计算机科学
COMPUTER SCIENCE

结合元学习的去中心化联邦增量学习方法

黄楠, 李冬冬, 姚佳, 王喆

引用本文

黄楠, 李冬冬, 姚佳, 王喆. 结合元学习的去中心化联邦增量学习方法[J]. 计算机科学, 2024, 51(3): 271-279.

HUANG Nan, LI Dongdong, YAO Jia, WANG Zhe. Decentralized Federated Continual Learning Method Combined with Meta-learning [J]. Computer Science, 2024, 51(3): 271-279.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.230100125

结合元学习的去中心化联邦增量学习方法

黄 楠 李冬冬 姚 佳 王 喆
华东理工大学信息科学与工程学院 上海 200237
(ivyhuang1225@outlook.com)

摘 要 针对联邦增量场景中持续学习和数据安全的问题,构建了结合元学习的去中心化联邦增量学习框架。首先,为解决增量场景中持续学习带来的灾难性遗忘问题,提出了结合最近类均值样本回放的增量元学习方法 NMR-cMAML,利用元训练对不同任务流的快速适应进行元更新,得到适用于新旧样本的模型。然后,为解决联邦增量场景中的数据安全问题,设计了基于对等网络架构的去中心化联邦增量学习框架,对等架构中每个客户端采用 NMR-cMAML 对私有的持续任务流进行增量学习。不同于传统的基于服务器-客户端的中心化架构,该去中心化架构采用客户端间通信的策略,消除了传统中央服务器易被攻击的隐患;同时,在联邦通信过程中,通过共享元学习的模型参数实现客户端间知识的有效迁移。最后在图像数据集(Cifar100 和 Imagenet50)上进行了不同任务场景的实验,结果表明所提方法能在提高系统的数据安全性的同时提升客户端本地性能。

关键词:去中心化联邦学习;数据安全;增量学习;元学习
中图分类号 R318;TN911.7

Decentralized Federated Continual Learning Method Combined with Meta-learning

HUANG Nan,LI Dongdong,YAO Jia and WANG Zhe
School of Information Science and Engineering,East China University of Science and Technology,Shanghai 200237,China

Abstract For the problems of continual learning and data security in federated continual scenarios,a decentralized federated continual learning framework combined with meta-learning is constructed. First,in order to solve the problem of catastrophic forgetting in incremental scenarios,an incremental meta-learning method based nearest mean-of-exemplars replaying called NMR-cMAML is proposed. Then,to solve the problem of privacy security in federated continual scenarios,a decentralized federated continual framework based on peer-to-peer network architecture is designed,which is different from the center architecture based on server-client. Each client in the decentralized framework adopts NMR-cMAML to learn the continuous tasks incrementally,and the effective knowledge migration between clients is realized by sharing the meta-learning model in the federal communication process. Finally,experiments are conducted on image data sets(Cifar100 and Imagenet50) to verify that the proposed method improves the data privacy security of the system and improves the local performance of the client.

Keywords Decentralized federated learning,Datasecurity,Continual learning,Meta learning

1 引言

在万物互联的时代,人们在产生不断增长的数据的同时,也越来越注重隐私安全[1]。现实生活中数据来自各个分布式的边缘设备,将庞大的数据集中训练,可以提高模型的准确性和鲁棒性,但是这对云设备的存储和计算力有很高的要求,还有可能带来边缘设备的隐私风险和数据泄露的威胁[2]。每个分布式机构只单独训练它们自己的数据,这可以保护每个边缘设备的数据隐私,但是会大幅降低每个分布式模型的准确性和泛化性[3]。

联邦学习(Federated Learning,FL)的提出实现了在不共享数据的情况下,通过共享系统中边缘设备的本地模型参数来训练得到一个全局模型,每个分布式节点交换的是模型参数或者模型梯度而不是原始数据,以达到保护每个节点数据隐私的目的[4]。当前,大多数的联邦学习方法关注在整个训练过程中保持不变的静态本地数据。然而在真实场景中,每个客户端设备的任务数据源源不断地到来,这无疑给联邦学习带来了困难[5]。一方面,当一个新的任务流到来时,每个客户端都需要基于所有的训练样本重新训练出一个新的模型,以适用于所有任务,这会导致内存的占用和时间的浪费[6];另一方面,当各客户端间的数据是非独立同分布时[7],如果只基于当前新任务的数据进行训练,那么模型梯度将会

到稿日期:2023-01-30 返修日期:2023-06-18
基金项目:上海市科技计划(21511100800);国家自然科学基金(62276098)
This work was supported by the Science and Technology Program of Shanghai(21511100800) and National Natural Science Foundation of China (62276098).
通信作者:李冬冬(ldd@ecust.edu.cn)

偏向新任务，导致对旧任务产生灾难性遗忘问题[8]。

因此，联邦增量学习（Federated Continual Learning，FCL）[9]应运而生，其旨在解决联邦学习中各个客户端针对持续任务流的增量学习问题。目前，对联邦增量学习的研究尚处于初步阶段。2020 年，FedCL[9]提出使用弹性权重回放（Elastic Weight Consolidation，EWC）进行持续的局部训练，利用在服务器的测试集上估计的重要权值矩阵作为指导，减少增量场景下联邦学习中局部模型和全局模型的权值发散。2021 年，FedWeIT[10]将模型参数分解为密集的全局参数和稀疏的任务自适应参数，并在所有客户端之间共享。同年，Casado 等[11]针对轻量级分布式设备的单任务 FCL 场景，提出了基于半监督标记的全局模型和基于漂移检测和自适应的本地模型。现有的 FCL 方法都是采用经典的基于服务器-客户端的中心化联邦架构。如图 1(a)所示，在该联邦框架下，有一个中央服务器负责聚合和分发模型参数，并且多个客户端只基于私有数据集进行本地更新。联邦平均算法（Federated Average，简称 FedAvg）[12]是一种中央服务器将接收到的模型信息进行加权平均聚合的联邦方法，是最常用的中心化联邦学习方法之一。在 FedAvg 基础上，FedProx 算法[13]针对客户端添加修正项，通过提高整体收敛的稳定性来解决联邦架构中的数据异构和系统异构问题。然而，现实训练情况涉及大量数据，中央服务器易成为攻击的入口，从而危及整个用户数据库的隐私安全；同时，如果服务器出现故障，将会导致整个系统无法正常运行[14]。

为了弥补以上不足，去中心化架构[15]被提出以进一步增强分布设备的数据安全。如图 1(b)所示，去中心化联邦架构不涉及中央服务器，仅通过客户端对等交换协作学习模型，这样能够保证网络中所有参与方的安全和公平加入，提供高级别的数据安全保障[16]。对等网络架构（Peer-to-Peer，P2P）[14]是常用的去中心化联邦架构，在该框架下，客户端间使用安全链路互相传输参数，并且需要提前确定发送和接收信息的顺序。但是，目前并未有针对基于去中心化架构的 FCL 方法的研究。

综上，为了打破现有联邦增量学习方法的局限性，本文构建了一个新型的联邦增量学习框架，基于去中心化联邦学习和增量元学习实现数据安全和持续学习。第一步，针对任务增量场景，本文提出了一个结合最近类均值样本回放的增量元学习方法 NMR-cMAML（Nearest the Mean-of-exemplars Replaying Based Continual Model-Agnostic Meta-Learning），每个客户端采用该方法对私有任务流和数据进行本地训练。首先，由于元学习对多任务、少样本具备快速适应能力，所设计的 NMR-cMAML 基于强泛化性的初始化模型元学习方法，旨在通过对少量样本的训练来学习梯度下降的方向。然后，结合对旧任务中最近类均值样本的回放，NMR-cMAML 可以通过设置元目标和元训练来平衡新旧任务的梯度，避免在持续学习时梯度偏向于新任务而导致灾难性遗忘。第二步，针对联邦增量场景，本文构建了一个结合元学习的去中心化联邦增量学习方法。所构建的去中心化联邦增量框架是基于对等网络架构，不同于传统服务器-客户端架构中服务器易受攻击[14]和去中心化架构中循环更新慢[17]的现状，本方法采用随机选择客户端作为聚合节点的策略，其他客户端同时进行本地增量更新并同步和聚合节点进行通信。一方面，共享全局元参数相当于共享每个客户端训练得到的最优化初始参数，其可以实现客户端间知识的共享和正向迁移，并适用于来自各个客户端的所有已处理任务。另一方面，对等网络架构保证了系统的各方安全性，去中心化策略的随机性保证了系统的安全性，客户端的同步更新保证了系统的并发性，能够在保护数据安全的同时提高联邦效率。

2 相关概念

2.1 联邦学习的架构和原理

联邦学习是一种分布式机器学习算法，每个节点交换的是模型参数或者模型梯度而不是原始数据，以达到保护每个节点数据隐私的目的[4]。根据应用场景的不同，联邦学习可以分为涉及中央协调方（如图 1(a)）的中心化联邦学习（见 2.1.1 节）和不涉及中央协调方（如图 1(b)）的去中心化联邦学习（见 2.1.2 节）。

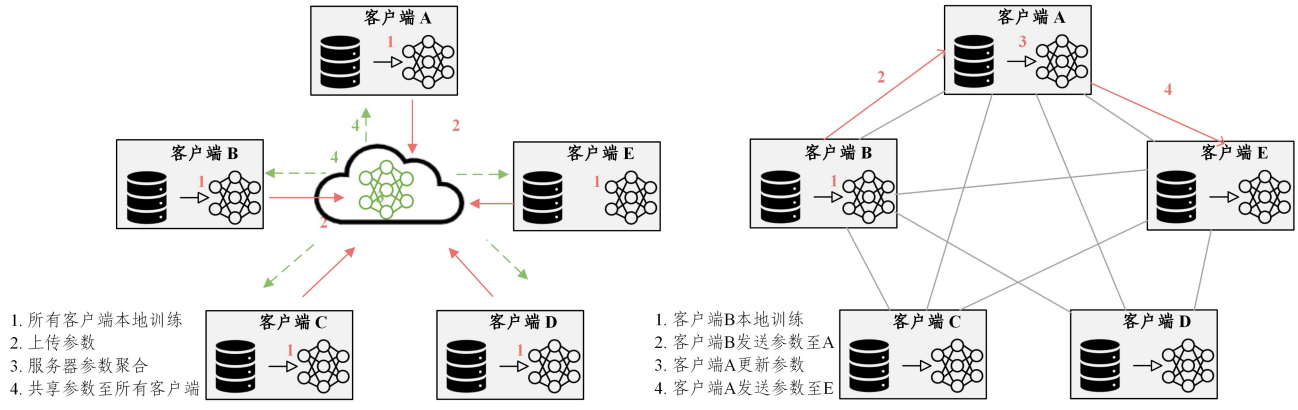

图 1 两种联邦学习架构对比图

Fig. 1 Comparison diagram of two federated learning architectures

2.1.1 中心化联邦学习

经典的联邦学习采用了基于中心化结构的服务器-客户端（Server-to-Client）架构，如图 1(a)所示，中心化联邦学习包括一个中央协调方（也称作中央服务器）和多个参与方（也称作客户端）。在此场景中，联邦学习的训练遵循以下 5 个步骤[18]：

1）中央服务器初始化模型，将参数发送至各客户端；

2）在第 c 轮通信时，客户端 k 基于私有数据集训练本地模型 Θ_k^c；

3）客户端 k 将更新后的模型参数 Θ_k^c 发送至中央服务器；

4）中央服务器将接收的参数进行加权聚合：

$$\Theta^c=\sum_{k=1}^{K}\frac{n_k}{n}\Theta_k^c$$

其中，K 表示参与的客户端总数，n 表示总数据量，n_k 表示客户端 k 的数据量；

5）中央服务器将共享聚合后的参数发送至各客户端。

重复步骤 2－步骤 5，直至模型收敛或者达到最大迭代次数。

然而，在现实情况下，基于服务器-客户端的联邦学习架构的大型中央服务器用于数据存储和模型参数的分析，过程中存在被恶意攻击或瘫痪的风险，从而危及整个联邦系统[4]。

2.1.2　去中心化联邦学习

另一种联邦学习架构是基于去中心化结构的对等（Peer-to-Peer，P2P）网络架构，该架构可以弥补基于服务器-客户端架构的联邦学习的不足，进一步保护分布式系统中的数据安全。如图 1(b)所示，去中心化联邦学习不存在中央服务器或者协调方，只有多个客户端。在此场景下，联邦学习的训练遵循以下 5 个步骤[19]：

1）各个客户端初始化本地模型，并随机选择第 i 个客户端；

2）在第 c 轮通信时，对于第 i 个客户端，基于私有数据集训练本地模型 Θ_i^c；

3）客户端 i 随机选择不同的客户端 j，发送 Θ_i^c 至客户端 j；

4）当客户端 j 接收到来自客户端 i 的模型参数 Θ_i^c 后，基于私有训练集更新收到的模型参数，得到 Θ_j^c；

5）将客户端 j 作为下一轮通信的客户端 i。

重复步骤 2－步骤 4，直到所有客户端均被选择且模型参数均收敛。

去中心化的对等网络架构因为去除了中央服务器，所以避免了服务器失灵带来的数据威胁，但是对等网络架构中的循环更新会导致训练模型花费更多的时间[17]。

2.2　增量学习的概念和研究现状

增量学习（Incremental Learning）也称持续学习（Continual Learning）[20]，指针对连续到达的任务流场景，研究不存储全量样本时如何学习一个对新旧任务都能有效分类的机器学习模型[21]。本文使用增量学习的目的是在不同客户端的连续且相关的任务流中不断从新数据中学习处理新任务，同时保留以前数据中学习到的知识[22]。本文研究的场景为任务增量型场景[23]（Task-Incremental Continual Learning），此场景下不同时刻需处理的数据属于不同的任务，某一时刻可以获得当前任务的全量数据，从而在独立同分布的假设下训练模型。

增量学习按技术可以分为以下 4 类方法[23]。1）基于正则化的增量学习方法：避免原始数据的存储，优先考虑隐私和减轻内存需求，通过扩展损失函数以及设计损失项，选择性巩固模型权重，在学习新数据时巩固先前的知识，如 EWC[24]。2）基于参数分离的增量学习方法：为不同任务分离不同的参数网络，通过固定前一任务的参数子集来保证最大的稳定性。基于参数分离的增量学习方法可以构建通用任务的固定结构（Fixed Architecture），如强注意力训练（Hard Attention Training，HAT）[25]。3）基于样本回放的增量学习方法：通过存储小部分旧任务的数据将过去的信息重播给模型，从而加强模型对旧任务的巩固，如经验回放（Experience Replay，ER）[26]。4）基于元学习的增量学习方法：基于元学习对多任务、少样本的快速适应以解决增量学习问题，如元经验回放（Meta-Experience Replay，MER）[27]结合了基于优化的元学习和经验回放以最大化每个任务的迁移和最小化基于未来梯度的干扰。

2.3　元学习的基本原理

元学习（Meta Learning）又被称为学会学习（Learn to Learn），指基于少量样本数据快速学习新的概念或技能，获得一个对不同任务有很强适应性和泛化性的元学习模型。因其对多任务和少样本具备快速适应能力，近年来元学习开始被应用于增量学习领域[27]，元学习算法的目的是最小化多任务识别的损失和对齐任务间的梯度，这与增量学习的目的不谋而合；同时，元学习的快速学习能力能够缓解联邦系统的数据异构问题，通过为不同客户端训练不同的个性化模型，从而解决联邦学习中客户端数据差异的问题[28]。

目前，元学习的研究中基于强泛化性的初始化参数元学习方法进展较大且性能优越[29]。本文构建的去中心化联邦增量学习方法结合了基于 MAML 的元学习模型，MAML（Model-Agnostic Meta-Learning，模型无关的元学习算法）是基于强泛化性的初始化参数元学习中实验效果最好的方法之一[30]。MAML 将对网络参数进行梯度下降的优化过程和优化损失函数过程中使用的任务数据相分离，实现了较好的泛化性[29]。MAML 由两层循环构成，在每轮训练过程中，内部循环根据任务的一个批次数据进行梯度下降，外部循环在任务的所有批次数据完成内部循环的梯度下降后再更新模型参数。MAML 的元学习训练过程遵循以下 4 个步骤[30]：

1）随机初始化模型参数 θ；

2）基于任务分布 $p(T)$，采样任务批次 T_i；

3）内部循环：对于任务 T_i 的每一个批次数据进行训练，计算梯度 $\nabla_\theta\mathscr{L}_{T_i}(f_\theta)$，梯度下降更新内部循环的模型：

$$\theta_i'=\theta-\alpha\nabla_\theta\mathscr{L}_{T_i}(f_\theta)$$

4）外部循环：基于内部循环计算的梯度，更新外部循环的模型：

$$\theta\leftarrow\theta-\beta\nabla_\theta\sum_{T_i\sim p(T)}\mathscr{L}_{T_i}(\theta_i')$$

3　本文方法

3.1　总体框架

为了解决联邦增量场景中持续学习和数据安全的问题，本文构建了结合元学习的去中心化联邦增量学习框架。专注于任务已知的任务增量场景，本文考虑的去中心化设置不同于传统的服务器-客户端架构，采用了只包含客户端的对等网络架构，通过客户端间直接进行模型参数的传输和合并，实现网络中各个参与的客户端的安全、透明和平等。

图 2 给出了本文提出的去中心化联邦增量学习的总体框架。首先，架构中的每个对等节点采用了 3.3 节介绍的

NMR-cMAML 增量方法作为本地模型，将最近类均值样本回放和元学习相结合，在元训练的过程中实现模型对新旧任务的平衡和记忆。然后，采用 3.4 节介绍的对等网络架构作为联邦策略，每轮通信随机选择一个客户端作为聚合节点，其余对等节点同步进行本地更新并与聚合节点进行通信，保证了联邦系统的随机性、安全性和并发性。

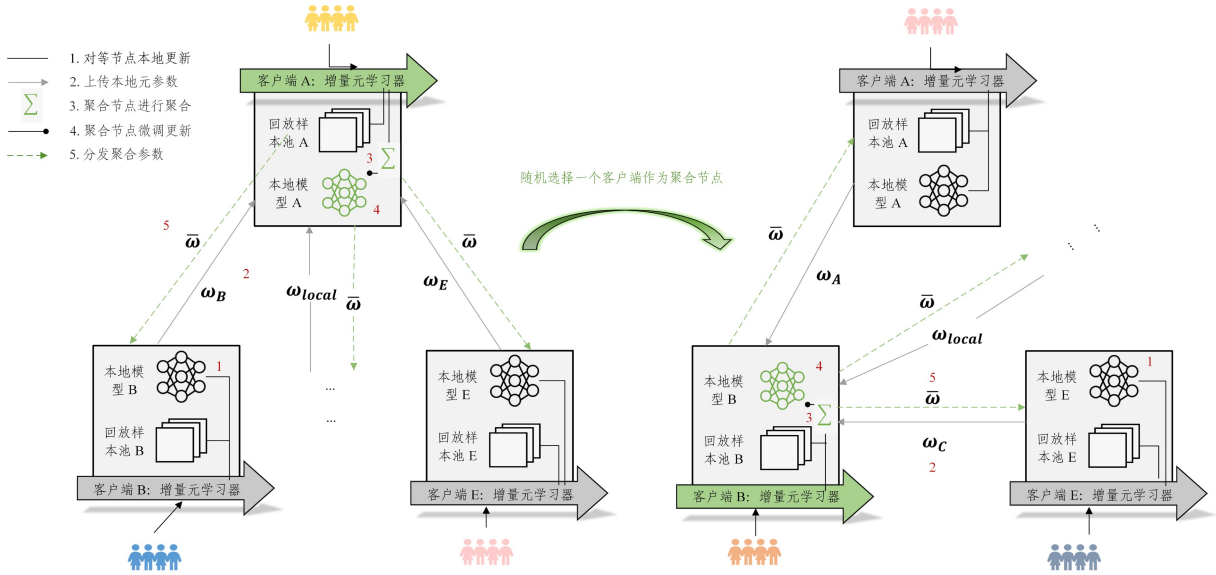

图 2 结合元学习的去中心化联邦增量学习方法框架图

Fig. 2 Framework diagram of the decentralized federated continual learning method combined with meta-learning

3.2 场景描述

本文考虑的增量设置中所有客户端同步参与每轮通信，在联邦通信过程中，每个客户端 $k(1\leqslant k\leqslant K$，联邦通信涉及共 K 个客户端)处理私有的任务流 $T_k=[T_k^1,T_k^2,\cdots,T_k^t,\cdots,T_k^T]$ $(1\leqslant t\leqslant T$，联邦过程共有 T 个任务)。具体表现为：在第 t 时刻，每个客户端 k 基于其私有任务 T_k^t 的样本训练其本地增量模型，其中任务 T_k^t 采样于私有数据集 D_k^t 且包含了共 n_k^t 个类别。假设样本空间共有 N 个类别标签，那么满足 $\sum_{t=1}^{T}n_k^t=N$。私有数据集 $D_k^t=\{X_k^t,Y_k^t\}$ 中，X_k^t 表示样本数据，Y_k^t 表示样本标签。

其中需要注意的是，对于客户端 k，不同任务处理的任务样本类别不重叠，即当时刻 $i\neq j$ 时处理的任务为 T_k^i 和 T_k^j 且 $Y_k^i\bigcap Y_k^j=\varnothing$；对于不同客户端 p 和 q，相同任务处理的样本类别可能存在重叠，即当 $p\neq q$ 时 $Y_p^c\bigcap Y_q^c\neq\varnothing$。

在去中心化联邦增量学习过程中，对于每个客户端，本文的目的是最大化客户端的本地模型对目前 T 个任务处理过的所有任务的分类准确率，和最小化前 $T-1$ 个任务涉及的所有任务的遗忘率。对于整体的去中心化框架，本文的目的是在实现客户端间知识迁移和共享的同时，提供高级别的数据安全保障。

3.3 增量元学习

在 t 时刻$(1\leqslant t\leqslant T)$，本文旨在最大化每个任务的迁移和最小化该客户端 k 处理过的所有任务 $T_k^{1:t}$ 的干扰。于是有代价目标函数：

$$\min\mathscr{L}_k(\Theta_k;X_k,Y_k)=\min\sum_{c=1}^{C}\ell_{k,c}(f_t(\Theta_k;X_k^t),Y_k^t)\tag{1}$$

其中，$L_k=\sum_{t=1}^{T}b_{k,t}$ 表示处理过的所有任务 $T_k^{1:T}$ 的模型损失，Θ_k 表示客户端 k 的本地增量模型参数。当 $t\geqslant 2$ 时，本文希望当前模型参数 Θ_k 不仅能够准确识别当前的任务 T_k^t，还能够准确识别过去处理过的任务 $T_k^{1:t-1}$。

为了利用旧任务的有限知识和学习新旧任务间的样本分布，本文提出了结合最近类均值样本回放的增量元学习方法 NMR-cMAML。联邦框架中，每一个客户端采用 NMR-cMAML 进行本地更新，主要由以下 3 部分实现：1)基于元学习进行多任务适应；2)基于最近类均值样本回放巩固旧知识；3)将元学习和最近类均值样本回放相结合实现持续学习。

1)元学习：本文采用 MAML 结构的元学习方法，通过学习出一个较好的权重初始化参数从而适应新旧样本的数据分布。

元学习训练的过程可以分为内部训练和外部训练。对于每个客户端 k 在 t 时刻，NMR-cMAML 基于从当前新任务 T_k^t 采样的小批次 b 进行内部训练，基于 b 和从样本池 $\mathscr{M}_k^{t-1}$ 采样的回放样本 m_{t-1} 的混合数据进行外部训练。于是，该方法可以在学习新数据分布的同时，确保新旧任务的梯度对齐。

首先，在 t 时刻，内部训练的目标可以表示为：

$$\begin{aligned}\min\mathscr{L}_{\text{inner}}(\theta_i^p;b)&=\min\mathbb{E}_{X,Y\sim b}[\ell_{\text{train}}(f(\theta_i^p;X^t),Y^t)]\\&=\min\left[\ell_{\text{inner}}(\theta_i^p)-\alpha\cdot\frac{\partial l_{\text{inner}}(\theta_i^p)}{\partial\theta_i^p}\right]\end{aligned}\tag{2}$$

其中，p 和 i 分别表示外部循环和内部循环的次数，θ_i^p 表示在第 p 次外部循环时进行 i 次内部训练得到的模型参数，$\{X^t,Y^t\}$ 是从当前任务 T_k^t 的小批次 b 中采样得到的训练数据。

然后，令 $b_m=m_{t-1}\cup b$ 为从样本池 $\mathscr{M}_k^{t-1}$ 采样的回放样本 m_{t-1} 和 b 的混合数据，基于内部训练得到的模型参数 θ_i^p 和混合数据 b_m 进行外部元训练得到本地元参数 Θ。于是，在 t 时刻，式(1)的目标可以改写为：

$$\begin{aligned}\min\mathscr{L}(\Theta;X,Y)&=\min\mathscr{L}_{\text{meta}}(\theta_i^p;b_m)\\&=\min\mathbb{E}_{X,Y\sim b_{1_m}}[\ell_{\text{meta}}(f(\theta_i^p;X^{1:t}),Y^{1:t})]\end{aligned}\tag{3}$$

其中，$\{X^{1:t},Y^{1:t}\}$是从b_m采样得到的目前处理过的1～t任务的样本数据。

2）最近类均值样本回放：m_{t-1}是从每轮任务中进行最近类均值采样得到的回放样本池$\mathcal{M}_k^{t-1}$中采样得到的，用于在学习新任务的同时加强对旧知识的巩固。

最近类均值样本回放方法使用了一个固定容量的回放样本池，其储存了旧任务中最近类均值的样本数据，用于在新任务训练过程中取出。最近类均值样本回放方法包括两个主要阶段：样本采样和样本池更新。样本采样阶段构建了限制大小的回放样本m（流程如算法1所示）；样本池更新阶段重建了客户端k时刻t固定容量的回放样本池$\mathcal{M}_k^t$（流程如算法2所示）。

算法1　样本采样算法 SampleExemplar

输入：客户端编号 k，t 时刻的回放样本池$\mathcal{M}_k^t$，t 时刻处理过的类别编号 1～u，回放样本大小 N

输出：采样的回放样本 m

1. 根据客户端 k 目前处理过的类别 1～u，将$\mathcal{M}_k^t$划分为$\{M_1,M_2,\cdots,M_u\}$
2. 定义函数$M'=\text{Sample}(M,n',m')$
   // 从样本 M 中随机采样n′个类、每个类平均 m′个样本作为M′
3. 当 N＞u 时，从每个类回放若干个样本，对于第 i 类（1≤i≤u）：

$$m_i=\text{Sample}\left(M_i,u,\left\lfloor\frac{N}{u}\right\rfloor\right)+\text{Sample}(M_i,N \bmod u,1)$$

4. 当 N≤u 时，从每个类随机采样 1 个样本，对于第 i 类（1≤i≤u）：

$$m_i=\text{Sample}(M_i,N,1)$$

5. 对于类别 1～u，构建 $m=\{m_1,m_2,\cdots,m_u\}$

算法2　样本池更新算法 UpdateExemplar

输入：客户端编号 k，t 时刻的新任务样本D_k^t，客户端 k 的增量模型参数Θ_k，t－1 时刻的回放样本池$\mathcal{M}_k^{t-1}$，回放样本池容量 M

输出：更新 t 时刻的回放样本池$\mathcal{M}_k^t$

1. 对于客户端 k，t 时刻前处理过类别 1～u，t 时刻时处理类别 u＋1～v
2. 此时，样本池内平均每个类别存储 $n=\frac{M}{v}$个样本
3. 对于旧任务的类别 1～u，更新回放样本：
   3.1. 根据类别 1～u，将$\mathcal{M}_k^{t-1}$划分为$\{M_1,M_2,\cdots,M_u\}$
   3.2. 对于第 i 类（1≤i≤u），M_i只保留最近类均值的 n 个样本
4. 对于新任务的类别 u＋1～v，存储回放样本：
   4.1. 根据类别 u＋1～v，将D_k^t划分为$\{D_{u+1},D_{u+2},\cdots,D_v\}$
   4.2. 对于第 j 类（u＋1≤j≤v），基于模型参数计算D_j的样本均值

$$\mu_j=\frac{1}{|D_j|}\sum_{d\in D_j}\Theta_k(d)$$

   4.3. 对于第 j 类，保留距离类均值μ_j最近的 n 个样本作为M_j
5. 对于类别 1～v，得$\mathcal{M}_k^t=\{M_1,\cdots,M_u,\cdots,M_v\}$

3）将元学习和最近类均值样本回放相结合：如图3所示，NMR-cMAML 元学习训练的过程可以分为内部训练和外部训练。对于每个客户端k在t时刻，本方法基于从当前新任务T_k^t采样的小批次b进行内部训练，基于b和从样本池M_k^{t-1}采样的回放样本m的混合数据进行外部训练。客户端k在本地增量学习的训练过程 NMR-cMAML 如算法3所示。

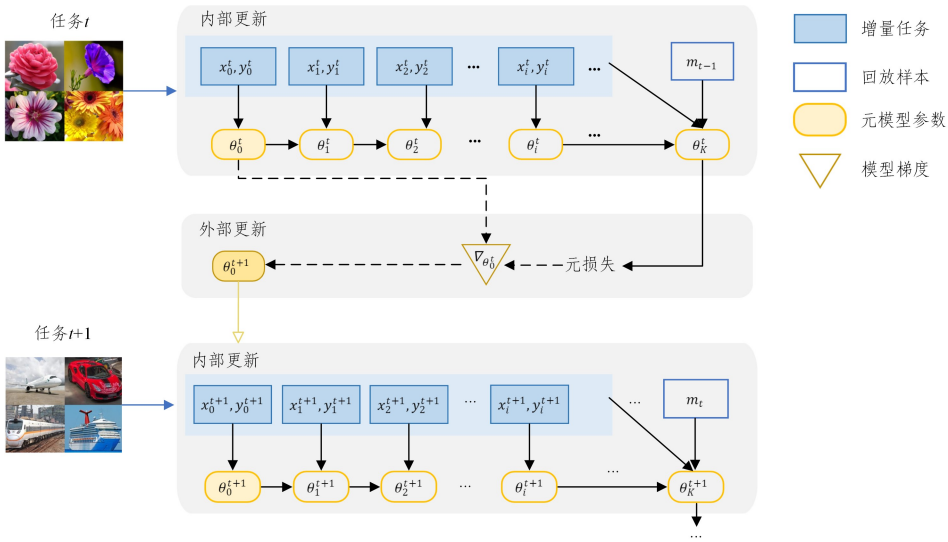

图3　结合最近类均值样本回放的增量元学习方法 NMR-cMAML 流程图

Fig. 3　Flow chart of NMR-cMAML: a continual meta-learning method based nearest mean-of-exemplars replaying

算法3　NMR-cMAML 增量学习 IncrementalTrain

输入：客户端编号 k，t 时刻的新任务T_k^t，样本D_k^t，t－1 时刻的本地增量模型参数Θ_k，t－1 时刻的回放样本池M_k^{t-1}，客户端本地迭代的轮次 E，回放样本大小 N，内部循环学习率 α，外部循环学习率 β

输出：客户端 k 的当前元参数Θ_k，数据规模d_k

1. 初始化元参数$\boldsymbol{\theta}_0^t=\Theta_k$
2. 数据规模$d_k=|D_k^t|$
3. For ep from 1 to E：
   3.1. 开始元学习外部循环：令 t＝0
   3.2. For batch b in$(X^t,Y^t)\sim D_k^t$：
      3.2.1. 采样回放样本：
         $m=\text{SampleExemplar}(k,\mathcal{M}_k^{t-1},N)$
      3.2.2. $b_m=m\cup b$
      3.2.3. 开始元学习内部循环：令 i＝0
      3.2.4. For$(x_i,y_i)\sim b$：
         3.2.4.1. 更新$\boldsymbol{\theta}_i^t$：

$$\boldsymbol{\theta}_{i+1}^t=\boldsymbol{\theta}_i^t-\alpha\cdot\nabla_{\boldsymbol{\theta}_i^t}\mathcal{L}_{CE}(\boldsymbol{\theta}_i^t;x_i,y_i)$$

         3.2.4.2. 内部循环自增：i＝i＋1
      3.2.5. 计算元损失$\mathcal{L}_{meta}=\mathcal{L}_{CE}(\boldsymbol{\theta}_i^t;b_m)$
      3.2.6. 更新$\boldsymbol{\theta}_0^t$：

$$\boldsymbol{\theta}_0^{t+1}=\boldsymbol{\theta}_0^t-\beta\cdot\nabla_{\boldsymbol{\theta}_0^t}\mathscr{L}_{meta}$$

3.2.7. 外部循环自增：t=t+1

4. $\Theta_k=\boldsymbol{\theta}_0^t$

5. 更新回放样本池：

$$\mathscr{M}_k^t=\text{UpdateExemplar}(k,D_k^t,\Theta_k,\mathscr{M}_k^{t-1})$$

最后，客户端将元学习训练得到的最优权重初始化参数通过联邦框架进行上传。

3.4 去中心化联邦增量学习

为了实现任务增量场景下联邦系统的数据安全和客户端间的知识迁移，本文提出了一个基于对等网络架构的去中心化联邦增量学习框架(如图 2 所示)。

为了避免传统服务器-客户端联邦框架中服务器节点受攻击而导致的隐私泄露问题，本文采取了只包含客户端通信的对等网络架构。每个客户端均采用了 3.3 节介绍的 NMR-cMAML，基于每一轮的当前新任务和回放样本池的旧任务采样，本地更新学习得到本地元参数。为了解决文献[17]中提到的循环更新带来的训练时间增多的问题，本文采用了随机并发更新的方法。不同于循环更新中每次只更新一个客户端的模型参数，本文方法在每轮通信中都会随机选择一个客户端作为聚合节点，其他客户端同步进行更新，以实现随机性、对等性和并发性。

去中心化联邦通信的流程如算法 4 所示，每轮通信会随机选择一个客户端作为聚合节点，其余客户端作为对等节点：1)对等节点基于当前通信轮次的私有任务流数据进行训练，本地更新得到本地元参数；2)对等节点上传本地元参数至聚合节点；3)聚合节点聚合来自其他对等节点的元参数，并根据数据规模进行加权平均；4)聚合节点基于私有任务流数据，对聚合元参数进行微调；5)聚合节点将更新后的聚合元参数分发给其他所有对等节点。在通信过程中，每轮通信随机选择的客户端增强了联邦框架的随机性，保证了通信框架的数据隐私安全和每个参与客户端的公平性。

算法 4 基于对等网络架构的去中心化联邦增量学习方法

输入：客户端数量 num，每个任务的通信轮次 R，增量任务数量 T，客户端本地迭代的轮次 E

1. 初始化每个客户端在 T 个任务通信的本地增量任务流 $T_k=[T_k^1,T_k^2,\cdots,T_k^t,\cdots,T_k^T]$ $(1\leqslant k\leqslant num)$

2. 初始化 num 个客户端的本地模型参数 $[\Theta_1,\cdots,\Theta_k,\cdots,\Theta_{num}]$

3. For t from 1 to T：

3.1. For r from 1 to R：

3.1.1. 从 num 个客户端中随机选择第 num′个作为聚合节点，其余作为对等节点

3.1.2. 初始化 $d^t=0$

3.1.3. 平行执行 For k in 对等节点：

3.1.3.1. 采用 NMR-cMAML 本地更新得到元参数：$d_k^t,\Theta_k=\text{IncrementalTrain}(k,T_k,\Theta_k,E)$

3.1.3.2. 上传 d_k,Θ_k 至聚合节点

3.1.3.3. $d^t=d^t+d_k^t$

3.1.4. 聚合节点进行聚合：

$$\Theta_{num'}=\sum_{1\leqslant k\leqslant num\ and\ k\neq num'}\frac{d_k^t}{d^t}\Theta_k$$

3.1.5. 聚合节点进行微调：

$$\_,\Theta_{num'}=\text{IncrementalTrain}(num',T_{num'},\Theta_{num'},E)$$

3.1.6. 聚合节点将 $\Theta_{num'}$ 下发至所有对等节点

4 实验分析

4.1 数据集介绍

本文实验使用 ImageNet50 和 CIFAR100 数据集。ImageNet50 数据集包含 50 个类别共 30 000 张 64×64 RGB 图片，是 ImageNet 数据集的一个子集，每个类别包含 500 张训练图片和 100 张测试图片。ImageNet50 数据集被划分为 10 个任务，每个任务为不相交的 5 个类别增量。在去中心化联邦场景中，设置客户端数量为 5、客户端参与率为 1.0、本地训练轮数为 2、每个客户端的回放样本池容量为 250。

CIFAR100 数据集包含 100 个类别共 60 000 张 32×32 RGB 图片，每个类别包含 500 张训练图片和 100 张测试图片。CIFAR100 数据集被划分为 20 个任务，每个任务为不相交的 5 个类别增量。在去中心化联邦场景中，设置客户端数量为 5、客户端参与率为 1.0、本地训练轮数为 2、每个客户端的回放样本池容量为 500。

4.2 实验设置

为了验证所提出的去中心化增量学习方法的可行性和鲁棒性，本文针对所有客户端处理任务流的顺序场景和乱序场景进行了实验和分析。在顺序任务流场景下，所有客户端处理的任务顺序相同，即所有客户端的私有任务流为 $T=[T^1,\cdots,T^c,\cdots,T^C]$；在相同的任务通信轮次下，所有客户端处理的任务和类别标签相同，私有的任务样本不重叠。在乱序任务流场景下，每个客户端处理的任务顺序不同，即每个客户端 k 的私有任务流为 $T_k=[T_k^1,T_k^2,\cdots,T_k^c,\cdots,T_k^C]$，$T_1\sim T_K$ 各不相同。

本文将中心化的服务器-客户端架构和去中心化的对等网络架构进行对比，并在每个联邦设置中将本文提出的 NMR-cMAML 方法与常用增量学习方法 ER 以及 MER 进行对比。

ER[26]：经验回放方法(Experience Replay)采用蓄水池采样进行样本回放，是增量学习中常见的基线方法。

MER[27]：元经验回放方法(Meta-Experience Replay)结合了经验回放方法和元学习，利用样本回放来保持新旧任务梯度的对齐。

本文采用学习完所有任务的客户端平均值 Accuracy 作为联邦增量方法的评估指标。首先，定义 $A_k\in\mathbb{R}^{T\times T}$，其中 $A_k^{i,j}$ 表示客户端 k 的增量模型在学习完最新任务 *taski* 后对任务 *taskj* 的分类准确率 $(1\leqslant i,j\leqslant T)$。于是，在 K 个客户端共 T 个增量任务的场景下，客户端平均值 Accuracy 表示为：

$$Accuracy=\frac{1}{K}\sum_{k=1}^{K}\left(\frac{1}{C}\sum_{j=1}^{C}A_k^{C,j}\right)\tag{4}$$

本文实验都基于 Python3.8，用于实验数据运行的服务器系统为 Linux VM-0-16-ubuntu，CPU 为 Platinum 8255C@1.50GHz，内存大小为 128GB，GPU 为 Tesla V100，显存大小为 32GB，CUDA 版本为 10.1，保证了通信框架的数据安全和每个参与客户端的公平性。

4.3 实验结果分析

4.3.1 顺序任务流下的去中心化联邦增量结果

在顺序任务流场景下，所有客户端处理的任务顺序相同，

即所有客户端的私有任务流为$[T^1,\cdots,T^c,\cdots,T^C]$。表1列出了在该场景下，不同联邦策略组合增量学习方法在不同通信轮次的联邦增量性能。在去中心化的对等网络架构中，本文提出的NMR-cMAML增量学习方法在所有通信轮次下均取得了最高的客户端平均准确率；在通信轮次分别为1，2，3，4轮的情况下，在Imagenet-50数据集上，去中心化的NMR-cMAML比去中心化的ER基线的客户端平均准确率分别提高了15.93%，13.47%，13.3%，13.5%，在CIFAR-100数据集上分别提高了16.07%，14.75%，13.44%，13.74%。去中心化的对等网络架构相较于传统的服务器-客户端架构，在不同增量方法的所有通信轮次下均取得了较高的客户端平均准确率；在通信轮次分别为1，2，3，4轮的情况下，在Imagenet-50数据集上，去中心化的NMR-cMAML比服务器-客户端架构的NMR-cMAML的客户端平均准确率分别提高了6.3%，4.15%，2.57%，2.29%，在CIFAR-100数据集上分别提高了2.51%，1.02%，0.67%，0.78%。实验结果证明了去中心化框架和NMR-cMAML在联邦学习和增量学习上结合的有效性，且证明了去中心化方法能够在保证数据安全的基础上，提升客户端的本地性能。

表1　顺序任务流场景下不同联邦方法的客户端平均准确率

Table 1　Average client accuracy of different methods in sequential task-flow scenario

(%)

顺序：联邦策略 通信轮次		Imagenet-50(5*10)				CIFAR-100(5*20)			
		1	2	3	4	1	2	3	4
服务器-客户端架构(central)	ER	38.82	44.05	46.55	47.27	46.78	52.00	54.25	55.88
	MER	45.96	49.92	52.65	53.27	56.48	60.05	61.53	62.45
	NMR-cMAML	**51.12**	**56.74**	**59.38**	**60.55**	**62.94**	**66.80**	**68.61**	**69.65**
去中心化-对等架构(decentral)	ER	41.49	47.42	48.65	49.34	49.38	53.07	55.84	56.69
	MER	47.89	52.44	54.87	55.28	57.71	61.18	62.72	63.46
	NMR-cMAML	**57.42**	**60.89**	**61.95**	**62.84**	**65.45**	**67.82**	**69.28**	**70.43**

图4给出了在CIFAR-100数据集上，在通信轮次分别为1，2，3，4的场景下，随着任务的增加，不同联邦方法对于已处理过的任务的客户端识别平均准确率曲线图。首先比较传统的中心化架构和本文所提出的去中心化架构的性能。以NMR-cMAML为例，去中心化架构中的NMR-cMAML(简称decentral-NMR-cMAML)的表现优于中心化架构中的NMR-cMAML(central-NMR-cMAML)：因聚合节点对全局模型的微调，去中心化方法的任务平均准确率均高于中心化方法，可以证明所提出的去中心化架构的联邦增量性能较好。然后比较常用的增量方法和本文所提出的NMR-cMAML的性能。以去中心化架构为例(中心化架构同理)，3.3节提出的NMR-cMAML表现优于ER(简称decentral-ER)和MER(简称decentral-MER)：随着任务增加，decentral-NMR-cMAML的客户端平均准确率变化平稳且有上升的趋势，而decentral-ER和decentral-MER的客户端平均准确率有明显的下降，证明了所提出NMR-cMAML的增量性能较好。最后比较去中心化架构在不同通信轮次时的增量性能。当通信轮次为1时，decentral-NMR-cMAML在第一个任务时刻的准确率较低；随着任务的增加，decentral-NMR-cMAML充分学习了任务分布，增量准确率上升。当通信轮次为2，3，4时，decentral-NMR-cMAML训练到了任务间的数据分布，准确率在各个任务时刻优于其他联邦增量方法，证明了所提出的去中心化增量方法的鲁棒性。

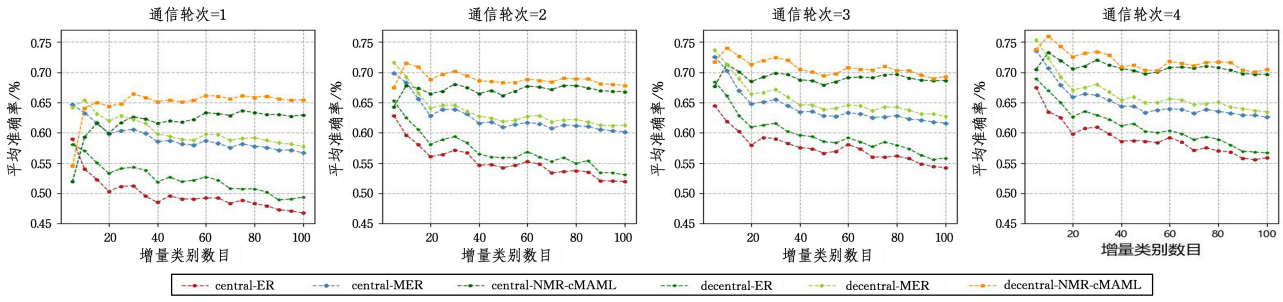

图4　Cifar100数据集上不同联邦增量方法平均准确率的变化曲线图

Fig. 4　Cifar100: a plot of the change in the average accuracy in different federated continual methods on Cifar100 dataset

4.3.2　乱序任务流下的去中心化联邦增量结果

在乱序任务流场景下，每个客户端处理的任务顺序不同，即每个客户端k的私有任务流为$T_k=[T_k^1,T_k^2,\cdots,T_k^c,\cdots,T_k^C]$，$T_1\sim T_K$各不相同。表2列出了在该场景下，不同联邦策略组合增量学习方法在不同通信轮次下的联邦增量性能。decentral-NMR-cMAML方法在两个数据集上取得了最好的效果，证明了本文提出的方法同样适用于乱序任务流。通过比较表1和表2发现，Imagenet-50数据集在通信轮次为1/3/4、CIFAR-100数据集在通信轮次为2/3/4时，decentral-NMR-cMAML在乱序任务流中的表现优于顺序任务流，证明了该方法能够学习到任务间样本分布并在客户端间实现有效的任务迁移。

表 2 乱序任务流场景下不同联邦方法的客户端平均准确率

Table 2 Average client accuracy of different methods in disorder task-flow scenario

(%)

乱序:联邦策略		Imagenet-50(5*10)				CIFAR-100(5*20)			
通信轮次		1	2	3	4	1	2	3	4
服务器-客户端架构(central)	ER	35.25	38.92	43.36	45.03	50.15	54.14	56.35	58.18
	MER	42.82	48.66	54.71	**55.98**	59.5	63.34	65.32	65.58
	NMR-cMAML	**43.87**	**52.13**	**53.89**	55.35	**60.97**	**66.08**	**68.46**	**70.16**
去中心化-对等架构(decentral)	ER	43.29	48.85	51.35	52.97	51.93	58.71	60.73	61.89
	MER	44.84	51.08	55.82	56.82	57.98	61.21	63.87	64.68
	NMR-cMAML	**57.50**	**60.80**	**62.92**	**64.89**	**65.44**	**69.47**	**71.32**	**72.84**

为更直观地表现在联邦通信过程中客户端间的知识迁移,本文绘制了 Imagenet50 数据集通信轮次为 2、随机种子为 2 的情况下前 3 个增量任务流的任务识别率分布图。该场景下,每个客户端处理的前 3 个任务流编号和柱形颜色如表 3 所列。图 5 给出了基于 decentral-NMR-cMAML 各个客户端对乱序任务流的增量学习和知识共享效果。由图 5 可知,在任务增量和联邦通信的过程中,每个客户端可以学习到本地任务之外的任务特征,在不交换原始数据的基础上实现客户端间的知识迁移。

表 3 Imagenet50 数据集上各客户端在前 3 个类型及图 5 中的对应颜色

Table 3 The first 3 flow types of each clients and the task color of Fig. 5 on Imagenet50 dataset

	前 3 个任务流	任务颜色
客户端 1	6,10,4	砖红色
客户端 2	2,6,7	茶色
客户端 3	9,3,1	黄绿色
客户端 4	3,4,2	橘黄色
客户端 5	6,9,4	深绿色

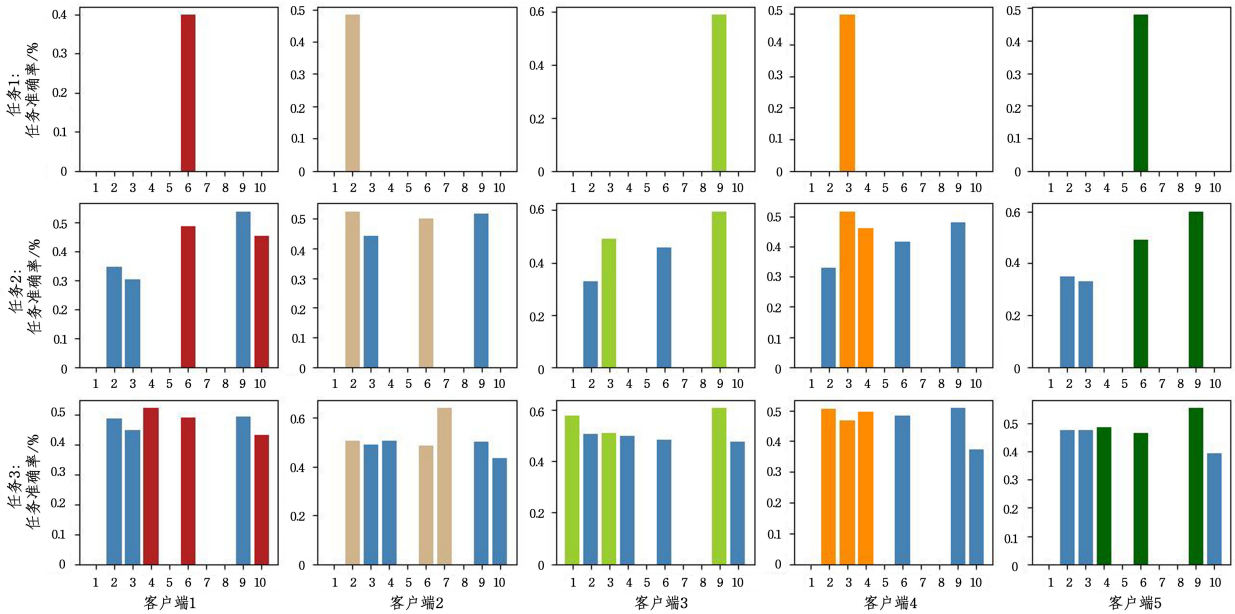

图 5 Imagenet50 数据集基于 decentral-NMR-cMAML 的前 3 个任务流的客户端准确率分布(电子版为彩图)

Fig. 5 Plot of clients' accuracy distribution of the first 3 clients based on decentral-NMR-cMAML on Imagenet50 dataset

结束语 本文提出了一种结合元学习的去中心化联邦增量学习方法,首先通过构建一个基于对等网络的去中心化框架达到对每个节点数据安全的强保护,同时可以实现去中心化联邦框架的公平性和可并发性;然后设计了一种结合最近类均值样本回放的增量元学习方法 NMR-cMAML 以达到每个客户端对本地增量任务流持续学习的目的,联邦学习和元学习的结合使得元学习训练得到最优公共点,共享使其可以快速适应不同的任务分布。通过在不同图像数据集上进行实验分析,讨论了顺序任务流和乱序任务流的情况,验证了所提方法在不同联邦增量场景下的有效性。在实验过程中发现,处理乱序任务流时的识别准确率要略高于顺序任务流,说明所提方法可以学习到不同任务间的知识迁移和客户端间的知识共享。在未来的工作中,会进一步考虑如何设计联邦框架,使得任务间的共性能够被进一步利用和识别。

参 考 文 献

[1] LIN J, YU W, ZHANG N, et al. A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications[J]. IEEE Internet of Things Journal, 2017, 4(5): 1125-1142.

[2] ZHU H, XU J, LIU S, et al. Federated learning on non-IID data: A survey[J]. Neurocomputing, 2021, 465: 371-390.

[3] RAHMAN S A, TOUT H, MOURAD A, et al. FedMCCS: Multicriteria Client Selection Model for Optimal IoT Federated Learning[J]. IEEE Internet of Things Journal, 2021, 8(6): 4723-4735.

[4] YANG Q, LIU Y, CHEN T, et al. Federated Machine Learning:

Concept and Applications[J]. ACM Trans. Intell. Syst. Technol.，2019，10(2)：12：1-12：19.

[5] MAI Z，LI R，JEONG J，et al. Online continual learning in image classification：An empirical survey[J]. Neurocomputing，2022，469：28-51.

[6] LIU L Y，QIAN H，XING H J，et al. Incremental Classification Model Based on Q-Learning Algorithm[J]. Computer Science，2020，47(8)：171-177.

[7] QI X M，WU Y B，JIANG X L. Federated Data Augmentation Algorithm for Non-independent and Identical Distributed Data [J]. Computer Science，2022，49(12)：33-39.

[8] LI Z Z，HOLEM D. Learning without forgetting[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence，2017，40(2)：2935-2947.

[9] YAO X，SUN L. Continual Local Training For Better Initialization Of Federated Models[C]// 2020 IEEE International Conference on Image Processing (ICIP). Abu Dhabi，United Arab Emirates：IEEE，2020：1736-1740.

[10] YOON J，JEONG W，LEE G，et al. Federated Continual Learning with Weighted Inter-client Transfer[C]// Proceedings of the 38th International Conference on Machine Learning (ICML). Virtual：PMLR，2021：12073-12086.

[11] CASADO F，LEMA D，LGLESIAS R，et al. Federated and continual learning for classification tasks in a society of devices[J]. arXiv：2006.07129，2020.

[12] MCMAHAN B，MOORE E，RAMAGE D，et al. Communication-Efficient Learning of Deep Networks from Decentralized Data[C]// Artificial Intelligence and Statistics(AISTATS). Ft. Lauderdale，FL，USA：PMLR，2017：1273-1282.

[13] LI T，SAHU A，ZAHEER M，et al. Federated optimization in heterogeneous networks[J]. Proceedings of Machine Learning and Systems，2020，2：429-450.

[14] ZANTEDESCHI V，BELLET A，TOMMASI M. Fully Decentralized Joint Learning of Personalized Models and Collaboration Graphs[C]// The 23rd International Conference on Artificial Intelligence and Statistics(AISTATS 2020). Palermo，Sicily，Italy：PMLR，2020：864-874.

[15] HEGEDUS I，DANNER G，JELASITY M. Decentralized learning works：An empirical comparison of gossip learning and federated learning[J]. Journal of Parallel and Distributed Computing，2021(148)：109-124.

[16] WARNET S，SCHULTZE H，SHASTR K L，et al. Swarm Learning for decentralized and confidential clinical machine learning[J]. Nature，2021，594(7862)：265-270.

[17] HEGEDUS I，DANNER G，JELASITY M. Gossip Learning as a Decentralized Alternative to Federated Learning[C]// Distributed Applications and Interoperable Systems：19th IFIP WG 6.1 International Conference(DAIS). Kongens Lyngby，Denmark：Springer International Publishing，2019：74-90.

[18] MOTHUKURI V，PARIZI R，POURIYEH S，et al. A survey on security and privacy of federated learning[J]. Future Gener. Comput. Syst.，2021，115：619-640.

[19] LIU Y，LIU J，BASAR T. Differentially Private Gossip Gradient Descent[C]// 2018 IEEE Conference on Decision and Control (CDC). Fontainebleau Miami Beach，USA：IEEE，2018：2777-2782.

[20] THRUN S，PRATT L. Lifelong Learning Algorithms [C]// Learning to Learn. Boston：Springer，1998：181-209.

[21] VEN G，TOLAIS A. Three scenarios for continual learning[J]. arXiv：1904.07734，2019.

[22] LANGE M，ALJUNDI R，MASANA M，et al. A Continual Learning Survey：Defying Forgetting in Classification Tasks[J]. IEEE Trans. Pattern Anal. Mach. Intell.，2022，44(7)：3366-3385.

[23] MAI Z，LI R，JEONG J，et al. Online continual learning in image classification：An empirical survey[J]. Neurocomputing，2022，469：28-51.

[24] LIU H，YANG Y，WANG X. Overcoming Catastrophic Forgetting in Graph Neural Networks[C]// Proceedings of the AAAI Conference on Artificial Intelligence. Virtual：AAAI，2021：8653-8661.

[25] SERRA J，SURIS D，MIRON M，et al. Overcoming catastrophic forgetting with hard attention to the task[C]// Proceedings of the 35th International Conference on Machine Learning(ICML). Stockholmsmässan，Sweden：PMLR，2018：4548-4557.

[26] ZHOU F，CAO C. Overcoming Catastrophic Forgetting in Graph Neural Networks with Experience Replay[C]// Proceedings of the AAAI Conference on Artificial Intelligence. Virtual：AAAI，2021：4714-4722.

[27] RIEMER M，CASES I，AJEMIAN R，et al. Learning to Learn without Forgetting by Maximizing Transfer and Minimizing Interference[C]// 7th International Conference on Learning Representations. New Orleans，USA：ICLR，2019：1-31.

[28] ZHANG C Y，SI S J，WANG J Z，et al. Federated Meta Learning：A Review[J]. Big Data Research，2023，9(2)：112-146.

[29] LI F C，LIU Y，WU P X. A Survey onRecent Advances in Meta-Learning[J]. Chinese Journal of Computer，2021，44(2)：422-446.

[30] FINN C，ABBEL P，LEVIINE S. Model-Agnostic Meta-Learning for Fast Adaptation of Deep Networks[C]// International Conference on Machine Learning (ICML). Sydney，Australia：PMLR，2017：1126-1135.

HUANG Nan，born in 1997，postgraduate. Her main research interests include federated learning and biometric recognition.

LI Dongdong，born in 1981，Ph.D，associate professor，is a member of CCF (No. 15173M). Her main research interests include speech processing and emotion computing.

（责任编辑：何杨）