面向联邦算力物联网的隐私预算自适应优化方案

马文玉[1]，陈谦[2]，胡宇翔[1]，闫皓楠[2]，胡涛[1]，伊鹏[1]
（1. 信息工程大学，河南 郑州 450001；2. 西安电子科技大学，陕西 西安 710126）

摘　要：联邦算力物联网（IoT, Internet of things）旨在通过联邦学习深度融合算力与物联网资源，从而实现对泛在离散部署的海量物联网数据和异构资源的高效利用。为了应对联邦算力物联网中模型反演和梯度泄露等新兴隐私攻击威胁，学术界和产业界对差分隐私（DP, differential privacy）这一高效的隐私保护技术进行了广泛研究和应用。然而，现有差分隐私技术在设定隐私预算时，未考虑本地算力节点的数据特征和隐私预算分配公平性的问题，造成了严重的模型精度损失。因此，提出了一种面向联邦算力物联网的隐私预算自适应优化方案——基于克拉美罗下界差分隐私的联邦学习（FedCDP, federated learning based on Cramér-Rao lower bound differential privacy）。首先，基于克拉美罗下界理论分析边缘算力节点的隐私预算估计值，实现自适应隐私预算规划；其次，通过计算边缘算力节点的上传模型与算力聚合服务器的聚合模型之间的相似度和隐私预算占比，分析得到每个节点的全局贡献度，进一步联合隐私预算估计值公平实时地优化隐私预算设定。理论分析证明了该方案可确保本地模型严格遵守 ε-差分隐私，并保证全局模型收敛。基于多个公开数据集上的实验结果表明，在满足相同隐私保护需求的前提下，该方案将全局模型精确度最多提升了 10.19%。

关键词：联邦算力物联网；差分隐私；隐私预算；自适应优化
中图分类号：TP309.2
文献标志码：A
doi：10.11959/j.issn.2096−3750.2024.00440

A privacy budget adaptive optimization scheme for federated computing power Internet of things

MA Wenyu[1], CHEN Qian[2], HU Yuxiang[1], YAN Haonan[2], HU Tao[1], YI Peng[1]
1. Information Engineering University, Zhengzhou 450001, China
2. Xidian University, Xi'an 710126, China

Abstract: Federated computing power Internet of things (IoT) is designed to deeply integrate computing power with IoT resources, facilitating the efficient utilization of vast and ubiquitously dispersed IoT data and heterogeneous resources through federated learning. Faced with the threats of emerging privacy attacks, e.g., model inversion attacks and gradient leakage attacks, the academic and industrial communities have widely investigated and applied differential privacy (DP) as an effective privacy protection technique. However, two severe challenges have not been taken into account in the existing DP budget settings, i.e., data heterogeneity issue of local computing power nodes and the fairness of privacy budget allocation, which lead to a significant loss in model accuracy. Therefore, an adaptive optimization scheme for privacy budget was proposed in federated computing power IoT, which was called federated learning based on Cramér-Rao lower bound differential privacy (FedCDP). In specific, to adaptively adjust privacy budgets, the privacy budget estimates for edge computing power nodes based on the Cramér-Rao lower bound theory were analyzed. Furthermore, by assessing the simi-

收稿日期：2024−10−16；修回日期：2024−11−24
通信作者：陈谦，chenqian_sec@163.com
基金项目：国家重点研发计划（No. 2022YFB2901500）；国家自然科学基金资助项目（No. 62402373）
Foundation Items: The National Key Research and Development Program of China (No. 2022YFB2901500), The National Natural Science Foundation of China (No. 62402373)

larity between the local model and the aggregated model, as well as their respective privacy budget proportions, the global contribution of each node was determined, which was used to fairly, also in real time, optimize and adjust the privacy budget settings in conjunction with the estimated privacy budget. Through rigorous theoretical analysis, FedCDP achieves ε-DP for local models, and ensures the convergence of the global model. Experimental results on multiple public datasets show that the proposed scheme improves the accuracy of the global model by up to 10.19% under the premise of satisfying the same privacy protection requirements.

Key words: federated computing power IoT, differential privacy, privacy budget, adaptive optimization

0　引言

算力物联网作为一种新兴计算范式，其核心特点是物联网中分布式计算资源的聚合与优化利用，通过整合分散的计算能力，形成庞大的计算资源池，为各种应用提供有力的计算支撑[1-2]。联邦学习作为一种分布式机器学习技术，能够在数据不出本地的前提下，实现多节点对全局模型的协同训练，确保了节点数据的隐私和通信效率[3-4]。联邦学习赋能算力物联网为其发展注入了新活力，通过充分利用各个边缘节点的隐私数据和计算资源，实现了模型的分布式训练，确保了算力物联网中数据安全地共享和利用，将算力物联网应用方向拓展至智能学习[5]、卫星物联网[6]、电力物联网[7]、车联网[8]等应用。

尽管联邦算力物联网备受工业界和学术界的关注和重视，但在实际应用过程中仍面临数据隐私泄露和模型性能降级等严峻的挑战。以模型反演[9]和梯度泄露[10]为代表的隐私攻击严重威胁联邦算力物联网的安全性和隐私保护，攻击者可以根据上传的模型参数逆向推演和泄露用户的原始数据，从而获取敏感信息，威胁用户的隐私。此外，算力物联网中边端节点基于地理、时间和人文等因素分散式部署，节点本地异构数据存在非独立同分布（Non-IID, non-independent identically distributed）现象[11]。基于此类数据进行联邦模型训练会引发模型收敛困难和预测性能降级等问题[12]。

围绕上述挑战，当前已有大量工作面向联邦算力物联网的数据隐私和模型可用性开展研究。一方面，针对联邦算力物联网中数据隐私保护，相关研究人员引入同态加密[13]、安全多方计算[14]、差分隐私（DP, differential privacy）[15]等技术对本地模型进行安全聚合，其中，差分隐私方法[16-20]通常通过对本地模型更新参数进行基于随机噪声的扰动来提供理论可证的隐私性能保障，但为每一轮数据查询或学习过程设置固定的隐私预算，无法有效地解决数据的异构特性引发的隐私泄露风险，也无法平衡隐私保护需求和模型性能；另一方面，尽管针对数据异构环境下联邦算力物联网的模型性能降级问题，研究者提出了FedAvg[21]、个性化联邦算力物联网[22]、多任务学习[23]、元学习[24]等方法进行模型性能优化，但此类算法均无法有效地抵御隐私攻击威胁。汤东汰[25]提出了一种基于交替方向乘子法的差分隐私联邦学习算法DP-FedADMM。该算法综合考虑梯度二范式、训练损失、模型准确率和时间因素，刻画评分函数，实现噪声的自适应添加。但DP-FedADMM未考虑隐私预算对添加噪声量的影响，无法获得高预测精度的全局模型。另外，由于数据和算力分布在边缘节点，算力聚合服务器难以掌握用户数据的详细情况，无法监管具体细节。因此，边缘算力节点为了个人隐私可能虚报隐私损失，这种普遍的夸大行为会在多轮迭代计算中累积，将严重损害模型性能。

综上所述，联邦算力物联网的现有研究工作主要存在以下不足：1) 固定的差分隐私预算影响模型隐私性及性能；2) 隐私预算设定未考虑边缘算力节点的本地数据的异构特性；3) 算力聚合服务器分配隐私预算时未考虑全局及本地模型实时状态。以上不足揭示了数据异构背景下兼顾隐私保护需求和模型预测性能的联邦算力物联网算法的缺失。对该问题的求解须综合考量节点差异化隐私需求与数据异构特性对模型性能产生的影响。一方面，若侧重于提升模型性能，则须确保在集成差分隐私机制后，模型的准确性与收敛速率受到的负面影响最小化；另一方面，若侧重于强化隐私保护，则须确保在模型训练过程中通过恰当地引入噪声来满足隐私保护标准，同时确保这些措施不会对模型性能造成过度的损害。另外，联邦算力物联网中数据的高度异构性和多样化的用户隐私需求增加了问题的复杂性。

针对此问题，本文提出了一种面向联邦算力物联网的隐私预算自适应优化方案——基于克拉美罗下界差分隐私的联邦学习（FedCDP, federated learning based on Cramér-Rao lower bound differential privacy）。该方案的核心思路是根据边缘算力节点的本地模型参数特征和算力聚合服务器的实时反馈，动态调整各参与方的隐私预算。在联邦算力物联网模型协同训练的每一轮次迭代中，对于边缘算力节点更新后的本地模型参数和聚合后的全局模型参数，基于克拉美罗下界（CRLB, Cramér-Rao lower bound）理论分析边缘算力节点的隐私预算估计值。进而基于模型相似度和隐私预算占比分析节点全局贡献度，联合隐私预算估计值和全局贡献度构建隐私预算动态调整函数，实现迭代调整边缘算力节点的隐私预算设定并更新下发。基于上述内容，本文的主要贡献总结如下。

1) 本文提出了基于差分隐私的FedCDP方案，通过同时优化边缘算力节点的隐私预算规划和算力聚合服务器的隐私预算分配，以有效地兼顾模型隐私保护和性能效用。该方案由基于CRLB的隐私预算规划算法和隐私预算公平反馈算法两个核心组件构成，分别实现了自适应隐私预算规划和隐私预算公平实时优化。

2) 本文理论分析了所提方案的隐私性和收敛性。FedCDP能够确保本地模型参数实现ε-差分隐私，并能够保障本地数据非独立同分布情况下的模型收敛。

3) 基于公开数据集MNIST和CIFAR10开展实验评估。实验结果表明，与最先进方法相比，FedCDP能够在满足差分隐私需求的前提下将全局模型准确率最多提升10.19%。

1　相关工作和预备知识

1.1　相关工作

以算力物联网为代表的分布式计算架构，将分散的计算资源（如边缘算力节点、云计算中心等）连接成网络，提供弹性的计算能力，以满足各种计算需求，优化数据处理速度和效率。随着算力物联网的智能化和数字化水平的不断提升，分布式机器学习与算力物联网深度融合。作为其中的典型代表，联邦算力物联网基于联邦学习架构，允许数据保留在分布式边缘算力节点本地，基于算力聚合服务器共同训练一个融合所有数据特性的高质量全局模型，FedAvg[26]是其中的一个代表，但本地数据固有的Non-IID特性[27-28]仍带来了巨大的挑战，个性化联邦算力物联网应运而生。主流个性化联邦算力物联网算法包括LG-FedAvg[29]、FedPer[30]、CEFMR[31]和FedBABU[32]等，其中，LG-FedAvg[29]利用固定的本地参数来提取本地数据特征，从而实现个性化，但这种静态分区方法缺乏适应不同数据特征的灵活性。此外，FedPer[30]和FedBABU[32]算法通过在本地保留特定层来实现个性化，可以更好地迎合本地数据特征，但在模型个性化方面存在灵活性不足的问题。

差分隐私通过最小化单个数据变化对计算输出的影响，在联邦算力物联网中提供了大量的隐私[33-38]。在联邦算力物联网中，用户级DP是通过DP机制加噪实现的。增加的噪声导致的性能下降和限幅导致的较慢收敛，这些挑战已经通过几种方法解决，包括LUS[39]、BLUR[39]和DP-FedSAM[36]。LUS和BLUR采用稀疏化和统一正则化技术来减轻添加噪声的影响并增强模型的收敛性，但它们不能充分解决DP中噪声添加引起的问题。它们没能找到噪声扰动问题的本质，在联邦学习模型训练过程中，所有参数都会受到不恰当噪声的影响，导致模型性能下降。

在DP机制中，隐私预算作为关键参数，是由算力聚合服务器下发到各边缘算力节点的，可以控制隐私保护水平。现有的DP机制大部分是固定每一轮隐私预算，而固定隐私预算会导致隐私保护的不足或过度。如果隐私预算设置过小，那么为了保护隐私，需要添加过多的噪声，这会降低模型的准确性和可用性。相反，如果隐私预算设置过大，将无法提供足够的隐私保护，从而增加数据泄露的风险。此外，固定隐私预算无法适应不同的数据集大小和查询次数，导致隐私损失的累积，进而在多次查询后可能无法维持预期的隐私保护水平。现有研究已经注意到了隐私预算的重要性，PrivateKub[40]是一个扩展了流行的Kubernetes数据中心编排器的项目，增加了隐私作为一种新的资源，与传统的计算资源如CPU、GPU和内存一起来管理。BR-DP（budget recycling differential privacy）[41]旨在为现有的DP机制提供软有界的噪声输出，通过“软有界”，指的是该机制能够在预定义的错误边界内发布大多数输出，从而在保证隐私的同时提高模型准确率。DPBalance[41]开发了一个结合了数据分析师级别的主导份额和联邦算力物联网特定的性能指标

的综合效用函数，然后设计了一个使用拉格朗日乘数法和有效的贪婪启发式方法的顺序分配机制，是一个针对联邦算力物联网的隐私预算调度机制。尽管现有的隐私预算分配机制在保护用户隐私方面取得了一定的进展，但在动态调整隐私预算以适应不同数据集和查询模式方面还存在不足。因此，本文提出了面向联邦算力物联网的隐私预算自适应优化方案——FedCDP，该方案能够根据数据的特点和查询的需求，动态调整隐私预算，以实现更有效的隐私保护和模型性能之间的平衡。

1.2　预备知识

1.2.1　联邦算力物联网

联邦算力物联网[15]由两个主要部分组成：算力聚合服务器S和边缘算力节点n_i，$i \in \{1,2,\cdots,N\}$，每个边缘算力节点n_i具有本地数据集D_i，大小为$|D_i|$，而各节点的本地数据集中通常包含生物识别信息、特定身份信息等敏感信息。算力聚合服务器的训练目标是在无法完全获取各边缘算力节点的敏感信息的情况下，学习所有节点数据的模型。所有边缘算力节点的目标是以保护隐私的方式，在算力聚合服务器的指导下协作训练全局模型。

参与本地训练的边缘算力节点需要找到模型权重向量$\boldsymbol{w}_i$以最小化损失函数，算力聚合服务器需要聚合N个边缘算力节点上传的模型的权重，如式(1)和式(2)所示。

$$\boldsymbol{w} = \sum_{i=1}^{N} p_i \boldsymbol{w}_i \tag{1}$$

$$p_i = \frac{|D_i|}{\sum_{i=1}^{N} |D_i|} \tag{2}$$

其中，$\boldsymbol{w}_i$是在边缘算力节点i的模型参数，p_i是聚合权重，$\boldsymbol{w}$是聚合后的全局模型参数，N是边缘算力节点数量。因此，联邦算力物联网模型训练目标如式(3)所示。

$$\boldsymbol{w}^* = \arg\min_{\boldsymbol{w}} \sum_{i=1}^{N} p_i L_i(\boldsymbol{w}, D_i) \tag{3}$$

其中，$L_i(\cdot)$是边缘算力节点i的损失函数。

1.2.2　克拉美罗下界

CRLB[42]是统计估计理论中的一个重要结果，它为参数估计的方差提供了一个理论上的下界。在联邦算力物联网的训练过程中，CRLB可以用于评估模型参数估计的准确性和可靠性。在DP的背景下，CRLB可以用来确定在不泄露个人信息的前提下，从数据中提取信息的理论极限。计算模型参数的Fisher信息量，可以确定在添加DP噪声时，为了达到特定隐私保护水平，所必需的最小噪声水平。

1.2.3　差分隐私

定义 1　ε-差分隐私[19]。对于任意算法M，Range(M)为M输出的取值范围，若算法M在数据集D和D'上任意输出结果$O\left(O \in \text{Range}(M)\right)$满足下列不等式式(4)，则称$M$满足$\varepsilon$-差分隐私。

$$\Pr[M(D) = O] \leqslant \exp(\varepsilon) \times \Pr[M(D') = O] \tag{4}$$

其中，ε为隐私预算，可以控制隐私保护水平；$\exp(\varepsilon)$是ε的指数函数；数据集D和D'为邻近数据集；Pr表示将算法M作用于数据集D和D'输出Range(M)的概率。

联邦算力物联网通过向本地训练后模型参数添加适量噪声来实现DP。为了保证严格的隐私界限，面向联邦算力物联网，本文采用基于Laplace噪声的差分隐私机制。

定义 2　Laplace机制[43]。通过向真实查询结果中加入服从Laplace分布的随机噪声来实现ε-差分隐私保护。记均值为0、尺度参数为σ的Laplace分布为Lap(σ)，其概率密度函数为

$$P(x) = \frac{1}{2\sigma} \exp\left(-\frac{|x|}{\sigma} \right) \tag{5}$$

2　方案设计

本节首先分析联邦算力物联网的威胁模型，接着针对隐私攻击威胁提出FedCDP的整体方案框架，进而详细阐述其核心组件基于CRLB的隐私预算规划算法和隐私预算公平反馈算法。

2.1　威胁模型

联邦算力物联网架构及其威胁模型如图1所示，分析威胁模型之前，首先简述联邦算力物联网的基本运行流程[44-45]，该流程分为3个步骤。

步骤 1　本地训练。算力聚合服务器初始化全局模型，并下发给所有边缘算力节点，各边缘算力节点利用本地数据进行训练，并将本地训练的模型梯度发送到算力聚合服务器。

步骤 2　模型聚合。算力聚合服务器将N个边缘算力节点上传的模型梯度安全聚合，并将聚合的模型梯度广播给边缘算力节点。

步骤 3　模型更新。边缘算力节点基于聚合后的模型参数更新它们各自的本地模型，并开始新一轮

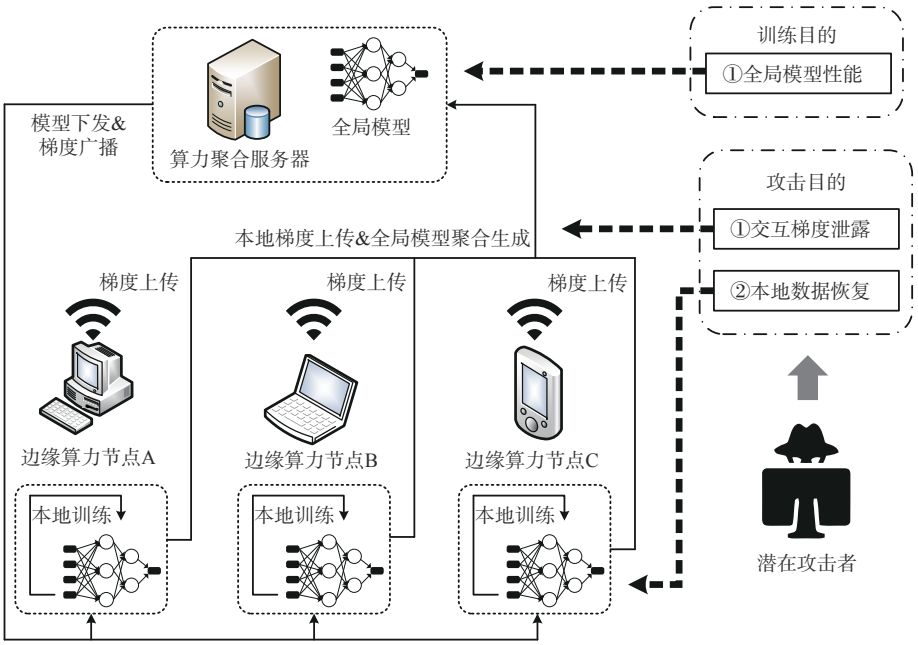

图 1　联邦算力物联网架构及其威胁模型

的本地训练和模型上传过程。

基于上述典型流程，广泛考虑半诚实的威胁模型[11, 13]。如图 1 所示，该威胁模型假设攻击者是诚实但好奇的算力聚合服务器或边缘算力节点，同时存在活跃的外部攻击者，它们都属于潜在威胁对象，会试图提取有关其他边缘算力节点的敏感信息，通过攻击从捕获的模型参数中重构边缘算力节点的本地隐私数据或者推测某个数据样本是否属于某个边缘算力节点的本地数据集。例如，攻击者可以采用梯度泄露攻击分析窃取的模型参数 $\boldsymbol{w}$ 来恢复联邦算力物联网中边缘算力节点 i 的本地数据集 D_i，目标函数如式(6)所示。

$$\arg\min_{D_n^*} E\left[\left|\sum_{x_n^*\in D_n^*}\nabla L(x_n^*;\boldsymbol{w})-\sum_{x_n\in D_n}\nabla L(x_n;\boldsymbol{w})\right|\right] \quad (6)$$

其中，x_n 为边缘算力节点 n 的真实数据集 D_n 中的样本，D_n^* 为由合成数据样本 x_n^* 组成的重构数据集，L 为攻击损失函数。

在式(6)中，攻击者通过最小化重构数据集中所有数据对应梯度和真实数据集中所有数据样本对应梯度之间的平均绝对误差来确保数据隐私窃取的有效性。因此，本文的威胁模型是合理且现实的。在此基础上，威胁模型具体假设如下：

1) 攻击者会诚实地按照规则训练和更新模型，不会干扰对训练有益的参数的产生；

2) 攻击者只能获得其他节点上传到服务器的模型和梯度，无法获得更多信息；

3) 攻击者只能反向推断数据信息，不知道实际攻击目标；

4) 攻击者是外部对手时，能够在执行训练协议时窃听任何共享消息，不会自发地在信息传递中添加虚假信息或干扰信息传递。

2.2　方案框架

FedCDP 整体框架如图 2 所示，设计核心包括基于 CRLB 的隐私预算规划算法（详见第 2.3 节）和隐私预算公平反馈算法（详见第 2.4 节），目标是根据边缘算力节点的本地模型参数和算力聚合服务器的实时反馈动态调整各参与方的隐私预算。在联邦算力物联网的每一轮次迭代中，算力聚合服务器根据边缘算力节点上传的本地模型参数计算得出 CRLB 和该节点的全局贡献度，通过隐私预算调整函数对二者进行结合，从而自适应地计算调整隐私预算并注入相应的 Laplace 隐私噪声。基于上述框架设计，面向联邦算力物联网的隐私预算自适应优化方案的工作流程如图 3 所示，整体上分为以下 3 个阶段。

阶段 1　初始化阶段。在联邦算力物联网的任意第 t（$t\geqslant 1$）轮次通信中，算力聚合服务器初始化全局模型 $\boldsymbol{w}^t$ 和隐私预算 ε^t，并将二者分发给所有参与的边缘算力节点，确保边缘算力节点都从相同的模型参数开始训练。同时，初始隐私预算 ε^t 用于指导边缘算

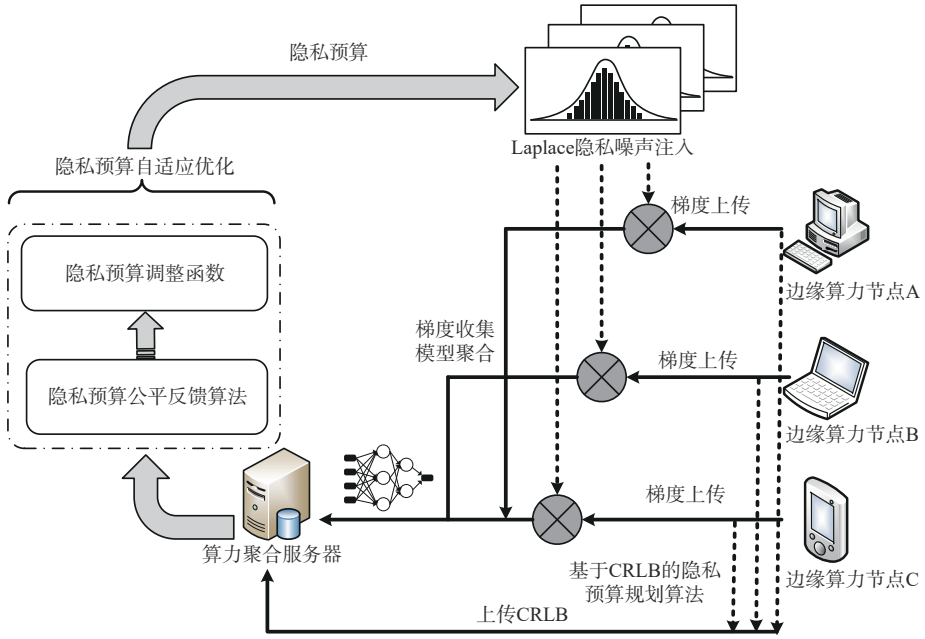

图 2　FedCDP 整体框架

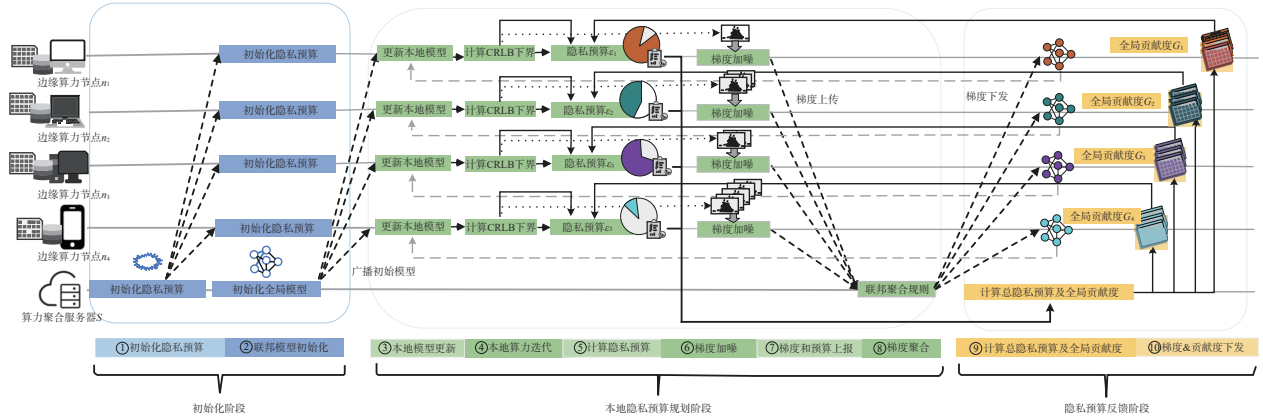

图 3　面向联邦算力物联网的隐私预算自适应优化方案的工作流程

力节点本轮次向本地模型参数所添加的DP噪声量。

阶段 2　本地隐私预算规划阶段。边缘算力节点首先基于本地隐私数据集训练更新本地模型，并对梯度进行规范化和裁剪，限制敏感度。在分配的隐私预算ε^t的指导下，向本地模型参数添加Laplace噪声以得到$\boldsymbol{w}_i^t$。结合本地模型参数$\boldsymbol{w}_i^t$的Fisher信息矩阵[42]，基于CRLB理论预测模型参数下一轮次所能添加的隐私预算估计值Var_i^{t+1}。最后，将加噪后的本地模型参数和隐私预算估计值Var_i^{t+1}上传到算力聚合服务器。

阶段 3　隐私预算反馈阶段。算力聚合服务器首先聚合所有边缘算力节点上传的带噪声模型参数以更新全局模型参数$\boldsymbol{w}^{t+1}$，并基于全局模型参数$\boldsymbol{w}^{t+1}$和本地上传的模型参数$\boldsymbol{w}_i^t$的参数余弦相似度和隐私预算占比，联合评估节点对于模型性能效用的全局贡献度G_i^{t+1}。然后，综合考虑每个边缘算力节点的隐私预算估计值Var_i^{t+1}和全局贡献度G_i^{t+1}，动态调整隐私预算分配，连同更新后的全局模型反馈下发至相应节点，以实时调整边缘算力节点下一轮次隐私预算设定。隐私预算动态调整函数如式(7)所示。

$$\varepsilon_i^{t+1}=\varepsilon_i^t\cdot[\rho\cdot\mathrm{Var}_i^{t+1}+(1-\rho)\cdot G_i^{t+1}] \tag{7}$$

其中，ε_i^t表示t轮次边缘算力节点i的隐私预算分配值；ε_i^{t+1}、Var_i^{t+1}和G_i^{t+1}分别表示t+1轮次边缘算力节点i的隐私预算分配值、隐私预算估计值

和全局贡献度；ρ 为调整因子，控制 CRLB 隐私预算估计值和全局贡献度对隐私预算影响的占比。如果 ρ 接近 1，隐私预算的调整更多依赖于 CRLB 隐私预算估计值，这有助于保护本地模型参数更敏感的边缘算力节点；相反，如果 ρ 接近 0，隐私预算的调整更多依赖于全局贡献度，这有助于奖励那些对全局模型性能提升贡献较大的边缘算力节点。

上述 3 个阶段依据联邦学习全局通信轮次迭代实施，从而联邦算力物联网根据本地边缘算力节点实时反馈和模型参数，动态调整 DP 噪声水平，以有效地兼顾模型隐私保护和性能效用。FedCDP 工作流程如算法 1 所示。

算法 1 FedCDP 工作流程

输入 边缘算力节点数量 N，迭代轮次 T，初始化全局模型参数 $\boldsymbol{w}$，隐私预算 ε，隐私预算调整因子 ρ

输出 最终的全局模型参数 $\boldsymbol{w}_g$

初始化全局模型参数 $\boldsymbol{w}$ 和隐私预算 ε；

for $t = 1, \cdots, T$ **do**

for $i = 1, \cdots, N$ **do**

边缘算力节点开始训练；

接收全局模型参数 $\boldsymbol{w}^t$；

本地模型训练更新，计算模型参数 $\boldsymbol{w}_i^t$；

计算 L2 范数 $\| \boldsymbol{w}_i^t \|_2$；

梯度规范化 $\| \boldsymbol{w}_i^t \|_2 \neq 0$，$\boldsymbol{w}_i^{t'} = \boldsymbol{w}_i^t / \| \boldsymbol{w}_i^t \|$；

梯度裁剪 $\nabla \boldsymbol{w}_i^t = \min(\max(\boldsymbol{w}_i^{t'}, -C), C)$，$C$ 为裁剪阈值；

添加 Laplace 噪声 $\boldsymbol{w}_i^t = \nabla \boldsymbol{w}_i^t + \text{Laplace}(0, \Delta f / \varepsilon_i^t)$；

计算隐私预算估计值 Var_i^{t+1}；（详见算法 2）

上传模型参数 $\boldsymbol{w}_i^t$ 和隐私预算估计值 Var_i^{t+1}；

end for

算力聚合服务器开始聚合，更新全局模型参数 $\boldsymbol{w}^{t+1}$；

计算节点全局贡献度 G_i^{t+1}；（详见算法 3）

for $i = 1$ to, $\cdots, N$ **do**

动态调整隐私预算 $\varepsilon_i^{t+1} = \varepsilon_i^t \cdot [\rho \cdot \text{Var}_i^{t+1} + (1 - \rho) \cdot G_i^{t+1}]$；

下发全局模型参数 $\boldsymbol{w}^{t+1}$、隐私预算 ε_i^{t+1}；

end for

end for

输出分发最终的全局模型参数 $\boldsymbol{w}_g$；

2.3 基于 CRLB 的隐私预算规划算法

该算法旨在通过 CRLB 规划各边缘算力节点的隐私预算。以边缘算力节点 i 为例，基于 CRLB 的隐私预算规划算法如算法 2 所示。首先，基于边缘算力节点 i 更新后的本地模型参数 $\boldsymbol{w}_i$，计算对数似然函数关于 $\boldsymbol{w}_i$ 的梯度 $S_i(\boldsymbol{w}_i)$，如式(8)所示，其中 $l(\cdot)$ 为对数似然函数。然后，在此基础上，计算，Fisher 信息量 $I(\boldsymbol{w}_i)$，如式(9)所示，该信息量表征了模型参数估计的可变性与表示模型性能的数据信息含量之间的关系。最后，基于 CLRB 理论，以 Fisher 信息量 $I(\boldsymbol{w}_i)$ 的逆 $I(\boldsymbol{w}_i)^{-1}$ 作为边缘算力节点 i 的隐私预算估计 Var_i。

$$S_i(\boldsymbol{w}_i) = \frac{\partial l(\boldsymbol{w}_i, x)}{\partial \boldsymbol{w}_i} \tag{8}$$

$$I(\boldsymbol{w}_i) = E\{[S_i(\boldsymbol{w}_i)]^{\mathrm{T}} S_i(\boldsymbol{w}_i)\} \tag{9}$$

鉴于 CRLB 提供了在无噪声情况下模型参数估计的最小方差，所以可以利用 CRLB 的值确定在添加噪声时模型参数估计的方差下限。当在梯度上添加噪声时，实际方差将大于或等于 CRLB 的估计值 Var_i。因此，基于 CRLB 的隐私预算规划算法能够有效地提供满足模型效用情况下的隐私预算估计最小值。

算法 2 基于 CRLB 的隐私预算规划算法

输入 边缘算力节点 i 本地更新后的参数 $\boldsymbol{w}_i$，训练数据集 $D_i(x, y)$

输出 边缘算力节点 i 的隐私预算估计值 Var_i

基于 Fisher 信息矩阵计算对数似然函数关于 $\boldsymbol{w}_i$ 的梯度 $S_i(\boldsymbol{w}_i)$；

计算参数 $\boldsymbol{w}_i$ 的 Fisher 信息量 $I(\boldsymbol{w}_i) = E\{[S_i(\boldsymbol{w}_i)]^{\mathrm{T}} S_i(\boldsymbol{w}_i)\}$；

基于 Fisher 信息量，计算 $I(\boldsymbol{w}_i)$ 的逆；

生成边缘算力节点 i 的隐私预算估计 $\text{Var}_i = I(\boldsymbol{w}_i)^{-1}$；

输出 Var_i；

2.4 隐私预算公平反馈算法

在联邦算力物联网中，为确保全局贡献较多的边缘算力节点获得更多隐私预算，设计了隐私预算公平反馈算法，隐私预算公平反馈算法如算法 3 所示。首先通过余弦相似度来衡量每个边缘算力节点上传的本地模型参数与算力聚合服务器的全

局模型参数之间的相似性，如式(10)所示；然后计算每个边缘算力节点的隐私预算占全局隐私预算的占比，如式(11)所示；进而结合相似度和隐私预算占比，计算每个节点的全局贡献度，如式(12)所示，其中，φ为用于调整相似度和隐私预算占比的比例系数。

$$A_i = \frac{\boldsymbol{w}_i \cdot \boldsymbol{w}_g}{\|\boldsymbol{w}_i\| \cdot \|\boldsymbol{w}_g\|} \tag{10}$$

$$P_i = \frac{\varepsilon_i^t}{\sum_{i=1}^{N} \varepsilon_i^t} \tag{11}$$

$$G_i = \varphi \cdot A_i + (1 - \varphi) \cdot P_i \tag{12}$$

本算法通过余弦相似性反映了每个节点对全局模型更新方向的贡献，高相似性意味着节点的梯度方向与全局梯度方向一致，这表明节点对全局模型更新有积极的贡献。而隐私预算占比考虑了节点在整体隐私保护中的份额，反映了节点在整体隐私保护策略中的重要性，有助于在不同节点之间公平地分配隐私预算。

算法3　隐私预算公平反馈算法

输入　边缘算力节点上传的模型参数$\boldsymbol{w}_i$，聚合后的全局模型参数$\boldsymbol{w}_g$，前一轮次隐私预算ε_i^t

输出　边缘算力节点的全局贡献度G_i^t

for $i = 1, \cdots, N$ **do**

计算$\boldsymbol{w}_i$与$\boldsymbol{w}_g$的模型参数相似度$A_i = \frac{\boldsymbol{w}_i \cdot \boldsymbol{w}_g}{\|\boldsymbol{w}_i\| \cdot \|\boldsymbol{w}_g\|}$；

计算隐私预算占比$P_i = \frac{\varepsilon_i^t}{\sum_{i=1}^{N} \varepsilon_i^t}$；

计算全局贡献度$G_i = \varphi \cdot A_i + (1 - \varphi) \cdot P_i$；

end for

输出全局贡献度集合$G = \{ G_i^t | i = 1, \cdots, N \}$；

3　理论分析

本节对FedCDP在拉普拉斯机制下的差分隐私需求和在非独立同分布数据下的模型收敛性能进行理论分析。

3.1　隐私性分析

本文通过自适应调整每个节点每一轮的隐私预算，更加合理地向模型梯度中加入噪声以保护模型隐私。为了证明FedCDP满足差分隐私，首先证明FedCDP中每个边缘算力节点的每个通信轮次内隐私预算是有界的（定理1）；然后，证明有界隐私预算的Laplace机制符合DP，且利用DP的序列组合定理可以推导出，如果每一轮都符合DP，那么整个FedCDP也符合DP（定理2）。

定理1　FedCDP中每个边缘算力节点的每个通信轮次内隐私预算ε是有界的。

证明　首先分析基础情况，对于$k = 0$，假设初始隐私预算ε_0是一个给定的正数，且是有限的。则基础情况下隐私预算是有限的。基于此，归纳假设如下，对于某个任意的$k = n$，隐私预算ε_n是有界的，即存在一个常数$M > 0$，使得$\varepsilon_n \leqslant M$。则须证明$k = n + 1$时，隐私预算$\varepsilon_{n+1}$也是有界的。

根据式(17)可知，$\varepsilon_i^{t+1} = \varepsilon_i^t \cdot [\rho \cdot \mathrm{Var}_i^{t+1} + (1 - \rho) \cdot G_i^{t+1}]$，其中，$\rho$是调整因子，满足$0 < \rho < 1$。Var是一个固定的下界，用于估计模型参数的方差。G是全局贡献度，也是一个有界的值。由于Var和G都是有界的，设$\mathrm{Var} = B$和$G = C$，且B和C是有限的正数。同时，由于$0 < \rho < 1$，定义新的常数$K = \rho \cdot B + (1 - \rho) \cdot C$，它也是有限且正的。基于上述分析对基础情况进行推广，使用归纳假设$\varepsilon_n \leqslant M$，可得$\varepsilon_{n+1} \leqslant M \cdot [\rho \cdot B + (1 - \rho) \cdot C] = K \cdot M$，由于$K$是有限正数，$M$是归纳假设中$\varepsilon_n$的上界，因此$K \cdot M$是有限正数，则$\varepsilon_{n+1}$是有界的。

证毕

定理2　FedCDP中每个边缘算力节点的每个通信轮次内都符合ε-差分隐私，且FedCDP整体上也符合ε-差分隐私。

证明　首先证明FedCDP中每个边缘算力节点的每个通信轮次内都符合ε-差分隐私。在定理1的基础上，可证得每一轮的隐私预算ε_k都有界（详见定理1），即存在一个正数$\varepsilon_{\max}$使得对于所有的k，$\varepsilon_k \leqslant \varepsilon_{\max}$。现需要证明对于任意的$k$，算法$F_k$（表示第$k$轮的算法）满足$\varepsilon_k$-差分隐私。根据Laplace噪声的性质，对于任意的t，可推导出式(13)和式(14)。因此，联合式(13)和式(14)，结合$\varepsilon_k \leqslant \varepsilon_{\max}$，可推导出式(15)。

$$\sigma = \frac{\Delta f}{\varepsilon_k} \tag{13}$$

$$\frac{P(\mathrm{Lap}(0, \sigma^2) \leqslant t)}{P(\mathrm{Lap}(0, \sigma^2) \leqslant t')} = \exp\left(- \frac{|t - t'|}{\sigma} \right) \tag{14}$$

$$\frac{P(\tilde{f}(D) \in S)}{P(\tilde{f}(D') \in S)} \leqslant \exp\left(\frac{\varepsilon_{\max} \| M(D) - M(D') \|}{\Delta f} \right) \tag{15}$$

鉴于敏感度 Δf 属于固定正数，因此可推导出式(16)，即表明对于任意 k，算法 F_k 满足 $\varepsilon_{\max}$-差分隐私。基于 $\varepsilon_{\max}$ 是有限正数，表明 FedCDP 每个通信轮次都符合 DP。

$$\frac{P(\tilde{f}(D)\in S)}{P(\tilde{f}(D')\in S)}\leqslant \exp(\varepsilon_{\max}) \tag{16}$$

下面继续证明整个 FedCDP 方案在 T 轮后仍然满足差分隐私。设每轮的隐私预算为 ε_k，其中，$k=1,2,\cdots,T$。使用序列组合定理，FedCDP 每个轮次都有自己的隐私预算 $\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_n$，那么整个机制在 T 轮后的总隐私预算 $\varepsilon_{\text{total}}$，如式(17)所示，其中，$\delta$ 是一个非常小的正数，用于处理总隐私损失超过 $\varepsilon_{\text{total}}$ 的极小概率。

$$\varepsilon_{\text{total}}=\ln\left(\frac{T}{\delta}\right)+\sum_{k=1}^{T}\varepsilon_k \tag{17}$$

由于每一轮的隐私预算 ε_k 都有界，即 $\varepsilon_k\leqslant\varepsilon_{\max}$ 对所有 k 成立，可以推导出式(18)。

$$\sum_{k=1}^{T}\varepsilon_k\leqslant T\cdot\varepsilon_{\max} \tag{18}$$

将上述不等式代入序列组合定理中，可推导出式(19)，为了简化计算，设定 $\delta=1/T$，则可推导出式(20)。

$$\varepsilon_{\text{total}}\leqslant\ln\left(\frac{T}{\delta}\right)+T\cdot\varepsilon_{\max} \tag{19}$$

$$\varepsilon_{\text{total}}\leqslant 2\ln(T)+T\cdot\varepsilon_{\max} \tag{20}$$

由于 $\varepsilon_{\text{total}}$ 是有限的，这意味着整个 FedCDP 在 T 轮后满足 $\varepsilon_{\text{total}}$-差分隐私。因此，在 FedCDP 中，只要每一轮都满足 DP，整体也满足 DP，且总隐私损失是有界的。

证毕

3.2　收敛性分析

为了证明所提 FedCDP 机制收敛，需要证明目标函数 f 的梯度在添加噪声后仍然能够引导算法向唯一解靠近。收敛性分析目标是证明算法能够在联邦学习的环境中稳定收敛，即随着迭代次数的增加，模型参数能够接近一个固定的解。在实际应用中，尤其是在分布式和隐私敏感的背景下，找到一个全局最优解并不总是必要的。相反，能够找到一个在给定隐私保护水平下提供满意性能的解，即是一个足够好的解，这通常是更加实际和重要的目标[46]。算法设计了隐私预算调整机制，以确保在保护用户隐私的同时实现模型的有效训练，这意味着在某些情况下会牺牲一部分性能以换取更高的隐私保护。接下来本文将分步骤详细解释并推导，使用巴拿赫不动点定理[47]来确立收敛性。

步骤 1　证明梯度符合 L-Lipschitz 连续性[48]。

在联邦学习训练过程中，交叉熵损失函数在训练过程中扮演着至关重要的角色。它衡量模型预测值与真实值之间的差距，并作为优化算法的目标函数，指导模型训练的方向。对于交叉熵损失函数，它在机器学习中被广泛用于分类问题。对于多分类问题，交叉熵损失函数计算如式(21)所示。其中，Z 是类别的总数，y_i 是真实标签的独热编码，p_i 是模型预测为第 i 类的概率。

$$f(y,p)=-\sum_{i=1}^{Z}y_i\lg(p_i) \tag{21}$$

要证明交叉熵损失函数满足 L-Lipschitz 连续性，需要证明其梯度满足 Lipschitz 连续性。为了简化分析，以二分类问题为例，交叉熵损失函数的梯度如式(22)所示。

$$\nabla_p f(y,p)=-\frac{y}{p}+\frac{1-y}{1-p} \tag{22}$$

该梯度是关于 p 的函数，需要证明存在一个常数 L，即 Lipschitz 常数，使得对于所有的 p 和 q 可以推导出式(23)。当 p 接近 0 或 1 时，即接近决策边界的区域，梯度变化非常快，这意味着交叉熵损失函数的梯度可能不满足 L-Lipschitz 连续性。

$$\left\|\frac{y}{p}-\frac{1-y}{1-p}-\left(\frac{y}{q}-\frac{1-y}{1-q}\right)\right\|\leqslant L\left|p-q\right| \tag{23}$$

本方案中梯度裁剪限制了梯度大小，确保了梯度向量的范数不会超过某个阈值 C。裁剪后的梯度 ∇W_i^t 表示为式(24)。为了证明裁剪后的梯度满足 Lipschitz 连续性，需要证明对于任意的 x 和 y 满足式(25)。

$$\nabla W_i^t=\begin{cases}\nabla W_i^t, & \left\|\nabla W_i^t\right\|\leqslant C\\ \dfrac{C}{\left\|\nabla W_i^t\right\|}\nabla W_i^t, & \left\|\nabla W_i^t\right\|>C\end{cases} \tag{24}$$

$$\left\|\nabla W_i^t(x)-\nabla W_i^t(y)\right\|\leqslant L\left\|x-y\right\| \tag{25}$$

由于梯度裁剪限制了梯度的最大值，可以选择 L 等于裁剪阈值 C，这样对于任意的 x 和 y，裁剪后的梯度变化量都不会超过 C，从而满足 Lipschitz 连续性的条件。

步骤 2　巴拿赫不动点定理证明梯度收敛性。

在联邦算力物联网中，参数更新通常由梯度下降步骤定义，如式(26)所示。

$$\boldsymbol{w}_{n+1} = T(\boldsymbol{w}_n) = \boldsymbol{w}_n - \eta \nabla f(\boldsymbol{w}_n) \tag{26}$$

其中，$\boldsymbol{w}_n$是第n轮模型参数，η是学习率，$\nabla f(\boldsymbol{w}_n)$是目标函数$f$在$\boldsymbol{w}_n$处的梯度。

为了应用巴拿赫不动点定理，需要证明映射T是一个压缩映射。这意味着存在一个常数$0 \leqslant c < 1$使得对于所有$\boldsymbol{w}_1$和$\boldsymbol{w}_2$满足式(27)。

$$\| T(\boldsymbol{w}_1) - T(\boldsymbol{w}_2) \| \leqslant c \| \boldsymbol{w}_1 - \boldsymbol{w}_2 \| \tag{27}$$

利用梯度L-Lipschitz的性质，可得式(28)。

$$\| \nabla f(\boldsymbol{w}_1) - \nabla f(\boldsymbol{w}_2) \| \leqslant L \| \boldsymbol{w}_1 - \boldsymbol{w}_2 \| \tag{28}$$

将式(28)代入T定义，能够得到$\| T(\boldsymbol{w}_1) - T(\boldsymbol{w}_2) \| = \| \eta(\nabla f(\boldsymbol{w}_1) - \nabla f(\boldsymbol{w}_2)) \| \leqslant \eta L \| \boldsymbol{w}_1 - \boldsymbol{w}_2 \|$，选择学习率$\eta$使得$0 < \eta < 1/L$，确保$c = \eta L < 1$。因此，$T$是压缩映射。进而，根据巴拿赫不动点定理，存在唯一不动点$\boldsymbol{w}^*$使$T(\boldsymbol{w}^*) = \boldsymbol{w}^*$。这意味着对于任意初始点$\boldsymbol{w}_0$，迭代序列$\{\boldsymbol{w}_n\}$将收敛到$\boldsymbol{w}^*$。

4　实验评估

4.1　实验设置

4.1.1　实验环境

本文的实验环境分为硬件环境和软件环境。硬件环境包括CPU（Xeon CPU E5-2650 v4 @ 2.20 GHz）、GPU（NVIDIA GeForce RTX 2080型号）、内存（128 GB）。软件环境包括操作系统（Ubuntu 20.04版本）、Python语言（3.11.1版本）、Pytorch平台（2.2.0版本）和实验数据集，其中，实验数据集基于联邦学习中广泛采用的MNIST[49]和CIFAR10[49]数据集，以模拟联邦算力物联网中边缘算力节点的本地隐私数据。MNIST数据集由10个类共70 000张灰度图像组成，包含60 000个训练样本和10 000个测试样本。CIFAR10数据集由10个类共60 000张彩色图像组成，包含50 000个训练样本和10 000个测试样本。

4.1.2　参数设置

深度学习参数设置。依据常用参数设置[49]，边缘算力节点（即客户端）数量为100，全局通信轮次为200，本地训练周期为5，批处理大小为128，学习率为0.1，动量为0.9。

Non-IID数据设置。为了模拟联邦算力物联网中数据异构分布，本文基于狄利克雷分布[48]为各边缘算力节点随机分配不同大小的本地数据集和标签数量，确保每个边缘算力节点数据都具有较强的数据统计异质性以满足Non-IID。本文将狄利克雷分布值参数设置为0.1，为模型训练提供更为复杂的条件。

神经网络模型设置。对于MNIST数据集，使用两个5 × 5卷积层、一个全连接层和一个softmax输出层的4层CNN神经网络进行训练，并将梯度裁剪阈值设置为0.2。对于CIFAR10，使用两个5 × 5卷积层、两个全连接层和一个softmax输出层的5层CNN神经网络，并将梯度裁剪阈值设置为0.1。

超参数设置。在当前实验设置下，模型性能达到最优时超参数设置为，对于MNIST数据集，初始隐私预算设置为10，调整因子设置为0.4，裁剪阈值设置为0.2，对于CIFAR10数据集，初始隐私预算设置为15，调整因子设置为0.4，裁剪阈值设置为0.1。第4.3节将对最优超参数取值对模型性能影响的实验进行详细分析。

4.1.3　对比方案

本文方案与现有的FedAvg[26]、FedProx[50]、DP-FedAvg[51]和DP-FedADMM[25]方法进行对比测试。FedAvg是联邦学习领域内最早被提出的方法，作为一种基线方法，主要思想是服务器和各个参与方协同训练一个全局共享模型。FedProx是在FedAvg算法上的优化算法，用于处理数据在不同客户端之间可能存在的不均匀分布的问题，但这两种方法都没有考虑隐私噪声。DP-FedAVG的核心思想是在每个参与方本地计算梯度时，对梯度进行随机扰动以增加噪声，防止恶意参与方根据梯度信息推断出其他参与方的数据。而DP-FedADMM进一步提出了一种新型基于交替方向乘子法的DP联邦学习算法，主要思想是联合考虑梯度二范式、训练损失、模型准确率和时间因素的评分函数，用于实现噪声的自适应添加。

4.2　实验结果

为了验证在Non-IID数据下FedCDP的有效性，本文将FedCDP与FedAvg、FedProx进行实验对比，同时，在初始隐私预算相同（MNIST设置为10，CIFAR10设置为15）的情况下与DP-FedAvg、DP-FedADMM进行实验比较。

4.2.1　全局模型准确率

MNIST数据集上全局模型准确率如图4所示，CIFAR10数据集上全局模型准确率如图5所示。

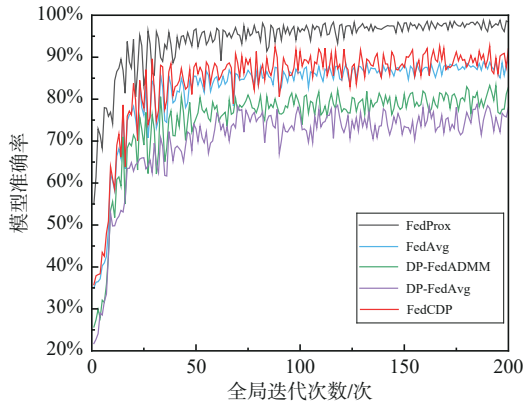

图4　MNIST数据集上全局模型准确率

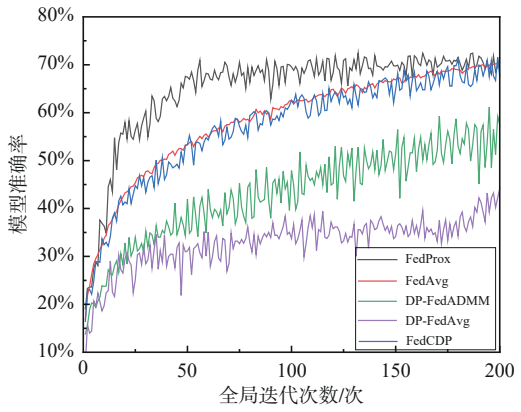

图5　CIFAR10数据集上全局模型准确率

从图4可以看出，在MNIST数据集上，FedProx和FedAvg的全局准确率分别达到了98.41%和89.41%，当初始隐私预算为10时，DP-FedAvg和DP-FedADMM的全局模型准确率分别达到了72.76%和82.81%，而本文所提的FedCDP的全局模型准确率达到了92.01%。从图5可以看出，在CIFAR10数据集上，FedProx和FedAvg的全局准确率分别达到了71.48%和70.45%，当初始隐私预算为15时，DP-FedAvg和DP-FedADMM的全局模型准确率分别达到了44.24%和57.46%，而本文所提的FedCDP的全局模型准确率达到了67.65%。由此可知，FedCDP的全局模型准确率低于FedProx，但与FedAvg的全局模型准确率是较为接近的，因为数据集规模或Non-IID具体数据环境不同的情况下，模型的全局准确率有所波动。FedCDP相比于DP-FedAvg和DP-FedADMM的全局模型准确率都有较高提升，说明FedCDP算法通过结合CRLB全局贡献度的自适应隐私预算分配机制，有利于模型在保护隐私的同时有效地利用每个节点的数据，从而提高模型的准确率。

4.2.2　损失函数值

MNIST数据集上的损失函数值如图6所示，CIFAR10数据集上的损失函数值如图7所示。

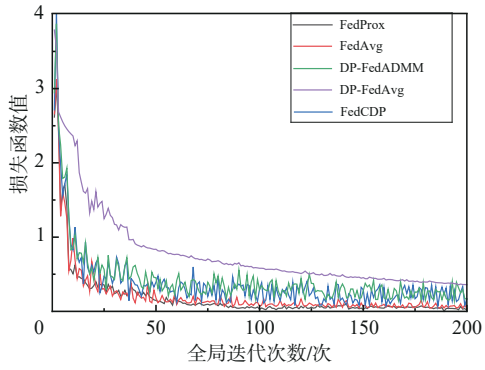

图6　MNIST数据集上的损失函数值

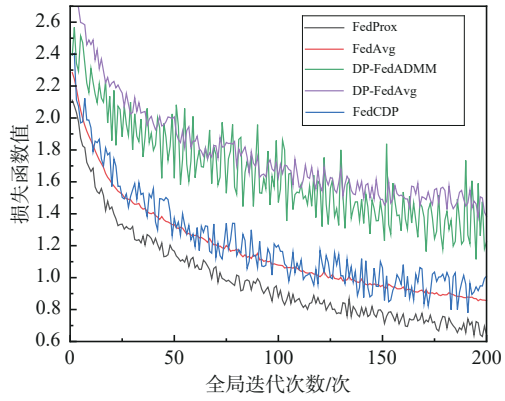

图7　CIFAR10数据集上的损失函数值

从图6可以看出，在MNIST数据集上，FedProx和FedAvg的损失函数值分别达到了0.016 5和0.038 3，当初始隐私预算为10时，DP-FedAvg和DP-FedADMM的损失函数值分别达到了0.358 6和0.172 5，而本文所提的FedCDP的损失函数值达到了0.153 0。从图7可以看出，在CIFAR10数据集上，FedProx和FedAvg的损失函数值分别达到了0.640 2和0.856 0，当初始隐私预算为15时，DP-FedAvg和DP-FedADMM的损失函数值分别达到了1.224 4和1.384 0，而本文所提的FedCDP的损失函数值达到了1.009 0。由此可见，FedCDP相比于FedProx和FedAvg的损失函数值略大，因为FedCDP加入了DP机制，通常会引入额外的噪声到模型更新中，会干扰模型的训练过程，导致损失函数值增加。而FedCDP相比于DP-FedAvg和DP-FedADMM的损失函数值略小，是因为FedCDP引入隐私预算自适应机制，降低了隐私保护对模型性

能的影响，从而降低了损失函数值，实现了模型效能提升的目标。

4.3　参数分析

4.3.1　初始隐私预算ε

DP应用于联邦算力物联网时，必须考虑隐私预算与模型准确率之间的平衡性，为使模型准确率和隐私保护取得最佳水平，在MNIST数据集上，ε为3、5、10和15时进行实验，在CIFAR10数据集上，ε为10、15、20和30时进行实验。MNIST数据集上初始隐私预算对模型准确率和损失函数值的影响如图8所示，CIFAR10数据集上初始隐私预算对模型准确率和损失函数值的影响如图9所示。

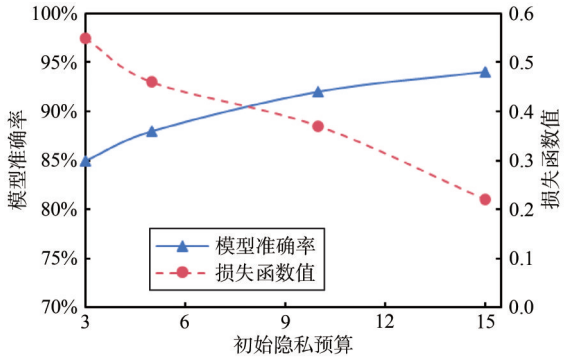

图8　MNIST数据集上初始隐私预算对模型准确率和损失函数值的影响

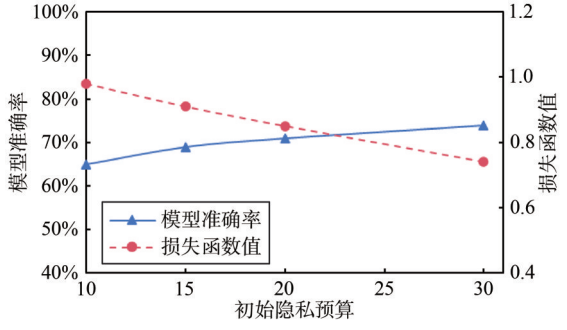

图9　CIFAR10数据集上初始隐私预算对模型准确率和损失函数值的影响

由图8和图9可知，随着初始隐私预算值变大，FedCDP中模型准确率也随之增加，损失函数值随之减少，即隐私预算越小，隐私保护越强，但模型准确率越低，损失函数值越高；隐私预算越大，模型准确率得到提高，损失函数值变低，但隐私保护变弱。

4.3.2　调整因子ρ

在方案总体框架的式(7)中，调整因子ρ通过调节CRLB隐私预算估计值和全局贡献度之间的比例，控制隐私预算的增加或减少。MNIST数据集上调整因子对模型准确率和损失函数值的影响如图10所示，CIFAR10数据集上调整因子对模型准确率和损失函数值的影响如图11所示。

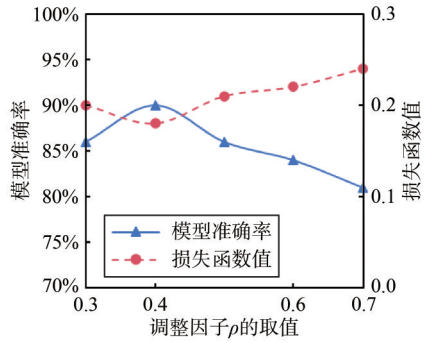

图10　MNIST数据集上调整因子对模型准确率和损失函数值的影响

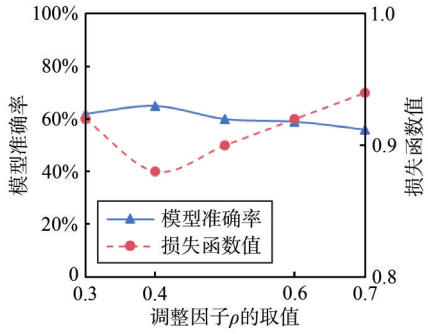

图11　CIFAR10数据集上调整因子对模型准确率和损失函数值的影响

4.3.3　裁剪阈值C

为了限制训练中对梯度所加噪声的敏感度大小，需要保证梯度有界，因此通常要对梯度进行裁剪，而裁剪阈值是梯度裁剪中最重要的超参数。裁剪阈值过大会导致所需噪声量过高，裁剪阈值过小会导致裁剪梯度造成的精度损失过高。裁剪阈值设置过大或过小，均会影响用户上传的梯度的真实有效性，使其无法达到足够的精度。

在MNIST数据集上，当裁剪阈值为0.01、0.05、0.10、0.15和0.20时进行实验，在CIFAR10数据集上，当裁剪阈值为0.01、0.03、0.05、0.07和0.10时进行实验。MNIST数据集上裁剪阈值对模型准确率和损失函数值的影响如图12所示，CIFAR10数据集上裁剪阈值对模型准确率和损失函数值的影响如图13所示。由图12和图13可知，随着裁剪阈值变大，FedCDP中模型准确率也随之先增

加后减少，损失函数值随之先减少后增加，因为在裁剪阈值较低时，适度的梯度裁剪有助于抑制梯度爆炸，提高模型的稳定性，因此准确率有所提高。但是当裁剪阈值过高时，会导致过多的梯度信息被裁剪掉，模型无法有效学习，导致准确率下降。

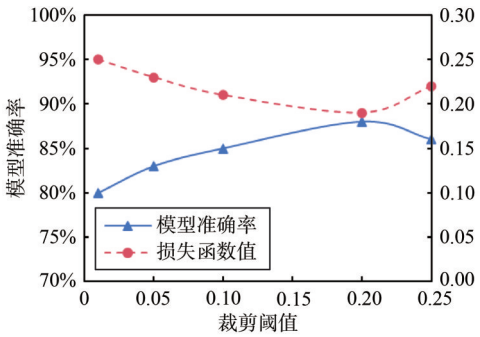

图 12　MNIST 数据集上裁剪阈值对模型准确率和损失函数值的影响

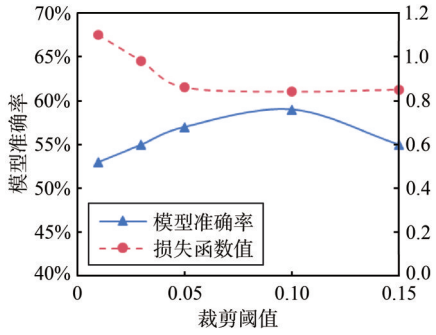

图 13　CIFAR10 数据集上裁剪阈值对模型准确率和损失函数值的影响

5　结束语

针对现有基于 DP 的联邦算力物联网未充分考虑本地节点数据特性和隐私预算分配公正性所导致的模型精度下降的问题，本文提出了一种隐私预算自适应优化方案 FedCDP。首先利用 Fisher 信息矩阵和 CRLB 理论估算边缘算力节点的隐私预算，以实现隐私预算的自适应规划。同时，通过比较边缘算力节点上传的模型与算力聚合服务器中聚合模型之间的相似性及隐私预算占比，评估每个节点的全局贡献度，并据此公平且实时地调整隐私预算分配。理论分析了该方案的隐私性和全局收敛性，实验结果表明，在满足 DP 要求的同时，该方案能够有效平衡模型的隐私保护和准确度。

本文提出的 FedCDP 方案虽然在满足相同隐私保护需求的前提下，全局模型精确度提升成效显著，但也不可避免地带来了 DP 自适应优化过程的额外计算成本。在实际应用中，这一成本会显著影响算法的实施可行性。因此，对算法的计算复杂度和开销进行精确量化显得尤为重要。当前研究尚未深入探讨这一方面，未来工作将重点关注此问题，旨在全面评估算法在现实世界应用中的性能表现，以便更全面地评估 FedCDP 方案在现实场景中的性能表现和适用性。

参考文献：

[1] 王永江, 孙文静, 张凌, 等. 物联网环境下的边缘算力部署研究[J]. 智能物联技术, 2024, 7(5): 149-152.
WANG Y J, SUN W J, ZHANG L, et al. Research on edge computing deployment in the Internet of things environment[J]. Technology of IoT & AI, 2024, 7(5): 149-152.

[2] 陈心瑜, 阮凯斌. 基于物联网节点算力性能优化分析[J]. 新型工业化, 2021, 11(2): 7-9, 13.
CHEN X Y, RUAN K B. Optimization analysis of computing performance based on Internet of things nodes[J]. The Journal of New Industrialization, 2021, 11(2): 7-9, 13.

[3] 王志良, 何刚, 俞文心, 等. 边缘场景下动态联邦学习优化方法[J]. 计算机技术与发展, 2024, 34(2): 98-104.
WANG Z L, HE G, YU W X, et al. Dynamic federated learning optimization method in edge scenarios[J]. Computer Technology and Development, 2024, 34(2): 98-104.

[4] 程帆, 王瑞锦, 张凤荔. 边缘场景下动态权重的联邦学习优化方法[J]. 计算机科学, 2022, 49(12): 53-58.
CHENG F, WANG R J, ZHANG F L. Federated learning optimization method for dynamic weights in edge scenarios[J]. Computer Science, 2022, 49(12): 53-58.

[5] 胡卓尔. 基于边缘智能学习的安全可信物联网研究[D]. 北京: 北京邮电大学, 2022.
HU Z E. Research on secure and trusted Internet of things based on edge intelligent learning[D]. Beijing: Beijing University of Posts and Telecommunications, 2022.

[6] 涂晓儒, 刘子威, 张更新. 基于语义通信的卫星物联网边缘计算架构[J]. 通信技术, 2024, 57(7): 680-687.
TU X R, LIU Z W, ZHANG G X. Edge computing architecture of satellite IoT based on semantic communication[J]. Communications Technology, 2024, 57(7): 680-687.

[7] 岑伯维. 基于云原生的电力物联网边缘计算模型与方法[D]. 广州: 华南理工大学, 2023.
CEN B W. Cloud native-based edge computing model and method for power Internet of things[D]. Guangzhou: South China University of Technology, 2023.

[8] WU Q, WANG X B, FAN P Y, et al. Vehicle selection for C-V2X mode 4 based federated edge learning systems[J]. arXiv preprint, 2024, arXiv: 2401.07224.

[9] FREDRIKSON M, JHA S, RISTENPART T. Model inversion attacks that exploit confidence information and basic countermeasures[C]//Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2015: 1322-1333.

[10] ZHU L, LIU Z, HAN S. Deep leakage from gradients[C]//Proceedings of the Advances in Neural Information Processing Systems 32: Annual Conference on Neural Information Processing Systems 2019, Piscataway : IEEE , 2019:14747-14756.

[11] 中国移动通信集团有限公司．算力网络技术白皮书[R]. 2022.
China Mobile Communications Group Co.,Ltd.. Computing force network technology whitepaper[R]. 2022.

[12] 李铭轩, 曹畅, 唐雄燕, 等. 面向算力网络的边缘资源调度解决方案研究[J]. 数据与计算发展前沿, 2020, 2(4): 80-91.
LI M X, CAO C, TANG X Y, et al. Research on edge resource scheduling solutions for computing power network[J]. Frontiers of Data & Computing, 2020, 2(4): 80-91.

[13] YAO P, WANG H, ZHENG C, et al. Efficient federated learning aggregation protocol using approximate homomorphic encryption[C]//Proceedings of the 2023 26th International Conference on Computer Supported Cooperative Work in Design (CSCWD). Piscataway: IEEE Press, 2023: 1884-1889.

[14] YIN L H, FENG J Y, XUN H, et al. A privacy-preserving federated learning for multiparty data sharing in social IoTs[J]. IEEE Transactions on Network Science and Engineering, 2021, 8(3): 2706-2718.

[15] 徐茹枝, 戴理朋, 夏迪娅, 等. 基于联邦学习的中心化差分隐私保护算法研究[J]. 信息网络安全, 2024, 24(1): 69-79.
XU R Z, DAI L P, XIA D Y, et al. Research on centralized differential privacy algorithm for federated learning[J]. Netinfo Security, 2024, 24(1): 69-79.

[16] CHEN Q, WANG Z L, CHEN J W, et al. Dap-FL: federated learning flourishes by adaptive tuning and secure aggregation[J]. IEEE Transactions on Parallel and Distributed Systems, 2023, 34(6): 1923-1941.

[17] WEI K, LI J, DING M, et al. Federated learning with differential privacy: algorithms and performance analysis[J]. IEEE Transactions on Information Forensics and Security, 2020, 15: 3454-3469.

[18] CHENG S Y, LI P, WANG R C, et al. Differentially private federated learning with non-IID data[J]. Computing, 2024, 106(7): 2459-2488.

[19] 唐钰慧. 针对联邦学习中梯度泄露攻击的改进方法[J]. 信息技术与信息化, 2023(9): 56-59.
TANG Y H. An improved method for gradient leakage attack in federated learning[J]. Information Technology and Informatization, 2023(9): 56-59.

[20] 马卓然. 隐私保护的联邦学习关键技术研究[D]. 西安: 西安电子科技大学, 2022.
MA Z R. Research on key technologies of federated learning for privacy protection[D]. Xi'an: Xidian University, 2022.

[21] MCMAHAN H B, MOORE E, RAMAGE D, et al. Communication-efficient learning of deep networks from decentralized data[J]. arXiv preprint, 2016, arXiv: 1602.05629.

[22] BI M H, YAN C H, LIN R, et al. Client scheduling and bandwidth slicing for multiple federated learning tasks over multiple passive optical networks[J]. Computer Networks, 2024, 243: 110309.

[23] HESSEL M, SOYER H, ESPEHOLT L, et al. Multi-task deep reinforcement learning with PopArt[J]. Proceedings of the AAAI Conference on Artificial Intelligence, 2019, 33(1): 3796-3803.

[24] TU J F, HUANG J M, YANG L, et al. Personalized federated learning with layer-wise feature transformation via meta-learning[J]. ACM Transactions on Knowledge Discovery from Data, 2023, 18: 1-21.

[25] 汤东汰. 基于差分隐私的联邦学习算法优化研究[D]. 西安: 西安理工大学, 2023.
TANG D T. Research on optimization of federated learning algorithm based on differential privacy[D]. Xi'an: Xi'an University of Technology, 2023.

[26] SU L, XU J, YANG P. A non-parametric view of FedAvg and FedProx: beyond stationary points[J]. The Journal of Machine Learning Research, 2024, 24(1): 9713-9760.

[27] 张兰, 程一航, 李向阳. 提升联邦学习在Non-IID和Mismatched场景下性能的方法: CN113379067A[P]. 2021.
ZHANG L, CHENG Y H, LI X Y. Method for improving federated learning performance in Non-IID and mismatched scenarios. CN patent, CN113379067A[P]. 2021-09-10.

[28] 侯铭楷. 面向数据和系统异构的高效联邦学习算法研究[D]. 长春: 吉林大学, 2023.
HOU M K. Research on efficient federated learning algorithm for heterogeneous data and systems[D]. Changchun: Jilin University, 2023.

[29] LIANG P P, LIU T, LIU Z Y, et al. Think locally, act globally: federated learning with local and global representations[J]. arXiv preprint, 2020, arXiv: 2001.01523.

[30] ARIVAZHAGAN M G, AGGARWAL V, SINGH A K, et al. Federated learning with personalization layers[J]. arXiv preprint, 2019, arXiv: 1912.00818.

[31] WU Q, WANG W H, FAN P Y, et al. Cooperative edge caching based on elastic federated and multi-agent deep reinforcement learning in next-generation networks[J]. IEEE Transactions on Network and Service Management, 2024, 21(4): 4179-4196.

[32] DEBADITYA S, OMER W, ULLAH K W. Federated learning and next generation wireless communications: a survey on bidirectional relationship[J]. Transactions on Emerging Telecommunications Technologies, 2022, 33(7): e4458.

[33] XIE Y A, KANG J W, NIYATO D, et al. Securing federated learn-

ing: a covert communication-based approach[J]. IEEE Network, 2023, 37(1): 118-124.

[34] 宋祺鹏, 王继东, 张丽伟, 等. 本地化差分隐私下的电力物联网终端数据隐私保护方法[J]. 重庆邮电大学学报(自然科学版), 2023, 35(6): 1001-1010.
SONG Q P, WANG J D, ZHANG L W, et al. Terminal data privacy protection method for power Internet of things based on localized differential privacy[J]. Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition), 2023, 35(6): 1001-1010.

[35] KHAN L U, PANDEY S R, TRAN N H, et al. Federated learning for edge networks: resource optimization and incentive mechanism[J]. IEEE Communications Magazine, 2020, 58(10): 88-93.

[36] 王鑫, 李美庆, 王黎明, 等. 一种基于合同理论的可激励联邦学习模型[J]. 电子与信息学报, 2023, 45(3): 874-883.
WANG X, LI M Q, WANG L M, et al. An incentivized federated learning model based on contract theory[J]. Journal of Electronics & Information Technology, 2023, 45(3): 874-883.

[37] LIU W, ZHANG Y H, HAN G, et al. Secure and efficient smart healthcare system based on federated learning[J]. International Journal of Intelligent Systems, 2023, 2023: 8017489.

[38] 刘洋. 工业物联网环境下支持数据共享的联邦学习方法研究[D]. 南宁：广西大学，2024.
LIU Y. Research on federated learning method supporting data sharing in industrial Internet of things environment[D]. Nanning: Guangxi University, 2024.

[39] LUO T, PAN M, THOLONIAT P, et al. Privacy budget scheduling[C]// The 15th USENIX Symposium on Operating Systems Design and Implementation. Virtual Event, 2021: 55-74.

[40] LIU Y, WANG Z B, ZHU Y F, et al. DPBalance: efficient and fair privacy budget scheduling for federated learning as a service[C]// Proceedings of the IEEE INFOCOM 2024-IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2024: 21-30.

[41] THOLONIAT P, KOSTOPOULOU K, MCNEELY P, et al. Cookie monster: efficient on-device budgeting for differentially-private ad-measurement systems[J]. arXiv Preprint, 2024, arXiv: 2405.16719.

[42] PELEG S, PORAT B. The Cramer-Rao lower bound for signals with constant amplitude and polynomial phase[J]. IEEE Transactions on Signal Processing, 1991, 39(3): 749-752.

[43] 李洪涛, 任晓宇, 王洁, 等. 基于差分隐私的连续位置隐私保护机制[J]. 通信学报, 2021, 42(8): 164-175.
LI H T, REN X Y, WANG J, et al. Continuous location privacy protection mechanism based on differential privacy[J]. Journal on Communications, 2021, 42(8): 164-175.

[44] 周赞, 张笑燕, 杨树杰, 等. 面向联邦算力网络的隐私计算自适激励机制[J]. 计算机学报, 2023, 46(12): 2705-2725.
ZHOU Z, ZHANG X Y, YANG S J, et al. Adaptive incentive mechanism for privacy computing in federated compute first networks[J]. Chinese Journal of Computers, 2023, 46(12): 2705-2725.

[45] 陈谦, 柴政, 王子龙, 等. 基于生成对抗网络的联邦学习中投毒攻击检测方案[J]. 计算机应用, 2023, 43(12): 3790-3798.
CHEN Q, CHAI Z, WANG Z L, et al. Poisoning attack detection scheme based on generative adversarial network for federated learning[J]. Journal of Computer Applications, 2023, 43(12): 3790-3798.

[46] LI X, HUANG K, YANG W, et al. On the convergence of FedAvg on Non-IID data[C]//Proceedings of 8th International Conference on Learning Representations. Washington DC: ICLR, 2020.

[47] 邓志颖, 潘建辉. 巴拿赫不动点定理及其应用[J]. 高等数学研究, 2013, 16(4): 78-80, 92.
DENG Z Y, PAN J H. Banach fixed point theorem and its applications[J]. Studies in College Mathematics, 2013, 16(4): 78-80, 92.

[48] 谷峰. 两个有限族一致L-Lipschitz映象的平行迭代算法的强收敛定理[J]. 数学学报, 2010, 53(6): 1209-1216.
GU F. Strong convergence theorems of a parallel iterative algorithm for two finite families of uniformly L-Lipschitzian mappings[J]. Acta Mathematica Sinica, 2010, 53(6): 1209-1216.

[49] 张少波，张激勇，朱更明，等. 基于Bregman散度和差分隐私的个性化联邦学习方法[J]. 软件学报, 2024, 35(11): 5249-5262.
ZHANG S B, ZHANG J Y, ZHU G M, et al. Personalized federated learning method based on Bregman divergence and differential privacy[J]. Journal of Software, 2024, 35(11): 5249-5262.

[50] LI T, SAHU A K, ZAHEER M, et al. Federated optimization in heterogeneous networks[C]//Proceedings of the Third Conference on Machine Learning and Systems. TX, USA: MLSys, 2020.

[51] ABADI M, CHU A, GOODFELLOW I, et al. Deep learning with differential privacy[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2016: 308-318.

[作者简介]

马文玉（2001– ），女，信息工程大学博士生，主要研究方向为联邦学习、物联网安全。

陈谦（1993– ），男，博士，西安电子科技大学，菁英副教授，主要研究方向为联邦学习、应用密码学、人工智能安全。

胡宇翔（1982– ），男，博士，信息工程大学教授，主要研究方向为新型网络体系架构、网络通信安全。

胡涛（1993– ），男，博士，信息工程大学助理研究员，主要研究方向为新型网络体系、网络主动防御。

闫皓楠（1996– ），男，西安电子科技大学博士生，主要研究方向为可信人工智能、隐私计算。

伊鹏（1977– ），男，博士，信息工程大学研究员，信息技术研究所所长，主要研究方向为多模态网络架构、网络内生安全。