DOI：10.13334/j.0258-8013.pcsee.241994 文章编号：0258-8013 (2026) 03-0942-15 中图分类号：TM 74 文献标识码：A

配电网量测数据动态联邦学习框架、自适应隐私保护模型和边缘侧贡献度评估

王路遥[1]，龚钢军[1]，陆俊[1]，杨佳轩[1*]，杨超[2]，刘礼[1]，强仁[1]

(1. 北京市能源电力信息安全工程技术研究中心(华北电力大学)，北京市 昌平区 102206;
2. 国网辽宁省电力有限公司，辽宁省 沈阳市 110004)

Dynamic Federated Learning Framework, Adaptive Privacy Protection Model and Edge-side Contribution Assessment for Distribution Network Measurement Data

WANG Luyao[1], GONG Gangjun[1], LU Jun[1], YANG Jiaxuan[1*], YANG Chao[2], LIU Li[1], QIANG Ren[1]

(1. Beijing Engineering Research Center of Energy Electric Power Information Security
(North China Electric Power University), Changping District, Beijing 102206, China;
2. State Grid Liaoning Electric Power Co., Ltd., Shenyang 110004, Liaoning Province, China)

ABSTRACT: Measurement data, as a crucial operational element for all stakeholders in distribution network management and a cornerstone asset for enterprises, exhibit diverse characteristics such as varying privacy protection requirements among stakeholders and heterogeneous forms of datasets. These characteristics significantly constrain the empowerment potential of measurement data. Federated learning has garnered widespread attention for its ability to address data silo issues. However, traditional federated learning frameworks are plagued by inadequate privacy protection for participant data, decreased model performance due to data heterogeneity, and a lack of effective incentive mechanisms. To tackle these issues, the adaptive privacy-protected dynamic federated learning framework (AP-DFL) is proposed. First, considering the different emphasis of privacy protection for different load types, the sensitivity of the dataset is defined from the two-dimensional perspectives of anonymity and confidentiality. On this basis, the privacy budget for each round of training on the edge side is dynamically adjusted to achieve adaptive local differential perturbation. Then, combined with the global differential perturbation on the main station side, privacy attacks are effectively avoided. Next, a participant contribution assessment model based on matrix decomposition Shapley values is proposed. This model efficiently calculates contribution values through the reconstructed method of value matrix decomposition under sampling. The aggregation weights are adaptively adjusted based on the contribution values to achieve dynamic federated aggregation, thus enhancing the convergence speed of the model under data heterogeneity. Finally, experimental analysis is conducted on this federated learning framework in typical distribution network scenarios, demonstrating its feasibility.

KEY WORDS: federated learning; differential privacy; Shapley value; matrix factorization; measurement data

摘要：量测数据作为配电网运行重要生产要素和企业核心数据资产，具有各参与方隐私保护诉求不同、数据集异构形态多等特征，极大限制了量测数据价值的赋能空间。联邦学习因能解决数据孤岛问题而被广泛关注，但传统联邦学习框架存在参与方数据隐私保护不足、数据异构异质导致模型性能下降和缺乏有效激励机制等问题。为此，提出自适应隐私保护的配电网动态联邦学习框架(adaptive privacy-protected dynamic federated learning framework，AP-DFL)。首先，考虑到不同负荷类型隐私保护的侧重点不同，从匿名性和机密性的二维角度定义数据集敏感度，基于此动态调整边缘侧每轮训练的隐私预算，实现自适应本地差分扰动，在此基础上结合站侧的全局差分扰动，有效避免了隐私攻击；其次，提出基于矩阵分解 Shapley 值的参与方贡献度评估模型，通过采样下的价值矩阵分解重构法高效求解贡献度值，根据贡献度自适应调节聚合权重以实现动态联邦聚合，提高数据异构下的模型性能；最后，通过对此联邦学习框架在配电网典型业务上进行实验分析，证明框架的可行性。

关键词：联邦学习；差分隐私；Shapley 值；矩阵分解；量测数据

0 引言

当前，数据作为新型生产要素的重要性已得到

基金项目：国家重点研发计划项目(2022YFB3105100)。
National Key R&D Program of China (2022YFB3105100).

广泛共识[1]，国家陆续出台的《数据安全法》《关键信息基础设施保护条例》等法律法规均对其提出了明确的保护要求[2]。电力系统作为国家的关键基础设施，重要电力数据已经纳入关键信息基础设施范畴。但数据要素具有可复制性等核心属性，致使数据要素价值的释放与应用面临数据安全与隐私保护的考验[3]。量测数据作为确保配电网稳定运行的关键元素，为配网业务应用提供重要支撑[4-7]，具有较高的要素价值[8]。因此，如何在兼顾配电网量测数据隐私安全的前提下发挥其要素价值是当前配电网的重要研究方向之一[9]。联邦学习(federated learning，FL)作为数据要素安全流通的关键技术之一[10]，因其“原始数据不出域，数据可用不可见”的特性在电力行业受到越来越多的关注及应用[11]。

一方面，安全性和隐私保护是联邦学习的核心问题[12]，但研究发现联邦学习架构依然存在隐私泄露风险[13]，攻击者可以通过模型参数(或梯度)来还原部分的敏感信息[14]。目前，主流的 FL 隐私保护研究方法是将经典的机器学习隐私保护技术融入 FL 中[15-16]。相比于同态加密、秘密共享等传统密码学技术，差分隐私(differential privacy，DP)因其强大的信息理论保障、简单灵活且易于部署的算法及相对较少的系统开销[17]，更适合作为算力薄弱的边缘侧隐私保护方法。目前，大多数基于 DP 的 FL 研究工作都采用固定敏感度以及噪声尺度的方式[18-19]，在一定程度上提供 DP 保证。然而，配电网中各台区的负荷类型和数据分布具有显著差异，其隐私保护需求也因此有所不同。统一的噪声注入方式无法有效满足多样化的隐私保护需求，往往导致隐私预算的浪费。文献[20]提出了一种两阶段的基于个性化差分隐私的联邦学习(federated learning with personalized differential privacy，PDP-FL)算法，根据用户的主观隐私偏好实现个性化隐私保护；文献[21]提出了一种新的兼顾通信效率与效用的自适应高斯差分隐私个性化联邦学习方法；文献[22]提出了个性化隐私保护的异步联邦窃电检测方法，结合异步联邦训练方式和个性化差分隐私机制，平衡参与方个性化隐私保护需求与模型性能。以上研究主要通过影响不同轮次或不同参与方间的加扰程度来实现隐私保护的优化，尚未从隐私保护侧重点的角度来量化参与方本地数据的隐私保护需求。

另一方面，配电网台区数据质量不平衡、分布呈现异构性，边缘侧通信资源有限且防护能力薄弱，易受到数据篡改、数据注入等恶意攻击。在联邦学习实践中难以保证所有台区均能提供高价值和无恶意的数据。为保证联邦模型性能，抵御恶意参与方攻击是联邦学习的一个重要研究议题[23]。文献[24]通过多权重动态评估方法来计算单轮模型和参与方评估值，以此作为参与方贡献的依据，确保激励机制的公平性；文献[25]提出改进 FedAvg 算法的 FedF1，通过基于本地测试模型打分和数据量来动态调整聚合权重；文献[26]提出了一种非可信中心服务器下动态聚合权重的隐私保护联邦学习框架(differentially private-dynamic federated learning，DP-DFL)，通过从不同参与方的数据中直接学习模型聚合权重实现动态聚合。以上研究主要是采用个体法[27]的方式来衡量参与方的贡献度以实现动态聚合，未考虑参与方个体为联邦集体的价值增益。文献[28]提出了基于 Shapley 值的能量-调频联合市场竞价模型，实现市场成员效益合理分配；文献[29]从可解释人工智能的角度研究合作多代理强化学习环境中代理贡献度评估方法，进行效益的公平分配；文献[30]发现联邦学习中用户参与顺序与其贡献度存在相关性，提出了面向用户参与顺序的 Shapley 值计算方法。以上研究主要通过博弈的方式实现效益或权重分配，但对计算过程导致的维数灾难问题涉及较少。

本文面向配电网台区量测数据赋能赋效价值空间需求，从配电网量测数据的动态联邦学习、自适应隐私保护和边缘侧贡献度评估 3 个方面开展研究，提出自适应隐私保护的配电网动态联邦学习框架，并在中国北方某地区实际配电线路异物识别图像数据和配网窃电检测数据上进行试验，结果表明所提框架在较好保护数据隐私的同时，可提高模型的性能。论文主要贡献如下：

1）针对差分隐私统一性加扰方式难以满足配电网台区差异化隐私保护需求的问题，提出基于自适应差分隐私的联邦学习模型，实现细粒度台区数据隐私保护。

2）针对传统联邦学习框架平均聚合机制不符合配电网台区数据质量不平衡、数据异构的场景特征，从而导致的全局模型性能下降的问题，引入了基于参与方贡献度的动态聚合机制，提高了全局模型的准确率和收敛速度。

3）针对基于 Shapley 值的贡献度求解方法不符合配电网台区数量多、算力资源有限等场景特征的问题，引入了基于采样下价值矩阵分解-重构的拟合

机制，在准确率约束范围内极大提高了贡献度求解速率。

1 自适应隐私保护的配电网动态联邦学习框架

针对传统联邦学习框架存在参与方数据隐私保护不足、数据异构异质导致模型性能下降和缺乏有效激励机制的问题，基于配电网下参与方和量测数据的特征分析，考虑到边缘侧计算、通信资源有限的现状[31]，提出了自适应隐私保护的配电网动态联邦学习框架(adaptive privacy-protected dynamic federated learning framework，AP-DFL)，通过AP-DFL实现配电网业务模型的构建。整体架构如图1所示。

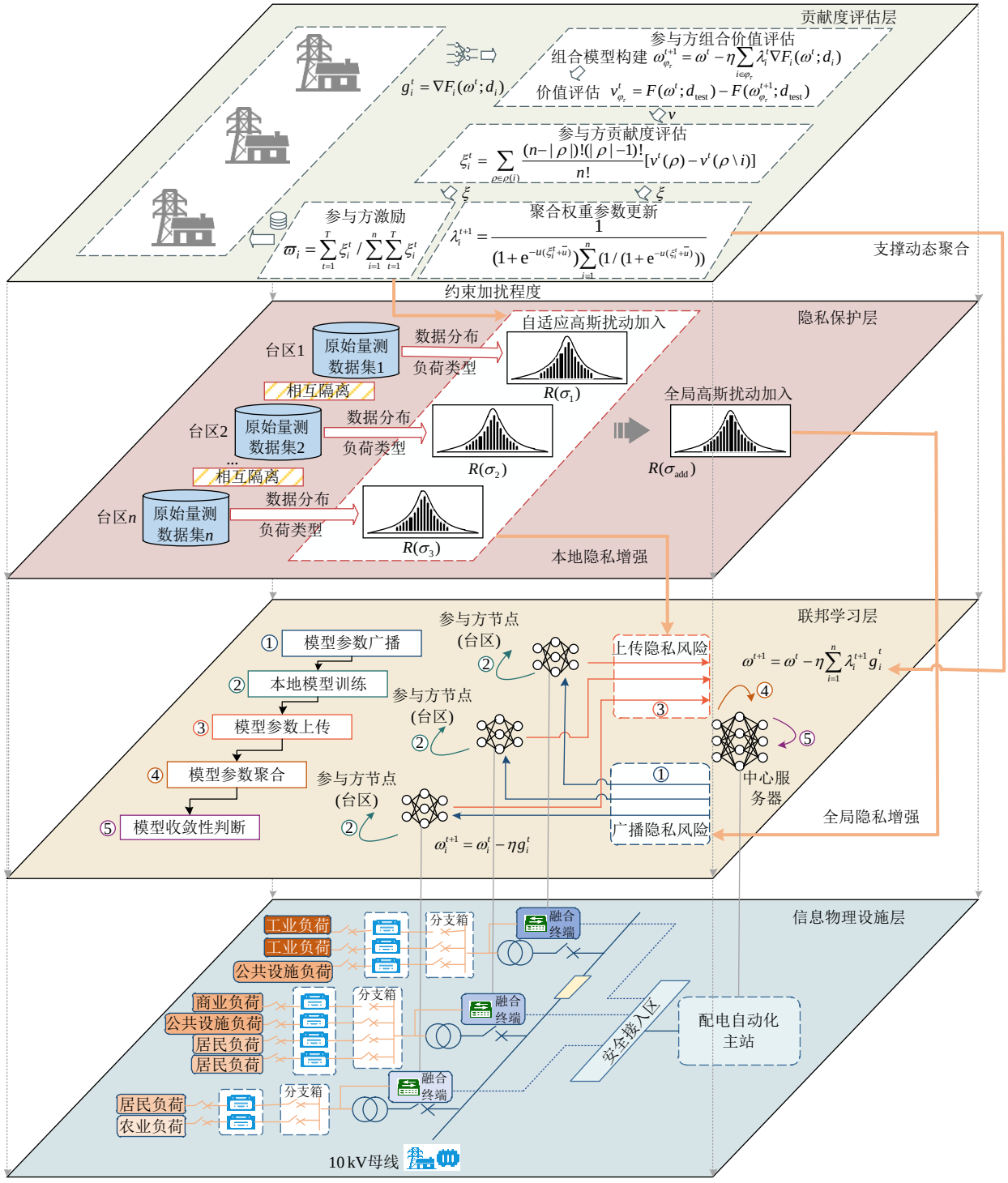


图 1 AP-DFL 框架

Fig. 1 AP-DFL framework

AP-DFL 着重描绘了配电网场景下，原始量测数据通过联邦学习的方式进行要素价值融合；通过自适应差分扰动保护数据隐私；通过动态聚合机制提高模型性能的场景。场景的每一个环节自下而上映射不同层级，涉及信息物理设施层、联邦学习层、隐私保护层和贡献度评估层。

1）信息物理设施层：从物理背景描绘了配电网 10 kV 母线下各融合终端周期性地采集与集中存储不同台区的原始量测数据[32]。融合终端与配电网主站间通过公网进行交互，其过程需通过安全接入区并进行纵向认证的安全策略。

2）联邦学习层：聚焦于学习-传输-聚合过程，各参与方基于中心服务器广播的预模型训练本地模型并将模型梯度上传，中心服务器负责全局模型聚合与广播，经过一定次数的迭代后，模型的全局目标函数可以达到收敛。全局模型和参与方本地模型在优化过程中进行中间参数的上传与广播，其中间参数面临着上传隐私风险和广播隐私风险。

3）隐私保护层：侧重于对抗配电网联邦学习过程中的重构攻击和推断攻击[33]，引入了基于自适应差分隐私的模型梯度隐私保护机制，对不同隐私敏感程度量测数据训练得到的模型进行动态保护以避免敏感数据保护不足、非敏感数据过度保护的问题，并通过边缘侧和主站侧的双重扰动，实现了边缘侧和主站侧的双向隐私保护。

4）贡献度评估层：着眼于解决不同业务目标下，配电台区量测数据质量不平衡、数据异构等问题凸显[34]导致的全局模型性能下降和出于自身利益考量扩大隐私预算需求而造成的冗余准确率损失问题，前者采用动态加权的聚合方式，通过动态调整聚合权重来减小低贡献参与方对全局模型的影响，增大高贡献参与方对全局模型的影响；后者通过对各参与方在该联邦学习任务下的贡献度给予激励，以提高各参与方上传参数的可用性。

2　多主体自适应保护的差分隐私策略

2.1　配电网隐私威胁模型分析

联邦学习将原始量测数据保存在本地，依靠传输模型梯度信息在一定程度上保护数据隐私安全，但这仍然会面临数据集泄漏的风险[35]。在配电网场景下，主站服务器和融合终端通常不会出现恶意行为[36]，且交互数据会进行严格的安全认证[37]，系统外部难以对配网内部数据和模型进行篡改[38]，因此在威胁模型中，将主站服务器、终端和系统外部的特征定义为“诚实但好奇[39]”(honest but curious)。拥有这类特征的攻击者严格遵守训练协议和流程，不会对模型性能发起攻击造成破坏，但是会尝试窃取本地数据集中的数据或信息。

2.2　基于自适应差分隐私的联邦学习模型

防御重构与推断攻击，无需依赖同态加密等复杂的密码学方法。差分隐私技术以其严谨的理论保障、部署的灵活性及较低的系统开销，成为算力薄弱配电台区的更优选择。本文采用差分隐私技术对上传和广播的中间参数进行隐私保护，使得攻击方尽可能少的推理出敏感信息。考虑到因配电网中各台区负荷类型和数据分布具有显著差异而导致隐私保护需求不同的现状，提出一种基于自适应差分隐私的联邦学习模型(federated learning model based on adaptive differential privacy，FL-ADP)，具体过程如图 2 所示。

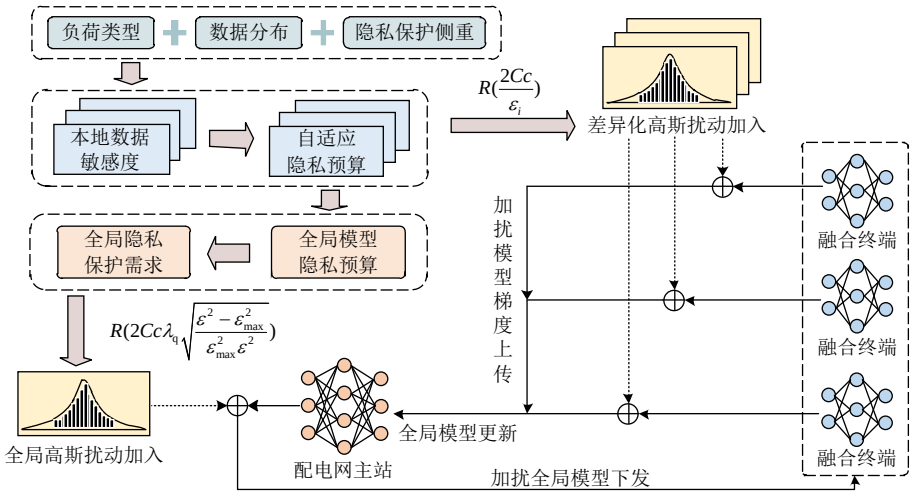


图 2　FL-ADP 模型

Fig. 2　FL-ADP model

FL-ADP 模型主要分为 2 个阶段：1）上传隐私保护阶段，在联邦学习开始之前，融合终端根据负荷类型、数据分布及隐私保护侧重点计算本地数据集敏感度，基于此调节隐私预算，对上传梯度参数加入自适应高斯扰动以实现上传隐私保护；2）广播隐私阶段，配网主站计算全局模型隐私预算，根据隐私约束条件确定全局隐私保护需求，通过向全局模型加入自适应高斯扰动并下发至各终端，实现广播隐私保护。为了在理论上更好地实现上述模型功能，给出以下定义：

定义 1 松弛差分隐私[40]。若所有临近输入 $x \sim x'$ 和随机函数 F 满足式(1)时，则随机函数 F 满足松弛差分隐私 (ε,δ)-DP，即随机函数 F 能保证 $1-\delta$ 的概率满足式(1)，通常情况下 δ 取值为 10^{-5}，特别的，当 $\delta=0$ 时退化为严格差分隐私 ε-DP。

$$\Pr[F(x)\subset Y]\le \mathrm{e}^{\varepsilon}\Pr[F(x')\subset Y]+\delta \tag{1}$$

定义 1 要求 2 个近似输入经过随机函数的处理后，得到的输出不可区分。$\Pr[F(x)\subset Y]$ 表示 $F(x)$ 属于 Y 的概率。

定义 2 个性化差分隐私[41-42]。相同参与方的任意 2 条记录 t 和 t' 经过随机函数 F 后得到相同的输出 t^*，如式(2)所示，则随机函数 F 满足个性化差分隐私 (ε_i,δ)-PDP。

$$\Pr[F_i(t)=t^*]\le \mathrm{e}^{\varepsilon_i}\Pr[F_i(t')=t^*]+\delta \tag{2}$$

不同参与方的隐私预算 ε_i 取决于本地数据集的整体敏感度 S_i、给定隐私预算 ε 和敏感作用参数 θ $(\theta>1)$，如式(3)所示。

$$\varepsilon_i=\varepsilon\theta^{S_i-1/2} \tag{3}$$

因此，融合终端根据本地数据的敏感度，通过升高或降低隐私预算 ε_i 来减弱或增强隐私保护程度，以此达到细粒度隐私保护的目的。

定义 3 匿名性敏感度[43]。已知本地数据集中属性的熵、最大离散熵，属性匿名性敏感度定义如式(4)所示。

$$S_{i,j}^{\mathrm{A}}(d_{i,j})=\frac{H_{\max}(d_{i,j})-H(d_{i,j})}{H_{\max}(d_{i,j})} \tag{4}$$

式中：$S_{i,j}^{\mathrm{A}}(d_{i,j})\in[0,1]$；$H_{\max}(d_{i,j})$ 为最大离散熵，数据属性离散熵 $H(d_{i,j})$ 越大，属性匿名性敏感度 $S_{i,j}^{\mathrm{A}}(d_{i,j})$ 越小，代表越敏感，反之越不敏感。从分布而言，数据属性分布越均匀，越容易被攻击者将敏感数据与标识符或准标识符进行对应，有更大的隐私泄露风险；而当分布不均匀时，出现数据集中在某些范围内，攻击者则较难将其与标识符或准标识符进行对应，隐私泄露风险相对较低。由此，匿名性敏感度 $S_i^{\mathrm{A}}(d_i)$ 如式(5)所示。

$$S_i^{\mathrm{A}}(d_i)=\sum_{j\in i}p_{i,j}S_{i,j}^{\mathrm{A}}(d_{i,j}) \tag{5}$$

式中：$S_j^{\mathrm{A}}(d_i)\in[0,1]$；$p_{i,j}$ 为数据属性 j 所占整个数据集中的比例。此定义从数据分布的角度对数据的敏感度进行度量，侧重于某条数据在整个数据集中的匿名性。

定义 4 机密性敏感度。已知本地数据集中负荷类型及比例，机密性敏感度 $S_i^{\mathrm{C}}(\beta_i)$ 定义为

$$S_i^{\mathrm{C}}(\beta_i)=1-\frac{\sum_{\beta\in i}p_{i,\beta}\beta}{\beta_{\max}} \tag{6}$$

式中：β 为数据重要程度，取决于负荷类型；$p_{i,\beta}$ 为数据重要程度为 β 的数据量占该台区总体数据量的比例；$\beta_{\max}$ 为最高数据重要程度。

定义 5 本地数据集敏感度。已知本地数据集中的匿名性敏感度、机密性敏感度和台区负荷类型，本地数据集敏感度定义如式(7)所示。

$$S_i(d_i)=\alpha_i S_i^{\mathrm{A}}(d_i)+(1-\alpha_i)S_i^{\mathrm{C}}(\beta_i) \tag{7}$$

式中：$S_i(d_i)\in[0,1]$，从数据匿名性需求和数据机密性需求的二维角度对本地数据集 d_i 的敏感度进行度量；$\alpha_i\in(0,1)$，为隐私侧重权重参数，由台区负荷类型及其比例决定(如式(8)所示)，以适应不同类型负荷数据隐私保护的侧重。例如居民负荷数据涉及个人用电习惯，隐私保护需注重个人用电数据的高度匿名性，因此选择较大 α_i 以提高匿名性敏感度的权重；工业负荷可能涉及企业机密，隐私保护需重点关注数据的机密性，因此选择较小的 α_i 以提高机密性敏感度的权重。

$$\alpha_i=\sum_{k\in i}p_{i,k}\alpha_k \tag{8}$$

式中：$p_{i,k}$ 为负荷类型为 k 的数据量占该台区总体数据量的比例；α_k 为负荷类型为 k 所对应的动态权重参数。此定义立足于不同负荷类型的隐私保护侧重，综合考虑本地数据的分布和重要度，实现更全面的台区隐私保护需求量化。

定义 6 高斯机制。设查询函数 $s:d\to\mathbf{R}^D$，此函数敏感度 $\Delta s=\max\|s(d)-s(d')\|_2$。随机算法 $F=s(d)+R(0,\Delta s/\varepsilon)$ 能够满足 (ε,δ)-DP 隐私需求，其中 $c\ge\sqrt{2\ln(1.25/\delta)}$。高斯分布如下：

$$p(x)=\frac{1}{\sqrt{2\pi}\sigma}\mathrm{e}^{-\frac{(x-\mu)^2}{2\sigma^2}} \tag{9}$$

式中：μ 为高斯分布的期望；σ^2 为其方差。

2.3 FL-ADP 算法

本节从 FL-ADP 的总体流程、本地更新和中央聚合 3 个阶段介绍 FL-ADP 算法。

1）FL-ADP 总体流程：配电网主站向各终端下发全局模型参数 ω，n 个参与联邦学习的融合终端执行 FL-ADP 本地更新流程，配电网主站执行 FL-ADP 中央聚合流程，获得全局模型参数 ω。

2）FL-ADP 本地更新：首先，融合终端根据配电网主站下发的预模型 ω^t，利用本地数据对模型进行训练，形成本地模型 ω_i^{t+1} 并得到梯度 g_i^{t+1}。

$$\omega_i^{t+1}=\omega_i^t-\eta g_i^t \tag{10}$$

$$g_i^t=\nabla F_i(\omega^t;d_i) \tag{11}$$

式中：F 为损失函数；η 为学习率。其次，对训练模型得到的梯度 g_i^t 进行裁剪，用以约束梯度的敏感度，如式(12)所示。

$$\overline{g}_i^t=g_i^t/\max(1,\|g_i^t\|_2/C) \tag{12}$$

式中 C 为 g_i 的裁剪阈值。再次，计算本地梯度敏感度 $\Delta s_L^{d_i}$。

$$\Delta s_{\mathrm{L}}^{d_i,t}=\max_{d_i,d_i'}\|g_i^t(d_i)-g_i^t(d_i')\|\le 2C \tag{13}$$

式中 d_i 与 d_i' 为临近数据集。

接着，对裁剪后的梯度施加差异化高斯噪声 $R(\sigma_{\mathrm{L},i})$，如式(14)所示，以满足 (ε_i,δ)-DP，实现差异化加扰。

$$g_i^t=\overline{g}_i^t+R(\sigma_{\mathrm{L},i}^t) \tag{14}$$

$$\sigma_{\mathrm{L},i}^t=c\frac{\Delta s_{\mathrm{L}}^{d_i,t}}{\varepsilon_i^t}=\frac{2Cc}{\varepsilon_i^t} \tag{15}$$

最后，将扰动后的梯度 g_i^t 和隐私预算 ε_i^t 上传到配电网主站。

3）FL-ADP 中央聚合。配电网主站更新全局模型，如式(16)所示。

$$\omega^{t+1}=\omega^t-\eta\sum_{i=1}^n\lambda_i^{t+1}g_i^t \tag{16}$$

式中 λ_i^{t+1} 为聚合权重。并根据是否满足全局差分隐私进行二次加扰，将处理完成后的模型参数 ω^{t+1} 下发至各融合终端，做下一轮联邦训练的预模型，具体过程如下。

全局模型敏感度 $\Delta s_{\mathrm{all}}^{t+1}$ 如下：

$$\begin{aligned}\Delta s_{\mathrm{all}}^{t+1}&=\max\{\max_{d_i,d_i'}\|\lambda_i^{t+1}[g_i^t(d_i)-g_i^t(d_i')]\|\}\\&=\max\{\lambda_i^{t+1}\Delta s_{\mathrm{L}}^{d_i,t}\}=\lambda_{\mathrm{q}}^{t+1}\Delta s_{\mathrm{L}}^{d_{\mathrm{q}},t}\le 2C\lambda_{\mathrm{q}}^{t+1}\end{aligned} \tag{17}$$

式中 $\lambda_{\mathrm{q}}^{t+1}$ 为 $\lambda_i^{t+1}\Delta s_{\mathrm{L}}^{d_i,t}$ 取值最大时对应的 λ_i^{t+1}。全局加扰需求 $\sigma_{\mathrm{all}}^{t+1}$ 如下：

$$\sigma_{\mathrm{all}}^{t+1}=c\frac{\Delta s_{\mathrm{all}}^{t+1}}{\varepsilon_{\max}}=\frac{2Cc\lambda_{\mathrm{q}}^{t+1}}{\varepsilon_{\max}} \tag{18}$$

式中 $\varepsilon_{\max}$ 为全局隐私预算阈值。

全局模型的扰动标准差 $\sigma_{\mathrm{L}}^{t+1}$ 如下：

$$\sigma_{\mathrm{L}}^{t+1}=c\frac{\Delta s_{\mathrm{all}}^{t+1}}{\varepsilon_{\mathrm{all}}^t}=\frac{2Cc\lambda_{\mathrm{q}}^{t+1}}{\varepsilon_{\mathrm{all}}^t} \tag{19}$$

$$\varepsilon_{\mathrm{all}}^{t+1}=\sum_{i=1}^n\lambda_i^{t+1}\varepsilon_i^{t+1} \tag{20}$$

当全局模型隐私预算 $\varepsilon_{\mathrm{all}}^{t+1}$ 不足以满足全局隐私保护时，即 $\varepsilon_{\mathrm{all}}^{t+1}>\varepsilon_{\max}$，配电网主站对全局模型进行二次加扰：

$$\sigma_{\mathrm{add}}=\sqrt{(\sigma_{\mathrm{all}}^{t+1})^2-(\sigma_{\mathrm{L}}^{t+1})^2}=2Cc\lambda_{\mathrm{q}}^{t+1}\sqrt{\frac{(\varepsilon_{\mathrm{all}}^{t+1})^2-\varepsilon_{\max}^2}{\varepsilon_{\max}^2(\varepsilon_{\mathrm{all}}^{t+1})^2}} \tag{21}$$

2.4 FL-ADP 隐私性分析

引理 FL-ADP 算法满足全局差分隐私。

证明 假设 $s(g)$ 是不符合 (ε_i,δ)-ADP 的查询函数，$F(\omega)$ 是符合 (ε_i,δ)-ADI 的随机函数，满足 $F(\omega)=s(g)+R$，R 服从均值为 0、标准差为 $c\Delta s/\varepsilon$ 的高斯分布，$R\sim(0,c\Delta s/\varepsilon)$。

$$\frac{\Pr[F(g)=\Lambda^*]}{\Pr[F(g')=\Lambda^*]}=\frac{\Pr[s(g)+R=\Lambda^*]}{\Pr[s(g')+R=\Lambda^*]}=$$

$$\frac{\Pr[R=\Lambda^*-s(g)]}{\Pr[R=\Lambda^*-s(g')]}=\frac{\exp[(\frac{-1}{2\sigma^2})R^2]}{\exp[(\frac{-1}{2\sigma^2})(R+\Delta s)^2]}=$$

$$\exp[\frac{1}{2\sigma^2}(2R\Delta s+(\Delta s)^2)] \tag{22}$$

式中：g、g' 为 2 个相异的模型梯度；$\Lambda^*\in\Lambda$，Λ 为差分隐私结果集；R 无法恒小于某定值，因此只需满足定义 1 即可。即证：

$$\Pr[R\ge\frac{\sigma^2\varepsilon_i}{\Delta s}-\frac{\Delta s}{2}]<\frac{\delta}{2} \tag{23}$$

设 $\frac{\sigma^2\varepsilon_i}{\Delta s}-\frac{\Delta s}{2}=\vartheta$，则 $\Pr[R\ge\vartheta]$ 的边界为

$$\Pr[R\ge\vartheta]=\int_\vartheta^\infty\frac{1}{\sqrt{2\pi}\sigma_{\mathrm{all}}}\mathrm{e}^{-\frac{R^2}{2\sigma_{\mathrm{all}}^2}}\mathrm{d}x\le\frac{\sigma_{\mathrm{all}}}{\sqrt{2\pi}\vartheta}\mathrm{e}^{-\frac{\vartheta^2}{2\sigma_{\mathrm{all}}^2}} \tag{24}$$

即证：

$$\ln\left(\frac{\vartheta}{\sigma_{\text{all}}}\right)+\frac{\vartheta^2}{2\sigma_{\text{all}}^2}>\ln\left(\sqrt{\frac{2}{\pi}}\frac{1}{\delta}\right) \tag{25}$$

当全局模型达到全局隐私约束时，令式(25)中 $\sigma_{\text{all}}=\sigma_L=c\Delta s_{\text{all}}/\varepsilon_{\text{all}}$，可得 $c\geq\sqrt{2\ln(1.25\delta}$；当全局模型未达到全局隐私约束时，令式(25)中 $\sigma_{\text{all}}=c\Delta s_{\text{all}}/\varepsilon_{\max}$，可得 $c\geq\sqrt{2\ln(1.25/\delta)}$。因此，扰动满足全局差分隐私。

3 基于矩阵分解 Shapley 值的联邦学习模型性能优化及激励机制

配网台区(参与方)因设备故障、网络通信堵塞、停机和计划外维护等原因导致数据质量存在差异性[44]；因地理位置、负荷类型和数据分布等存在差异将导致数据异构[45]。这将致使联邦模型准确率降低、收敛速度慢。本节提出基于矩阵分解 Shapley 值的联邦学习性能优化模型，此模型利用基于矩阵分解 Shapley 值的方式求解参与方的贡献度，基于贡献度动态调整参与方在联邦训练中的参与程度并给予激励，增强对低价值、恶意数据的鲁棒性，提高模型准确率和收敛速度，具体过程如图 3 所示。

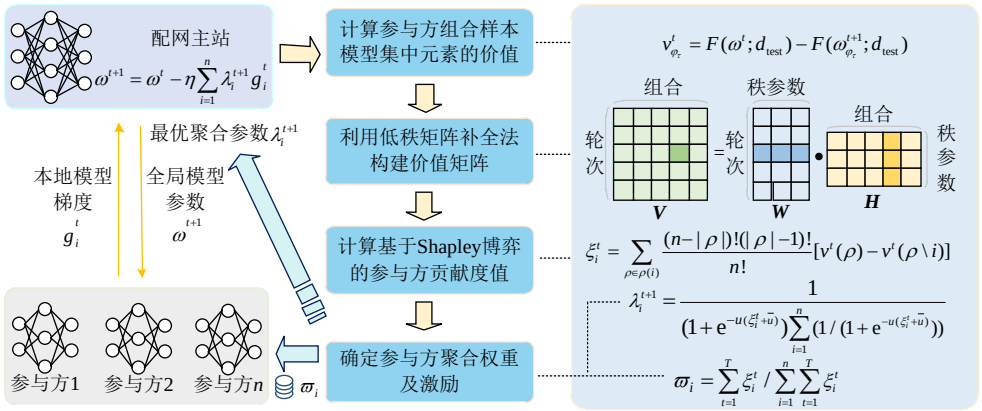


图 3 基于矩阵分解 Shapley 值的联邦学习性能优化模型

Fig. 3 A performance optimization model for federated learning based on matrix decomposition Shapley values

参与方贡献度评估需综合考虑数据价值和边际增益 2 方面。其分析步骤包括：1）通过损失来度量参与方组合的价值 v_{φ_τ}；2）通过 Shapley 博弈的方式，从边际增益的角度计算参与方贡献度 ξ_i。

3.1 基于价值矩阵分解-重构的参与方组合价值度量

本文将参与方组合模型的损失差定义为该组合在业务下的联邦训练价值。鉴于配网台区数量大，其组合随数量成指数级增长，这将导致高昂的算力代价。因此，通过构建价值矩阵实现价值度量。

1）残缺价值矩阵构建。

首先，配电网主站枚举所有参与方组合构成参与方组合集 $\rho=\{\rho_1,\rho_2,...,\rho_\kappa,...,\rho_{2^n-1}\}$。为在误差允许范围内尽可能降低算力资源占用，采用蒙特卡洛法对参与方组合集中的元素进行抽样，形成参与方组合样本集 $\varphi^t=\{\varphi_1^t,\varphi_2^t,...,\varphi_\tau^t,...,\varphi_\gamma^t\}$，其中 $t\in T$，$\Upsilon=\gamma/(2^n-1)$ 为蒙特卡洛参与率。

然后，对全局模型进行权重梯度下降，形成样本模型集 $\omega_\varphi^{t+1}=\{\omega_{\varphi_1}^{t+1},\omega_{\varphi_2}^{t+1},...,\omega_{\varphi_\tau}^{t+1},...,\omega_{\varphi_\gamma}^{t+1}\}$，如式(26)所示。

$$\omega_{\varphi_\tau}^{t+1}=\omega^t-\eta\sum_{i\in\varphi_\tau}\lambda_i^t\nabla F_i(\omega^t;d_i) \tag{26}$$

计算样本模型集中元素的价值 $v_{\varphi_\tau}^t$，即第 t 轮次下的参与方组合价值，如式(27)所示。

$$v_{\varphi_\tau}^t=F(\omega^t;d_{\text{test}})-F(\omega_{\varphi_\tau}^{t+1};d_{\text{test}}) \tag{27}$$

最后依据样本模型集中元素的价值 $v_{\varphi_\tau}^t$ 构建残缺价值矩阵 $V'\in\mathbf{R}^{T\times(2^n-1)}$，如图 4 所示。

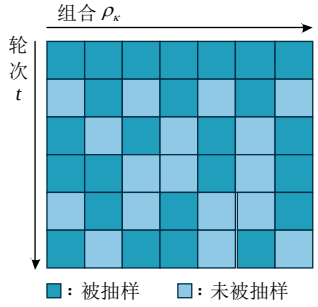


图 4 残缺价值矩阵图

Fig. 4 Incomplete value matrix diagram

2）价值矩阵拟合。

同一轮次下，相似组合的价值相似，不同轮次下，同一组合的价值相似，即价值矩阵 $\boldsymbol{V}$ 的行、列之间存在相似性，这使得此矩阵满足近似低秩的特性。因此，采用基于因式分解的低秩矩阵补全法来

补全残缺价值矩阵$\boldsymbol{V}'$，而$\boldsymbol{V}'$分解补全问题最终转化为优化问题$\min\|\boldsymbol{V}'-\boldsymbol{W}\boldsymbol{H}\|$，矩阵$\boldsymbol{W}$和$\boldsymbol{H}$的构建如式(28)所示，价值矩阵$\boldsymbol{V}$的拟合如式(29)所示。

$$\min_{\substack{W\in\mathbf{R}^{T\times r}\\ H\in\mathbf{R}^{(2^n-1)\times r}}}\sum_{t=1}^{T}\sum_{\varphi_\tau\in\varphi}(v_{\varphi_\tau}^t-w_t h_{\varphi_\tau})^2+\psi(\|\boldsymbol{W}\|_F^2+\|\boldsymbol{H}\|_F^2) \tag{28}$$

$$\boldsymbol{V}=\boldsymbol{W}\boldsymbol{H} \tag{29}$$

式中：价值矩阵$\boldsymbol{V}$中的元素$v_{\varphi_\tau}^t$表示参与方组合φ_τ在第t轮次的价值；r为秩参数；ψ为正则化参数；$\|\cdot\|_F$为 Frobenious 范数；w_t和$h_{\varphi_\tau}^t$分别为矩阵$\boldsymbol{W}$第t行的行向量和矩阵$\boldsymbol{H}$第φ_τ列的列向量。

3.2　基于 Shapley 值的参与方贡献度度量

在评估参与方组合的价值后，本节进一步度量参与方在联邦学习中的贡献。相较于采用个体法[27]会忽略参与方模型梯度对联邦模型带来的边际效应和留一法[46]仅注重边际效应导致的不公平，提出基于 Shapley 值[47]的参与方贡献度度量策略，将参与方的 Shapley 值作为该参与方在联邦训练中的贡献，如式(30)所示。其中$|\rho|$表示组合ρ的参与方数目，$\rho(i)$表示包含参与方i的所有组合，$v(\rho\setminus i)$表示组合ρ中去掉参与方i后的组合价值。

$$\xi_i^t=\sum_{\rho\in\rho(i)}\frac{(n-|\rho|)!(|\rho|-1)!}{n!}[v^t(\rho)-v^t(\rho\setminus i)] \tag{30}$$

该策略满足合理性(group rationality)、对称性(symmetry)、零贡献(zero element)和可加性(additivity)[48]。

3.3　基于参与方贡献度的模型性能优化和参与方激励机制

1）模型性能优化。

在配电网场景下的联邦学习实践中，无法保证所有参与方的数据对目标业务模型都是高价值且无恶意的。为了提高模型准确率和收敛速度，提出基于参与方对目标业务模型贡献度的联邦学习动态聚合机制，根据不同轮次下贡献度ξ_i^t动态调整参与方邦聚合权重λ_i^{t+1}。

$$\lambda_i^{t+1}=\frac{1}{(1+\mathrm{e}^{-u(\xi_i^t+\bar{u})})\sum_{i=1}^{n}(1/(1+\mathrm{e}^{-u(\xi_i^t+\bar{u})}))} \tag{31}$$

式中归一化伸缩参数u、偏移参数$\bar{u}$都为定值。

2）参与方激励机制。

为约束参与方加扰程度并促进拥有优秀数据集的参与方加入联邦学习，提出基于贡献度的参与方激励机制，根据参与方对联邦学习模型的贡献度ξ_i^t给予参与方激励ϖ_i。

$$\varpi_i=\sum_{t=1}^{T}\xi_i^t/\sum_{i=1}^{n}\sum_{t=1}^{T}\xi_i^t \tag{32}$$

3.4　价值拟合收敛性分析

引理　价值矩阵满足近似低秩的特性。

证明　假设$\hat{\lambda}>0$是r阶矩阵$\boldsymbol{Z}$逼近价值矩阵$\boldsymbol{V}$的容差，则$\boldsymbol{V}$在容差为$\hat{\lambda}$下的秩$\mathrm{rank}_{\hat{\lambda}}(\boldsymbol{V})$如下：

$$\mathrm{rank}_{\hat{\lambda}}(\boldsymbol{V})=\min\{\mathrm{rank}(\boldsymbol{Z}):\boldsymbol{Z}\in\mathbf{R}^{T\times 2^n-1},\|\boldsymbol{Z}-\boldsymbol{V}\|_{\max}\le\hat{\lambda}\} \tag{33}$$

通常情况下，损失函数F为凸函数且满足L_1-Lipschitz 和L_2-smooth[49]，由式(34)可知，相同参与方组合价值在相邻时刻上的差存在上界。

$$\begin{aligned}
&|v_{\varphi_\tau}^t-v_{\varphi_\tau}^{t+1}|=|[F(\omega^t;d_{\text{test}})-F(\omega_{\varphi_\tau}^{t+1};d_{\text{test}})]-\\
&[F(\omega^{t+1};d_{\text{test}})-F(\omega_{\varphi_\tau}^{t+2};d_{\text{test}})]|\le\\
&|F(\omega^t;d_{\text{test}})-F(\omega^{t+1};d_{\text{test}})|+\\
&|F(\omega_{\varphi_\tau}^{t+1};d_{\text{test}})-F(\omega_{\varphi_\tau}^{t+2};d_{\text{test}})|\le\\
&L_1\|\omega^t-\omega^{t+1}\|+L_1\|\omega_{\varphi_\tau}^{t+1}-\omega_{\varphi_\tau}^{t+2}\|=\\
&L_1\|\omega^t-\omega^{t+1}\|+L_1\|[\omega^t-\eta\sum_{i\in\varphi_\tau}\lambda_i^t\nabla F_i(\omega^t;d_i)]-\\
&[\omega^{t+1}-\eta\sum_{i\in\varphi_\tau}\lambda_i^{t+1}\nabla F_i(\omega^{t+1};d_i)]\|\le\\
&2L_1\|\omega^t-\omega^{t+1}\|+\\
&\max(\lambda_i^t,\lambda_i^{t+1})L_1\eta\sum_{i\in\varphi_\tau}\|\nabla F_i(\omega^t;d_i)-\nabla F_i(\omega^{t+1};d_i)\|\le\\
&(2+\eta L_2)L_1\|\omega^t-\omega^{t+1}\|
\end{aligned} \tag{34}$$

由此可知价值矩阵的列满足L_1-Lipschitz 和L_2-smooth。

$$\sum_{t=1}^{T-1}\|\boldsymbol{v}^t-\boldsymbol{v}^{t+1}\|_{\max}\le(2+\eta L_2)L_1\sum_{t=1}^{T-1}\|\omega^t-\omega^{t+1}\| \tag{35}$$

式中$\boldsymbol{v}^t$和$\boldsymbol{v}^{t+1}$表示价值矩阵$\boldsymbol{V}$的第t和$t+1$行的行向量。由式(35)可知，相邻时刻间任意组合的价值之差存在上界，即价值矩阵的行和列均满足L_1-Lipschitz 和L_2-smooth。因此，对于任意$\hat{\lambda}>0$，价值矩阵满足式(36)。

$$\mathrm{rank}_{\hat{\lambda}}(\boldsymbol{V})=\frac{(2+\eta L_2)L_1\sum_{t=1}^{T-1}\|\omega^t-\omega^{t+1}\|}{\hat{\lambda}} \tag{36}$$

当损失函数F满足m强凸时，结合上述条件可得 FedAvg 具有次线性收敛速度$O(1/T)$。AP-DFL 在此条件下收敛速度与 FedAvg 处于同一量级，考虑到本文所采用的损失函数不满足强凸性，故收敛速度ℓ满足：

$$\ell_{\text{AP-DFL}_{\text{conv}}} \le \ell_{\text{FedAvg}_{\text{strongly-conv}}} \le 1/T \tag{37}$$

因此，可知 $\sum_{t=1}^{T}\| \omega^{t}-\omega^{t+1} \|$ 的上界为

$$\sum_{t=1}^{T-1}\| \omega_{\text{AP-DFL}_{\text{conv}}}^{t}-\omega_{\text{AP-DFL}_{\text{conv}}}^{t+1} \| \le \sum_{t=1}^{T-1}\| \omega_{\text{FedAvg}_{\text{strongly-conv}}}^{t}-\omega_{\text{FedAvg}_{\text{strongly-conv}}}^{t+1} \| \le \sum_{t=1}^{T-1}\eta L_1(T-1) \tag{38}$$

价值矩阵 $\boldsymbol{V}$ 的秩 r 的上界为

$$\text{rank}_{\hat{\lambda}}(\boldsymbol{V}) \le \frac{(2+\eta L_2)L_1\eta L_1(T-1)}{\hat{\lambda}} \tag{39}$$

因此，价值矩阵满足近似低秩特性。

4 算例分析

4.1 实验设置

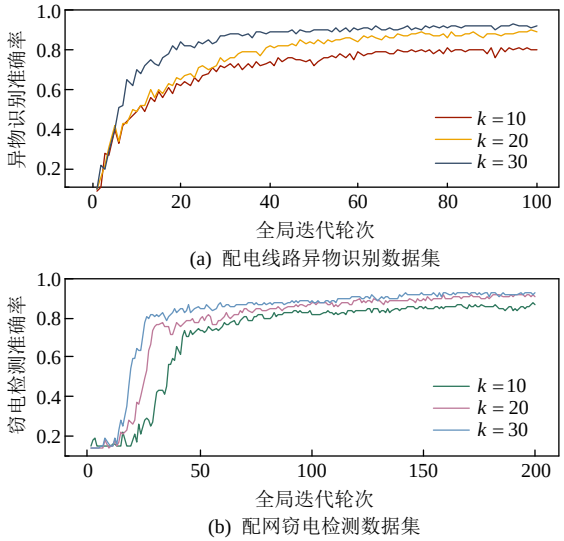
实验配置了 Intel(R) Xeon(R) Bronze 3140CPU，64 GB RAM 和 RTX4090 的硬件环境，软件环境为 Python3.9 和 Pytorch1.12.0。实验数据集采用配电线路异物识别图像数据集和配网窃电检测数据集，其中，配电线路异物识别图像数据集来源于我国北方某地区共 3 000 张配电线路航拍图像，其中无异物和有异物的分别为 1 200 张和 1 800 张，在有异物的图像中，将风筝、塑料布、防尘网和鸟巢作为配电线路异物识别特征以判断配网线路是否存在异物，且图像数据间因航拍距离、设备像素和拍摄时间等导致其清晰度和明暗度存在差异；配网窃电检测数据集来源于我国北方地区多家供电公司共 7 000 组经智能电表采集得到的用电用户时序电能数据，其中存在少量数据缺失和噪声，采集周期为 1 个自然日(24 h)，采集间隔为 15 min。数据集经初步数据清洗后，每个样本数据维度为 96 维，等比例分布表征正常状态、“比例缩减”类异常、“削峰窃电”类异常、“下调窃电”类异常、“区间置零窃电”类异常、“随机削减窃电”和“移峰窃电”类异常的样本。考虑到各配电网台区因地理位置不同、负荷类型及比例不同、数据分布差异等导致的数据异构情况[45]，实验为尽可能符合大多数地区配电网主站所辖台区的个数并模拟各台区数据集间的异构性，利用狄利克雷分布策略将完整数据集划分到 50 个参与方，并将狄利克雷分布值设置为 0.05，以确保各台区间数据具有较强 Non-iid。

实验分别用卷积神经网络(convolutional neural network，CNN)模型和长短期记忆网络(long short-term memory，LSTM)模型对配电线路异物识别图像数据集和配网窃电检测数据集进行训练。在模型训练过程中，训练样本集和测试样本集比例为 4:1。

4.2 不同条件下的 AP-DFL 性能分析

1）参与方选择数量 k。

实验在配电线路异物识别数据集和配网窃电检测数据集上分析了不同参与方选择数量 k 对 AP-DFL 测试准确率的影响。实验选择 3 种不同的参与方选择数量(10、20、30)，结果如图 5 所示。可见，模型测试准确率随参与方选择数量的增多而提高。为平衡模型准确率和算力、通信开销，后续实验的参与方数量均选择 k =10。



(a) 配电线路异物识别数据集

(b) 配网窃电检测数据集

图 5 参与方选择数量对 AP-DFL 准确率的影响

Fig. 5 Impact of the number of participants on the accuracy of AP-DFL

2）敏感作用参数 θ。

本文定义敏感作用参数 θ 将参与方本地数据集敏感度与其隐私预算需求联系起来，通过敏感作用参数来控制参与方本地数据集敏感度对本地隐私预算的影响程度。实验选择 4 种不同的敏感作用参数(1、10、30、50)，结果如图 6 所示。可见，模型测试准确率随敏感作用参数的增加而略微提高。

3）高敏感参与方比例。

实验在不同敏感作用参数 θ 下，分析了不同高敏感参与方比例对 AP-DFL 测试准确率的影响。其中高敏感参与方的敏感度 $S_i(d_i)$ 默认为 0。实验选择 5 种不同的比例，分别为 0.1、0.3、0.5、0.7 和 0.9，结果如图 7 所示。可见，当 $\theta \ne 1$ 时，随着高敏感参与方比例的降低，测试准确率呈现上升趋势，且 θ 越大上升趋势越明显。

4）隐私预算 ε。

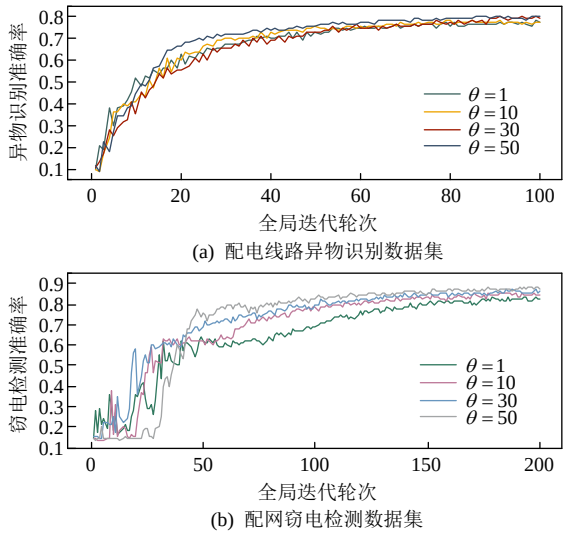


图 6　敏感作用参数对 AP-DFL 准确率的影响

Fig. 6　Impact of privacy attenuation parameters on the accuracy of AP-DFL

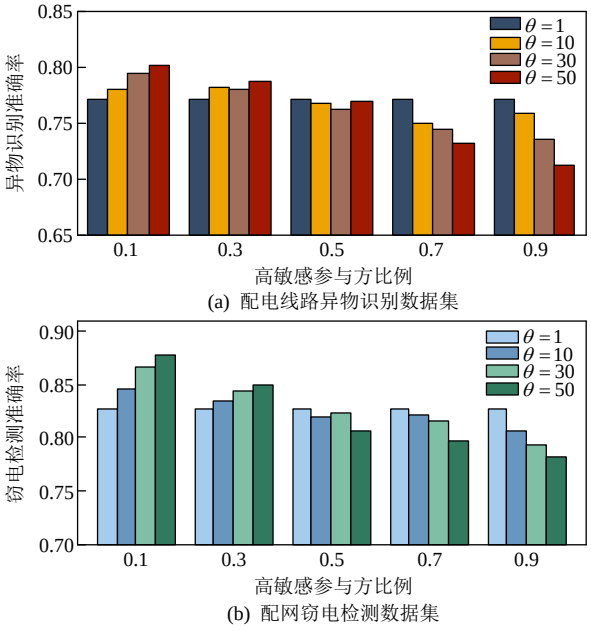


图 7　高敏感参与方比例对 AP-DFL 准确率的影响

Fig. 7　Impact of high sensitivity participant ratio on the accuracy of AP-DFL

为平衡隐私保护程度和模型准确率，分别在配电线路异物识别数据集和配网窃电检测数据集下选择 ε 为 2.0、1.0、0.5、0.1 和 ε 为 10、7、4、1 进行实验，结果如图 8 所示。可见，模型的测试准确率随着隐私预算的减小而下降，这符合差分隐私理论中隐私预算与加扰强度成反比的性质。

5）价值矩阵蒙特卡洛参与率 Υ。

实验在不同参与方选择数量 k 下，分析了不同蒙特卡洛参与率对 AP-DFL 计算所需时间的影响。实验选择 3 种不同的参与率，分别为 0.3、0.5 和 1，其中，当参与率为 1 时，模型退化为直接求取参与

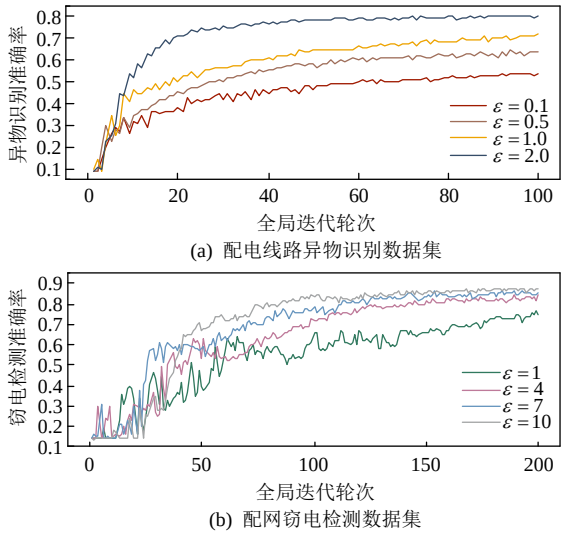


图 8　隐私预算对 AP-DFL 准确率的影响

Fig. 8　Impact of privacy budget on the accuracy of AP-DFL

方的 Shapley 值。结果如图 9 所示，其中 $R^{\text{ratio}}(0.3)$、$R^{\text{ratio}}(0.5)$ 分别表示参与率为 0.3、0.5 与参与率为 1 的计算时间之比，随着蒙特卡洛参与率变大，所需计算时间变长，并且随着参与方数量的增加，$R^{\text{ratio}}(0.3)$ 与 $R^{\text{ratio}}(0.5)$ 的值分别接近于一个稳定的常数，即参与率。

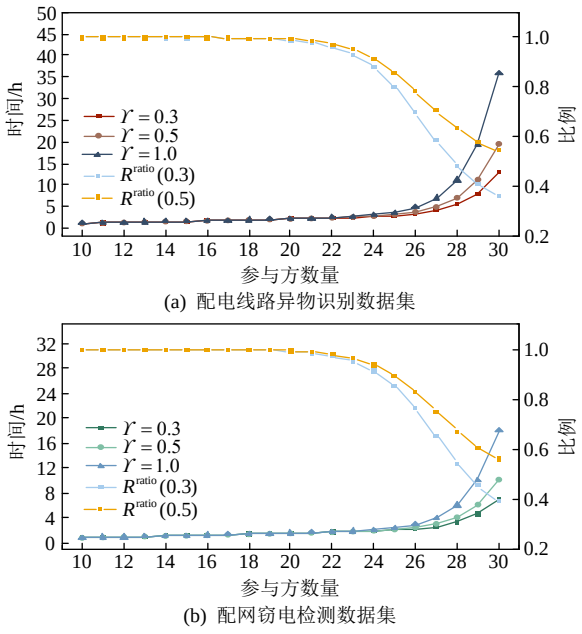


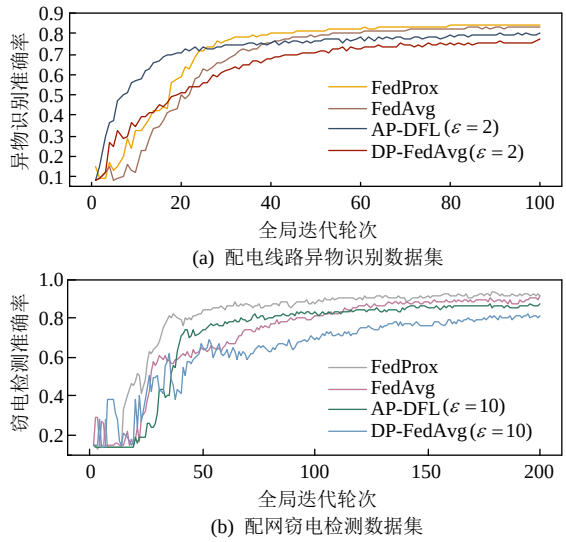
图 9　蒙特卡洛参与率对 AP-DFL 计算时间的影响

Fig. 9　Impact of Monte Carlo participation rate on the calculation time of AP-DFL

4.3　对比实验

为了验证在配网量测数据下 AP-DFL 框架的有效性，本节在配电线路异物识别和配网窃电检测问题上将 AP-DFL 与 FedAvg、FedProx 和 DP-FedAvg

进行对比实验，如图 10 所示。以下分别从模型的测试准确率和收敛趋势上进行分析：



(a) 配电线路异物识别数据集

(b) 配网窃电检测数据集

图 10 不同联邦学习框架准确率对比

Fig. 10 Accuracy comparison of different federated learning frameworks

1）测试准确率。

FedAvg 与 FedProx 在配电线路异物识别数据集上的识别准确率分别为 83.48%和 84.57%，在配网窃电检测数据集上的检测准确率分别为 91.51%和 91.86%；当 $\varepsilon=2$ 时，DP-FedAvg 与 AP-DFL 的配电线路异物识别准确率分别为 77.21%和 79.89%，AP-DFL 比 DP-FedAvg 略高 2.68%；当 $\varepsilon=10$ 时，DP-FedAvg 与 AP-DFL 的窃电检测准确率分别为 81.57%和 86.93%，AP-DFL 比 DP-FedAvg 高 5.36%。由此可见，AP-DFL 的准确率略低于 FedAvg 与 FedProx，是因为 AP-DFL 对参数引入了差异化高斯噪声，实现了台区本地数据的细粒度隐私保护，然而扰动的噪声将不可避免地影响模型的性能，考虑到配电网量测数据包含敏感的用户用采数据和关键电力设施运行状态数据等，其隐私安全至关重要，因此需要在模型准确率和数据隐私安全上有所平衡；在隐私增强的前提下，AP-DFL 的准确率高于 DP-FedAvg，是由于引入了基于贡献度的动态聚合机制，通过动态调节权重实现模型准确度的提升。

2）收敛趋势。

实验分别采用稳定收敛轮次 τ^* 和学习曲线下面积(area under the curve，AUC) $\mathfrak{I}^*$ 来量化模型的收敛速度和收敛稳定性。稳定收敛轮次 τ^* 表示模型达到稳定收敛时的迭代轮次，反映模型在训练过程中达到稳定状态所需的计算、通信资源，即当 τ^* 越小时，模型训练所需的计算、通信资源消耗越低，这在资源受限的配电网中尤其重要。定义如下：

$$\tau^* = T - \tau \tag{40}$$

式中 T 为总迭代轮次。

稳定收敛定义为模型在最后连续 τ 轮内的准确率变化小于某个阈值(选用 0.03)、平均准确率与最终准确率之差小于某个阈值(选用 0.01)；学习曲线下面积 $\mathfrak{I}^*$ 的大小反应了整个训练模型过程中的综合表现，$\mathfrak{I}^*$ 较大的模型通常在整个训练过程中表现更好，波动较小，这表明模型在面对实际配电网数据时具有更高的稳定性和鲁棒性。定义如下：

$$\mathfrak{I}^* = \sum_{t=1}^{T} z(t) \tag{41}$$

式中 $z(t)$ 为关于迭代轮次 t 的模型准确率函数。

收敛趋势分析结果如表 1 所示，AP-DFL 相比于 FedAvg 和 DP-FedAvg 有着更快的收敛速度和更好的收敛稳定性。这是因为全局模型在进行聚合时通过动态调整聚合权重参数来减小低贡献参与方的影响，增大高贡献参与方的影响。更快的收敛速度意味着更短的模型训练轮次，而联邦学习涉及各个节点之间的多轮通信和模型参数更新，模型在更短的训练轮次下收敛能有效减少通信资源和计算资源的消耗，从而提升系统的整体效率；更好的收敛稳定性意味着模型在面对异质、异构的量测数据时，能有效地让损失函数平稳下降，避免梯度震荡或不稳定的波动，降低噪声和异常数据的影响，确保训练结果的一致性和鲁棒性。

表 1 不同联邦学习框架收敛趋势对比分析

Table 1 Comparative analysis of convergence trends of different federated learning frameworks

联邦学习框架	异物识别稳定收敛轮次 τ_1^*	窃电检测稳定收敛轮次 τ_2^*	异物识别 AUC $\mathfrak{I}_1^*$	窃电检测 AUC $\mathfrak{I}_2^*$
FedProx	75	122	71.1	160.8
FedAvg	81	190	66.8	142.6
AP-DFL	73	127	72.1	144.1
DP-FedAvg	91	168	63.3	128.9

结合上述 2 方面分析，总体对比如表 2 所示，表中，平均收敛速度 υ^* 和平均收敛稳定度 $\tilde{\mathfrak{I}}^*$ 的定义分别为

$$\upsilon^* = \frac{\chi_1}{2\tau_1^*} + \frac{\chi_2}{\tau_2^*} \tag{42}$$

$$\tilde{\mathfrak{I}}^* = 2\mathfrak{I}_1^* + \mathfrak{I}_2^* \tag{43}$$

综上，FedProx 和 FedAvg 没有在联邦学习的基

表 2　不同联邦学习框架性能对比分析

Table 2　Comparative analysis of the performance of different federated learning frameworks

联邦学习框架	异物识别准确率 χ_1/%	窃电检测准确率 χ_2/%	平均收敛速度 υ^*/%	平均收敛稳定度 $\tilde{\mathfrak{I}}^*$	隐私保护增强
FedProx	84.57	91.86	0.013 2	303.0	无
FedAvg	83.48	91.51	0.009 9	276.2	无
AP-DFL	79.89	86.93	0.012 4	288.3	精细化保护
DP-FedAvg	77.21	81.57	0.009 1	255.5	统一保护

础上进行隐私增强，难以抵御隐私攻击，存在较大隐私泄露风险；在保护隐私的前提下，相比于 DP-FedAvg，AP-DFL 实现了更精细化的隐私保护，并提高了模型准确率、收敛速度和收敛稳定性。

5　结论

随着数字化进程的深入，人工智能技术在电力系统中的广泛应用对配电网量测数据的价值挖掘提出了更高要求。数据共享作为释放数据潜能、支撑新型电力系统建设的关键环节，亦面临隐私泄露风险。联邦学习作为一种隐私保护计算范式，已逐步应用于电力领域，然而传统框架在隐私保护强度与模型性能方面仍存在不足。为此，本文基于配电网典型业务场景特征，提出了 AP-DFL。针对配电网各台区差异化隐私需求，构建了 FL-ADP。针对台区间数据非独立同分布导致的全局模型性能退化问题，提出了基于矩阵分解与 Shapley 值的联邦学习性能优化方法。在典型配电网场景的实验表明，相较于此前的 DP-FedAvg 方法，本框架在实现更精细化隐私保护的同时，显著优化了模型的准确率与收敛效能。

参考文献

[1] 冯晓青．数字经济时代数据产权结构及其制度构建[J]．比较法研究，2023，190(6)：16-32．
FENG Xiaoqing．The structure and institutional construction of data property rights in the era of digital economy[J]．Journal of Comparative Law，2023，190(6)：16-32(in Chinese)．

[2] 洪延青．我国数据安全法的体系逻辑与实施优化[J]．法学杂志，2023，44(2)：38-53．
HONG Yanqing．The logical deconstruction and institutional construction of China's data security legislation[J]．Law Science Magazine，2023，44(2)：38-53(in Chinese)．

[3] WANG Jianxiao，GAO Feng，ZHOU Yangze，et al．Data sharing in energy systems[J]．Advances in Applied Energy，2023，10：100132．

[4] 陈光宇，徐嘉杰，卢兆军，等．基于相关性度量算法的台区线损异常判断及精准定位[J]．电力工程技术，2022，41(4)：67-74．
CHEN Guangyu，XU Jiajie，LU Zhaojun，et al．Judgment and precise location of abnormal line loss in station area based on correlation measurement algorithm[J]．Electric Power Engineering Technology，2022，41(4)：67-74(in Chinese)．

[5] 陈锦铭，陈烨，韦磊，等．基于多业务融合分析的配变量测数据完整性异常辨识技术[J]．电力信息与通信技术，2023，21(10)：41-47．
CHEN Jinming，CHEN Ye，WEI Lei，et al．Abnormal identification technology for measurement data integrity of distribution transformer based on multi-business fusion analysis[J]．Electric Power Information and Communication Technology，2023，21(10)：41-47(in Chinese)．

[6] 陈徵粼，刘灏，毕天姝．基于配电网 PMU 的无监督电力系统扰动特征提取与分类[J]．中国电机工程学报，2024，44(15)：5858-5870．
CHEN Zhilin，LIU Hao，BI Tianshu．Unsupervised power system disturbance feature extraction and classification using PMUs in distribution network[J]．Proceedings of the CSEE，2024，44(15)：5858-5870(in Chinese)．

[7] 邓丰，陈依林，曾哲，等．数据-知识联合驱动的配电网高阻接地故障检测方法[J]．中国电机工程学报，2024，44(24)：9618-9632．
DENG Feng，CHEN Yilin，ZENG Zhe，et al．Combined data-knowledge driven detection method for high impedance faults in distribution networks[J]．Proceedings of the CSEE，2024，44(24)：9618-9632(in Chinese)．

[8] 蒲天骄，杜帅，李烨，等．面向隐私保护基于联邦强化学习的分布式电源协同优化策略[J]．电力系统自动化，2023，47(8)：62-70．
PU Tianjiao，DU Shuai，LI Ye，et al．Collaborative optimization strategy of distributed generators based on federated reinforcement learning for privacy preservation [J]．Automation of Electric Power Systems，2023，47(8)：62-70(in Chinese)．

[9] 郭庆来，田年丰，孙宏斌．支撑能源互联网协同优化的隐私计算关键技术[J]．电力系统自动化，2023，47(8)：2-14．
GUO Qinglai，TIAN Nianfeng，SUN Hongbin．Key technologies of privacy computation supporting collaborative optimization of energy internet [J]．Automation of Electric Power Systems，2023，47(8)：2-14(in Chinese)．

[10] YANG Qiang，LIU Yang，CHEN Tianjian，et al．Federated

machine learning: concept and applications[J]. Intelligent Systems and Technology, 2019, 10(2): 12.

[11] 凡航，徐葳，范晓昱，等. 隐私计算在新型电力系统中的应用分析与展望[J]. 电力系统自动化，2023，47(19)：187-199.
FAN Hang, XU Wei, FAN Xiaoyu, et al. Application analysis and prospect of privacy-preserving computation in new power system[J]. Automation of Electric Power Systems, 2023, 47(19): 187-199(in Chinese).

[12] 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 Shaobo, ZHANG Jiyong, ZHU Gengming, et al. Personalized federated learning method based on Bregman divergence and differential privacy[J]. Journal of Software, 2024, 35(11): 5249-5262(in Chinese).

[13] 刘俊旭，孟小峰. 机器学习的隐私保护研究综述[J]. 计算机研究与发展，2020，57(2)：346-362.
LIU Junxu, MENG Xiaofeng. Survey on privacy-preserving machine learning[J]. Journal of Computer Research and Development, 2020, 57(2): 346-362(in Chinese).

[14] MELIS L, SONG Congzheng, DE CRISTOFARO E, et al. Exploiting unintended feature leakage in collaborative learning[C]//Proceedings of the 40th IEEE Symposium on Security and Privacy(SP). San Francisco: IEEE, 2019: 691-706.

[15] 肖雄，唐卓，肖斌，等. 联邦学习的隐私保护与安全防御研究综述[J]. 计算机学报，2023，46(5)：1019-1044.
XIAO Xiong, TANG Zhuo, XIAO Bin, et al. A survey on privacy and security issues in federated learning [J]. Chinese Journal of Computers, 2023, 46(5): 1019-1044(in Chinese).

[16] 郑楷洪，肖勇，王鑫，等. 一个面向电力计量系统的联邦学习框架[J]. 中国电机工程学报，2020，40(S1)：122-133.
ZHENG Kaihong, XIAO Yong, WANG Xin, et al. A federated learning framework for power grid metering system[J]. Proceedings of the CSEE, 2020, 40(S1): 122-133(in Chinese).

[17] DWORK C, ROTH A. The algorithmic foundations of differential privacy[J]. Foundations and Trends in Theoretical Computer Science, 2014, 9(3-4): 211-407.

[18] LU Yunlong, HUANG Xiaohong, DAI Yueyue, et al. Differentially private asynchronous federated learning for mobile edge computing in urban informatics[J]. IEEE Transactions on Industrial Informatics, 2020, 16(3): 2134-2143.

[19] 余兴兴，李元诚，王庆乐，等. 基于联邦强化学习的社区共享储能日前调度[J]. 中国电机工程学报，2024，44(20)：8103-8112.
YU Xingxing, LI Yuancheng, WANG Qingle, et al. Day-ahead scheduling of community shared energy storage based on federated reinforcement learning [J]. Proceedings of the CSEE, 2024, 44(20): 8103-8112(in Chinese).

[20] 尹春勇，屈锐. 基于个性化差分隐私的联邦学习算法[J]. 计算机应用，2023，43(4)：1160-1168.
YIN Chunyong, QU Rui. Federated learning algorithm based on personalized differential privacy[J]. Journal of Computer Applications, 2023, 43(4): 1160-1168(in Chinese).

[21] 李敏，肖迪，陈律君. 兼顾通信效率与效用的自适应高斯差分隐私个性化联邦学习[J]. 计算机学报，2024，47(4)：924-946.
LI Min, XIAO Di, CHEN Lvjun. Communication-efficient and utility-aware adaptive Gaussian differential privacy for personalized federated learning[J]. Chinese Journal of Computers, 2024, 47(4): 924-946(in Chinese).

[22] 杨会峰，陈连栋，程凯，等. 支持个性化隐私保护的异步联邦窃电检测方法[J]. 电力信息与通信技术，2023，21(6)：15-23.
YANG Huifeng, CHEN Liandong, CHENG Kai, et al. An asynchronous federated learning electricity theft detection method for personalized privacy-preserving[J]. Electric Power Information and Communication Technology, 2023, 21(6): 15-23(in Chinese).

[23] 王勇，李国良，李开宇. 联邦学习贡献评估综述[J]. 软件学报，2023，34(3)：1168-1192.
WANG Yong, LI Guoliang, LI Kaiyu. Survey on contribution evaluation for federated learning[J]. Journal of Software, 2023, 34(3): 1168-1192(in Chinese).

[24] 刘炜，唐琮轲，马杰，等. 基于区块链和动态评估的隐私保护联邦学习模型[J]. 计算机研究与发展，2023，60(11)：2583-2593.
LIU Wei, TANG Congke, MA Jie, et al. A federated learning model for privacy protection based on blockchain and dynamic evaluation[J]. Journal of Computer Research and Development, 2023, 60(11): 2583-2593(in Chinese).

[25] 张晓龙，罗文华. 利用动态裁剪差分隐私实现联邦学习入侵检测[J]. 小型微型计算机系统，2024，45(6)：1474-1481.
ZHANG Xiaolong, LUO Wenhua. Implementing federated learning intrusion detection using dynamic clipping differential privacy[J]. Journal of Chinese Computer Systems, 2024, 45(6): 1474-1481(in Chinese).

[26] 应作斌，方一晨，张怡文. 动态聚合权重的隐私保护联邦学习框架[J]. 网络与信息安全学报，2022，8(5)：56-65.
YING Zuobin, FANG Yichen, ZHANG Yiwen. Privacy-preserving federated learning framework with

dynamic weight aggregation[J]. Chinese Journal of Network and Information Security，2022，8(5)：56-65(in Chinese).

[27] KANG Jiawen，XIONG Zehui．NIYATO D，et al．Incentive mechanism for reliable federated learning：A joint optimization approach to combining reputation and contract theory[J]. IEEE Internet of Things Journal，2019，6(6)：10700-10714．

[28] 李杨，刘伟佳，文福拴，等．电转气设备与燃气机组的联合竞价策略[J]．电力系统自动化，2017，41(1)：9-17．
LI Yang，LIU Weijia，WEN Fushuan，et al．Combined bidding strategies between power-to-gas facilities and natural gas generating units[J]．Automation of Electric Power Systems，2017，41(1)：9-17(in Chinese)．

[29] HEUILLET A，COUTHOUIS F，D ÍAZ-RODR ÍGUEZ N．Collective eXplainable AI：explaining cooperative strategies and agent contribution in multiagent reinforcement learning with shapley values[J]．IEEE computational intelligence magazine，2022，17(1)：59-71．

[30] WANG Tianhao，RAUSCH J，ZHANG Ce，et al．A principled approach to data valuation for federated learning[M]//YANG Qiang，FAN Lixin，Yu Han．Federated Learning-Privacy and Incentive．Berlin：Springer，2020：153-167．

[31] 刘林，祁兵，李彬，等．面向电力物联网新业务的电力通信网需求及发展趋势[J]．电网技术，2020，44(8)：3114-3128．
LIU Lin，QI Bing，LI Bin，et al．Requirements and developing trends of electric power communication network for new services in electric internet of things [J]．Power System Technology，2020，44(8)：3114-3128(in Chinese)．

[32] 胡江溢，祝恩国，杜新纲，等．用电信息采集系统应用现状及发展趋势[J]．电力系统自动化，2014，38(2)：131-135．
HU Jiangyi，ZHU Enguo，DU Xingang，et al．Application status and development trend of power consumption information collection system[J]．Automation of Electric Power Systems，2014，38(2)：131-135(in Chinese)．

[33] 刘艺璇，陈红，刘宇涵，等．联邦学习中的隐私保护技术[J]．软件学报，2022，33(3)：1057-1092．
LIU Yixuan，CHEN Hong，LIU Yuhan，et al．Privacy-preserving techniques in federated learning [J]．Journal of Software，2022，33(3)：1057-1092(in Chinese)．

[34] 孙静，彭勇刚，倪旖旎，等．基于改进联邦学习算法的电力负荷预测方法[J]．高电压技术，2024，50(7)：3039-3049．
SUN Jing，PENG Yonggang，NI Yini，et al．Power load forecasting method based on improved federated learning algorithm[J]．High Voltage Engineering，2024，50(7)：3039-3049(in Chinese)．

[35] 李洪裕，董骁翀，王新迎，等．考虑数据隐私保护的可再生能源场景生成框架[J]．电网技术，2023，47(9)：3690-3698．
LI Hongyu，DONG Xiaochong，WANG Xinying，et al．Framework for renewable energy scenario generation considering data privacy-preservation[J]．Power System Technology，2023，47(9)：3690-3698(in Chinese)．

[36] 易叶青，易颖杰，刘云如，等．面向电力物联网流数据的一种具有隐私保护的 KNN 查询方法[J]．计算机应用研究，2024，41(4)：1198-1207．
YI Yeqing，YI Yingjie，LIU Yunru，et al．Privacy-preserving KNN query method for streaming data in power internet of things[J]．Application Research of Computers，2024，41(4)：1198-1207(in Chinese)．

[37] 朵春红，杨甜，张铭泉，等．面向配电网分布式终端的安全接入认证方案设计[J]．电网技术，2023，47(11)：4778-4790．
DUO Chunhong，YANG Tian，ZHANG Mingquan，et al．Design of secure access authentication scheme for distributed terminals in distribution networks[J]．Power System Technology，2023，47(11)：4778-4790(in Chinese)．

[38] 郭少勇，刘岩，邵苏杰，等．新型电力系统数据跨域流通泛安全边界防护技术[J]．电力系统自动化，2024，48(6)：96-111．
GUO Shaoyong，LIU Yan，SHAO Sujie，et al．Ubiquitous security boundary protection technology for cross-domain data circulation in new power system[J]．Automation of Electric Power Systems，2024，48(6)：96-111(in Chinese)．

[39] 陈学斌，任志强，张宏扬．联邦学习中的安全威胁与防御措施综述[J]．计算机应用，2024，44(6)：1663-1672．
CHEN Xuebin，REN Zhiqiang，ZHANG Hongyang．Review on security threats and defense measures in federated learning[J]．Journal of Computer Applications，2024，44(6)：1663-1672(in Chinese)．

[40] MCMAHAN H B，RAMAGE D，TALWAR K，et al．Learning differentially private recurrent language models[C]//ICLR 2018．Vancouver：ICLR，2018．

[41] JORGENSEN Z，YU Tian，CORMODE G．Conservative or liberal? personalized differential privacy[C]// Proceedings of the IEEE 31st International Conference on Data Engineering．Seoul：IEEE，2015：1023-1034．

[42] ZHANG Yuping，QU Youyang，GAO Longxiang，et al．GPDP：game-enhanced personalized differentially private smart community[C]//Proceedings of the 2021 IEEE International Conferences on Internet of Things and IEEE Green Computing and Communications and IEEE Cyber，Physical and Social Computing and IEEE Smart Data and IEEE Congress on Cybermatics．Melbourne：IEEE，2021：

238-243.

[43] 何文竹，彭长根，王毛妮，等. 面向结构化数据集的敏感属性识别与分级算法[J]. 计算机应用研究，2020，37(10)：3077-3082.
HE Wenzhu，PENG Changgen，WANG Maoni，et al. Sensitive attribute recognition and classification algorithm for structure dataset[J] . Application Research of Computers，2020，37(10)：3077-3082(in Chinese).

[44] 刘清蝉，钟尧，林聪，等. 基于稳健非负矩阵分解的用电数据清洗和插补[J]. 电网技术，2024，48(5)：2103-2112.
LIU Qingchan，ZHONG Yao，LIN Cong，et al. Electricity consumption data cleansing and imputation based on robust nonnegative matrix factorization[J]. Power System Technology，2024，48(5)：2103-2112(in Chinese).

[45] SU Zhou，WANG Yuntao，LUAN T H，et al. Secure and efficient federated learning for smart grid with edge-cloud collaboration[J] . IEEE Transactions on Industrial Informatics，2022，18(2)：1333-1344.

[46] WANG Guan，DANG C X Q，ZHOU Ziye. Measure contribution of participants in federated learning[C]// Proceedings of the IEEE International Conference on Big Data(Big Data). Los Angeles：IEEE，2019：2597-2604.

[47] SHAPLEY L. A value for n-person games[M]//KUHN H，TUCKER A. Contributions to the Theory of Games II. Princeton：Princeton University Press，1953：307-317.

[48] DUBEY P. On the uniqueness of the Shapley value [J]. International Journal of Game Theory，1975，4(3)：131-139.

[49] UDELL M，TOWNSEND A. Why are big data matrices approximately low rank?[J] . SIAM Journal on Mathematics of Data Science，2019，l(1)：144-160.

王路遥

在线出版日期：2025-03-05。
收稿日期：2024-08-19。

作者简介：

王路遥(1998)，男，博士研究生，主要研究方向为智能配用电、数据安全，120242101039@ncepu.edu.cn；

龚钢军(1974)，男，博士，教授，博士生导师，主要研究方向为智能配用电、能源电力信息安全、数据安全，gong@ncepu.edu.cn；

*通信作者：杨佳轩(1997)，男，博士研究生，主要研究方向为综合能源系统、能源电力信息安全，yangjx@ncepu.edu.cn。

(责任编辑　李泽荣)