冗余数据去除的联邦学习高效通信方法

李开菊[1,2]，许强[3]，王豪[1,4]

（1. 重庆邮电大学计算机科学与技术学院，重庆 400065；2. 重庆大学计算机学院，重庆 400044；
3. 香港城市大学电机工程系，香港 999077；4. 旅游多源数据感知与决策技术文化和旅游部重点实验室，重庆 400065）

摘 要：为了应对终端设备网络带宽受限对联邦学习通信效率的影响，高效地传输本地模型更新以完成模型聚合，提出了一种冗余数据去除的联邦学习高效通信方法。该方法通过分析冗余更新参数产生的本质原因，根据联邦学习中数据非独立同分布特性和模型分布式训练特点，给出新的核心数据集敏感度和损失函数容忍度定义，提出联邦核心数据集构建算法。此外，为了适配所提取的核心数据，设计了分布式自适应模型演化机制，在每次训练迭代前动态调整训练模型的结构和大小，在减少终端与云服务器通信比特数传输的同时，保证了训练模型的准确率。仿真实验表明，与目前最优的方法相比，所提方法减少了 17%的通信比特数，且只有 0.5%的模型准确率降低。

关键词：联邦学习；通信效率；核心数据；模型演化；准确率

中图分类号：TP391

文献标志码：A

DOI: 10.11959/j.issn.1000−436x.2023072

Communication-efficient federated learning method via redundant data elimination

LI Kaiju[1,2], XU Qiang[3], WANG Hao[1,4]

1. School of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China
2. College of Computer Science, Chongqing University, Chongqing 400044, China
3. Department of Electrical Engineering, City University of Hong Kong, Hong Kong 999077, China
4. Key Laboratory of Tourism Multisource Data Perception and Decision, Ministry of Culture and Tourism, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

Abstract: To address the influence of limited network bandwidth of edge devices on the communication efficiency of federated learning, and efficiently transmit local model update to complete model aggregation, a communication-efficient federated learning method via redundant data elimination was proposed. The essential reasons for generation of redundant update parameters and according to non-IID properties and model distributed training features of FL were analyzed, a novel sensitivity and loss function tolerance definitions for coreset was given, and a novel federated coreset construction algorithm was proposed. Furthermore, to fit the extracted coreset, a novel distributed adaptive sparse network model evolution mechanism was designed to dynamically adjust the structure and the training model size before each global training iteration, which reduced the number of communication bits between edge devices and the server while also guarantees the training model accuracy. Experimental results show that the proposed method achieves 17% reduction in communication bits transmission while only 0.5% degradation in model accuracy compared with state-of-the-art method.

Keywords: federated learning, communication efficiency, coreset, model evolution, accuracy

收稿日期：2022−10−16；**修回日期：**2023−02−04

通信作者：王豪，haowang@cqupt.edu.cn

基金项目：国家自然科学基金资助项目（No.42001398）；重庆市自然科学基金资助项目（No.cstc2020jcyj-msxmX0635）；重庆市博士后研究项目特别资助项目（No.2021XM3009）；中国博士后基金资助项目（No.2021M693929）

Foundation Items: The National Natural Science Foundation of China (No.42001398), The Natural Science Foundation of Chongqing (No.cstc2020jcyj-msxmX0635), Chongqing Postdoctoral Research Program Special Funding (No.2021XM3009), China Postdoctoral Foundation (No.2021M693929)

0 引言

随着智能边缘设备的普及和应用，个性化、低时延的人工智能应用需求，如人脸识别、智能驾驶、智能监控等不断涌现。传统的基于云的集中式机器学习（ML, machine learning）[1]算法虽然可以训练更加准确的人工智能模型，但存在高传输时延、高网络带宽压力以及用户隐私泄露等弊端。联邦学习（FL, federated learning）[2]允许多个分布式边缘设备在云服务器的统一协调下，协作完成一个全局模型的训练，而不需要传输自身所采集的原始数据。与直接传输原始数据的集中式 ML 算法相比，FL 选择上传训练后的模型参数，能有效地降低对云端的网络带宽压力，同时保护用户的隐私[3]。

然而，由于联邦学习中边缘设备网络带宽资源受限，通信效率问题一直是制约联邦学习落地实现的一个重要瓶颈[4]。目前，已有不少提高联邦学习通信效率的方法。一类是通过降低总的通信轮数加快模型收敛的方法[5]；另一类是减少单次模型聚合中总通信比特数的方法，如模型的稀疏化、量化等数据压缩技术[6]。传统的基于模型压缩的方法的主要思想是从原始的训练参数中去除一部分冗余的更新，只传输少量的梯度信息来达到减少通信量的目的。模型压缩的方法虽然已被证明能在一定程度上提高联邦学习的通信效率，但并没有从本质上探索冗余更新参数产生的根本原因。

因此，如何从本质上探究冗余更新参数产生的原因，进而提高联邦学习的通信效率是本文的主要研究内容。随着智能设备使用量的急剧增长，设备所产生和采集的原始数据规模也呈现海量增长的趋势。为满足高质量智能应用服务的需求，需要在边缘设备上布置高度复杂化的人工智能模型来完成模型训练，这间接导致在多个分布式设备上产生高维模型更新参数。然而，在联邦学习场景中，边缘设备所采集的原始数据通常具有冗余特性[7-8]，如视频和智能感知数据，仅有小部分数据对模型训练来说是重要的或者有用的。例如，图像数据就包含了大量的冗余数据，尤其是图像中变化不明显的部分[9]。冗余信息只能对模型训练带来极小的帮助，但需要布置更复杂的网络模型来完成训练，这间接导致网络模型参数数量也呈现高维增长的趋势。

本文旨在提出一种新的提高联邦学习通信效率的优化方法。该方法通过探索冗余更新参数产生的本质原因，从数据的角度考虑，从原始数据集中去除一部分冗余数据，并布置一个适配的小型演化模型使训练所需的网络模型更小，在减少终端与云服务器间通信量的同时，保证训练模型的准确率。本文的主要贡献如下。

1) 提出了冗余数据去除的联邦学习高效通信优化框架。该框架探索了冗余更新参数产生的本质原因，并从根本上提高了联邦学习的通信效率，为提高联邦学习通信效率开辟了一个新的视角。与目前基于模型压缩的方法相比，所提方法从原始数据集中去除冗余数据，并部署一个更小的匹配的演化网络模型，间接地减少了每个边缘设备总的传输比特。

2) 提出了一种联邦核心数据集构建算法，以去除原始数据集中的冗余数据。该算法在充分考虑联邦学习的非独立同分布（non-IID, non-independently identically distribution）特性的基础上，重新定义了核心数据集敏感度和损失函数容忍度公式，扩展了现有集中式或基于独立同分布（IID, independently identically distribution）的核心数据集构建算法在联邦场景中的应用。

3) 提出了一种分布式自适应模型演化机制。该机制考虑初始化稀疏的网络模型、本地模型和聚合模型的自适应演化，定义网络模型连接重要性以及重要性评估机制，在每次训练迭代前动态调整了训练模型的结构和大小，在降低边缘设备模型复杂度的同时，保证了训练模型的准确率。

4) 理论上证明了所提方法的收敛性，且在实验中验证了所提方法的有效性。仿真实验表明，与目前最优的方法相比，所提方法减少了 17%的通信比特传输数目，且只有 0.5%的模型准确率降低。

1 相关工作

与本文密切相关的工作主要包括模型的稀疏化和模型参数的量化减少 2 个方面，下面分别对这 2 个方面的相关工作进行阐述。

模型的稀疏化主要是从原始更新向量中选择一部分更新参数上传至云服务器，来减少每轮迭代终端与云端的通信比特数。文献[10-12]主要基于评估局部更新对全局模型的贡献度，选择一部分重要的[11]或者相关的[12]本地更新参与全局模型的聚合。文献[4, 13-14]研究联合减少上行和下行通信量的优化方法。其中，文献[4]提出稀疏三元

压缩（STC, sparse ternary compression）框架，扩展了现有的 top-k 梯度稀疏化压缩技术，实现了下游压缩以及权重更新的三元化和最优 Golomb 编码；文献[13]提出联合训练的三元量化（FTTQ, federated trained ternary quantization）算法，通过自我学习的量化因子优化客户端的量化网络；文献[14]提出通用梯度稀疏化（GGS, general gradient sparsification）框架，设计梯度修正和本地梯度更新批归一化层 2 个机制。文献[15-17]考虑通信与其他因素的平衡，包括梯度稀疏程度控制的最佳通信与计算[15]、测试精度与稀疏编码开销[16]，以及通信效率与隐私保护[17]之间的均衡。

模型参数的量化减少是通过将原始更新参数限制在一个缩小的数值集上。文献[18-20]研究有精度损失的模型量化方法。其中，文献[18]提出 signSGD 的量化方法，该方法把更新参数的每个梯度值量化为二进制符号；文献[19]联合考虑周期性平均、部分设备参与以及量化消息传递 3 个关键特征，提出一种具有周期性平均和量化的通信优化方法；文献[20]联合量化模型训练过程中的局部更新和全局更新。文献[21-22]研究通信与精度均衡的模型量化方法。其中，文献[21]动态调整通信和精度之间的平衡，提出增强的 FFL（fast federated learning）方案；文献[22]提出 AdaQuantFL 的自适应量化策略，通过在训练过程中自适应地改变模型量化的水平来实现通信效率和模型误差之间的均衡。文献[23-24]研究其他方法来实现模型参数的量化。其中，文献[23]将随机梯度分解为规范梯度和归一化块梯度，提出分层梯度量化框架；文献[24]提出由量化指标模块、量化策略模块和量化优化模块组成的自动梯度量化方法。

无论是模型的稀疏化还是模型参数的量化方法，它们都只是从模型更新参数的角度，通过从原始更新向量中选择一部分子更新梯度或者是量化的更新上传至云服务器，来减少冗余更新参数的传输，从而达到减少通信量的目的。这些方法虽然已被证明能在一定程度上提高联邦学习的通信效率，但并没有探索冗余更新参数产生的根本原因。

此外，文献[25]针对 k-center 和 k-median 聚类问题提出了基于最远点算法的核心数据集构建方法。该方法最初是针对中心式环境的最小闭包球（MEB, minimum enclosing ball）问题提出的，其主要思想是通过迭代地在原始数据集中选择离当前中心足够远或者最远的点添加至核心数据集，直至核心数据集包含了给定范围内的所有数据点为止。文献[26]提出了一种基于随机采样的核心数据集构造算法，其主要思想是从原始数据集中随机采样构建一个核心集。这类方法虽然在一定程度上提高了核心数据集的构建效率，但通常需要一个大的核心集来实现与原始数据集的良好近似。Lu 等[27]提出了一种支持各种 ML 问题的鲁棒性核心数据集构建算法，该算法可以支持各种机器学习问题。

虽然上述方法在实践中被证明有效，但这些方法要么只考虑了集中式环境下的核心数据集构造，要么只考虑了典型的满足数据 IID 的分布式场景的数据集构造，而这与典型的联邦学习 non-IID 去中心化场景有着本质区别。因此，不能直接将现有的基于中心式或者传统分布式的核心数据集构建算法直接应用于本文的联邦学习场景中，需要根据联邦学习数据的 non-IID 特性，设计新的核心数据集构建算法。

2　冗余数据去除的高效通信方法

2.1　问题定义

表 1 总结了本文所用到的符号和对应的含义。为了提高联邦学习的通信效率，本文将联邦学习的整个优化过程表示为一个双目标优化问题。第一个优化目标 P_1 是减少终端设备与云服务器之间的总传输比特数，主要包括上行和下行传输比特数。具体地，定义 b_t 为所有设备在第 t 轮迭代上传至云服务器的总传输比特，b_t' 为第 t 轮迭代服务器传输至终端设备的下行传输比特数。那么，整个模型训练过程的总传输比特数可定义为每轮迭代传输比特数的累加。假设全局模型经过 T 轮迭代后收敛，记 B_T 为累计通信比特数，则有

$$B_T = \sum_{t=1}^{T}[b_t + b_t'] \tag{1}$$

那么，第一个优化目标 P_1 为

$$P_1 = \text{minimize} \quad B_T \tag{2}$$

由于通信比特的减少不应该以牺牲模型的准确率为代价，因此，本文的第二个优化目标 P_2 是保证训练模型的准确率。记 A_T 为经过 T 轮迭代后全局模型的收敛准确率，则有

$$P_2 = \text{maximize} \quad A_T \tag{3}$$

表 1　　符号和对应的含义

符号	含义
$F(\boldsymbol{\omega})$	全局加权平均损失函数
$F_i(\boldsymbol{\omega})$	设备 N_i 第 t 轮迭代的本地损失函数
$\nabla F_i(\boldsymbol{\omega}_t)$	设备 N_i 第 t 轮迭代的梯度值
η_i	设备 N_i 的学习率
$\boldsymbol{\upsilon}_{i,t}$	设备 N_i 第 t 轮迭代的本地模型更新
$\boldsymbol{\omega}_t$	第 t 轮迭代的全局模型参数
$\boldsymbol{\omega}_T$	第 T 轮迭代的全局模型参数
D_i	设备的本地数据集
D	全体样本空间
N	终端设备数目
ε	损失函数容忍度
Γ	原始数据集 X 的核心数据集
A_T	全局模型的收敛准确率
B_T	累计通信比特数

2.2　模型框架

为了实现式(3)中的目标，本文从数据冗余的角度，提出了冗余数据去除的联邦学习高效通信方法。如图 1 所示，所提方法的总体流程主要包括 4 个步骤，以第 t 轮迭代为例进行如下说明。

1) 核心数据集构建。每个设备 $\mathcal{N}_i$ 从其原始数据集 $\mathcal{D}_i$ 中去除一部分冗余数据，得到核心数据集 $\mathcal{C}_i$。注意，虽然 $\mathcal{C}_i$ 的规模比 $\mathcal{D}_i$ 要小很多，但 $\mathcal{C}_i$ 具有与 $\mathcal{D}_i$ 相同的样本空间。

2) 本地模型训练。每个设备 $\mathcal{N}_i$ 根据其核心数据集 $\mathcal{C}_i$ 进行本地模型训练，得到其本地模型更新 $\upsilon_{i,t}$。

3) 模型演化。每个设备 $\mathcal{N}_i$ 根据第 t 轮迭代的模型剪枝率 γ_t 对其本地模型进行稀疏化，然后上传稀疏化后的本地模型 $\hat{\upsilon}_{i,t}$ 至云服务器。云服务器在接收到稀疏化后的本地模型之后，进行全局模型聚合，并得到更新的全局模型 $\boldsymbol{\omega}_{t+1}$。此外，为了适配所有用户的核心数据和减少下行的通信比特数，所提方法在云服务器端对更新的全局模型进行二次剪枝。

4) 模型下发。云服务器将剪枝之后的全局模型 $\hat{\boldsymbol{\omega}}_{t+1}$ 下发给每个设备，模型训练进入第 $t+1$ 轮迭代。

2.3　联邦核心数据集构建

基于敏感度取样的核心数据集构建是目前主流

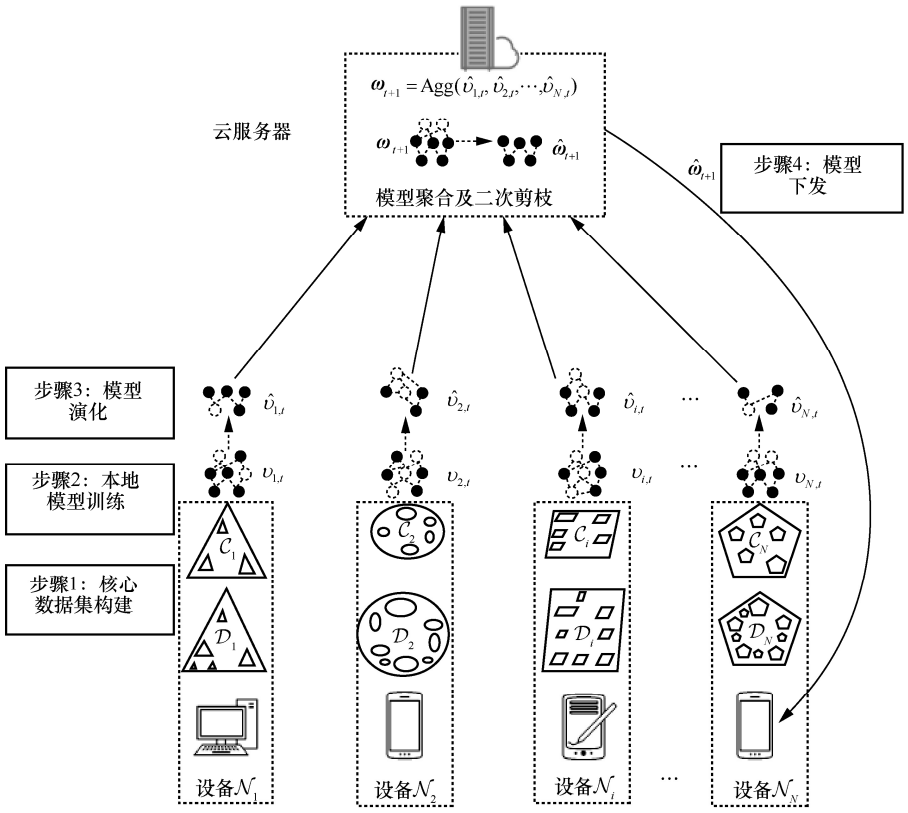


图 1　冗余数据去除的联邦学习高效通信方法

的工作，其主要包括集中式[28]和分布式[29]2 种场景。直接将现有方法应用于联邦学习场景不仅会严重影响核心数据集的提取质量，改变原有数据的分布特点，甚至会严重降低训练模型的准确率。与传统方法相比，所提方法进行了 2 个方面的改进。一方面，基于联邦学习的 non-IID 特性，给出了新的核心数据集损失函数容忍度 ε 的定义。设置核心数据集联合损失函数容忍度 ε，并将 ε 定义为只有一个设备的核心数据集被用于模型训练时对全局模型损失函数的影响；另一方面，定义了一个新的敏感度，考虑不同数据点的不同权重，并将每个数据点的敏感度定义为由该点所产生的损失函数相对于所有数据点的加权平均损失函数的比重。接下来，描述几个与所提方法相关的定义和定理。

定义 1　ε-容忍度。假设可以从设备 $\mathcal{N}_i$ 的原始数据集 $\mathcal{D}_i$ 中去除一部分冗余数据，得到子数据集 $\mathcal{C}_i$ 满足 $|\mathcal{C}_i| \ll |\mathcal{D}_i|$，且使用 $\mathcal{C}_i$ 进行模型训练，对全局模型的影响满足式(4)，则称 $\mathcal{C}_i$ 是 $\mathcal{D}_i$ 的 ε 接近。

$$\begin{aligned}&\left|F(\mathcal{D}_1,\mathcal{D}_i,\cdots,\mathcal{D}_N)-F(\mathcal{D}_1,\mathcal{C}_i,\cdots,\mathcal{D}_N)\right| \leqslant \\ &\varepsilon_i\left|F(\mathcal{D}_1,\mathcal{D}_i,\cdots,\mathcal{D}_N)\right|\end{aligned} \tag{4}$$

其中，$0<\varepsilon_i<1$ 表示设备 $\mathcal{N}_i$ 的全局模型损失函数容忍度，$F(\mathcal{D}_1,\mathcal{D}_i,\cdots,\mathcal{D}_N)$ 表示所有设备使用原始数据集进行模型训练所得到的全局损失函数，$F(\mathcal{D}_1,\mathcal{C}_i,\cdots,\mathcal{D}_N)$ 表示所有用户中仅有用户 $\mathcal{N}_i$ 使用子集 $\mathcal{C}_i$ 进行模型训练所得到的全局损失函数。

定理 1　假设从设备 $\mathcal{N}_i$ 的原始数据集 $\mathcal{D}_i$ 中提取了一个子集 $\mathcal{C}_i$，所有用户的全局模型损失函数的容忍度为 ε，每个用户的模型损失函数的容忍度为 ε_i。根据联邦学习的基本定义和性质，有

$$\left|F(\mathcal{D}_i)-F(\mathcal{C}_i)\right| \leqslant \frac{|\mathcal{D}|}{|\mathcal{D}_i|}\varepsilon_i\left|F(\mathcal{D}_1,\mathcal{D}_i,\cdots,\mathcal{D}_N)\right| \tag{5}$$

当数据满足 IID 时，有 $\frac{|\mathcal{D}|}{|\mathcal{D}_1|}=\frac{|\mathcal{D}|}{|\mathcal{D}_i|}=\cdots=\frac{|\mathcal{D}|}{|\mathcal{D}_N|}=1$ 以及 $\varepsilon_1=\varepsilon_i=\cdots=\varepsilon_N=\frac{\varepsilon}{N}$。当数据满足 non-IID 时，有 $\frac{|\mathcal{D}|}{|\mathcal{D}_1|}=\frac{|\mathcal{D}|}{|\mathcal{D}_i|}\neq\ldots\neq\frac{|\mathcal{D}|}{|\mathcal{D}_N|}$、$\varepsilon_1\neq\varepsilon_i\neq\cdots\neq\varepsilon_N$ 以及 $\varepsilon_i=\frac{|\mathcal{D}|}{|\mathcal{D}_i|}\varepsilon, i=1,2,\cdots,N$。注意，当数据满足 non-IID 时，每个设备的损失函数容忍度为 $\varepsilon_i=\frac{|\mathcal{D}|}{|\mathcal{D}_i|}\varepsilon$。其主要思想如下：如果数据集的大小比较小，那么去除少量数据对全局模型影响较大，因此，设置更大的损失函数容忍度；反之，冗余数据较多，对全局模型的影响较小，故设置更严格的损失函数容忍度。终端设备数据集大小的参数可以通过同态加密等安全技术和云服务器进行交互。

证明　根据联邦学习的性质，有

$$F(\mathcal{D}_1,\mathcal{D}_i,\cdots,\mathcal{D}_N)=\sum_{i=1}^{N}\frac{|\mathcal{D}_i|}{|\mathcal{D}|}F(\mathcal{D}_i) \tag{6}$$

$$F(\mathcal{D}_1,\mathcal{C}_i,\cdots,\mathcal{D}_N)=\sum_{i=1}^{N^{-i}}\frac{|\mathcal{D}_i|}{|\mathcal{D}|}F(D_i)+\frac{|\mathcal{D}_i|}{|\mathcal{D}|}F(\mathcal{C}_i) \tag{7}$$

其中，N^{-i} 表示除去设备 $\mathcal{N}_i$。

基于式(6)和式(7)，定义 1 中的式(4)可修改为

$$\left|F(\mathcal{D}_i)-F(\mathcal{C}_i)\right| \leqslant \frac{|\mathcal{D}|}{|\mathcal{D}_i|}\varepsilon_i\left|F(\mathcal{D}_1,\mathcal{D}_i,\cdots,\mathcal{D}_N)\right| \tag{8}$$

当数据满足 IID 时，式(7)可修改为

$$\left|F(\mathcal{D}_i)-F(\mathcal{C}_i)\right| \leqslant \frac{\varepsilon}{N}\left|F(\mathcal{D}_1,\mathcal{D}_i,\cdots,\mathcal{D}_N)\right| \tag{9}$$

损失累加后，表示为

$$\left|\sum_{i=1}^{N}F(\mathcal{D}_i)-\sum_{i=1}^{N}F(\mathcal{C}_i)\right| \leqslant \varepsilon\sum_{i=1}^{N}F(\mathcal{D}_i) \tag{10}$$

当数据满足 non-IID 时，式(8)可表示为

$$\left|F(\mathcal{D}_i)-F(\mathcal{C}_i)\right|\frac{|\mathcal{D}_i|}{|\mathcal{D}|} \leqslant \varepsilon_i\frac{|\mathcal{D}_i|}{|\mathcal{D}|}\left|F(\mathcal{D}_1,\mathcal{D}_i,\cdots,\mathcal{D}_N)\right| \tag{11}$$

损失累加后，有

$$\begin{aligned}&\left|\sum_{i=1}^{N}\frac{|\mathcal{D}_i|}{|\mathcal{D}|}F(\mathcal{D}_i)-\sum_{i=1}^{N}\frac{|\mathcal{D}_i|}{|\mathcal{D}|}F(\mathcal{C}_i)\right| \leqslant \varepsilon_i\frac{|\mathcal{D}_i|}{|\mathcal{D}|}\sum_{i=1}^{N}F(\mathcal{D}_i) \leqslant \\ &\sum_{i=1}^{N}\frac{|\mathcal{D}_i|}{|\mathcal{D}|}F(\mathcal{D}_i)\left[\frac{|\mathcal{D}_1|}{|\mathcal{D}|}\varepsilon+\frac{|\mathcal{D}_j|}{|\mathcal{D}|}\varepsilon+\cdots+\frac{|\mathcal{D}_N|}{|\mathcal{D}|}\varepsilon\right] \leqslant \\ &\varepsilon\sum_{i=1}^{N}\frac{|\mathcal{D}_i|}{|\mathcal{D}|}F(\mathcal{D}_i)\end{aligned} \tag{12}$$

证毕。

在定义了全局模型损失函数容忍度 ε 之后，为了从原始数据集中去除冗余数据，需要重新定义每个数据点的冗余度。与文献[28-29]类似，所提方法采用敏感度来量化每个数据点的冗余度。不同的是，所提方法考虑了不同数据点的不同权重，将每个数据点的敏感度定义为该数据点的损失函数与数据集中所有数据点加权平均损失函数的差距。差距越大，表示该数据点对全局模型越重要，则越不

冗余；差距越小，表示该数据点对全局模型来说影响较小，越冗余，具体如定义 2 所示。

定义 2 敏感度。记 $\rho_{i,j}$ 为数据集 $\mathcal{D}_i$ 中任意的数据点 j 对应的权重，则该数据点 j 的敏感度 $\vartheta_{i,j}$ 可表示为

$$\vartheta_{i,j}=\sup_{w\in\omega}\frac{\rho_{i,j}F(x_j)}{\sum_{j=1}^{|\mathcal{D}_i|}\rho_{i,j}F(x_j)} \tag{13}$$

其中，$\vartheta_{i,j}$ 表示在 $w(w\in\boldsymbol{\omega})$ 变化时数据点 j 对数据集中所有数据点的模型损失函数的影响。$\vartheta_{i,j}$ 的值越大，数据点 j 越重要，越应该被包含在核心数据集中。

通过定义 2 可以发现，由于给定的模型参数 w 是不断变化的，很难直接给出数据点 j 的敏感度。因此，与前期研究相似，本文采用计算敏感度边界的方法来评估每个数据点的敏感度。首先，采用聚类的方法将原始数据集划分为多个聚类簇检测冗余和异常数据。然后，将聚类在一起除聚类中心点的数据点视作冗余数据，而远离其他数据点的异常数据点和聚类中心点数据看作核心数据。具体地，将原始数据集 $\mathcal{D}_i$ 划分为 K 个聚类簇，每个聚类簇用 $\mathcal{G}_i^k$ 表示。在任意的簇 $\mathcal{G}_i^k$ 中，记 $\rho_{i,j}^k$ 为任意数据点 j 的权重，$\mathcal{G}_{i,j}^k$ 为聚类簇 k 中与数据点 j 标签相同的数据点集合，$\mathcal{G}_{i,j^-}^k$ 为与数据点 j 标签不相同的数据点集合，$W_{i,j}^k$ 为 $\mathcal{G}_{i,j}^k$ 中所有数据点的权重之和，W_{i,j^-}^k 为 $\mathcal{G}_{i,j^-}^k$ 中所有数据点的权重之和，且 $\mathcal{G}_{i,j^-}^k=\sum_{(x_p,y_p)\in\mathcal{G}_{i,j}^k}\rho_{i,j}^k$，$W_{i,j^-}^k=\sum_{(x_p,y_p)\in\mathcal{G}_{i,j^-}^k}\rho_{i,j}^k$。具体的敏感度边界如定义 3 所示。

定义 3 敏感度边界。记 $S_{i,j}$ 为数据集 $\mathcal{D}_i$ 中数据点 j 的敏感度边界，满足

$$\vartheta_{i,j}\leqslant S_{i,j}=\frac{1}{\rho_{i,j}+\sum_{k=1}^{K}\left[W_{i,j^-}^k\mathrm{dx}_{i,j}+W_{i,j^-}^k\mathrm{dx}_{i,j}^-\right]} \tag{14}$$

其中，$\mathrm{dx}_{i,j}=\mathrm{e}^{-\lambda\left\|\sum_{(x_p,y_p)\in\mathcal{G}_{i,j}^k}(x_p-x_j)W_{p,j}\right\|^2}$ 表示数据点 j 与其标签相同的数据点集合 $\mathcal{G}_{i,j}^k$ 中所有数据点的加权平均距离，$W_{p,j}=\dfrac{\rho_{i,j}^k}{\sum_{(x_p,y_p)\in C_{i,j}^k}\rho_{i,j}^k}$，$\lambda=\dfrac{a}{\sqrt{I}}$ 表示利普希茨常数，I 表示聚类中心的平均距离，a 由实际数据集计算得到，取值范围为 $2.5\leqslant a\leqslant 3.5$；$\mathrm{dx}_{i,j}^-=\mathrm{e}^{-\lambda\left\|\sum_{(x_p,y_p)\in\mathcal{G}_{i,j^-}^k}(x_p-x_j)W_{p,j^-}\right\|^2}$ 表示数据点 j 与其标签相同的数据点集合 $\mathcal{G}_{i,j^-}^k$ 中所有数据点的加权平均距离，$W_{p,j^-}=\dfrac{\rho_{i,j}^k}{\sum_{(x_p,y_p)\in\mathcal{G}_{i,j}}\rho_{i,j}^k}$。

敏感度边界表示数据点与每个簇中数据点集合中所有数据点的加权平均距离，距离较大说明该数据点离其他数据点较远，与其他数据点不相似，冗余度较低；反之，冗余度较高。敏感度边界是一个可以计算得到的实数值，计算得到敏感度边界后就可以根据敏感度边界的加权平均值计算核心数据集的抽取概率，进行核心数据集抽取。联邦核心数据集构建如算法 1 所示。

算法 1 联邦核心数据集构建

输入 设备集合 $\mathcal{N}=\{\mathcal{N}_i\}_{i=1}^N$，数据集集合 $\mathcal{D}=\{\mathcal{D}_i\}_{i=1}^N$，全局模型损失函数容忍度 ε，错误率 σ，参数 λ，簇个数 K

输出 核心数据集 $\mathcal{C}_i$

1) 划分 $\mathcal{D}_i$ 为 K 个聚类簇
2) for 数据点 $j=1:\mathcal{D}_i$ do
3) for 簇 $k\in K$ do
4) 评估 $W_{p,j}$、W_{p,j^-}、$\mathrm{dx}_{i,j}$ 以及 $\mathrm{dx}_{i,j}^-$
5) end for
6) 根据式(13)评估 $S_{i,j}$
7) end for
8) $\overline{S}_i\leftarrow\dfrac{1}{|\mathcal{D}_i|}\sum_{j=1}^{|\mathcal{D}_i|}S_{i,j}$
9) for 数据点 $j=1:\mathcal{D}_i$ do
10) $P_{i,j}\leftarrow\dfrac{S_{i,j}}{\sum_{j=1}^{|\mathcal{D}_i|}S_{i,j}}$
11) end for
12) $|\mathcal{C}_i|\leftarrow\dfrac{c\overline{S}_i}{\left(\dfrac{|\mathcal{D}|}{|\overline{D}_i|}\varepsilon\right)^2}\left[\left(|\mathcal{D}_i|+1\right)\log\left(\overline{S}_i\right)+\log\left(\dfrac{1}{\sigma}\right)\right]$
13) 从数据集 $\mathcal{D}_i$ 中提取核心数据集 $\mathcal{C}_i$

2.4 分布式自适应模型演化

为了更好地适配所提取的核心数据，保证训练模型的性能，终端设备需要布置一个适配的小型训练模型。然而，由于不同的终端具有不同的核心数

据集，因此很难直接给出一个最优的神经网络模型去适配所有的核心数据集。神经网络模型稀疏演化是一种构建稀疏网络的重要方法，被成功且广泛应用于机器学习的各个领域。其中，稀疏演化训练（SET, sparse evolutionary training）[30]算法自适应地训练稀疏化网络模型，从一个初始的 Erdos-Rnyi 随机网络开始，每个相邻层都满足如式(15)的连接概率 $P(w_{m,v}^{l})$。在每次迭代训练中，SET 删除固定比例的不重要网络连接，并将相同比例的重要网络连接重新加入训练模型中。重复这一步骤，直至得到最优的演化模型。

$$P(w_{m,v}^{l})=\frac{\beta(n^{l}+n^{l-1})}{n^{l}n^{l-1}} \tag{15}$$

其中，n^{l} 和 n^{l-1} 分别为层 l 和层 $l-1$ 的神经元个数，β 为模型稀疏化比例，$\beta(n^{l}+n^{l-1})$ 为层 l 和层 $l-1$ 之间的网络连接数。

SET 算法可以有效地演化网络模型的拓扑结构，但它的应用场景主要集中在单一模型的集中式训练环境中。这与联邦学习的分布式环境具有本质的区别。因此，本文提出了一种新的分布式自适应模型演化算法，如算法 2 所示。

算法 2　分布式自适应模型演化

输入　设备集合 $\mathcal{N}=\{\mathcal{N}_i\}_{i=1}^{N}$，核心数据集 $\mathcal{C}=\{\mathcal{C}_i\}_{i=1}^{N}$，稀疏化参数 β，用户参与比率 r，训练块大小 B，本地训练轮数 E，模型层数 L 及参数 χ

输出　全局模型 $\boldsymbol{\omega}_T$，通信比特数 B_T

1) 服务器：
2) 初始化初始剪枝率 ζ_i^0、B_T 及全连接网络模型
3) for 层 $l\in L$ do
4) 根据式(14)初始化稀疏网络模型
5) end for
6) 初始化 $\boldsymbol{\omega}_0$
7) for $t=0,1,2,\cdots,T$ do
8) $m\leftarrow|\mathcal{N}|r$，　$\boldsymbol{\omega}_t\leftarrow\boldsymbol{\omega}_{t-1}-\frac{1}{m}\sum_{i=1}^{m}\boldsymbol{\omega}_i^t$
9) 从 $\boldsymbol{\omega}_t$ 中去除 ζ_i^0%不重要的连接
10) $B_T=B_T+m|\boldsymbol{\omega}_t|+\sum_{i=1}^{m}|\boldsymbol{\omega}_i^t|$
11) end for
12) 用户 $\mathcal{N}_i$：
13) $\boldsymbol{\omega}_i^t\leftarrow\boldsymbol{\omega}_t$
14) for $e=1,2,\cdots,E$ do
15) for $b\in B$ do
16) $\boldsymbol{\omega}_i^t\leftarrow\boldsymbol{\omega}_i^t-\eta_i\nabla F_i(\boldsymbol{\omega}_i^t,b)$
17) end for
18) end for
19) for 从 $\boldsymbol{\omega}_i^t$ 中的每条连接 j do
20) 根据式(16)评估 $I_{i,j}^t$
21) end for
22) 根据式(17)评估第 t 轮的剪枝率 ζ_i^t
23) 从 $\boldsymbol{\omega}_i^t$ 中去除 ζ_i^t%不重要的连接
24) 上传演化的本地模型 $\boldsymbol{\omega}_i^t$ 至云服务器

具体地，所提算法进行了 2 个方面的改进。首先，将原来的集中式模型演化扩展到分布式场景。其次，根据联邦学习的特点设计了一种新的模型演化方式，包括如何确定不重要的连接以及如何删除这些连接。具体来说，所提算法包括如下几个阶段。

在初始全局模型上进行网络模型稀疏化。在联邦学习训练之前，根据式(15)中的稀疏化控制变量 β 初始化一个稀疏的全局模型，并将稀疏化的全局模型下发给每个选择的终端。构建初始化稀疏模型有如下几方面的优势。首先，布置一个小型稀疏模型开始联邦学习训练可以大大减少每个参与设备在每轮迭代时所产生的网络模型参数；其次，使用小型稀疏模型可以更好地适应所提取的核心数据集；最后，使用小型稀疏模型可以减少本地设备训练所使用的计算资源的消耗。

每个终端根据其自身的模型剪枝率动态地对本地模型进行稀疏化操作。每个终端根据定义 4 和定义 5 的连接重要性和重要性评估机制，自适应地从本地模型中去除一部分不重要的模型参数及网络连接，并将演化之后的模型传输给云服务器。为每个用户设置动态变化的剪枝率主要有 2 个方面的考虑。一方面，每个终端可以根据自身的剪枝率对本地模型而非全局模型进行剪枝，充分考虑了不同终端的个性化特性；另一方面，设置动态变化的剪枝率，可以更好地满足学习模型越来越收敛的特性。

全局模型聚合，并在聚合的全局模型上进行二次网络模型演化。由于从每个终端上传稀疏化本地模型只考虑了其自身的个性化特征，并不能表征其他所有设备的全局特征。同时，为了更好地减少下行的通信比特数，本文在标准的联邦平均聚合之后，进行进一步的网络模型演化。

值得注意的是，由于在每个局部训练迭代中去除一部分不重要的连接和模型参数可能会引起模型性能的波动。因此，本文采用在最后一个局部模型训练迭代时进行去除操作。

定义 4 连接重要性。记设备 $\mathcal{N}_i$ 在第 t 轮迭代根据其本地核心数据集进行本地训练，所得到的本地模型更新为 $\boldsymbol{\omega}_i^t$，且 $\boldsymbol{\omega}_i^t=\{\omega_{i,1}^t,\omega_{i,j}^t,\cdots,\omega_{i,N}^t\}$，更新参数 $\boldsymbol{\omega}_i^t$ 中每个子更新 $\omega_{i,j}^t$ 的重要性表示为 $I_{i,j}^t$，且 $I_{i,j}^t$ 定义为去除子更新参数 $\omega_{i,j}^t$ 对模型损失函数的均方差，即

$$I_{i,j}^t=\left(F(C_i,\boldsymbol{\omega}_i^t)-F(C_i,\boldsymbol{\omega}_i^t\left|\omega_{i,j}^t=0\right.)\right)^2 \tag{16}$$

其中，$F(C_i,\boldsymbol{\omega}_i^t)$ 和 $F(C_i,\boldsymbol{\omega}_i^t\mid\omega_{i,j}^t=0)$ 分别表示不去除和去除第 j 个子更新时的模型损失函数值。

从式(16)可知，如果要评估去除每个子参数对模型的损失函数影响，需要评估 N 个不同版本的网络模型，这是非常耗时的。因此，为了解决这个问题，本文采用泰勒级数展开来近似连接重要性 $I_{i,j}^t$，具体的近似值如定理 2 所示。

定理 2 记 $\omega_{i,j}^t$ 和 $g_{i,j}^t$ 分别表示第 j 个子更新以及其相应的子更新梯度值，第 j 条连接的重要性 $I_{i,j}^t$ 可近似表示为

$$I_{i,j}^t=\left(g_{i,j}^t\omega_{i,j}^t-\frac{1}{2}\omega_{i,j}^t\boldsymbol{H}_{i,j}^t\boldsymbol{\omega}_i^t\right) \tag{17}$$

其中，$g_{i,j}^t=\dfrac{\partial F}{\partial\omega_{i,j}^t}$ 表示第 j 个子更新梯度值，$\boldsymbol{H}_{i,j}^t$ 表示第 j 行 Hessian 矩阵（二阶导数矩阵）。

定义 5 重要性评估机制。由于训练模型是随着通信迭代轮数的增加越来越收敛的。因此，本文设计了一个动态的自适应连接重要性评估机制。其主要思想是在联邦学习的开始阶段，通过从当前模型中去除更多不重要的连接或参数来加速模型收敛速度。当训练得到一个更适应的模型时，所提方法就动态地减少被去除的连接数，以保证模型的稳定性和准确性。具体地，记设备 $\mathcal{N}_i$ 的初始剪枝率为 ζ_i^0，训练过程中使用指数衰减来表征模型剪枝率的变化，则迭代轮数 t 时的剪枝率 ζ_i^t 为

$$\zeta_i^t=\frac{\zeta_i^0}{\exp(\tau t)} \tag{18}$$

随着通信迭代轮数 t 的增加，训练模型变得更加收敛，阈值 ζ_i^t 也变得非常小，这使从当前网络模型中删除的连接数大大减少。通过不断保留网络中不重要或无用的网络连接和模型参数，可以保证训练模型的准确性。

由于全局模型是根据每个设备自身的剪枝率进行的演化，并不适配所有的用户数据。因此，所提方法在聚合的全局模型上进行第二次网络模型演化，即在聚合的全局模型上去除一部分权重为 0 的参数更新，一方面使全局模型更加紧致，减少了下行通信比特数；另一方面，对聚合的全局模型进行演化，使所训练的模型在保证满足设备个性化特征的同时又能满足其他所有设备的数据特点。

3 收敛性证明

本节给出所提方法的收敛性证明。神经网络中的损失函数通常满足如下 2 个性质[10,12]。

性质 1 α-平滑性[10]。损失函数 F 为 β-平滑函数，则对于 $\forall\boldsymbol{\theta},\boldsymbol{\upsilon}$，有

$$F(\boldsymbol{\theta})-F(\boldsymbol{\upsilon})\leqslant\left\langle(\boldsymbol{\theta}-\boldsymbol{\upsilon}),\nabla F(\boldsymbol{\theta})\right\rangle+\frac{\alpha}{2}\|\boldsymbol{\theta}-\boldsymbol{\upsilon}\|^2 \tag{19}$$

其中，$\langle\cdot\rangle$ 表示 2 个向量的内积，$\nabla F(\cdot)$ 表示梯度函数，$\|\cdot\|$ 表示范数。

性质 2 Lipschitz 条件[12]。损失函数 F 满足 μ-Lipschitz 条件，则对于 $\forall\boldsymbol{\theta},\boldsymbol{\upsilon}$，有

$$F(\boldsymbol{\theta})-F(\boldsymbol{\upsilon})\leqslant\mu\|\boldsymbol{\upsilon}-\boldsymbol{\theta}\| \tag{20}$$

基于以上损失函数的 2 个性质，本节给出了如下的收敛性证明，其函数收敛性满足定理 3。

定理 3 收敛性保证。假设全局模型损失函数 F 满足 α-平滑性和 μ-Lipschitz 条件。记 $\hat{\boldsymbol{\omega}}_t$ 为第 t 轮迭代经过全局剪枝之后的全局模型参数，$\boldsymbol{\omega}_*$ 为全局模型参数最优值，经过迭代轮数 T，全局损失函数 F 满足式(21)，其表明随着迭代轮数的增加，全局参数向量最终收敛至一个固定值。

$$\begin{aligned}\mathbb{E}\left[F(\boldsymbol{\omega}_T)-F(\boldsymbol{\omega}_*)\right]\leqslant&\left[F(\boldsymbol{\omega}_0)-F(\boldsymbol{\omega}_*)\right]+\\&(\alpha-\eta\mu)^T\sum_{t=0}^{T-1}\mathbb{E}\left[\left\|\boldsymbol{\omega}_T-\hat{\boldsymbol{\omega}}_{t-1}\right\|\right]+\frac{\eta^2\mu\psi^2}{2}\end{aligned} \tag{21}$$

其中，$\boldsymbol{\omega}_T$ 为经过 T 轮迭代的全局模型参数，$\mathbb{E}\left[\left\|\nabla F(\boldsymbol{\omega}_t)\right\|^2\right]\leqslant\psi^2$。

证明 由于下一轮迭代的模型更新值是在上一轮剪枝之后的模型更新基础上进行迭代训练

所得到的，因此一次 SGD 迭代的模型更新可以表示为

$$\boldsymbol{\omega}_{t+1}=\hat{\boldsymbol{\omega}}_t-\eta\nabla F(\hat{\boldsymbol{\omega}}_t;b)\odot m(\hat{\boldsymbol{\omega}}_t) \tag{22}$$

其中，$\hat{\boldsymbol{\omega}}_t$ 为第 t 轮迭代经过全局剪枝之后的全局模型参数，$\boldsymbol{\omega}_{t+1}$ 为第 t 轮迭代的全局模型参数，$m(\hat{\boldsymbol{\omega}}_t)$ 为模型参数 $\boldsymbol{\omega}_t$ 的掩码向量，$\odot$ 为 2 个矩阵对应位置元素进行乘积。

由于训练过程中 $\hat{\boldsymbol{\omega}}_t$ 不可以提前获得，因此 $\nabla F(\hat{\boldsymbol{\omega}}_t;b)\approx\nabla F(\boldsymbol{\omega}_t;b)$，$m(\hat{\boldsymbol{\omega}}_t)\approx m(\boldsymbol{\omega}_t)$，为了简化证明，下面将 $\nabla F(\boldsymbol{\omega}_t;b)$ 和 $m(\boldsymbol{\omega}_t)$ 分别表示为 $\nabla F(\boldsymbol{\omega}_t)$ 和 m_t，则式(22)等价于

$$\boldsymbol{\omega}_{t+1}=\hat{\boldsymbol{\omega}}_t-\eta\nabla F(\hat{\boldsymbol{\omega}}_t)\odot m_t \tag{23}$$

基于式(23)和假设 1，有

$$\begin{aligned}&\mathbb{E}\left[F(\boldsymbol{\omega}_{t+1})-F(\boldsymbol{\omega}_*)\,|\,\hat{\boldsymbol{\omega}}_t,m_t\right]\leqslant\left[F(\boldsymbol{\omega}_t)-F(\boldsymbol{\omega}_*)\right]-\\&\eta\left\langle\nabla F(\hat{\boldsymbol{\omega}}_t)-\nabla F(\boldsymbol{\omega}_*),\mathbb{E}\left[\nabla F(\hat{\boldsymbol{\omega}}_t)\odot m_t\,|\,\hat{\boldsymbol{\omega}}_t,m_t\right]\right\rangle+\\&\frac{\eta^2\mu}{2}\mathbb{E}\left[\left\|\nabla F(\boldsymbol{\omega}_t)\odot m_t\right\|^2\,|\,\hat{\boldsymbol{\omega}}_t,m_t\right]\end{aligned} \tag{24}$$

进一步地，因为 $\mathbb{E}\left[\nabla F(\boldsymbol{\omega}_t)\odot m_t\,|\,\hat{\boldsymbol{\omega}}_t,m_t\right]=\mathbb{E}\left[\nabla F(\boldsymbol{\omega}_t)\,|\,\hat{\boldsymbol{\omega}}_t\odot m_t\right]$，则式(24)可表示为

$$\begin{aligned}&\mathbb{E}\left[F(\boldsymbol{\omega}_{t+1})-F(\boldsymbol{\omega}_*)\,|\,\hat{\boldsymbol{\omega}}_t,m_t\right]\leqslant\left[F(\boldsymbol{\omega}_t)-F(\boldsymbol{\omega}_*)\right]-\\&\eta\left\langle\nabla F(\hat{\boldsymbol{\omega}}_t)-\nabla F(\boldsymbol{\omega}_*),\mathbb{E}\left[\nabla F(\boldsymbol{\omega}_t)\odot m_t\,|\,\hat{\boldsymbol{\omega}}_t,m_t\right]\right\rangle+\\&\frac{\eta^2\mu}{2}\mathbb{E}\left[\left\|\nabla F(\boldsymbol{\omega}_t)\odot m_t\right\|^2\,|\,\hat{\boldsymbol{\omega}}_t,m_t\right]=\\&\left[F(\boldsymbol{\omega}_t)-F(\boldsymbol{\omega}_*)\right]-\eta\left\langle\nabla F(\hat{\boldsymbol{\omega}}_t)-\nabla F(\boldsymbol{\omega}_*),\nabla F(\hat{\boldsymbol{\omega}}_t)\odot m_t\right\rangle+\\&\frac{\eta^2\mu}{2}\mathbb{E}\left[\left\|\nabla F(\boldsymbol{\omega}_t)\odot m_t\right\|^2\,|\,\hat{\boldsymbol{\omega}}_t,m_t\right]\leqslant\\&\left[F(\boldsymbol{\omega}_t)-F(\boldsymbol{\omega}_*)\right]-\eta\left\|\left(\nabla F(\boldsymbol{\omega}_t)-\nabla F(\boldsymbol{\omega}_*)\right)\nabla F(\hat{\boldsymbol{\omega}}_t)\odot m_t\right\|^2+\\&\frac{\eta^2\mu}{2}\mathbb{E}\left[\left\|\nabla F(\boldsymbol{\omega}_t)\odot m_t\right\|^2\,|\,\hat{\boldsymbol{\omega}}_t,m_t\right]\end{aligned} \tag{25}$$

由于 $\mathbb{E}\left[\left\|\nabla F(\boldsymbol{\omega}_t)\odot m_t\right\|^2\right]\leqslant\mathbb{E}\left[\left\|\nabla F(\boldsymbol{\omega}_t)\right\|^2\right]\leqslant\psi^2$，则式(25)可表示为

$$\begin{aligned}&\mathbb{E}\left[F(\boldsymbol{\omega}_{t+1})-F(\boldsymbol{\omega}_*)\,|\,\hat{\boldsymbol{\omega}}_t,m_t\right]\leqslant\left[F(\boldsymbol{\omega}_t)-F(\boldsymbol{\omega}_*)\right]-\\&\eta\left\|\left(\nabla F(\boldsymbol{\omega}_t)-\nabla F(\boldsymbol{\omega}_*)\right)\nabla F(\hat{\boldsymbol{\omega}}_t)\odot m_t\right\|^2+\frac{\eta^2\mu\psi^2}{2}\end{aligned} \tag{26}$$

由于损失函数 F 满足 Lipschitz 条件，则根据性质 2，有

$$\left[F(\hat{\boldsymbol{\omega}}_t)-F(\boldsymbol{\omega}_t)\right]\leqslant\mu\left\|\boldsymbol{\omega}_t-\hat{\boldsymbol{\omega}}_t\right\| \tag{27}$$

根据式(27)，式(26)可进一步表示为

$$\begin{aligned}&\mathbb{E}\left[F(\boldsymbol{\omega}_{t+1})-F(\boldsymbol{\omega}_*)\,|\,\hat{\boldsymbol{\omega}}_t,m_t\right]\leqslant F(\boldsymbol{\omega}_t)-F(\boldsymbol{\omega}_*)-\\&\eta\left\|\left(\nabla F(\boldsymbol{\omega}_t)-\nabla F(\boldsymbol{\omega}_*)\right)\nabla F(\hat{\boldsymbol{\omega}}_t)\odot m_t\right\|^2+\frac{\eta^2\mu\psi^2}{2}\leqslant\\&F(\boldsymbol{\omega}_t)+\alpha\left\|\boldsymbol{\omega}_t-\hat{\boldsymbol{\omega}}_t\right\|-F(\boldsymbol{\omega}_*)-\\&\eta\left\|\left(\nabla F(\boldsymbol{\omega}_t)-\nabla F(\boldsymbol{\omega}_*)\right)\odot m_t\right\|^2+\frac{\eta^2\mu\psi^2}{2}\leqslant\\&F(\boldsymbol{\omega}_t)+\alpha\left\|\boldsymbol{\omega}_t-\hat{\boldsymbol{\omega}}_t\right\|-F(\boldsymbol{\omega}_*)-\\&\eta\mu\left\|\left(\boldsymbol{\omega}_t-\boldsymbol{\omega}_*\right)\odot m_t\right\|^2+\frac{\eta^2\mu\psi^2}{2}\leqslant F(\boldsymbol{\omega}_t)+\\&\alpha\left\|\boldsymbol{\omega}_t-\hat{\boldsymbol{\omega}}_t\right\|-F(\boldsymbol{\omega}_*)-\eta\mu\left\|\left(\boldsymbol{\omega}_t-\boldsymbol{\omega}_*\right)\right\|^2+\frac{\eta^2\mu\psi^2}{2}\leqslant\\&F(\boldsymbol{\omega}_t)-F(\boldsymbol{\omega}_*)+\alpha\left\|\boldsymbol{\omega}_t-\hat{\boldsymbol{\omega}}_t\right\|-\eta\mu\left\|\left(\boldsymbol{\omega}_t-\hat{\boldsymbol{\omega}}_t\right)\right\|^2+\\&\frac{\eta^2\mu\psi^2}{2}=F(\boldsymbol{\omega}_t)-F(\boldsymbol{\omega}_*)+\left(\alpha-\eta\mu\right)\left\|\boldsymbol{\omega}_t-\hat{\boldsymbol{\omega}}_t\right\|+\frac{\eta^2\mu\psi^2}{2}\end{aligned} \tag{28}$$

将式(28)两边展开，可以得到

$$\begin{aligned}&\mathbb{E}\left[F(\boldsymbol{\omega}_{t+1})-F(\boldsymbol{\omega}_*)\right]\leqslant\mathbb{E}\left[F(\boldsymbol{\omega}_t)\right]-\mathbb{E}\left[F(\boldsymbol{\omega}_*)\right]+\\&\left(\alpha-\eta\mu\right)\mathbb{E}\left[\left\|\boldsymbol{\omega}_t-\hat{\boldsymbol{\omega}}_t\right\|\right]+\frac{\eta^2\mu\psi^2}{2}\end{aligned} \tag{29}$$

根据式(29)，经过 T 轮迭代，有

$$\begin{aligned}&\mathbb{E}\left[F(\boldsymbol{\omega}_T)-F(\boldsymbol{\omega}_*)\right]\leqslant\mathbb{E}\left[F(\boldsymbol{\omega}_0)\right]-\mathbb{E}\left[F(\boldsymbol{\omega}_*)\right]+\\&\left(\alpha-\eta\mu\right)^T\sum_{t=0}^{T-1}\mathbb{E}\left[\left\|\boldsymbol{\omega}_t-\hat{\boldsymbol{\omega}}_t\right\|\right]+\frac{\eta^2\mu\psi^2T}{2}\leqslant F(\boldsymbol{\omega}_0)-\\&F(\boldsymbol{\omega}_*)+\left(\alpha-\eta\mu\right)^T\sum_{t=0}^{T-1}\mathbb{E}\left[\left\|\boldsymbol{\omega}_t-\hat{\boldsymbol{\omega}}_t\right\|\right]+\frac{\eta^2\mu\psi^2T}{2}\end{aligned} \tag{30}$$

证毕。

4　实验

4.1　实验配置

网络模型和数据集。与文献[2,6]类似，本文使用联邦学习常用的 MLP 和 CNN 模型进行训练。MLP 模型由一个输入层、2 个隐藏层以及一个输出层组成。其中，每个隐藏层包含 200 个神经元节点。在整个模型训练过程中，使用 ReLU 作为激活函数。CNN 模型包含 10 个 5×5 的卷积层（第一个卷积层具有 32 个通道，第二个卷积层具有 64 个通道，每个卷积层之后都设置了一个 2×2 的最大池化层），一个具有 512 个神经元单元的全连接层，ReLU 激活层，以及最后的 softmax 输出层。实验中，使用 MNIST 和 CIFAR-10 这 2 个图像数据集对所提方法性能进行测试。

数据划分及联邦环境。设置用户数目 N 和每轮通信迭代的用户参与比例 r 分别为 100 和 1。模型训练最小的块大小 B =10，本地模型训练轮数 E =5，学习率 η =0.01。同时，为了研究不同数据分布对模型训练的影响，以 MNIST 数据集为例，本文实验测试了 2 种不同的数据划分方式。一种是 IID，将训练数据集随机划分给参与训练的 100 个用户，每个用户分配 600 个采样样本；另一种是 non-IID，将训练数据集按照其标签排序分成 200 个大小为 300 的碎片，给每个参与训练的用户随机分配 2 个碎片，且每个参与用户只包含 2 个不同类别的标签。

核心数据集构建和模型演化。表 2 给出了本文主要实验参数设置。由于参数 λ 以及聚类簇个数 K 是核心数据集构建过程中的 2 个重要因素，因此本文测试了 5 组不同 λ 和 K 的取值，即 $(\lambda,K)=\{(5,16),(4,8),(3,6),(2,4),(1,2)\}$。除此之外，设置全局模型的损失函数容忍度 ε 和错误率 σ 分别为 0.05 和 0.08。同时，为了更加全面地分析不同模型演化参数对所提方法性能的影响，测试了在相同核心数据集构建参数条件下，$\beta=\{100,50,30\}$、$\zeta=\{0,0.1,0.5,1.0\}$ 以及 $\varsigma=\{0,0.1,0.5,1.0\}$ 不同取值情况下训练模型的性能。指数函数衰减率 τ 设置为 0.01。

表 2　主要实验参数设置

参数	取值
N	100
r	1
B	10
E	5
η	0.01
ε	0.05
σ	0.08
β	{100,50,30}
ζ	{0,0.1,0.5,1.0}
ς	{0,0.1,0.5,1.0}
(λ,K)	{(5,16), (4,8), (3,6), (2,4), (1,2)}
τ	0.01

4.2　实验结果及分析

实验首先测试了 5 组不同核心数据集构建情形下所提方法及基准方法（FedAvg）的模型性能，并与现有最新方法 eSGD[12]、LotteryFL[31]进行了性能对比，分别描述了这 5 种情形下模型性能之间的关系。eSGD 残差梯度的指数衰减速率 $\beta=0.9$，学习率 $\eta=\frac{0.1}{2e}$，其中，e 是迭代次数。LotteryFL 的本地模型训练轮数 E =10，模型训练最小的块大小 B =32，学习率 η =0.2，剪枝率为 0.1、0.3、0.5。

本文分别对比了模型训练准确率（Acc）、网络连接数（Conn）、核心数据集构建时间（CT）、模型演化时间（ET）和累计通信比特数（TB）5 种指标下的性能，如图 2～图 5 所示。分别对比图 2 和图 4、图 3 和图 5 可以看出：一方面，(λ,K) 数值越大，核心数据集规模越大，所提方法的模型准确率越高；另一方面，(λ,K) 数值越小，所提方法减少的通信比特传输数越多。本文分别选取了 $(\lambda,K)=(5,16)$ 和 $(\lambda,K)=(1,2)$ 2 种参数情况下的数据进行了测试，这两组参数值分别对应所提方法的最好和最差边界。对于本文的数据集来说，λ 的取值范围为 $1\leqslant\lambda\leqslant5$，$K$ 的取值范围为 $2\leqslant K\leqslant16$，额外的实验结果表明，当 λ 和 K 的取值位于此范围内时，实验结果的范围在 $(\lambda,K)=(5,16)$ 和 $(\lambda,K)=(1,2)$ 的性能之间。其中，图 2 和图 4 是使用 MNIST 数据集进行模型训练的实验结果，图 3 和图 5 是使用 CIFRA-10 数据集进行模型训练的实验结果。对于网络模型演化参数的不同取值，本文选择了具有代表性的 5 种情况进行了描述，分别为 $(\beta,\zeta,\varsigma)=(100,0,0)$、$(\beta,\zeta,\varsigma)=(50,0,0)$、$(\beta,\zeta,\varsigma)=(50,0,0.1)$、$(\beta,\zeta,\varsigma)=(50,0.1,0)$ 和 $(\beta,\zeta,\varsigma)=(50,0.1,0.1)$。

从图 2 和图 4 中可以看出，FedAvg 方法具有最快的模型收敛速度和最高的最终测试模型准确率，但是 FedAvg 方法需要传输最多的模型更新比特数。例如，当数据满足 IID 使用 MLP 模型进行训练时，FedAvg 方法可以达到 98.35%的模型准确率，传输 18 490 572 的通信比特数，最终的收敛模型连接数为 198 800。与使用 FedAvg 方法相比，核心数据集全网络（CDFN）传输了相同的通信比特数（为 18 490 572），但获得了相对较慢的模型收敛速度和轻微降低的模型准确率。这是因为 CDFN 表示的是使用核心数据集且布置全连接模型训练的情形。相较于 CDFN，FedAvg 方法可以学习更多的局部模型特征，从而导致全局模型可以更好地表达每个局部模型。

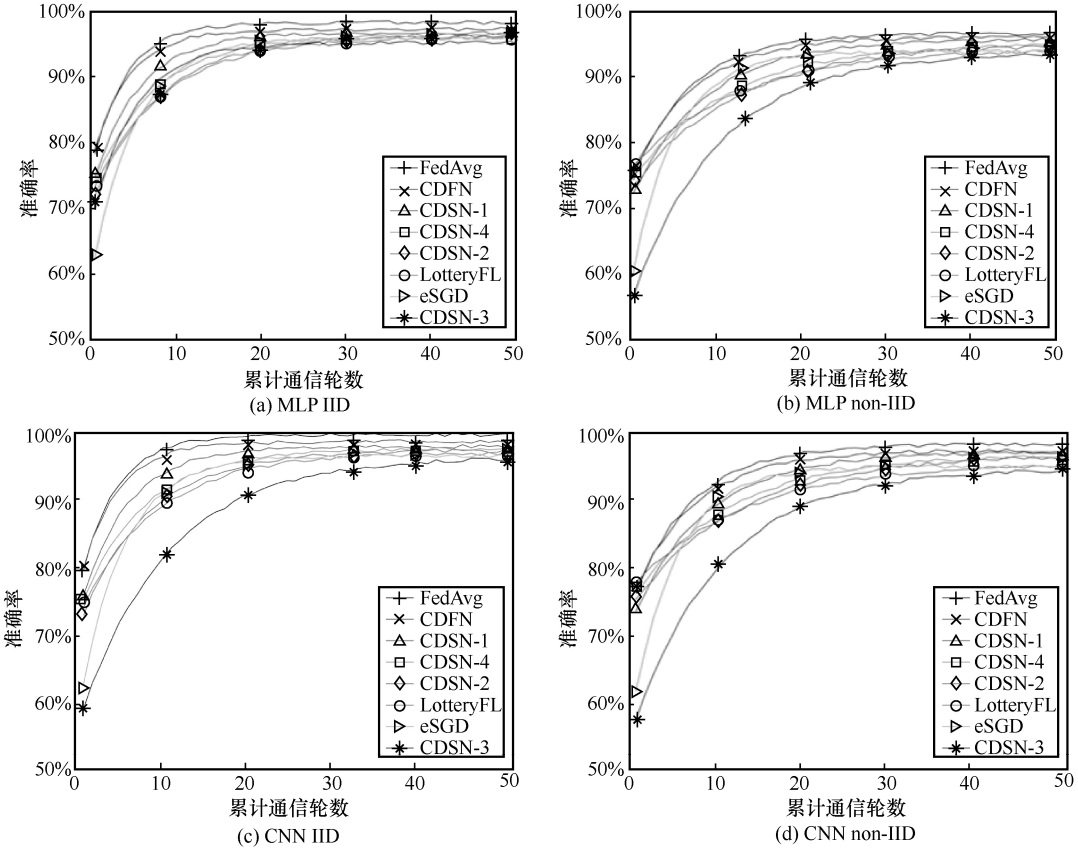


图 2　$(\lambda, K) = (5, 16)$ 情形下使用 MNIST 数据集进行训练的实验结果

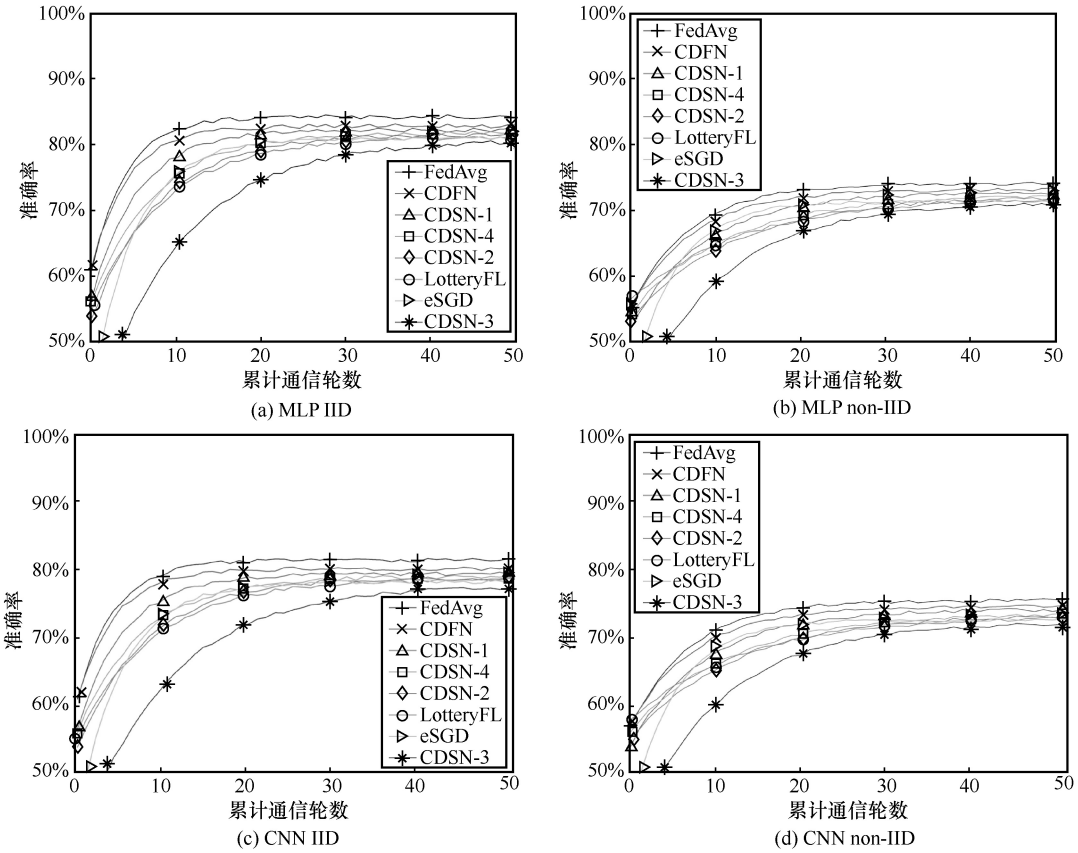


图 3　$(\lambda, K) = (5, 16)$ 情形下使用 CIFAR-10 数据集进行训练的实验结果

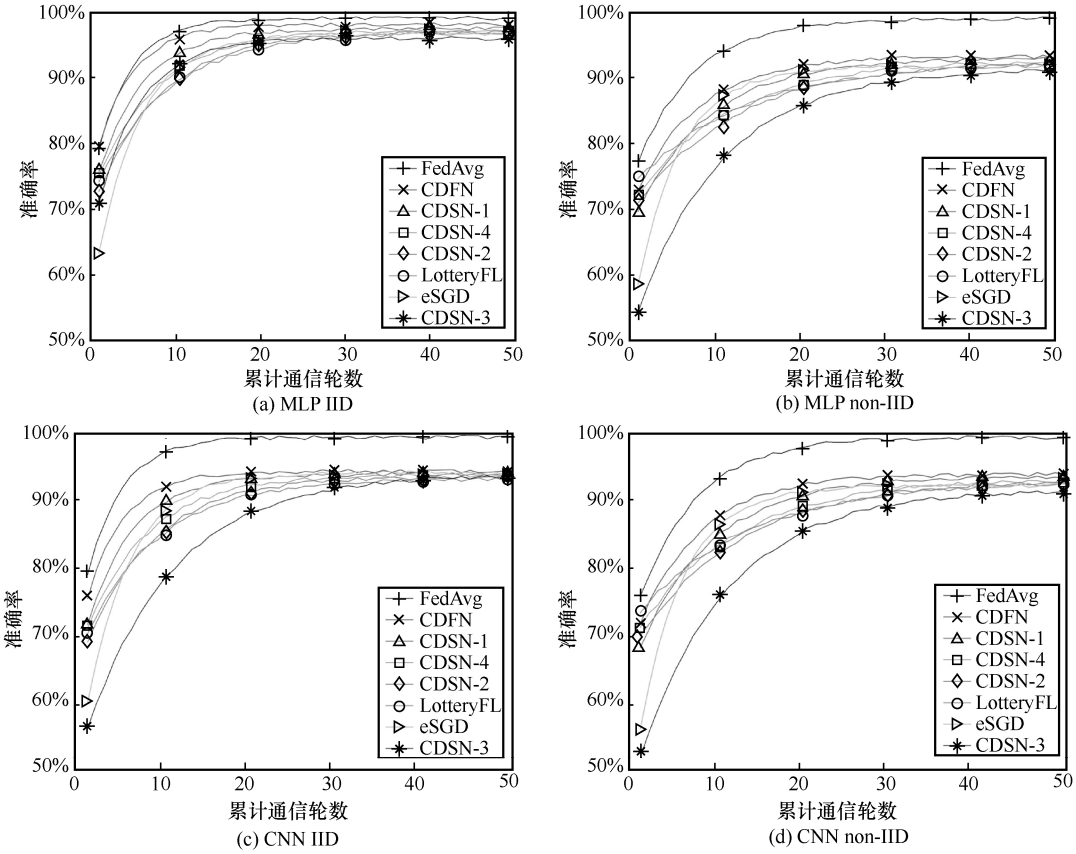


图 4　$(\lambda, K) = (2, 4)$ 情形下使用 MNIST 数据集进行训练的实验结果

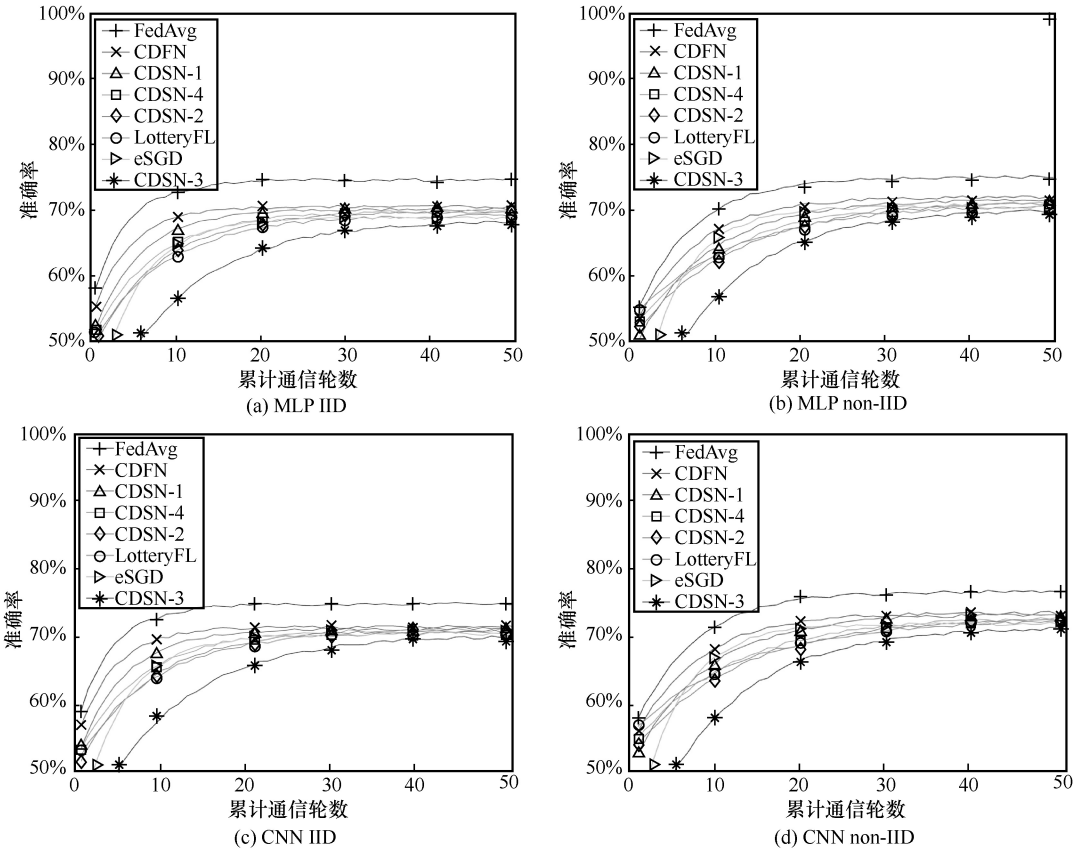


图 5　$(\lambda, K) = (2, 4)$情形下使用 CIFAR-10 数据集进行训练的实验结果

$(\beta,\zeta,\varsigma)=(50,0,0)$ 的情形对应的环境为核心数据集稀疏网络（CDSN-1）。与前面 2 种方法使用规则网络进行训练相比，CDSN-1 布置了一个稀疏化的初始化网络模型进行训练，其每轮迭代只需传输稀疏化的本地模型参数而不需要传输全连接的模型更新参数至云中心，极大地减少了终端与云服务器之间通信比特的传输。但同时，由于 CDSN-1 需要更多的通信轮数来达到模型的收敛，因此，与使用全连接模型训练相比，只有较小的模型的准确率较低。$(\beta,\zeta,\varsigma)=(50,0.1,0)$ 的情形对应的环境为核心数据集稀疏网络（CDSN-2），$(\beta,\zeta,\varsigma)=(50,0,0.1)$ 的情形对应的环境为核心数据集稀疏网络（CDSN-4）。它们分别表示在使用初始稀疏化模型的基础上，要么对本地模型进行剪枝之后再上传至数据中心进行模型聚合，要么直接在聚合的全局模型上进行剪枝。

在通信比特数传输方面，这 2 种情形相较于 CDSN-1 是固定稀疏化的模型，使用了动态模型演化的方法，进一步缩小了训练模型的结构和大小，获得了更少的通信比特数传输。在模型准确率方面，相较于直接在聚合的全局模型上进行演化考虑的是所有用户的统计特征，直接在本地模型更新上进行剪枝则考虑的是每个用户的个性化特性。因此，CDSN-2 较 CDSN-3 具有更高的模型准确率。FedAvg、CDSN-1、CDSN-2、CDSN-3、CDSN-4 以及 eSGD 分别传输 18 490 572、10 563 786、8 857 562、1 702 333、9 949 398 以及 1 877 041 的通信比特数，分别获得了 98.35%、96.87%、96.23%、95.53%、96.78%以及 95.79%的模型准确率。与基准的 FedAvg 方法相比，CDSN-1、CDSN-2 以及 CDSN-4 分别减少了 42.9%、52.1%以及 46.2%的通信比特数传输，同时只降低了 1.48%、2.12%以及 1.57%的模型准确率。其中，CDSN-1、CDSN-2 分别比现有最优的 LotteryFL 提高了 0.71%以及 0.07%的模型准确率，CDSN-3 比现有最优的 eSGD 分别减少了 5.6%的网络连接数和 9.3%的累计通信比特数。$(\beta,\zeta,\varsigma)=(50,0.1,0.1)$ 的情形对应的环境为核心数据集稀疏网络（CDSN-3），该种情形同时考虑了上行和下行比特数传输。同时，在每一轮通信迭代中，CDSN-3 既保证了每个用户的个性化特征，同时又学习了所有用户的统计特性。与其他 5 种情况相比，CDSN-3 传输了最少的通信比特数，却获得了更优的模型性能。与基准方法相比，CDSN-3 减少了将近 90.8%的通信比特数的传输，获得了 2.82%的模型准确率的降低。当数据满足 non-IID 时，所提方法也具有相同的效果。使用核心数据集进行稀疏化模型训练的 FedAvg、CDSN-1、CDSN-2、CDSN-3、CDSN-4 以及 eSGD 分别传输 18 490 572、10 698 148、8 864 973、1 706 799、9 678 799 以及 1 795 477 的通信比特数，分别获得了 97.14%、95.95%、95.10%、93.67%、95.44%以及 94.18%的模型准确率。与基准的 FedAvg 方法相比，CDSN-1、CDSN-2 以及 CDSN-4 节约了 42.1%、52.1%以及 47.7%的通信比特数传输，同时只损失了 1.19%、2.04%以及 1.70%的模型准确率。而同时考虑上行和下行传输的 CDSN-3，减少了 90.8%的通信比特数，损失了 3.47%的模型准确率。使用 CIFAR-10 数据集进行实验时，从图 3 和图 5 可以看出，无论是在 IID 还是在 non-IID 情形下，使用所提方法都能以较少的准确率损失来获得较大的通信比特数减少。特别是在 CDSN-3 情形下，CNN 模型在 non-IID 条件下减少了约 90%的通信比特数，同时只损失了 3.47%的模型准确率。通过以上实验，得出以下实验结论。

1) 与 FedAvg 方法相比，本文所提方法损失了准确率。其中，CDFN 相比 FedAvg 减少了 1.03%的准确率，在可容忍范围内，且采用本文框架的 CDFN、CDSN-1、CDSN-4、CDSN-2 方法的准确率均高于对比方法 eSGD 和 LotteryFL。这是因为本文所提方法采用了较小的核心集和训练网络，可以在相同的训练时间内训练更多的轮次，从而保证训练模型的准确率。

2) 本文所提方法大幅减少了训练所需的通信比特数，其中，相比于 FedAvg 方法，通信比特数减少到 10%以下；相比于目前最优的 LottryFL 方法，通信比特数减少到 40%以上，且核心数据集构建和网络演化的时间在秒级，不会大幅增加模型训练所需的时间。

核心数据集构建参数的影响。本文还评估了不同核心数据集构建参数对所提方法性能的影响，主要包括不同 (λ,K) 取值情形下全局模型准确率和总通信比特数。例如，对于 CNN IID，当 $(\lambda,K)=(5,16)$ 时，所提方法在 CDSN-3 情形下的全局模型获得了 93.87%的模型准确率，同时传输了 7 931 111 通信比特数；当 $(\lambda,K)=(2,4)$ 时，全局模型获得了更高的模型准确率，即 95.54%，但传输了更多的通信比

特数（为 16 287 381）。对于 CNN non-IID，当 $(\lambda, K) = (2,4)$ 时，所提方法在 CDSN-3 情形下获得了 90.76%的模型准确率，传输了 7 321 789 的通信比特数；当 $(\lambda, K) = (5,16)$ 时，可以达到更高的模型准确率（为 94.62%），但需要传输更多的通信比特数（为 16 222 491）。这主要是因为 (λ, K) 取值越大，核心数据集的平均敏感度数值越大，所得到的核心数据集规模越大，使用核心数据集进行模型训练时需要布置的模型结构越大。因此，全局模型获得的准确率就越高，但同时每轮通信迭代产生的模型更新参数越多，即需要传输的总通信比特数越大。

此外，本文还评估了所提方法其他方面的性能，包括核心数据集构建时间（CT）和模型演化时间（ET）两方面。例如，当使用 MLP 模型在 MNIST 数据集上进行模型训练时，在 CDSN-3 情形下，CT 和 ET 分别为 22 s 和 24 s。即使使用更加复杂的 CNN 模型在 CIFAR-10 数据集进行训练，所提方法也仅仅消耗了 607 s 和 608 s 的 CT 和 ET。虽然本文方法可以在很大程度上减少 FL 中的比特传输，但它将花费一些时间来完成核心集的构建和网络演化。但事实上，本文方法只需要在初始化阶段构建一次核心集，而不需要在整个训练阶段构建核心集，所以只在初始化阶段花费时间。在网络演化方面，本文方法是在服务器和终端设备上进行的。由于现在计算设备和云服务器强大的计算能力，实验设置中的服务器和终端可以快速完成网络演化。

5 结束语

本文通过分析冗余更新参数产生的本质原因提出了一种冗余数据去除的联邦学习高效通信方法。该方法考虑从原始数据中去除一部分冗余数据，布置一个适配的小型训练模型，能够在减少终端与云中心通信比特数传输的同时，保证训练模型的准确率。为了从原始数据中去除一部分冗余数据，本文根据联邦学习数据的 non-IID 特性，给出了新的核心数据集敏感度以及损失函数容忍度的定义，并在此基础上提出了联邦核心数据集构建算法。此外，为了适配所提取的核心数据集，保证训练模型的性能，本文基于联邦学习的特点给出了新的模型参数重要性和参数重要性评估机制，并设计了一个新的分布式自适应模型演化算法。同时，本文证明了所提方法的收敛性。实验结果表明，与使用原始冗余数据相比，所提方法减少了 17%的通信比特数，且只有 0.5%的模型准确率降低。未来研究工作中，作者将会探讨本文提出的框架和方法在其他类型数据集中的适用性及性能，以及模型剪枝的安全性问题。

参考文献：

[1] RODRIGUES T K, SUTO K, KATO N. Edge cloud server deployment with transmission power control through machine learning for 6G Internet of things[J]. IEEE Transactions on Emerging Topics in Computing, 2021, 9(4): 2099-2108.

[2] MCMAHAN B, MOORE E, RAMAGE D, et al. Communication-efficient learning of deep networks from decentralized data[C]//Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS). Piscataway: IEEE Press, 2017: 1273-1282.

[3] LI K J, XIAO C H. CBFL: a communication-efficient federated learning framework from data redundancy perspective[J]. IEEE Systems Journal, 2022, 16(4): 5572-5583.

[4] SATTLER F, WIEDEMANN S, MÜLLER K R, et al. Robust and communication-efficient federated learning from non-i.i.d. data[J]. IEEE Transactions on Neural Networks and Learning Systems, 2019, 31(9): 3400-3413.

[5] LI K J, XIAO C H. PBFL: communication-efficient federated learning via parameter predicting[J]. The Computer Journal, 2023, 66(3): 626-642.

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

[7] LI T, SAHU A K, TALWALKAR A, et al. Federated learning: challenges, methods, and future directions[J]. IEEE Signal Processing Magazine, 2020, 37(3): 50-60.

[8] LI K J, XIAO C H. Federated learning communication-efficiency framework via corset construction[J]. Computer Journal, 2022, doi: 10.1093/comjnl/bxac062.

[9] TELLEZ D, LITJENS G, LAAK J, et al. Neural image compression for gigapixel histopathology image analysis[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2021, 43(2): 567-578.

[10] LI X, HUANG K X, YANG W H, et al. On the convergence of FedAvg on Non-IID data[C]//Proceedings of the International Conference on Learning Representations (ICLR). Piscataway: IEEE Press, 2020: 1-26.

[11] TAO Z, LI Q. eSGD: communication efficient distributed deep learning on the edge[C]//2018 Hot Topics in Edge Computing (HotEdge 18). Piscataway: IEEE Press, 2018: 1-6.

[12] YU H, YANG S, ZHU S H. Parallel restarted SGD with faster convergence and less communication: demystifying why model averaging works for deep learning[C]//Proceedings of the AAAI Conference on Artificial Intelligence. Palo Alto: AAAI Press, 2019: 5693-5700.

[13] XU J J, DU W L, JIN Y C, et al. Ternary compression for communication-efficient federated learning[J]. IEEE Transactions on Neural Networks and Learning Systems, 2022, 33(3): 1162-1176.

[14] LI S Q, QI Q, WANG J Y, et al. GGS: general gradient sparsification for federated learning in edge computing[C]//Proceedings of 2020 IEEE International Conference on Communications (ICC). Piscataway:

IEEE Press, 2020: 1-7.

[15] HAN P C, WANG S Q, LEUNG K K. Adaptive gradient sparsification for efficient federated learning: an online learning approach[C]// Proceedings of 2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS). Piscataway: IEEE Press, 2021: 300-310.

[16] OZFATURA E, OZFATURA K, GÜNDÜZ D. Time-correlated sparsification for communication-efficient federated learning[C]// Proceedings of 2021 IEEE International Symposium on Information Theory (ISIT). Piscataway: IEEE Press, 2021: 461-466.

[17] ASAD M, MOUSTAFA A, ITO T. FedOpt: towards communication efficiency and privacy preservation in federated learning[J]. Applied Sciences, 2020, 10(8): 2864.

[18] BERNSTEIN J, WANG Y, AZIZZADENESHELI K, et al. signSGD: compressed optimisation for non-convex problems[C]//Proceedings of the 35th International Conference on Machine Learning. Piscataway: IEEE Press, 2018: 560-569.

[19] REISIZADEH A, MOKHTARI A, HASSANI H, et al. FedPAQ: a communication-efficient federated learning method with periodic averaging and quantization[C]//Proceedings of the 23rdInternational Conference on Artificial Intelligence and Statistics (AISTATS). Piscataway: IEEE Press, 2020: 2021-2031.

[20] AMIRI M M, GUNDUZ D, KULKARNI S R, et al. Federated learning with quantized global model updates[J]. arXiv Preprint, arXiv: 2020.10672, 2020.

[21] NORI M K, YUN S, KIM I M. Fast federated learning by balancing communication trade-offs[J]. IEEE Transactions on Communications, 2021, 69(8): 5168-5182.

[22] JHUNJHUNWALA D, GADHIKAR A, JOSHI G, et al. Adaptive quantization of model updates for communication-efficient federated learning[C]//Proceedings of 2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). Piscataway: IEEE Press, 2021: 3110-3114.

[23] DU Y, YANG S, HUANG H. High-dimensional stochastic gradient quantization for communication-efficient edge learning[C]//Proceed ings of 2019 IEEE Global Conference on Signal and Information Processing (Global SIP). Piscataway: IEEE Press, 2019: 1-5.

[24] LIAN Z, CAO Z, ZUO Y, et al. AGQFL: communication-efficient federated learning via automatic gradient quantization in edge heterogeneous systems[C]//Proceedings of 2021 IEEE 39th International Conference on Computer Design (ICCD). Piscataway: IEEE Press, 2021: 551-558.

[25] BĀDOIU M, HAR-PELED S, INDYK P. Approximate clustering via core-sets[C]//Proceedings of the 34th Annual ACM Symposium on Theory of Computing. New York: ACM Press, 2002: 250-257.

[26] VLADIMIR B, DAN F, HARRY L, et al. Efficient coreset constructions via sensitivity sampling[C]//Proceedings of the 13th Asian Conference on Machine Learning. Piscataway: IEEE Press, 2021: 948-963.

[27] LU H L, LI M J, HE T, et al. Robust coreset construction for distributed machine learning[J]. IEEE Journal on Selected Areas in Communications, 2020, 38(10): 2400-2417.

[28] CAMPBELL T, BRODERICK T. Bayesian coreset construction via greedy iterative geodesic ascent[C]//Proceedings of the 35th International Conference on Machine Learning. Piscataway: IEEE Press, 2018: 698-706.

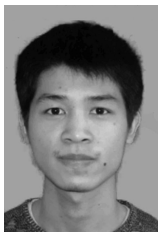
[29] FAN Y W, LI H S. Communication efficient coreset sampling for distributed learning[C]//Proceedings of 2018 IEEE 19th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC). Piscataway: IEEE Press, 2018: 1-5.

[30] MOCANU D C, MOCANU E, STONE P, et al. Scalable training of artificial neural networks with adaptive sparse connectivity inspired by network science[J]. Nature Communications, 2018, 9: 2383.

[31] LI A, SUN J, WANG B, et al. LotteryFL: personalized and communication-efficient federated learning with lottery ticket hypothesis on non-IID datasets[J]. arXiv Preprint, arXiv: 2008.03371, 2020.

[作者简介]

李开菊（1992– ），女，土家族，湖北恩施人，重庆大学博士生，主要研究方向为联邦学习、隐私保护。



许强（1992– ），男，江西赣州人，博士，香港城市大学在站博士后，主要研究方向为视频安全、图像处理等。

王豪（1990– ），男，河南驻马店人，博士，重庆邮电大学副教授，主要研究方向为联邦学习、隐私保护。