

[4] Li T, Sahu AK, Talwalkar A, Smith V. Federated learning: Challenges, methods, and future directions. IEEE Signal Processing Magazine, 2020, 37(3): 50–60. [doi: 10.1109/MSP.2020.2975749]

[5] McMahan B, Moore E, Ramage D, Hampson S, Arcas BAY. Communication-efficient learning of deep networks from decentralized data. In: Proc. of the 20th Int'l Conf. on Artificial Intelligence and Statistics. Fort Lauderdale: PMLR, 2017. 1273–1282.

[6] Yang Q, Liu Y, Chen TJ, Tong YX. Federated machine learning: Concept and applications. ACM Trans. on Intelligent Systems and Technology, 2019, 10(2): 12. [doi: 10.1145/3298981]

[7] Kairouz P, McMahan HB, Avent B, *et al*. Advances and open problems in federated learning. Foundations and Trends® in Machine Learning, 2021, 14(1–2): 1–210. [doi: 10.1561/2200000083]

[8] Li X, Huang KX, Yang WH, Wang SS, Zhang ZH. On the convergence of FedAvg on non-IID data. In: Proc. of the 8th Int'l Conf. on Learning Representations. Addis Ababa: OpenReview.net, 2020.

[9] Li T, Sahu AK, Zaheer M, Sanjabi M, Talwalkar A, Smith V. Federated optimization in heterogeneous networks. In: Proc. of the 2020 Machine Learning and Systems. Austin: mlsys.org, 2020. 429–450.

[10] Reddi SJ, Charles Z, Zaheer M, Garrett Z, Rush K, Konečný J, Kumar S, McMahan HB. Adaptive federated optimization. In: Proc. of the 9th Int'l Conf. on Learning Representations. OpenReview.net, 2021.

[11] Cho YJ, Wang JY, Joshi G. Client selection in federated learning: Convergence analysis and power-of-choice selection strategies. arXiv:2010.01243, 2020.

[12] Hard A, Rao K, Mathews R, Ramaswamy S, Beaufays F, Augenstein S, Eichner H, Kiddon C, Ramage D. Federated learning for mobile keyboard prediction. arXiv:1811.03604, 2018.

[13] Paulik M, Seigel M, Mason H, *et al*. Federated evaluation and tuning for on-device personalization: System design & applications. arXiv:2102.08503, 2021.

[14] Zhan YF, Zhang J, Hong ZC, Wu LJ, Li P, Guo S. A survey of incentive mechanism design for federated learning. IEEE Trans. on Emerging Topics in Computing, 2022, 10(2): 1035–1044. [doi: 10.1109/TETC.2021.3063517]

[15] Zeng RF, Zeng C, Wang XW, Li B, Chu XW. A comprehensive survey of incentive mechanism for federated learning. arXiv:2106.15406, 2021.

[16] Mothukuri V, Parizi RM, Pouriyeh S, Huang Y, Dehghantanha A, Srivastava G. A survey on security and privacy of federated learning. Future Generation Computer Systems, 2021, 115: 619–640. [doi: 10.1016/j.future.2020.10.007]

[17] Shi YX, Yu H, Leung C. Towards fairness-aware federated learning. arXiv:2111.01872, 2021.

[18] Lin WW, Shi F, Zeng L, Li DD, Xu YH, Liu B. Survey of federated learning open-source frameworks. Journal of Computer Research and Development, 2023, 60(7): 1551–1580 (in Chinese with English abstract). [doi: 10.7544/issn1000-1239.202220148]

[19] Zhao Y, Li M, Lai LZ, Suda N, Civin D, Chandra V. Federated learning with non-IID data. arXiv:1806.00582, 2018.

[20] Wolfrath J, Sreekumar N, Kumar D, Wang YL, Chandra A. HACCS: Heterogeneity-aware clustered client selection for accelerated federated learning. In: Proc. of the 2022 IEEE Int'l Parallel and Distributed Processing Symp. Lyon: IEEE, 2022. 985–995. [doi: 10.1109/IPDPS53621.2022.00100]

[21] Xie C, Koyejo S, Gupta I. Asynchronous federated optimization. arXiv:1903.03934, 2019.

[22] Wang JY, Charles Z, Xu Z, *et al*. A field guide to federated optimization. arXiv:2107.06917, 2021.

[23] Chai Z, Fayyaz H, Fayyaz Z, Anwar A, Zhou Y, Baracaldo N, Ludwig H, Cheng Y. Towards taming the resource and data heterogeneity in federated learning. In: Proc. of the 2019 USENIX Conf. on Operational Machine Learning. Santa Clara: USENIX Association, 2019. 19–21.

[24] Bonawitz KA, Eichner H, Grieskamp W, Huba D, Ingerman A, Ivanov V, Kiddon C, Konečný J, Mazzocchi S, McMahan B, van Overveldt T, Petrou D, Ramage D, Roselander J. Towards federated learning at scale: System design. In: Proc. of the 2019 Machine Learning and Systems. Stanford: mlsys.org, 2019. 374–388.

[25] Chen YJ, Ning Y, Slawski M, Rangwala H. Asynchronous online federated learning for edge devices with non-IID data. In: Proc. of the 2020 IEEE Int'l Conf. on Big Data (Big Data). Atlanta: IEEE, 2020. 15–24. [doi: 10.1109/BigData50022.2020.9378161]

[26] Abadi M, Chu A, Goodfellow I, McMahan HB, Mironov I, Talwar K, Zhang L. Deep learning with differential privacy. In: Proc. of the 2016 ACM SIGSAC Conf. on Computer and Communications Security. Vienna: ACM, 2016. 308–318. [doi: 10.1145/2976749.2978318]

[27] Bonawitz K, Ivanov V, Kreuter B, Marcedone A, McMahan HB, Patel S, Ramage D, Segal A, Seth K. Practical secure aggregation for privacy-preserving machine learning. In: Proc. of the 2017 ACM SIGSAC Conf. on Computer and Communications Security. Dallas: ACM, 2017. 1175–1191. [doi: 10.1145/3133956.3133982]

[28] McMahan HB, Ramage D, Talwar K, Zhang L. Learning differentially private recurrent language models. In: Proc. of the 6th Int'l Conf. on Learning Representations. Vancouver: OpenReview.net, 2018.

[29] Konečný J, McMahan HB, Yu FX, Richtárik P, Suresh AT, Bacon D. Federated learning: Strategies for improving communication efficiency. arXiv:1610.05492, 2016.

[30] Kamp M, Adilova L, Sicking J, Hüger F, Schlicht P, Wirtz T, Wrobel S. Efficient decentralized deep learning by dynamic model averaging. In: Proc. of the 2019 Joint European Conf. on Machine Learning and Knowledge Discovery in Databases. Dublin: Springer, 2019. 393–409. [doi: 10.1007/978-3-030-10925-7_24]

[31] Li T, Sahu AK, Zaheer M, Sanjabi M, Talwalkar A, Smithy V. FedDANE: A federated Newton-type method. In: Proc. of the 53rd Asilomar Conf. on Signals, Systems, and Computers. Pacific Grove: IEEE, 2019. 1227–1231. [doi: 10.1109/IEEECONF44664.2019.9049023]

[32] Micikevicius P, Narang S, Alben J, Diamos GF, Elsen E, Garcia D, Ginsburg B, Houston M, Kuchaiev O, Venkatesh G, Wu H. Mixed precision training. In: Proc. of the 6th Int'l Conf. on Learning Representations. Vancouver: OpenReview.net, 2018.

[33] Mammen PM. Federated learning: Opportunities and challenges. arXiv:2101.05428, 2021.

[34] Huang YT, Chu LY, Zhou ZR, Wang LJ, Liu JC, Pei J, Zhang Y. Personalized cross-silo federated learning on non-IID data. In: Proc. of the 35th AAAI Conf. on Artificial Intelligence. AAAI, 2021. 7865–7873. [doi: 10.1609/aaai.v35i9.16960]

[35] Fraboni Y, Vidal R, Kameni L, Lorenzi M. Clustered sampling: Low-variance and improved representativity for clients selection in federated learning. In: Proc. of the 38th Int'l Conf. on Machine Learning. PMLR, 2021. 3407–3416.

[36] Lamport L, Shostak R, Pease M. The Byzantine generals problem. In: Malkhi D, ed., Concurrency: The Works of Leslie Lamport. New York: ACM, 2019. 203–226.

[37] Wu YZ, Kang Y, Luo JH, He YQ, Fan LX, Pan R, Yang Q. FedCG: Leverage conditional GAN for protecting privacy and maintaining competitive performance in federated learning. In: Proc. of the 31st Int'l Joint Conf. on Artificial Intelligence. Vienna: IJCAI.org, 2022. 2334–2340. [doi: 10.24963/ijcai.2022/324]

[38] Liu SY, Viotti P, Cachin C, Quéma V, Vukolić M. XFT: Practical fault tolerance beyond crashes. In: Proc. of the 12th USENIX Symp. on Operating Systems Design and Implementation. Savannah: USENIX Association, 2016. 485–500.

[39] Nishio T, Yonetani R. Client selection for federated learning with heterogeneous resources in mobile edge. In: Proc. of the 2019 IEEE Int'l Conf. on Communications (ICC). Shanghai: IEEE, 2019. 1–7. [doi: 10.1109/ICC.2019.8761315]

[40] Wang H, Kaplan Z, Niu D, Li BC. Optimizing federated learning on non-IID data with reinforcement learning. In: Proc. of the 2020 IEEE Conf. on Computer Communications. Toronto: IEEE, 2020. 1698–1707. [doi: 10.1109/INFOCOM41043.2020.9155494]

[41] Zhang ZB, Dong DJ, Ma YH, Ying YL, Jiang DW, Chen K, Shou LD, Chen G. Refiner: A reliable incentive-driven federated learning

system powered by blockchain. Proc. of the VLDB Endowment, 2021, 14(12): 2659–2662. [doi: 10.14778/3476311.3476313]

[42] Amari SI. Backpropagation and stochastic gradient descent method. Neurocomputing, 1993, 5(4–5): 185–196. [doi: 10.1016/0925-2312(93)90006-O]

[43] Li CN, Zeng X, Zhang M, Cao ZC. PyramidFL: A fine-grained client selection framework for efficient federated learning. In: Proc. of the 28th Annual Int'l Conf. on Mobile Computing and Networking. Sydney: ACM, 2022. 158–171. [doi: 10.1145/3495243.3517017]

[44] Ribero M, Vikalo H. Communication-efficient federated learning via optimal client sampling. arXiv:2007.15197, 2020.

[45] Zeng RF, Zhang SX, Wang JQ, Chu XW. FMore: An incentive scheme of multi-dimensional auction for federated learning in MEC. In: Proc. of the 40th IEEE Int'l Conf. on Distributed Computing Systems (ICDCS). Singapore: IEEE, 2020. 278–288. [doi: 10.1109/ICDCS47774.2020.00094]

[46] Zhao Y, Zhao J, Jiang LS, Tan R, Niyato D. Mobile edge computing, blockchain and reputation-based crowdsourcing IoT federated learning: A secure, decentralized and privacy-preserving system. arXiv:1906.10893, 2019.

[47] ur Rehman MH, Salah K, Damiani E, Svetinovic D. Towards blockchain-based reputation-aware federated learning. In: Proc. of the 2020 IEEE Conf. on Computer Communications Workshops (INFOCOM WKSHPS). Toronto: IEEE, 2020. 183–188. [doi: 10.1109/INFOCOMWKSHPS50562.2020.9163027]

[48] Fishburn PC. Utility Theory for Decision Making. McLean: Research Analysis Corp, 1970.

[49] Deng YH, Lyu F, Ren J, Wu HQ, Zhou YZ, Zhang YX, Shen XM. AUCTION: Automated and quality-aware client selection framework for efficient federated learning. IEEE Trans. on Parallel and Distributed Systems, 2022, 33(8): 1996–2009. [doi: 10.1109/TPDS.2021.3134647]

[50] Jiao YT, Wang P, Niyato D, Lin B, Kim DI. Toward an automated auction framework for wireless federated learning services market. IEEE Trans. on Mobile Computing, 2021, 20(10): 3034–3048. [doi: 10.1109/TMC.2020.2994639]

[51] Cho YJ, Wang JY, Joshi G. Towards understanding biased client selection in federated learning. In: Proc. of the 2022 Int'l Conf. on Artificial Intelligence and Statistics. PMLR, 2022. 10351–10375.

[52] Goetz J, Malik K, Bui D, Moon S, Liu HL, Kumar A. Active federated learning. arXiv:1909.12641, 2019.

[53] Abdulrahman S, Tout H, Mourad A, Talhi C. FedMCCS: Multicriteria client selection model for optimal IoT federated learning. IEEE Internet of Things Journal, 2021, 8(6): 4723–4735. [doi: 10.1109/JIOT.2020.3028742]

[54] Chai Z, Ali A, Zawad S, Truex S, Anwar A, Baracaldo N, Zhou Y, Ludwig H, Yan F, Cheng Y. TiFL: A tier-based federated learning system. In: Proc. of the 29th Int'l Symp. on High-performance Parallel and Distributed Computing. Stockholm: ACM, 2020. 125–136. [doi: 10.1145/3369583.3392686]

[55] Lai F, Zhu XF, Madhyastha HV, Chowdhury M. Oort: Efficient federated learning via guided participant selection. In: Proc. of the 15th USENIX Symp. on Operating Systems Design and Implementation. USENIX Association, 2021. 19–35.

[56] Kang JW, Xiong ZH, Niyato D, Xie SL, Zhang JS. Incentive mechanism for reliable federated learning: A joint optimization approach to combining reputation and contract theory. IEEE Internet of Things Journal, 2019, 6(6): 10700–10714. [doi: 10.1109/JIOT.2019.2940820]

[57] Wang LP, Wang W, Li B. CMFL: Mitigating communication overhead for federated learning. In: Proc. of the 39th IEEE Int'l Conf. on Distributed Computing Systems (ICDCS). Dallas: IEEE, 2019. 954–964. [doi: 10.1109/ICDCS.2019.00099]

[58] Zhang C, Xie Y, Bai H, Yu B, Li WH, Gao Y. A survey on federated learning. Knowledge-based Systems, 2021, 216: 106775. [doi: 10.1016/j.knosys.2021.106775]

[59] Zhu XD, Li H, Yu Y. Blockchain-based privacy preserving deep learning. In: Proc. of the 14th Int'l Conf. on Information Security and Cryptology. Fuzhou: Springer, 2019. 370–383. [doi: 10.1007/978-3-030-14234-6_20]

[60] Auer P, Cesa-Bianchi N, Fischer P. Finite-time analysis of the multiarmed bandit problem. Machine Learning, 2002, 47(2–3): 235–256. [doi: 10.1023/A:1013689704352]

[61] Cho K, van Merriënboer B, Gulcehre C, Bahdanau D, Bougares F, Schwenk H, Bengio Y. Learning phrase representations using RNN encoder-decoder for statistical machine translation. In: Proc. of the 2014 Conf. on Empirical Methods in Natural Language Processing (EMNLP). Doha: Association for Computational Linguistics, 2014. 1724–1734. [doi: 10.3115/v1/D14-1179]

[62] Li T, Sanjabi M, Beirami A, Smith V. Fair resource allocation in federated learning. In: Proc. of the 8th Int'l Conf. on Learning Representations. Addis Ababa: OpenReview.net, 2020.

[63] Zhou ZR, Chu LY, Liu CX, Wang LJ, Pei J, Zhang Y. Towards fair federated learning. In: Proc. of the 27th ACM SIGKDD Conf. on Knowledge Discovery & Data Mining. ACM, 2021. 4100–4101. [doi: 10.1145/3447548.3470814]

[64] Li T, Hu SY, Beirami A, Smith V. Ditto: Fair and robust federated learning through personalization. In: Proc. of the 38th Int'l Conf. on Machine Learning. PMLR, 2021. 6357–6368.

[65] Mohri M, Sivek G, Suresh AT. Agnostic federated learning. In: Proc. of the 36th Int'l Conf. on Machine Learning. Long Beach: PMLR,

2019. 4615–4625.

[66] Huang TS, Lin WW, Wu WT, He LG, Li KQ, Zomaya AY. An efficiency-boosting client selection scheme for federated learning with fairness guarantee. IEEE Trans. on Parallel and Distributed Systems, 2021, 32(7): 1552–1564. [doi: 10.1109/TPDS.2020.3040887]

[67] Huang TS, Lin WW, Shen L, Li KQ, Zomaya AY. Stochastic client selection for federated learning with volatile clients. IEEE Internet of Things Journal, 2022, 9(20): 20055–20070. [doi: 10.1109/JIOT.2022.3172113]

[68] Song ZD, Sun HG, Yang HH, Wang XJ, Zhang Y, Quek TQS. Reputation-based federated learning for secure wireless networks. IEEE Internet of Things Journal, 2022, 9(2): 1212–1226. [doi: 10.1109/JIOT.2021.3079104]

[69] Cho YJ, Gupta S, Joshi G, Yağan O. Bandit-based communication-efficient client selection strategies for federated learning. In: Proc. of the 54th Asilomar Conf. on Signals, Systems, and Computers. Pacific Grove: IEEE, 2020. 1066–1069. [doi: 10.1109/IEEECONF51394.2020.9443523]

[70] Jain RK, Chiu DM, Hawe WR. A quantitative measure of fairness and discrimination for resource allocation in shared computer system. 1984. https://www.semanticscholar.org/paper/A-Quantitative-Measure-Of-Fairness-And-For-Resource-Jain-Chiu/980773ca869fc17562e4fbcf4202a8f21893b114

[71] Hosseinzadeh M, Hudson N, Heshmati S, Khamfroush H. Communication-loss trade-off in federated learning: A distributed client selection algorithm. In: Proc. of the 19th IEEE Annual Consumer Communications & Networking Conf. Las Vegas: IEEE, 2022. 1–6. [doi: 10.1109/CCNC49033.2022.9700601]

[72] Xin F, Zhang JH, Luo JZ, Dong F. Federated learning client selection mechanism under system and data heterogeneity. In: Proc. of the 25th IEEE Int'l Conf. on Computer Supported Cooperative Work in Design (CSCWD). Hangzhou: IEEE, 2022. 1239–1244. [doi: 10.1109/CSCWD54268.2022.9776061]

[73] Phong LT, Aono Y, Hayashi T, Wang LH, Moriai S. Privacy-preserving deep learning via additively homomorphic encryption. IEEE Trans. on Information Forensics and Security, 2018, 13(5): 1333–1345. [doi: 10.1109/TIFS.2017.2787987]

[74] Tolpegin V, Truex S, Gursoy ME, Liu L. Data poisoning attacks against federated learning systems. In: Proc. of the 25th European Symp. on Research in Computer Security. Guildford: Springer, 2020. 480–501. [doi: 10.1007/978-3-030-58951-6_24]

[75] Li YB. Model update optimization for heterogeneous clients in federated learning [MS. Thesis]. Harbin: Harbin Institute of Technology, 2020 (in Chinese with English abstract). [doi: 10.27061/d.cnki.ghgdu.2021.001095]

[76] Jiang AH, Wong DLK, Zhou G, Andersen DG, Dean J, Ganger GR, Joshi G, Kaminksy M, Kozuch M, Lipton ZC, Pillai P. Accelerating deep learning by focusing on the biggest losers. arXiv:1910.00762, 2019.

[77] Katharopoulos A, Fleuret F. Not all samples are created equal: Deep learning with importance sampling. In: Proc. of the 35th Int'l Conf. on Machine Learning. Stockholm: PMLR, 2018. 2530–2539.

[78] Shah V, Wu XX, Sanghavi S. Choosing the sample with lowest loss makes SGD robust. In: Proc. of the 23rd Int'l Conf. on Artificial Intelligence and Statistics. Sicily: PMLR, 2020. 2120–2130.

[79] Kim T, Bae S, Lee JW, Yun S. Accurate and fast federated learning via combinatorial multi-armed bandits. arXiv:2012.03270, 2020.

[80] Bubeck S, Cesa-Bianchi N. Regret analysis of stochastic and nonstochastic multi-armed bandit problems. Foundations and Trends® in Machine Learning, 2012, 5(1): 1–122. [doi: 10.1561/2200000024]

[81] Balakrishnan R, Li T, Zhou TY, Himayat N, Smith V, Bilmes JA. Diverse client selection for federated learning via submodular maximization. In: Proc. of the 10th Int'l Conf. on Learning Representations. OpenReview.net, 2022.

[82] Cornuejols G, Fisher M, Nemhauser GL. On the uncapacitated location problem. Annals of Discrete Mathematics, 1977, 1: 163–177. [doi: 10.1016/S0167-5060(08)70732-5]

[83] Nemhauser GL, Wolsey LA, Fisher ML. An analysis of approximations for maximizing submodular set functions—I. Mathematical Programming, 1978, 14(1): 265–294. [doi: 10.1007/BF01588971]

[84] Xu J, Wang HQ. Client selection and bandwidth allocation in wireless federated learning networks: A long-term perspective. IEEE Trans. on Wireless Communications, 2021, 20(2): 1188–1200. [doi: 10.1109/TWC.2020.3031503]

[85] Yu LK, Albelaihi R, Sun X, Ansari N, Devetsikiotis M. Jointly optimizing client selection and resource management in wireless federated learning for Internet of Things. IEEE Internet of Things Journal, 2022, 9(6): 4385–4395. [doi: 10.1109/JIOT.2021.3103715]

[86] Chen WL, Horvath S, Richtarik P. Optimal client sampling for federated learning. arXiv:2010.13723, 2020.

[87] Zhao PL, Zhang T. Stochastic optimization with importance sampling for regularized loss minimization. In: Proc. of the 32nd Int'l Conf. on Machine Learning. Lille: JMLR.org, 2015. 1–9.

[88] Zhang RL, Xu ZN, Yin H. Scout: An efficient federated learning client selection algorithm driven by heterogeneous data and resource. In: Proc. of the 2023 IEEE Int'l Conf. on Joint Cloud Computing (JCC). Athens: IEEE, 2023. 46–49. [doi: 10.1109/JCC59055.2023.00012]

[89] Qiao ZF, Shen YF, Yu XH, Zhang J, Song SH, Letaief KB. Content-aware client selection for federated learning in wireless networks. In: Proc. of the 2022 IEEE Int'l Mediterranean Conf. on Communications and Networking (MeditCom). Athens: IEEE, 2022. 49–54. [doi: 10.1109/MeditCom55741.2022.9928665]

[90] Vavilapalli VK, Murthy AC, Douglas C, Agarwal S, Konar M, Evans R, Graves T, Lowe J, Shah H, Seth S, Saha B, Curino C, O'Malley O, Radia S, Reed B, Baldeschwieler E. Apache Hadoop YARN: Yet another resource negotiator. In: Proc. of the 4th Annual Symp. on Cloud Computing. Santa Clara: ACM, 2013. 5. [doi: 10.1145/2523616.2523633]

[91] Schwarzkopf M, Konwinski A, Abd-El-Malek M, Wilkes J. Omega: Flexible, scalable schedulers for large compute clusters. In: Proc. of the 8th ACM European Conf. on Computer Systems. Prague: ACM, 2013. 351–364. [doi: 10.1145/2465351.2465386]

[92] Liu ZT, Xiang YX, Shi J, Gao P, Wang HY, Xiao XS, Wen BH, Hu YC. HyperService: Interoperability and programmability across heterogeneous blockchains. In: Proc. of the 2019 ACM SIGSAC Conf. on Computer and Communications Security. London: ACM, 2019. 549–566. [doi: 10.1145/3319535.3355503]

附中文参考文献:

[18] 林伟伟, 石方, 曾岚, 李董东, 许银海, 刘波. 联邦学习开源框架综述. 计算机研究与发展, 2023, 60(7): 1551–1580. [doi: 10.7544/issn1000-1239.202220148]

[75] 李宜柄. 联邦学习中针对客户端异构性的模型参数更新优化方法 [硕士学位论文]. 哈尔滨: 哈尔滨工业大学, 2020. [doi: 10.27061/d.cnki.ghgdu.2021.001095]

张瑞麟(1998－), 男, 硕士, 主要研究领域为联邦学习, 区块链.

尹浩(1974－), 男, 博士, 研究员, 博士生导师, 主要研究领域为计算机网络, 大数据, 区块链.

杜晋华(2000－), 男, 博士生, 主要研究领域为机器学习, 自然语言处理, 大语言模型.