面向动态算力节点的联邦学习差分隐私重校准方法

陈宁江[1,2,3]，郑泽章[1]，章德华[1]
（1.广西大学计算机与电子信息学院，广西 南宁 530004；2.广西智能数字服务技术创新中心，广西 南宁 530004；
3.广西高校并行分布与智能计算重点实验室，广西 南宁 530004）

摘 要：为解决算力网络中节点动态参与导致的隐私预算超限、通信效率低下及训练时延高问题，提出一种联邦学习差分隐私重校准方法。该方法首先设计动态隐私预算校准机制，通过节点退出概率建模与实时预算回收算法，并结合训练阶段自适应调整噪声强度。其次，构建贡献度驱动的稀疏梯度编码协议，基于梯度重要性筛选关键参数，并采用分层噪声注入与8 bit量化压缩技术显著减少通信量。提出算力感知批量调整算法，依据设备计算能力动态分配本地批量大小以降低时延。实验表明，该方法在节点动态变化时节省约30.1%隐私预算，并在维持模型性能的同时降低19.6%通信量，有效提升了模型精度、通信效率与系统鲁棒性。

关键词：算力网络；联邦学习；差分隐私；稀疏梯度编码
中图分类号：TP18
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2025219

Federated learning with differential privacy recalibration for dynamic computing nodes

CHEN Ningjiang[1,2,3], ZHENG Zezhang[1], ZHANG Dehua[1]
1. School of Computer and Electronic Information, Guangxi University, Nanning 530004, China
2. Guangxi Center of Technology Innovation for Intelligent Digital Services, Nanning 530004, China
3. Key Laboratory of Parallel, Distributed and Intelligent Computing(Guangxi University), Education Department of Guangxi Zhuang Autonomous Region, Nanning 530004, China

Abstract: To address the issues of privacy budget overrun, low communication efficiency, and high training latency caused by the dynamic participation of computing nodes in computing networks, a federated learning differential privacy recalibration method was proposed. Firstly, a dynamic privacy budget calibration mechanism was designed by modeling node-exit probabilities and applying real-time budget recycling, along with adaptive noise-intensity adjustments during training. Subsequently, it constructs a contribution-driven sparse gradient encoding protocol that filters critical parameters based on gradient importance weights, employing layered noise injection and 8 bit quantization compression to significantly reduce communication overhead. Simultaneously, a computing-capacity-aware batch adjustment algorithm dynamically allocates local batch sizes according to device computational capabilities to minimize latency. Experiments demonstrate that this method achieves 30.1% privacy budget savings under dynamic node variations while reducing communication volume by 19.6% and maintaining comparable model performance, effectively enhancing model accuracy, communication efficiency, and system robustness.

Keywords: computing power network, federated learning, differential privacy, sparse gradient encoding

收稿日期：2025–09–23；修回日期：2025–11–10
通信作者：郑泽章，1334043617@qq.com
基金项目：国家自然科学基金资助项目（No.62162003）
Foundation Item：The National Natural Science Foundation of China (No.62162003)

0　引言

算力网络的兴起为分布式机器学习提供了强大的底层支撑，其动态节点架构允许多样化设备协同参与计算任务[1]。然而，这种节点动态性，如设备因资源耗尽、网络波动或恶意频繁加入/退出行为等情况，在带来灵活性的同时，也深刻改变了联邦学习（FL, federated learning ）的运行环境[2]。联邦学习能够显著提升训练效率，但基于静态节点假设构建的传统隐私保护方式可能引发严重的安全与隐私风险[3]。

在联邦学习领域，差分隐私（DP, differential privacy）作为主流的隐私保护技术，在动态算力网络环境下遭遇显著瓶颈[4]。如图 1 的静态与动态隐私预算分配策略对比，一方面，静态隐私预算分配策略无法有效回收退出节点的未使用预算，加剧了全局预算超限风险[5-6]。另一方面，异构节点对噪声的敏感性差异未被充分考虑，同时，全量参数传输方式在节点频繁变动时产生巨大的通信开销。这些问题共同制约了联邦学习在真实动态算力网络中的实用性、安全性与扩展性，亟须研究能够协同优化隐私保护、模型效用与通信效率的新方法[7-8]。

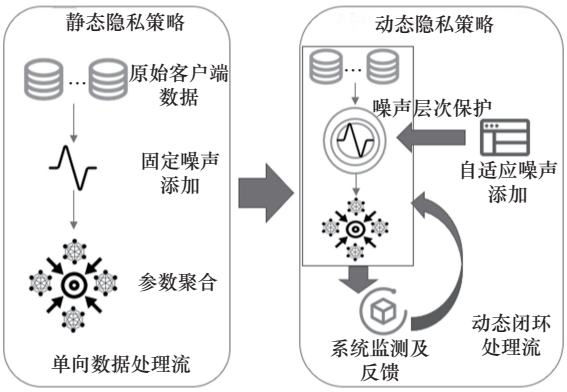

图 1　静态与动态隐私预算分配策略

为解决上述问题，本文提出一种联邦学习差分隐私重校准（DDPR-FL, federated learning differential privacy recalibration）方法，其核心思想是打破静态框架，建立动态适配机制。针对节点退出导致预算浪费的问题，系统可实时监控节点状态并回收其剩余隐私预算，通过缓冲池机制进行弹性再分配；同时，通信过程并非简单压缩，而是基于梯度重要性进行智能筛选与差异化处理；以上策略共同构成了动态环境下隐私–性能协同优化的基础。本文的主要工作如下。

1) 提出一种动态隐私预算校准策略。该机制突破静态隐私预算分配的局限，通过建模节点退出概率并设计实时预算回收算法，动态调整活跃节点的隐私资源分配。结合缓冲池策略和参与轮次限制，确保即使在节点频繁变动的场景下，全局隐私预算约束也能得到严格保障，并优化了预算资源的利用效率。

2) 提出利用贡献度驱动的索引化通信机制。首先量化客户端参数的贡献度权重，筛选出关键的部分梯度参数。随后，利用哈希编码与符号化传输等轻量化技术，对筛选后的稀疏梯度进行高效压缩和安全传输，显著减少了通信数据量，同时通过贡献度感知机制维持了模型更新的方向性。

3) 提出基于算力感知的本地批量调整算法。该算法首先在预热阶段评估客户端设备的计算能力，并据此在后续训练中动态调整每个客户端的本地批量大小，高算力设备被分配更大的批量以提升计算吞吐，而低算力设备则采用较小批量以避免过载，从而均衡系统整体训练效率，降低本地迭代时延。

1　相关工作

基于算力网络数据的特殊性，每个算力边缘服务器由海量边缘设备组成，且包含大量的隐私信息[9]。在算力网络的数据共享过程中，一旦终端设备或服务器节点的敏感数据发生泄露，不仅会直接威胁相关用户的隐私安全，还会削弱整个算力网络的可信度与安全信誉体系。随着信任基础的动摇，各计算节点对外共享本地数据的意愿将显著下降，从而进一步阻碍网络中资源协同、模型训练与服务优化的有效开展，最终影响算力网络的整体性能与稳定运行[10-12]。图 2 描述了联邦学习各阶段存在的攻击，在动态持续学习场景下，隐私保护技术需应对多轮交互中的累积隐私泄露风险[13]。其中同态加密存在计算效率瓶颈，全同态加密需对每个梯度参数进行多项式级运算，导致模型更新耗时过长[14]。区块链受制于共识效率和扩展性，难以支撑分钟级更新，且模型全生命周期上链存储成本超拍字节（PB, petabyte）级并与隐私需求冲突[15-16]。相比之下，差分隐私通过本地噪声注入与动态隐私预算分配，实现轻量化计算与可控精度损失，并提供可证的抗逆向工程安全性[17]。

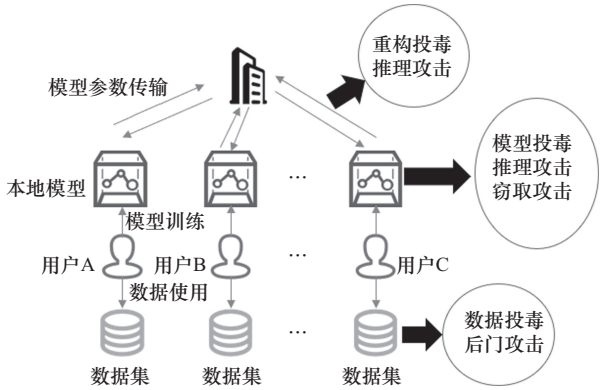

图2　联邦学习隐私安全问题

传统差分隐私方法直接应用于联邦学习时因噪声持续叠加易引发模型收敛速度下降与精度损失[18]。针对这一挑战，Batool等[19]提出的车联网算力网络双层联邦学习隐私框架通过本地差分隐私前置扰动与边缘服务器协同训练机制，在车辆边缘架构中构建数据共享与模型更新的双重安全屏障。Ling等[20]聚焦异构客户端场景，提出基于隐私预算权重动态分配与梯度扰动加权聚合的算力网络联邦学习方法，通过精准适配多客户端隐私需求实现资源优化与模型性能协同提升。在应急场景的极端通信条件下，Pauu等[21]开发的辅助联邦学习框架创新性地结合动态差分隐私机制与智能反射面辅助通信架构，通过动态噪声注入与学习率自适应调整策略，在非视距链路场景下突破隐私保护与通信效能的传统矛盾，为灾害响应场景构建了边缘智能协同范式。Yang等[22]进一步引入动态聚类中心自适应调整策略，在相同隐私预算约束下实现模型准确率提升与隐私风险的双重优化，但其对动态节点退出时的预算回收机制仍存在理论缺口。针对通信效率与隐私保护协同难题，Song等[23]提出的高效隐私保护数据聚合方案通过轻量化加密协议设计，在降低通信开销的同时保障数据隐私性，为边缘计算场景提供可行路径。在系统级优化层面，Chen等[24]提出的方法通过融合自适应学习率、梯度量化与差分隐私噪声注入的联合优化框架，实现通信轮次减少且模型隐私泄露风险下降，标志着联邦学习从单一技术突破向多目标协同优化的范式转变。上述差分隐私方法已经形成逐层递进的技术方案，但仍需在动态环境适应性、噪声耦合效应抑制等核心问题上寻求突破。

此外，现有研究在动态节点环境、算力异构与隐私预算管理三者联动下的联邦学习方案仍存在明显不足。具体而言，在隐私预算分配方向，Hong等[25]在单机差分隐私梯度下降中提出了“动态隐私预算调度”策略，通过逐轮调整噪声强度以提升数据利用效率。随后，Aldaghri等[26]将该思路扩展至联邦学习场景，提出“异构差分隐私”框架，使具有不同隐私需求（异构ε）的客户端能够自适应分配更合适的预算以提升整体效用。进一步地，Kiani等[27]提出时间适应型隐私预算机制，通过在早期保守使用预算、后期集中投入，实现更优的隐私–效用平衡。在此基础上，Guo等[28]又提出结合动态差分隐私的联邦学习方法，通过训练阶段自适应调节噪声强度与隐私预算以提升模型效用。然而，这些方法大多仍假设客户端持续在线，缺乏对节点动态退出与算力异构条件下隐私预算利用率与系统稳定性的系统性建模。因此，本文提出的联邦学习差分隐私重校准方法，在框架中首次将隐私预算重校准机制、节点算力异构感知与梯度通信压缩协同融合，构建了“隐私–算力–通信”三维联动的优化模型，为动态环境下联邦学习的高效与稳健运行提供了新的解决思路。

2　方法设计

2.1　问题模型

本文构建如图3所示的差分隐私重校准协同框架，通过动态隐私预算、索引化通信、算力感知批量调整等三维机制协同优化实现隐私、性能与效率的平衡。

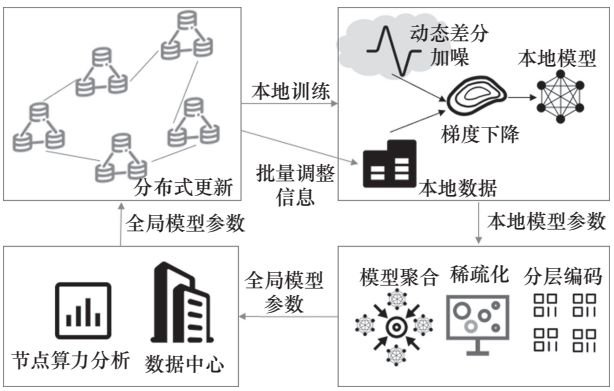

图3　差分隐私重校准协同框架

综合考虑了隐私强度、通信效率与本地时延的综合影响，本文定义模型性能指标为

$$\mathcal{P}=\underbrace{\frac{1}{\rho_{\text{total}}}}_{\text{隐私强度}}\cdot\underbrace{\frac{1}{T}\sum_{t=1}^{T}\frac{\|g^{\text{sparse}}(t)\|}{\|g(t)\|}}_{\text{通信效率}}\cdot\underbrace{\frac{B_{\text{avg}}}{B_{\text{base}}}}_{\text{时延优化}}\tag{1}$$

其中，ρ_{total}为总隐私损失，$\frac{\|g^{\text{sparse}}(t)\|}{\|g(t)\|}$为稀疏化梯度保留比例，$\frac{B_{\text{avg}}}{B_{\text{base}}}$为平均批量大小相对于基线的比值，$T$表示联邦学习的总通信轮次。系统通过最大化$\mathcal{P}$来实现隐私强度、通信效率与本地时延的协同优化以提升全局模型性能。

2.2　动态差分隐私重校准机制

首先构建面向动态联邦学习的隐私预算优化机制，从3个方面实现隐私与模型效用的协同提升。动态联邦学习的差分隐私保护流程如图4所示，依据训练阶段特性设计动态差分隐私策略：训练初期注入较大噪声增强保护，参数接近收敛时逐步降低噪声提升精度。其次，结合节点动态参与，引入预算回收与梯度敏感度控制机制，动态分配节点级隐私资源，避免因频繁退出或异常行为造成预算失衡。最后，通过更严格的隐私定义和累积控制降低长期迭代的预算消耗。

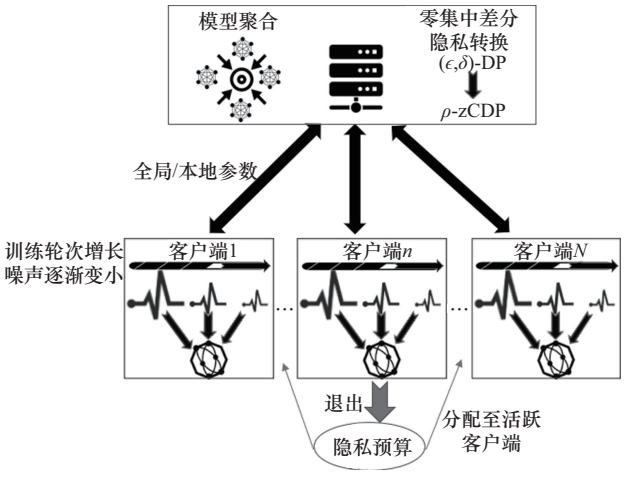

图4　动态联邦学习的差分隐私保护流程

下面详细描述动态差分隐私重校准机制流程。

1) 基于训练阶段的动态噪声调整

为适应联邦学习中模型训练不同阶段的噪声需求差异，构建隐私损失动态增长模型，首先根据训练轮次动态调整当前隐私损失值（零集中差分隐私形式）ρ_{current}。

$$\rho_{\text{current}}=(1+\beta t)\rho_{\min}\tag{2}$$

其中，$\rho_{\min}$表示初始最小隐私损失，β为增长率系数，t为当前训练轮次。当ρ_{current}增长至预设上限$\rho_{\max}$时，其值不再变化，以此适应训练初期（参数随机、梯度幅值大）需高噪声保护隐私，而后期（参数接近最优值）需低噪声保障精度的特性。

基于此模型，噪声方差σ^2与ρ_{current}呈负相关，计算式为

$$\sigma^2=\frac{2C^2}{|D_i|^2\rho_{\text{current}}}\tag{3}$$

其中，C为梯度裁剪阈值，$|D_i|$为节点本地数据量。训练初期，ρ_{current}较小，噪声方差较大，可有效掩盖敏感信息；随着训练轮次增加，ρ_{current}逐步增大，噪声方差减小，从而在保护隐私的同时减少对模型收敛方向的干扰。

2) 与节点退出机制的协同

在动态节点环境下，需结合预算回收机制动态分配回收的预算至活跃节点，并调整其ρ_{current}，实现“节点级”与“训练阶段级”预算优化的双重平衡。

首先进行梯度裁剪，本地训练后，对参数ω_i进行裁剪。

$$\omega_i^{(t+1)}=\frac{\omega_i^{(t+1)}}{\max\left(1,\frac{\left(\omega_i^{(t+1)}\right)}{C}\right)}\tag{4}$$

梯度敏感度$\Delta_2 f$用于衡量当客户端本地数据集中仅改变一个样本时，其平均梯度可能产生的最大变化幅度，确保$\Delta_2 f\leqslant\frac{2C}{|D_i|}$，约束噪声方差上限。再对全局敏感度计算，通过裁剪后的参数计算全局敏感度$\Delta\omega=\max\left(\frac{2Cp_i}{|D_i|}\right)$，用于噪声生成。裁剪操作限制了单节点对全局模型的潜在影响，降低敏感度$\Delta_2 f$，从而减少噪声量。

3) 零集中差分隐私与预算累积控制

为降低多次迭代中的隐私预算累积，引入零集中差分隐私（zCDP, zero-concentrated differential privacy）转换，通过式(5)将(ϵ,δ)-DP转换为ρ-zCDP。

$$\epsilon=\rho+2\sqrt{\rho\ln\left(\frac{1}{\delta}\right)}\tag{5}$$

结合动态ρ_{current}，实现更严格的隐私保障。经过T轮训练后，总隐私损失为

$$\rho_{\text{total}} = \frac{a\rho_{\min}\left[2+\beta(a-1)\right]}{2} + (T-a)\rho_{\max} \tag{6}$$

其中，a为达到$\rho_{\max}$所需的轮次，零集中差分隐私提供更紧的隐私损失上界，尤其在多次迭代中显著优于传统(ϵ,δ)-DP。动态分配策略通过控制ρ_{current}的增长速率β，进一步抑制总预算累积。同时，为实现ρ-zCDP与动态噪声调整机制的有机结合，本文在训练阶段引入阶段性噪声方差序列$\{\sigma_t^2\}_{t=1}^{T}$。在zCDP框架下，每轮噪声注入对应的隐私损失可表示为

$$\rho_t = \frac{C^2}{2\sigma_t^2} \tag{7}$$

其中，σ_t为第t轮的噪声标准差。动态噪声调整策略使σ_t随训练阶段单调变化，从而实现前期高噪声抑制敏感梯度，后期低噪声保持精度的平衡。依据ρ-zCDP的可加性，总隐私预算为各轮隐私损失的累积。

$$\rho_{\text{total}} = \sum_{t=1}^{T}\frac{C^2}{2\sigma_t^2} \tag{8}$$

当节点退出或预算回收时，系统将未消耗的部分重新分配至后续轮次，以保持ρ_{total}的稳定上界。该分配方式使动态噪声机制在zCDP框架下具备可解析的预算约束关系。

最后，对高频参与节点（计数器$c_j > \tau_{\max}$），可冻结其资格并回收预算，同时将其ρ_{current}重置为$\rho_{\min}$，避免恶意节点通过高频参与消耗过多预算。

2.3 基于稀疏梯度编码的高效通信机制

在兼容动态隐私预算校准的基础上，如图5所示，通过梯度稀疏化与分层编码技术减少通信数据量，同时结合动态噪声调整机制维持隐私保护强度，实现通信效率、隐私保护与模型性能的三维优化。

1) 贡献度权重分析

在梯度稀疏化与噪声分配前，需量化客户端参数的贡献度权重。首先对客户端C_i计算本地梯度$g_i = \nabla L\left(D_i, w\right)$。服务器下发上一轮聚合的全局梯度$g_{\text{global}}$，客户端计算其与本地梯度的余弦相似度。

$$w_i = \frac{g_i \cdot g_{\text{global}}}{\|g_i\| \cdot \|g_{\text{global}}\|} \tag{9}$$

对梯度中的每个参数j，根据其绝对值和全局重要性分配权重。

$$w_{i,j} = \frac{\left|g_{i,j}\right|}{\|g_i\|_1} \cdot w_i \tag{10}$$

其中，$w_{i,j}$表示客户端C_i中参数j的贡献度权重。

2) 梯度稀疏化与重要性筛选

基于贡献度权重$w_{i,j}$，系统筛选出梯度中重要性最高的前S%参数（例如$S=10$），生成稀疏化掩码$M_{i,j}$。

$$M_{i,j} = \begin{cases} 1, & w_{i,j} \geqslant w_i\text{的第}(100-S)\%\text{分位数} \\ 0, & \text{其他} \end{cases} \tag{11}$$

通过逐元素乘法操作$\odot$提取稀疏梯度$g_i^{\text{sparse}} = g_i \odot M$，仅保留关键参数。此步骤显著减少传输数据量（如仅传输10%梯度），从而降低通信负载，同时确保高贡献梯度不被遗漏。

3) 分层噪声注入与编码压缩

在动态噪声调整策略的基础上，对稀疏化后的梯度g_i^{sparse}，系统根据贡献度权重$w_{i,j}$动态分配噪声方差，噪声生成式为

$$\sigma_{i,j}^{\text{sparse}} = \sigma_{\text{base}} \cdot \left(1 + \alpha \cdot \tanh\left(\beta \cdot \left(1 - w_{i,j}\right)\right)\right)^{\omega} \tag{12}$$

其中，高贡献层分配低噪声（$\sigma_{i,j}^{\text{sparse}} \approx \sigma_{\text{base}}$），低贡献层噪声增强（$\sigma_{i,j}^{\text{sparse}} \approx 1.5\sigma_{\text{base}}$）。加噪后梯度$\tilde{g}_i^{\text{sparse}} = g_i^{\text{sparse}} + \xi$，进一步通过分层编码压缩，保留高贡献梯度的完整精度，避免模型收敛方向偏差。并对低贡献梯度进行8 bit量化。

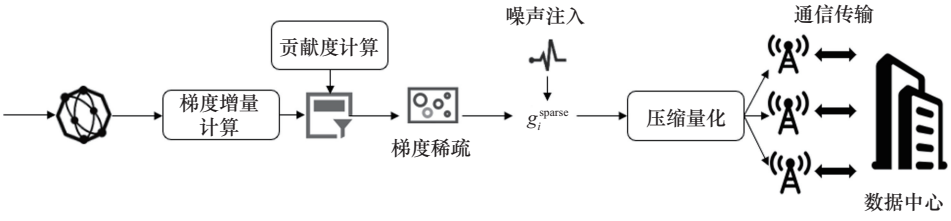

图5 基于稀疏梯度编码的动态高效通信机制

$$\left(\tilde{g}_i^{\text{quant}} = \text{Quantize}\left(\tilde{g}_i^{\text{sparse}}, \text{bit} = 8\right)\right) \tag{13}$$

此设计在减少通信数据量的同时，通过差异化噪声与编码策略平衡隐私保护与模型效用。

4) 动态预算协同与传输优化

稀疏化后的隐私预算按梯度稀疏比例动态调整。

$$\rho_{\text{sparse}} = \rho_{\text{total}} \cdot \frac{\|g_i^{\text{sparse}}\|_1}{\|g_i\|_1} \tag{14}$$

同时结合前文的动态预算重校准机制，系统将回收的预算按掩码比例分配至活跃节点。通信协议中，客户端仅上传编码后的稀疏梯度$\tilde{g}_i^{\text{quant}}$和掩码$M$，服务器端通过解码与填充操作恢复完整梯度。

$$\hat{g}_i = \tilde{g}_i^{\text{quant}} \odot M + \text{ZeroFill}(M) \tag{15}$$

其中，$\text{ZeroFill}(M)$将非稀疏位置补零。此方法在突发节点退出时，利用缓冲池临时支持通信，避免全局约束瞬时超限。稀疏化后的隐私预算ρ_{sparse}可无缝集成至节点退出时的预算回收机制。

2.4　算力感知批量调整算法

1) 初始化与预热阶段（前T_{warmup}轮）

中央服务器下发初始模型，所有客户端使用统一基础批量大小B_{base}进行本地训练。客户端在第t轮（$t \leqslant T_{\text{warmup}}$）完成训练后，上报本地训练时间$T_i^{(t)}$和本地数据量$|D_i|$。服务器记录各客户端的训练时间，并计算单位数据训练时间以消除数据量差异的影响。

$$\tilde{T}_i^{(t)} = \frac{T_i^{(t)}}{|D_i| \cdot B_{\text{base}}} \tag{16}$$

2) 计算能力推测

基于预热阶段采集的时延数据，构建客户端计算能力评分模型。

$$\hat{\mathcal{F}}_i^{\left(T_{\text{warmup}}\right)} = \frac{T_{\text{warmup}}}{\sum_{t=1}^{T_{\text{warmup}}} \tilde{T}_i^{(t)}} \tag{17}$$

其中，$\hat{\mathcal{F}}_i^{\left(T_{\text{warmup}}\right)}$表示客户端$i$的初始计算能力评分，$T_{\text{warmup}}$表示预热轮次。评分与设备实际算力正相关，实现异构设备的量化评估。

3) 动态批量调整

从第$T_{\text{warmup}}+1$轮开始，根据推测的计算能力动态调整批量大小。

$$B_i^{(t)} = \min\left(B_{\max}, \left| B_{\text{base}} \cdot \sqrt{\frac{\hat{\mathcal{F}}_i^{(t)}}{\hat{\mathcal{F}}_{\text{avg}}^{(t)}}} \right|\right) \tag{18}$$

其中，$\hat{\mathcal{F}}_{\text{avg}}^{(t)} = \frac{1}{|C|}\sum_{j \in C} \hat{\mathcal{F}}_j^{(t)}$表示当前活跃客户端$C$的平均计算能力评分，$B_{\max}$为批量大小上限，防止内存溢出。该分配策略在保证设备内存安全的前提下，使高算力设备处理更大批量，提升整体训练效率。

4) 持续更新计算能力推测

在后续训练中，每轮更新客户端的计算能力评分以适配资源波动。

$$\hat{\mathcal{F}}_i^{(t)} = \lambda \cdot \hat{\mathcal{F}}_i^{(t-1)} + (1-\lambda) \cdot \frac{1}{\tilde{T}_i^{(t)}} \tag{19}$$

其中，λ表示平滑系数，控制历史数据的权重，$\tilde{T}_i^{(t)}$表示当前轮次的单位数据训练时间。该机制可自适应设备资源的时变特性，有效应对计算节点突发性负载波动。而在实际部署中，为防止客户端上报训练时间失真，算法采用滑动平均与指数平滑机制计算算力评分，并结合上传时延特征进行交叉验证，保持系统鲁棒性与均衡性。

本文提出的联邦差分隐私重校准算法的伪代码如算法1所示。

算法1　联邦差分隐私重校准算法

输入　全局模型$w^{(0)}$，隐私参数$\rho_{\min}$、$\rho_{\max}$、β，裁剪阈值C，稀疏率S%，基线批量B_{base}，训练轮次T

输出　优化后模型$w^{(T)}$，总隐私损失ρ_{total}

1) 初始化：服务器下发$w^{(0)}$，各客户端初始化算力评分$\hat{\mathcal{F}}_i^{(0)}$，设置预算池$\rho_{\text{pool}}=0$，活跃节点集合$C=\{1,2,\cdots,N\}$，设随机种子 seed 用于噪声与有样的一致性复现；
2) for t = 1 to T do：
3)　根据式(2)计算当前隐私损失；
4)　if 当前节点<原有节点 then
5)　　回收其剩余预算至ρ_{pool}；
6)　　按活跃节点数重新分配ρ_{current}；
7)　end if
8)　根据式(3)生成噪声方差；
9)　　for 客户端$i \in C$ do：
10)　　计算本地梯度g_i，裁剪至$(g_i) \leqslant C$；
11)　　计算重要度分数（幅值x余弦相似），生成Top-k掩码；

12) 量化:$q\_i \leftarrow \text{Quantize}(g\_i \odot m\_i$，bit=8/16 按层自适应)；

13) 筛选前 $S\%$ 参数生成掩码 M_i，稀疏梯度；

14) 按贡献度权重注入分层噪声，生成 $\tilde{g}_i^{\text{quant}}$；

15) 上传 $\tilde{g}_i^{\text{quant}}$ 和 M_i；

16) end for

17) if $t \leqslant T_{\text{warmup}}$ then

18) 记录单位训练时间，计算初始算力评分；

19) else

20) 算力感知批量调整：持续更新算力评分，

21) 动态调整批量 $B_i^{(t)}$，更新算力评分，

end if

22) 聚合各客户端模型得到全局模型 $w^{(t)}$；

23) 全局隐私记账与安全检查：降低下一轮的目标隐私预算

24) if 预算池不足 then

25) 触发回退策略：

26) 降低稀疏率、提升裁剪阈值，

27) end if

28) end for

29) 累加每轮隐私预算得到 $\rho_{\text{total}} = \sum_{t=1}^{T} \rho_{\text{current}}^{(t)}$；

30) 输出优化后模型 $w^{(T)}$，总隐私损失 ρ_{total}；

以上算法的时间复杂度为 $O(N \cdot T \cdot d)$，其中 N 为参与客户端数量，d 为模型参数量，主要时间开销集中在梯度稀疏化筛选与分层噪声注入 2 个环节。空间复杂度方面，稀疏化梯度存储仅需保留前 $S\%$ 的关键参数，占用空间为 $O(S\% \cdot d)$，相较于全量梯度显著降低内存需求。此外，模块化设计使其能够无缝集成至主流联邦学习框架（如 PySyft、TensorFlow Federated），仅需调用标准化的梯度聚合接口即可实现功能扩展，显著提升实际部署的灵活性。

3 实验分析

本文实验目标是验证在算力网络动态场景下，隐私预算的利用率和模型准确率。分析退出设备的预算回收机制对全局隐私预算的影响，比较动态噪声策略与固定噪声策略的性能差异，以及不同压缩比下的通信开销和模型性能。

3.1 实验设计

1) 数据集设置

实验采用 2 类基准数据集验证方法性能。

CIFAR-100：包含 60 000 张 32×32 彩色训练图像和 10 000 张测试图像（100 类）。为模拟数据偏移，将其按非独立同分布形式划分，每个客户端随机获得 10~20 个类别，每类 50~200 张样本，以体现数据异构性。

Fashion-MNIST：共 70 000 张图像（10 类）。依据类别分布熵进行划分，高熵客户端包含多类均衡样本，低熵客户端主要集中于 1~2 个类别，用于验证动态隐私预算策略对分布差异的适应性。

为评估更复杂任务下的可扩展性，引入 Tiny-ImageNet 数据集（200 类，每类 500 张训练图像、50 张验证图像）。采用 Dirichlet(α=0.5)的 Non-IID 划分，使不同客户端在类别覆盖度和样本数量上均表现出显著异构性。

2) 模型与训练设置

视觉任务采用轻量化残差网络：在 CIFAR-100 与 Fashion-MNIST 上使用简化的残差网络-18（以 3×3 卷积替换 7×7，并保留 4 个残差块），以减少模型复杂度对隐私预算与收敛特性的干扰；在 Tiny-ImageNet 上采用轻量残差网络-34（适度加深网络并控制通道规模），通过全局平均池化接 200 维分类层，实现表达能力与通信成本的平衡。优化器为带动量的随机梯度下降（动量 0.9、权重衰减 5×10^{-4}）。训练设置方面，10 客户端场景采用 200 轮通信、批量大小 32、学习率 0.001、本地轮次 E=5，梯度裁剪阈值 1.0；在 100 客户端下通信轮次提升至 300 轮，初始批量设为 64，并由算力感知机制动态调整。学习率采用分段衰减策略：前 150 轮保持 0.01，于第 150 与 250 轮分别降至 0.1 与 0.01，以增强后期收敛稳定性。

3) 通信效率实验设置

通信效率评估基于 CIFAR-100，并保持与前述实验一致的模型与训练参数，仅在梯度传输与压缩策略上做区分。设置 0、10%、20%、40% 及动态调整等稀疏率，并结合 8 bit、16 bit 与自适应分层量化构成多种通信方案。通过统计每轮客户端上传与服务器下发的字节数获得单轮及全程通信开销，并计算相对基线的降低比例。同时记录客户端每轮

本地训练耗时，通过平均值与四分位数衡量不同方法在异构算力环境下的时延与稳定性。

4) 节点动态变化设置

为增强节点动态性建模的可复现性，本文在模拟节点状态变化时引入基于泊松过程的节点状态转换模型，用以刻画算力网络中节点的随机退出与重新加入行为。设节点在第t轮的加入与退出事件服从参数为λ_t的泊松分布，即单位时间内的事件数满足$N_t \sim \text{Poisson}(\lambda_t)$。定义节点的瞬时退出概率为

$$P_{\text{exit}}^{(i)} = 1 - \mathrm{e}^{-\frac{\lambda_t}{R_i}} \tag{20}$$

其中，R_i为节点的算力评分，评分越高则退出概率越低。预算回收比例α_i依据退出风险动态分配。

$$\alpha_i = \frac{P_{\text{exit}}^{(i)}}{\sum_{j \in \mathcal{A}} P_{\text{exit}}^{(j)}} \times B_{\text{pool}} \tag{21}$$

其中，$\mathcal{A}$为当前活跃节点集合，B_{pool}为缓冲池预算。该设置实现了对节点随机退出的动态响应，确保预算回收与再分配过程既符合算力异构特征，又维持全局隐私预算约束的稳定性。

5) 模型反演攻击实验设置

为评估本文方法对模型反演攻击的防护效果，将服务器建模为半诚实推断攻击者，其严格遵循训练协议，但会尝试利用模型参数或梯度信息恢复客户端的本地敏感样本。攻击阶段固定训练完成的全局模型θ，并用随机噪声初始化伪样本$\hat{x}$。攻击者通过优化如下反演损失，对伪样本进行迭代更新，以最大化模型对目标类别的响应。

$$x^* = \arg\min_{\hat{x}} \mathcal{L}_{\text{inv}}(\hat{x}) = \arg\min_{\hat{x}} \left(-\ln f_{y_t}(\hat{x};\theta) + \lambda \|\hat{x}\|_2^2 \right) \tag{22}$$

其中，$f_{y_t}(\cdot)$表示模型对类别y_t的输出概率，第一项提升伪样本对目标标签的置信度，第二项为正则项限制可行输入空间。攻击者采用梯度下降更新伪样本。

$$\hat{x} \leftarrow \hat{x} - \eta \nabla_{\hat{x}} \mathcal{L}_{\text{inv}}(\hat{x}) \tag{23}$$

最终得到的重构图像x^*与真实样本在像素空间与特征空间上的均方误差（MSE, mean squared error）作为评估指标，用于衡量反演得到的重构样本与真实样本之间的差异，其计算方式为

$$\text{MSE}(x, x^*) = \frac{1}{N} \sum_{i=1}^{N} (x_i - x_i^*)^2 \tag{24}$$

其中，N为样本的像素或特征总维度，x_i与x_i^*分别表示真实样本与重构样本在第i个维度的取值。MSE的数值反映了攻击者重构质量的好坏，若MSE较小，说明x^*与x高度接近，模型反演攻击成功率高，隐私泄露风险显著；若MSE较大，则说明重构样本与真实样本存在明显差异，隐私保护机制有效阻断了攻击者对敏感数据的恢复能力。通过比较不同隐私机制下的平均重构质量与攻击成功率，可以分析本文方法对模型反演攻击的抑制效果。

6) 对比基线

①联邦平均算法（FedAvg）[29]。②高效隐私保护联邦学习（EPP-FL）[18]：结合异构差分隐私的高效联邦学习隐私保护方法。③基于差分隐私的贝叶斯优化方法（DP-GSGLD）[20]：基于贝叶斯优化与差分隐私的防御隐私泄漏算法。④高效隐私保护数据聚合方法（EPPDA）[21]：高效隐私保护数据聚合方案，降低通信开销的同时保护数据隐私。⑤联邦优化算法（Fedopt）[22]：综合优化通信效率与隐私保护的联邦学习方法。⑥时间自适应隐私预算分配联邦学习（TAPS-FL）[27]：结合时间自适应隐私预算分配的联邦学习方法。⑦动态差分隐私联邦学习（DDP-FL）[28]：一种结合动态差分隐私的联邦学习方案，根据训练阶段自适应调整噪声强度。这些基线共同覆盖了联邦学习隐私保护的主要挑战（效率、隐私、异构数据），通过对比可全面评估新方法在各项指标上的表现。

3.2　噪声敏感度与模型精度对比

为验证动态隐私预算调整策略对联邦学习系统性能的优化效果，本文设计了3组对比实验。

1) 固定高噪声组$(\rho_{\text{static}} = 0.02)$：全程注入高噪声（噪声方差$\sigma^2 = \dfrac{2C^2}{|D_1|^2 \cdot 0.2}$），隐私保护强度高。

2) 固定低噪声组$(\rho_{\text{static}} = 0.1)$：全程注入较低噪声，隐私预算累积风险较高。

3) 动态调整组：噪声强度从初始隐私损失$\rho_{\min} = 0.01$线性增长至$\rho_{\max} = 0.2$（增长率系数$\beta = 0.03$），初期高噪声保护隐私，后期逐步降低，减少对模型优化的干扰。

如图6所示，将3组分别与无噪声组（Noise-free）进行对比，固定高噪声组（$\rho = 0.01$）曲线呈现剧烈振荡（波动幅度达±10.3%），最终准确率仅79%左右，表明高强度噪声严重干扰梯度方向。固

定低噪声组（$\rho = 0.2$）虽然曲线平滑度提升（波动幅度±5.1%），但准确率仅达81.5%左右，且由于隐私预算过度消耗，面临成员推断攻击成功率升高的安全隐患。若继续增大隐私损失参数（$\rho > 0.2$）以降低噪声强度，虽可提升准确率，但将导致累积隐私预算突破$\epsilon = 10$的安全阈值，无法满足实际部署需求。

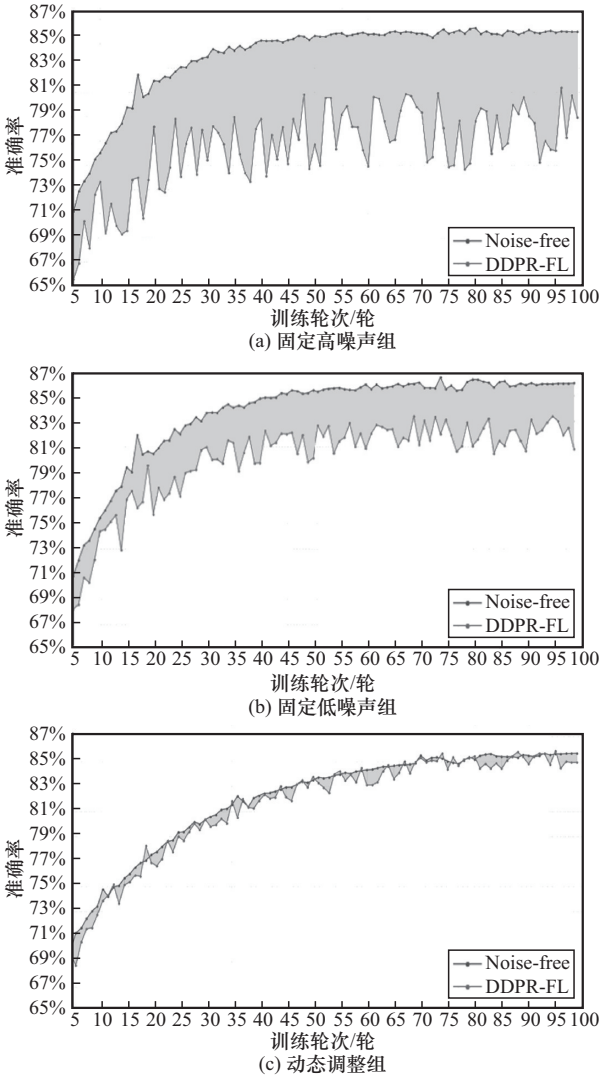

图6 动态隐私预算调整策略对联邦学习系统性能的优化效果

采用动态隐私预算调整策略后（$\rho_{\min} = 0.01$，$\rho_{\max} = 0.2$，$\beta = 0.03$），模型准确率曲线与无噪声基准线的拟合度很高，最终测试准确率为86.2%。该策略通过三阶段噪声控制实现安全与效能的协同，结合零集中差分隐私转换机制，在保证模型实用性的同时满足严格隐私约束。

如图7所示，DDPR-FL在隐私–性能平衡维度展现出显著优势。在总隐私预算ρ_{total}=100时，DDPR-FL在Fashion-MNIST下达到78.7%的峰值准确率，较Fedopt（69.2%）、EPPDA（60.5%）、DP-GSGLD（62.1%）和EPP-FL（56.4%）分别提升9.5%、18.2%、16.6%和22.3%。其低预算区间的准确率跃升幅度尤为突出，当ρ_{total}=40时准确率为62.3%，较第二名EPPDA（50.1%）领先12.2%。这是由于动态机制通过隐私预算的渐进式释放，在横向维度实现隐私保护强度与模型精度的正向关联，纵向维度完成节点级预算分配与训练阶段噪声调控的双重优化。

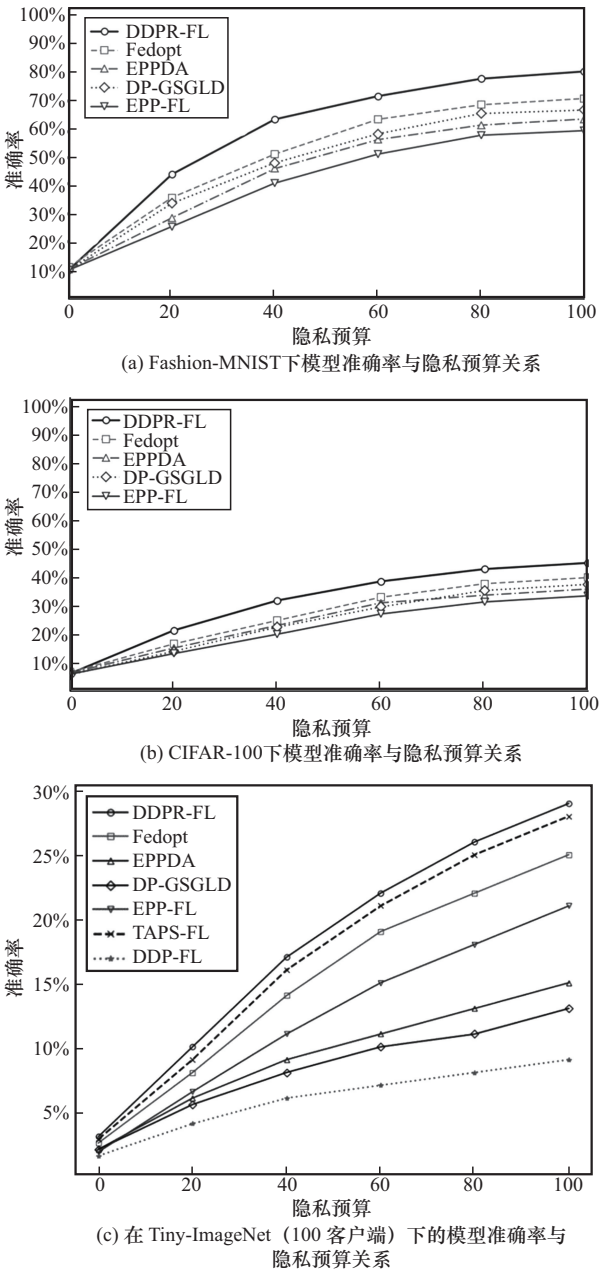

图7 3种数据集下模型准确率与隐私预算关系

为进一步验证DDPR-FL在高难度视觉任务和大规模客户端环境中的适应性，将7种主流联邦学习方法部署在Tiny-ImageNet及100客户端的强异构场景下进行对比，如图7(c)所示。在整体隐私预算受限的条件下，所有方法的模型精度均显著低于CIFAR-100场景。其中，DDPR-FL始终保持最优性能，在ρ_{total}=100时达到29%的准确率，明显优于Fedopt（25%）和EPP-FL（21%）。TAPS-FL的表现接近DDPR-FL，但总体略低，说明其在动态噪声干扰下仍存在收敛稳定性不足的问题。

3.3　节点动态隐私预算管理分析

表1展示了动态联邦学习场景下隐私预算分配与系统活跃节点数量的关联关系。随着训练轮次从20轮增至100轮，本文对活跃节点数量进行主动调整，而隐私预算随着节点数量，呈现跟随式增长特征，验证了动态预算回收机制对节点波动的强适应性。

表1　系统活跃节点数量对隐私预算分配的影响

训练轮次/轮	活跃节点数/个	单轮隐私预算
20	60	0.030
40	40	0.020
60	30	0.012
80	50	0.026
100	65	0.028

图8中，当节点变化率达+10%时，DDPR-FL的隐私预算节省率稳定在30.1%，较排名第二的DP-GSGLD（18.6%）提高11.5%，尤其在节点骤增骤减的极端场景下，其节省率依然达到了15.4%和28.3%，说明节点级动态预算重分配策略有效抑制了节点动态变化对系统带来的冲击。在节点频繁变化的边缘计算场景中，DDPR-FL的预算管理策略可减少约20%的隐私预算冗余，同时保证模型训练稳定性。

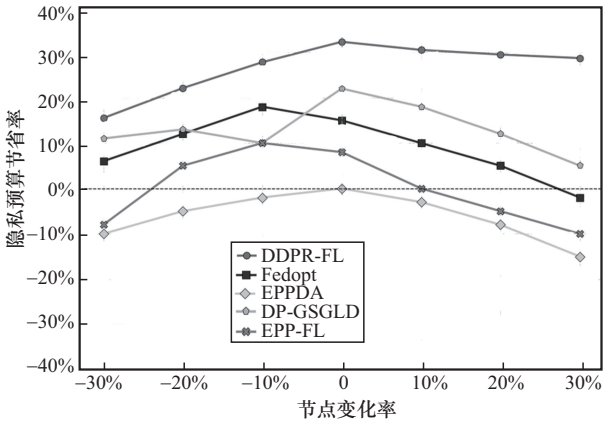

图8　DDPR-FL与基线的节点变化对隐私预算节省率的影响对比

表2数据验证了DDPR-FL在动态节点变化下的收敛效率优势。在FMNIST上，当节点变化率从−30%激增至30%时，DDPR-FL的收敛轮次仅从24轮线性增至37轮，相较Fedopt（28→38）、EPP-FL（30→40）和DP-GSGLD（30→40）分别节省了6.7%~7.5%的收敛轮次。突发性批量退出（Burst，40%节点瞬时离线）与周期性恶意退出混合（Malicious，攻击节点频繁上下线）的极端条件下，虽然各方法的收敛轮次均有所上升，但DDPR-FL的收敛速度提高仍保持在2.4%~16.7%，性能下降幅度低于其他方法，说明动态预算回收与弹性重分配机制能够在极端波动环境中维持基本稳定性。该结果进一步验证了本文方法在高不确定性算力网络环境中的鲁棒性。

表2　FMNIST数据集下节点变化对各系统收敛速度的影响

方法	节点变化率					突发性批量退出	周期性恶意退出
	−30%	−10%	0	10%	30%		
Fedopt	28	30	32	35	38	45	53
EPP-FL	30	32	34	37	40	48	51
EPPDA	32	34	36	39	43	52	60
DP-GSGLD	30	32	35	37	40	46	55
FedAvg	22	24	25	29	33	42	48
TAPS-FL	30	33	34	38	44	48	50
DDP-FL	35	38	40	43	49	60	70
DDPR-FL	24	27	28	31	37	40	44

注:表中数值为全局模型在不同节点动态变化条件下达到稳定收敛所需的通信轮次。

表3的结果显示，在Tiny-ImageNet（100客户端）强异构场景下，各方法的收敛速度均明显慢于FMNIST，但性能排序保持一致。DDPR-FL始终表现最佳，在节点变化率从−30%增至30%期间，其收敛轮次仅由55轮上升到78轮，并在突发性节点退出与周期性恶意退出下分别保持在90轮和104轮，退化幅度最小。TAPS-FL为次优方法，在动态节点变化与攻击下收敛速度略弱于DDPR-FL，但依然优于Fedopt、FedAvg等传统方法。相比之下，EPP-FL、EPPDA与DP-GSGLD在高波动环境中收敛速度下降更为明显，而DDP-FL受节点波动和噪声扰动影响最为严重，在周期性恶意退出下收敛轮次高达160轮。整体来看，DDPR-FL在大规模复杂任务与动态算力波动条件下保持了最优的收敛效率与鲁棒性，验证了其动态预算重校准和噪声自适应机制的有效性。

3.4 模型反演攻击结果分析

图9对比了不同隐私机制下模型反演攻击MSE对比。由图9可知，DDPR-FL在模型反演攻击场景下取得了最高的MSE（0.095），显著高于DDP-FL（0.082）以及TAPS-FL、DP-GSGLD和EPP-FL等基线方法。这主要得益于DDPR-FL将动态隐私预算重校准、分层噪声注入与稀疏梯度编码进行协同设计。相比之下，DDP-FL虽然同样采用了动态差分隐私机制，但缺乏对梯度结构与通信压缩的协同优化，因而在抵御模型反演攻击方面略逊一筹。

3.5 通信开销量化分析

实验结果表明，DDPR-FL基于贡献度分析的稀疏梯度编码与动态分层噪声机制，在通信效率与模型性能间实现了显著优化。如表4所示，当采用

表3 Tiny-ImageNet（100客户端）下节点变化对各系统收敛速度的影响

方法	节点变化率					突发性批量退出	周期性恶意退出
	−30%	−10%	0	+10%	+30%		
Fedopt	65	70	72	78	88	105	120
EPP-FL	70	75	78	85	96	115	132
EPPDA	75	80	82	90	102	120	138
DP-GSGLD	73	78	80	88	100	118	136
FedAvg	60	63	65	72	84	98	112
TAPS-FL	58	62	66	72	82	95	110
DDP-FL	90	93	95	105	120	140	160
DDPR-FL	55	58	60	66	78	90	104

注：表中数值为全局模型在不同节点动态变化条件下达到稳定收敛所需的通信轮次。

表4 DDPR-FL与各基线通信性能对比

梯度稀疏比例	分层编码策略	方法	通信字节数/B	通信开销降低率		模型准确率
				与Fedopt相比	与EPP-FL相比	
0	无	Fedopt	15 353	—	—	37.3%
0	无	EPP-FL	16 420	—	—	34.8%
0	无	本文方法	18 731	↑22.0%	↑14.1%	40.8%
10%	8 bit量化	本文方法	15 607	↑1.6%	↓5.0%	35.4%
20%	8 bit量化	本文方法	12 840	↓16.4%	↓21.8%	32.6%
40%	8 bit量化	本文方法	10 433	↓32.0%	↓36.4%	22.9%
10%	16 bit量化	本文方法	16 410	↑6.9%	↑0.2%	37.2%
20%	16 bit量化	本文方法	14 320	↓6.7%	↓12.8%	34.0%
40%	16 bit量化	本文方法	12 554	↓18.2%	↓23.5%	25.7%
动态调整	自适应分层量化	本文方法	12 347	↓19.6%	↓24.8%	39.5%

动态自适应分层量化策略时，DDPR-FL 通信字节数降至 12 347，较基线 Fedopt（15 353）降低 19.6%，同时维持 39.5% 的模型准确率。

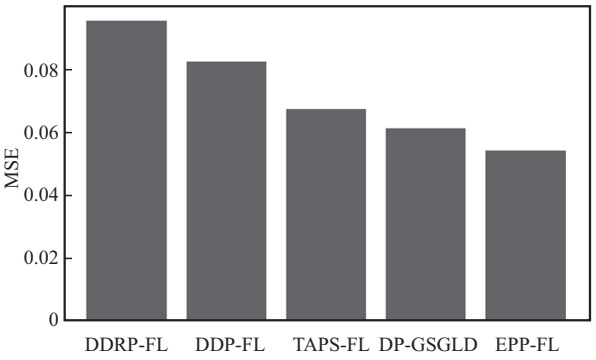

图 9　不同隐私机制下模型反演攻击 MSE 对比

图 10 对比了 3 种方法的本地训练时延差异分布。相较于其他 2 种方法，本文方法呈现出更紧凑的箱体结构，说明各参与设备的训练耗时更为集中。优化后的箱线图四分位距显著收窄，且异常值数量减少，表明系统能有效平衡异构设备的计算能力差异。这种均衡化处理使联邦学习在复杂网络环境中的通信效率得到整体提升，训练过程的时间稳定性进一步增强。

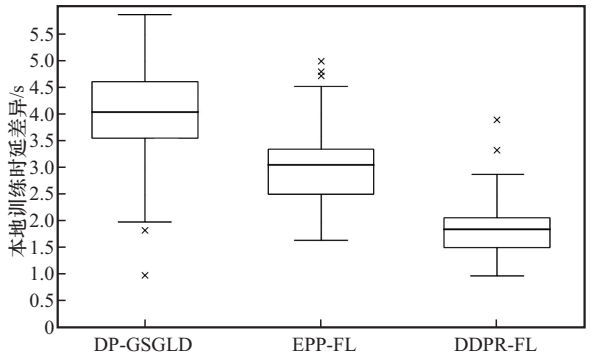

图 10　3 种方法的本地训练时延差异

在本地时延层面，DDPR-FL 通过算力感知动态批量调度策略，在联邦学习效率优化维度实现了本地时延的较大降低。如图 11 所示，在通信轮次增大至 200 轮时，DDPR-FL 的本地训练时延曲线始终处于最低位，尤其在第 200 轮时本地时延仅为 1 245 s，较 FedAvg（3 961 s）、Fedopt（2 207 s）、和 EPP-FL（1937 s）分别降低 68.6%、43.6% 和 35.7%。这种效率优势直接受益于该策略对异构节点算力的动态建模能力与批量调整机制。

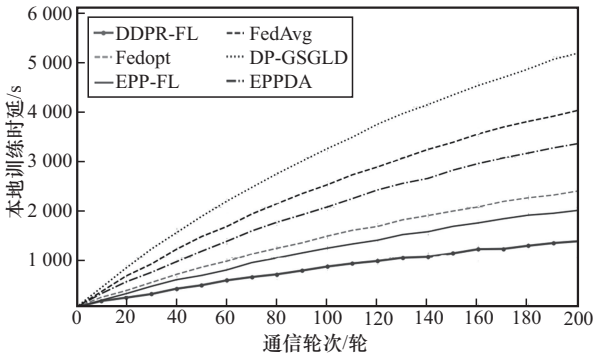

图 11　DDPR-FL 与各基线方法本地训练时延对比

4　结束语

本文提出面向动态算力节点的差分隐私重校准联邦学习方法，通过动态隐私预算校准机制、贡献度感知加噪模型和索引化通信协议三维协同优化框架，创新性地融合了基于训练阶段的动态噪声调整策略、贡献度驱动稀疏梯度编码与分层量化压缩技术，以及动态算力感知批量调整机制。该方法在 CIFAR-100 和 Fashion-MNIST 实验中实现了隐私预算利用率平均提升 23.8%、模型准确率达 78.7%（较基线方法平均提升 15.5%）、通信开销降低 19.6% 的三重突破。通过动态噪声方差调节与梯度稀疏化的联动机制，有效平衡了隐私保护强度与模型收敛稳定性。在未来工作中，稀疏编码协议对非结构化梯度特征的适应性仍需优化，同时在极端高动态场景（节点变化率>50%）下的预算再分配时延仍需进一步思考。

参考文献：

[1] 贾庆民, 丁瑞, 刘辉, 等. 算力网络研究进展综述[J]. 网络与信息安全学报, 2021, 7(5): 1-12.
JIA Q M, DING R, LIU H, et al. Survey on research progress for compute first networking[J]. Chinese Journal of Network and Information Security, 2021, 7(5): 1-12.

[2] TANG X Y, CAO C, WANG Y X, et al. Computing power network: the architecture of convergence of computing and networking towards 6G requirement[J]. China Communications, 2021, 18(2): 175-185.

[3] WANG R J, LAI J S, ZHANG Z Y, et al. Privacy-preserving federated learning for Internet of medical things under edge computing[J]. IEEE Journal of Biomedical and Health Informatics, 2023, 27(2): 854-865.

[4] WEN J, ZHANG Z X, LAN Y, et al. A survey on federated learning: challenges and applications[J]. International Journal of Machine Learning and Cybernetics, 2023, 14(2): 513-535.

[5] BANABILAH S, ALOQAILY M, ALSAYED E, et al. Federated learning review: fundamentals, enabling technologies, and future applications[J]. Information Processing & Management, 2022, 59(6): 103061.

[6] ZHANG J P, ZHU H, WANG F W, et al. Security and privacy threats to federated learning: issues, methods, and challenges[J]. Security and Communication Networks, 2022, 2022(1): 2886795.
[7] 贾庆民, 胡玉姣, 张华宇, 等. 确定性算力网络研究[J]. 通信学报, 2022, 43(10): 55-64.
JIA Q M, HU Y J, ZHANG H Y, et al. Research on deterministic computing power network[J]. Journal on Communications, 2022, 43(10): 55-64.
[8] SUN Y K, LEI B, LIU J L, et al. Computing power network: a survey[J]. China Communications, 2024, 21(9): 109-145.
[9] SHENAJ D, TOLDO M, RIGON A, et al. Asynchronous federated continual learning[C]//Proceedings of the 2023 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW). Piscataway: IEEE Press, 2023: 5055-5063.
[10] LI T, SAHU A K, TALWALKAR A, et al. Federated learning: challenges, methods, and future directions[J]. IEEE Signal Processing Magazine, 2020, 37(3): 50-60.
[11] MOHAMMADZADEH A, MASDARI M, GHAREHCHOPOGH F S, et al. Improved chaotic binary grey wolf optimization algorithm for workflow scheduling in green cloud computing[J]. Evolutionary Intelligence, 2021, 14(4): 1997-2025.
[12] 王瑞锦, 王金波, 张凤荔, 等. 联邦原型学习的特征图中毒攻击和双重防御机制[J]. 软件学报, 2025, 36(3): 1355-1374.
WANG R J, WANG J B, ZHANG F L, et al. Feature map poisoning attack and dual defense mechanism for federated prototype learning[J]. Journal of Software, 2025, 36(3): 1355-1374.
[13] CHEN Y Q, JIANG C F, YAN L C, et al. Research progress on computing power network for the power industry[C]//Proceedings of the 2024 IEEE 12th International Conference on Information, Communication and Networks (ICICN). Piscataway: IEEE Press, 2024: 201-210.
[14] LUO Q Y, HU S H, LI C L, et al. Resource scheduling in edge computing: a survey[J]. IEEE Communications Surveys & Tutorials, 2021, 23(4): 2131-2165.
[15] LI H Z, ZHOU S J, YUAN B, et al. Optimizing intelligent edge computing resource scheduling based on federated learning[J]. Journal of Knowledge Learning and Science Technology, 2024, 3(3): 235-260.
[16] CHEN X J, LI Z Y, NI W, et al. Toward dynamic resource allocation and client scheduling in hierarchical federated learning: a two-phase deep reinforcement learning approach[J]. IEEE Transactions on Communications, 2024, 72(12): 7798-7813.
[17] CAI J H, CHEN B J, WEN J, et al. A joint vehicular device scheduling and uncertain resource management scheme for Federated learning in Internet of Vehicles[J]. Information Sciences, 2025, 690: 121552.
[18] GUPTA M, KUMAR M, DHIR R. Unleashing the prospective of blockchain-federated learning fusion for IoT security: a comprehensive review[J]. Computer Science Review, 2024, 54: 100685.
[19] BATOOL H, ANJUM A, KHAN A, et al. A secure and privacy preserved infrastructure for VANETs based on federated learning with local differential privacy[J]. Information Sciences, 2024, 652: 119717.
[20] LING J, ZHENG J C, CHEN J H. Efficient federated learning privacy preservation method with heterogeneous differential privacy[J]. Computers & Security, 2024, 139: 103715.
[21] PAUU K T, PAN Q Q, WU J, et al. IRS-aided federated learning with dynamic differential privacy for UAVs in emergency response[J]. IEEE Internet of Things Magazine, 2024, 7(4): 108-115.
[22] YANG C Y, JIA K, KONG D L, et al. DP-GSGLD: a Bayesian optimizer inspired by differential privacy defending against privacy leakage in federated learning[J]. Computers & Security, 2024, 142: 103839.
[23] SONG J C, WANG W Z, GADEKALLU T R, et al. EPPDA: an efficient privacy-preserving data aggregation federated learning scheme[J]. IEEE Transactions on Network Science and Engineering, 2023, 10(5): 3047-3057.
[24] CHEN Z J, LIAO G C, MA Q, et al. Adaptive privacy budget allocation in federated learning: a multi-agent reinforcement learning approach[C]//Proceedings of the ICC 2024 - IEEE International Conference on Communications. Piscataway: IEEE Press, 2024: 5166-5171.
[25] HONG J Y, WANG Z Y, ZHOU J Y. Dynamic privacy budget allocation improves data efficiency of differentially private gradient descent[C]//Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency. New York: ACM Press, 2022: 11-35.
[26] ALDAGHRI N, MAHDAVIFAR H, BEIRAMI A. Federated learning with heterogeneous differential privacy[J]. arXiv Preprint, arXiv: 2110.15252, 2021.
[27] KIANI S, KULKARNI N, DZIEDZIC A, et al. Differentially private federated learning with time-adaptive privacy spending[J]. arXiv Preprint, arXiv: 2502.18706, 2025.
[28] GUO S N, WANG X B, LONG S G, et al. A federated learning scheme meets dynamic differential privacy[J]. CAAI Transactions on Intelligence Technology, 2023, 8(3): 1087-1100.
[29] MCMAHAN H B, MOORE E, RAMAGE D, et al. Communication-efficient learning of deep networks from decentralized data[J]. arXiv Preprint, arXiv: 1602.05629, 2016.

[作者简介]

陈宁江（1975– ），男，广西南宁人，博士，广西大学教授、博士生导师，主要研究方向为云计算和大数据、智能软件工程等。

郑泽章（1997– ），男，江西抚州人，主要研究方向为联邦学习、算力网络、隐私保护等。

章德华（2001– ），男，壮族，江西抚州人，广西大学硕士生，主要研究方向为边缘计算、联邦学习等。