**说 明 书**

**基于夏普利值的联邦学习移动设备选择方法**

**技术领域**

1. 本发明涉及的是一种联邦学习场景下基于数据内在属性的移动终端选择方法，具体是一种基于联邦学习（Federated Learning）和夏普利值（Shapley Value）的移动设备选择方法，在联邦学习过程中本方法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，。

**背景技术**

1. 随着移动网络的不断发展，移动终端实时产生的数据量越来越大，数据之间的关联越来越复杂，人工地管理整个网络变得越来越不可能。将人工智能应用于网络领域能够实现移动设备的快速自动化管理。同时，人工智能模型，例如深度神经网络，已被广泛应用于图像识别、视频分析和目标检测等任务。
2. 虽然人工智能模型解决了人工管理的诸多问题，但是它的良好表现高度依赖庞大的训练数据量。传统的模型训练方法要求一个中心服务器从各个移动终端采集数据，然后集中式地训练模型。这在移动网络领域是不可行的，因为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。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。
3. 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、降低了模型的收敛速度和最终性能。
4. 许多工作证明了不同训练数据对于模型训练的重要程度也是不同的，我们能够通过挑选好的训练数据样本、去除不好的训练数据样本来提升模型的最终表现和加快模型的收敛。同时，已经有一些工作提出了联邦学习场景下基于数据的移动设备选择算法，例如基于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。已有的基于夏普利值的方法将联邦学习的每一轮训练都看作是独立的，以每个移动设备在前面多轮训练中的夏普利值之和（或重要性之和）作为选择的标准和指标。但是，每一轮的模型更新和表现都依赖于上一轮的最终模型结果，二者并非独立的训练过程，所以分开计算其对应的指标并求和当做最终选择的指标是不合理的。

**发明内容**

1. 本发明针对现有技术存在的上述不足，提出一种新的基于夏普利值的联邦学习移动设备选择算法。
2. 本发明定义了每个移动设备的联邦夏普利值（Fed-Shapley），并以其在全局模型更新方向上的投影作为设备选择的标准。所述夏普利值的定义为，为移动设备在第轮的联邦夏普利值；为所有移动设备的集合；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。由于上述选择标准需要重复整个联邦学习过程指数次，本发明提出一个估计方法来简化计算，使得中心在不重复训练的前提下估计每个设备的联邦夏普利值，并具有理论上界。
3. 本发明所述的估计方案为：联邦夏普利值可以表示为，表示在训练过程中从总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：，为第个设备的数据集大小；为设备子集的总数据集大小；为学习率；表示当模型参数为时，模型在数据集上的损失函数；表示只在第轮将设备数据集移除后全局模型的参数。同时，将传统的Monte-Carlo采样方法和本发明的估计方法结合，可以得到时间复杂度更低的估计方法。
4. 所述的Monte-Carlo采样是指：随机选取包含所有设备的多个排列，按照顺序计算每一个排列当中每个移动设备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. 所述边际贡献是指：将此设备加入训练后全局模型参数的变化。
6. 本发明的设备选择方法是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：如果设备的数据集对于模型性能没有影响，则其价值为0；如果对于两个设备，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。同时，为了解决夏普利值高时间复杂度的问题，本发明提出了高效准确的数据价值估计方法，在理论上具有有限误差上界，并在实验中得到验证。
7. 当模型损失函数为凸函数时，理论上本发明对联邦夏普利值的估计误差上界与训练轮数有线性关系；当模型损失函数为非凸函数时理论上本发明对联邦夏普利值的估计误差上界与训练轮数有指数关系。
8. 本发明的估计误差还来源于移动设备数据集的分布差异和方差。对于后者，本发明提出了减小误差的方法：在估计联邦夏普利值时，不考虑当移除的客户子集规模过大的情况。
9. 本发明是通过以下技术方案实现的，本方法包括以下步骤：
10. 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。
11. 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。
12. 步骤3、中心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。
13. 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。

**技术效果**

1. 与现有技术相比，本发明优点包括：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；
2. 本发明提出的高效的联邦夏普利值估计方法具有理论误差上界和较小的实验误差。
3. 本发明提出的客户端选择方法经实验证明能够加快模型的收敛速度，提升模型的最终表现。

**附图说明**

1. 图1为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。
2. 图2为当模型损失函数为凸函数时，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。
3. 图3为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。
4. 图4为应用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。
5. 图5为当模型损失函数为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，其中：a为设备数据集独立同分布时的情况，b为设备数据集不独立同分布时的情况。
6. 图6为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。
7. 图7为所用数据集的说明。

**具体实施方式**

1. 下面对本发明的实施例作详细说明，本实施例在以本发明技术方案为前提下进行实施，给出了详细的实施方式和具体的操作过程，但本发明的保护范围不限于下述的实施例。

**实施例1**

1. 本实施例包括8个移动设备，其相关信息如图7所示，实施步骤如下所示：
2. 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。
3. 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。
4. 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。
5. 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。

**模拟实验结果**

1. 图7展示了实验部分所涉及数据集和训练模型的相关信息。
2. 图1展示了当损失函数为凸函数时，本发明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。它证明了我们的理论分析：当损失函数为凸函数时，本发明对模型参数变化的估计误差上界与训练轮数有线性关系。
3. 图2展示了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1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。当我们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，对于模型变化的估计很不准确。
4. 为了解决上述问题，我们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，本发明对联邦夏普利值的估计误差如图3所示。
5. 为了找到仅仅由本发明估计方法导致的误差，我们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，而非少数个全排列中其边际贡献。由图4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，我们将估计方法与Monte-Carlo采样相结合来降低时间复杂度。本发明尝试了不同的采样数量，例如，其中为设备数量。从图4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，我们采用之前所述的改进方法并尝试了不同，由图4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，有较大方差设备的估计误差从2.5降到0.3。
6. 图5中的a和b展示了当模型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，本发明对设备联邦夏普利值的估计误差随训练轮数的变化。它验证了我们的理论分析：损失函数为非凸时，估计误差与训练轮数有指数关系。
7. 图6展示了将联邦夏普利值应用于参与设备选择后的实验效果，我们选取有有较大、较小联邦夏普利值的设备，并重复联邦学习的训练过程，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。

**说 明 书 附 图**

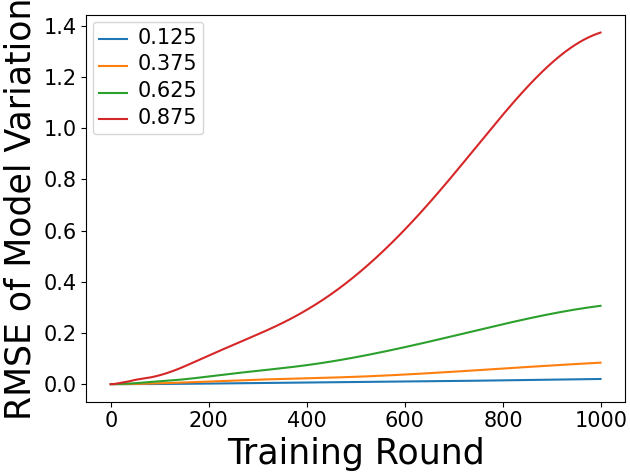


图1

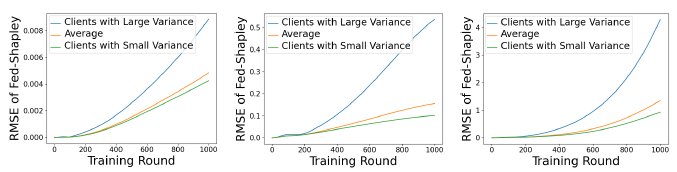


图2

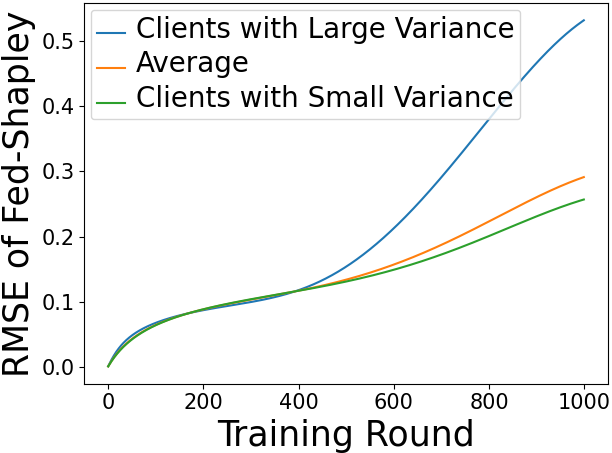


图3

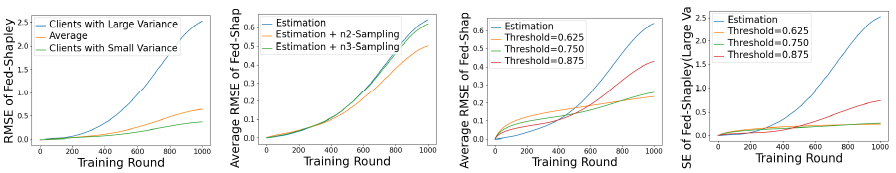
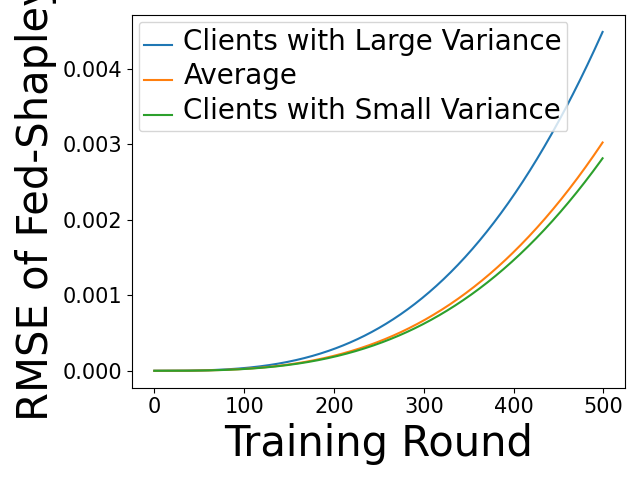
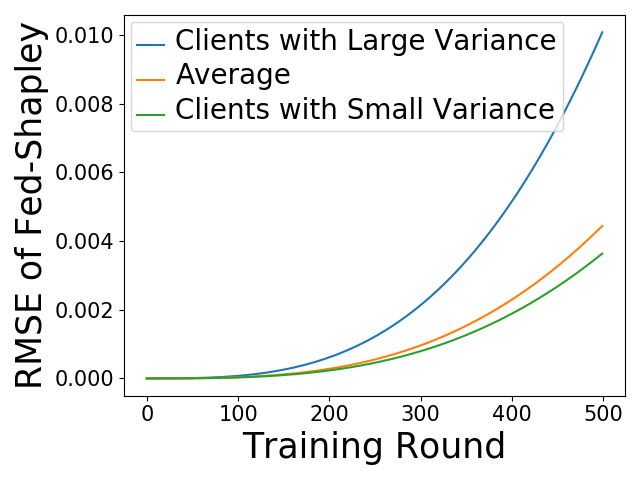


图4



a

图5



b

图5

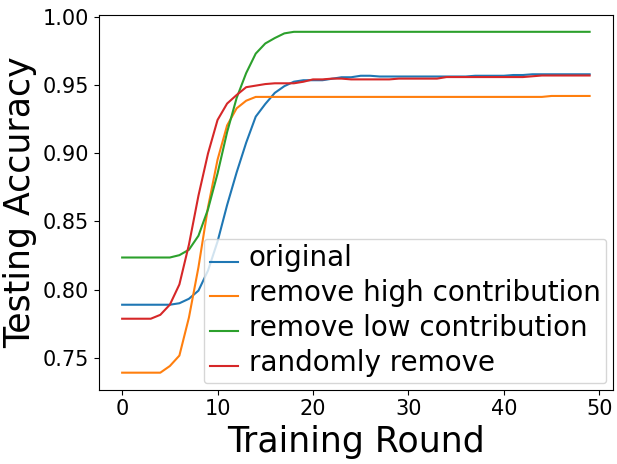


图6

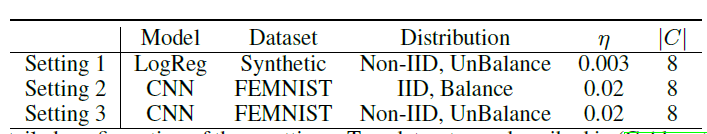


图7

**权 利 要 求 书**

1. 一种联邦学习场景下基于夏普利值的移动设备选择方法，其特征在于，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。

**说 明 书 摘 要**

一种联邦学习场景下基于夏普利值的移动设备选择方法。因为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，本发明基于夏普利值定义了各个联邦学习移动设备对模型的重要性与贡献度，即联邦夏普利值。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。同时，本发明通过数学推导，得到无需重复训练模型的联邦夏普利值的估计方法，将其与Monte-Carlo采样方法相结合能够大幅度下降夏普利值的计算复杂度。经实验证明，本发明的估计方法有着较小、可容忍的误差，且依据所定义的联邦夏普利值来选择客户端能够提升最终模型精度、缩短训练时间。

**摘 要 附 图**

