面向数据交易的质量感知联邦学习贡献评价方法

田有亮[1,2,3]，支睿[1,2]，王帅[1,2]，金昆龙[1,2]
（1.贵州大学计算机科学与技术学院，贵州 贵阳 550025；2.贵州省密码学与区块链技术特色重点实验室，贵州 贵阳 550025；
3.贵州大学大数据与信息工程学院，贵州 贵阳 550025）

摘要：针对现有联邦学习贡献评价方法仍面临准确性不足、计算开销较高或鲁棒性受限，难以有效支撑数据交易中贡献结算与收益分配的问题，提出了一种面向数据交易的联邦学习贡献评价方法。首先，设计具备数据质量感知能力的客户端权重优化方法，通过优化客户端聚合权重得到反映客户端质量差异的基础信号。然后，结合权重变化量、当轮边际收益与历史表现，引入主观逻辑将多源信号转化为包含正向证据、负向证据与不确定性的主观意见，实现贡献值动态映射。在文本、音频和图像数据集上的实验表明，所提方法在贡献评价准确性、计算效率和抗攻击鲁棒性方面均表现良好，并具备动态性与一定的可解释性。

关键词：联邦学习；贡献评价；质量感知权重优化；主观逻辑
中图分类号：TP309
文献标志码：A
doi：10.11959/j.issn.1000–436x.TXXB260254

Quality-aware contribution evaluation method for federated learning in data trading

Tian Youliang[1,2,3], Zhi Rui[1,2], Wang Shuai[1,2], Jin Kunlong[1,2]
1. College of Computer Science and Technology, Guizhou University, Guiyang 550025, China
2. Guizhou Provincial Key Laboratory of Cryptography and Blockchain Technology, Guiyang 550025, China
3. College of Big Data and Information Engineering, Guizhou University, Guiyang 550025, China

Abstract: To address the problem that existing federated learning contribution evaluation methods suffered from insufficient accuracy, high computational overhead, or limited robustness, and thus could not effectively support contribution settlement and revenue allocation in data trading, a federated learning contribution evaluation method for data trading was proposed. First, a quality-aware client weight optimization method was designed to obtain foundational signals reflecting client quality differences by optimizing client aggregation weights. Then, weight variations, per-round marginal gains, and historical performance were incorporated, and multi-source signals were transformed into subjective opinions containing positive evidence, negative evidence, and uncertainty through subjective logic, thereby enabling dynamic contribution mapping. Experiments conducted on text, audio, and image datasets demonstrate that the proposed method achieves good performance in contribution evaluation accuracy, computational efficiency, and attack robustness, while also exhibiting dynamic adaptability and interpretability.

Key words: federated learning, contribution evaluation, quality-aware weight optimization, subjective logic

收稿日期：2026–05–07；修回日期：2026–07–31
通信作者：支睿，gs.rzhi24@gzu.edu.cn
基金项目：贵州省科技创新平台科研项目（黔科合平台CXPTXM[2025]024）；贵州省基础研究计划（自然科学）面上项目（黔科合基础MS[2026]175）；国家自然科学基金资助项目（No.62272123）；国家重点研发计划基金资助项目（No.2025YFB3109800）
Foundation Items：Scientific and Technological Innovation Platform Research Project of Guizhou Province (No.CXPTXM[2025]024), Guizhou Provincial Basic Research Program (Natural Science) General Project (No.MS[2026]175), The National Natural Science Foundation of China (No.62272123), The National Key Research and Development Program of China (No.2025YFB3109800)

0　引言

《数字中国发展报告（2025 年）》显示，我国数字经济核心产业增加值已占国内生产总值的 10.5% 以上，数据流通与交易需求持续增长[1]。自 2014 年贵阳大数据交易所成立以来，我国数据交易市场不断探索制度创新与平台化运行路径，数据要素市场化配置已形成一定实践基础[2]。然而，与传统商品交易不同，数据交易具有隐私敏感性，数据提供方难以直接开放原始数据内容[3]。随着《可信数据空间发展行动计划（2024—2028 年）》等政策持续强化数据安全与隐私保护要求，传统依赖原始数据直接流转的交易模式已难以满足合规流通需求[4-5]。

联邦学习（federated learning, FL）允许数据提供方在不共享原始数据的条件下共同训练全局模型，从而为隐私保护约束下的数据交易提供新的技术支撑[6-7]。然而，联邦学习并未解决数据交易中的价值衡量问题。由于不同客户端在数据质量、类别分布、任务匹配度以及训练行为等方面存在显著差异，各参与方对模型性能提升的有效贡献并不相同[8]。同时，在隐私保护约束下，平台难以直接判断参与方本地数据及模型更新的质量，进而导致数据价值难定价、收益难分配等现实障碍。若缺乏有效的贡献评价方法，联邦学习仍难以支撑隐私保护下数据交易的实际落地[9]。

联邦学习贡献评价方法的优劣主要体现在准确性、效率与鲁棒性 3 个核心维度[10]，在数据交易场景下，还应满足动态性与可解释性的要求。其中，准确性要求贡献结果能够反映客户端对全局模型的有效作用，使高质量和诚实参与的客户端在长期统计意义上获得更高贡献。效率决定方法能否实际部署。鲁棒性要求方法在噪声数据、恶意更新和复杂异质环境下仍能保持稳定可靠。动态性要求方法适应客户端随机参与、动态加入退出等训练机制。可解释性则要求贡献结果能够反映其形成依据。

现有主流联邦学习贡献评价方法可分为自报告法、基于个体性能的方法、基于夏普利值（Shapley value, SV）的方法和基于模型相似度的方法[11]。

（1）在准确性方面，自报告法依赖客户端主动披露私有信息，服务器难以验证其真实性，因此准确性易受影响。基于个体性能的方法主要依据本地模型表现评估贡献，未能考虑联邦协作产生的贡献，因此准确性仍然受限。

（2）在效率方面，基于 SV 的方法虽然具有较强的公平性理论基础，但需要重复评估大量客户端联盟，且计算开销较高，难以满足高效性。

（3）在鲁棒性方面，基于模型相似度的方法计算效率较高，但通常假设当前全局更新方向能够代表有效优化方向，在噪声数据、恶意更新或强异质环境下容易产生贡献误判，鲁棒性受到限制。

各类方法优缺点总结如表 1 所示。由表 1 可知，现有方法在准确性、效率和鲁棒性等贡献评价核心维度上仍存在不同程度的不足[10]。同时，部分方法需要固定客户端参与并完成完整的联邦学习过程，难以适应联邦学习中客户端随机选择的动态训练机制。此外，多数方法缺乏对贡献形成过程的解释。总体而言，现有方法尚难满足数据交易场景对贡献评价机制的综合要求。

表 1　　各类方法优缺点总结

方法	准确性	效率	鲁棒性
自报告法	低	高	低
基于个体性能的方法	中	中	中
基于 SV 的方法	高	低	高
基于模型相似度的方法	中	高	低

为此，本文提出了一种面向数据交易的数据质量感知联邦学习贡献评价方法。首先，该方法利用数据需求方提供的验收集计算客户端本地模型的验收集损失，并且求取该损失关于客户端聚合权重的梯度。然后，通过数据质量感知权重优化算法提升高质量更新的聚合权重，抑制低质量更新或异常更新的聚合影响，从而获得能够反映客户端数据质量差异的优化后权重。最后，本文综合考虑权重变化、单轮边际作用与历史表现，引入主观逻辑将多源训练信号映射为客户端贡献值。

本文的具体贡献如下。

（1）提出了一种新颖的质量感知联邦学习贡献评价方法。该方法通过自适应权重优化提取客户端质量基础信号，并结合主观逻辑实现贡献值映射，从而在联邦训练过程中在线评估客户端有效贡献，在贡献评价准确性、效率和鲁棒性方面均取得良好效果。

（2）提出了一种基于主观逻辑的客户端贡献映

射方法。该方法综合考虑客户端优化权重信号、当轮边际收益及历史信息，将训练过程中的动态表现映射为客户端贡献，并在一定程度上赋予贡献评价结果可解释性。

（3）在文本、音频和图像数据以及对应模型上开展实验，从贡献评价准确性、效率、鲁棒性和可解释性等多个方面验证了本文方法的有效性。

1 相关工作

在联邦学习支撑的数据交易场景中，贡献评价是实现数据定价和收益分配的基础。然而，联邦学习数据不可见的特性使平台难以检查参与方数据质量，从而增加了贡献评价的难度。围绕这一问题，现有研究提出了多类贡献评价方法，主要包括参与者自报告法、基于个体性能的方法、基于 SV 的方法以及基于模型相似度的方法。

1.1 参与者自报告法

这类方法要求客户端在上传模型更新之外，需额外向服务器提供与自身数据质量、资源条件或参与成本相关的信息，服务器再依据这些信息对客户端进行质量判断。

Jiang 等[12]提出的恶意客户端检测联邦学习（malicious client detection federated learning, MCDFL）要求客户端在本地计算并回传数据质量分数，服务器再基于这些质量分数进行聚类以判断客户端的实际质量。Zeng 等[13]提出了 FMore 方法，该方法要求节点在参与前提交包含资源质量与期望支付的投标信息，服务器再依据预设评分函数对各客户端进行排序，从而进行优质参与者的筛选。

此类方法实现简单，但其有效性往往依赖客户端对额外信息的诚实反馈，且难以验证这些信息的真实性与一致性，因此在实际场景中容易受到主观申报偏差的影响，难以稳定支撑准确的贡献评价。

1.2 基于个体性能的方法

这类方法通过评估客户端本地模型或模型更新在精度、损失或收益等指标上的表现来度量其价值，并据此完成奖励分配或贡献预测。

Pandey 等[14]通过引入本地相对精度作为核心量化指标，将每个客户端的个体性能与其获得的奖励直接关联。Lyu 等[15]通过服务器计算每个参与者在公共验证集上的模型更新准确率来评价其个体性能，并据此赋予声誉、分配奖励。Zhao 等[16]通过强化学习训练一个评估器，用于学习优质客户端的梯度特征，进而在后续预测客户端上传的模型更新带来的贡献。

此类方法评价过程较为直观，但主要关注客户端个体模型的局部性能，难以刻画多客户端协同训练产生的联合收益。当某些客户端单独表现一般、但与其他客户端协作后能够提升全局模型质量时，该类方法对其协同价值的评估存在局限。

1.3 基于 SV 的方法

这类方法从合作博弈视角出发，通过评估客户端加入不同联盟前后的性能边际变化来定义贡献。

Fan 等[17]提出了 FedSV，通过矩阵补全技术补全所有可能子联盟的边际贡献，从而提升联邦 SV 的分配公平性。Liu 等[18]发现了标准 SV 在实际实施中会低估异构客户端的贡献并且为其赋予不公正的负值，并基于此提出了合作夏普利值（cooperative Shapley value, CSV），通过策略等价性理论优化了效率与实际实施公平性。Lei 等[19]提出了蒙特卡洛变体采样近似算法，通过前部位置采样与后部截断来减少子联盟效用计算，从而提升估计效率。文献[18]和文献[19]均采用单轮合作博弈，将整个训练过程分解为逐轮子过程，以适应客户端随机加入与退出的动态训练场景。

但是此类方法普遍面临效率和准确性的权衡问题，或者仅当满足某些强假设时才能达成。例如，文献[19]的近似精度对截断位置和采样规模较为敏感。而文献[18]假设客户端之间存在策略等价性，并且可以通过聚类将同簇客户端视为具有同一策略；但现实场景下策略等价性假设未必成立，此时方法将退化为标准 SV。

1.4 基于模型相似度的方法

这类方法通常通过客户端本地模型更新方向与全局模型更新方向之间的关系来定义贡献，从而避免对验证集的依赖。

Wu 等[20]提出了 CoAst，利用客户端当前局部模型与后续若干轮全局更新方向之间的符号相似性衡量贡献。Jiang 等[21]提出了 FedCE，利用客户端本地梯度与其他客户端聚合梯度之间的余弦差异估计贡献，认为梯度方向越不同，客户端提供的新增信息越多，贡献越大。Guo 等[22]提出了 LCEFL，通过将客户端局部模型更新投影到全局模型收敛方

向上，并结合夹角余弦与投影长度计算贡献值，再通过跨轮累加获得最终贡献，同时利用代表层选择降低投影计算开销。

此类方法通常具有较高效率，但其核心假设是全局更新方向能够代表有效优化方向。当存在噪声数据、异常更新或恶意攻击时，全局更新方向本身可能发生偏移，此时方向一致性未必等价于有效贡献，因此其准确性与鲁棒性仍存在一定局限。

尽管上述研究为联邦学习贡献评价提供了有益思路，但现有方法仍难以同时满足隐私保护与数据交易场景对准确性、效率、鲁棒性、动态性与可解释性的综合要求。

进一步，现有方法大多将贡献评价视为训练结束后的分析过程，较少从联邦聚合过程本身出发构建内生的质量感知信号，也较少将客户端单轮边际影响、历史表现与不确定性因素统一纳入贡献建模框架。基于此，本文受客户端权重优化和联邦学习双层优化思想的启发[23-29]，提出了一种面向数据交易的质量感知联邦学习贡献评价方法。

相较于参与者自报告法与基于个体性能的方法，本文基于客户端权重变化和单轮边际作用构造贡献评价依据，减少了对客户端主观申报和单独本地性能的依赖，从而提升贡献评价的准确性。相较于SV类方法，本文避免了大量客户端联盟枚举，提高了效率。相较于基于模型相似度的方法，本文利用需求方验收集构造任务导向的数据质量感知信号，降低了噪声数据和异构分布导致的贡献误判，从而增强了贡献评价的鲁棒性。此外，主观逻辑对多源信号的证据化映射也为贡献评价结果提供了一定的可解释性。据作者所知，现有研究尚未将质量感知权重优化与主观逻辑统一用于联邦学习贡献评价。

2　预备知识

2.1　联邦学习

FL是一种面向分布式数据场景的协同建模方法，其核心思想是在不暴露参与方原始数据的条件下，通过模型参数的交互实现联合训练，从而可以在一定程度上支撑隐私保护下的数据流通[30]。

在典型的横向FL场景中，系统通常由一个中心服务器和多个客户端组成。设客户端集合为$\mathcal{U}=\{u_1,u_2,\cdots,u_N\}$，其中$N$表示客户端总数。客户端$u_i$持有本地数据集$D_i$，其样本量为$n_i=|D_i|$，总样本量为$n=\sum_{i=1}^{N}n_i$。FL的目标是利用所有客户端的分布式数据，联合优化一个共享模型$\boldsymbol{w}$，从而最小化整体经验风险。

$$\min_{\boldsymbol{w}}F(\boldsymbol{w})=\sum_{i=1}^{N}\frac{n_i}{n}F_i(\boldsymbol{w}) \tag{1}$$

其中，$F_i(\boldsymbol{w})$表示模型$\boldsymbol{w}$在客户端u_i本地数据集上的损失函数。在此目标下，联邦平均（federated averaging, FedAvg）是最经典的聚合方法之一。设第t轮被选中的客户端集合为S_t，客户端$u_i\in S_t$经过本地训练后得到本地模型$\boldsymbol{w}_i^t$，则服务器可按样本量进行加权聚合。

$$\boldsymbol{w}^{t+1}=\sum_{i\in S_t}\alpha_i^t\boldsymbol{w}_i^t \tag{2}$$

其中，$\alpha_i^t=\dfrac{n_i}{\sum_{j\in S_t}n_j}$且有$\alpha_i^t\geqslant 0$，$\sum_{i\in S_t}\alpha_i^t=1$。

FedAvg由于形式简单、实现高效，已成为FL研究中的基础聚合方法。然而在实际场景中，不同客户端的数据分布、样本规模和训练行为往往并不一致，这会导致局部更新对全局模型的作用存在明显差异[31]。同时，联邦学习通常采用部分客户端参与机制，不同轮次的参与集合动态变化，进一步增加了客户端贡献评估的复杂性。

2.2　主观逻辑

主观逻辑（subjective logic, SL）是一种面向不确定推理的形式化证据表达框架，适用于在证据不充分或信息存在不确定性的条件下，对命题的支持、反对与不确定状态进行建模[32]。在二元命题场景中，命题x的主观意见通常可表示为：

$$\omega_x=(b_x,d_x,u_x,e_x) \tag{3}$$

其中，b_x表示对命题x的信念度，d_x表示对命题x的否定度，u_x表示由于证据不足而保留下来的不确定性，e_x表示命题x的基率，前三项满足归一化约束：

$$b_x+d_x+u_x=1,\quad b_x,d_x,u_x\in[0,1] \tag{4}$$

SL中的意见通常源于对正向与负向证据的统计。设支持命题x的正向证据量为r_x，反对命题x的负向证据量为s_x，同时引入非负先验常数c控制在证据不足时不确定性所占的比例，则对应的意见可写为：

$$b_x = \frac{r_x}{r_x + s_x + c}$$

$$d_x = \frac{s_x}{r_x + s_x + c}$$

$$u_x = \frac{c}{r_x + s_x + c} \tag{5}$$

除了意见三元组之外，SL 还引入基率 e_x，用于在不确定性部分内部进行先验分配。基率通常可理解为在缺乏额外证据时，对命题 x 的先验偏好。基于意见三元组和基率，可以进一步定义命题 x 的期望值为：

$$E_x = b_x + e_x u_x \tag{6}$$

式(6)说明，当不确定性较低时，期望值主要由显式证据驱动；当不确定性较高时，基率将在贡献结果中发挥更明显作用。因此，SL 是一种兼具表达与解释能力的证据建模工具[33]。它能够为不确定环境下的判断问题提供更加细致的描述方式，这也为多源训练信号的统一表示和可解释评价提供了形式化支撑[34]。

3 系统架构

为形式化描述隐私保护约束下数据交易中的参与主体、交互关系及运行流程，本文构建了一个由数据提供方、数据需求方和数据交易平台组成的联邦数据交易系统，并据此展开实体定义与系统框架说明。

3.1 实体定义

（1）数据提供方

数据提供方是参与联邦训练的客户端集合，不共享原始数据，仅在平台协调下完成模型训练并上传至本地更新。由于各数据提供方在数据质量、类别分布及训练行为等方面存在差异，其对全局模型的有效贡献并不相同，部分数据提供方可能存在上传低质量更新甚至恶意更新的行为。

（2）数据需求方

数据需求方是任务发布方，自身缺乏足够的训练数据但具有明确的任务需求。需求方向平台提交任务描述，并提供一个与目标任务一致的小规模验收集 D_{proxy}，该验收集不参与客户端本地训练，仅在平台侧用于贡献评价与模型质量校验。数据需求方有动机保证验收集的标签质量。

（3）数据交易平台

数据交易平台是联邦训练任务的服务器与交易协调者，负责接收需求方的任务与验收集、发布训练任务、组织客户端选择与全局聚合、执行贡献评价和收益结算，并在模型达标后交付给数据需求方。数据交易平台被视为诚实可信的中介，不拥有客户端训练数据，但可访问数据需求方提供的验收集。

需要指出的是，本文引入的验收集并非传统的公共测试集假设，而是数据交易场景中由数据需求方提供的任务验收依据。相较于 SV 等方法需要大规模测试集反复评估不同联盟模型，本文方法仅需较小规模验收集即可实现聚合优化与贡献评价，既符合数据交易场景的模型验收需求，也降低了评价过程对额外验证数据的依赖。

3.2 系统框架

本文面向隐私保护约束下的数据交易场景，构建了由数据提供方、数据需求方和数据交易平台组成的联邦数据交易系统。该系统在不暴露数据提供方原始数据的前提下，完成面向特定任务的联合模型训练，并基于训练过程中的贡献实现收益分配。系统框架如图 1 所示，主要包括任务提交、任务发布、本地训练与模型上传、贡献评价与优化聚合和模型交付与收益分配 5 个阶段。

（1）任务提交：数据需求方向数据交易平台提交任务描述与验收集。

（2）任务发布：数据交易平台初始化全局模型，并向市场中的数据提供方发布联邦训练任务，组织参与方接入训练过程。

（3）本地训练与模型上传：各数据提供方基于本地私有数据完成局部训练，并向数据交易平台上传本地模型更新。

（4）贡献评价与优化聚合：数据交易平台结合客户端上传的模型更新与数据需求方提供的验收集，采用本文方法对各参与方贡献进行动态评估，并同时进行模型优化聚合。上述本地训练、贡献评价与优化聚合过程持续迭代，直至全局模型达到数据需求方目标。

（5）模型交付与收益分配：当全局模型达到预设验收要求后，数据交易平台将最终模型交付给数据需求方；随后，数据需求方支付总报酬，并在泛化场景下使用模型。数据交易平台依据最终贡献评价结果完成收益分配。

综上所述，本文实现了从任务发布、隐私约束下联合训练、贡献评价到模型交付与收益分配的数据交易完整闭环。为便于后续形式化描述，系统中涉及的主要符号定义如表 2 所示。

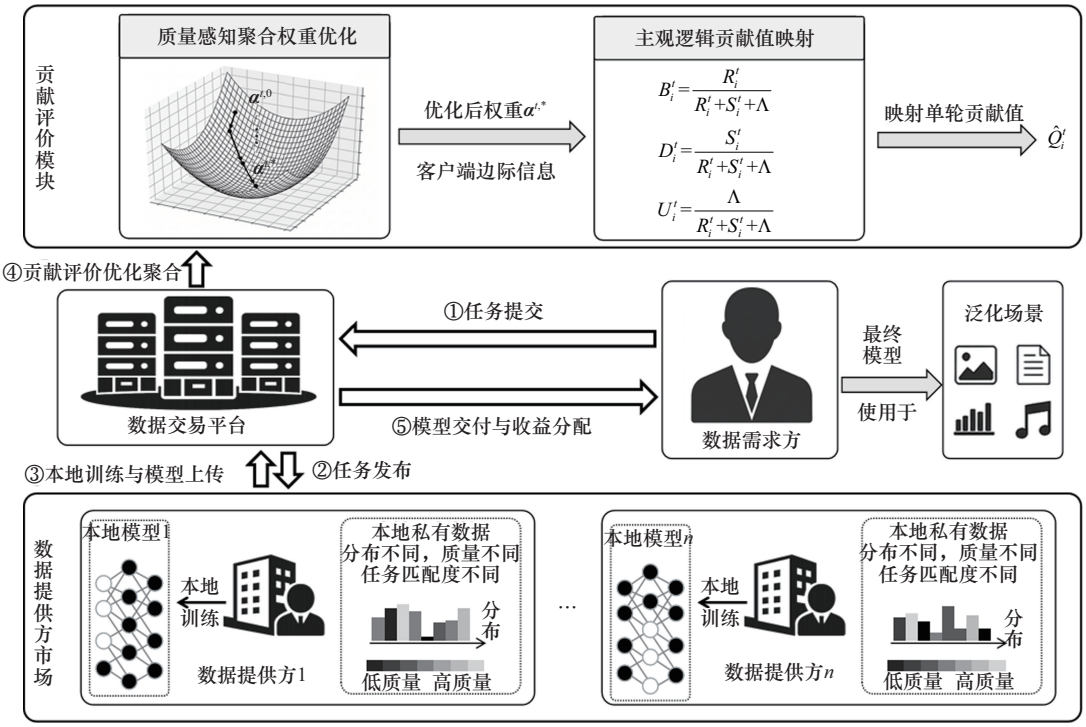


图1　系统框架

表2　符号说明

符号	定义
t	联邦训练轮次索引
s	服务器端第s次权重优化步
S_t	第t轮被选中的客户端集合
$\boldsymbol{w}^t$	第t轮全局模型参数
$\boldsymbol{w}_i^t$	客户端i在第t轮本地训练后上传的模型参数
$\boldsymbol{\alpha}^{t,s}$	第t轮第s次服务器优化时的聚合权重向量
$\alpha_i^{t,s}$	客户端i在第t轮第s次优化时的聚合权重
$\boldsymbol{\alpha}^{t,*}$	经权重优化后得到的当轮最终权重向量
$\alpha_i^{t,*}$	客户端i经权重优化后得到的当轮权重
$\bar{\boldsymbol{w}}^t(\boldsymbol{\alpha}^{t,s})$	基于当前聚合权重构建的临时聚合模型
D_{proxy}	数据需求方提供的验收集
$g_i^{t,s}$	验收集损失对客户端i聚合权重的梯度
$P_{1,i}^t,N_{1,i}^t$	客户端i的权重正证据与负证据
$P_{2,i}^t,N_{2,i}^t$	客户端i的边际作用正证据与负证据
$\hat{Q}_i^t$	客户端i在第t轮的最终贡献值

4　具体方案

4.1　具备质量感知的聚合权重优化方法

FedAvg按照客户端样本量n_i对本地模型进行加权平均，即默认样本规模越大，其更新对全局模型越重要。然而，在存在数据质量差异、局部偏移或训练噪声的联邦环境中，样本量并不能体现客户端更新对当前目标任务的实际价值。为此，本文不再仅依据样本量确定聚合权重，而是在数据需求方提供的验收集D_{proxy}上评估各客户端更新对目标任务损失的影响，并提取客户端质量的基础信号。

设第t轮被选中的客户端集合为S_t，其中$|S_t|=m$，客户端$i\in S_t$基于当前全局模型$\boldsymbol{w}^t$完成本地训练后，上传本地模型参数$\boldsymbol{w}_i^t$，本文将客户端聚合系数显式建模为可优化向量。

$$\boldsymbol{\alpha}^{t,s}=\{\alpha_i^{t,s}\}_{i\in S_t} \tag{7}$$

其中，s表示服务器侧第s次权重优化步，且满足：

$$\alpha_i^{t,s}\geqslant 0,\ \sum_{i\in S_t}\alpha_i^{t,s}=1 \tag{8}$$

在初始化阶段，将初始聚合权重设定为FedAvg的标准权重$\alpha_i^{t,0}=\dfrac{n_i}{\sum_{j\in S_t}n_j}$，保证方法与FedAvg在初始条件上一致，同时为后续质量感知优化提供稳定起点。

给定当前服务器优化步的权重向量$\boldsymbol{\alpha}^{t,s}$，服务器首先构造临时聚合模型。

$$\bar{\boldsymbol{w}}^t(\boldsymbol{\alpha}^{t,s}) = \sum_{i \in S_t} \alpha_i^{t,s} \boldsymbol{w}_i^t \tag{9}$$

随后，在数据需求方提供的代理验收集D_{proxy}上定义验收集损失函数。

$$\mathcal{L}_{\text{proxy}}^t(\boldsymbol{\alpha}^{t,s}) = \frac{1}{B_t} \sum_{b=1}^{B_t} \ell(\bar{\boldsymbol{w}}^t(\boldsymbol{\alpha}^{t,s}); \mathcal{B}_b^t) \tag{10}$$

其中，$\{\mathcal{B}_b^t\}_{b=1}^{B_t}$表示代理集划分得到的$B_t$个小批次，$\mathcal{B}_b^t$表示第$b$个小批次，$\ell(\cdot)$表示交叉熵损失函数。由于本地模型$\{\boldsymbol{w}_i^t\}_{i \in S_t}$在服务器优化阶段保持固定，因此服务器实际优化的对象仅为聚合权重$\boldsymbol{\alpha}^{t,s}$。

基于上述目标，服务器计算验收集损失关于聚合权重的梯度为：

$$g_i^{t,s} = \frac{\partial \mathcal{L}_{\text{proxy}}^t(\boldsymbol{\alpha}^{t,s})}{\partial \alpha_i^{t,s}}, \quad i \in S_t \tag{11}$$

该梯度反映了客户端i的聚合权重变化对当前代理任务损失的影响。当$g_i^{t,s} > 0$时，增大该客户端的权重会导致验收集损失升高，说明其更新与当前任务目标的一致性相对较弱；当$g_i^{t,s} < 0$时，增大其权重会降低验收集损失，表明其更新对当前任务更具正向作用。因此，$\{g_i^{t,s}\}$为质量感知的权重优化提供了核心信号。

为避免服务器更新步长依赖固定超参数而难以适应不同轮次的客户端质量差异，本文设计了最小梯度间隙驱动的自适应服务器步长。首先，令：

$$g_{\min^{t,s}} = \min_{i \in S_t} g_i^{t,s} \tag{12}$$

然后，定义各客户端相对于最小梯度的间隙为：

$$\Delta_i^{t,s} = g_i^{t,s} - g_{\min^{t,s}} \tag{13}$$

在此基础上，本文将未截断的服务器步长定义为：

$$\eta_{\text{raw}}^{t,s} = \sum_{i \in S_t} \Delta_i^{t,s} \tag{14}$$

通过上界$\eta_{\max}$对其进行约束，得到实际服务器步长为：

$$\eta^{t,s} = \min(\eta_{\text{raw}}^{t,s}, \eta_{\max}) \tag{15}$$

其中，最小梯度间隙机制仅用于构造当前轮服务器权重优化的整体步长，而不直接作为每个客户端的个体更新项。其作用在于：当各客户端代理梯度差异较大时，说明当前轮客户端质量可分性较强，服务器应采用更积极的权重重分配；当各客户端梯度接近时，说明质量差异不显著，服务器则应保持保守更新。

在获得服务器整体步长后，本文并不直接采用原始梯度进行更新，而是按梯度绝对值总量对其进行带阻尼归一化。记为：

$$G^{t,s} = \sum_{j \in S_t} |g_j^{t,s}| \tag{16}$$

则归一化梯度定义为：

$$\tilde{g}_i^{t,s} = \frac{g_i^{t,s}}{G^{t,s} + \lambda} \tag{17}$$

其中，$\lambda > 0$为阻尼系数。阻尼项的引入能够有效抑制整体梯度较小时可能出现的过强更新，从而提高服务器优化过程的数值稳定性。

在此基础上，本文采用指数乘法更新机制对聚合权重进行重分配。对于客户端$i \in S_t$，其未归一化权重更新形式为：

$$\hat{\alpha}_i^{t,s} = \alpha_i^{t,s} \exp(-\eta^{t,s} \tilde{g}_i^{t,s}) \tag{18}$$

随后，再进行归一化处理，得到下一步的聚合权重为：

$$\alpha_i^{t,s+1} = \frac{\hat{\alpha}_i^{t,s}}{\sum_{j \in S_t} \hat{\alpha}_j^{t,s}} \tag{19}$$

该更新方式具有两方面优势：一方面，它保证聚合权重始终非负且和为1；另一方面，它能够在连续空间中平滑地增强高质量客户端的影响并抑制低质量客户端的作用。由式(17)可知，$g_i^{t,s} < 0$则$\tilde{g}_i^{t,s} < 0$，从而有$\exp(-\eta^{t,s} \tilde{g}_i^{t,s}) > 1$，该客户端权重倾向于上升。反之，若$g_i^{t,s} > 0$，则其权重倾向于下降。需要指出的是，即使当前轮客户端梯度符号相同，客户端之间仍存在相对竞争关系，即梯度更小的客户端将获得更大的乘法增权效果，因此在相同初始权重条件下，其归一化后聚合权重更大。此外，随着服务器权重优化过程持续进行，客户端之间梯度差异通常会减小，从而使最小梯度间隙驱动的服务器步长下降；同时，梯度绝对值整体往往减弱，使带阻尼归一化后的有效梯度幅值进一步缩小。二者共同作用使聚合权重更新逐渐趋于平稳。

服务器按照固定步数重复上述优化。最终得到本轮优化后的聚合权重$\boldsymbol{\alpha}^{t,*}$，然后利用该权重完成当前轮全局模型聚合得到下一轮的全局模型。

$$\boldsymbol{w}^{t+1}=\sum_{i\in S_t}\boldsymbol{\alpha}_i^{t,*}\boldsymbol{w}_i^t \tag{20}$$

综上所述，本文提出的聚合权重优化方法通过代理集损失、最小梯度间隙驱动步长、阻尼归一化和指数乘法重加权 4 个关键环节，实现了对客户端聚合权重的动态优化。需要强调的是，本文引入该机制的目的不仅在于改进聚合效果，更在于通过重加权过程显式区分客户端之间的质量差异。客户端相对于初始权重的变化量能够直接反映服务器对其更新价值的动态评估，因此可作为后续主观逻辑贡献映射的核心基础信号。具备质量感知的聚合权重优化方法如算法 1 所示。

算法 1　具备质量感知的聚合权重优化方法

输入　第 t 轮选中客户端集合 S_t，各客户端本地模型 $\{w_i^t|i\in S_t\}$，初始权重 $\boldsymbol{\alpha}^{t,0}$，验收集 D_{proxy}，最大服务器步长 $\eta_{\max}$，服务器优化步数 K，阻尼系数 λ

输出　第 t 轮优化后聚合权重 $\boldsymbol{\alpha}^{t,*}$

1) for $s=0$ to $K-1$ do
2) 　根据当前聚合权重 $\boldsymbol{\alpha}^{t,s}$ 构造临时聚合模型 $\bar{w}^t(\boldsymbol{\alpha}^{t,s})$
3) 　在验收集 D_{proxy} 上计算验收损失 $\mathcal{L}^t_{\text{proxy}}(\boldsymbol{\alpha}^{t,s})$
4) 　根据式(11)计算验收损失关于聚合权重的梯度 $g_i^{t,s}$
5) 　根据式(12)~式(15)计算最小梯度间隙驱动的服务器步长 $\eta^{t,s}$
6) 　根据式(16)和式(17)对原始梯度进行带阻尼归一化，得到 $\tilde{g}_i^{t,s}$
7) 　根据式(18)计算客户端权重 $\hat{\alpha}_i^{t,s}=\alpha_i^{t,s}\exp(-\eta^{t,s}\tilde{g}_i^{t,s})$
8) 　根据式(19)对 $\hat{\alpha}_i^{t,s}$ 进行归一化，得到下一步的聚合权重 $\alpha_i^{t,s+1}$
9) end for
10) 记第 t 轮优化后聚合权重为 $\boldsymbol{\alpha}^{t,*}$
11) 利用 $\boldsymbol{\alpha}^{t,*}$ 对本轮模型进行加权聚合，得到全局模型 $\boldsymbol{w}^{(t+1)}$
12) return $\boldsymbol{\alpha}^{t,*}$

4.2　基于主观逻辑的客户端贡献映射方法

算法 1 通过具备质量感知的聚合权重优化方法，提取了反映客户端质量的优化后聚合权重。然而，优化后的聚合权重本身仍主要反映服务器在当前轮次中的重加权结果，并且权重优化结果受联邦学习当前轮次、客户端随机组合等因素的共同影响，缺乏历史稳定性与可解释性。为此，本文进一步引入主观逻辑映射模块，将训练阶段得到的权重变化信号与单轮边际作用信号统一映射为具有正负证据语义和历史先验约束的贡献值。

4.2.1　证据构造与意见建模

设客户端 i 在第 t 轮被选中，其基础聚合权重记为 $\alpha_i^{t,0}$，优化后聚合权重记为 $\alpha_i^{t,*}$。本文首先利用二者的差异提取权重侧证据。若优化后聚合权重相对初始权重增加，则视为正证据；若其下降，则视为负证据。因此，定义：

$$\begin{aligned}P^t_{1,i}&=\max(\alpha_i^{t,*}-\alpha_i^{t,0},0)\\N^t_{1,i}&=\max(\alpha_i^{t,0}-\alpha_i^{t,*},0)\end{aligned} \tag{21}$$

其中，$P^t_{1,i}$ 表示服务器在本轮优化中主动增强了客户端 i 的聚合影响，可视为权重提升正证据；$N^t_{1,i}$ 表示服务器主动削弱了其聚合影响，对应权重下降负证据。

除权重变化外，本文还引入单轮边际作用信号作为辅助证据项。具体而言，设第 t 轮在初始权重 $\boldsymbol{\alpha}^{t,0}$ 下的完整验收集损失为 $\mathcal{L}^t_{\text{full}}$，对于客户端 i，将其对应初始权重置零并对剩余客户端权重重新归一化，可得到去除客户端 i 后的验收集损失 $\mathcal{L}^t_{-i}$。据此定义客户端 i 在第 t 轮的单轮边际作用信号为：

$$\Delta^t_{i,\text{marg}}=\mathcal{L}^t_{-i}-\mathcal{L}^t_{\text{full}} \tag{22}$$

若 $\Delta^t_{i,\text{marg}}>0$，说明移除客户端 i 后验收集损失升高，即该客户端对当前轮任务具有正向边际作用；若 $\Delta^t_{i,\text{marg}}<0$，则说明移除该客户端后验收集损失反而降低，其更新可能偏离当前任务目标。基于此，定义边际作用侧正负证据为：

$$\begin{aligned}\overline{P}^t_{2,i}&=\max(\Delta^t_{i,\text{marg}},0)\\\overline{N}^t_{2,i}&=\max(-\Delta^t_{i,\text{marg}},0)\end{aligned} \tag{23}$$

考虑到在攻击或强异质场景下，边际作用差值的数值范围可能显著大于权重变化信号，若直接将 $\overline{P}^t_{2,i}$ 与 $\overline{N}^t_{2,i}$ 参与证据融合，容易使辅助证据主导最终评价，从而削弱服务器权重优化提取的基础质量信号。为此，本文引入同轮量级压缩机制，对边际作用侧证据进行线性缩放。定义 $M^t_{P_1}=\max_{j\in S_t}P^t_{1,j}$，$M^t_{\bar{P}_2}=\max_{j\in S_t}\bar{P}^t_{2,j}$，则正向边际证据调整为：

$$P^t_{2,i}=\begin{cases}\bar{P}^t_{2,i}, & M^t_{\bar{P}_2}\leqslant M^t_{P_1}\\ \dfrac{M^t_{P_1}}{M^t_{\bar{P}_2}}\bar{P}^t_{2,i}, & M^t_{\bar{P}_2}>M^t_{P_1}\end{cases} \tag{24}$$

同理，负向边际证据调整为：

$$N_{2,i}^{t}=\begin{cases}\bar{N}_{2,i}^{t}, & M_{\bar{N}_2}^{t}\leqslant M_{N_1}^{t}\\ \dfrac{M_{N_1}^{t}}{M_{\bar{N}_2}^{t}}\bar{N}_{2,i}^{t}, & M_{\bar{N}_2}^{t}>M_{N_1}^{t}\end{cases}\tag{25}$$

由此，客户端 i 在第 t 轮共获得 4 项基础证据：权重提升正证据 P_1、单轮边际作用正证据 P_2、权重下降负证据 N_1 和单轮边际作用负证据 N_2。为避免单一证据源在数值上过度主导，本文对正负证据分别取均值，构造单轮正负证据总量为：

$$R_i^t=\frac{P_{1,i}^t+P_{2,i}^t}{2},S_i^t=\frac{N_{1,i}^t+N_{2,i}^t}{2}\tag{26}$$

其中，R_i^t 表示客户端在当前轮的综合正向支持强度，S_i^t 表示其在当前轮的综合负向抑制强度。

在获得正负证据后，本文采用主观逻辑中的信念三元组对客户端状态进行建模。设主观逻辑先验质量常数为 Λ，该设置使正负证据均较弱时，保留一定比例的不确定性。客户端 i 在第 t 轮的信任度、否定度和不确定性分别定义为：

$$\begin{aligned}B_i^t&=\frac{R_i^t}{R_i^t+S_i^t+\Lambda}\\ D_i^t&=\frac{S_i^t}{R_i^t+S_i^t+\Lambda}\\ U_i^t&=\frac{\Lambda}{R_i^t+S_i^t+\Lambda}\end{aligned}\tag{27}$$

其中，B_i^t、D_i^t 和 U_i^t 分别表示该客户端在当前轮具有正向贡献的信任度、否定度和不确定性，且满足 $B_i^t+D_i^t+U_i^t=1$。

4.2.2 历史先验与贝叶斯收缩

仅依赖单轮证据容易使贡献判断受到随机波动影响，尤其在联邦训练早期，各客户端被选次数较少、服务器重加权尚不稳定，若直接根据当前轮证据输出贡献值，容易放大局部偶然性。为此，本文进一步引入基于历史优化权重的贝叶斯收缩先验。设客户端 i 在第 t 轮之前共被选中 k_i^{t-1} 次，其中 $\tau<t$ 表示历史训练轮次。其历史优化权重累计和为 $\sum_{\tau<t,i\in S_\tau}\alpha_i^{\tau,*}$，给定伪计数超参数 $M>0$，定义客户端 i 在第 t 轮的历史平滑权重为：

$$H_i^t=\frac{M\alpha_i^{t,0}+\sum\limits_{\tau<t,i\in S_\tau}\alpha_i^{\tau,*}}{M+k_i^{t-1}}\tag{28}$$

当 $k_i^{t-1}=0$ 时，式(28)自然退化为 $H_i^t=\alpha_i^{t,0}$。该设计意味着当客户端历史观测较少时，其先验更多依赖当前初始权重。随着被选次数增加，历史优化表现逐渐主导该先验，从而提高长期质量估计的稳定性。

在此基础上，本文进一步构造不确定性基率为：

$$A_i^t=\frac{\alpha_i^{t,0}+H_i^t}{2}\tag{29}$$

这表示在不确定性项的分配上，本文对当前初始权重与历史平滑权重进行等权融合，从而在短期局部信息与长期历史表现之间取得平衡。

4.2.3 贡献值映射

根据主观逻辑期望形式，客户端 i 在第 t 轮的原始期望贡献定义为：

$$Q_{i,\mathrm{raw}}^t=B_i^t+A_i^tU_i^t\tag{30}$$

其中，B_i^t 表示显式正证据对贡献值的直接支撑，$A_i^tU_i^t$ 表示在不确定条件下，由初始权重与历史先验共同分配给客户端的保守贡献。即当轮次证据充分时，贡献值主要由正负证据差异决定；当轮次证据不足时，贡献值会更多回退到由初始权重和历史表现共同反映的先验水平。因此，$Q_{i,\mathrm{raw}}^t$ 并不是单轮的瞬时评分，而是在证据和历史行为共同作用下的贡献估计。

尽管原始期望贡献已经引入了不确定性与历史先验，但在训练早期，客户端之间的证据仍可能不稳定。为抑制早期波动对贡献评估的影响，本文进一步引入基于轮次的收缩机制。设收缩阈值为 T_0，定义第 t 轮的收缩系数为 $\rho_t=\min\left(\frac{t}{T_0},1\right)$，则客户端 i 在第 t 轮的最终期望贡献定义为：

$$Q_i^t=\alpha_i^{t,0}+\rho_t(Q_{i,\mathrm{raw}}^t-\alpha_i^{t,0})\tag{31}$$

式(31)表明，在联邦训练早期，当 $t<T_0$ 时，最终贡献值将向初始权重收缩；随着训练轮次增加，ρ_t 逐步逼近 1，系统才允许贡献值更充分地反映由证据和历史先验共同决定的质量差异。该机制能够有效避免前期个别轮次的异常信号对最终贡献评估造成过大影响。

为得到第轮 t 内部可比较的贡献分布，本文对所有被选客户端的最终期望贡献进行归一化，定义客户端 i 在第 t 轮的归一化贡献为：

$$\hat{Q}_i^t=\frac{Q_i^t}{\sum\limits_{j\in S_t}Q_j^t}\tag{32}$$

$\hat{Q}_i^t$为本文最终映射得到的单轮客户端贡献值。基于主观逻辑的贡献映射方法如算法2所示。

算法2　基于主观逻辑的贡献映射方法

输入　单轮训练信息，先验质量常数Λ，历史伪计数M，收缩阈值T_0

输出　各轮客户端归一化贡献$\hat{Q}_i^t$

1) 初始化各客户端历史累计量与历史计数
2) for $t = 1$ to T do
3) for每个被选中客户端 $i \in S_t$ do
4) 根据式(21)计算权重信号证据$P_{1,i}^t$和$N_{1,i}^t$
5) 根据式(22)~式(25)计算边际作用证据$P_{2,i}^t$和$N_{2,i}^t$
6) 根据式(26)和式(27)对客户端状态进行建模
7) 根据式(28)计算历史平滑权重H_i^t
8) 根据式(29)计算不确定性基率A_i^t
9) 根据式(30)计算原始期望贡献$Q_{i,\mathrm{raw}}^t = B_i^t + A_i^t U_i^t$
10) 根据式(31)计算贡献$Q_i^t = \alpha_i^{t,0} + \rho_t(Q_{i,\mathrm{raw}}^t - \alpha_i^{t,0})$
11) end for
12) 根据式(32)计算当前轮归一化贡献
13) 更新各客户端历史统计量
14) end for
15) return $\hat{Q}_i^t$

5　实验分析

5.1　实验设置

为支持实验复现，本文实验在1块NVIDIA A30 Tensor Core GPU上进行，所有实验均使用Python和PyTorch实现。为验证所提方法的有效性，本文采用文本、音频和图像数据集以及对应模型展开实验，数据集和对应模型如表3所示。

表3　数据集与对应模型

数据集	模型
Yahoo Answers（YA）	Text-CNN
Speech Commands（SC）	Audio-CNN
CIFAR-10（CF-10）	ResNet-18

为了验证本文方法在异构情况下的稳定性，设置了3种数据划分方式，分别是独立同分布（independent identically distributed, IID）、Dirichlet $a = 1$分布和Dirichlet $a = 0.5$分布。

为验证所提方法的有效性，本文选择4类具有代表性的贡献评价方法作为对比基线。

（1）标准SV[35]：经典合作博弈贡献评价方法。

（2）LOO[36]：基于边际性能变化的直接贡献评价方法。

（3）LCEFL[22]：基于模型投影思想的高效贡献评价较新代表方法。

（4）DIG-FL[37]：基于梯度内积近似的高效贡献评价方法。

由于多数SV类改进方法主要围绕计算效率优化或特定场景适配展开，其评价结果通常仍以标准SV为参考，因此本文保留标准SV作为参考基线。

本文的主要公共实验参数如表4所示，其余参数根据数据模态进行适配，如CF-10与SC使用5轮本地训练，YA使用1轮本地训练；CF-10与SC的本地优化器为SGD，而YA使用Adam优化器。

表4　主要公共实验参数

参数	值
客户端总数	50
每轮参与客户端数	10
联邦训练轮数	100
学习率	0.01
本地批次大小	64
测试批次大小	512
数据需求方验收集大小	1 000
泛化测试集大小	10 000
单轮验收集批次	1
服务器优化步数	10
梯度阻尼项	5
贡献值轮次收缩阈值T_0	5
贝叶斯收缩的伪计数M	3
主观逻辑先验质量常数Λ	0.3
随机种子	42

5.2　准确性分析

为了验证所提方法的贡献评价准确性，本文选

取了两种场景：一种是基于常规联邦学习的随机选择场景；另一种是排除其余干扰的受控选择场景。

5.2.1　*动态随机选取下准确性分析*

图 2 展示了 CF-10 数据集在 IID 条件下，经过 100 轮随机客户端采样训练后，各客户端的平均贡献值。可以观察到，在客户端数据质量一致和数据分布一致的设定下，各客户端的平均贡献整体接近均匀分布。这说明，本文方法在随机采样条件下不会凭空引入额外偏置，能够在质量一致场景中保持较好的分配公平性。

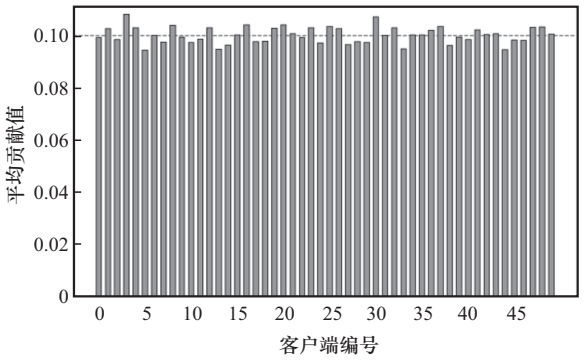


图 2　IID 状态下各客户端的平均贡献值

图 3 展示了不同数据模态与数据分布条件下，各类客户端的平均权重与平均贡献值。其中，本文设置 20 个干净客户端，噪声率为 20%、40% 和 60% 的客户端各 10 个；噪声在训练开始前通过随机标签翻转注入，并在整个训练过程中保持不变。从图 3 中可以看出，无论是在文本、语音还是图像数据集上，也无论是在 IID、Dirichlet a = 1 分布还是 Dirichlet a = 0.5 分布下，各类客户端的平均权重与平均贡献值均基本呈现出一致的单调排序关系，即干净客户端最高，其后依次为含 20%、40% 和 60% 噪声的客户端。这一结果表明，本文方法能够较稳定地区分不同质量客户端的更新价值，并且这种区分能力不依赖特定数据模态或特定分布设定。

图 4 展示了在 Dirichlet a = 0.5 分布下不同模态，各噪声类别客户端的窗口平均权重与平均贡献值。从整体趋势可以看出，在异构分布场景下，各类客户端的窗口平均贡献值整体上仍能保持与数据质量一致的排序关系。即干净客户端贡献最高，随后依次为 20%、40% 和 60% 噪声客户端。这说明，本文方法从局部训练窗口来看仍能够稳定反映不同

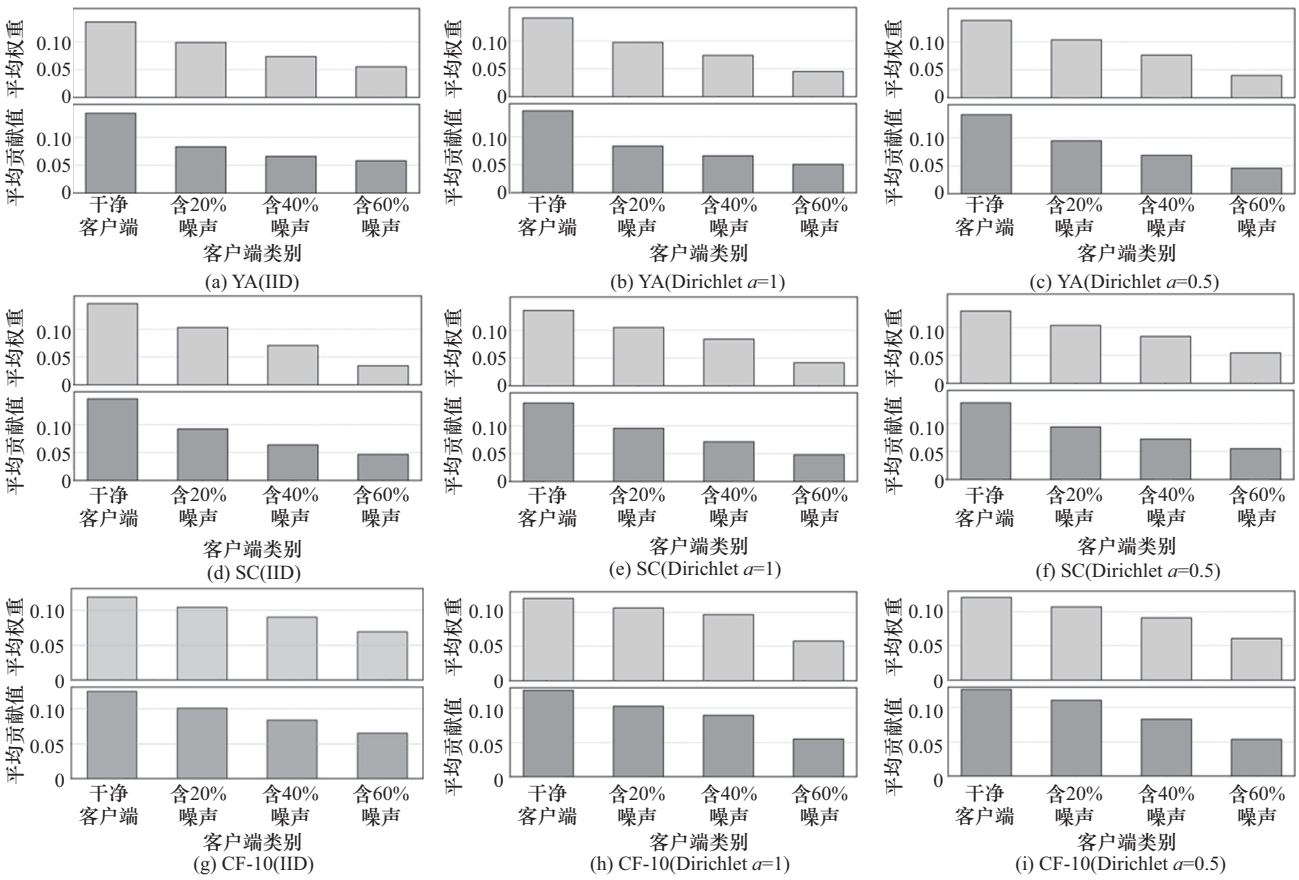


图 3　不同分布不同质量情况下各类型客户端的平均权重与平均贡献值

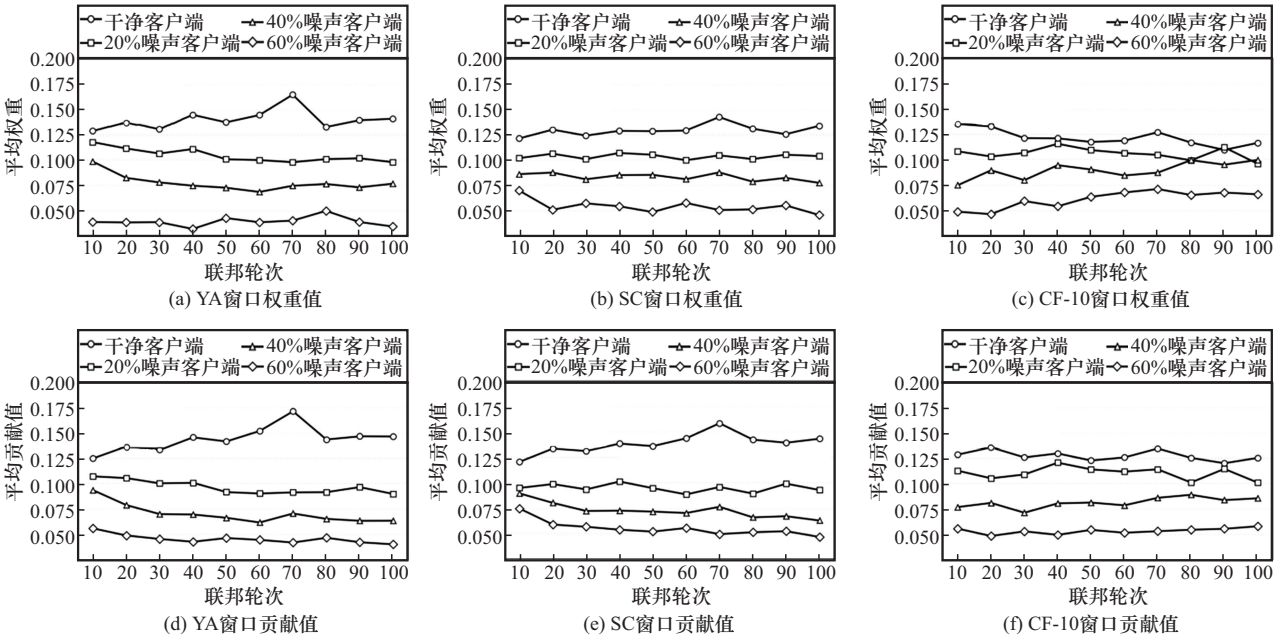


图4　异构情况下窗口平均权重与平均贡献值

质量客户端的相对贡献，而不会因单轮训练波动产生明显的排序偏移。值得注意的是，CF-10 窗口平均权重在训练后期出现了轻微交叉现象。这表明随着训练逐渐收敛，全局模型趋于稳定，服务器侧权重优化信号有所减弱，导致不同噪声类别之间的权重差异缩小。然而，在引入主观逻辑贡献映射后，窗口平均贡献值仍能够较好地保持与客户端质量一致的单调排序关系。该结果说明，主观逻辑映射不仅继承了服务器侧权重优化提供的质量信号，还能够结合历史先验与单轮边际作用，对后期较弱或波动的权重信息进行平滑和修正，从而提升贡献评价结果的稳定性。

本文将客户端数据质量定义为其有效数据比例，即将质量分数记为$r_i = 1 - \text{noise}_i$。该定义描述了客户端本地数据中可为全局模型提供有效训练信号的数据样本占比，因此能够较直观地反映不同噪声客户端之间的质量差异。为评估所提方法的贡献评价准确性，本文在多种模态数据集上计算客户端最终贡献值与质量分数之间的皮尔逊相关系数（Pearson correlation coefficient, PCC）、Spearman 秩相关系数以及单调性比例，结果如表 5 所示。

从表 5 可以看出，本文方法在 3 类数据集上均取得了较高的评价准确性。各设置下的 Spearman 秩相关系数和 PCC 均保持在较高水平，单调性比例也普遍接近 1，说明本文方法得到的贡献排序与客户端有效数据质量之间具有较强的一致性。但在 Dirichlet $a = 0.5$ 分布下，随着数据分布异质性增强，相关性指标有所下降，尤其在 CF-10 数据集上更为明显，但其 PCC、Spearman 和单调性比例仍分别达到 0.867 1、0.840 5 和 0.939 5，说明本文方法在客户端随机选取且复杂异构环境中依然具有较好的稳定性与准确性。

表 5　贡献评价准确性

数据集	分布	PCC	Spearman	单调性比例
YA	IID	0.929 6	0.955 1	1.000 0
	Dirichlet $a = 1$	0.926 7	0.955 1	1.000 0
	Dirichlet $a = 0.5$	0.909 3	0.940 0	0.991 8
SC	IID	0.969 1	0.955 1	1.000 0
	Dirichlet $a = 1$	0.972 4	0.953 1	0.998 3
	Dirichlet $a = 0.5$	0.948 0	0.945 1	0.991 8
CF-10	IID	0.934 0	0.927 5	0.981 2
	Dirichlet $a = 1$	0.891 6	0.901 3	0.965 7
	Dirichlet $a = 0.5$	0.867 1	0.840 5	0.939 5

消融实验结果如表 6 所示，移除质量感知权重优化后，PCC 从 0.934 降至 0.009、Spearman 从 0.927 5 降至 0.063 4、单调性比例从 0.981 2 降至 0.680 8，表明权重优化是本文方法的核心基础。移

除边际贡献证据后，3 项指标同步下降，说明边际证据贡献了区分信息。移除主观逻辑映射后，3 项指标同样下降，表明该映射对评价值的稳定性具有重要作用。移除轮次收缩因子后，3 项指标仅小幅下降，说明该机制主要抑制早期波动。消融实验结果表明，质量感知权重优化、主观逻辑映射与边际作用信号三者互为补充，共同支撑了方法在贡献评价准确性上的综合表现。

表 6　　消融实验

方法	PCC	Spearman	单调性比例
完整方法	0.934 0	0.927 5	0.981 2
消融权重优化	0.009 0	0.063 4	0.680 8
消融边际证据	0.686 2	0.726 4	0.876 7
消融主观逻辑	0.706 2	0.735 0	0.882 4
消融轮次收缩	0.809 8	0.844 1	0.932 2

5.2.2　受控场景下的质量一致性对比

为比较不同贡献评价方法对受控数据质量差异的贡献分配表现，本文将所提方法与 LCEFL、标准 SV、LOO 和 DIG-FL 进行对比[22,35-37]。基于客户端质量定义 $r_i = 1 - \text{noise}_i$，本文构造受控场景下的质量一致性参考目标为 $Q_i^* = \dfrac{r_i}{\sum_{j=1}^{N} r_j}$，其中 N 表示参与客户端数。该参考目标并非一般场景下贡献评价的贡献真值，而是在训练设置保持一致的受控条件下，由客户端有效数据质量归一化得到的数据质量参考分布。本文采用 L_1 距离衡量不同方法所得贡献分布与该参考目标之间的偏差，L_1 距离越小，表示贡献评价结果与数据质量参考分布越接近。为更清晰地验证各方法的贡献分配能力，本文设计了两类受控场景：其一为同质量场景，即所有客户端数据质量相同，用于考察方法在完全均质条件下是否会产生额外偏置；其二为细粒度差异场景，即客户端噪声水平按照 0、10%、20%、30%、40% 和 50% 逐级变化，用于检验方法对细微质量差异的分辨能力。

实验结果如表 7 所示，在同质量场景下，L_1 距离为 0.011 1，说明本文方法能够为同质量客户端分配近似一致的贡献值。在细粒度差异场景下 L_1 距离为 0.041 7，低于 LCEFL[22]、标准 SV[35]、DIG-FL[37] 和 LOO[36]，表明本文方法所得贡献分布与受控场景下的数据质量参考目标具有更高一致性。

需要指出的是，LCEFL 在含噪场景下出现逆向排序，可能与其基于客户端更新在全局模型更新方向上的投影有关。当噪声更新已经使全局模型方向偏离实际最优方向时，干净客户端无法在已偏方向上取得更大投影；相反，噪声客户端由于局部更新幅值更大，往往会获得更高的投影值。归一化后，这种幅值优势进一步放大，最终导致质量越低的客户端反而获得更高的贡献值。

表 7　　受控场景下贡献评价一致性对比

场景	方法	客户端贡献值						L_1 距离
		u_1	u_2	u_3	u_4	u_5	u_6	
同质量	参考目标	0.166 6	0.166 6	0.166 6	0.166 6	0.166 6	0.166 6	0.000 0
	本文方法	0.169 1	0.164 4	0.164 0	0.165 9	0.168 8	0.167 5	0.011 1
	LCEFL[22]	0.159 3	0.172 1	0.174 0	0.162 6	0.168 0	0.163 6	0.028 6
	SV[35]	0.165 5	0.168 4	0.172 5	0.165 5	0.163 5	0.164 4	0.015 2
	LOO[36]	0.161 6	0.156 0	0.168 2	0.177 0	0.172 2	0.164 7	0.035 1
	DIG-FL[37]	0.170 5	0.167 3	0.188 5	0.143 9	0.154 6	0.175 0	0.069 4
细粒度差异	参考目标	0.222 2	0.200 0	0.177 8	0.155 6	0.133 3	0.111 1	0.000 0
	本文方法	0.225 1	0.194 5	0.163 9	0.158 4	0.131 7	0.126 1	0.041 7
	LCEFL[22]	0.082 7	0.110 9	0.137 4	0.198 9	0.234 2	0.235 6	0.537 7
	SV[35]	0.370 3	0.282 8	0.193 6	0.107 3	0.045 8	0.000 0	0.493 6
	LOO[36]	0.471 9	0.265 2	0.187 9	0.074 8	0.000 0	0.000 0	0.650 2
	DIG-FL[37]	0.378 2	0.257 3	0.155 5	0.090 2	0.070 3	0.048 4	0.426 7

5.3　效率分析

由表 8 可知，不同贡献评价方法在单轮时间复杂度上存在显著差异。本文方法的单轮时间复杂度为 $O(C_{\text{train}} + nd + Knd + n^2d + C_{\text{sub}})$，其中 C_{train} 表示并行本地训练开销，n 表示当轮参与人数，nd 表示模型聚合开销，Knd 表示服务器权重优化开销，n^2d 表示单轮边际作用计算开销，C_{sub} 表示主观逻辑贡献映射开销。由于 C_{sub} 仅涉及线性运算，且联邦学习中本地训练通常占据主要时间开销，因此本文方法的复杂度主导项仍为 $O(C_{\text{train}})$。LCEFL[22]的单轮时间复杂度为 $O(C_{\text{train}} + nd_s + nd)$，$d_s$ 表示用于代表层投影计算的参数维度，复杂度主导项同样为 $O(C_{\text{train}})$；DIG-FL[37]的单轮时间复杂度为 $O(n \cdot (C_{\text{train}} + d) + C_{\text{val}})$，其中 C_{val} 表示在验证集上计算一次全模型梯度的开销。LOO[36]和SV[35]的单轮时间复杂度分别为 $O(n(C_{\text{train}} + nd))$ 和 $O(2^n(C_{\text{train}} + nd))$，其复杂度主导项分别为 $O(nC_{\text{train}})$ 和 $O(2^nC_{\text{train}})$。

表 8　　各贡献评价方法单轮时间复杂度

方法	单轮时间复杂度	复杂度主导项
本文方法	$O(C_{\text{train}} + nd + Knd + n^2d + C_{\text{sub}})$	$O(C_{\text{train}})$
LCEFL[22]	$O(C_{\text{train}} + nd_s + nd)$	$O(C_{\text{train}})$
SV[35]	$O(2^n(C_{\text{train}} + nd))$	$O(2^nC_{\text{train}})$
LOO[36]	$O(n(C_{\text{train}} + nd))$	$O(nC_{\text{train}})$
DIG-FL[37]	$O(n(C_{\text{train}} + d) + C_{\text{val}})$	$O(nC_{\text{train}})$

总体来看，本文方法虽然额外引入了服务器侧权重优化和单轮边际作用计算，但其复杂度主导项仍与 LCEFL 一样保持在 $O(C_{\text{train}})$ 量级，明显优于 LOO 的线性增长和 SV 的指数增长。

由图 5 可知，本文方法与 LCEFL 的整体耗时始终保持在较低水平，且随客户端数量变化仅出现小幅波动，说明二者都具有较好的效率表现。相比之下，DIG-FL[37]的耗时随客户端数量呈近似线性增长，其每轮需在验证集上计算全模型梯度，引入了额外串行负载，导致实际运行时间与 LOO 相近，而 SV 则以指数趋势增长。进一步来看，本文方法的实际运行时间略低于 LCEFL。其原因在于，LCEFL 需要先通过联邦训练确定代表层和全局模型更新方向，再回溯计算各客户端的模型投影贡献，因此在实际运行中会产生额外的记录、回退和投影计算开销。相比之下，本文方法仅需一次联邦训练，并在训练过程中完成服务器侧权重优化与边际作用分析，因此整体效率更优。本文方法在保证贡献评价能力的同时，体现了其高效性。

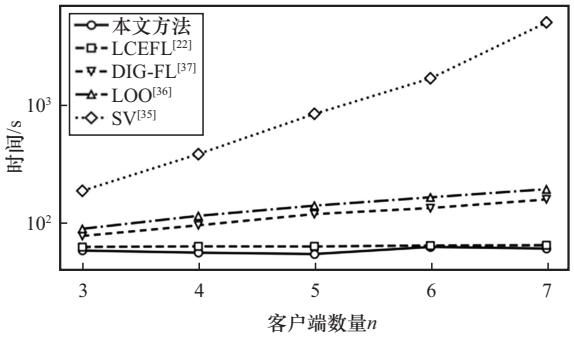


图 5　单轮平均所需时间与客户端数量的关系

5.4　贡献评价鲁棒性分析

为进一步验证本文方法在复杂环境下的贡献评价鲁棒性，本文在图像数据集上构造了同时包含客户端随机选取、恶意攻击、噪声干扰和非独立同分布数据划分的实验场景，以考察所提方法在多重扰动条件下的稳定性。设置 Dirichlet $a = 0.5$，在 50 个客户端中，设置 25 个干净客户端、10 个拜占庭恶意客户端，以及噪声率分别为 20%、40% 和 60% 的客户端各 5 个。对于良性客户端，其质量分数定义为 $r_i = 1 - \text{noise}_i$；对于恶意客户端，由于其上传更新旨在破坏全局模型，本文将其质量分数设为 0。

需明确，本文并非专门设计拜占庭防御机制，因此攻击实验的目标不是抵御目前最强的自适应攻击，而是验证在典型模型投毒扰动下，所提方法是否仍能保持贡献评价能力。为此，本文选取方向反转、幅值放大和随机扰动 3 类典型攻击，分别对应 Sign-Flipping (SF)、Scaling Attack (SA) 和 Gaussian Noise Injection (GN)[38-40]。

由表 9 可知，即使在恶意攻击、标签噪声与非独立同分布同时存在的情况下，本文方法得到的贡献分布仍与质量分数保持较强的一致性，说明所提贡献评价机制具有复杂场景的鲁棒性。

表 9　　攻击条件下的贡献评价结果

攻击	PCC	Spearman	单调性比例
SF[38]	0.873 3	0.754 6	0.914 2
SA[39]	0.928 4	0.801 6	0.937 1
GN[40]	0.926 1	0.784 5	0.925 7

结合图6可以看出，攻击条件下各类客户端的平均权重与贡献值仍保持合理排序。这说明本文方法能够在复杂扰动下识别有害的恶意更新。不过，与无攻击场景相比，图6中不同噪声类别之间的区分度有所下降。造成这种现象的原因在于攻击条件下的贡献信号不仅由客户端自身数据质量决定，还受到恶意更新干扰、随机参与组合以及数据非独立同分布的共同影响。首先，恶意客户端会显著扰动全局模型更新方向，使服务器在代理集上观测到的优化信号更偏向于区分明显有害与非明显有害的客户端，而对良性噪声客户端之间的细粒度差异变得不再敏感。其次，在随机选取机制下，当某一轮存在多个恶意客户端时，良性但含噪的客户端可能因为相对恶意更新危害更小而表现出接近的边际作用，从而压缩了良性类别之间的差异。

图7表明，本文方法在3种恶意攻击下均能明显优于受攻击的FedAvg，说明服务器侧权重优化能够在训练阶段有效削弱恶意更新对全局模型的破坏，并在一定程度上保留高质量客户端的正向作用。实验结果说明，本文方法虽然并非专门的拜占庭防御机制，但在典型模型投毒攻击下，除了贡献评价鲁棒性之外，还具备一定的训练鲁棒性。

5.5　方法兼容性与适应性

由图8可知，在存在噪声与Dirichlet a = 0.5的复杂环境下，本文方法在3种模态数据集上采用不同聚合算法均能够带来精度提升。相较于FedAvg[6]、FedProx[31]和FedAvgM[41]，加入本文方法后全局模型均有更快的上升趋势和更高的最终精度。这表明，本文方法能够作为一种通用的优化机制，具有较好的聚合算法兼容性和场景适应性。

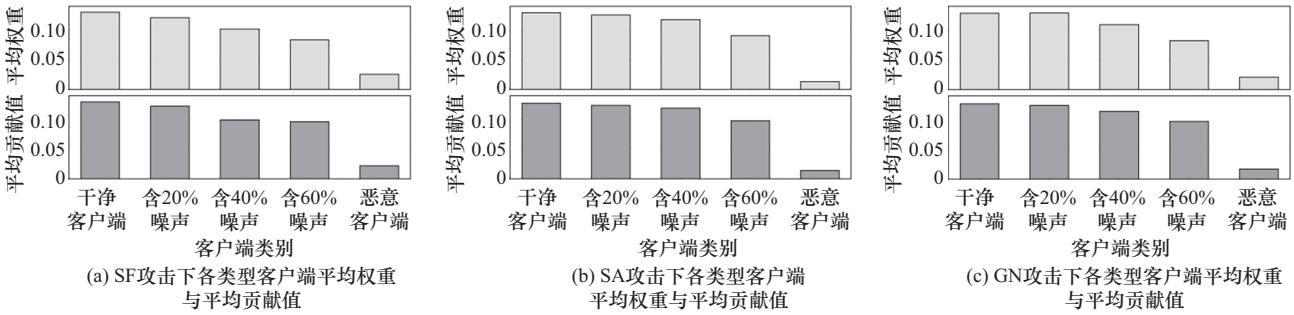
5.6　参数敏感性分析

表10表明，本文方法对验收集大小变化具有较强稳定性。验收集大小在100~2 000范围内，本文方法的指标始终保持在较高水平，说明方案在验收集大小变化的情况下总体稳定。

表10　　验收集大小对评价效果的影响

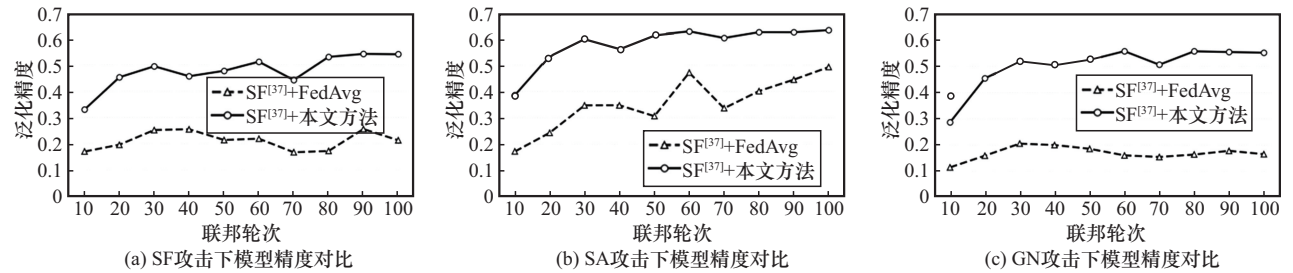
验收集大小	PCC	Spearman	单调性比例	泛化测试集精度
100	0.942 9	0.930 0	0.982 8	0.624 0
200	0.957 5	0.945 1	0.994 2	0.639 4
300	0.937 1	0.925 5	0.978 7	0.622 8
500	0.954 8	0.939 0	0.990 2	0.620 8
1 000	0.934 0	0.927 5	0.981 2	0.628 0
1 500	0.963 9	0.953 1	0.998 3	0.644 8
2 000	0.962 1	0.945 6	0.993 4	0.614 4

验收集偏移对评价效果的影响如表11所示。当验收集从全类别降至9类时，PCC由0.934 0降至



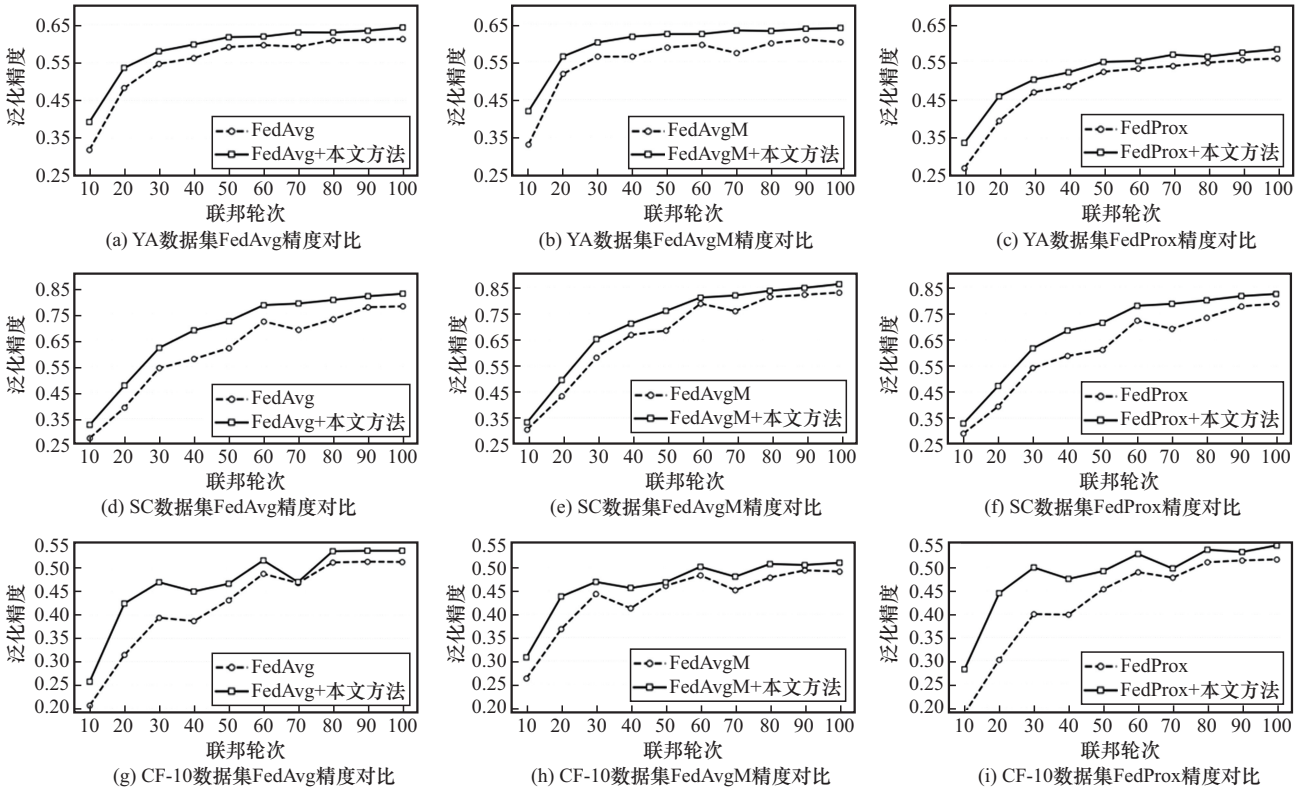
(a) SF攻击下各类型客户端平均权重与平均贡献值　(b) SA攻击下各类型客户端平均权重与平均贡献值　(c) GN攻击下各类型客户端平均权重与平均贡献值

图6　各类客户端的平均权重与平均贡献值



(a) SF攻击下模型精度对比　(b) SA攻击下模型精度对比　(c) GN攻击下模型精度对比

图7　恶意攻击下模型精度对比



(a) YA数据集FedAvg精度对比　(b) YA数据集FedAvgM精度对比　(c) YA数据集FedProx精度对比

(d) SC数据集FedAvg精度对比　(e) SC数据集FedAvgM精度对比　(f) SC数据集FedProx精度对比

(g) CF-10数据集FedAvg精度对比　(h) CF-10数据集FedAvgM精度对比　(i) CF-10数据集FedProx精度对比

图8　精度优化作用

0.828 0，方法仍保持较高鲁棒性；当降至7类和5类时，PCC进一步分别降至0.750 5和0.746 0，但下降幅度趋缓。当仅保留3类时，PCC、Spearman和单调性比例分别降至0.542 1、0.546 9和0.811 4，贡献评价显著退化。说明贡献评价的准确性依赖验收集对真实任务分布的代表性。

表11　验收集偏移对评价效果的影响

类别数	PCC	Spearman	单调性比例	泛化测试集精度
全类别	0.934 0	0.927 5	0.981 2	0.628 0
9	0.828 0	0.851 1	0.933 0	0.631 0
7	0.750 5	0.781 2	0.904 5	0.638 3
5	0.746 0	0.766 6	0.901 2	0.623 6
3	0.542 1	0.546 9	0.811 4	0.627 5

5.7　可解释性说明

表12展示了随机抽取的案例。以客户端3为例，此时位于第24轮，该轮次属于全局模型性能稳定提升的轮次。客户端3第4次被选中，该客户端的历史平滑权重为0.119 7，倾向于优质客户端。本轮优化后权重为0.115 3，表现为正证据，同时其单轮边际作用也表现为正证据。这说明该客户端在当前轮中既获得了服务器侧增权，也对当前轮全局任务产生了正向边际作用，因此其主观逻辑值在同轮参与客户端中位列靠前。其不确定度为0.918 7，当轮贡献值向历史先验收缩，最终映射得到当轮贡献值为0.129 2。

同理，其他客户端的贡献结果也可依据上述例子进行解释。

表12　主观逻辑映射的贡献评价可解释性说明

id	类型	联邦轮次	被选中轮次	历史平滑权重	本轮优化后权重	正证据		负证据		不确定度	当轮贡献值
						P_1	P_2	N_1	N_2	U	
3	clean	24	4	0.119 7	0.115 3	0.015 3	0.037 7	0	0	0.918 7	**0.129 2**
24	noise20	55	9	0.085 5	0.082 3	0	0.021 9	0.017 7	0	0.938 1	**0.096 3**
33	noise40	33	5	0.100 3	0.101 8	0.001 8	0	0	0.009 9	0.980 8	**0.074 6**
41	noise60	27	6	0.0846	0.0921	0	0	0.0079	0.0405	0.9254	**0.061 0**

需要注意的是，不确定度并非表示当轮观测不可信，而是本文主观逻辑框架内的分配比例机制。不确定度越高，当轮贡献越依赖该客户端的历史平均表现而非瞬时证据。这一设计的核心目的在于避免联邦学习中因随机采样而偶发的局部噪声点过度影响贡献评价。贡献值是跨轮累积的结果，单轮波动由不确定度缓冲，长期收敛方向由持续证据驱动。先验质量常数决定了单轮证据与历史先验之间的权重分配比。

6 结束语

本文面向隐私保护约束下的数据交易场景，提出了一种联邦学习贡献评价方法。该方法将质量感知的客户端权重优化与主观逻辑映射相结合，能够在不访问原始数据的条件下对客户端有效贡献进行评估，并为数据交易中的数据定价、收益分配与公平激励提供方法支撑。实验结果表明，本文方法在贡献评价准确性、效率和鲁棒性方面表现良好，同时具备动态性与一定的可解释性。

参考文献：

[1] 窦悦, 徐舒扬, 崔佳佳, 等. 数据流通利用视角下培育全国一体化数据市场路径研究[J]. 大数据, 2026, 12(2): 18-31.
Dou Y, Xu S Y, Cui J J, et al. Research on the path to cultivate a national integrated data market from the perspective of data circulation and utilization[J]. Big Data Research, 2026, 12(2): 18-31.

[2] 乔夫, 王庆德. 加快我国数据交易所生态系统建设的现实基础与发展路径研究[J]. 价格理论与实践, 2025(5): 88-94, 242.
Qiao F, Wang Q D. Research on the realistic foundation and implementation pathways for accelerating the construction of China’s data exchange ecosystem[J]. Price (Theory & Practice), 2025(5): 88-94, 242.

[3] Feng Z N, Yu S J, Zhu Y M. Towards personalized privacy preference aware data trading: a contract theory based approach[J]. Computer Networks, 2023, 224: 109637.

[4] 周烨. 培育五大可信数据空间 加速构建全国一体化数据市场: 解读《可信数据空间发展行动计划(2024—2028 年)》[J]. 中国科技产业, 2025(1): 8-9.
Zhou Y. Cultivating five major trusted data spaces to accelerate the construction of a national integrated data market: interpreting the ‘Action Plan for the Development of Trusted Data Spaces (2024—2028)’ [J]. Science & Technology Industry of China, 2025(1): 8-9.

[5] Bonawitz K, Kairouz P, McMahan B, et al. Federated learning and privacy: building privacy-preserving systems for machine learning and data science on decentralized data[J]. Queue, 2021, 19(5): 87-114.

[6] McMahan H 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. New York: PMLR, 2017: 1273-1282.

[7] Sun P, Liao G C, Chen X, et al. A socially optimal data marketplace with differentially private federated learning[J]. IEEE/ACM Transactions on Networking, 2024, 32(3): 2221-2236.

[8] Chai D, Wang L Y, Yang L, et al. A survey for federated learning evaluations: goals and measures[J]. IEEE Transactions on Knowledge and Data Engineering, 2024, 36(10): 5007-5024.

[9] Ma S C, Cao Y, Xiong L. Transparent contribution evaluation for secure federated learning on blockchain[C]//Proceedings of the 2021 IEEE 37th International Conference on Data Engineering Workshops (ICDEW). Piscataway: IEEE Press, 2021: 88-91.

[10] Chen Y W, Li K Y, Li G L, et al. Contributions estimation in federated learning: a comprehensive experimental evaluation[J]. Proceedings of the VLDB Endowment, 2024, 17(8): 2077-2090.

[11] Liu Z L, Chen Y Y, Yu H, et al. GTG-shapley: efficient and accurate participant contribution evaluation in federated learning[J]. ACM Transactions on Intelligent Systems and Technology, 2022, 13(4): 1-21.

[12] Jiang Y F, Zhang W W, Chen Y X. Data quality detection mechanism against label flipping attacks in federated learning[J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 1625-1637.

[13] Zeng R F, Zhang S X, Wang J Q, et al. FMore: an incentive scheme of multi-dimensional auction for federated learning in MEC[C]//Proceedings of the 2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS). Piscataway: IEEE Press, 2020: 278-288.

[14] Pandey S R, Tran N H, Bennis M, et al. A crowdsourcing framework for on-device federated learning[J]. IEEE Transactions on Wireless Communications, 2020, 19(5): 3241-3256.

[15] Lyu L J, Xu X Y, Wang Q, et al. Collaborative fairness in federated learning[C]//Federated Learning: Privacy and Incentive. Berlin: Springer International Publishing, 2020: 189-204.

[16] Zhao J, Zhu X H, Wang J Z, et al. Efficient client contribution evaluation for horizontal federated learning[C]//Proceedings of the ICASSP 2021-2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). Piscataway: IEEE Press, 2021: 3060-3064.

[17] Fan Z N, Fang H, Zhou Z R, et al. Improving fairness for data valuation in horizontal federated learning[C]//Proceedings of the 2022 IEEE 38th International Conference on Data Engineering (ICDE). Piscataway: IEEE Press, 2022: 2440-2453.

[18] Liu Y Q, Chang S, Liu Y, et al. FairFed: improving fairness and efficiency of contribution evaluation in federated learning via cooperative shapley value[C]//Proceedings of the IEEE INFOCOM 2024-IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2024: 621-630.

[19] Lei K J, Ren X B, Yang S S, et al. FedDSV: shapley value-based contribution estimation in federated learning with dynamic participation[J]. IEEE Transactions on Mobile Computing, 2025, 24(10): 11019-11033.

[20] Wu H, Zhang L K, Li S C, et al. CoAst: validation-free contribution assessment for federated learning based on cross-round valuation[C]//Proceedings of the 32nd ACM International Conference on Multimedia. New York: ACM Press, 2024: 1839-1847.

[21] Jiang M R, Roth H R, Li W Q, et al. Fair federated medical image segmentation via client contribution estimation[C]//Proceedings of the 2023 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). Piscataway: IEEE Press, 2023: 16302-16311.

[22] Guo J J, Li J X, Liu Z Q, et al. LCEFL: a lightweight contribution

evaluation approach for federated learning[J]. IEEE Transactions on Mobile Computing, 2025, 24(7): 6643-6657.

[23] Yang Y F, Xiao P Y, Ma S Q, et al. First-order federated bilevel learning[J]. Proceedings of the AAAI Conference on Artificial Intelligence, 2025, 39(21): 22029-22037.

[24] Xie Y Q, Zhang W Z, Pi R J, et al. Optimizing server-side aggregation for robust federated learning via subspace training[PP]. V2. (2022-11-10)[2026-05-07]. arXiv: arXiv.2211.05554.

[25] Huang W K, Shi Z K, Ye M, et al. Self-driven entropy aggregation for Byzantine-robust heterogeneous federated learning[C]//Proceedings of the 41st International Conference on Machine Learning. New York: ACM Press, 2024: 20096-20110.

[26] Li Z X, Lin T, Shang X Y, et al. Revisiting weighted aggregation in federated learning with neural networks[C]//Proceedings of the 40th International Conference on Machine Learning. New York: PMLR, 2023: 19767-19788.

[27] Parsa J, Daghestani A H, Teixeira A M H, et al. Byzantine-robust federated learning with learnable aggregation weights[PP]. V2. (2026-05-25)[2026-05-07]. arXiv: arXiv.2511.03529.

[28] Nourmohammadi R, Zhang K W, Talhi C. BlockFed: a novel federated learning framework based on hierarchical weighted aggregation[C]//Proceedings of the 19th ACM International Conference on Distributed and Event-based Systems. New York: ACM Press, 2025: 134-145.

[29] Shi C L, Zhao H, Zhang B J, et al. FedAWA: adaptive optimization of aggregation weights in federated learning using client vectors[C]//Proceedings of the 2025 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). Piscataway: IEEE Press, 2025: 30651-30660.

[30] Kairouz P, McMahan H B. Advances and open problems in federated learning[J]. Foundations and Trends® in Machine Learning, 2021, 14(1/2): 1-210.

[31] 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.

[32] Jøsang A. Subjective logic: a formalism for reasoning under uncertainty[M]. Springer Publishing Company, Incorporated, 2018.

[33] Rashid M M, Xiang Y, Uddin M P, et al. Trustworthy and fair federated learning via reputation-based consensus and adaptive incentives[J]. IEEE Transactions on Information Forensics and Security, 2025, 20: 2868-2882.

[34] Roy P, Sarker S, Razzaque M A, et al. Distributed task allocation in mobile device cloud exploiting federated learning and subjective logic[J]. Journal of Systems Architecture, 2021, 113: 101972.

[35] Song T S, Tong Y X, Wei S Y. Profit allocation for federated learning[C]//Proceedings of the 2019 IEEE International Conference on Big Data (Big Data). Piscataway: IEEE Press, 2019: 2577-2586.

[36] Wang G, Dang C X, Zhou Z Y. Measure contribution of participants in federated learning[C]//Proceedings of the 2019 IEEE International Conference on Big Data (Big Data). Piscataway: IEEE Press, 2019: 2597-2604.

[37] Wang J H, Zhang L, Li A R, et al. Efficient participant contribution evaluation for horizontal and vertical federated learning[C]//Proceedings of the 2022 IEEE 38th International Conference on Data Engineering (ICDE). Piscataway: IEEE Press, 2022: 911-923.

[38] Damaskinos G, El-Mhamdi E, Guerraoui R, et al. Asynchronous Byzantine machine learning (the case of SGD)[C]//Proceedings of the 35th International Conference on Machine Learning. New York: PMLR, 2018: 1145-1154.

[39] Bagdasaryan E, Veit A, Hua Y Q, et al. How to backdoor federated learning[C]//Proceedings of the Twenty Third International Conference on Artificial Intelligence and Statistics. New York: PMLR, 2020: 2938-2948.

[40] Lu S W, Li R H, Chen X, et al. Defense against local model poisoning attacks to Byzantine-robust federated learning[J]. Frontiers of Computer Science, 2022, 16(6): 166337.

[41] Hsu T H, Qi H, Brown M. Measuring the effects of non-identical data distribution for federated visual classification[PP]. V1. (2019-09-13)[2026-05-07]. arXiv: arXiv.1909.06335.

[作者简介]



田有亮（1982– ），男，博士，贵州大学教授、博士生导师，主要研究方向为博弈论、密码学与安全协议、大数据隐私保护等。



支睿（2000– ），男，贵州大学硕士生，主要研究方向为隐私保护、分布式学习、激励机制、合作博弈等。



王帅（2000– ），男，贵州大学博士生，主要研究方向为隐私保护机器学习、分布式学习和安全聚合。



金昆龙（2000– ），男，贵州大学硕士生，主要研究方向为隐私保护、联邦学习、后门攻击。