基于背包模型的联邦学习客户端选择方法

郭佳慧[1]，陈卓越[1]，高玮[1]，王玺钧[1]，孙兴华[1]，高林[2]
（1. 中山大学，广东 广州 510006；2. 哈尔滨工业大学（深圳），广东 深圳 518055）

摘 要：近年来，为了打破数据“壁垒”，联邦学习被广泛关注。联邦学习不需要客户端上传原始数据就能完成模型训练，保护了用户的隐私。针对客户端设备具有异构性的问题，考虑各个客户端对加速全局模型收敛的贡献程度和系统的通信开销，以最大化客户端在本地训练模型的权重变化量为优化目标，解决在一定系统训练周期下的联邦学习中的客户端选择优化问题。由此，提出了两个基于背包模型的联邦学习协议，分别是 OfflineKP-FL 协议和 OnlineKP-FL 协议。OfflineKP-FL 协议基于离线背包模型选择合适的客户端参与全局模型的聚合更新。为了降低 OfflineKP-FL 协议的复杂度，进一步基于在线背包模型选择用户提出了 OnlineKP-FL 协议。通过仿真发现，在特定情况下 OfflineKP-FL 协议有更高的收敛速度，优于之前提出的方法。而与 OfflineKP-FL 协议和 FedCS 协议相比，OnlineKP-FL 协议下，系统不仅每轮选择更少的用户，而且能够在 FedCS 协议所需时间的 64.1%内完成模型训练，使全局模型达到相同精度。

关键词：联邦学习；客户端选择；背包模型
中图分类号：TP391.4
文献标志码：A
doi: 10.11959/j.issn.2096−3750.2022.00299

Clients selection method based on knapsack model in federated learning

GUO Jiahui[1], CHEN Zhuoyue[1], GAO Wei[1], WANG Xijun[1], SUN Xinghua[1], GAO Lin[2]
1. Sun Yat-sen University, Guangzhou 510006, China
2. Harbin Institute of Technology (Shenzhen), Shenzhen 518055, China

Abstract: In recent years, to break down data barriers, federated learning (FL) has received extensive attention. In FL, clientscan complete the model training without uploading the raw data, which protects the user’s data privacy. For the issue of clients’ heterogeneity, the contribution of each client to accelerating convergence of the global model as well as the communication cost in the system was considered, aiming at maximizing the weight change of the client's local training model, a client selection optimization problem in FL under theconstraint ofthe delay foreach training round was solved. Subsequently, two federated learning protocols based on the knapsack model were proposed, namely OfflineKP-FL protocol and OnlineKP-FL protocol. OfflineKP-FL protocol was based on the offline knapsack model to select appropriate clients to participate in the aggregation and update of the global model. In order to reduce the complexity of the OfflineKP-FL protocol, OnlineKP-FL protocol based on the online knapsack model to select clients was proposed. Through simulations, it is found that OfflineKP-FL protocol converges faster than the previously proposed methods in certain cases. Furthermore, compared with OfflineKP-FL protocol and FedCS protocol, underthe proposed OnlineKP-FL protocol, not only does the system select fewer clients per round, but also it can complete the model training in 64.1% of the time required by FedCS protocol to achieve the same accuracy for the global model.

Key words: federated learning, client selection, knapsack model

收稿日期：2022−07−04；**修回日期：**2022−09−12
通信作者：孙兴华，sunxinghua@mail.sysu.edu.cn
基金项目：国家重点研发计划（No.2021YFB2900300）；国家自然科学基金资助项目（No.62271513，No.61972113）；广东省基础与应用基础研究基金资助项目（No.2021A1515012631）；深圳市科技研发基金资助项目（No.JCYJ20190806112215116，No.KQTD20190929172545139，No.ZDSYS20210623091808025）

Foundation Items: The National Key Research and Development Program of China (No.2021YFB2900300), The National Natural Science Foundation of China (No.62271513, No.61972113), Guangdong Basic and Applied Basic Research Foundation (No.2021A1515012631), The Shenzhen Science and Technology Program (No.JCYJ20190806112215116, No.KQTD20190929172545139, No.ZDSYS20210623091808025)

0　引言

随着大数据和人工智能技术的盛行，传统分布式机器学习开始升级与变革，但也不可避免地给客户端的数据隐私带来了挑战。各行业各部门的数据隐私保护机制，要求客户端的数据不出本地。由谷歌研究院率先提出的联邦学习技术能够实现在数据不共享的情况下各个客户端学习一个统一的模型。但是，在联邦学习环境中，参与训练客户端的硬件配置、通信信道等参数不同，所以各个终端设备的计算能力、通信速度各不相同。例如，一些客户端的计算资源有限，在本地训练模型需要更长的时间，这将使整个训练过程效率低下。

目前有大量研究尝试改进优化联邦学习算法，包括使用分层学习框架[1]、调整通信的资源分配[2]，用计算替代通信[3-5]、压缩模型[6-7]、选择客户端[8-42]等方法。选择合适的客户端参与本地模型训练和全局模型的聚合更新可以有效降低通信量，是很多优化联邦学习算法的切入点。许多学者利用客户端与服务器间的通信条件[8-17]和用户自身的资源信息[9-11, 18-41]等选择用户，提高全局模型的性能指标。根据客户端与服务器间的通信条件，中心服务器在设定的系统训练时间内选择通信条件更好或者耗时更短的客户端，例如，文献[8]提出了优先选择耗时较低的用户的贪心选择算法 FedCS。类似地，文献[12]提出了一种针对移动设备的自适应系统训练周期确定算法，其中自适应确定客户端在每一轮的训练时长。与传统的固定时间阈值算法相比，该算法的收敛时间可减少 50%以上。文献[13]和文献[14]的优化目标分别是最小化系统每轮训练时间和系统中的通信时延。而文献[15]提出了一种优先选择信道条件好、信噪比高的用户选择方法。但是以上文献都没有根据用户的自身信息选择合适的客户端，例如，FedCS 算法没有考虑各个客户端对加速全局模型收敛的贡献程度，有些客户端可能拥有大量重复的数据，如果这些客户端参与模型训练并上载模型参数，那么必然会大大降低全局模型的收敛速度并且带来更多的资源消耗。而在利用客户端自身的资源信息选择用户的研究中，作者能收集到的资源信息包括模型训练能力、模型梯度信息等，它们都反映了个体差异，服务器便据此选择合适的用户。例如，在文献[18]中，作者使用客户端局部模型更新前后的权重之差的二范数选择参与全局模型聚合更新的用户。经验证，该二范数越大，客户端对加速全局模型收敛的贡献越大，该客户端越有可能被选择。除此之外，文献[19]基于分层的抽样过滤位于同一时区的客户端，然后使用多准则选择方法决定参加全局模型聚合更新的用户；文献[20]提出了基于样本数量和基于相似性的两种聚类抽样方法，并通过实验证明了采用聚类抽样进行用户选择可以使全局模型更快更平滑地收敛。文献[25]利用客户端数据异质性的信息，减少了系统 Non-IID 设置下的通信轮数。文献[26]则是选择 Non-IID 度较低的用户，以加快全局模型的收敛速度。文献[27-28,32-33]都是通过选择可信的参与者，提高系统的可靠性。文献[35]从参与训练的设备中排除不利于全局模型收敛的本地模型，利用剩余的本地模型完成全局模型的聚合更新，增加系统的训练准确率。文献[36]根据用户的资源信息，平衡参与者的标签分配，以此选择合适的客户端。但是这些文献没有考虑用户通信条件的差异性对客户端选择算法的影响。

本文基于用户对加速全局模型收敛的贡献程度，提出了分别基于离线背包模型和在线背包模型的两种选择客户端的协议，命名为 OfflineKP-FL 协议和 OnlineKP-FL 协议。具体地说，这两种协议要求客户端在联邦学习框架下，每轮都在设定的时间内下载、更新模型，其中，被中心服务器选择的客户端再继续上载更新后的模型参数，以便中心服务器高效地完成模型聚合。本文提出的两种协议依据用户的通信条件和模型训练前后的梯度信息选取合适的客户端，提出在一定时延下最大化梯度信息变化量的优化问题。为了求解该优化问题，考虑使用背包模型，把每个客户端的梯度信息变化量当作背包模型中物品的价值，系统总训练时间充当背包容量，以提高系统训练的效率。为了降低离线背包模型的算法复杂度，本文进一步提出了基于在线背包模型的 OnlineKP-FL 协议，降低系统的总计算量和全局模型达到相同精度时的总时延。最后，通过在公开的大规模图像数据集 MNIST 上的仿真分析发现，在特定的系统训练时间下，OfflineKP-FL 协议有更高的收敛速度，优于之前提出的 FedCS 协议[8]。而与 OfflineKP-FL 协议和 FedCS 协议相比，相同条件下，OnlineKP-FL 协议具有更好的效果，能够在更短的时间内完成模型训练。

1　系统模型

联邦学习系统模型如图 1 所示，联邦学习系统由一个中心服务器和 N 个客户端组成。系统训练之

前，中心服务器首先初始化一个全局模型，并请求所有用户的资源信息，包括用户在本地训练模型的能力和与服务器通信的能力等。在系统训练的过程中，服务器将初始化的全局模型下发给当前可用的用户，然后这些用户在本地用自己的数据训练模型，并将训练后的结果上传至服务器。服务器利用接收到的训练结果更新全局模型的参数。接下来，系统训练进入下一轮，服务器将当前全局模型下发给客户端，客户端重复上一轮中的步骤，更新全局模型。系统重复训练多轮，直至全局模型的精度达到预期。

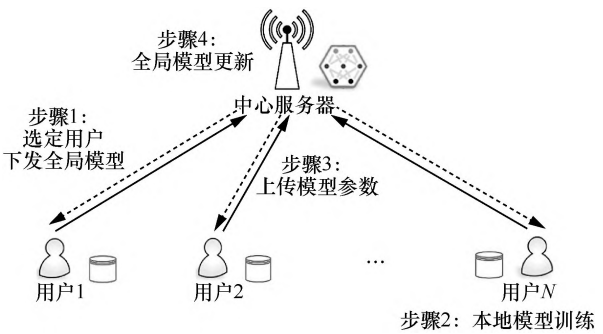


图 1 联邦学习系统模型

本文主要考虑每轮训练时间一定的情况下模型训练效果。基于此，对系统中各步骤的耗时进行假设。由于中心服务器仅在第一轮初始化全局模型并请求所有客户端的资源信息，所以，本文忽略了花费在初始化和资源请求上的时间。对于每个客户端，中心服务器的响应时间（包括服务器下发全局模型和选择客户端的耗时）和聚合全局模型的时间是一个固定的常数，因此，忽略花费在这上面的时间。假设所有客户端在本地训练模型的速率符合均匀分布。用 f_k 表示客户端 k 在本地训练模型的速率，c_k 表示客户端 k 在本地训练局部模型的迭代次数，客户端 k 的本地模型大小是 M_k，那么，客户端 k 在本地训练局部模型的时间为

$$t_k^{\mathrm{UC}}=\frac{c_k M_k}{f_k} \tag{1}$$

假设客户端串行上载新的模型参数，也就是说，同一时间只有一个客户端可以上载参数，在一个客户端完成局部模型训练后，如果没有其他客户端正在上载其模型参数，那么，该客户端可以立即开始上载。假设每轮每个客户端的信道状态稳定，用 SNR_k 表示客户端 k 的信噪比。所以，客户端 k 在无线信道中的最大信息传送速率 $C_k=B\times\mathrm{lb}\left(1+\mathrm{SNR}_k\right)\left(\mathrm{bit}/(\mathrm{s}\cdot\mathrm{Hz})\right)$。用 D_k 代表客户端 k 局部模型的数据大小，则上载模型参数需要的时间为

$$t_k^{\mathrm{UL}}=\frac{D_k}{C_k}=\frac{D_k}{\gamma B\mathrm{lb}(1+\mathrm{SNR}_k)} \tag{2}$$

2 算法设计

2.1 计算更新前后的权重差值的二范数

文献[18]推导验证了一种选择客户端的策略：用客户端在本地训练的局部模型更新前后的权重差值的二范数作为选择客户端的指标，如果该权重差值的二范数大于设定的阈值，则选择该客户端，通过验证表明该策略能够提高联邦学习算法的性能。也就是说，更新前后的权重差值的二范数越大，客户端对加速全局模型收敛的贡献越大。客户端 k 的权重差值的二范数 $\left\|\Delta\boldsymbol{\omega}_k(t)\right\|_2$ 的具体计算方法为

$$\left\|\Delta\boldsymbol{\omega}_k(t)\right\|_2=\left\|\boldsymbol{\omega}_k(t)-\boldsymbol{\omega}(t-1)\right\|_2 \tag{3}$$

其中，$\boldsymbol{\omega}_k(t)$ 表示联邦学习系统训练至第 t 轮时，客户端 k 的本地局部模型的权重，$\boldsymbol{\omega}(t-1)$ 表示第 $(t-1)$ 轮时全局模型的权重。

值得注意的是，与上载模型参数的时间相比，客户端上传权重差值的二范数的时间非常短，所以，该段时间会被忽略。

2.2 基于离线背包模型的联邦学习：OfflineKP-FL

2.2.1 OfflineKP-FL 协议

OfflineKP-FL 协议的关键思想是基于离线背包模型选择客户端。该协议大致有如下 4 步。

1) 中心服务器收集客户端的先验资源信息，包括计算能力、信道状态和与当前模型训练相关的数据资源。

2) 中心服务器下发全局模型，客户端在本地同时训练更新模型，更新完毕后，客户端计算模型更新前后的权重差值的二范数，并立即将权重差值的二范数上传给中心服务器。

3) OfflineKP-FL 协议下系统完成一轮训练的工作过程如图 2 所示，一旦有一个客户端（如用户 1）上传完权重差值的二范数，服务器就立即在所有上传完权重差值的二范数的用户中基于离线背包模型选择参与全局模型更新的客户，直到选择用户时得到的 $V\left[T_{\mathrm{remain}}\right]\left[K^{''}\right]$ 取得极大值，服务器才能够确定本轮被选择的客户端集合。

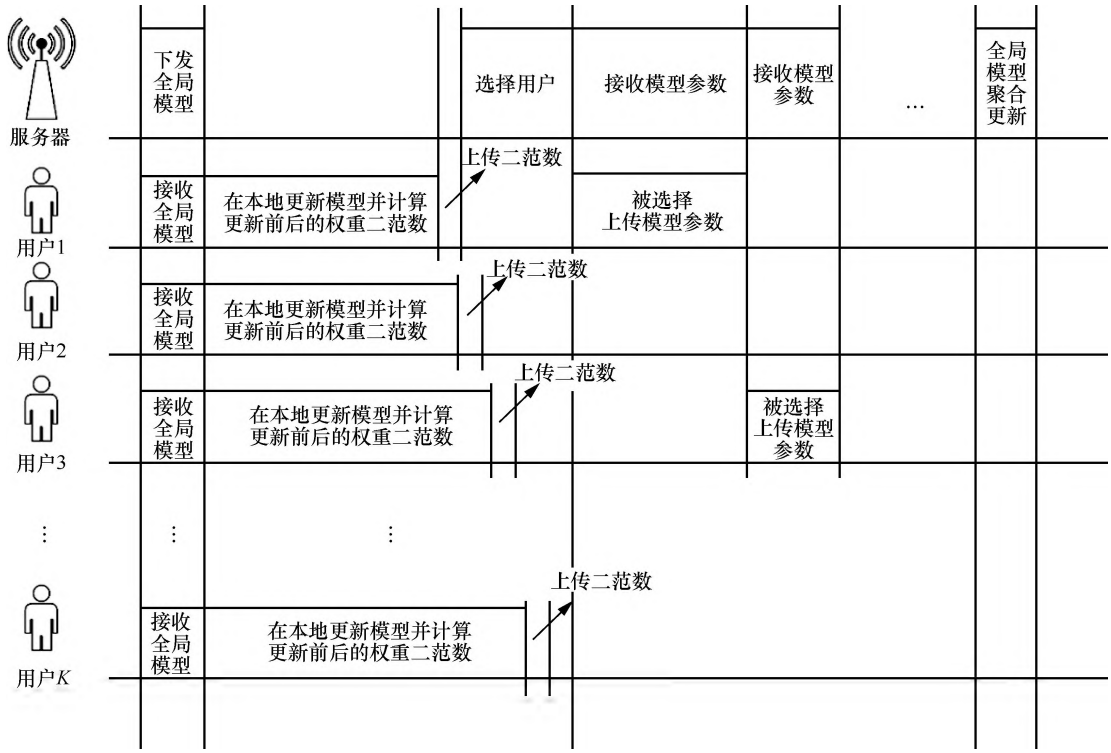


图 2　OfflineKP-FL 协议下系统完成一轮训练的工作过程

4) 被选择的客户端(图 2 中的用户 1 和用户 3)依次串行上载训练完的模型参数，待被选择的用户全部完成参数上传，中心服务器开始全局模型的聚合更新，与 FedAvg（federated averaging）算法[43]中全局模型聚合的方法一致。重复执行除了初始化之外的步骤直到全局模型的性能达到预期的目标。

2.2.2　基于离线背包模型的客户端选择

在基于离线背包模型的客户端选择中，根据对加速全局模型收敛贡献程度的高低选择客户端，考虑最大化被选择的客户端更新前后的权重差值的二范数，其中，中心服务器最终选择的客户端构成了集合 $S=\{k_1,k_2,\cdots,k_{|S|}\}$，同时，要求每轮所有客户端花费的总时间 T_{cost} 小于设定的数值 T_{round}，那么，客户端选择算法可以用如下的优化问题描述

$$\max\left\{\sum_{i=1}^{|S|}\left\|\Delta\boldsymbol{\omega}_{k_i}(t+1)\right\|_2\right\} \tag{4}$$

$$\text{s.t. } T_{\text{cost}}\leqslant T_{\text{round}} \tag{5}$$

由于上述优化问题与离线背包模型类似，所以，把客户端看作背包问题中的物品，客户端更新前后的权重差值的二范数被看作物品的价值，新的模型参数的上载时间相当于物品的质量，设定的每轮时间上限 T_{round} 减去当前已经完成模型训练的客户端训练模型所需的最长时间相当于背包的承重上限。一轮训练中基于离线背包的客户端选择见算法 1，通过动态规划，求解离线背包模型，选择客户端。

用数学符号描述此算法，根据先验信息，将客户端按照其在本地训练模型的时间由短到长的顺序排序，$C=\{1,\cdots,k,\cdots,K\}$ 代表按照上述规则排序后 K 个客户端的索引，$T^d\in R_+$ 是花费在下发全局模型上的时间。在前 k 个客户端完成模型训练后，$T_{\text{CS}}\in R_+$ 代表中心服务器选择客户端需要的总时间。等算法 1 返回的 $V\left[T_{\text{remain}}\right]\left[K^*\right]$ 达到极大值，此时，完成模型训练的客户端构成了集合 $C^*\subseteq C$，通过算法 1 选择的客户端构成了 C 的另一个子集 $S=\{k_1,k_2,\cdots,k_{|S|}\}\subseteq C$。对于客户端 k，$t_k^{\text{UC}}\in R_+$ 表示在本地训练局部模型的时间；$t_k^{\text{UL}}\in R_+$ 表示花费在上载模型参数上的时间。$T_{\text{agg}}\in R_+$ 是全局模型聚合需要的时间，$T_{\text{round}}\in R_+$ 是设定的每轮总时间。如第 2 节中所述，$T^d=0$，$T_{\text{CS}}=0$，$T_{\text{agg}}=0$。所以，系统每轮训练花费的总时间为

$$T_{\text{cost}}=\max_{k\in C^*}\left\{t_k^{\text{UC}}\right\}+\sum_{i=1}^{|S|}t_{k_i}^{\text{UL}} \tag{6}$$

算法 1 一轮训练中基于离线背包的客户端选择

输入：当前完成模型训练的客户端集合：$C^{"}=\{1,\cdots,k,\cdots,K^{"}\}\subseteq C$；$\|\Delta\boldsymbol{\omega}_k\|_2$，$k\in C^{"}$；$t_k^{\mathrm{UC}}$、$t_k^{\mathrm{UL}}$，$k\in C$；设定的每轮总时间$T_{\mathrm{round}}$；当前轮次的剩余时间$T_{\mathrm{remain}}$；当前背包中物品的总价值$V\left[T_{\mathrm{remain}}\right]\left[K^{"}\right]$

如果当前背包中物品的总价值$V\left[T_{\mathrm{remain}}\right]\left[K^{"}\right]$大于上一次求出的背包中物品的总价值

当又有一个客户端$K^{"}+1$完成本地模型训练并上传完权重差值的二范数时

把$K^{"}+1$加到集合$C^{"}$中

$T_{\mathrm{remain}}\leftarrow T_{\mathrm{round}}-\max\limits_{k\in C^{"}}\max\limits_{k\in C^{"}}\left\{t_k^{\mathrm{UC}}\right\}$

$S\leftarrow\varnothing$

$V\left[T_{\mathrm{remain}}\right]\left[K^{"}\right]\leftarrow 0$

基于背包容量T_{remain}、物品价值$\|\Delta\boldsymbol{\omega}_k\|_2$和物品重量$t_k^{\mathrm{UL}}$，对集合$C^{"}$中的客户端使用 0-1 背包模型求解当前被选择的客户端集合S和当前背包中物品的总价值$V\left[T_{\mathrm{remain}}\right]\left[K^{"}\right]$

如果当前背包中物品的总价值$V\left[T_{\mathrm{remain}}\right]\left[K^{"}\right]$不大于上一次求出的背包中物品的总价值

本轮客户端选择结束

输出：$S, V\left[T_{\mathrm{remain}}\right]\left[K^{"}\right]$

虽然，算法 1 使用了离线背包模型优化选择客户端的算法，但是先训练完模型的客户端需要等算法 1 返回的$V\left[T_{\mathrm{remain}}\right]\left[K^{"}\right]$达到极大值后才能确定自己是否需要上载模型参数。也就是说，相较于 FedCS 协议，OfflineKP-FL 协议虽然考虑了客户端对加速全局模型收敛的贡献程度，但是会浪费更多时间，因此，全局模型的收敛速度是否明显地提高需要进行仿真验证。同时，为了降低算法的复杂度，本文又考虑了另一种背包模型：在线背包模型，下文将利用这种模型选择客户。

2.3 基于在线背包模型的联邦学习：OnlineKP-FL

2.3.1 OnlineKP-FL 协议

为了降低计算的复杂度，本节提出了 OnlineKP-FL 协议。不同于 OfflineKP-FL 协议，该协议的关键思想是用在线背包模型[44]选择客户端。

与 OfflineKP-FL 协议类似，该协议大致分为 4 步，其中前两步与 OfflineKP-FL 协议的相同。在 OnlineKP-FL 协议下系统完成一轮训练的工作过程如图 3 所示，中心服务器在收到来自客户端（如用户 1）的权重差值的二范数后，基于在线背包模型立即确定该客户端是否参与全局模型的聚合更新。图 3 中的用户 1 被选择，所以立即上传训练完的模型参数。而在用户 1 之后上传权重差值的二范数的用户 2 未被选择，不会上载参数。由于同一时间只

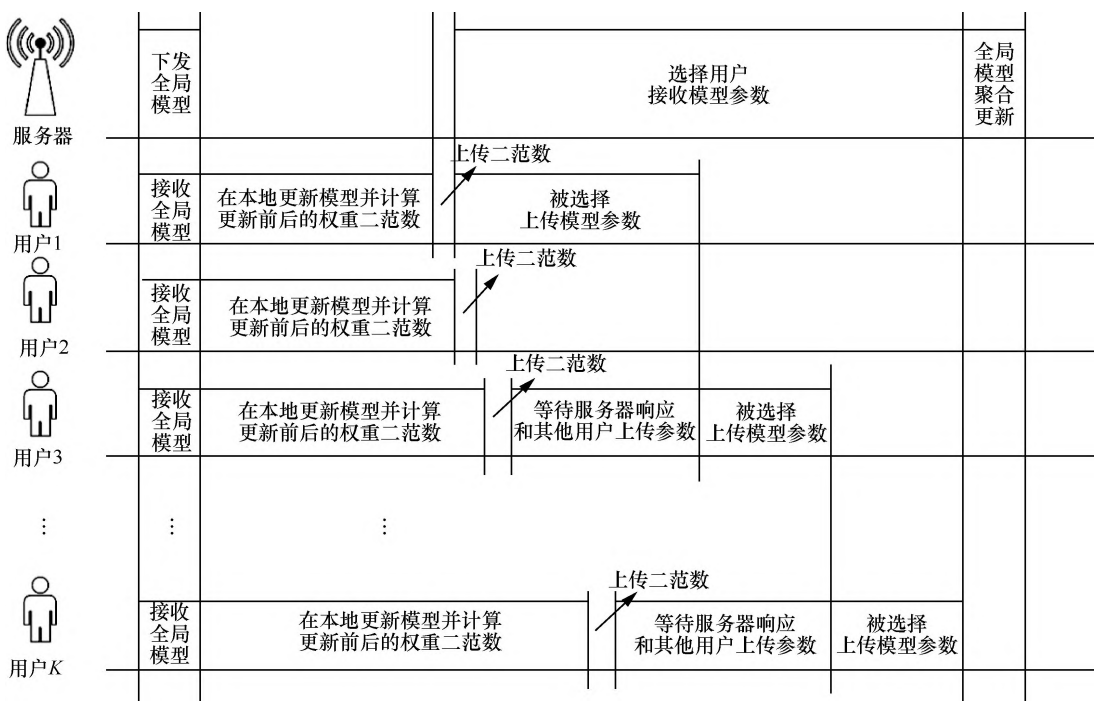


图 3 在 OnlineKP-FL 协议下系统完成一轮训练的工作过程

能有一个用户上传模型参数，所以，即使用户 3 已经上传完权重差值的二范数并且被服务器选择，还是需要等待用户 1 完成参数的上传。在所有被选择的客户端完成参数上载后，中心服务器开始全局模型的更新，与 FedAvg 算法[43]中全局模型聚合的方法一致。重复执行进行除了初始化之外的步骤多次直到全局模型的性能达到预期的目标。

2.3.2　基于在线背包模型的客户端选择

在线背包模型中，仍需要已知有限数量物品的重量与价值，要求选择物品放入具有承重上限的背包中，使背包中的物品总价值最大。所以，在基于在线背包模型的客户端选择中，仍旧用式(4)和式(5)描述选择客户端的优化问题。根据在线背包模型的求解方法，一旦知道了物品的重量与价值，就可以立即确定是否要将该物品放入背包。因此，与算法 1 不同的是，在基于在线背包模型的客户端选择中，用归一化更新前后的权重差值的二范数代表物品的价值，客户端上载模型参数的时间加上该客户端与上一个客户端（即上一个训练完模型训练的客户端）在本地训练模型用时的差值相当于物品的重量，并通过 Chakrabarty D 等[44]提出的 ON-KP-THRESHOLD 算法，求解在线背包模型，选择客户端，面向一个用户的基于在线背包模型的客户端选择见算法 2。

用数学符号描述此算法，根据先验信息，将客户端按照其在本地训练模型的时间由短到长的顺序排序，$C=\{1,\cdots,k,\cdots,K\}$ 代表按照上述规则排序后 K 个客户端的索引，$T^d\in R_+$ 是花费在下发全局模型上的时间。客户端 k 完成模型训练后，$T_{\mathrm{CS}}^k\in R_+$ 代表中心服务器判断客户端 k 是否上载模型参数需要的时间，同样地，如第 2 节所述，$T_{\mathrm{CS}}^k=0,\forall k\in\mathbf{K}$。在达到设定的每轮总时间之前，在本地训练完局部模型的客户端构成了 C 的子集 $C^{'}\subseteq C$。最终被选中的客户端构成了 C 的另一个子集 $S\subseteq C$。其余数学符号的表示与第 2.2.2 节中的一致。

由于客户端在本地同时训练模型，串行上载模型参数，所以，被选中的客户端上载模型参数的时间总和就是本轮花费在上载模型参数上的总时间，另外，当有客户端上载模型参数时，其他客户端可以同时在本地训练模型，因此，单个客户端在本地训练模型和计算权重差值的二范数的时间之和 t_k^{UC} 不会消耗 T_k^{UC}，只要它被包括在之前经过的时间 Θ_{k-1} 内。

$$\Theta_k=\begin{cases}0 & ,k=0\\ T_k^{\mathrm{UC}}+t_k^{\mathrm{UL}} & ,\text{客户端}k\text{被选择}\\ T_k^{\mathrm{UC}} & ,\text{其他}\end{cases}\tag{7}$$

$$T_k^{\mathrm{UC}}=\max\{0,t_k^{\mathrm{UC}}-\Theta_{k-1}\}\tag{8}$$

综上，用式(10)所示的优化问题描述基于在线背包模型的客户端选择算法。

$$\max\{\sum_{k\in S}\left\|\Delta\boldsymbol{\omega}_k(t+1)\right\|_2\}\tag{9}$$

$$\text{s.t. } T_{\mathrm{round}}\geqslant T^d+\sum_{k=1}^{K'}\Theta_k+\mathrm{Tagg}\tag{10}$$

算法 2　面向一个用户的基于在线背包模型的客户端选择

输入：上一轮中所有客户端的权重差值的二范数的最大值 $\left\|\Delta\omega(t-1)\right\|_{2\max}$；第 t 轮中，当前完成模型训练的客户端集合 $C'\subseteq C$；$\left\|\Delta\omega_k(t)\right\|$，$k\in C'$；$t_k^{\mathrm{UC}}$、$t_k^{\mathrm{UL}}$，$k\in C$；设定的每轮时间上限 T_{round}；参数 $L_0\in R_+$；参数 $U\in R_+$；当前被选择的客户端集合 S

当客户端 k 完成本地模型训练并上传完权重差值的二范数时

当前剩余时间 $T_{\mathrm{remain}}\leftarrow T_{\mathrm{round}}-\sum_{k=1}^{C^{'}}\Theta_k$

if $\left\|\Delta\omega(t-1)\right\|_{2\max}==0$

　$L\leftarrow L_0$

else

　$L\leftarrow\dfrac{\left\|\Delta\omega_{\mathrm{k}}(t)\right\|_2}{\left\|\Delta\omega(t-1)\right\|_{2\max}\times L_0}$

　$C\leftarrow\dfrac{1}{1+\ln\left(\dfrac{U}{L}\right)}$

　$z_k\leftarrow\dfrac{T_{\mathrm{remain}}}{T_{\mathrm{round}}}$

　if $z_k\leqslant C$

　　$\Psi\leftarrow L$

　　if $z_k<1$

　　$\Psi\leftarrow\left(\dfrac{U\times\mathrm{e}}{L}\right)^{z_k}\left(\dfrac{L}{\mathrm{e}}\right)$

　　else

　　$\Psi\leftarrow U$

　if $\dfrac{\left\|\Delta\omega_k(t)\right\|_2}{t_k^{\mathrm{UC}}-t_{k-1}^{\mathrm{UC}}+t_k^{\mathrm{UL}}}\geqslant\Psi$

　　把客户端 k 加到集合 S 中

　把客户端 k 加到集合 C' 中

输出：集合 S

在算法 2 中使用了在线背包模型，在客户端完成模型训练并上传完权重差值的二范数后，中心服务器可以立即决定是否选择该客户端。如果被选择，那么该客户端可以立即准备上载模型参数。与 OfflineKP-FL 协议相比，OnlineKP-FL 协议中，被选中的客户端不必等待其他客户端完成模型训练，就可以立即准备上载模型参数。再加上考虑了客户端对加速全局模型收敛的贡献程度，理论上，在这种协议下，全局模型的收敛速度会明显地提高。

3 仿真分析

为了证明提出的协议对加速全局模型收敛的有效性，本节模拟了基本的联邦学习框架，并使用公共可用的大规模数据集 MNIST[45]进行了真实的神经网络训练。

3.1 仿真设置

仿真实验中，搭建了一个由 20 个客户端和 1 个中心服务器组成的联邦学习框架，仿真实验参数见表 1。在实验中，假设所有用户的信道增益$|\mathrm{h}_k|^2$服从均值为 1 的指数分布。由此可知，客户端 k 的信噪比为

$$\mathrm{SNR}_k = \frac{p_k |h_k|^2}{\sigma^2} \tag{11}$$

其中，σ^2是噪声功率。

在仿真过程中，用 IID 方式分配 MNIST 数据集：即从 MNIST 的整个训练数据集中随机采样指定数量的图像分配给各个客户端，要求每个客户端都被分配 10 种不同手写体数字的图像，同时，为了在一定程度上满足客户端资源的异构性，每个客户端被分配的图像数量有所不同，总体上呈正态分布。另外，使用测试数据集测试全局模型的性能。

初始化的全局模型由两个 5×5 卷积层（分别是 10、20 个通道，每个通道后面都是 2×2 最大池）、两个全连接层（分别是 320、50 个单元）组成，激活函数采用的是 ReLU 函数，同时引入 dropout 来防止过拟合。最后，设置学习率为 0.01，并且将T_{round}分别设置 1 000、1 500 和 2 000 共 3 种情况。

表 1 仿真实验参数

参数	取值
所有客户端在本地训练模型的速率服从的均匀分布的均值	5 bit/s
客户端 k 在本地训练局部模型的迭代次数 c_k	5 次
模型大小 M_k	50 bit
客户端的传输功率 p_k	10^{-3} W
噪声功率 σ^2	10^{-3} W
客户端在本地训练模型时数据的批次大小	50 个

3.2 仿真结果和分析

3.2.1 验证更新前后权重差值的二范数的有效性

仿真实验中，对比了 IID 设置下两种选择客户端的方法的性能，即分别利用两种方法在 20 个客户端中选 10 个。这两种选择客户端的方法分别是随机选择客户端参与全局模型的聚合更新和选择权重差值的二范数更大的客户端。随机选择客户端时，要求所有客户端都参与每轮的局部模型的训练，并且每轮都从 20 个客户端中随机选出 10 个进行全局模型的聚合更新，最后绘制全局模型在测试集上的准确率曲线；选择权重差值的二范数更大的客户端时，仍要求所有客户端都参与每轮的局部模型的训练，并且每轮都从 20 个客户端中选出 10 个权重差值的二范数最大的客户端进行全局模型的聚合更新，再绘制全局模型在测试集上的准确率曲线，与随机选择客户端进行对比。

随机选择客户端和选择权重差值的二范数更大的客户端的性能对比如图 4 所示，全局模型在测试集上的准确率达到相同的值时，选 10 个权重差值的二范数最大的客户端比任选客户端所用的总轮数更少。由此可见，在 IID 设置下，选择权重差值的二范数更大的客户端比任选客户端对加速全局模型的收敛更有利。

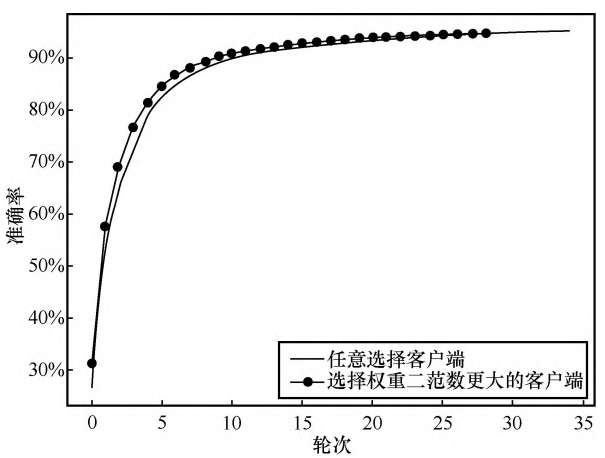


图 4 随机选择客户端和选择权重差值的二范数更大的客户端的性能对比

3.2.2　对比在 3 种协议下全局模型的收敛效果

本节仿真了 T_{round} 取不同的值时，FedCS 协议、OfflineKP-FL 协议和 OnlineKP-FL 协议下，全局模型分别在测试集上准确率的变化情况，以验证本文提出的协议对加速全局模型收敛的有效性。

T_{round} 取不同值时，3 种协议下全局模型的准确率的变化情况对比如图 5 所示，无论 T_{round} 取 1 000、1 500、2 000，与其余两种协议相比，在 OnlineKP-FL 协议下，全局模型经过最少的时间在测试集上能够达到相同的准确率，也就是说，全局模型的收敛速度明显更快，而在 OfflineKP-FL 协议下，只有 $T_{\text{round}}=1\,000$ 时，全局模型的收敛速度比 FedCS 协议快。由此可知，OnlineKP-FL 协议能够加速全局模型的收敛速度，要比 FedCS 协议下全局模型收敛地快。在 OfflineKP-FL 协议下，在一定的时间周期内，全局模型的收敛速度才会有所提高。

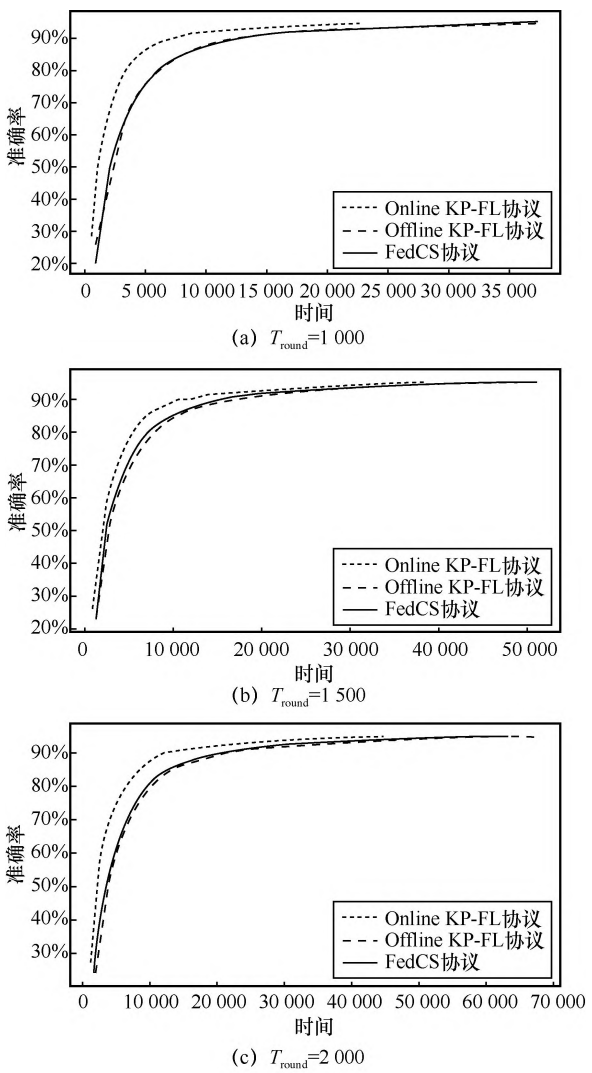


图 5　T_{round} 取不同值时，3 种协议下全局模型的准确率的变化情况对比

T_{round} 分别取 1 000、1 500、2 000 时，3 种协议达到相同准确率所需要的时间见表 2，其中，ToA@0.95 表示准确率达到 95%时所需的时间。

可以看出，在 T_{round} 分别取 1 000、1 500、2 000 时，OnlineKP-FL 协议下全局模型在测试集上达到 95%的准确率所需要的时间最短，且在 $T_{\text{round}}=1\,000$ 时，OnlineKP-FL 协议下所需时间可以达到 FedCS 协议下的 64.1%，大大节省了系统训练时间，提高了训练效率。而 OfflineKP-FL 协议与 FedCS 协议下需要的时间差不多，甚至在 T_{round} 取 1 500 和 2 000 时，前者需要更长的时间，这是由于在 OfflineKP-FL 协议下，先完成局部模型训练的客户端不能确定自己是否需要上载模型参数，需要等待一段时间，直到背包中的（被选中的）客户端的权重差值的二范数达到极大值。换言之，选择权重差值的二范数更大的客户端并没有弥补由于离线背包的高复杂度求解方法带来的时间损耗，这表明了 OfflineKP-FL 协议的局限性。对比之下，OnlineKP-FL 协议下联邦学习不存在时间损耗，同时利用了客户端的权重差值的二范数确定它们对加速全局模型收敛的贡献，并以此为标准选择客户端。综上所述，OnlineKP-FL 协议能够加速全局模型的收敛速度，效果要比 FedCS 协议好，而 OfflineKP-FL 协议具有一定的局限性，只在一定的时间周期内，全局模型的收敛速度优于 FedCS 协议。

表 2　T_{round} 分别取 1 000、1 500、2 000 时，3 种协议达到相同准确率所需要的时间

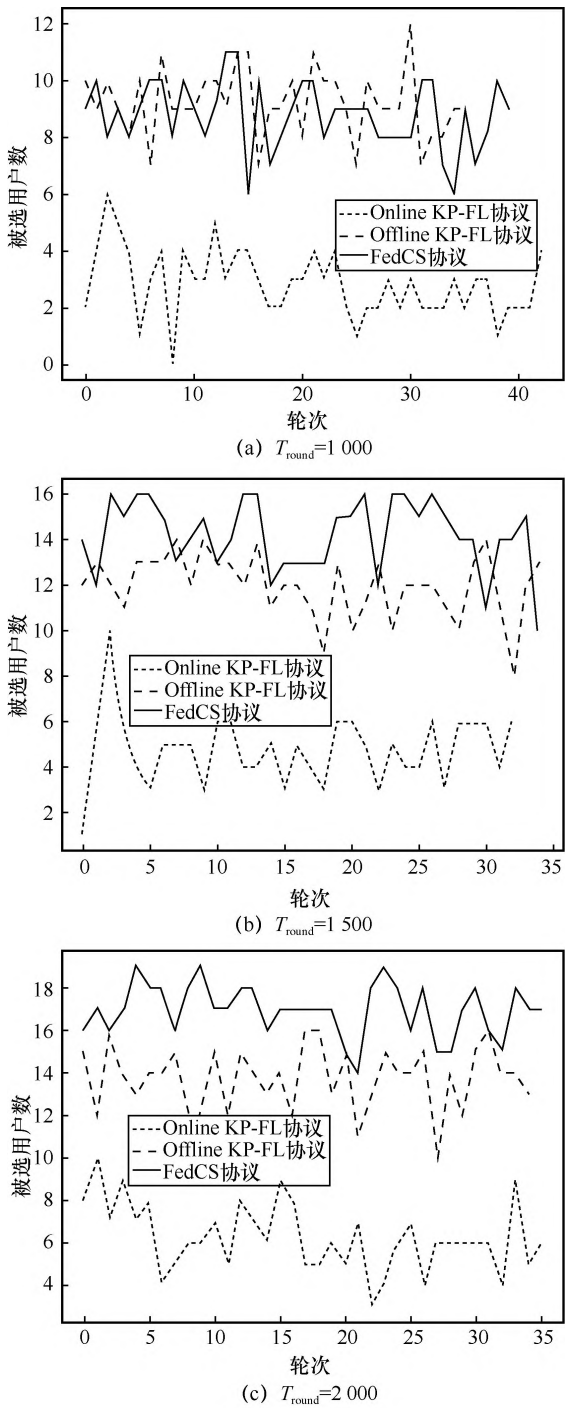
协议每轮时间上限	FedCS 协议	OnlineKP-FL 协议	OfflineKP-FL 协议
	ToA@0.95		
T_{round}=1 000	36 060	23 100	35 460
T_{round}=1 500	48 360	38 700	51 660
T_{round}=2 000	63 060	44 760	67 560

3.2.3　对比在 3 种协议下服务器挑选的客户端数量

T_{round} 分别取 1 000、1 500、2 000 时，3 种协议下每轮选择的用户数量的变化情况对比如图 6 所示，T_{round} 分别取 1 000、1 500、2 000 时，3 种协议每轮平均选择的用户数见表 3。

仿真发现，在 OfflineKP-FL 协议下，只有 T_{round} 取 1 500 和 2 000 时，每轮平均选择的用户数小于 FedCS 协议，说明了 OfflineKP-FL 协议的局限性，即只能在特定的情况下优于 FedCS 协议。而对于 OnlineKP-FL 协议，不论 T_{round} 取何值，每轮选择的客户端数量都是最少的，甚至有时会少于另外两种协议

下选择的客户端数量的一半，同时，OnlineKP-FL 协议下全局模型的收敛取得了最好的效果，由此可见，OnlineKP-FL 协议下不需要太多的客户端参与全局模型的聚合更新就可以加快全局模型的收敛速度，大大提高了联邦学习算法的性能。但是 OfflineKP-FL 协议下，只有当系统训练周期取定部分数值时，每轮选择用户的数量才会低于 FedCS 协议。



(a) T_{round}=1 000

(b) T_{round}=1 500

(c) T_{round}=2 000

图 6　T_{round} 分别取 1 000、1 500、2 000 时，3 种协议下每轮选择的用户数量的变化情况对比

表 3　T_{round} 分别取 1 000、1 500、2 000 时，3 种协议每轮平均选择的用户数

协议	FedCS 协议	OnlineKP-FL 协议	OfflineKP-FL 协议
每轮时间上限	平均每轮选择的客户端数量		
T_{round}=1 000	8.8	2.8	9.2
T_{round}=1 500	14.2	4.8	12.0
T_{round}=2 000	17.0	6.3	13.8

4　结束语

本文提出了两个通过优化选择客户端算法提高性能的联邦学习的协议，分别是 OfflineKP-FL 协议和 OnlineKP-FL 协议。这两种协议分别基于离线背包和在线背包模型选择客户端，并考虑了客户端对加速全局模型收敛的贡献程度，即客户端局部模型更新前后的权重差值的二范数。通过仿真验证，OnlineKP-FL 协议下全局模型的收敛速度明显比 FedCS 协议和 OfflineKP-FL 协议下的快。而 OfflineKP-FL 协议，由于需要先完成局部模型训练的客户端等待大部分客户端完成模型训练后才能确定是否需要排队上载模型参数，所以全局模型的收敛速度取决于设定的联邦学习系统每轮的时间周期，在一定的时间周期内，全局模型的收敛速度优于 FedCS 协议，具有一定局限性。另外，本文提出的 OnlineKP-FL 协议仅考虑了 IID 数据分布，所以未来的研究重点在于对 Non-IID 数据分布的适用性上。

参考文献：

[1] HAN M Q, SUN X H, ZHENG S H, et al. Resource rationing for federated learning with reinforcement learning[C]//2021 Proc. ComComAp. [S.l.:s.n], 2021:150-155.

[2] XU B, XIA W C, ZHANG J, et al. Dynamic client association for energy-aware hierarchical federated learning[C]//2021 IEEE Wireless Communications and Networking Conference (WCNC). Piscataway: IEEE Press, 2021:1-6.

[3] KONEČNÝ J. Stochastic, distributed and federated optimization for machine learning[J]. arXiv preprint, 2017, arXiv:1707.01155.

[4] SAHU A K, LI T, SANJABI M, et al. Federated optimization for heterogeneous networks[J]. arXiv preprint, 2018, arXiv:1812.06127.

[5] LIU Y, MUPPALA J K, VEERARAGHAVAN M, et al. Data center networks: topologies, architectures and fault-tolerance characteristics[M]. Heidelberg: Springer Science & Business Media, 2013.

[6] KONEČNÝ J, MCMAHAN H B, YU F X, et al. Federated learning: strategies for improving communication efficiency[J]. arXiv preprint,2016,arXiv:1610.05492.

[7] CALDAS S, KONEČNY J, MCMAHAN H B, et al. Expanding the

reach of federated learning by reducing client resource requirements[J]. arXiv preprint, 2018,arXiv:1812.07210.

[8] NISHIO T, YONETANI R. Client selection for federated learning with heterogeneous resources in mobile edge[C]//Proceedings of ICC 2019 - 2019 IEEE International Conference on Communications. Piscataway: IEEE Press, 2019: 1-7.

[9] SHIN J, LI Y C, LIU Y X, et al. FedBalancer: data and pace control for efficient federated learning on heterogeneous clients[C]//Proceedings of the 20th Annual International Conference on Mobile Systems, Applications and Services. New York: ACM Press, 2022: 436–449.

[10] TAHIR A, CHEN Y, NILAYAM P. FedSS: federated learning with smart selection of clients[J]. arXiv preprint, 2022, arXiv:2207.04569.

[11] REN J K, HE Y H, WEN D Z, et al. Scheduling for cellular federated edge learning with importance and channel awareness[J]. IEEE Transactions on Wireless Communications, 2020, 19(11): 7690-7703.

[12] LEE J, KO H, PACK S. Adaptive deadline determination for mobile device selection in federated learning[J]. IEEE Transactions on Vehicular Technology, 2022, 71(3): 3367-3371.

[13] XIA W C, QUEKT Q S, GUO K, et al. Multi-armed bandit-based client scheduling for federated learning[J]. IEEE Transactions on Wireless Communications, 2020, 19(11): 7108-7123.

[14] HUANG T S, LIN W W, WU W T, et al. An efficiency-boosting client selection scheme for federated learning with fairness guarantee[J]. IEEE Transactions on Parallel and Distributed Systems, 2021, 32(7): 1552-1564.

[15] YANG H H, LIU Z Z, QUEK T Q S, et al. Scheduling policies for federated learning in wireless networks[J]. IEEE Transactions on Communications, 2020, 68(1): 317-333.

[16] XU J, WANG H Q. Client selection and bandwidth allocation in wireless federated learning networks: along-term perspective[J]. IEEE Transactions on Wireless Communications, 2021, 20(2): 1188-1200.

[17] SHI W Q, ZHOU S, NIU Z S, et al. Joint device scheduling and resource allocation for latency constrained wireless federated learning[J]. IEEE Transactions on Wireless Communications, 2021, 20(1): 453-467.

[18] RIBERO M, VIKALO H. Communication-efficient federated learning via optimal client sampling[EB]. 2020.

[19] ABDULRAHMAN S, TOUT H, MOURAD A, et al. FedMCCS: multicriteria client selection model for optimal IoT federated learning[J]. IEEE Internet of Things Journal, 2021, 8(6): 4723-4735.

[20] FRABONI Y, VIDAL R, KAMENI L, et al. Clustered sampling: low-variance and improved represent ativity for clients selection in federated learning[C]//International Conference on Machine Learning. New York: PMLR, 2021: 3407-3416.

[21] WANG L, GUO Y X, LIN T, et al. Client selection in non convex federated learning: improved convergence analysis for optimal unbiased sampling strategy[EB]. 2022.

[22] MARNISSI O, HAMMOUTI H E, BERGOU E H. Client selection in federated learning based on gradients importance[J]. arXiv preprint, 2021, arXiv:2111.11204.

[23] NAGALAPATTI L, NARAYANAM R. Game of gradients: mitigating irrelevant clients in federated learning[C]//Proceedings of the AAAI Conference on Artificial Intelligence. 2021, 35(10):9046-9054.

[24] TABATABAI S, MOHAMMED I, QOLOMANY B, et al. Exploration and exploitation in federated learning to exclude clients with poisoned data[C]//Proceedings of 2022 International Wireless Communications and Mobile Computing (IWCMC). Piscataway: IEEE Press, 2022: 407-412.

[25] WANG H, KAPLAN Z, NIU D, et al. Optimizing federated learning on non-IID data with reinforcement learning[C]//Proceedings of IEEE INFOCOM 2020 - IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2020: 1698-1707.

[26] ZHANG W Y, WANG X M, ZHOU P, et al. Client selection for federated learning with non-IID data in mobile edge computing[J]. IEEE Access, 9: 24462-24474.

[27] KANG J W, XIONG Z H, 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.

[28] KANG J W, XIONG Z H, NIYATO D, et al. Reliable federated learning for mobile networks[J]. IEEE Wireless Communications, 2020, 27(2): 72-80.

[29] MAHMOOD A, SHENGQ Z, SIDDIQUIS A, et al. When trust meets the Internet of vehicles: opportunities, challenges, and future prospects[C]//Proceedings of 2021 IEEE 7th International Conference on Collaboration and Internet Computing. Piscataway: IEEE Press, 2021:60-67.

[30] MAHMOOD A, SIDDIQUIS A, SHENGQ Z, et al. Trust on wheels: towards secure and resource efficient IoV networks[J]. Computing, 2022, 104(6): 1337-1358.

[31] LIU Y N, LI K Q, JIN Y W, et al. A novel reputation computation model based on subjective logic for mobile ad hoc networks[J]. Future Generation Computer Systems, 2011, 27(5): 547-554.

[32] ZOU Y, SHEN F, YAN F, et al. Reputation-based regional federated learning for knowledge trading in blockchain-enhanced IoV[C]//Proceedings of 2021 IEEE Wireless Communications and Networking Conference. Piscataway: IEEE Press, 2021: 1-6.

[33] SONG Z D, SUN H G, YANG H H, et al. Reputation-based federated learning for secure wireless networks[J]. IEEE Internet of Things Journal, 2022, 9(2): 1212-1226.

[34] PERAZZONE J, WANG S Q, JIM Y, et al. Communication-efficient device scheduling for federated learning using stochastic optimization[C]//Proceedings of IEEE INFOCOM 2022 - IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2022: 1449-1458.

[35] WU H D, WANG P. Node selection toward faster convergence for federated learning on non-IID data[J]. IEEE Transactions on Network Science and Engineering, 2022,PP(99): 1.

[36] MA J H, SUN X H, XIA W C, et al. Client selection based on label quantity information for federated learning[C]//Proceedings of 2021 IEEE 32nd Annual International Symposium on Personal, Indoor and Mobile Radio Communications. Piscataway: IEEE Press, 2021: 1-6.

[37] ZHAO J X, CHANG X Y, FENG Y H, et al. Participant selection for

federated learning with heterogeneous data in intelligent transport system[J]. IEEE Transactions on Intelligent Transportation Systems, 2022, PP(99): 1-10.

[38] WANG S, LEEM Y, HOSSEINALIPOUR S, et al. Device sampling for heterogeneous federated learning: theory, algorithms, and implementation[C]//Proceedings of IEEE INFOCOM 2021 - IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2021: 1-10.

[39] WU W T, HE L G, LIN WW, et al. Accelerating federated learning over reliability-agnostic clients in mobile edge computing systems[J]. IEEE Transactions on Parallel and Distributed Systems, 2021, 32(7): 1539-1551.

[40] NGUYEN H T, SEHWAG V, HOSSEINALIPOUR S, et al. Fast-convergent federated learning[J]. IEEE Journal on Selected Areas in Communications, 2021, 39(1): 201-218.

[41] YEGANEH Y, FARSHAD A, NAVAB N, et al. Inverse distance aggregation for federated learning with non-IID data[C]//Domain Adaptation and Representation Transfer, and Distributed and Collaborative Learning, 2020: 150-159.

[42] 马嘉华, 孙兴华, 夏文超, 等. 基于标签量信息的联邦学习节点选择算法[J]. 物联网学报, 2021, 5(4): 46-53.
MA J H, SUN X H, XIA W C, et al. Node selection based on label quantity information in federated learning[J]. Chinese Journal on Internet of Things, 2021, 5(4): 46-53.

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

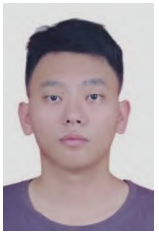
[44] CHAKRABARTY D, ZHOU Y, LUKOSE R. Online knapsack problems[C]//Workshop on Internet and Network Economics (WINE). 2008.

[45] YANN L. The MNIST database of handwritten digits[EB]. 1998.

[作者简介]

郭佳慧（2000– ），女，中山大学电子与通信工程学院在读，主要研究方向为联邦学习等。

陈卓越（2000– ），男，中山大学电子与通信工程学院硕士生，主要研究方向为拥塞控制、在线学习、联邦学习等。



高玮（1999– ），男，中山大学电子秘通信工程学院硕士生，主要研究方向为联邦学习、无人机集群、目标跟踪等。

王玺钧（1984– ），男，博士，中山大学电子与信息工程学院副教授，主要研究方向为信息年龄、强化学习等。

孙兴华（1985– ），男，博士，中山大学电子与通信工程学院副教授，主要研究方向为下一代无线通信网络、智能通信等。

高林（1980– ），男，博士，哈尔滨工业大学（深圳）电子与信息工程学院副教授，主要研究方向为移动边缘计算、群智计算、群体智能、博弈论、强化学习、联邦学习等。