课题组已核实初稿及修改稿中所有建议，确认已无其他技术细节未补充并按以下文本提交专利局，接受专利局的审查决定。

项目负责人签字 郑臻哲

2022 年04 月 14 日

说 明 书

基于夏普利值的联邦学习移动设备分布数据处理方法

技术领域

[0001] 本发明涉及的是一种分布式数据处理领域的技术，具体是一种基于联邦学习(Federated Learning)和夏普利值(Shapley Value)的移动设备分布数据处理方法。

背景技术

[0002] 随着移动网络的不断发展，不同网络层的设备实时产生的数据量越来越大，格式越来越复杂，需要人工智能模型来自动地管理整个网络。传统的模型训练方法要求一个中心服务器从各个移动设备采集数据，然后集中式地训练模型。但是，传输大量数据会带来高昂的通信开销，并且上传用户数据会侵犯移动设备的隐私。

[0003] 联邦学习框架作为一种分布式的机器学习方法被提出来解决上述问题，在每轮训练中，移动设备上传模型更新而非用户数据，在减小通信开销的同时避免了客户私密数据的泄露。受到中心服务器通信带宽和计算资源的限制，在每一轮的联邦学习过程中，仅有部分移动设备能够被中心服务器选中参与到模型的训练过程，极大地限制了每次模型更新所涉及的训练数据量，从而降低了模型的收敛速度和最终性能。

[0004] 许多工作证明了不同训练数据样本对于模型训练的重要程度也是不同的，仅挑选部分重要的样本参与训练能够在减少训练时长的同时保证模型的最终精度。已有一些工作提出了集中式学习场景下的训练数据选择方法，包括基于 LOO(Leave-one-out)的方法，基于影响函数(Influence Function)的方法和基于数据夏普利值(Data Shapley)的方法。相比于前两种方法，以夏普利值作为选择的标准具有三条令人满意的性质：有效性(Efficiency)、对称性(Symmetry)和可加性(Additivity)，所以被广泛地认为是最公平合理的选择方法。

发明内容

[0005] 本发明针对现有移动设备的算力资源和模型表现无直接关联、没有考虑移动设备的数据特点和当前中心节点的模型，仅凭借算力选择移动设备，无法从理论上加快模型收敛、提升模型精度的缺陷，提出一种基于夏普利值的联邦学习移动设备分布数据处理方法，将夏普利值更为合理地应用于联邦学习来解决移动设备的选择问题；提出联邦夏普利值的估计方法来避免指数次的模型重复训练，并结合传统的 Monte-Carlo 采样方法进一步度简化夏普利值的计算复杂度，从而能够衡量各个移动终端的数据集对模型训练过程的影响，从而在每轮选择高贡献度的设备参与训练，减少数据通信开销，加快收敛速度，提升模型表现。

[0006] 本发明是通过以下技术方案实现的：

[0007] 本发明涉及一种基于夏普利值的联邦学习移动设备分布数据处理方法，将多个移动设备构建联邦学习集群，在联邦学习的每一轮中，中心节点应用 Monte-Carlo 采样方法估计各个联邦学习移动设备当前的联邦夏普利值(Fed-Shapley)，并将其在全局模型参数相对于初始参数的变化方向上的投影作为其对模型的重要性与贡献度，并基于联邦夏普利值选择联邦学习移动设备参与本轮的模型训练能够有效加快模型收敛速度，提升模型最终的精度。

[0008] 所述的夏普利值为：$\bar{\phi}_t(k)=\sum_{S\subseteq C\setminus\{k\}}\frac{\bar{w}_t(S\cup\{k\})-\bar{w}_t(S)}{|C|\times\binom{|C|-1}{|S|}}=E_{S\subseteq C\setminus\{k\}}[\bar{w}_t(S\cup\{k\})-\bar{w}_t(S)]$，其中：$\bar{\phi}_t(k)$为联邦学习移动设备 k 在第t轮的联邦夏普利值；C为所有联邦学习移动设备的集合；S为移动设备子集；$\bar{w}_t(S)$为只有移动设备子集S参与到联邦学习训练过程时，全局模型在第t轮的参数，其值需要通过重新训练模型得到。

[0009] 所述的联邦夏普利值(Fed-Shapley)，通过以下方式估计得到：$\bar{\phi}_t(k)=\sum_{S\subseteq C\setminus\{k\}}\frac{\bar{w}_t(S\cup\{k\})-\bar{w}_t(S)}{|C|\times\binom{|C|-1}{|S|}}=\sum_{Q\subseteq C\setminus\{k\}}\frac{[\bar{w}_t(C\setminus Q)-\bar{w}_t(C)]-[\bar{w}_t(C\setminus\{Q,k\})-\bar{w}_t(C)]}{|C|\times\binom{|C|-1}{|Q|}}=\sum_{Q\subseteq C\setminus\{k\}}\frac{\epsilon_t^{-Q,*}-\epsilon_t^{-Q-k,*}}{|C|\times\binom{|C|-1}{|Q|}}$，其中：$\bar{\phi}_t(k)$为联邦学习移动设备k在第t轮的联邦夏普利值；C为所有联邦学习移动设备的集合；S 和 Q表示联邦学习移动设备子集；$\bar{w}_t(S)$为只有联邦学习移动设备子集S参与到联邦学习训练过程时，全局模型在第t轮的参数；$\epsilon_t^{-Q,*}$表示在训练过程中从总联邦学习移动设备集合C移除设备子集Q后，模型在第t轮的参数变化。其值可以通过本发明的估计方法得到：$\epsilon_t^{-Q,*}\approx\epsilon_t^{-Q}=\sum_{k\in C_t\setminus Q}\frac{n_k}{N(C_t\setminus Q)}\prod_{i=0}^{m-1}\left[I-\eta\nabla_w^2L\left(\bar{w}_{t,i}^k(C_t),D_k\right)\right]\epsilon_{t-1}^{-Q}+\bar{w}_t\left(\mathrm{C_t}\rightarrow\mathrm{C_t}\setminus\mathrm{Q}\right)-\bar{w}_t(C)$，其中：$C_t$为当前参与模型训练的移动设备集合；$\mathrm{n_k}$为第k个联邦学习移动设备的数据集大小；$N(C_t\setminus Q)$为设备子集$\mathrm{C_t}\setminus\mathrm{Q}$的总数据集大小；m为移动设备本地更新模型的次数；I为单位矩阵；η为学习率；$\mathrm{L}\left(\bar{w}_{t,i}^k(\mathrm{C_t}),\mathrm{D_k}\right)$表示当模型参数为$\bar{w}_{t,i}^k(\mathrm{C_t})$时，模型在设备k的数据集$\mathrm{D_k}$上的损失函数；$\bar{w}_{t,i}^k(C_t)$为第t轮联邦学习过程中移动设备k在本地数据集上更新i次后的模型；$\bar{w}_t(\mathrm{C_t}\rightarrow\mathrm{C_t}\setminus\mathrm{Q})$表示只在第t轮将联邦学习移动设备子集Q移除后全局模型的参数。因为联邦夏普利值$\bar{\phi}_t(k)$的计算需要遍历移动设备集合C的每一个子集，用 Monte-Carlo 采样方法来估计可以得到时间复杂度更低的估计方法。

[0010] 所述的 Monte-Carlo 采样是指：随机选取包含所有联邦学习移动的多个排列，按照顺序计算每一个排列当中每个联邦学习移动对排列中位于其之前的移动设备集合的边际贡献。最后对每个联邦学习移动设备的边际贡献求取平均值即为每个设备的重要性，即移动设备选择的标准。

[0011] 所述的边际贡献是指：将此联邦学习移动设备加入训练后全局模型参数的变化。

[0012] 所述的联邦学习移动设备选择算法，基于博弈论的经典概念夏普利值(Shapley Value)，具有与之类似的三条公平性定理：当设备k的数据集对于模型性能没有影响，则其价值为 0；

当对于两个设备k_1, k_2，将其数据集分别添加到任意子集$S \subseteq C \setminus k_1, k_2$后模型性能相同，则$k_1$和$k_2$具有相同的价值；任意多种评估方法得到的数据集价值等于这些评估方法结合在一起得到的数据集价值。

[0013] 所述的模型训练，具体包括：1)中心节点下发全局模型给被选中的联邦学习移动设备；2)联邦学习移动设备根据本地数据样本更新模型，并将更新后的模型参数上传给中心节点；3)中心节点聚合各个联邦学习移动设备上传的模型参数为新一轮的全局模型。

[0014] 所述方法，具体包括：

[0015] 步骤 1、在联邦学习过程的开始阶段，中心节点应用 Monte-Carlo 采样方法选取 p 个包含所有联邦学习移动设备的排列$A_i, i = 0,1,\ldots,p-1$，对于每个排列里的每个移动设备$A_i[j]$，中心初始化该设备与其之前设备所组成的设备子集对模型影响的估计，即$\epsilon_t^{-Q} = 0, Q = A_i[0{:}j], j = 0,1,\ldots,|C|, i = 0,..,p$。

[0016] 步骤 2、在训练过程中的每一轮，参与训练的联邦学习移动设备 k 不仅上传经过本地更新后的模型，而且上传本地多次迭代对应的参数修正项，具体为：$\prod_{i=0}^{m-1}\left[I - \eta\nabla_w^2 L\left(\bar{w}_{t,i}^k(C_t), D_k\right)\right]$，其中：m为移动设备本地更新模型的次数；I为单位矩阵；η为学习率；$\bar{w}_{t,i}^k(C_t)$为第t轮联邦学习过程中移动设备k在本地数据集上更新i次后的模型；$\nabla_w^2 L\left(\bar{w}_{t,i}^k(C_t), D_k\right)$为模型$\bar{w}_{t,i}^k(C_t)$在数据集$D_k$上损失函数的二阶导数。

[0017] 步骤 3、中心节点依据各个设备上传的修正项更新本地的设备子集对模型影响的估计，更新公式为$\epsilon_t^{-Q} = \sum_{k \subseteq C_t \setminus Q} \frac{n_k}{N(C_t \setminus Q)} \prod_{i=0}^{m-1}\left[I - \eta\nabla_w^2 L\left(\bar{w}_{t,i}^k(C_t), D_k\right)\right] \epsilon_{t-1}^{-Q} + \bar{w}_t\,(\mathrm{C_t} \rightarrow \mathrm{C_t} \setminus \mathrm{Q}) - \bar{w}_t(C)$。

[0018] 步骤 4、对于每个移动设备 k，中心估计其联邦夏普利值，并将其投影到全局模型的变化方向作为标准选择下一轮参与训练的客户端。所述估计方法为，求取p个排列中该设备对于其之前的设备子集Q的边际贡献，其均值为该设备联邦夏普利值的估计值。所述边际贡献为$\epsilon_t^{-Q} - \epsilon_t^{-Q-k}$，Q为各个排列中位于移动设备k之前的所有移动设备与设备k组成的集合。

[0019] 本发明涉及一种实现上述方法的系统，包括：采样单元、夏普利值计算单元、移动设备选择单元、下发单元、移动设备计算单元、收集单元和中心节点计算单元，其中：采样单元在联邦学习的开始阶段根据采样得到的多个包含所有设备的全排列，对于每个排列里的每个设备，中心初始化该设备与排列中其之前设备所组成的设备子集对模型影响，得到各个设备子集对模型影响的初始估计结果；夏普利值计算单元在每一轮训练中，根据上一轮采样单元计算得到的各个排列中设备子集的模型影响，计算各个移动设备的边际贡献均值，得到各个移动设备联邦夏普利值的估计值结果；移动设备选择单元根据各个设备的联邦夏普利值，计算其在全局模型参数变化方向上的投影值作为选择标准，得到本轮参与模型训练的移动设

备集合；下发单元根据选择的移动设备集合，下发当前中心节点的模型；移动设备计算单元根据接收到的模型信息，进行本地模型更新和本地修正项的计算，得到更新后的模型参数和本轮对应的修正项；收集单元回传各个参与设备的模型参数和修正项给中心节点；中心节点计算单元根据接收到的更新后的模型参数，进行参数聚合处理，得到新一轮的模型参数；采样单元根据接收到的各个参与设备的修正项，进行各个排列中多个移动设备子集对模型影响的更新。

技术效果

[0020] 本发明通过在联邦学习每一轮训练中基于夏普利值进行移动设备选择的同时，通过低复杂度估计单个移动设备夏普利值，与现有技术相比显著提升联邦学习中全局模型的最终精度、减少模型训练时间。

附图说明

[0021] 图 1 为本发明流程图；

[0022] 图 2 为本发明系统示意图；

[0023] 图 3 为实施例中当移除不同数目的设备后，本方法对全局模型参数变化的估计误差随训练轮数的变化；

[0024] 图 4 为实施例中当模型损失函数为实施例中凸函数时，且当设备数据集分布相同且方差都较小、分布不同但方差都较小、分布不同且方差较大时，联邦夏普利值的估计误差随训练轮数变化的关系；

[0025] 图 5 为实施例中应用本发明针对方差较大的改进方法后，联邦夏普利值的估计误差随训练轮数变化的关系；

[0026] 图 6 为实施例中应用 Monte-Carlo 采样方法后，本发明对联邦夏普利值估计的误差随训练轮数的变化关系以及应用改进方法后误差的变化；

[0027] 图 7 为实施例中当模型损失函数为实施例中非凸函数时联邦夏普利值的估计误差随训练轮数的变化关系；

[0028] 图中：a 为实施例中设备数据集独立同分布时的情况，b 为实施例中设备数据集不独立同分布时的情况；

[0029] 图 8 为实施例中依据联邦夏普利值选择不同的移动设备参与模型训练时的训练曲线。

具体实施方式

[0030] 本实施例包括 8 个联邦学习移动设备，其数据的相关信息如图 7 所示，实施步骤如下所示：

[0031] 步骤 1、在联邦学习过程的开始阶段，中心节点应用 Monte-Carlo 采样方法选取 p 个

包含所有联邦学习移动设备的排列$A_i, i = 1,2,\ldots,p$。对于每个排列里的每个设备$A_i[j]$，中心初始化该设备与其之前设备所组成的设备子集对模型影响的估计，即$\epsilon_t^{-Q} = 0, Q = A_i[0{:}j], i = 1,\ldots,p, j = 1,\ldots,8$。

[0032] 步骤 2、在联邦学习训练过程中的每一轮，每个参与训练的设备 k 不仅上传在本地数据上更新m次后的模型$\bar{w}_{t,i}^k$，而且上传本地多次迭代对应的参数修正项δ_t^k。所述修正项为$\delta_t^k = \prod_{i=0}^{m-1}\left[I - \eta\nabla_w^2 L\left(\bar{w}_{t,i}^k(C_t), D_k\right)\right]$，其中m为设备更新模型的次数；I为单位矩阵；$\eta$为学习率；$\bar{w}_{t,i}^k$为在移动设备数据上更新i次后的模型；$D_k$为移动设备的数据。

[0033] 步骤 3、中心依据各个移动设备上传的修正项，更新存储的各个设备子集对模型影响的估计，即$\epsilon_t^{-Q}, Q = A_i[0{:}j], i = 1,\ldots,p, j = 1,\ldots,8$。更新公式为$\epsilon_t^{-Q} = \sum_{k\subseteq C_t\setminus Q}\frac{n_k}{N(C_t\setminus Q)}\delta_t^k\epsilon_{t-1}^{-Q} + \bar{w}_t\left(\mathrm{C_t}\to\mathrm{C_t}\setminus\mathrm{Q}\right) - \bar{w}_t(C)$，其中：k单个移动设备；$C_t$为参与本轮联邦联邦学习的移动设备集合；$n_k$为设备k的数据集规模；$N(C_t\setminus Q)$为联邦移动设备子集$C_t\setminus Q$的总数聚集规模；$\delta_t^k$为设备k上传的修正项；$\bar{w}_t(\mathrm{C_t}\to\mathrm{C_t}\setminus\mathrm{Q})$=$\sum_{k\subseteq C_t\setminus Q}\frac{n_k}{N(C_t\setminus Q)}\bar{w}_t^k$为当不考虑设备子集Q上传的模型参数更新时，中心节点聚合得到的模型参数；$\bar{w}_t(C)$=$\sum_{k\subseteq C_t}\frac{n_k}{N(C_t)}\bar{w}_t^k$为中心节点聚合本轮所有参与训练的移动设备上传的参数更新所得到的模型。

[0034] 步骤 4、中心根据存储的移动设备子集对模型的影响，估计每个移动设备k的联邦夏普利值，并将其投影到全局模型的变化方向作为标准选择下一轮参与训练的客户端。所述估计方法为，求取p个排列中该设备对于其之前的设备子集Q的边际贡献，其均值为该移动设备联邦夏普利值的估计值，即$\bar{\phi}_t(k) = \frac{1}{p}\sum_{i=1}^{p}\epsilon_t^{-A_i[0:j_{i,k}]} - \epsilon_t^{-A_i[0:j_{i,k}-1]}$，其中：$\bar{\phi}_t(k)$为设备k在当前训练轮的联邦夏普利值；p为 Monte-Carlo 采样得到的排列数目；$j_{i,k}$为第i个排列中移动设备k的位置；$A_i[0{:}j_{i,k}]$为第i个排列中设备k和位于其之前的设备组成的移动设备子集。所述投影值为$\langle\bar{\phi}_t(k), \bar{w}_t - \bar{w}_0\rangle$，其中$\bar{\phi}_t(k)$为移动设备k的联邦夏普利值，$\bar{w}_t$为当前联邦学习的模型参数，$\bar{w}_0$为联邦学习的初始化模型参数。

[0035] 如图 7 所示，实验部分所涉及数据集和训练模型的相关信息。

	模型	数据集	分布情况	学习率	移动设备总数
场景一	逻辑斯蒂回归模型	人工数据集	Non-IID	0.003	8
场景二	卷积神经网络	FEMNIST	Non-IID	0.02	8

[0036] 如图 3 所示，在场景一中，当模型为逻辑斯蒂回归，损失函数为凸函数时，本方法对移除不同设备子集Q后模型参数变化ϵ_t^{-Q}的估计误差随训练轮数的变化关系。它证明了本实施例的理论分析：当损失函数为凸函数时，本方法对模型参数变化的估计误差上界与训练轮数t

有线性关系。

[0037] 如图 4 所示，在场景一中，当模型损失函数为凸函数且当设备数据集分布相同且方差都较小、分布不同但方差都较小、分布不同且方差较大时，联邦夏普利值的估计误差随训练轮数变化的关系。它与图 3 一起证明了设备数据集的分布差异性越大，模型的参数变化越大，进一步使得联邦夏普利值的平均估计误差从 0.004 上升到 0.15。当本实施例将小部分设备数据集替换为方差更大的数据集时，联邦夏普利值的平均估计误差上升到 4.0。这个异常大的误差来源于当移除的设备数量过多时，对于联邦移动设备自己对模型的影响，即ϵ_t^{-Q}，的估计很不准确。

[0038] 为了解决上述问题，本实施例在通过式子$\bar{\phi}_t(k) = E_{Q\subseteq C\setminus c_k}[\epsilon_t^{-Q,*} - \epsilon_t^{-Q-k,*}]$计算每个设备的联邦夏普利值时，忽略当移除的设备子集Q的数量即|Q|很大的情况。改进估计方法后，本方法对联邦夏普利值的估计误差如图 5 所示。

[0039] 为了找到仅仅由本方法估计方法导致的误差，本实施例首先在计算每个设备的联邦夏普利值时考虑所有可能的边际贡献。由图 6 可以看到有着较大数据方差的设备也有着较大的估计误差。然后，本实施例将估计方法与 Monte-Carlo 采样相结合来降低时间复杂度。本方法尝试了不同的采样数量，例如$|C|^2, |C|^3$，其中|C|为设备数量，在本实施例中为 8。从图 6 中可以发现与估计方法导致的误差相比，采样带来的误差可以忽略不计。为了解决数据方差大带来估计误差大的问题，本实施例采用之前所述的改进方法并尝试了不同移动设备自己|Q|作为阈值，由图 6 可以看到，平均联邦夏普利值的估计误差从 0.6 降到了 0.2，有较大方差的移动设备的联邦夏普利值估计误差从 2.5 降到 0.3。

[0040] 如图 7 中的 a 和 b 所示，在场景二中，当模型为卷积神经网络，损失函数是非凸的且设备数据集时独立同分布或者非独立同分布时，本方法对设备联邦夏普利值的估计误差随训练轮数的变化。它验证了本实施例的理论分析：损失函数为非凸时，估计误差与训练轮数t有指数关系。

[0041] 如图 8 所示，将联邦夏普利值应用于参与设备选择后的实验效果，本实施例选取有较大、较小联邦夏普利值在模型更新方向上投影值的设备进行联邦学习模型，比较模型性能和表现的变化。实验结果证明选取具有较大夏普利值的设备参与训练能够加快模型收敛、提升最终精度，选取具有较小夏普利值的设备参与训练会损害模型的性能，延长其训练时间。

[0042] 经过具体实际实验，当有 8 个移动设备参与联邦学习，各个移动设备的数据为 FEMNIST(手写数字识别)数据集且非独立同分布，每一轮各个参与模型训练的设备更新 2 次模型，模型的学习率为 0.02 时，能够得到的实验数据是：相比于随机选取移动设备参与模型的训练，选取有较大联邦夏普利值在模型更新方向投影值的设备参与每轮的联邦学习，能够将

模型的最终精度从 0.95 提升至 0.99，模型达到目标精度（0.95）所需要的训练轮数从 30 轮降低至 13 轮。

[0043] 与现有技术相比，本方法通过选取有较大联邦夏普利值在模型更新方向投影值的设备参与每轮的联邦学习，能够提升模型最终精度，实施例中从 0.95 提升至 0.99，降低模型训练至目标精度所需要的训练轮数，实施例中模型训练至目标精度（0.95）所需要的训练轮数从 30 轮降低至 13 轮。

[0044] **上述具体实施可由本领域技术人员在不背离本发明原理和宗旨的前提下以不同的方式对其进行局部调整，本发明的保护范围以权利要求书为准且不由上述具体实施所限，在其范围内的各个实现方案均受本发明之约束。**

说 明 书 附 图

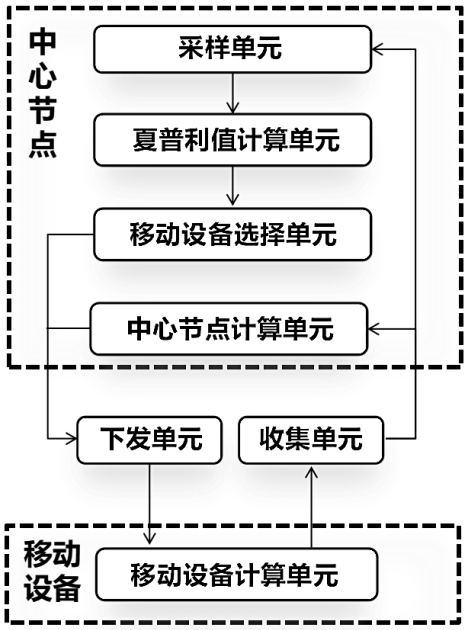


图 1

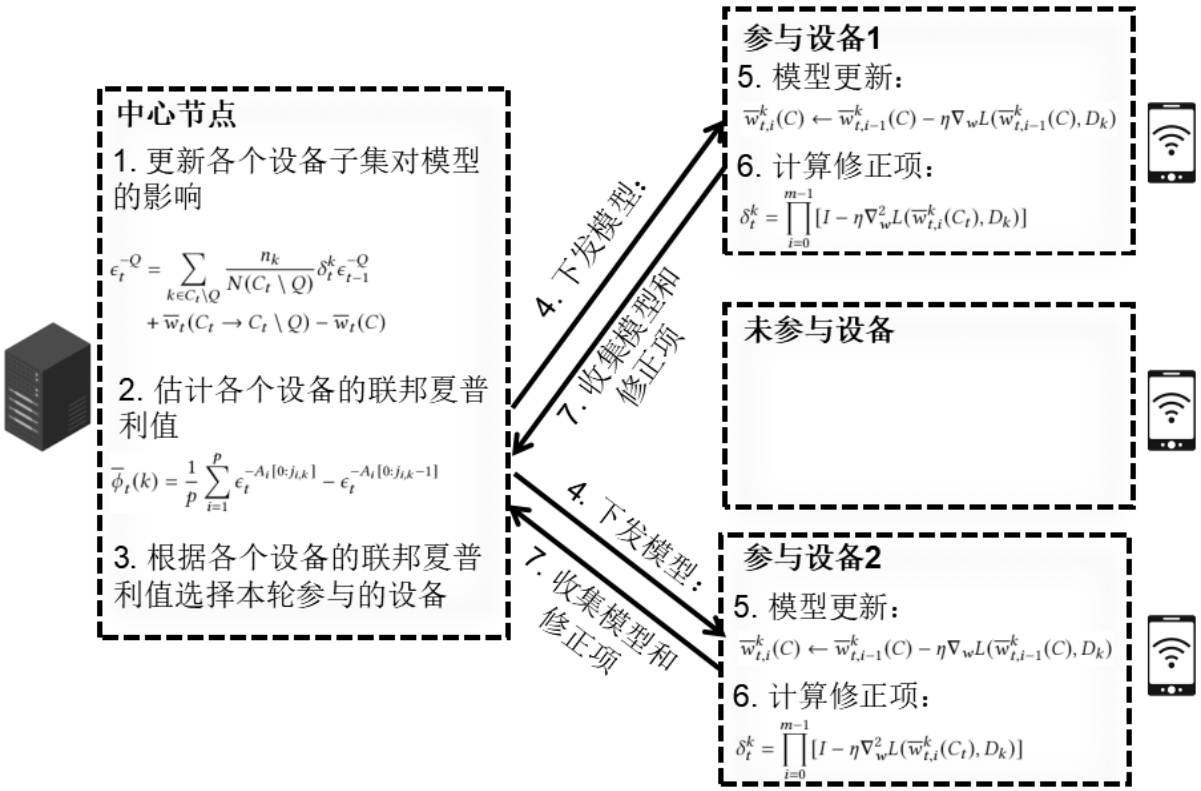


图 2

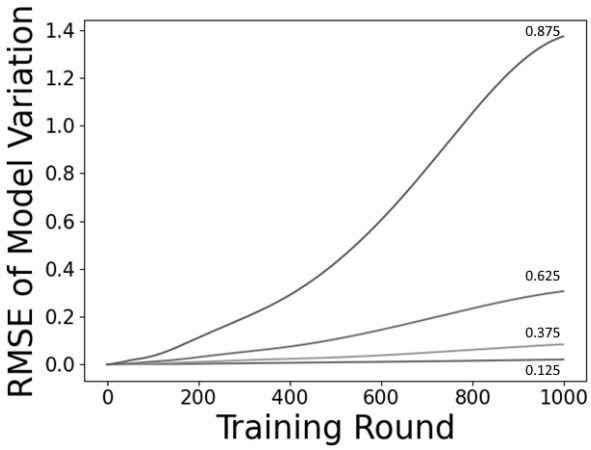
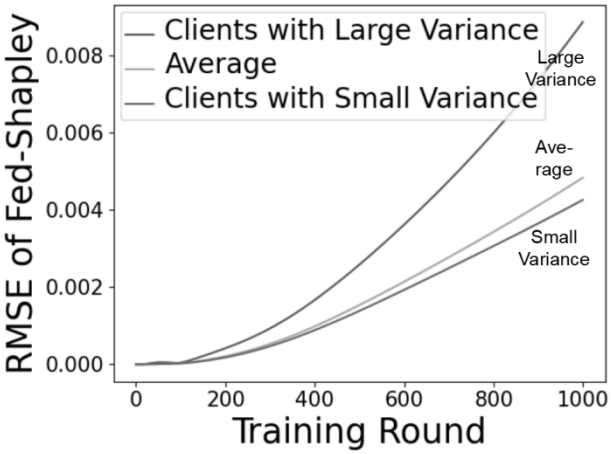
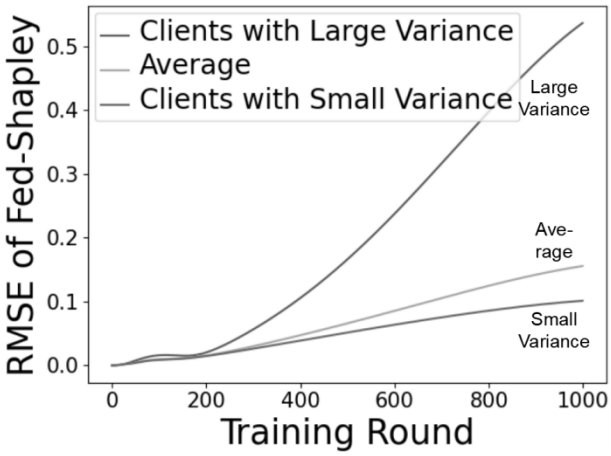


图 3





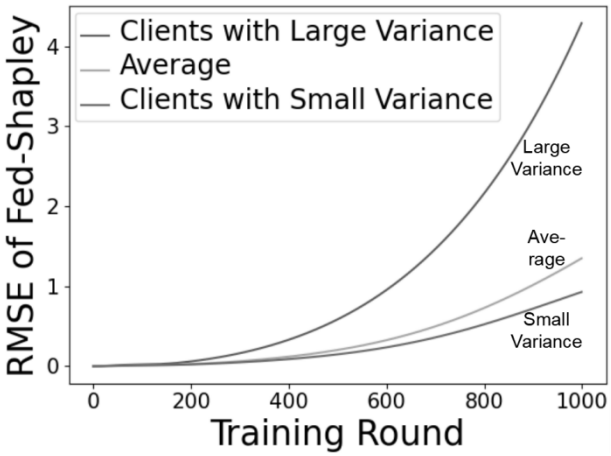


图 4

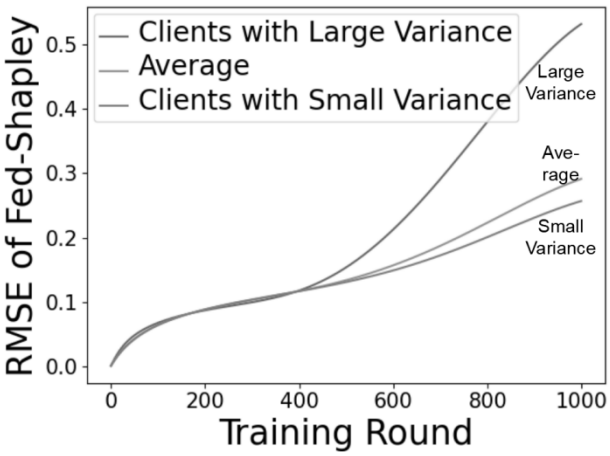
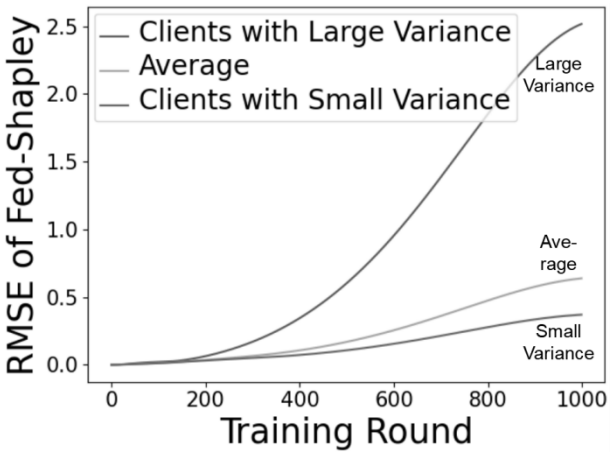


图 5



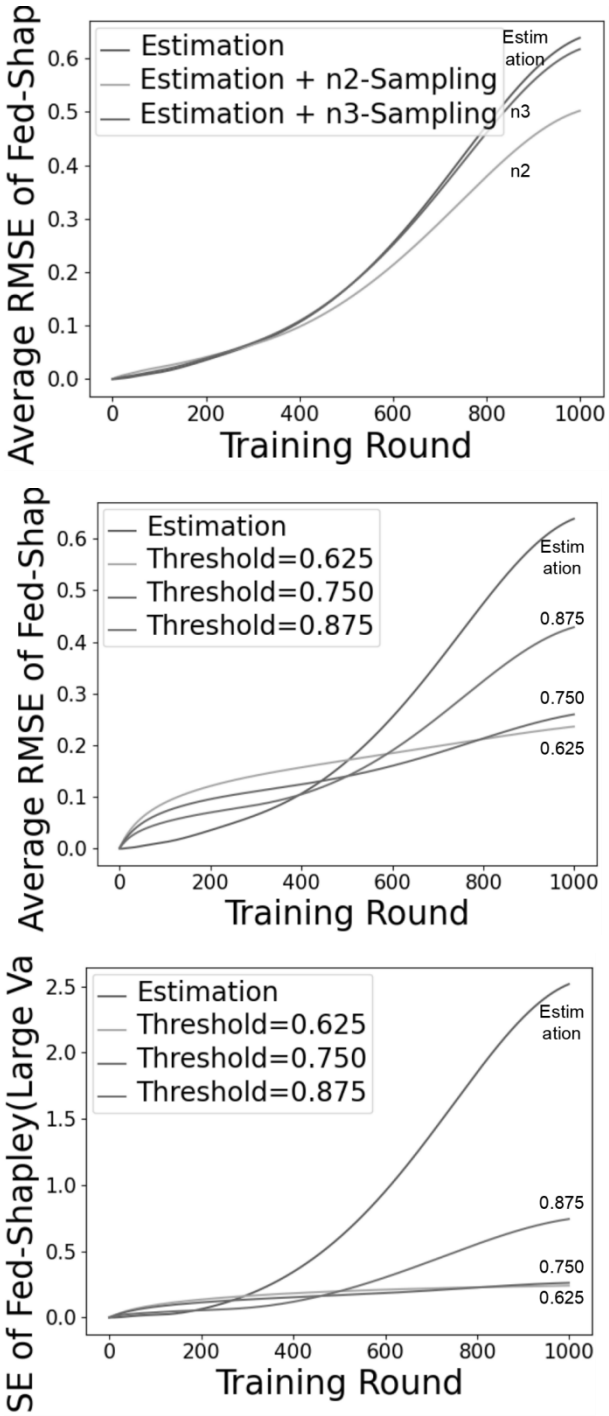


图 6

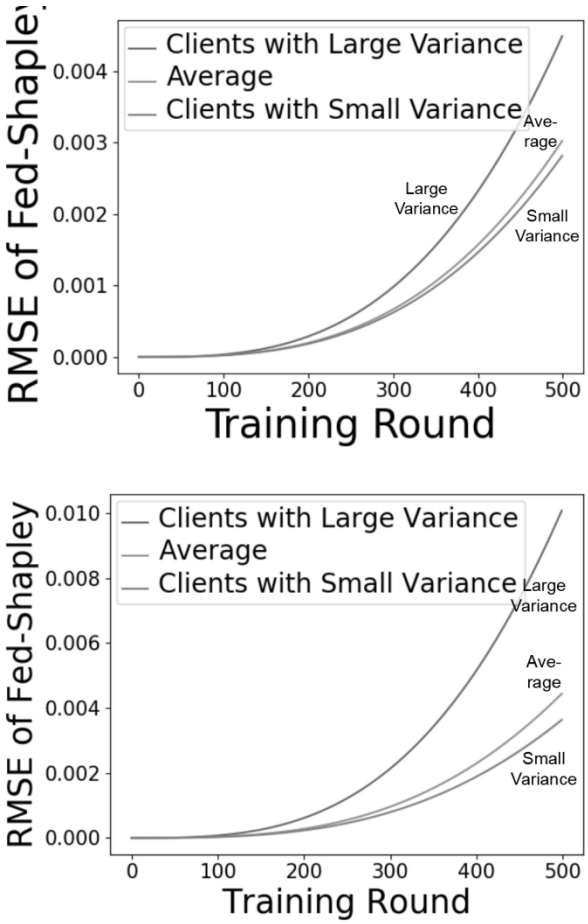


图 7

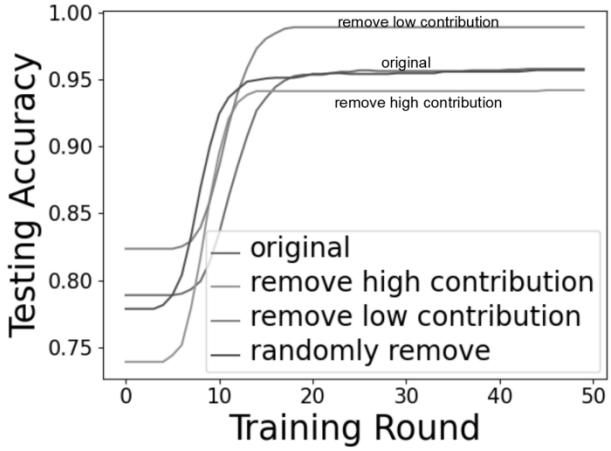


图 8

权 利 要 求 书

1、一种基于夏普利值的联邦学习移动设备分布数据处理方法，其特征在于，将多个移动设备构建联邦学习集群，在联邦学习的每一轮中，中心节点应用 Monte-Carlo 采样方法估计各个联邦学习移动设备当前的联邦夏普利值，并将其在全局模型参数相对于初始参数的变化方向上的投影作为其对模型的重要性与贡献度，并基于联邦夏普利值选择联邦学习移动设备参与本轮的模型训练能够有效加快模型收敛速度，提升模型最终的精度。

2、根据权利要求 1 所述的基于夏普利值的联邦学习移动设备分布数据处理方法，其特征是，所述的夏普利值为：$\bar{\phi}_t(k)=\sum_{S\subseteq C\setminus\{k\}}\frac{\bar{w}_t(S\cup\{k\})-\bar{w}_t(S)}{|C|\times\binom{|C|-1}{|S|}}=E_{S\subseteq C\setminus\{k\}}[\bar{w}_t(S\cup\{k\})-\bar{w}_t(S)]$，其中：$\bar{\phi}_t(k)$为联邦学习移动设备 k 在第t轮的联邦夏普利值；C为所有联邦学习移动设备的集合；S为移动设备子集；$\bar{w}_t(S)$为只有移动设备子集S参与到联邦学习训练过程时，全局模型在第t轮的参数，其值需要通过重新训练模型得到。

3、根据权利要求 1 所述的基于夏普利值的联邦学习移动设备分布数据处理方法，其特征是，所述的联邦夏普利值，通过以下方式估计得到：$\bar{\phi}_t(k)=\sum_{S\subseteq C\setminus\{k\}}\frac{\bar{w}_t(S\cup\{k\})-\bar{w}_t(S)}{|C|\times\binom{|C|-1}{|S|}}=\sum_{Q\subseteq C\setminus\{k\}}\frac{[\bar{w}_t(C\setminus Q)-\bar{w}_t(C)]-[\bar{w}_t(C\setminus\{Q,k\})-\bar{w}_t(C)]}{|C|\times\binom{|C|-1}{|Q|}}=\sum_{Q\subseteq C\setminus\{k\}}\frac{\epsilon_t^{-Q,*}-\epsilon_t^{-Q-k,*}}{|C|\times\binom{|C|-1}{|Q|}}$，其中：$\bar{\phi}_t(k)$为联邦学习移动设备k在第t轮的联邦夏普利值；C为所有联邦学习移动设备的集合；S 和 Q表示联邦学习移动设备子集；$\bar{w}_t(S)$为只有联邦学习移动设备子集S参与到联邦学习训练过程时，全局模型在第t轮的参数；$\epsilon_t^{-Q,*}$表示在训练过程中从总联邦学习移动设备集合C移除设备子集Q后，模型在第t轮的参数变化。其值可以通过本发明的估计方法得到：$\epsilon_t^{-Q,*}\approx\epsilon_t^{-Q}=\sum_{k\in C_t\setminus Q}\frac{n_k}{N(C_t\setminus Q)}\prod_{i=0}^{m-1}[I-\eta\nabla_w^2 L(\bar{w}_{t,i}^k(C_t),D_k)]\,\epsilon_{t-1}^{-Q}+\bar{w}_t(\mathrm{C_t}\to\mathrm{C_t}\setminus\mathrm{Q})-\bar{w}_t(C)$，其中：$C_t$为当前参与模型训练的移动设备集合；$\mathrm{n_k}$为第k个联邦学习移动设备的数据集大小；$N(C_t\setminus Q)$为设备子集$\mathrm{C_t}\setminus\mathrm{Q}$的总数据集大小；m为移动设备本地更新模型的次数；I为单位矩阵；η为学习率；$\mathrm{L}(\bar{w}_{t,i}^k(\mathrm{C_t}),\mathrm{D_k})$表示当模型参数为$\bar{w}_{t,i}^k(\mathrm{C_t})$时，模型在设备k的数据集$\mathrm{D_k}$上的损失函数；$\bar{w}_{t,i}^k(C_t)$为第t轮联邦学习过程中移动设备k在本地数据集上更新i次后的模型；$\bar{w}_t(\mathrm{C_t}\to\mathrm{C_t}\setminus\mathrm{Q})$表示只在第t轮将联邦学习移动设备子集Q移除后全局模型的参数。因为联邦夏普利值$\bar{\phi}_t(k)$的计算需要遍历移动设备集合C的每一个子集，用 Monte-Carlo 采样方法来估计可以得到时间复杂度更低的估计方法。

4、根据权利要求 1 所述的基于夏普利值的联邦学习移动设备分布数据处理方法，其特征

是，所述的 Monte-Carlo 采样是指：随机选取包含所有联邦学习移动的多个排列，按照顺序计算每一个排列当中每个联邦学习移动对排列中位于其之前的移动设备集合的边际贡献。最后对每个联邦学习移动设备的边际贡献求取平均值即为每个设备的重要性，即移动设备选择的标准。

5、根据权利要求 1 所述的基于夏普利值的联邦学习移动设备分布数据处理方法，其特征是，所述的边际贡献是指：将此联邦学习移动设备加入训练后全局模型参数的变化。

6、根据权利要求 1 所述的基于夏普利值的联邦学习移动设备分布数据处理方法，其特征是，所述的联邦学习移动设备选择算法，基于博弈论的经典概念夏普利值(Shapley Value)，具有与之类似的三条公平性定理：当设备k的数据集对于模型性能没有影响，则其价值为 0；当对于两个设备$\mathrm{k}_1,\mathrm{k}_2$，将其数据集分别添加到任意子集$\mathrm{S}\subseteq \mathrm{C}\setminus \mathrm{k}_1,\mathrm{k}_2$后模型性能相同，则$\mathrm{k}_1$和$\mathrm{k}_2$具有相同的价值；任意多种评估方法得到的数据集价值等于这些评估方法结合在一起得到的数据集价值。

7、根据权利要求 1 所述的基于夏普利值的联邦学习移动设备分布数据处理方法，其特征是，所述的模型训练，具体包括：1)中心节点下发全局模型给被选中的联邦学习移动设备；2)联邦学习移动设备根据本地数据样本更新模型，并将更新后的模型参数上传给中心节点；3)中心节点聚合各个联邦学习移动设备上传的模型参数为新一轮的全局模型。

8、根据权利要求 1~7 中任一所述的基于夏普利值的联邦学习移动设备分布数据处理方法，其特征是，具体包括：

步骤 1、在联邦学习过程的开始阶段，中心节点应用 Monte-Carlo 采样方法选取 p 个包含所有联邦学习移动设备的排列$A_i, i=0,1,\ldots,p-1$，对于每个排列里的每个移动设备$A_i[j]$，中心初始化该设备与其之前设备所组成的设备子集对模型影响的估计，即$\epsilon_t^{-Q}=0, Q=A_i[0{:}j], j=0,1,\ldots,|C|, i=0,..,p$；

步骤 2、在训练过程中的每一轮，参与训练的联邦学习移动设备 k 不仅上传经过本地更新后的模型，而且上传本地多次迭代对应的参数修正项，具体为：$\prod_{i=0}^{m-1}\left[I-\eta\nabla_w^2 L\left(\overline{w}_{t,i}^k(C_t), D_k\right)\right]$，其中：m为移动设备本地更新模型的次数；I为单位矩阵；η为学习率；$\overline{w}_{t,i}^k(C_t)$为第t轮联邦学习过程中移动设备k在本地数据集上更新i次后的模型；$\nabla_w^2 L\left(\overline{w}_{t,i}^k(C_t), D_k\right)$为模型$\overline{w}_{t,i}^k(C_t)$在数据集$D_k$上损失函数的二阶导数；

步骤 3、中心节点依据各个设备上传的修正项更新本地的设备子集对模型影响的估计，更

新公式为 $\epsilon_t^{-Q} = \sum_{k \subseteq C_t \setminus Q} \frac{n_k}{N(C_t \setminus Q)} \prod_{i=0}^{m-1} \left[I - \eta \nabla_w^2 L\left(\bar{w}_{t,i}^k (C_t), D_k \right) \right] \epsilon_{t-1}^{-Q} + \bar{w}_t \left(\mathrm{C_t} \rightarrow \mathrm{C_t} \setminus \mathrm{Q} \right) - \bar{w}_t(C)$；

步骤 4、对于每个移动设备 k，中心估计其联邦夏普利值，并将其投影到全局模型的变化方向作为标准选择下一轮参与训练的客户端；所述估计方法为，求取p个排列中该设备对于其之前的设备子集Q的边际贡献，其均值为该设备联邦夏普利值的估计值；所述边际贡献为 $\epsilon_t^{-Q} - \epsilon_t^{-Q-k}$，Q为各个排列中位于移动设备k之前的所有移动设备与设备k组成的集合。

9、一种实现权利要求 1~8 中任一所述上述基于夏普利值的联邦学习移动设备分布数据处理方法的系统，其特征在于，包括：采样单元、夏普利值计算单元、移动设备选择单元、下发单元、移动设备计算单元、收集单元和中心节点计算单元，其中：采样单元在联邦学习的开始阶段根据采样得到的多个包含所有设备的全排列，对于每个排列里的每个设备，中心初始化该设备与排列中其之前设备所组成的设备子集对模型影响，得到各个设备子集对模型影响的初始估计结果；夏普利值计算单元在每一轮的联邦学习过程中，根据上一轮采样单元计算得到的各个排列中设备子集的模型影响，计算各个移动设备的边际贡献均值，得到各个移动设备联邦夏普利值的估计值结果；移动设备选择单元根据各个设备的联邦夏普利值，计算其在全局模型参数变化方向上的投影值作为选择标准，得到本轮参与模型训练的移动设备集合；下发单元根据选择的移动设备集合，下发当前中心节点的模型；移动设备计算单元根据接收到的模型信息，进行本地模型更新和本地修正项的计算，得到更新后的模型参数和本轮对应的修正项；收集单元回传各个参与设备的模型参数和修正项给中心节点；中心节点计算单元根据接收到的更新后的模型参数，进行参数聚合处理，得到新一轮的模型参数；采样单元根据接收到的各个参与设备的修正项，进行各个排列中多个移动设备子集对模型影响的更新。

说 明 书 摘 要

一种基于夏普利值的联邦学习移动设备分布数据处理方法，将多个移动设备构建联邦学习集群，在联邦学习的每一轮中，中心节点应用 Monte-Carlo 采样方法估计各个联邦学习移动设备当前的联邦夏普利值，并将其在全局模型参数相对于初始参数的变化方向上的投影作为其对模型的重要性与贡献度，并基于联邦夏普利值选择联邦学习移动设备参与本轮的模型训练能够有效加快模型收敛速度，提升模型最终的精度。本发明能够衡量各个移动终端的数据集对模型训练过程的影响，从而在每轮选择高贡献度的设备参与训练，减少数据通信开销，加快收敛速度，提升模型表现。

摘 要 附 图