可靠性感知的分层联邦学习机制

刘晓燕[1],余 振[1],梁晶语[2],林伯韬[1],黄霁崴[1*]
(1. 中国石油大学(北京)石油数据挖掘北京市重点实验室,北京 102249;2. 中石油(北京)数智研究院有限公司,北京 102206)

摘 要: 分层联邦学习(Hierarchical Federated Learning,HFL)通过"终端-边缘-云"的层次化组织,在边缘侧执行组内聚合、云侧进行全局聚合,以实现跨区域的高效协同训练。然而,客户端数据普遍呈非独立同分布(Non-Independent and Identically Distributed,Non-IID)特性,易导致组内更新方向不一致、梯度偏移乃至收敛震荡,进而削弱全局模型性能。同时,边缘服务器受资源约束、负载波动与链路不稳定影响,存在性能退化甚至失效风险,可能引发组内聚合中断,降低系统稳定性与任务完成效率。对此,本文提出一种可靠性感知的分层联邦学习框架(Reliability-aware Hierarchical Federated Learning,R-HFL),将训练过程划分为可靠性感知分组阶段和全局聚合阶段。在分组阶段,综合客户端模型语义特征与地理邻近性进行联合聚类,以提升组内统计一致性并缓解 Non-IID 诱发的梯度偏移,同时引入边缘节点可靠性指标作为约束进行协同选择,优先选取高可靠性边缘服务器作为组内中间聚合器,从而降低聚合服务中断风险。进一步地,考虑边缘服务器可靠性的时变性与联邦训练的长期性,本文设计了失效触发的可靠性感知服务迁移机制。当组内聚合器发生故障时,将聚合任务动态迁移至可用边缘服务器,以保障训练连续性。为实现迁移过程的自适应决策,本文将多客户端迁移建模为马尔可夫决策过程(Markov Decision Process,MDP),采用多智能体近端策略优化(Multi-Agent Proximal Policy Optimization,MAPPO)于集中式训练、分布式执行(Centralized Training with Decentralized Execution,CTDE)框架中学习迁移策略;通过统一的奖励与约束机制动态权衡迁移成本、迁移后通信开销与语义分布相似度,从而实现迁移目标的自适应选择、迁移后快速适配与收敛稳定性维持。最后,在两个真实数据集及多种 Non-IID 划分场景下进行实验验证。结果表明,所提 R-HFL 在全局模型精度与收敛速度上优于基线方法,并能在边缘服务器失效情况下显著降低训练中断风险与迁移开销,提升系统整体鲁棒性和故障容忍能力。

关键词: 分层联邦学习;非独立同分布;边缘服务器失效;服务迁移;多智能体近端策略优化

基金项目: 国家自然科学基金(No. 62572484);中国石油大学(北京)学科前沿交叉探索专项资助(No.2462024XKQY003)

中图分类号: TP301;TN92 **文献标识码:** A **文章编号:** 0372-2112(2026)01-0262-14

电子学报 URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20250852

A Reliability-Aware Mechanism for Hierarchical Federated Learning

LIU Xiaoyan[1], YU Zhen[1], LIANG Jingyu[2], LIN Botao[1], HUANG Jiwei[1*]
(1. *Beijing Key Laboratory of Petroleum Data Mining*, *China University of Petroleum* (*Beijing*), *Beijing* 102249, *China*;
2. *PetroChina* (*Beijing*) *Digital Intelligent Research Institute Co.*, *Ltd.*, *Beijing* 102206, *China*)

Abstract: Hierarchical federated learning (HFL) operates in a client-edge-cloud architecture, where intra-group aggregation is carried out at the edge and global aggregation is performed in the cloud, enabling efficient distributed collaborative training. However, client data is typically non-independent and identically distributed (Non-IID), which may yield inconsistent local updates, leading to gradient drift and convergence instability, and degrading global model performance. Meanwhile, edge servers are subject to resource limitations, workload fluctuations, and unstable links, which can cause performance degradation or even failures. Such events may interrupt intra-group aggregation, undermining system stability and task completion efficiency. To address these challenges, this paper proposes a reliability-aware hierarchical federated learning framework (R-HFL) that decomposes the training procedure into a reliability-aware grouping stage and a global aggregation stage. In the grouping stage, we jointly cluster clients by integrating model semantic similarity and geographic proximity, improving intra-group statistical consistency and mitigating gradient drift induced by Non-IID data. In addition, an edge reliability metric is incorporated as a reliability-aware selection criterion, prioritizing highly reliable edge servers as group-level aggregators to reduce the risk of aggregation interruption. Furthermore, to account for the time-varying reliability of edge servers and the long-term horizon of federated training, we design a failure-triggered task migration mechanism: when a group-level aggregator fails, the aggregation task is dynamically migrated to an available edge server to maintain training

收稿日期:2025-09-27;录用日期:2026-01-21;责任编辑:覃怀银
*通信作者:黄霁崴

continuity. To enable adaptive migration decisions, we formulate the migration process as a markov decision process (MDP) and adopt multi-agent proximal policy optimization (MAPPO) under centralized training and decentralized execution (CTDE) to learn migration policies. A unified reward function with constraints is further designed to dynamically balance migration cost, post-migration communication overhead, and semantic distribution similarity, facilitating an adaptive trade-off among objectives, fast migration adaptation, and sustained convergence stability. Finally, extensive experiments are conducted on two real-world datasets under different Non-IID scenarios. The results demonstrate that R-HFL consistently outperforms baseline methods in terms of global accuracy and convergence rate, while substantially reducing the risk of training disruption and migration overhead under edge server failures, thereby improving overall system robustness and fault tolerance.

Keywords: hierarchical federated learning; non-independent and identically distributed; edge server failure; service migration; multi-agent proximal policy optimization

Foundation Item(s): National Natural Science Foundation of China (No.62572484); Frontier Interdisciplinary Exploration Research Program of China University of Petroleum, Beijing (No.2462024XKQY003)

0 引言

随着移动设备的快速普及与应用场景的不断拓展,数据规模呈指数级增长[1-2]。边缘计算(Edge Computing,EC)作为一种靠近数据源的计算范式,能够有效降低数据传输延迟、缓解网络带宽压力,并提升实时处理能力,在车联网(Internet of Vehicles,IoV)等场景中展现出显著优势[3-5]。然而,单个边缘设备在算力、存储及能源等方面普遍受限,难以独立完成复杂的大规模任务处理,因此需要借助服务器资源以满足高性能计算需求[6]。将本地数据直接上传至服务器虽可借助其高性能算力实现集中训练,但会带来隐私泄露风险,并显著增加带宽占用与传输开销[7-9]。为解决上述矛盾,联邦学习(Federated Learning,FL)作为一种新型分布式机器学习范式被提出。其核心思想是在不上传原始数据的前提下,由各客户端在本地完成模型训练,并仅上传模型更新(如梯度或参数)至服务器进行聚合,从而在保护数据隐私的同时实现协同学习。在此基础上,分层联邦学习(Hierarchical Federated Learning,HFL)作为一种边缘-云协同计算架构下的新兴训练框架应运而生,并在多个领域受到广泛关注[10-12]。HFL在传统FL的基础上引入多层级参数聚合结构,通常由客户端、边缘服务器、云服务器三层组成,使模型更新能够在边缘侧先聚合,再上传至云侧进行最终聚合。该方法通过多层次模型聚合实现分布式训练:云服务器将模型更新下发至中间节点(边缘服务器),中间节点再分发至实际执行训练的客户端(边缘设备),从而融合了集中式学习与联邦学习的优势,在降低通信开销的同时提升了训练效率与模型精度[13-14]。

尽管HFL在性能与通信效率方面展现出独特优势,但其训练过程仍面临数据异质性和系统可靠性等关键挑战。首先,由于数据来源、采样方式及环境条件存在差异,实际参与节点的本地数据往往具有显著差异,呈现出非独立同分布(Non-Independent and Identically Distributed,Non-IID)特征。Non-IID数据会使各客户端模型更新方向不一致,进而引发聚合偏差,导致全局模型的泛化能力下降,收敛速度降低,并在多层聚合结构中造成偏差传播与误差累积,从而降低训练效率[15-16]。其次,HFL训练过程对系统可靠性高度依赖。设备失效、网络波动和通信中断等因素都可能导致模型更新延迟甚至训练中断[17]。现有针对联邦学习可靠性的研究主要集中在通信可靠性[18-19]、模型可靠性[20-22]和设备可靠性[23-24]等方向,其中通信可靠性强调在复杂网络环境下的数据传输稳定性,模型可靠性关注防御恶意节点干扰,而设备可靠性则考虑客户端与云服务器的稳定性。然而,这些研究多假设边缘服务器处于理想状态。在边缘计算与物联网场景中,边缘服务器因部署环境复杂、运维条件受限,更易发生故障。作为组内聚合的核心节点,一旦失效,将引发局部聚合中断并对全局模型训练造成影响,因此亟须针对边缘服务器的可靠性进行研究。

针对上述挑战,本文受设备可靠性问题的启发,提出了一种可靠性感知的分层联邦学习(Reliability-aware Hierarchical Federated Learning,R-HFL)框架。该框架将训练过程划分为两个阶段:第一阶段为分组阶段,根据客户端与边缘服务器的地理位置、可靠性指标及语义特征进行分组,以优化聚合拓扑结构;第二阶段为全局模型聚合阶段,在分组内完成局部聚合后,将结果上传至中央服务器进行全局聚合。为进一步提升联邦学习系统在复杂环境下的鲁棒性,本文设计了一种可靠性感知的服务迁移策略:当边缘服务器发生故障时,能够将聚合任务动态迁移至其他可用服务器,在降低迁移开销的基础上,减轻故障对全局模型训练的影响。

本文的主要贡献如下。

(1)构建可靠性感知的分层联邦学习框架。在HFL中引入可靠性指标,优先选择高可靠性边缘服务器作为组内中间聚合器。同时,考虑边缘服务器可靠性的时变性与联邦训练的长期性,设计失效触发的迁移机制以保障训练连续性与聚合稳定性,并提升聚合效率与任务完成效率。

(2)设计语义-地理联合聚类和可靠性协同选择边缘服务器方法。基于客户端模型的语义表示与地理邻近性进行聚类,提升组内统计相似性,缓解Non-IID导致的梯度偏移。在此基础上结合可靠性指标进行协同决策,替代仅依赖参数距离或单一准则的选择方式,从源头降低聚合中断风险,增强系统鲁棒性。

(3)实现CTDE/MAPPO多目标动态迁移优化。将客户端迁移建模为MDP(Markov Decision Process),在CTDE框架下采用MAPPO进行可靠性驱动的多智能体迁移策略学习;通过奖励/约束统一权衡迁移成本、迁移后通信开销与语义分布匹配度,自适应选择目标边缘服务器,缓解迁移后的梯度发散,保持训练连续性与收敛效率,降低节点失效引发的中断与迁移开销。

(4)开展多场景实证验证。在真实数据集和不同的非独立同分布场景中进行实验。实验结果表明,所提方法在模型精度、收敛速度方面均优于其他方案。

1 相关研究

目前,关于联邦学习可靠性的研究主要集中于三个方面:通信可靠性、模型可靠性与设备可靠性。通信可靠性主要关注在联邦学习过程中由于通信环境不稳定所引发的问题;模型可靠性聚焦于参与节点在训练过程中的行为稳定性,尤其在面对潜在的恶意节点时;设备可靠性则指针对硬件故障或系统异常所设计的容错与恢复策略。

通信的不确定性及网络条件的动态变化,是影响联邦学习效率和模型收敛稳定性的关键因素。为此,研究者提出了多种机制以提升通信的稳健性。针对车联网中通信信道易受干扰的问题,Li等人[25]提出了一种基于可重构智能表面(Reconfigurable Intelligent Surface,RIS)的联邦学习架构。该方案通过优化RIS相移以增强车-边-云之间的通信链路,同时引入车辆能力指标来评估节点的可信度与资源状态,从物理层提升了通信质量。Ye等人[26]探讨了去中心化联邦学习在轻量级通信协议(如UDP)环境下的应用问题,提出Soft-DSGD算法以应对丢包与延迟问题。该算法可在部分信息丢失的情况下完成模型更新,并基于链路可靠性矩阵优化节点权重,从理论上保证了即使在通信不可靠网络中也能实现稳定收敛。Mao等人[27]进一步考虑了通信环境的动态性与不确定性,提出稀疏增强的联邦学习框架SAFARI。该方法通过本地稀疏学习减少通信开销,并结合客户端模型相似性对丢失的更新进行补偿,有效降低了由通信中断带来的模型偏差。

在模型行为层面,王鑫等人[28]针对数据拥有者参与意愿不足及模型易受攻击的问题,设计了基于区块链的激励与声誉机制。该机制基于训练效果与计算成本评估客户端贡献度,动态调整其声誉值,从而实现对参与节点行为的可控与可评估。Cai等人[29]提出联邦学习安全模型框架FLSM,引入实时恶意检测与模型审计机制,确保共享模型的完整性,有效防范模型中毒攻击,增强了系统协同的安全性。在客户端选择策略方面,Qin等人[30]提出了具备可解释性的个性化联邦学习方案RIPFL,基于社会学习机制筛选可靠节点参与训练,有效应对Non-IID数据引发的协同效率下降问题。为降低节点异质性和减少潜在敌对行为,Zhou等人[31]提出了分层社区式的联邦学习框架MR-FFL。该框架通过构建无人机节点的“同侪社区”与“同事社区”,结合社区信用机制,在提升系统公平性的同时增强了整体鲁棒性。

上述研究多数假设设备运行稳定,未考虑因节点失效导致的系统中断。然而,在边缘计算和物联网环境中,节点故障是普遍且不可避免的问题,其可能严重影响联邦学习任务的稳定执行。相比之下,关于设备可用性与硬件层面的容错研究仍较为有限。针对中间聚合设备,Sharma和Kaur[32]在云-雾-物环境中提出了一种可靠联邦学习机制,通过选取一组瞬时高可用的雾节点组成主导集作为本地聚合器,从节点可用性、通信延迟和计算能力等多维指标综合评估硬件可靠性,确保边缘计算资源的有效利用与训练任务的连续性。Han等人[33]针对客户端可靠性,提出了一种基于半马尔可夫过程的多维评估模型,用于定量分析客户端在遭受攻击及恢复过程中的表现,进而衡量其可靠性水平。Alosaime等人[34]提出了容错联邦学习框架FLARE,通过中央服务器的可用性预测模型对客户端进行智能选择,从而容忍设备可用性故障,提升系统稳定性。在全局服务器故障方面,Acar等人[35]通过部署多个全局模型副本,并采用共识算法同步其状态,即使主服务器故障也能保证系统继续运行。然而,多副本部署不仅显著增加了资源的消耗,而且未有效解决边缘层聚合节点失效问题,这一关键问题仍待进一步深入研究与解决。

云服务器通常由专业运维团队管理,具备较高的可靠性与冗余备份能力,发生故障的概率相对较低。终端设备在发生断线或故障时,主要影响其本地数据

的训练参与,对整体模型训练的影响相对有限,其他终端仍可继续完成本地更新。然而,边缘服务器通常部署在基站或网络边缘,地理位置分散且缺乏专业运维支持,其故障概率明显高于云端服务器。一旦边缘服务器发生故障,将导致所连接的大量终端设备所训练的本地模型无法完成聚合,严重影响模型的全局收敛速度与系统整体性能。因此,在边缘服务器发生故障时,如何实现终端设备的高效迁移与接入切换,是保障联邦学习系统鲁棒性与连续性的关键问题,其相关研究具有重要的价值。

2　系统模型与优化问题

2.1　联邦学习优化模型

在传统集中式的FL中,系统旨在通过单一中心服务器对所有客户端模型进行集中聚合,以最小化全局损失函数$L(W)$来学习全局模型参数,其优化目标可表示为

$$\min_w L(W)=\min_w \sum_{i=1}^{N}\frac{E_i}{E}\times L_i(w) \tag{1}$$

其中,E_i表示第i个客户端本地数据集的样本数量,E表示全部客户端总样本数量,$L_i(w)$表示客户端k的本地损失函数。

在实际应用中,各客户端的数据分布通常呈现显著的Non-IID特性,这会导致模型更新产生明显偏移,从而降低全局模型的收敛性能。针对Non-IID数据带来的性能退化与经典联邦学习的通信开销问题,本文设计分层联邦学习架构。客户端首先在边缘服务器侧进行组内聚合,再由云端执行组间聚合,以提升局部聚合的一致性并改善整体收敛性能。

$$\min_{\{w_k\}_{k=1}^{K}} \sum_{k=1}^{K}\frac{N_k}{N}F_k\left(w_k\right) \tag{2}$$

其中,w_k表示边缘服务器k聚合后的模型参数,$F_k\left(w_k\right)$表示边缘服务器k下的所有客户端的平均损失,K为边缘服务器的总数,N_k为边缘服务器k下参与训练的数据总量。

HFL虽能通过分层聚合缓解Non-IID导致的训练不稳定问题,但其云-边-端结构也产生了新问题:边缘服务器通常处于网络波动、资源受限或连接不稳定的环境中,存在一定的故障概率。一旦边缘服务器在训练过程中发生故障,组内聚合将被迫中断,会影响云端聚合的连续性,进一步影响式(2)的优化目标。为此,本文在后续章节中引入边缘服务器可靠性指标,并进一步提出可靠性感知的客户端聚类分组与迁移决策机制,以保障分层聚合过程的鲁棒性,进一步保障式(2)的可持续优化。

2.2　数据分布相似性计算模型

为了实现高效地聚类与客户端迁移决策,本文构建了数据分布相似性计算模型,用于衡量客户端间的统计差异与语义相关性。客户端的数据分布特性直接影响组内模型的梯度一致性与全局训练收敛性能。因此,一种准确、轻量且隐私友好的相似性度量机制对于聚类优化与迁移优化至关重要。

现有方法通常基于样本类别比例统计来刻画客户端的数据分布,虽然能够直观反映标签差异,但存在两方面问题。首先,类别统计信息需要在客户端间共享或上传至服务器,增加了额外的通信负担;其次,样本级统计可能间接暴露数据分布特征,带来潜在的隐私泄露风险,与联邦学习旨在降低数据泄露概率的初衷相悖。为避免直接传输样本信息,部分研究提出了基于特征原型的聚类方法,即各客户端利用本地模型提取不同类别的特征中心,并将其上传至服务器,从而实现聚类与迁移决策。然而,该类方法仍存在两点局限:一方面,特征原型的维度通常与神经网络中间层规模相关,随模型复杂度的增加而显著提升,从而导致通信和存储开销急剧上升;另一方面,上传高维特征原型仍需额外的本地前向计算与特征聚合操作,增加了客户端的计算负载。此外,传统的服务器选择方法往往依赖参数空间中的距离度量(如欧几里得距离)来衡量模型差异,但这种参数级的距离难以从语义层面反映模型性能的实际差别,且在高维空间中常出现“距离退化”现象,导致相似性评估不可靠。此外,部分服务器选择策略基于参数空间距离(如欧氏距离)度量模型差异,但此类参数级度量难以反映模型在语义输出空间的性能差异,并在高维空间中出现距离退化,导致相似性评估不稳定

鉴于上述不足,本文提出一种基于语义预测分布的相似性度量方法。该方法不直接传输样本数据,而是使用客户端模型在共享评估数据集上的预测概率分布,以此计算语义层面的模型相似性。该方法的核心思想是边缘服务器的选择应依据模型在特定任务中的预测行为(任务能力),而非仅依赖模型参数之间的距离,具体步骤如下。

(1)任务能力评估

在每轮训练结束后,服务器端使用预先准备的辅助共享数据集$\mathcal{D}_{\text{share}}$对各客户端本地模型进行统一评估。该数据集包含类别均衡的样本,不参与本地训练,仅用于相似性计算。对于客户端i的本地模型$f_i(\cdot;w_i)$,其在样本$\hat{x}\in\mathcal{D}_{\text{share}}$上的预测概率分布为

$$\boldsymbol{P}_i(\hat{x})=\sigma\left(f_{\text{dec}}\left(f_{\text{enc}}(\hat{x};w_i)\right)\right)\in\mathbb{R}^C \tag{3}$$

其中,f_{enc}是特征提取层,f_{dec}是决策层,w_i是客户端i的模型参数,$\hat{x}$是测试样本,C为类别总数,$\sigma(\cdot)$为Soft-

max 函数，向量 $\boldsymbol{P}_i(\hat{x})$ 的每一维表示模型预测该样本属于相应类别的概率。

(2)能力矩阵构建

将客户端 i 在全部 N 个辅助样本上的预测概率向量按样本顺序拼接，得到任务能力矩阵：

$$\boldsymbol{P}_i=\begin{bmatrix}\boldsymbol{P}_i(\hat{x}_1)^{\top}\\ \boldsymbol{P}_i(\hat{x}_2)^{\top}\\ \vdots\\ \boldsymbol{P}_i(\hat{x}_N)^{\top}\end{bmatrix}\in\mathbb{R}^{N\times C} \tag{4}$$

该矩阵综合反映了模型在不同样本及类别上的预测行为模式。

(3)语义相似性计算

为了衡量客户端间的预测模式相似度，本文采用基于 Frobenius 范数归一化的余弦相似度进行计算，其定义为

$$\boldsymbol{A}_{ij}=\frac{\left\langle \boldsymbol{P}_i,\boldsymbol{P}_j\right\rangle_F}{\left\|\boldsymbol{P}_i\right\|_F\cdot\left\|\boldsymbol{P}_j\right\|_F} \tag{5}$$

其中，$\langle\cdot,\cdot\rangle_F$ 表示矩阵的 Frobenius 内积，$\|\cdot\|_F$ 为 Frobenius 范数。该相似度取值范围为[0,1]，数值越大表示两个客户端模型的预测概率分布模式越接近。

从计算复杂度上看，辅助数据集仅用于前向推理，不涉及反向传播或参数更新，因此其计算量远低于本地训练过程。即便辅助样本数量增加，计算负载也仅线性增长，不会对总体效率造成显著影响。此外，当辅助样本覆盖主要类别后，语义相似性估计结果趋于稳定，聚类性能对样本规模变化不敏感，表明该机制在样本数量上具有良好的鲁棒性与可扩展性。

2.3 服务迁移模型

为了确保在边缘服务器发生故障时联邦学习过程仍能持续稳定运行，本文在迁移决策中综合考虑数据分布、迁移成本、通信开销及目标服务器的可靠性等因素。基于此，构建了服务迁移模型，用于量化终端设备从故障服务器迁移至可用服务器时产生的额外资源开销。该模型包括迁移成本与通信成本两部分。

2.3.1 迁移成本

终端设备从服务器 s_i 迁移到其他服务器 $s_j\in S$，产生迁移成本 b_i，假设该成本是 x 的非递减函数，其中 x 是 s_i 和 s_j 之间的距离，即 $x=\|s_j-s_i\|_2$。迁移成本函数定义为

$$b(x)=\begin{cases}0, & \text{if } x=0\\ \beta_c+\beta_l\mu^x, & \text{if } x>0\end{cases} \tag{6}$$

当 $x=0$ 时，表示未进行迁移；当 $x>0$ 时，代表客户端进行了迁移，成本主要包括固定成本 β_c 和指数成本 $\beta_l\mu^x$。β_c 代表迁移过程中不可避免的固定开销(如中断时间)，$\beta_l\mu^x$ 表明迁移成本随迁移距离增加呈指数增长，用以反映因长距离迁移条件下网络时延、数据传输时间及切换开销所导致的综合影响。

2.3.2 通信成本

除迁移成本外，客户端还需与新的中间聚合节点(边缘服务器)进行通信，从而产生额外的通信开销。通信成本与可能迁移后服务器和客户端之间的距离有关，定义为一般的非递减函数 $c(y)$，其中 $y=\|s_j-u_i\|_2$。设 $c(0)=0$，因此，通信成本可表示为

$$c(y)=\begin{cases}0, & \text{if } y=0\\ \delta_c+\delta_l\theta^y, & \text{if } y>0\end{cases} \tag{7}$$

其中，δ_c 是基础通信开销，反映了连接建立、信号初始化等固定成本；δ_l 与 θ 控制了传输成本的距离依赖性，通常以指数形式增长，以模拟由于距离增大带来的信号衰减、传输延迟增多及可能的误码率上升等问题。

2.4 问题定义

为实现分层联邦学习在云-边-端两级聚合结构下的优化目标(式(2))，本文从客户端聚类优化和迁移决策优化两个方面展开研究。前者旨在缓解数据异质性带来的梯度偏移与收敛不稳定问题，从而提升模型的整体收敛速度与训练效率；后者则针对边缘服务器失效的情形下，设计可靠性驱动的迁移机制，以保障训练的连续性与系统鲁棒性。

2.4.1 聚类优化问题

在实际的 HFL 框架中，客户端仅能与部分边缘服务器建立稳定通信连接。通信可达性受地理距离、信号覆盖及网络链路条件限制，因此客户端只能加入可通信的边缘服务器。此外，不同边缘服务器的可靠性存在差异，若选取可靠性较低的服务器作为聚合中心，可能导致局部模型聚合失败，从而影响全局收敛。与此同时，边缘服务器的带宽资源有限，无法同时接入过多客户端，因此在聚类过程中需要兼顾带宽约束与可靠性因素。

设客户端集合为 $C=1,2,\cdots,n$，边缘服务器集合为 $\mathcal{E}=e_1,e_2,\cdots,e_M$，对于客户端 i，其可通信集合为 $\mathcal{E}_i=\{e_m\in\mathcal{E}\,|\,i\leftrightarrow e_m\}$。

在保证客户端仅能分配至可通信服务器的前提下，定义聚类优化目标如下：

$$\text{P1:}\quad \min_{\{x_{i,m}\}}\sum_{i\in\mathcal{C}}\sum_{m=1}^{M}x_{i,m}\left(\lambda_1 D(c_i,g_m)-\lambda_2 R_m\right)$$

$$\text{s.t.}\begin{cases}\text{C1}\quad \sum_{m=1}^{M}x_{i,m}=1, & \forall i\in\mathcal{C}\\ \text{C2}\quad \sum_{i\in\mathcal{C}}x_{i,m}B_{i,m}\le B_m^{\max}, & \forall e_m\in\mathcal{E}\\ \text{C3}\quad x_{i,m}\in\{0,1\}, & \forall i\in\mathcal{C},\forall e_m\in\mathcal{E}\end{cases} \tag{8}$$

其中,$D(c_i,g_m)$表示客户端i与边缘服务器e_m所对应的聚类中心g_m在语义特征空间中的距离,R_m为边缘服务器e_m的可靠性指标,λ_1、λ_2为语义与可靠性权重系数,约束条件C1表示客户端c_i只能分配给一个服务器,约束条件C2表示每个边缘服务器的带宽资源有限,约束条件C3表示聚类变量为二元变量。

2.4.2　客户端迁移优化问题

为描述客户端迁移过程,构建一个基于数学规划的形式化模型,旨在带宽约束下优先选择高可靠性的目标边缘服务器,同时兼顾迁移后的数据分布一致性,并最小化整体迁移成本。设需要迁移的客户端集合为$\mathcal{I}=\{1,2,\cdots,N\}$,候选边缘服务器集合为$\mathcal{J}=\{1,2,\cdots,M\}$。每个客户端的效用可形式化表述为

$$K_i^{\text{tot}}=\lambda_{\text{sim}}\sum_{i\in\mathcal{I}}A_{ij}x_{ij}+\lambda_{\text{rel}}\sum_{i\in\mathcal{I}}R_j x_{ij}-\lambda_{\text{mir}}\sum_{i\in\mathcal{I}}b_{ij}x_{ij}-\lambda_{\text{com}}\sum_{i\in\mathcal{I}}c_{ij}x_{ij} \tag{9}$$

其中,$x_{ij}\in\{0,1\}$为二元决策变量,若$x_{ij}=1$,则表示客户端i迁移至服务器j;A_{ij}表示需要迁移的客户端i的数据分布情况与以边缘服务器j作为中间聚合节点的客户端数据分布的相似度;R_j表示服务器j的可靠性;b_{ij}表示客户端i迁移到边缘服务器j的迁移成本;c_{ij}表示客户端i迁移到边缘服务器j的通信成本。

为了优化系统的整体迁移性能,在单客户端的综合效用K_i^{tot}基础上定义平均系统效用K_{ave}。该概念表示当边缘服务器发生故障时,所有需要迁移的客户端的效用算术平均,能够反映系统层面的整体迁移效用。其形式化定义为

$$K_{\text{ave}}=\frac{1}{N}\sum_{i=1}^{N}K_i^{\text{tot}} \tag{10}$$

因此,优化目标可形式化表述为

$$\text{P2: }\max_{x_{ij}}\ \frac{1}{N}\sum_{i=1}^{N}K_i^{\text{tot}}$$

$$\text{s.t.}\begin{cases}\text{C1: }\ \sum_{j\in\mathcal{J}}x_{ij}=1, & \forall i\in\mathcal{I}\\ \text{C2: }\ \sum_{i\in\mathcal{I}}s_i x_{ij}\leqslant B_j, & \forall i\in\mathcal{I},\forall j\in\mathcal{J}\\ \text{C3: }\ x_{ij}\in\{0,1\}, & \forall i\in\mathcal{I},\forall j\in\mathcal{J}\\ \text{C4: }\ \sum_{n\in u(t)}B_j^n\leqslant B_j, & \forall j\in S_{\text{mid}}\end{cases} \tag{11}$$

其中,N表示需要迁移的客户端数量;约束条件C1和C2表示边缘设备i只能被分配到一个目标服务器,并且目标服务器的带宽资源不会被超出;约束条件C3表示客户端i是否迁移到边缘服务器j;约束条件C4表示中继节点(位于客户端与目标服务器之间、仅负责通信转发而不执行聚合的中间节点)的带宽占用不得超过其可用带宽资源。

由于客户端的服务迁移决策变量是二元变量,使得问题P2呈现出非凸性。此外,问题还需考虑资源的有限性与数据分布的特性,这进一步增加了问题求解的难度。传统优化方法在应对这类复杂性时往往表现不佳。相比之下,深度强化学习具备通过与环境的实时交互学习最优策略的能力。因此,本文提出了一种基于深度强化学习(Deep Reinforcement Learning,DRL)的方法来高效求解问题P2。

3　可靠性感知的分层联邦学习方法

在分层联邦学习场景下,考虑到边缘服务器靠近终端设备、易受资源限制或故障影响,本文在训练过程中引入可靠性感知机制。首先,在客户端与边缘服务器的可通信范围内,以语义相似度和地理位置为依据进行聚类,并优先选择高可靠、带宽充足的边缘服务器作为组内聚合节点,以缓解Non-IID数据导致的收敛不稳定问题。其次,当检测到服务器失效或性能异常时,将客户端迁移建模为马尔可夫决策过程(MDP),并基于深度强化学习设计最优迁移策略,从而在保证系统可靠性的前提下,最小化资源成本,维持联邦训练的连续性,并增强系统整体鲁棒性。

3.1　可靠性感知的聚类算法

为缓解Non-IID数据分布带来的模型收敛不稳定问题,本文提出可靠性感知的聚类方法。该方法通过在边缘层对客户端进行分组,使组内数据分布趋于一致性,从而提升模型的收敛速度与稳定性。首先筛选可用的聚合节点集合(边缘服务器),再在其可通信域内根据语义相似性对客户端进行分组。

考虑到边缘服务器的可靠性和带宽资源差异,依据前文定义的可靠性指标与通信约束条件,对边缘服务器进行初步筛选。候选服务器需同时满足可靠性阈值与带宽容量要求,以保证聚合过程的可行性与鲁棒性。筛选后的服务器集合将作为后续聚类的候选节点,筛选出的集合可形式化表示为

$$\mathcal{E}^{\star}=\left\{e_m\in\mathcal{E}\,\middle|\,R_m\geqslant R_{\text{th}},B_m^{\max}\geqslant B_{\min}\right\} \tag{12}$$

其中,$\mathcal{E}^{\star}$表示候选边缘服务器集合,R_m为边缘服务器e_m的可靠性指标,$B_m^{\max}$表示e_m最大可用带宽,R_{th}和$B_{\min}$分别表示可靠性与带宽阈值。

基于候选边缘服务器集合进行分组,主要步骤如下。

(1)根据客户端与服务器之间的可通信关系,确定每个服务器的可通信客户端集合,为后续语义聚类提供边界约束。

(2)在可通信域内,根据客户端模型特征或梯度分布的语义相似度进行分组,使同组内客户端的数据分布更加一致。

（3）在聚类过程中引入服务器可靠性，优先选择高可靠、带宽充足的服务器，以提升整体聚合的稳定性和通信效率。

3.2 基于MDP的客户端迁移算法

在分层联邦学习场景中，边缘服务器通常作为多个客户端的中间聚合节点。当某一边缘服务器发生故障时，其所属的多个客户端需同步触发迁移，并在多个候选边缘服务器之间完成选择，从而形成典型的多对多迁移问题。为此，本文将每个待迁移客户端建模为一个智能体，采用多智能体强化学习（Multi-Agent Reinforcement Learning，MARL），并在集中式训练-分布式执行（Centralized Training with Decentralized Execution，CTDE）范式下，基于多智能体近端策略优化（Multi-Agent Proximal Policy Optimization，MAPPO）学习最优迁移策略。为描述“多客户端-多边缘服务器”的迁移决策过程，本文在离散时刻 $t=0,1,\cdots,T$ 定义客户端集合 $\mathcal{I}=\{1,2,\cdots,N\}$、候选边缘服务器集合 $\mathcal{J}=\{1,2,\cdots,M\}$。以下分别给出全局状态（global state）、智能体的观测空间（observation space）、动作空间（action space）与奖励函数（reward function）的形式化定义。

全局状态。包括需要迁移客户端的模型、需要迁移客户端需要的带宽资源、目标边缘服务器可用的带宽资源、目标边缘服务器所在的边缘计算节点数据分布情况、目标边缘服务器的位置。

$$S(t)=(L_{\mathcal{I}}(t),b_{\mathcal{I}}(t),d_{\mathcal{I}},L_{\mathcal{J}}(t),B_{\mathcal{J}}(t),D_{\mathcal{J}},R_{\mathcal{J}}) \tag{13}$$

其中，关于客户端的变量是 N 维状态变量，边缘服务器的是 M 维状态变量。$L_{\mathcal{I}}(t)$ 表示所有需要迁移的客户端的位置，$L_{\mathcal{J}}(t)$ 表示可迁移边缘服务器的位置，$b_{\mathcal{I}}(t)$ 表示源边缘服务器分配给用户的带宽资源，$d_{\mathcal{I}}(t)$ 表示需要迁移的客户端的模型，$B_{\mathcal{J}}(t)$ 表示候选边缘服务器目前的剩余可用带宽资源，$D_{\mathcal{J}}$ 表示候选边缘服务器的模型，$R_{\mathcal{J}}$ 表示候选服务器的可靠性。

智能体观测空间。为保证分布式可执行性，客户端 i 在时刻 t 的局部观测定义为

$$o_i(t)=\left(L_i(t),b_i(t),d_i(t),\left\{L_s(t),B_s(t),D_s(t),R_s\right\}_{s\in\mathcal{J}}\right) \tag{14}$$

动作。在当前状态下 $S(t)/o_i(t)$ 下，客户端 i 的动作是选择目标边缘服务器。

$$a_i(t)\in\mathcal{J} \tag{15}$$

奖励。在当前状态下 S_t，系统执行动作 a_i 将获得一个奖励值。优化目标是最小化迁移成本，最大化选择服务器的可靠性和最大化数据分布的相似度，因此单个客户端的奖励可以定义为 $R=K_i^{\text{tot}}$。于是，本文将所有用户的平均奖励函数定义为

$$R_{\text{ave}}=\frac{1}{N}\sum_{i=1}^{N}U\left(s(t),a(t)\right) \tag{16}$$

3.3 可靠性感知的分层联邦学习算法

本文提出的可靠性感知的分层联邦学习（R-HFL）系统架构如图1所示，由客户端层、边缘层与云中心层三部分构成。整体流程如算法1所述。在分组阶段，依据客户端的数据分布特征与地理位置，并结合候选边缘服务器的可靠性指标与覆盖关系，对参与客户端进行分组；将选定的边缘服务器作为组内聚合节点，负责完成组内的初步模型聚合。在分层聚合阶段，各边缘服务器将组内模型聚合结果上传至云中心。云中心在汇集所有边缘聚合结果后进行全局模型聚合，并将更新后的全局模型下发至各边缘服务器，由其进一步分发至组内客户端，进行下一轮训练。上述过程不断迭代，直至模型收敛或达到最大训练轮次。

考虑到联邦训练过程中边缘服务器可能出现故障或性能退化问题，R-HFL设计了基于MAPPO的客户端服务迁移机制（框架见图2）。当监测到边缘节点失效或异常时，系统立即触发迁移策略，将其正在执行的聚合任务与关联客户端动态迁移至候选边缘服务器。迁移决策以最大化客户端平均效用为优化目标，兼顾服务器可靠性、带宽与容量约束以及数据分布一致性，从而在动态环境下保障训练过程的连续性与鲁棒性。

本文采用MAPPO的CTDE结构，训练期由集中式Critic接收全局状态，以估计团队价值并降低优势估计方差；执行期各分布式Actor仅依据客户端局部观测独立做出迁移选择。优化器采用PPO-clip，通过近端约束与熵正则提升训练稳定性与样本效率。具体如下所述。

Actor（客户端策略）。给定客户端 i 局部观测 o_i 与可行性掩码 $\text{mask}_{i,\cdot}\in\{0,1\}$（约束不可行动作，如带宽不足时，置为0），策略头输出动作概率如下：

$$\pi_\theta\left(s\middle|o_i\right)=\frac{\exp\left(z_{i,s}\right)}{\sum\limits_{s':\ \text{mask}_{i,s'}=1}\exp\left(z_{i,s'}\right)} \tag{17}$$

其中，s 为服务器动作索引，$z_{i,s}$ 表示未归一化得分，θ 为策略网络参数。

Critic（集中式价值网络）。对全局状态 s_t 估计团队回报：

$$V_\phi\left(s_t\right)\approx\mathbb{E}\left[\sum_{k\geqslant 0}\gamma^k r_{t+k}\middle|s_t\right] \tag{18}$$

其中，ϕ 为价值网络参数，$\gamma\in[0,1]$ 为折扣因子，r_t 为团队即时奖励。

广义优势估计（Generalized Advantage Estimation，

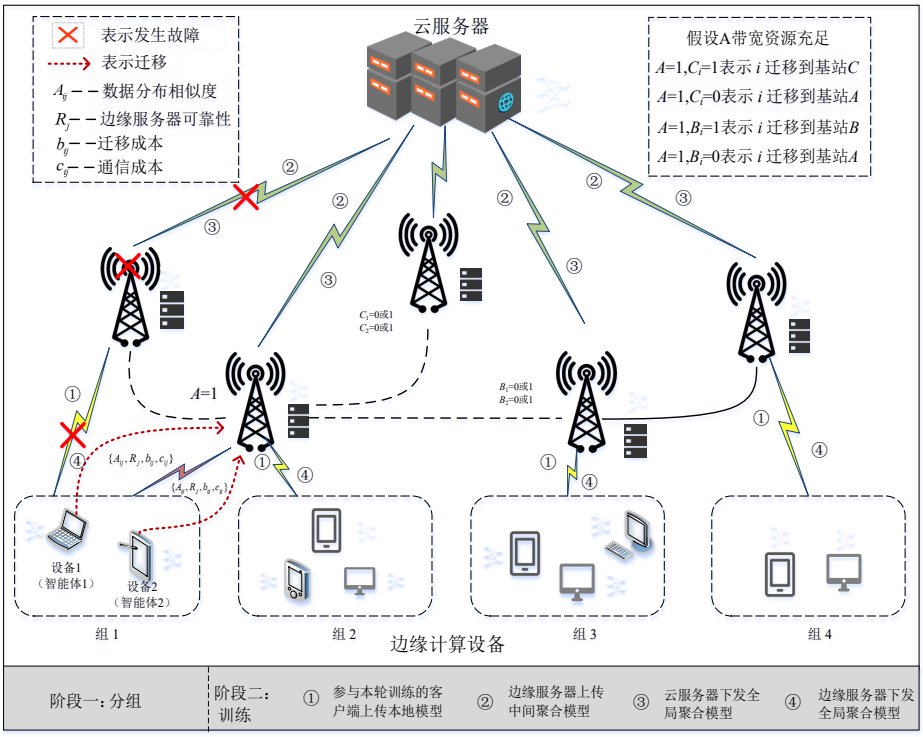

图 1　可靠性感知的分层联邦学习框架

Figure 1　Reliability-aware hierarchical federated learning framework

GAE):

$$\hat{A}_t=\sum_{\ell\geqslant 0}(\gamma\lambda)^{\ell}\left(r_{t+\ell}+\gamma V_{\phi}\left(s_{t+\ell+1}\right)-V_{\phi}\left(s_{t+\ell}\right)\right) \tag{19}$$

其中,$\lambda\in[0,1]$为 GAE 系数。

PPO-clip(Actor 损失):

$$L_{\text{actor}}=\mathbb{E}\Big[\min\left(\rho_t\hat{A}_t,\text{clip}\left(\rho_t,1-\varepsilon,1+\varepsilon\right)\hat{A}_t\right)+\beta_{\text{ent}}\mathcal{H}\left(\pi_{\theta}(\cdot\mid o)\right)\Big],\quad \rho_t=\frac{\pi_{\theta}(a\mid o)}{\pi_{\theta_{\text{old}}}(a\mid o)} \tag{20}$$

其中,a 与 o 为采样的动作与对应的观测,θ_{old} 为本轮更新前冻结的旧策略,$\varepsilon>0$ 为截断半径,$\beta_{\text{ent}}\geqslant 0$ 为熵正则系数,$\mathcal{H}(\cdot)$为策略熵。

Critic 损失:

$$L_{\text{critic}}=\mathbb{E}\left(V_{\phi}-\hat{V}_t\right)^2 \tag{21}$$

其中,$\hat{V}_t=\hat{A}_t+V_{\phi}(s_t)$为 Critic 的回归目标。

基于 MAPPO 进行客户端迁移算法主要包括样本采集和模型训练两个部分(见算法 2)。样本采集阶段采用顺序采样的原则,对需要迁移的客户端依次生成局部观测与可行性掩码,并在掩码约束下由 π_{θ} 选择迁移动作;动作执行后,即时更新边缘服务器的剩余资源和模型,并将样本写入经验池。模型训练阶段从经验池按小批量抽样,先用冻结的价值网络计算 GAE 优势与价值目标,再采用 PPO-clip 更新策略网络并以均方误差(Mean Squared Error,MSE)回归更新价值网络;本轮用毕的样本即弃,以保持近端性。所有客户端完成选择后,计算当前时隙的平均效用作为团队奖励,并对该时隙内样本统一回填。

4　实验验证

本节首先对实验设置进行简单说明,其次对 MAPPO 算法进行参数敏感性分析,最后通过消融实验及与其他方法的对比验证 R-HFL 算法的有效性。

4.1　实验设置

为了全面评估所提出算法的性能,本文分别采用 Mcmahan 等人[36]提出的 Pathological 分布方法和基于 Dirichlet 分布的划分策略,对数据集进行划分,设计了三类典型的非独立同分布(Non-IID)实验场景。其中,场景 1 与场景 2 体现标签类别分布的差异,而场景 3 用于模拟样本数量不均衡导致的 Non-IID 特性。

非独立同分布场景 1,采用 Pathological 划分方法,每个客户端仅包含 4 个不同类别的数据样本,类别之间重叠较少,能够体现高度异质性的数据分布。

非独立同分布场景 2,同样采用 Pathological 划分方法,但每个客户端包含 6 个不同类别的数据样本,客户端之间的类别重叠相对增多,属于中等异质性的数据分布。

非独立同分布场景 3,客户端数据划分遵循 Dirich-

算法 1 可靠性感知的分层联邦学习算法

输入：客户端集合 $C=\{1,2,\cdots,n\}$，辅助数据集 $\mathcal{D}_{\text{share}}$，边缘服务器集合 $\mathcal{E}=\{e_1,e_2,\cdots e_M\}$，阈值：$\alpha$，位置信息 $\text{cover}(i,m)\in\{0,1\}$

输出：最终全局模型 W^g

云服务器：

对客户端分组 GROUP_BY_SIMILARITY(w, cover, α, $\mathcal{E}$)

FOR 全局轮次 $t=1,2,\cdots,T$ DO

接收并聚合各边缘服务器上传的模型 w_e^t：

$$\theta_{\text{global}}^t \leftarrow \sum_{e=1}^{M}\frac{N_e}{N}w_e^t$$

向所有边缘服务器下发新一轮的全局聚合模型 θ_{global}^t

END FOR

边缘服务器：

FOR 每个边缘服务器 $e_M\in\mathcal{E}$ do

IF DETECT_FAILURE() = true THEN #判断边缘服务器是否可用

$C_m \leftarrow$ MIGRATE_ON_FAILURE(C_m, $\mathcal{E}$, cover)

END IF

END FOR

向所属客户端 $k\in C_m$ 下发最新的全局模型 θ_{global}^t

FOR $k\in C_m$ DO

$w_k \leftarrow$ CLIENT_UPDATE(w, h, b) #客户端进行本地训练，并将 w_k 上传到边缘服务器

END FOR

在边缘端进行模型聚合

$$\theta_{\text{middle}}=\sum_{k=1}^{K}\frac{E_k}{E}\times w_k$$

上传聚合模型 θ_{middle} 到云服务器

客户端：

CLIENT_UPDATE(w, h, b):

FOR epoch=1,2,$\cdots$,r DO

FOR 每个 batch b DO

$w \leftarrow w-\eta\cdot\nabla(w;b)$ #梯度下降

END FOR

返回训练后的模型参数 w

END FOR

let(α)分布，其中参数 α 用于控制数据异质性程度。具体而言，对每个类别的数据样本，依据 Dirichlet(α)分布生成各客户端的样本占比，再据此进行样本分配。

在上述不同场景下，客户端数量设置为 20，在第一轮对所有客户端进行分组，后续每一轮随机选取部分客户端参与训练，分别基于 CNN 模型在 MNIST[①]与 Fashion-MNIST[②]（FMNIST）两个公开数据集上开展实验。MNIST 数据集包含 70 000 张 28 × 28 灰度手写数字图像，类别数为 10；FMNIST 数据集同样包含 70 000 张 28 × 28 灰度图像，类别数为 10（服饰类别）。为模拟边缘服务器的动态不稳定性，本文基于 LANL[③]真实故障数据集获取服务器的可靠性，并在训练过程中引入故障机制。当某边缘服务器的可靠性值低于设定阈值时，将会触发故障，并退出聚合过程。该机制体现了服务器可靠性变化导致的失效特性，用以模拟网络波动、硬件异常等真实环境中的运行不确定性。同时，本文通过限制边缘服务器可连接客户端数量，模拟带宽资源的差异性。具体而言，每台服务器的可连接客户端上限服从[3,10]区间的离散均匀分布，反映边缘节点带宽资源的动态与异构性。

为验证本文所提方法的有效性与优势，设置了以下对比方案。其中，“无聚类方案”和“无迁移方案”作为消融实验，用于分别评估聚类机制与迁移策略的贡献。

（1）理想状况（Ideal）。考虑语义和地理位置进行分组，假设所有边缘服务器均稳定运行，无故障发生，作为性能上限参考。

（2）无聚类方案（No-Cluster）。不考虑客户端之间的语义或地理特征差异，所有客户端直接与单一云服务器进行全局聚合，不设置边缘层，也不涉及故障发生或迁移操作。该方案等价于经典的联邦平均（FedAvg）算法。

（3）无迁移方案（Failures（No-Migration））。考虑语义和地理位置进行分组，边缘服务器发生故障时，不采取迁移措施，体现系统最脆弱的情况。

（4）基于 DQN 的迁移策略（DQN Migration）。考虑语义和地理位置进行分组，在服务器发生故障时采用 DQN 学习迁移策略。

（5）EsPerRHFL[12]。一种云边端协同的个性化联邦学习算法，通过自适应参数融合与相似性聚合提升模型性能与跨边缘协作效果，不考虑发生故障时的处理策略。

在实验指标方面，本文重点考虑以下三个方面。

（1）测试准确度。衡量全局模型在测试集上的分类性能。

（2）收敛速度。以达到给定精度所需的通信轮次或训练轮次为评价标准。

（3）奖励值。在涉及迁移决策的实验中，通过奖励函数综合反映迁移策略在精度、通信与迁移开销等方面的综合效果。

实验平台为 Ubuntu 16.04 LTS 操作系统，硬件环境为 Dell PowerEdge R740 服务器，配备 128 GB 内存、8 TB 存储空间，并搭载 NVIDIA GeForce RTX 4080 GPU 作为计算加速器。联邦学习仿真环境基于 PyTorch 框架实现。

①http://yann.lecun.com/exdb/mnist。

②https://github.com/zalandoresearch/fashion-mnist。

③http://institute.lanl.gov/data/fdata/。

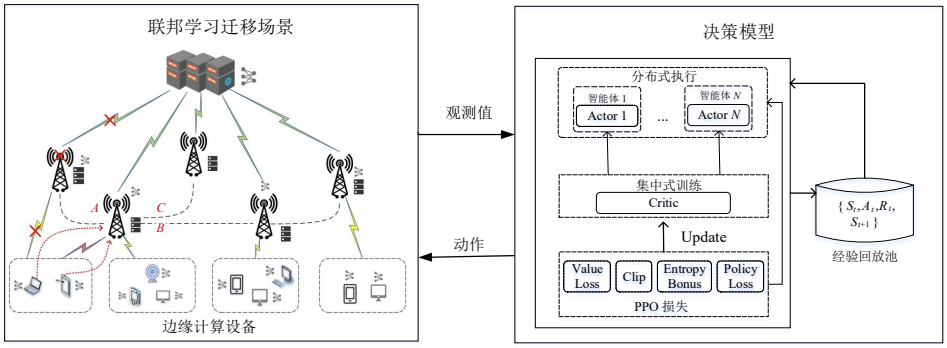

图2　基于MAPPO的聚合服务迁移框架

Figure 2　MAPPO-based aggregation service migration framework

算法2　顺序-基于MAPPO客户端迁移决策

输入:待迁移客户端集合$\mathcal{I}=\{1,2,\cdots,n\}$,边缘服务器集合$\mathcal{J}=\{1,2,\cdots,M\}$,位置信息$\text{cover}(i,m)\in\{0,1\}$

初始化:共享策略网络(Actor)π_θ,集中式价值网络(Critic)V_ϕ;经验池$D\leftarrow\phi$

样本采集

对需要迁移的客户端i依次执行:

Step1:生成客户端局部观测o_i与掩码(不可选的服务器设置为0);

Step2:由π_θ采样得到a_i;

Step3:根据客户端选择的动作a_i,即时更新服务器剩余资源情况和模型;

Step4:记录样本$(o_i,a_i,\log\pi_\theta,s_i,\text{mask}_i)$并存放到经验池$D$;

Step5:当客户端顺序执行完成后,计算所有客户端的平均效用,如式(10)所示。

模型训练

Step1:设定更新轮次,每次从经验池D中采样若干mini-batch的样本;

Step2:Critic基于全局状态序列使用GAE计算优势与目标回报,如式(19)所示;

Actor采用PPO-clip进行更新,如公式(19)所示;

Critic采用MSE回归,如公式(20)所示;

Step3:完成本轮后同步旧策略参数$\theta^{\text{old}}\leftarrow\theta$。

4.2　实验结果分析

本节首先对MAPPO超参数进行选取与敏感性分析,以获得稳定的迁移策略学习配置;然后,在此基础上进一步从平均迁移奖励、FL模型收敛速度、FL模型测试准确率三个方面对本文方案与对比方案进行系统评估。

图3展示了在仿真结果下,MAPPO在不同学习率下的平均奖励变化趋势。结果表明:(1)当学习率设置过低时,Actor的参数更新幅度过小,导致迭代效率偏低,模型难以及时收敛;(2)随着学习率的增加,收敛速度明显提升,但如果学习率过大,则在优化过程中更容易越过最优点,导致奖励值在高频振荡中趋于不稳定,甚至出现收敛减慢的现象。结合多组实验结果,本文最终将Actor和Critic的学习率均设定为9×10^{-4},以在收敛速度和稳定性之间取得平衡。图4进一步展示了在该学习率配置下Critic的收敛过程。可以观察到,Critic网络在早期阶段能够快速降低估计误差,并在后期保持较为平稳的收敛趋势。这表明合理的学习率不仅有助于Actor策略的更新,还能提升Critic对价值函数的拟合精度,从而整体改善MAPPO的训练稳定性与最终性能。

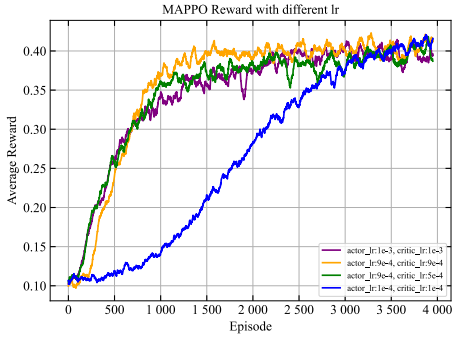

图3　MAPPO参数敏感性测试

Figure 3　MAPPO parameter sensitivity analysis

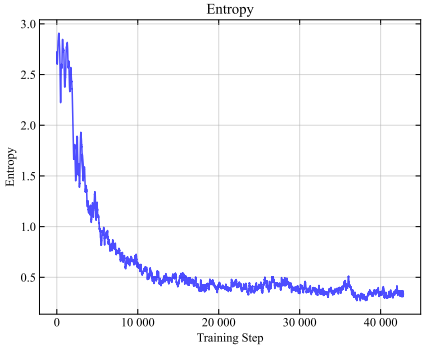

图4　MAPPO Critic收敛过程

Figure 4　MAPPO Critic convergence process

图5展示了基于DQN和基于MAPPO的两种迁移策略在仿真环境下的奖励表现。结果表明，DQN在训练初期能够凭借快速的Q值更新和离散动作优势暂时获得较高奖励。相比之下，MAPPO由于策略梯度更新较为保守且涉及多智能体的复杂性，前期奖励较低，但随着训练推进，其平均奖励最终超过DQN，展现出更优的稳定性和长期性能。

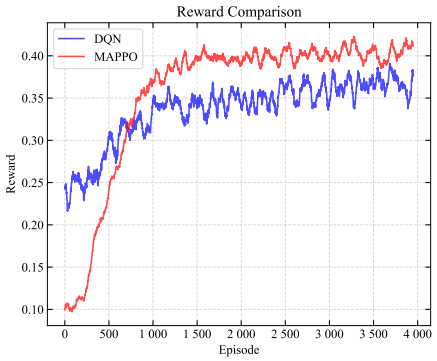

图5 不同DRL算法的奖励值收敛情况

Figure 5 Reward convergence of different DRL algorithms

图6和图7展示了在非独立同分布场景1下（使用MNIST数据集）各算法的对比。理想状况（Ideal）代表系统性能上限，作为参考。与之相比，无聚类（No-Cluster）方案的收敛速度与最终精度均显著降低，说明在Non-IId情况下缺乏聚类机制会导致梯度发散，从而减缓模型收敛。引入聚类机制后，模型整体收敛性得到提升，但当边缘服务器发生故障且未进行迁移（Failures-No Migration和EsPerHFL）时，收敛速度明显减慢，最终精度显著下降，表明在发生故障后，如不进行处理，就会对系统性能产生显著的不良影响。Failures-No Migration方案在初始阶段优先选择了可靠性较高的边缘服务器参与聚合，因此其在收敛速度和最终精度方面均优于缺乏故障感知机制的EsPerHFL。在可靠性约束下的聚类方案（包括Ideal、DQN Migration和本文提出的R-HFL）中，模型均在迭代约10轮后趋于收敛，测试精度普遍超过97%。在迁移策略方面，基于DQN的迁移方法（DQN Migration）能够在一定程度上减轻故障带来的性能下降，但相较于基于MAPPO的迁移策略，其在高维状态下的学习稳定性和策略泛化能力仍存在不足，这表明MAPPO更适用于本文所研究的故障恢复场景。值得注意的是，采用MAPPO迁移机制的R-HFL在迭代过程中展现出略优于理想情况下的收敛性能。其原因在于，该机制能够在边缘服务器发生随机故障后及时识别并迁移受影响的客户端，使部分服务器获得更丰富的数据规模，从而在保证系统可靠性的同时，使全局模型更接近最优解。

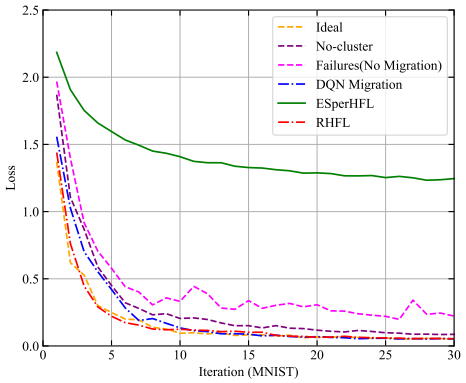

图6 联邦学习模型在不同算法下的收敛情况(场景1)

Figure 6 The convergence rate of the federated learning model under different algorithms (scenario 1)

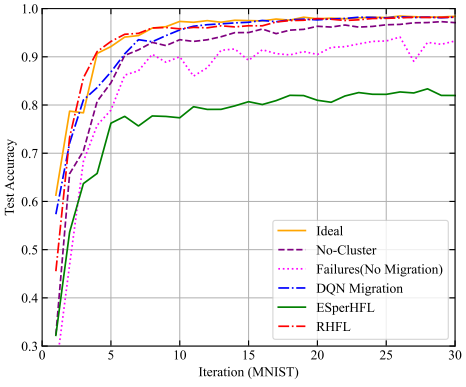

图7 不同算法达到特定准确率需要的迭代轮次(场景1)

Figure 7 The communication rounds required to reach a target accuracy under different algorithms (scenario 1)

为进一步验证本文方案的有效性，图8和图9展示了在非独立同分布场景2下（使用FMNIST数据集）的对比结果。整体来看，无聚类方案（No-Cluster）在训练过程中收敛波动明显，进一步验证了在Non-IID环境下引入聚类机制对于提升模型稳定性和收敛效率的重要性。在该场景中，本文提出的R-HFL方案整体性能最优，其精度曲线接近理想状况（Ideal），而基于DQN的迁移方法在多数迭代阶段低于理想状况。经过30轮训练后，各算法均趋于收敛，理想方案（Ideal）的最终测试精度为87.11%，无聚类方案为83.32%，发生故障未迁移方案（Failures-No Migration）为77.37%，EsPerHFL为71.60%，基于DQN迁移方案为85.37%，而本文提出的R-HFL方案达到85.62%，而且相比于基于DQN的迁移方案，本文方案具有更快的收敛速度。此外，无聚类方案（No-Cluster）在每轮训练中都需要所有客户端与全局模型进行参数交换，导致通信开销显著高于基于分层聚类的方案。综合来看，本文所提出的R-HFL在最终精度、收敛稳定性以及通信效率方面均表现出显著优势。

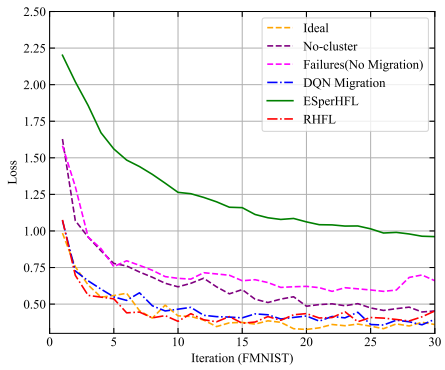

图 8　联邦学习模型在不同算法下的收敛情况(场景 2)

Figure 8　The convergence rate of the federated learning model under different algorithms (scenario 2)

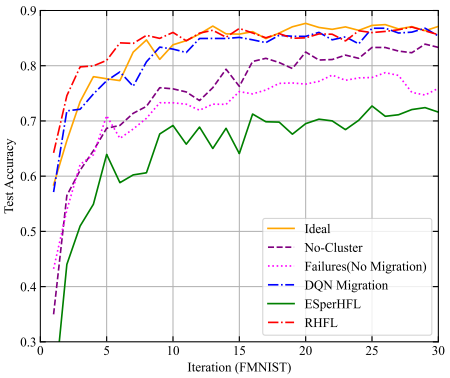

图 9　不同算法达到特定准确率需要的迭代轮次(场景 2)

Figure 9　The communication rounds required to reach a target accuracy under different algorithms (scenario 2)

为验证本文方法在其他 Non-IID 条件下的适应能力,图 10 和图 11 展示了在非独立同分布场景 3 下(使用 FMNIST 数据集)的损失和测试精度的变化情况。该场景中客户端数据依据 Dirichlet($\alpha=0.5$)分布进行划分,用以模拟样本数量不均衡的现实情况。实验结果表明,尽管存在明显的数据不均衡,本文提出的 R-HFL 方法仍能保持平稳的收敛趋势。在第 12 轮时,

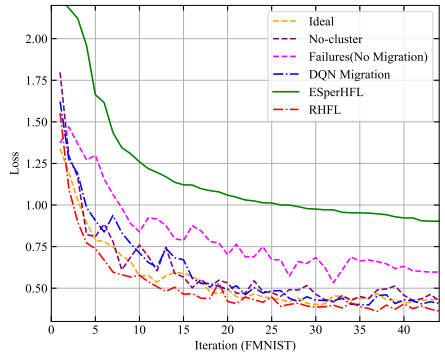

图 10　联邦学习模型在不同算法下的收敛情况(场景 3)

Figure 10　The convergence rate of the federated learning model under different algorithms (scenario 3)

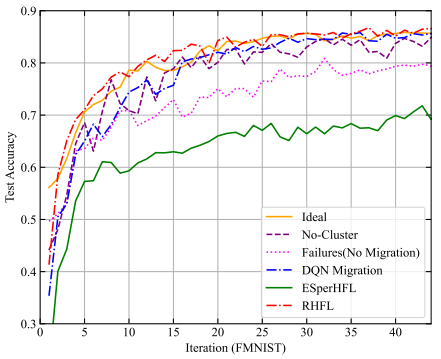

图 11　不同算法达到特定准确率需要的迭代轮次(场景 3)

Figure 11　The communication rounds required to reach a target accuracy under different algorithms (scenario 3)

模型测试精度已达到 80.56%,而其他对比方案均未超过 80%,进一步说明 R-HFL 在面对非 IID 与边缘服务器故障挑战时,依然具备良好的性能。

综合实验结果可知,本文提出的 R-HFL 方法在不同非独立同分布场景下均表现出良好的适应性与稳定性。面对边缘服务器失效等动态环境变化,该方法能够结合实时环境状态做出自适应迁移决策,从而在保障模型训练连续性的同时,有效提升全局模型的收敛速度与整体性能。

5　结论

针对分层联邦学习在边缘计算场景中面临的 Non-IID 导致梯度发散/收敛振荡以及边缘服务器失效引发组内聚合中断等问题,本文提出可靠性感知的分层联邦学习框架(R-HFL)。首先,基于客户端模型的语义特征与地理位置进行聚类分组,提高组内统计相似性,以缓解 Non-IID 造成的收敛不稳定与性能偏移。然后,优先选择高可靠性节点作为组内中间聚合器,降低失效率与聚合中断风险并提升聚合效率。进一步地,针对边缘服务器失效,将客户端迁移建模为马尔可夫决策过程(MDP),在集中式训练、分布式执行(CTDE)范式下采用多智能体近端策略优化(MAPPO)学习迁移策略;动态平衡迁移时延、迁移后通信开销与语义分布匹配度缓解迁移后的梯度发散,保障在新节点上的快速适配与训练连续性。实验结果表明,R-HFL 较主流基线在全局效用、模型精度、收敛速度等方面均有提升,并在边缘服务器失效情形下能够有效降低训练中断风险与迁移开销,显著增强系统整体鲁棒性。

未来工作可以把可靠性建模拓展至联邦大模型场景,构建可靠性感知训练与评估体系。与此同时,可以系统研究联邦大模型的资源分配问题,在通信、算力与能耗约束下实现效能与可靠性的联合优化。

参考文献

[1] 张晶, 关建峰, 刘科显, 等. 基于动态势博弈的边缘算力网络任务调度算法[J]. 电子学报, 2025, 53(1): 221-237.
Zhang Jing, Guan Jianfeng, Liu Kexian, et al. Task scheduling algorithm based on dynamic potential game for edge compute first networking[J]. Acta Electronica Sinica, 2025, 53(1): 221-237. (in Chinese)

[2] Guo T, Guo S, Wang J X, et al. PromptFL: Let federated participants cooperatively learn prompts instead of models-federated learning in age of foundation model[J]. IEEE Transactions on Mobile Computing, 2024, 23(5): 5179-5194.

[3] Quan H Y, Zhang Q M, Zhao J H. Federated learning assisted intelligent IoV mobile edge computing[J]. IEEE Transactions on Green Communications and Networking, 2025, 9(1): 228-241.

[4] Huang J W, Liu F Z, Zhang J B. Multi-dimensional QoS evaluation and optimization of mobile edge computing for IoT: A survey[J]. Chinese Journal of Electronics, 2024, 33(4): 859-874.

[5] 蒋伟进, 杜熙晨, 蒋意容, 等. 基于自适应联邦学习的环境监测群智感知算法[J]. 电子学报, 2025, 53(3): 821-835.
Jiang Weijin, Du Xichen, Jiang Yirong, et al. Adaptive federated learning based crowd sensing algorithm for environmental monitoring[J]. Acta Electronica Sinica, 2025, 53(3): 821-835. (in Chinese)

[6] Tu J K, Yang L, Cao J N. Distributed machine learning in edge computing: Challenges, solutions and future directions[J]. ACM Computing Surveys, 2025, 57(5): 1-37.

[7] Tang J, Li X H, Li H, et al. Joint class-balanced client selection and bandwidth allocation for cost-efficient federated learning in mobile edge computing networks[J]. IEEE Transactions on Mobile Computing, 2025, 24(7): 5681-5698.

[8] Letaief K B, Shi Y M, Lu J M, et al. Edge artificial intelligence for 6G: Vision, enabling technologies, and applications[J]. IEEE Journal on Selected Areas in Communications, 2022, 40(1): 5-36.

[9] 刘松, 罗杨宇, 许佳培, 等. 基于轻量自蒸馏的低成本联邦学习[J]. 电子学报, 2025, 53(1): 259-269.
Liu Song, Luo Yangyu, Xu Jiapei, et al. Low-cost federated learning based on lightweight self-distillation[J]. Acta Electronica Sinica, 2025, 53(1): 259-269. (in Chinese)

[10] Zhou X K, Ye X Z, Wang K I, et al. Hierarchical federated learning with social context clustering-based participant selection for Internet of medical things applications [J]. IEEE Transactions on Computational Social Systems, 2023, 10(4): 1742-1751.

[11] 康海燕, 冀珊珊. 面向无线边缘网络的分层Stackelberg博弈群体激励方法[J]. 电子学报, 2024, 52(7): 2382-2392.
Kang Haiyan, Ji Shanshan. Hierarchical Stackelberg game swarm learning incentive method forWireless edge network[J]. Acta Electronica Sinica, 2024, 52(7): 2382-2392. (in Chinese)

[12] Ma C M, Li X Q, Huang B G, et al. Personalized client-edge-cloud hierarchical federated learning in mobile edge computing[J]. Journal of Cloud Computing, 2024, 13(1): 161.

[13] Zhu G X, Wang Y, Huang K B. Broadband analog aggregation for low-latency federated edge learning[J]. IEEE Transactions on Wireless Communications, 2020, 19(1): 491-506.

[14] Xu Z C, Zhao D P, Liang W F, et al. HierFedML: Aggregator placement and UE assignment for hierarchical federated learning in mobile edge computing[J]. IEEE Transactions on Parallel and Distributed Systems, 2023, 34(1): 328-345.

[15] Singh N, Rupchandani J, Adhikari M. Personalized federated learning for heterogeneous edge device: Self-knowledge distillation approach[J]. IEEE Transactions on Consumer Electronics, 2024, 70(1): 4625-4632.

[16] Li T, Sahu A, Zaheer M, et al. Federated optimization in heterogeneous networks[J]. Proceedings of Machine Learning and Systems, 2020, 2(3): 429-450.

[17] Liang J Y, Ma B W, Feng Z H, et al. Reliability-aware task processing and offloading for data-intensive applications in edge computing[J]. IEEE Transactions on Network and Service Management, 2023, 20(4): 4668-4680.

[18] Lyu X T, Han Y F, Wang W, et al. Poisoning with Cerberus: Stealthy and colluded backdoor attack against federated learning[J]. Proceedings of the AAAI Conference on Artificial Intelligence, 2023, 37(7): 9020-9028.

[19] Abdelmoniem A M, Ho C Y, Papageorgiou P, et al. Empirical analysis of federated learning in heterogeneous environments[C]//Proceedings of the 2nd European Workshop on Machine Learning and Systems. New York: ACM, 2022: 3526969.

[20] Chen L M, Zhao D H, Tao L P, et al. A credible and fair federated learning framework based on blockchain[J]. IEEE Transactions on Artificial Intelligence, 2025, 6(2): 301-316.

[21] Ameen M, Khan R U, Wang P F, et al. Addressing unreliable local models in federated learning through unlearning[J]. Neural Networks, 2024, 180: 106688.

[22] Li J C, Li G B, Cheng H, et al. FedDiv: Collaborative noise filtering for federated learning with noisy labels[J]. Proceedings of the AAAI Conference on Artificial Intelligence, 2024, 38(4): 3118-3126.

[23] Zhang Z X, Cao X Y, Jia J Y, et al. FLDetector: Defending federated learning against model poisoning attacks via detecting malicious clients[C]//Proceedings of the 28th ACM SIGKDD Conference on Knowledge Discovery and Data Mining. New York: ACM, 2022: 2545-2555.

[24] Chen X H, Xu G Y, Xu X S, et al. Multicenter hierarchical

federated learning with fault-tolerance mechanisms for resilient edge computing networks[J]. IEEE Transactions on Neural Networks and Learning Systems, 2025, 36(1): 47-61.
[25] Li Z J, Wu H, Lu Y L, et al. Mitigating straggler effect in federated learning based on reconfigurable intelligent surface over Internet of Vehicles[J]. China Communications, 2024, 21(8): 62-78.
[26] Ye H, Liang L, Li G Y. Decentralized federated learning with unreliable communications[J]. IEEE Journal of Selected Topics in Signal Processing, 2022, 16(3): 487-500.
[27] Mao Y Z, Zhao Z H, Yang M L, et al. SAFARI: Sparsity-enabled federated learning with limited and unreliable communications[J]. IEEE Transactions on Mobile Computing, 2024, 23(5): 4819-4831.
[28] 王鑫, 周泽宝, 余芸, 等. 一种面向电能量数据的联邦学习可靠性激励机制[J]. 计算机科学, 2022, 49(3): 31-38.
Wang Xin, Zhou Zebao, Yu Yun, et al. Reliable incentive mechanism for federated learning of electric metering data[J]. Computer Science, 2022, 49(3): 31-38. (in Chinese)
[29] Cai H Y, Gao L J, Wang Jiahao, et al. Reliable incentive mechanism in hierarchical federated learning based on two-way reputation and contract theory[J]. Future Generation Computer Systems, 2024, 159: 533-544.
[30] Qin Z X, Yang L, Wang Q L, et al. Reliable and interpretable personalized federated learning[C]//2023 IEEE/CVF Conference on Computer Vision and Pattern Recognition. Piscataway: IEEE, 2023: 20422-20431.
[31] Zhou Z, Zhuang Y R, Li H J, et al. MR-FFL: A stratified community-based mutual reliability framework for fairness-aware federated learning in heterogeneous UAV networks[J]. IEEE Internet of Things Journal, 2024, 11(12): 20995-21009.
[32] Sharma M, Kaur P. Reliable federated learning in a cloud-fog-IoT environment[J]. The Journal of Supercomputing, 2023, 79(14): 15435-15458.
[33] Han X X, Zhang G Y, Yang L B, et al. Client dependability evaluation in federated learning framework[C]// Third International Conference on Communications, Information System, and Data Science. Washington: SPIE, 2025: 135190A.1-135190A.9.
[34] Alosaime S, Jhumka A. FLARE: Availability awareness for resource-efficient federated learning[C]//2024 IEEE 29th Pacific Rim International Symposium on Dependable Computing. Piscataway: IEEE, 2024: 66-75.
[35] Acar B, Sterling M. Ensuring federated learning reliability for infrastructure-enhanced autonomous driving[J]. Journal of Intelligent and Connected Vehicles, 2023, 6(3): 125-135.
[36] Mcmahan B, Moore E, Ramage D, et al. Communication-efficient learning of deep networks from decentralized data[C/OL]//Proceedings of Artificial Intelligence and Statistics. PMLR, 2017: 1273-1282. https://proceedings.mlr.press/v54/mcmahan17a.

作者简介

刘晓燕　女,1996年11月出生于山东省德州市。现为中国石油大学(北京)人工智能学院先进科学与工程计算专业博士研究生。主要研究方向为边缘智能、联邦学习。
E-mail: liuxy@student.cup.edu.cn

余　振　男,2004年2月生于河南省信阳市。现为中国石油大学(北京)人工智能学院人工智能专业本科生。主要研究方向为联邦学习、边缘智能。
E-mail: 2022012251@student.cup.edu.cn

梁晶语　女,1998年2月出生于安徽省宿州市。现为中石油(北京)数智研究院有限公司中级工程师。主要研究方向为边缘计算、工业软件。
E-mail: liangjingyu@petrochina.com.cn

林伯韬　男,1983年11月出生于福建省武平县。现为中国石油大学(北京)教授、博士生导师、人工智能学院院长。主要研究方向为智能石油工程、工业数字孪生和油气领域大模型。
E-mail: linbotao@cup.edu.cn

黄霁崴　男,1987年2月出生于北京市。2014年毕业于清华大学计算机科学与技术系,现为中国石油大学(北京)教授、博士生导师、人工智能学院副院长、石油数据挖掘北京市重点实验室主任。入选北京市科技新星、北京市优秀人才等。主要研究方向为物联网、边缘计算、服务计算。中国电子学会会员编号:E190158513M。
E-mail: huangjw@cup.edu.cn