**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**

1. 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**

1. 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。
2. 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。
3. 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。
4. 本实例设计了联邦学习场景下基于夏普利值的移动设备选择算法，相比于原本的随机选取算法，本实施例能够通过对每轮参与训练的移动设备进行选择，达到加快模型收敛速度、提升最终精度的目的。
5. 同时，经过对现有技术的检索发现，中国专利文献号CN112418342A公开日20210226，公开了一种联邦学习场景下的移动设备算力预测方法和装置，方法包括收集移动设备上的数据信息；将位置信息进行聚类，得到移动设备的热点位置；通过时间信息记录移动设备在热点位置上的停留时间；计算移动设备不同日期下在热点位置的平均网络状态和平均资源状态；将预处理后的数据作为训练数据，输入到循环神经网络模型进行预测，得到预置时间段后移动设备的网络信息和资源状态信息并输出。但该现有技术与本发明相比，其无法解决的技术问题包括（1）移动设备的算力资源和模型表现无直接关联，仅凭借算力选择移动设备，虽然能够减少模型训练的时间，但无法达到提高模型最终精度的目的；（2）没有考虑移动设备的数据特点和当前中心节点的模型，无法从理论上加快模型收敛、提升模型精度。

**发明内容**

1. 本发明针对现有技术存在的上述不足，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。
2. 本发明是通过以下技术方案实现的：
3. 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。
4. 所述的模型训练是指（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。
5. 所述的夏普利值为：，其中：为联邦学习移动设备k在第轮的联邦夏普利值；为所有联邦学习移动设备的集合；为移动设备子集；为只有移动设备子集参与到联邦学习训练过程时，全局模型在第轮的参数，其值需要通过重新训练模型得到。
6. 所述的联邦夏普利值(Fed-Shapley)，通过以下方式估计得到：，其中：为联邦学习移动设备在第轮的联邦夏普利值；为所有联邦学习移动设备的集合；表示联邦学习移动设备子集；为只有联邦学习移动设备子集参与到联邦学习训练过程时，全局模型在第轮的参数；表示在训练过程中从总联邦学习移动设备集合移除设备子集后，模型在第轮的参数变化。其值可以通过本发明的估计方法得到：，其中：为当前参与模型训练的移动设备集合；为第个联邦学习移动设备的数据集大小；为设备子集的总数据集大小；为移动设备本地更新模型的次数；为单位矩阵；为学习率；表示当模型参数为时，模型在设备的数据集上的损失函数；为第轮联邦学习过程中移动设备在本地数据集上更新次后的模型；表示只在第轮将联邦学习移动设备子集移除后全局模型的参数。因为联邦夏普利值的计算需要遍历移动设备集合的每一个子集，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。
7. 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。
8. 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。
9. 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，将其数据集分别添加到任意子集后模型性能相同，则和具有相同的价值；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。
10. 所述方法，具体包括：
11. 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，对于每个排列里的每个移动设备，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。
12. 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：，其中：为移动设备本地更新模型的次数；为单位矩阵；为学习率；为第轮联邦学习过程中移动设备在本地数据集上更新次后的模型；为模型在数据集上损失函数的二阶导数。
13. 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。
14. 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，求取个排列中该设备对于其之前的设备子集的边际贡献，其均值为该设备联邦夏普利值的估计值。所述边际贡献为，为各个排列中位于移动设备之前的所有移动设备与设备组成的集合。
15. 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，中心节点计算单元。
16. 在联邦学习的开始阶段，采样单元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。
17. 在每一轮的联邦学习过程中，夏普利值计算单元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**

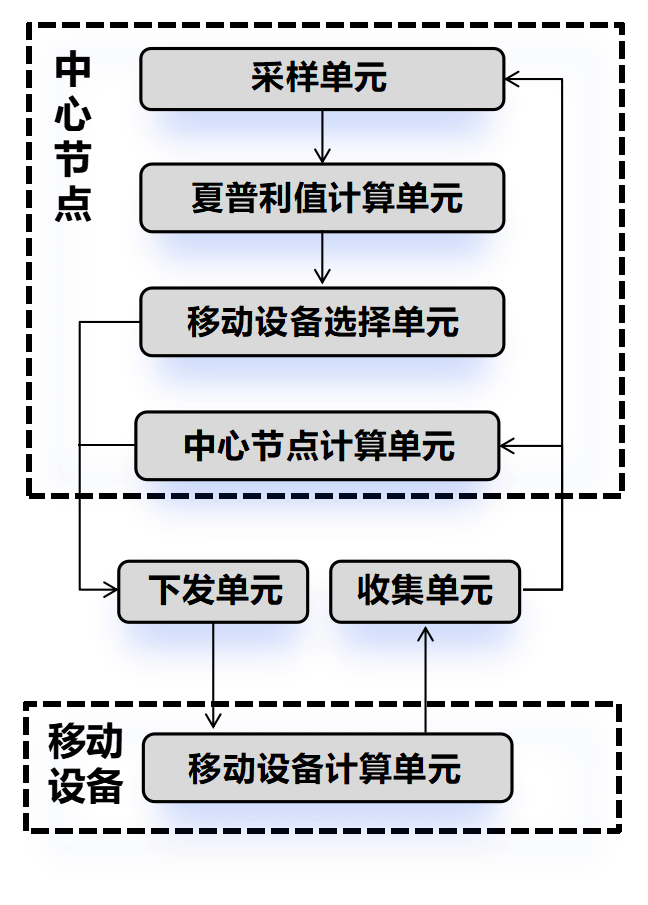
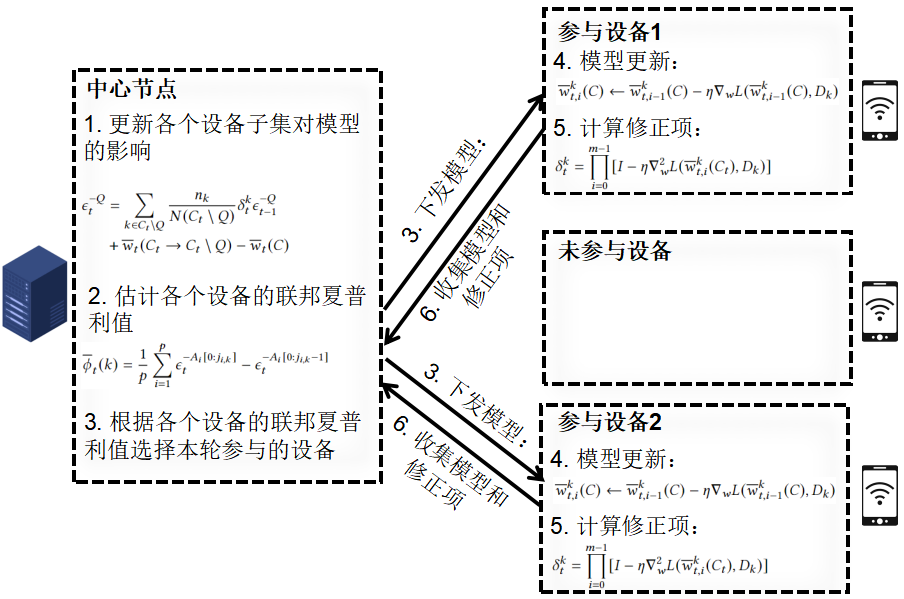
1. 本发明所揭示的从未被公开的技术手段为：（1）联邦学习每一轮训练中基于夏普利值的移动设备选择方法；（2）联邦学习中单个移动设备夏普利值的低复杂度估计方法。
2. 上述技术手段所带来的从未被公开的技术效果是：提升联邦学习中全局模型的最终精度。

**【注1】已经公开的论文、专利申请中已有的技术手段对应的效果并不是“本发明”的技术效果。**

**【注2】从已知的因素范围中通过现有技术手段求出/实验/推理/验算得到最优值一般不认为具有创造性。**

**【注3】现有技术手段/操作/材质/组件/模块的直接替换不具有创造性。**

**附图说明**

1. 图1为本发明流程图；
2. 图2为本发明系统示意图；
3. 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。
4. 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。
5. 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。
6. 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。
7. 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；
8. 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。
9. 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【以下部分需申请人提供能够复现上述技术效果的完整工程应用指导，包括但不限于必要操作过程步骤、结构参数等。其中涉及①已有文献记载的技术手段，建议给出明确的文献出处；②如为本发明独创的新技术(操作或结构)，应当详细说明具体细节并给出相关的实验数据或模拟数据或理论分析结果；③申请提交专利局审查后将不能追加任何技术信息，提交版本中如既没有详细说明也没有明确给出效果分析的操作步骤或结构设计在审查时将被专利局默认为不具有创造性】**
10. 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：
11. 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。对于每个排列里的每个设备，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。
12. 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次后的模型，而且上传本地多次迭代对应的参数修正项。所述修正项为，其中为设备更新模型的次数；为单位矩阵；为学习率；为在移动设备数据上更新次后的模型；为移动设备的数据。
13. 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。更新公式为，其中：单个移动设备；为参与本轮联邦联邦学习的移动设备集合；为设备的数据集规模；为联邦移动设备子集的总数聚集规模；为设备上传的修正项；=为当不考虑设备子集上传的模型参数更新时，中心节点聚合得到的模型参数；=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。
14. 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，求取个排列中该设备对于其之前的设备子集的边际贡献，其均值为该移动设备联邦夏普利值的估计值，即，其中：为设备在当前训练轮的联邦夏普利值；为Monte-Carlo采样得到的排列数目；为第个排列中移动设备的位置；为第个排列中设备和位于其之前的设备组成的移动设备子集。所述投影值为，其中为移动设备的联邦夏普利值，为当前联邦学习的模型参数，为联邦学习的初始化模型参数。
15. 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 |
| 场景一 | 卷积神经网络 | FEMNIST | Non-IID | 0.02 | 8 |

1. 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后模型参数变化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有线性关系。
2. 如图4所示，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，的估计很不准确。
3. 为了解决上述问题，本实施例在通过式子计算每个设备的联邦夏普利值时，忽略当移除的设备子集的数量即很大的情况。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。
4. 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，其中为设备数量，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，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。
5. 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有指数关系。
6. 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。
7. 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，模型收敛所需要的训练轮数从30轮降低至13轮。
8. 与现有技术相比，本方法的性能指标提升在于：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，降低模型收敛所需要的训练轮数，实施例中从30轮降低至13轮。
9. **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。**

**【专利制度基本原则在于“以对创新技术的充分公开换取垄断”，因此申请文件的主要目标在于客观清楚地表达发明人技术方案的具体创新改进点，由专利局本领域长期审查该领域技术的专业人员，就该改进点与现有技术进行客观比较并对存在创新的部分给予授权，如发明人未充分交底、故意隐藏关键技术、实验数据公开不充分或寄希望于审查阶段补充材料将直接导致申请文件无法实现上述目的】**

**说 明 书 附 图**

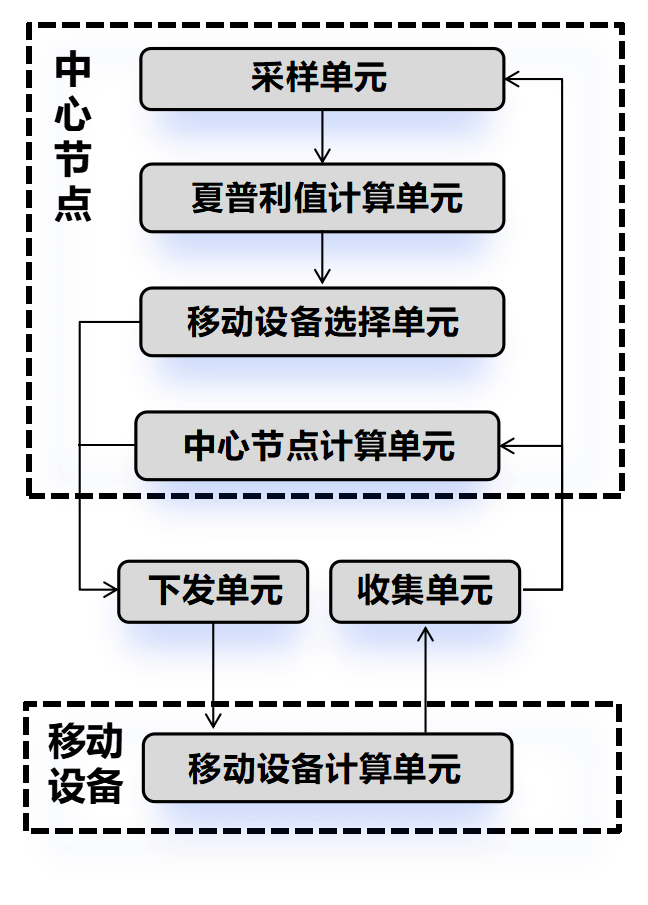


图1

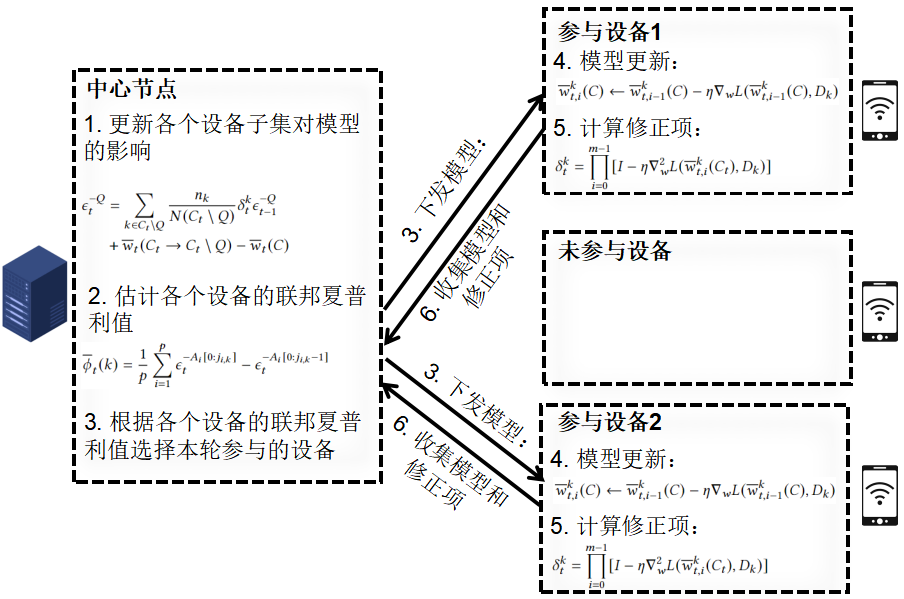


图2

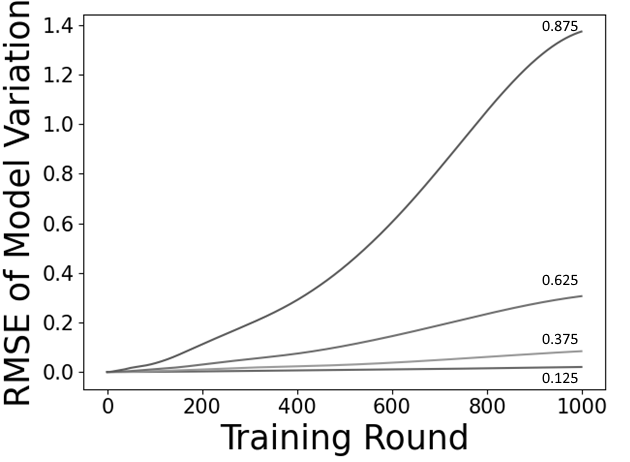
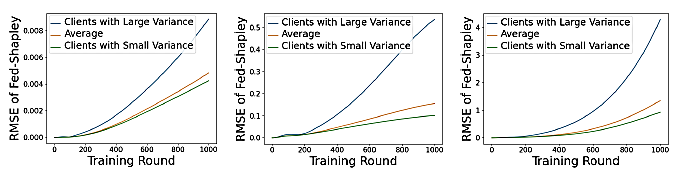
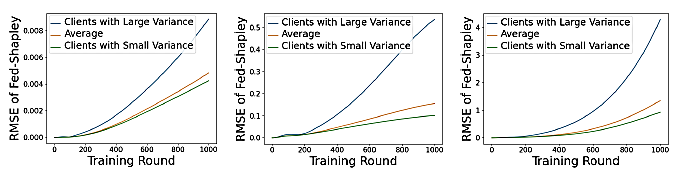
****

图3





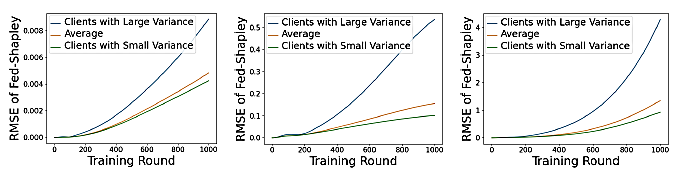


图4

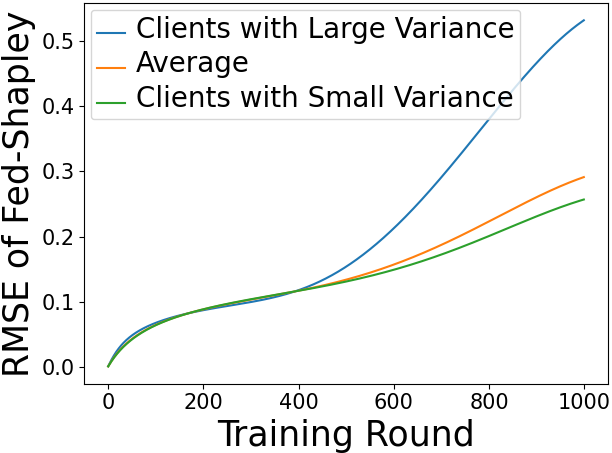
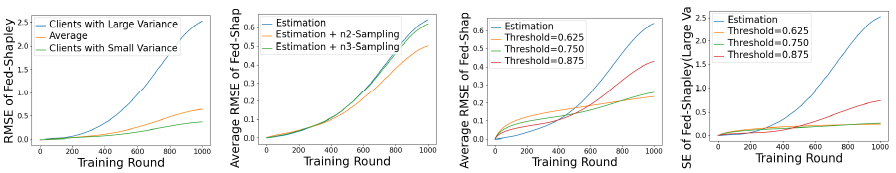
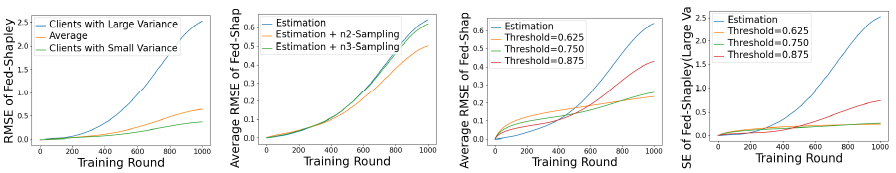
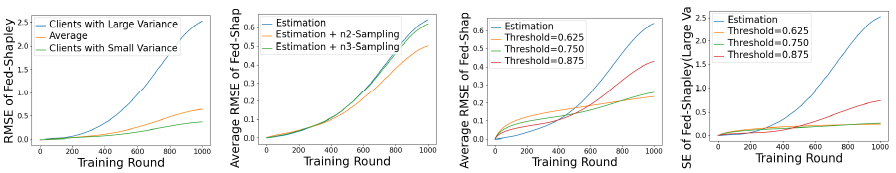


图5







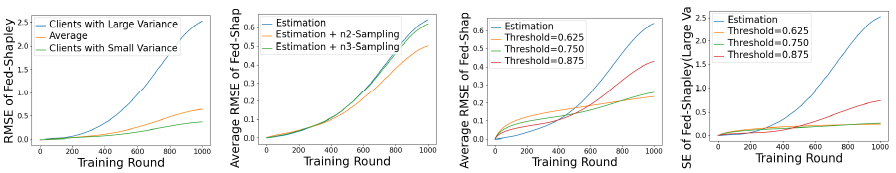
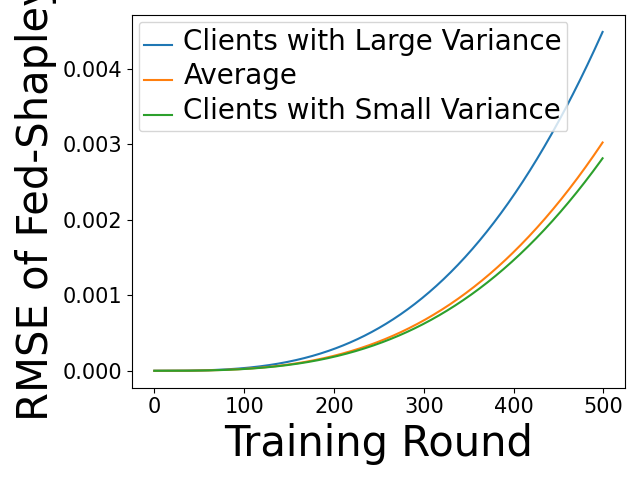
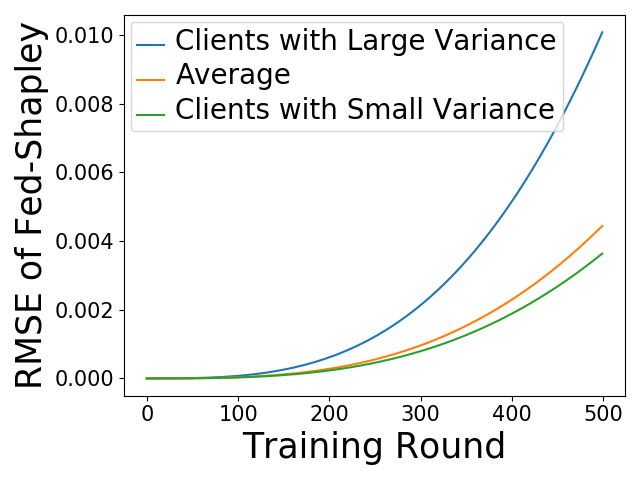


图6





图

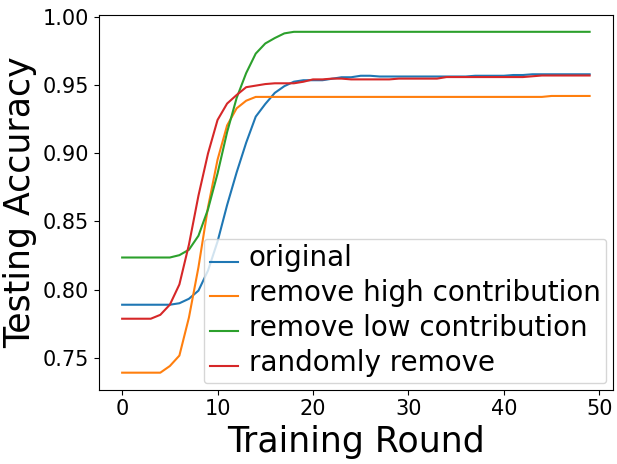


图8

**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，根据联邦学习中不同移动设备对模型的重要性不同，在每一轮的模型训练中，计算各个联邦学习移动设备的联邦夏普利值(Fed-Shapley)在全局模型更新方向上的投影，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客户端参与模型训练能够有效加快模型收敛速度，提升模型最终的收敛效果。

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，具体包括以下步骤：

步骤1、在联邦学习过程的开始阶段，中心应用Monte-Carlo采样方法选取p个包含所有设备的排列。对于每个排列里的每个设备，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。

步骤2、在训练过程中的每一轮，参与训练的设备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。所述修正项为。

步骤3、中心依据各个设备上传的修正项更新本地维护的设备子集对模型影响的估计，更新公式为。

步骤4、对于每个移动设备，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，求取个排列中该设备对于其之前的设备子集的边际贡献，其均值为该设备联邦夏普利值的估计值。所述边际贡献为。