基于联邦学习的多源异构网络无数据融合方法

段昕汝，陈桂茸，姬伟峰，申秀雨
（空军工程大学信息与导航学院，西安，710077）

摘要　在联合作战体系中，数据作为基础性战略资源发挥着重要的底层支撑作用，数据妥善管理和高效利用是推动作战能力整体跃迁和作战样式深度变革的重要动力。为实现不同作战系统间信息的互联互通，提出一种基于联邦学习的多源异构网络无数据融合方法。从多源数据融合面临的安全性和异构性问题出发，利用条件生成对抗网络提取本地知识和全局分布，集成数据信息；结合局部教师模型-全局模型架构，以无数据知识蒸馏的方式对局部模型知识进行迁移，融合异构网络，细化全局模型，实现不同系统间安全、高质量的信息交互，为智能化指挥信息系统建设提供技术支撑。实验结果表明：该方法在结构化数据和图像数据上具有可行性，整体准确率可达到 80％以上。

关键词　信息安全互联；联邦学习；网络融合；条件生成对抗网络；知识蒸馏
DOI　10.3969/j.issn.2097-1915.2024.01.014
中图分类号　TP391　　**文献标志码**　A　　**文章编号**　2097-1915(2024)01-0090-08

A Multi-Source Heterogeneous Network Compression without Data

DUAN Xinru, CHEN Guirong, JI Weifeng, SHEN Xiuyu
(Information and Navigation School, Air Force Engineering University, Xi'an 710077, China)

Abstract　Data serving as a basic strategic resource is playing an important underpinning role in joint combat system. The proper management and efficient use of data are an important driving force in promoting the overall transformation of combat capability and the deep transformation of combat style. In order to realize the information interconnection between different combat systems, a multi-source heterogeneous network data fusion method is proposed based on the federated learning. In view of the security and heterogeneity of multi-source data, the conditional generation adversarial network is utilized for extracting local knowledge and global distribution, and integrating data information. In combination with the local teacher model-global model architecture, the local model knowledge is transferred by distillation of knowledge without data, the heterogeneous network is fused, and the global model is refined to realize safe and high-quality information interaction between different systems, providing technical support for the construction of intelligent command information system. The experimental results show that the proposed method is feasible on structural data sets and image data sets, and the overall accuracy can be more than 80％.

Key words　information security interconnection; federated learning; network convergence; conditional generation adversarial network; knowledge distillation

收稿日期：2023-04-26
基金项目：国家自然科学基金(62301600)
作者简介：段昕汝(1997－)，女，陕西西安人，硕士生，研究方向为人工智能信息安全。E-mail:Duanxinru2021@163.com

引用格式：*段昕汝，陈桂茸，姬伟峰，等. 基于联邦学习的多源异构网络无数据融合方法[J]. 空军工程大学学报，2024，25(1)：90-97. DUAN Xinru, CHEN Guirong, JI Weifeng, et al. A Multi-Source Heterogeneous Network Compression without Data[J]. Journal of Air Force Engineering University, 2024, 25(1): 90-97.*

随着云计算、大数据、物联网、无人技术等为代表的现代信息技术在军事领域的广泛应用，未来战争呈现信息化、智能化、协同化发展趋势，联合作战成为打赢现代和未来战争的必然要求。在联合作战体系中，数据作为支撑高效指挥决策的战略资源，发挥着重要的底层支撑作用，数据妥善管理和高效利用成为推动作战能力整体跃迁和作战样式深度变革的重要动力。实现不同作战系统间的数据安全互联对进一步发挥数据资源在指挥决策中的支撑作用，实现高速计算、存储、检索的智能数据融合体系，构建大数据驱动的智能化模型，对加快推进智能化复杂网络信息系统建设、助力军事智能化发展具有重要意义。

由于前期系统建设的阶段性和独立性，以及战略目的的针对性，不同系统间隔离程度较高，数据孤岛成为军事数据建设的关键掣肘因素。军事数据的特殊战略性地位，使得大数据在军事领域的应用如同双刃剑，在加快国防军队现代化的同时也要充分考虑信息化过程中隐藏的信息泄露的风险[1-2]。

现有研究依托于“网-端-云”结构理论结合统一体系结构框架方法，对后勤与装备保障指挥信息系统进行建模，建立全域联通的信息网，然而这种大规模通信网络并不能满足对于安全需求较高的重要数据交互业务[3]。基于区块链的军事数据安全治理方法实现数据的安全共享，并对交互过程执行访问控制[4]，然而在实现了高质量的数据安全同时也受到区块链技术特性的限制，对于大数据业务交互效率较低。文献[5]结合联邦学习技术在联合作战场景下的应用进行分析建模，通过联邦学习跨域安全互联方法帮助不同作战域进行信息整合，保障数据安全的前提下充分利用保存在各作战域的数据资源，进而安全可靠的实施作战任务协同，然而该方法尚未充分考虑数据结构、特征、分布的差异性。

本文基于联邦学习技术开展进一步研究，提出多源异构网络无数据融合方法，从交互媒介层面对传统方法进行改进，弱化其对于局部模型和全局模型间的同构需求，同时已无数据方式知识迁移，保持对模型结构的不完全可知，一定程度上遏制了系统中的不安全因素。

1　相关工作

1.1　联邦学习

联邦学习（federated learning，FL）这一技术概念由 Google 公司首先提出并用于分布式语言模型的训练中以保护用户原始数据安全与隐私，在不共享原始数据的情况下通过模型梯度的周期性交互完成协同训练（见图 1），利用 FedAvg 算法最小化全局目标函数优化模型（见式(1)），解决了大规模分布式训练网络中的数据交互需求和隐私问题，同时实现了计算资源和数据分散化[6]。

$$\min f(\omega)=\frac{1}{n}\sum_{i=1}^{n}f_i(\omega) \tag{1}$$

式中：n 为参与训练的客户端总数；$f(\omega)$为全局目标函数；$f_i(\omega)=\ell(x_i,y_i;\omega)$表示局部参数化模型的损失函数。

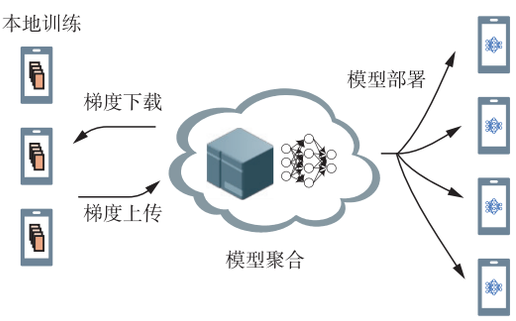


图 1　移动终端上的联邦学习方法原理

为进一步适应不同系统和数据分布的异构性，Li 等人改进的 FedProx 算法允许在不同的设备之间局部执行不同数量的工作，并在局部子问题上添加一个近端项以限制变量局部更新的影响[7]。如式(2)所示：

$$\omega_i^{t+1}\leftarrow F_i(\omega_i)+\frac{\mu}{2}\|\omega_i-\omega_i^t\|_2 \tag{2}$$

式中：ω_i 为第 i 个客户端的局部参数化模型；$F_i(\omega_i)$为对应的损失函数。

以上方法在模型更新上具有相似的原理，均采用了梯度平均的思想，通过聚合边缘节点上传的局部模型梯度实现全局模型的训练，此类方法要求各局部模型完全同构，一定程度上限制了模型对于本地数据的适应性。为解决联邦学习中跨设备数据集的非独立同分布（Non-IID）问题，Jeong 等[8]首次提出了联邦蒸馏（federated distillation，FD）的思想，打破了基于更新梯度传统方法，以模型输出代替模型梯度进行交互。Seo 等[9]设计了一种交换模型输出的分布式框架，从局部模型中提取 logit 输出向量的统计量，并以元数据形式进行共享，提取局部模型知识同时提高了模型的通信效率。

知识蒸馏（knowledge distillation，KD）可在神经网络模型之间传递知识[10-11]。区别于标准神经网络通过匹配样本的预测与真实标签进而优化模型

参数，知识蒸馏利用转移集，通过匹配教师模型与学生模型的软间隔优化模型，将教师模型中的规律传递到学生模型上来改善模型性能。该方法不强调教师模型和学生模型之间同构，将其与联邦学习相结合可以在保障本地数据安全的同时满足多源网络的异构性[12-16]。

1.2 生成对抗网络

生成对抗网络（generative adversarial network，GAN）是一种基于零和博弈理论的生成式模型，该模型由 2 个同时训练的模型构成，即生成器 G 和鉴别器 D，通过 2 个模型的动态博弈训练网络模型其达到纳什均衡，具体结构见图 2。近年来这一技术不断进化，在数据增广、迁移学习等领域展现出了巨大的潜力，在军事领域具有广阔的应用前景[17]。

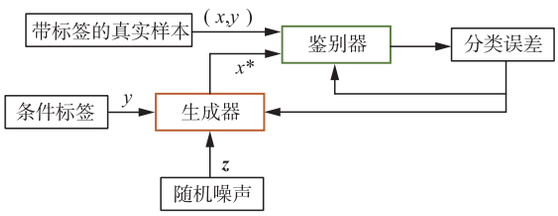


图 2 条件生成对抗网络结构图

条件生成对抗网络（conditional generative adversarial network，CGAN）[18]在 GAN 基础上添加了条件标签 y，其结构见图 2。生成器使用噪声向量 $\boldsymbol{z}$ 和条件标签 y 合成一个伪样本 $x*$，鉴别器接收带标签的真实样本 (x,y) 及带生成标签的伪样本 $(x*|y,y)$，利用真实样本－标签对训练鉴别器完成识别配对，同时利用伪样本-标签对学习识别伪样本并与真实样本区分开来，其目标函数为：

$$\min_G \max_D V(D,G)=E_{x\sim p(x)}[\log D(x|y)]+E_{z\sim p(z)}[\log(1-D(G(\boldsymbol{z}|y)))] \tag{3}$$

CGAN 用于样本增强可以在不依赖先验假设的情况下实现数据复杂分布特征的学习，生成与原始数据分布相似的高质量样本，通过扩充数据集提升模型在现有样本上的识别率。Lee 等[19]利用 CGAN 实现了虹膜图像数据增强，并使用这种增强方法提高了识别性能，缓解了神经网络训练中缺少标记样本的问题，解决了生物特征隐私问题。Souibgui 等[20]针对文档退化导致的读取困难问题，提出了一种有效的文档增强生成对抗网络（DE-GAN），使用 CGANs 来恢复严重退化的文档图像，生成高质量的降级文档。Yang 等[21]对于噪声鲁棒语音识别问题，利用 CGAN 实现音频数据增强，提高在噪声环境下的语音识别能力。Roheda 等[22]提出使用 CGAN 从传感器数据中提取知识，并增强低分辨率的目标检测。

2 基于联邦学习的信息交互方法

2.1 问题分析

信息化战争制胜的关键在于能否及时有效地对海量作战数据进行整合，将信息优势转化为作战优势。在联合作战场景中，样本数据来源广泛、特征迥异且具有战略特殊性，整合时需要重点考虑以下问题：

1）系统安全性。在进行信息融合的过程中通常涉及多个作战域的信息交互，作战数据中可能包含关键战略信息，此类数据在使用时需全面考虑交互过程中存在的安全风险，在保证数据安全的情况下对数据资源进行合理、高效、充分的利用。

2）数据异构性。用于训练的各单位数据往往普遍存在异构性。首先，全局数据与局部数据分布存在差异，即 $P_k \neq P_{\text{joint}}$，用户 k 的损失函数的期望可能不满足 $E_{Pk}[F_k(\omega)]=f(\omega)$，导致直接全局共享模型可能比单独训练私有数据的本地模型表现差；其次，各单位数据规模存在不平衡问题，基于数据安全设定，系统中的各单位不直接进行数据交互，可能导致收敛缓慢、全局模型飘移等问题。

3）目标差异性。针对不同的本地数据表示、不同的硬件能力、不同的任务，各作战域设计模型的目标和提取结构可能存在较大差异。其中服务器的目标是适合 $P_{\text{joint}}(x,y)$ 的广义模型，而客户端的目标是适合 $P_k(x,y)$ 的个性化模型，可能存在更新对联合模型训练有害但对本地模型有益的情况，因此基于本地数据训练单一可用的模型对各单位具体情况缺乏适用性。

2.2 联邦学习系统模型

为了解决以上问题，本文深入分析了联邦学习系统框架及模型训练流程，并从以下 2 个维度加以改进：

1）联邦学习机制中的信息交互介质。现有方法大多基于模型梯度完成信息共享，通过数学运算完成对局部模型的聚合。本文通过加密共享本地服务器上训练的完整网络模型，同时限制聚合时对局部网络结构的可知性。

2）联邦学习的聚合方法。通过局部教师模型-全局模型的架构对局部模型知识进行提取，允许局部模型与全局模型之间的差异性，允许各单位针对

性细化模型及训练算法，独立地训练个性化模型，并利用局部模型的集成知识丰富全局模型，缓解局部模型中由异构性引起的模型漂移，细化全局模型。

本文考虑了典型的联邦学习设置，即包括一个聚合服务器和 N 个持有本地数据集的私有域，这些本地数据集共享相同的特征空间且样本不重叠。在不进行数据互通前提下协同训练模型实现信息交互，基于联邦学习系统模型见图 3。

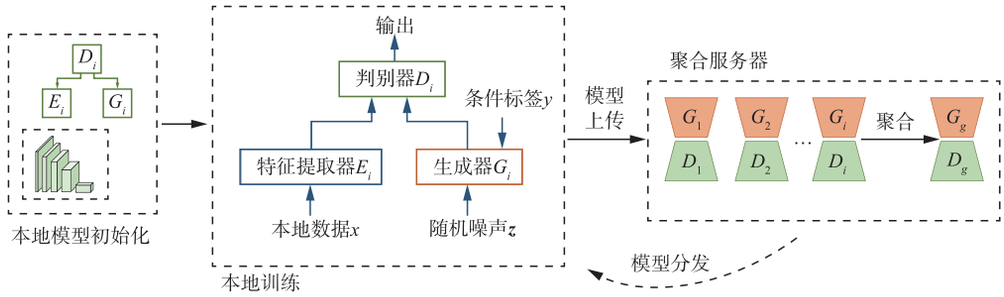


图 3　总体框架

具体来说，为了保证数据的安全性，在进行模型训练时通过设置一个私有特征提取器对原始数据进行特征提取，从而避免模型直接接触原始数据，保护源数据的隐私，进而保证了源数据在系统内的安全性。通过特征提取减少数据的维度，去除冗余信息，同时保留数据的重要特征，从而提高模型的精度和效率。其次，通过联合训练一个轻量级生成器，以无数据的方式集成用户信息，作为归纳偏差来调节局部数据并转移知识，以获得更好的收敛性能，缓解数据的异构性。最后利用知识蒸馏的方法进行模型聚合，将局部教师模型的知识转移到全局模型中，允许多个教师模型之间异构，即不同类型的模型可以参与知识蒸馏，从而实现在保证模型准确性的同时提高模型的效率和对局部目标的适用性。

3　多源异构网络无数据融合方法

3.1　符号定义

D 为所有数据样本的集合，X 为数据集中所包含的特征集合，Y 为样本 X 对应的标签集，D_k 为本地客户端数据子集，其中 $k\in K$，K 为参与训练的客户端集合。$X\subset\mathbb{R}^d$ 表示数据集 D 中的样本对应特征空间，$Z\subset\mathbb{R}^c$ 表示潜在空间，其中 $c<d$，$Y\subset\mathbb{R}$ 输出空间。

CGAN 参数化模型 (θ^G,θ^D)，其中 θ^G 为生成器 $G(z,y)=x^*\mid y,\theta^D$ 为判别器 $D(x^*\mid y,x)$。

在教师-学生架构中，ω_k 为教师模型，ω 为学生模型，D_t 为知识蒸馏转移集。

3.2　联邦无数据蒸馏算法

本算法通过训练 CGAN 网络提取关于数据分布的全局视图，向本地用户传达多方共识知识，指导局部模型的训练，并从给定的教师网络中生成图像，通过局部教师模型-全局模型的框架对各单位异构网络的知识进行迁移以训练全局模型。具体的算法如表 1 所示。

表 1　联邦无数据蒸馏算法(FedND)流程

初始化：全局模型 N_ω，本地模型 $\{N_{\omega_k}\}_{k=1}^K$，CGAN 模型 (θ^G,θ^D)，学习率 α,β

服务器随机选择参与本轮训练的单位 A，广播参数 (θ^G,θ^D)

模块 1：训练 CGAN 模型

for epoch **do**

　for k in K **do**

　　从训练集中随机抽取真实样本 x；

　　随机生成噪声向量 z，$x^*\leftarrow G(z,y)$；

　　用鉴别网络进行分类 $D(x^*\mid y,x)$；

　　计算分类误差并反向传播更新 (θ_k^G,θ_k^D)；

　　$\theta_k^G\leftarrow\theta_k^G-\alpha\nabla J(\theta_k^G,\theta_k^D)$

　　$\theta_k^D\leftarrow\theta_k^D-\alpha\nabla J(\theta_k^G,\theta_k^D)$

$\bar{\mathscr{L}}(\theta^G)=\min\frac{1}{K}\sum_{k=1}^K\bar{\mathscr{L}}_k(\theta_k^G)$

模块 2：训练全局模型

随机生成一组噪声向量 z，利用生成网络合成转移集 D_t $\leftarrow G(z,y)$

for k **do**

　在小批量转移集 D_t 上使用教师模型和学生模型：

　$\{p_k\leftarrow N_{\omega_k}[G(z,y)]\}_{k=1}^K$

　$p_{\text{global}}\leftarrow N_\omega[G(z,y)]$

计算知识蒸馏损失：

$\mathscr{L}_{\text{global}}=\mathscr{L}(y,\hat{y})+D_{KL}(\frac{1}{K}\sum_{k=1}^K p_k\,||\,p_{\text{global}})$

更新全局模型 $\omega\leftarrow\omega-\beta\nabla J(\omega)$

首先由中央服务器初始化并广播 CGAN 参数化模型，并由各客户端基于可用的本地数据训练 CGAN 网络使其达到纳什平衡。其目标函数：

$$\min_{G_k}\max_{D_k}V(G,D)=E_{x\sim p_k(x)}\{\log[D(x\mid y)]\}+E_{z\sim p_k(z)}\{\log[1-D(G(z\mid y))]\}\tag{4}$$

中央服务器利用各单位学习到的生成器以聚合

来自不同本地客户端的信息，计算全局最小化损失拟合局部模型使模型的损失降到最低。并通过训练生成网络，利用其潜在空间恢复一个诱导分布 $G^*:Y\to Z$（见式(5)）以缓解训练过程中的相关数据安全问题。

$$G^*=\underset{G:Y\to Z}{\operatorname{argmax}}E_{y\sim p(y)}\cdot E_{z\sim G(z|y)}\left[\frac{1}{K}\sum_{k=1}^{K}\log p(y\mid z;\theta_k^G)\right] \tag{5}$$

学习一个参数化条件生成器 θ^G 提取知识以优化以下目标：

$$\min_{\theta^G}J(\theta^G):=E_{y\sim p(y)}\cdot E_{z\sim G(z|y)}\left[l\left(\sigma\left(\frac{1}{K}\sum_{k=1}^{K}g(z\mid y;\theta_k^G),y\right)\right)\right] \tag{6}$$

式中：$g(\cdot)$ 和 $\sigma(\cdot)$ 是 logit 输出和激活函数。给定任意的目标标签 y，生成器可以产生特征 $z\sim G(\cdot\mid y)$。从用户模型的集合中诱导理想的预测，这与来自全局视图的用户数据是一致的。

局部设备利用生成器聚合知识识别出本地数据样本中缺少的目标标签，基于目标标签生成与全局数据分布相似的高质量样本，以实现样本增强直至满足 IID 特性，使全局数据分布 P_{joint} 与局部数据分布 P_k 满足 $P_k=P_{\text{joint}}$（见图 4）。

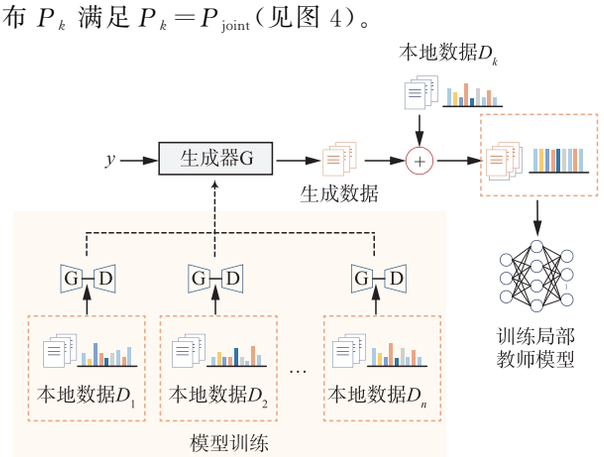


图 4 数据增强

其次，通过局部教师模型-全局模型的框架，利用生成器生成转移集 D_t 蒸馏细化全局模型（见图 5），最小化教师模型和学生模型 softmax 层对应输出向量的差距，具体计算方式如下：

$$\min_{\omega}E_{x^*\sim D_t}\{D_{KL}[\sigma\left(\frac{1}{K}\sum_{k=1}^{K}g(G(x^*\mid y),\omega_k)\right)\parallel \sigma(g((G(x^*\mid y),\omega))]\} \tag{7}$$

在计算损失 $\mathcal{L}(y,\hat{y})$ 时，本文使用了 Kullback-Leibler 散度来衡量教师模型 ω_k 和学生模型 ω 的最小化对数输出之间的差异，计算教师模型与学生模型之间的损失：

$$D_{KL}(\frac{1}{K}\sum_{k=1}^{K}p_k\parallel p_{\text{global}})=\sum_{i=1}^{n}\left\{\log\left[\frac{1}{K}\sum_{k=1}^{K}p_k(x_i)\right]-\log p_{\text{global}}(x_i)\right\} \tag{8}$$

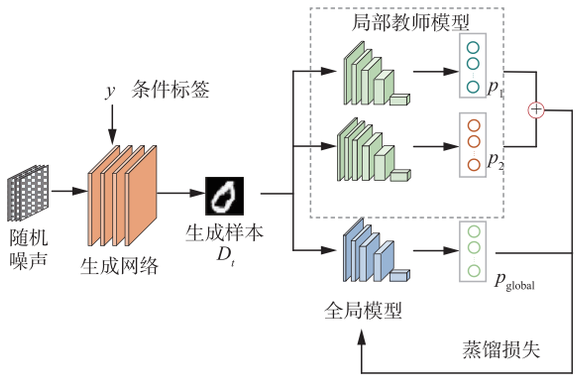


图 5 联邦无数据蒸馏聚合

与现有方法相比，本文方法具有以下优点：

1）将局部模型的训练从全局中解耦出来，以便根据局部目标调整训练算法与网络模型结构，允许多个数据源针对性训练局部模型；

2）利用教师-全局模型架构提取知识而不是直接对局部模型参数进项加权平均，允许对局部训练算法和模型结构保持一定的不可知性；

3）利用 CGAN 实现数据增强，提高模型训练效率和收敛速度，减小通信开销。

4）使用无数据融合的方法，用生成数据代替本地小批量样本作为转移集，保证了本地数据源的安全性。

4 实验及分析

4.1 数据集及实验设置

实验选取了不同数据集用以验证方法的有效性，包含广泛用于机器学习任务研究和评估的 MNIST、EMNIST、CELEBA 数据集和真实 FOQA 数据集。其中，MNIST 数据集包含了 70 000 个灰度图像样本，每个样本的维度为 28 像素×28 像素，对应 10 类样本标签；EMNIST 数据集是基于 MNIST 数据集扩展而来的一个数据集，包含大写字母、小写字母、数字和符号等 6 类样本；CELEBA 数据集包含 10 177 个名人身份的 202 599 张图片样本，并且都做好了特征标记，每个图像都附带了 40 个不同的属性标签。FOQA 数据集是 NASA 研究团队开源的真实数据集，包括 99 837 个不同航线的样本数据，对应 4 类标签，每个数据样本为 160×20 维。

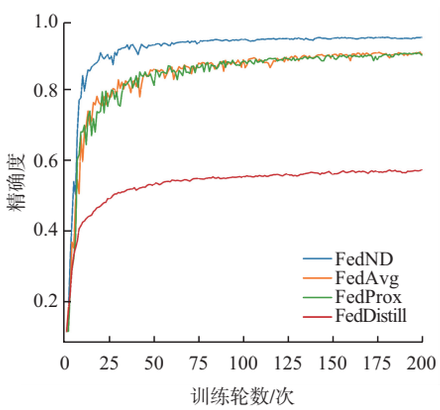
实验基于中心化的系统架构开展，包括 1 个聚合服务器和 20 个边缘训练节点，将训练集和测试集分成 20 组分发至不同的模拟边缘训练节点，以还原实际应用场景中不同节点间数据相互隔离的设定。实验设置了 200 轮迭代，并对所有边缘节点使用相同的超参进行设置，批处理大小 epochs 为 32，学习率 η 为 0.01，优化器为 Adam，蒸馏温度参数为 10。

为了验证本方法的有效性及可用性，实验结合卷积神经网络将本文的 FedND 算法与 FedAvg 算法[6]、FedProx 算法[7]、FedDistill 算法[8]性能进行对比，并采用如下指标对实验结果进行评估：①准确率 accuracy：分类正确的样本占全部测试样本的比例；②模型损失 loss：衡量全局模型的预测结果与真实标签之间的差异程度，记录全局模型的损失函数变化趋势。

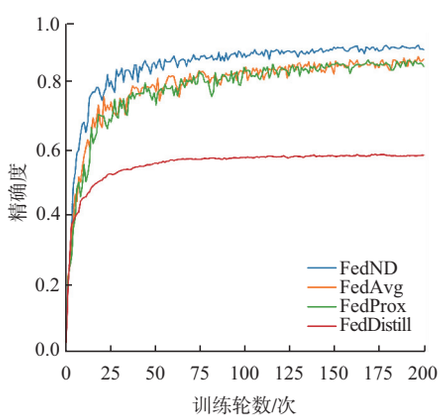
4.2　实验结果及分析

首先验证算法对于异构样本的有效性。对于 MNIST 和 EMNIST 数据集，本文使用 dirichlet 函数将数据集划分为 20 组，通过调整 Dirichlet 分布参数来控制生成的每组分配的样本数，使得每个数据子集的样本分布不同，满足数据异构性设定，并用于训练本地模型；对于 CELEBA 数据集，随机将属于不同名人的图片聚集成不相交的组来增加了数据的异构性；对于 FOQA 数据集，随机划分不同样本数据来表现数据子集的异构性。

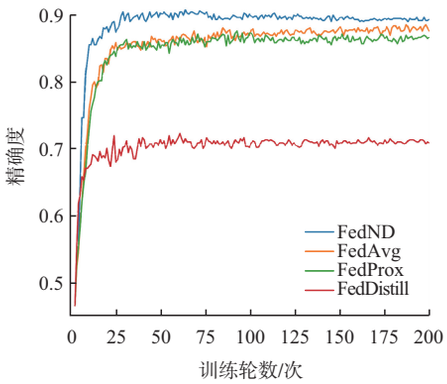
在 4 个数据集上不同算法下模型训练收敛过程对比见图 6，实验结果显示，在迭代轮数小于 200 时本算法能够更快地进行学习使全局模型收敛，且从模型精度上来看本方法略优于其他 3 个对照组。图中结果表明了在相同的条件下，本方法以更小的通信轮数达到更优的训练效果，减小了模型收敛所需的交互次数，从而减少实际应用中的通信开销和信息暴露面。



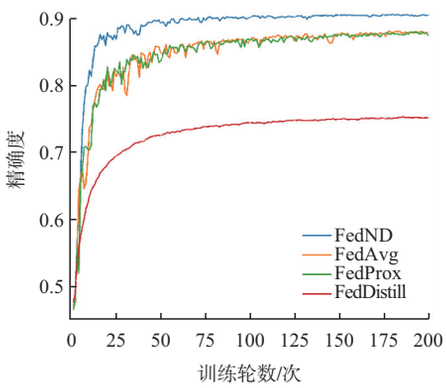
（a）MNIST



（b）EMNIST



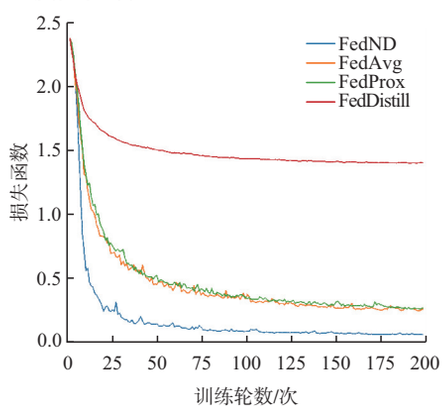
（c）CELEBA



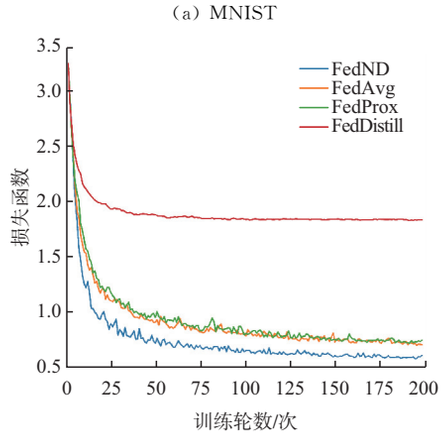
（d）FOQA

图 6　不同数据集上各算法模型准确率

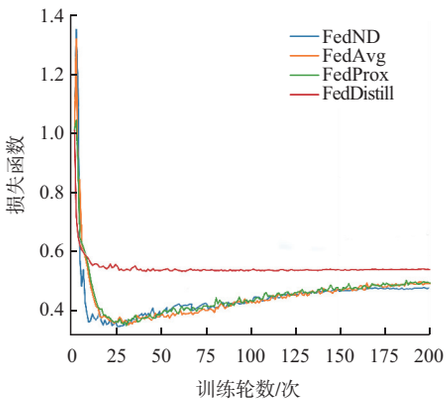
图 7 给出了不同算法下模型训练过程的损失对比，可以看出，随着迭代轮数的增加，FedND 在实验数据集上损失更低。



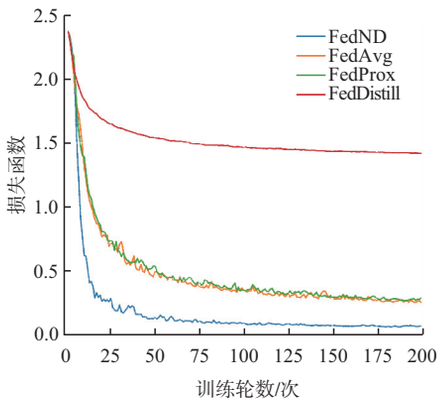
（a）MNIST



（b）EMNIST



(c) CELEBA



(d) FOQA

图 7 不同数据集上各算法模型损失

为进一步探讨数据异构性对模型精度的影响，本文利用 MNIST 和 EMNIST 数据集开展进一步验证。利用 numpy 库中的 Dirichlet 分布函数对数据子集的异构性程度进行量化，通过设置超参数 α 的值控制分布的形状，进而验证本方法下数据分布的异构程度与模型精度之间的关系。实验结果如表 2 所示，其中 α 值越大表示数据子集间的分布异构性越弱；α 值越小则概率分布更分散，数据子集间的分布异构性越强。首先实验结果表明，在同样的超参数条件下本文所提出的方法在模型精度上略高于其他对照组。其次，实验结果反映了数据异构性对模型性能的影响：FedND 对不同量级的异构性具有鲁棒性，特别是当数据分布高度异构时，本方法对全局模型的增益效果更为显著。

表 2 MNIST 和 EMNIST 数据集上的模型精度

算法	MNIST				EMNIST			
	$\alpha=0.1$	$\alpha=0.3$	$\alpha=0.5$	$\alpha=1.0$	$\alpha=0.1$	$\alpha=0.3$	$\alpha=0.5$	$\alpha=1.0$
FedAvg	0.900 63	0.927 31	0.945 58	0.948 76	0.895 26	0.912 56	0.935 12	0.941 15
FedProx	0.897 04	0.936 58	0.944 26	0.956 13	0.875 12	0.924 52	0.933 25	0.941 24
FedDistill	0.576 16	0.617 08	0.663 68	0.676 21	0.524 66	0.564 48	0.612 78	0.642 89
FedND	0.947 02	0.961 97	0.965 56	0.966 32	0.914 28	0.921 51	0.934 42	0.942 55

5 结语

本文提出了一种基于联邦学习的多源异构网络无数据融合方法，在传统的联邦优化算法的基础上加以改进，引入知识蒸馏用于解决各单位普遍存在的数据异构性问题，同时使用聚合知识细化服务器模型代替直接聚合的模型参数，强化了联邦学习系统的安全性，通过保持聚合服务器对局部模型的不可知性，减少安全风险保护代理数据；利用 CGAN 网络集成代理信息和数据成分布知识调节模型训练，实现不依赖于任何外部数据模型知识蒸馏。通过基于 MNIST 数据集和 CELEBA 数据集验证了方法的有效性，实验结果表明，对比于其他 3 种联邦学习算法，本文方法可以使用更少聚合轮数达到更好的效果，在收敛速度和模型精度上优于现有的联邦学习算法，可以有效减少边缘服务器和中央服务器之间的通信。

参考文献

[1] 李增华，蒋玉娇，臧雪珺，等. 美军数据建设发展路径研究[J]. 中国电子科学研究院学报，2021，16(7)：710-715，721.

[2] 高强，游宏梁，汤珊红，等. 军事数据治理概念与框架研究[J]. 情报理论与实践，2019，42(12)：55-59.

[3] 刘婧婷，郭继坤，邵芳. 基于统一体系结构框架的战区联合作战后勤与装备保障指挥信息系统架构[J]. 兵工学报，2021，42(2)：408-421.

[4] 易卓，叶军，张国超. 基于区块链的军事数据安全治理框架[J]. 信息安全与通信保密，2022(2)：81-90.

[5] 王蒙蒙，朱婉婷. 面向联合作战的跨域数据安全互联方法[J]. 中国电子科学研究院学报，2020，15(5)：442-448.

[6] MCMAHAN H B，MOORE E，RAMAGE D，et al. Federated Learning of Deep Networks Using Model Averaging [Z]. ARXiv Preprint ARXiv：1602.05629，2016.

[7] LI T，SAHU A K，ZAHEER M，et al. Federated Optimization in Heterogeneous Networks[J]. Proceedings of Machine Learning and Systems，2020(2)：429-450.

[8] JEONG E，OH S，KIM H，et al. Communication-Efficient on-Device Machine Learning：Federated Distillation and Augmentation under Non-Iid Private Data [Z]. ArXiv Preprint ArXiv：1811.11479，2018.

[9] SEO H，PARK J，OH S，et al. Federated Knowledge Distillation[J]. Machine Learning and Wireless

Communications，2022：457.

[10] HINTON G，VINYALS O，DEAN J. Distilling the Knowledge in a Neural Network[J]. ArXiv Preprint ArXiv：1503.02531，2015.

[11] 黄震华，杨顺志，林威，等. 知识蒸馏研究综述[J]. 计算机学报，2022，45(3)：624-653.

[12] CHEN H，GUO T，XU C，et al. Learning Student Networks in the Wild[C]//Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. Piscataway：IEEE，2021：6428-6437.

[13] WANG C，YANG G，PAPANASTASIOU G，et al. Industrial Cyber-Physical Systems-Based Cloud IoT Edge for Federated Heterogeneous Distillation[J]. IEEE Transactions on Industrial Informatics，2020，17(8)：5511-5521.

[14] LEE G，SHIN Y，JEONG M，et al. Preservation of the Global Knowledge by Not-True Self Knowledge Distillation in Federated Learning[Z]. ArXiv Preprint ArXiv：2106.03097，2021.

[15] ZHANG Y，CHEN H，CHEN X，et al. Data-Free Knowledge Distillation for Image Super-Resolution[C]//Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. Piscataway：IEEE，2021：7852-7861.

[16] ZHU Z，HONG J，ZHOU J. Data-Free Knowledge Distillation for Heterogeneous Federated Learning[C]//International Conference on Machine Learning. New York：PMLR，2021：12878-12889.

[17] 罗玲，李民. 应重视“生成对抗网络”技术[N]. 解放军报，2019-11-29(11).

[18] MIRZA M，OSINDERO S. Conditional Generative Adversarial Nets[Z]. ArXiv Preprint ArXiv：1411.1784，2014.

[19] LEE M B，KIM Y H，PARK K R. Conditional Generative Adversarial Network-Based Data Augmentation for Enhancement of Iris Recognition Accuracy[J]. IEEE Access，2019(7)：122134-122152.

[20] SOUIBGUI M A，KESSENTINI Y. DE-GAN：A Conditional Generative Adversarial Network for Document Enhancement[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence，2020，44(3)：1180-1191.

[21] SHENG P，YANG Z，HU H，et al. Data Augmentation Using Conditional Generative Adversarial Networks for Robust Speech Recognition[C]//2018 11th International Symposium on Chinese Spoken Language Processing (ISCSLP). Piscateway：IEEE，2018：121-125.

[22] ROHEDA S，RIGGAN B S，KRIM H，et al. Cross-Modality Distillation：A Case for Conditional Generative Adversarial Networks[C]//2018 IEEE International Conference on Acoustics，Speech and Signal Processing (ICASSP). Piscateway：IEEE，2018：2926-2930.

（编辑：徐敏）