DOI：10.13334/j.0258-8013.pcsee.242499 文章编号：0258-8013 (2026) 05-1928-14 中图分类号：TM 71 文献标识码：A

面向用户用电行为检测的协同优化联邦学习框架、数据二维分解策略和隐私优化博弈模型

王路遥[1]，龚钢军[1]，杨佳轩[1*]，陆俊[1]，杨超[2]，刘礼[1]，杨俊峰[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)

Collaborative Optimization Federated Learning Framework, Data Two-dimensional Decomposition Strategy, and Privacy Optimization Game Model for User Electricity Behavior Detection

WANG Luyao[1], GONG Gangjun[1], YANG Jiaxuan[1*], LU Jun[1], YANG Chao[2], LIU Li[1], YANG Junfeng[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: Data barriers exist in power metering systems, hindering cross-entity data sharing and integration, which leads to low accuracy in data-driven identification of abnormal electricity consumption behaviors. While federated learning can alleviate data silos, traditional methods struggle to meet the diverse needs of different entities regarding anomaly features. Additionally, issues such as insufficient privacy protection and lack of incentive mechanisms persist. To address these limitations, this study proposes a collaborative optimization federated learning framework that balances privacy and utility. The framework incorporates several key innovations. First, it employs wavelet decomposition to segregate user electricity data into approximation and detail coefficients, separating common and individual characteristics as well as low-sensitivity and high-sensitivity data components. Then, an optimal differential privacy strategy is derived through a master-slave game model, incentivizing power entities to share high-value raw data while balancing privacy protection and data utility. Finally, based on the optimal personalized privacy budget obtained from the game mode, a hierarchical differential protection is applied to highly sensitive personalized models. This approach integrates a novel federated aggregation method, combining average weight parameters from power entities and magnitude weight parameters from metering centers. It enhances the local adaptability of power entity models and the global universality of metering center models while ensuring robust data privacy and security. Experimental results on an abnormal electricity usage detection dataset demonstrate the effectiveness of the proposed framework in improving detection accuracy while maintaining data privacy and utility.

KEY WORDS: federated learning; wavelet decomposition; stackelberg game; differential privacy; electricity theft detection

摘要：电力计量系统存在数据壁垒，制约了跨主体数据共享与整合，导致数据驱动的异常用电行为识别准确率不高。联邦学习虽能缓解数据孤岛，但传统方法难以满足各主体在异常特征上的差异化需求，且仍存在隐私保护不足与激励机制缺失的问题。因此，提出隐私-效用权衡的协同优化联邦学习框架。首先，电力主体利用小波分解将用户用电数据分解为逼近系数和细节系数，实现用户用电数据的共性和个性、低敏感和高敏感分离；其次，通过主从博弈的方式确定最优差分保护策略，在数据隐私保护和可用性的权衡下激励电力主体积极贡献高价值原始数据；再次，根据博弈后的最优个性隐私预算对高敏感的个性模型进行阶梯式差分保护，结合电力主体平均权参式、计量中心量级权参式的联邦聚合方式，在数据隐私安全的情况下提升电力主体模型的本地适应性和计量中心模型的全局泛用性；最后，通过对此联邦学习方法在异常用电行为检测数据集上进行实验分析，证明此方法的可行性。

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

关键词：联邦学习；小波分解；主从博弈；差分隐私；窃电检测

0　引言

电网损耗通常分为技术损失和非技术损失，电力用户的窃电行为是造成电网非技术性损失的主要原因[1]，窃电行为不仅对电力公司造成巨大的经济损失，而且对电网安全稳定运行造成巨大风险[2]。随着高级量测体系[3]的广泛应用，显著提高了用电数据的利用率和分辨率[4]，有力推动了面向数据的窃电检测技术的发展[5-6]。然而，大部分电力主体如小规模电力公司、新接入电网的负荷聚集商等，由于时间短、管辖用户少、采集数据存在噪声问题等原因往往没有足够的数据样本和特征[7-8]，因此，需要多主体共享数据来提升窃电检测的准确度。由于电网主体间受限于信息安全的约束无法进行数据共享，因此如何在不完全信息下实现数据要素融合以提升窃电检测准确率是当下研究的热点。联邦学习(federated learning，FL)作为隐私保护的关键技术之一[9]，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[10]。

一方面，传统联邦学习通过分布式训练、中心汇聚、下发迭代的方式，实现了联邦模型的构建。但统一的模型难以适应不同主体的个性化需求，因此，个性化联邦学习 pFed 逐渐作为新的研究热点[11]，通过分组联邦[12]、神经网络分层联邦[13]、函数优化联邦[14]、数据分层联邦[15]等方式实现主体间个性化模型的构建，提高各主体模型在本地场景下的适应能力。上述研究主要侧重于提升参与主体模型在本地的适应性，对全局模型的泛用性需求关注相对有限。在用电异常行为检测场景中，主体需构建符合本地用电特征的个性化检测模型，而计量中心则需建立具备广泛识别能力的泛用性全局模型，以覆盖多样化的用电行为类型。

另一方面，隐私安全性是联邦学习的核心问题，研究发现，攻击者可通过对参数发动逆向攻击来还原部分的敏感信息[16]。当前 FL 隐私增强主要是将经典机器学习隐私保护技术与 FL 相结合[17-18]。相比于有着高算力资源需求的传统密码学技术，简单灵活、易于部署且相对较少系统开销的差分隐私(differential privacy，DP)[19]技术更适合作为算力资源有限的电力场景隐私保护方法。传统基于 DP 的 FL 研究工作是每轮全局通信时各个主体为参数注入相同的扰动[20]，这将导致较大的隐私预算冗余。因此，在参数上注入个性化 DP 的方式逐渐作为新的研究方向。文献[21]提出一种个性化的语义敏感轨迹发布算法 TSDP；文献[22]提出一种两阶段基于个性化差分隐私的联邦学习算法。以上研究主要通过改变不同轮次或不同电力主体间的加扰程度来实现隐私保护的优化，尚未深入地从数据分量的角度来分离敏感分量与非敏感分量，从而对电力主体的敏感分量进行隐私保护以实现更加精确的隐私增强。

此外，目前大多数的联邦学习优化方法假设电力主体无条件参与，由于参与联邦学习存在数据整理、数据隐私泄露、计算和能源消耗等成本[23]，如何在电力市场下对大量的个性化主体进行有效激励是实现联邦异常用电行为检测实际部署的关键步骤之一。文献[24]构建了以参与训练数据集大小作为评估指标的非合作博弈模型。文献[25]根据数据规模、模型训练效果和训练成本等方面确定数据电力主体的贡献度，以此作为激励电力主体的依据。以上研究主要通过基于数据体量、模型性能、计算和能源消耗成本以确定贡献的方式，实现效益或权重的分配，未从隐私预算的角度引导参与主体根据实际隐私损失理性选取隐私预算，激励其积极参与并真实共享本地数据。

数据分解通常可以将反映数据波动和隐私高敏感的高频分量、反映数据趋势和低敏感的低频分量分离；针对高敏感分量而言，通过主从博弈能够有效解决数据隐私保护与数据利用效率之间难以权衡的问题，因此，本文提出一种隐私-效用权衡的协同优化联邦学习框架(collaborative optimization federated learning framework with privacy utility balance，PUB-COFL)，此方法将数据分解为个性分量和共享分量、高敏感和低敏感分量，性能上实现电力主体个性化建模、计量中心泛用性建模；安全上实现高敏感针对性阶梯式隐私增强。在中国北方地区多家供电公司共 7 000 组用电用户时序电能数据上进行验证试验，结果表明，所提框架在较好保护数据隐私的同时，提高了异常用电行为检测的准确率。本文的主要贡献如下：

1）提出基于小波变换的数据分解策略，以揭示用户用电行为的普遍性和特殊性，实现数据分量的共性和个性、低敏感和高敏感分离。

2）构建了隐私-效用权衡的协同优化联邦学习

框架，通过仅针对高敏感分量的精确化阶梯式加扰、电力主体和计量中心双侧的协同优化聚合，实现各主体敏感数据隐私安全下，异常用电检测模型准确性的提升。

3）提出了基于主从博弈的自适应隐私保护策略，通过博弈优化隐私预算分配，确保整体的隐私保护水平和数据利用效率，推动各主体积极参与高质量数据共享。

1 隐私-效用权衡的协同优化联邦学习框架

1.1 总体框架及定义

在电力市场中，各主体因地域、用户构成等因素，其异常用电行为特征差异显著；而计量中心需具备跨区域、多类型的异常用电监测能力，且市场环境下主体往往因自身利益放大隐私需求，导致模型准确率损失[26]。针对传统联邦学习框架存在全局模型难以适应主体个性特征、缺乏有效激励机制和传统差分隐私保护造成隐私预算冗余的问题，提出 PUB-COFL 框架，通过 PUB-COFL 实现异常用电行为辨识模型的构建，整体架构如图 1 所示。

PUB-COFL 框架主要分为 3 个部分：1）数据预处理。各电力主体采用离散小波变换(discrete wavelet transformation，DWT)对用户用电数据进行分解，分离出高频细节系数与低频逼近系数，从而区分个性与共性、高敏感与低敏感特征；2）本地训练与加扰。基于分解后的系数，主体分别训练个性模型向量与共性模型，以捕捉用电行为的波动与趋势特征。为在隐私保护与数据可用性之间实现高效权衡，主体与计量中心通过主从博弈确定最优隐私预算，并对个性模型向量进行自适应阶梯式差分加扰，从而在增强隐私保护的同时提升各方参与积极性。3）全局模型聚合。计量中心分别横向聚合个性模型与共性模型，并将共性模型作为预模型下发。当迭代达到设定轮次后，主体与计量中心分别对个性模型向量与共性模型进行纵向聚合，形成本地联合模型与全局联合模型，从而兼顾模型的个性化服务能力与全局泛化能力。为从理论上支撑上述框架，给出如下定义：

定义 1 个性化差分隐私[27]。相同电力主体的所有临近输入 $x \sim x' \in X$ 和经过随机函数 f 后得到相同的输出 $y \in Y$，如式(1)所示，则随机函数 f 满足个性化差分隐私 ε_i-DP。

$$\Pr[f_i(x)=y] \le \mathrm{e}^{\varepsilon_i} \Pr[f_i(x')=y] \tag{1}$$

式中 $\varepsilon_i>0$ 为电力主体 i 的隐私预算，用来量化隐私保护的程度，此隐私预算取决于主从博弈后的最优选择。

定义 2 Laplace 机制。对于随机函数 f 在真实数据 x 上的输出 $f(x)$，Laplace 机制通过在 $f(x)$上添加 Laplace 分布的噪声来产生随机化的查询结果。

$$\tilde{f}(x) = f(x) + f_{\text{Laplace}}(\sigma) \tag{2}$$

$$\sigma = \Delta s_f / \varepsilon_i \tag{3}$$

式中：$f_{\text{Laplace}}(\sigma)$ 为服从标准差为 σ 的 Laplace 分布；Δs_f 为灵敏度。

定义 3 阶梯式隐私增强。已知个性分量的灵敏度向量 $\Delta \boldsymbol{s}_{f_i} = (\Delta s_{f_{i_1}}, \Delta s_{f_{i_2}}, \cdots, \Delta s_{f_{i_j}}, \cdots, \Delta s_{f_{i_m}})$、个性分量隐私预算向量 $\tilde{\boldsymbol{\varepsilon}}_i = (\tilde{\varepsilon}_{i_1}, \tilde{\varepsilon}_{i_2}, \cdots, \tilde{\varepsilon}_{i_j}, \cdots, \tilde{\varepsilon}_{i_m})$、个性梯度向量 $\boldsymbol{g}_{i,\mathrm{p}} = (g_{i_1,\mathrm{p}}, g_{i_2,\mathrm{p}}, \cdots, g_{i_j,\mathrm{p}}, \cdots, g_{i_m,\mathrm{p}})$，阶梯式隐私增强定义如式(4)所示。

$$\hat{\boldsymbol{g}}_{i,\mathrm{p}} = \boldsymbol{g}_{i,\mathrm{p}} + f_{\text{Laplace}}(\Delta \boldsymbol{s}_{f_i} / \tilde{\boldsymbol{\varepsilon}}_i) \tag{4}$$

式中：$\hat{g}_{i,p} = (\hat{g}_{i_1,\mathrm{p}}, \hat{g}_{i_2,\mathrm{p}}, \cdots, \hat{g}_{i_j,\mathrm{p}}, \cdots, \hat{g}_{i_m,\mathrm{p}})$ 为隐私增强后的个性分量梯度向量；$\tilde{\varepsilon}_{i_j}$ 为经衰减因子作用后的

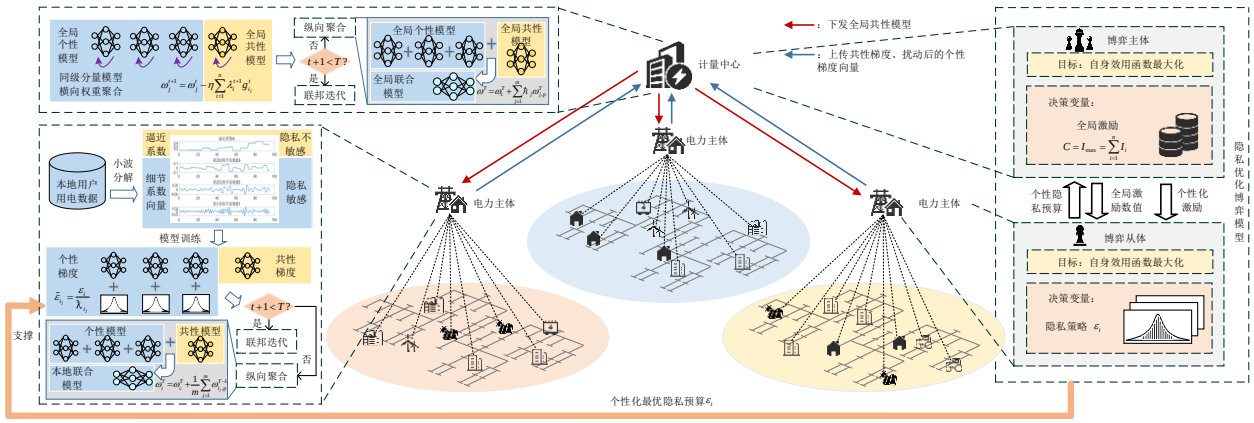

图 1 PUB-COFL 框架

Fig. 1 PUB-COFL framework

个性分量隐私预算，定义为

$$\tilde{\varepsilon}_{i_j}=\frac{\varepsilon_i}{\lambda_{i_j}} \tag{5}$$

式中：ε_i 为个性化隐私预算，取决于博弈电力主体 i 与计量中心博弈的均衡点；$\lambda_{i_j}\in[0,1]$ 为个性分量隐私衰减因子，取决于对应个性分量隐私敏感度，如式(6)所示。

$$\lambda_{i_j}=\frac{\varsigma_{i_j}}{\max(\varsigma_{i_j})} \tag{6}$$

式中 ς_{i_j} 为个性分量 j 的隐私敏感度。

定义 4　个性分量隐私敏感度。数据分量的突变或快速变化往往与特定的用电事件(如家用电器的开启或关闭)相关联，会揭示更多关于用户用电行为的信息，从而具有更高的隐私敏感度。因此，采用基于差值的能量矩 E_{i_j} 来量化个性分量的隐私敏感度 ς_{i_j}，如式(7)所示。

$$\varsigma_{i_j}=E_{i_j}=\sum_{k=1}^{K_j-1}|z_{k+1}-z_k|^2 \tag{7}$$

$$z_k=\frac{x_k-\min(x_k)}{\max(x_k)-\min(x_k)} \tag{8}$$

式中：x_k 为采样点在 k 处时的取值；z_k 为 x_k 归一化后的取值；K_j 为个性分量 j 的采样点数。

1.2　PUB-COFL 算法流程

本节从 PUB-COFL 的总体流程、本地更新和模型聚合 3 个阶段介绍 PUB-COFL 算法。

1）PUB-COFL 总体流程：计量中心向各电力主体下发全局模型 ω，n 个参与联邦学习的电力主体执行 PUB-COFL 本地更新流程，计量中心和电力主体执行 PUB-COFL 模型聚合流程，获得全局联合模型 ω^T 和本地联合模型 ω_i^T。

2）PUB-COFL 本地更新：首先，电力主体利用小波变换将原始用户用电数据分解为细节系数向量和逼近系数(数据分解详见 2 节)并进行归一化处理，如式(9)所示。

$$\boldsymbol{d}_i=\boldsymbol{d}_{i,\mathrm{p}}+d_{i,\mathrm{c}} \tag{9}$$

根据计量中心下发的预模型 ω^t，分别利用细节系数向量 $\boldsymbol{d}_{i,\mathrm{p}}=[d_{i_1,\mathrm{p}},d_{i_2,\mathrm{p}},...d_{i_j,\mathrm{p}},...d_{i_m,\mathrm{p}}]$ 和逼近系数 $d_{i,\mathrm{c}}$ 对预模型进行训练，形成本地个性模型向量 $\boldsymbol{\omega}_{i,\mathrm{p}}^{t+1}=[\omega_{i_1,\mathrm{p}}^{t+1},\omega_{i_2,\mathrm{p}}^{t+1},...,\omega_{i_j,\mathrm{p}}^{t+1},...,\omega_{i_m,\mathrm{p}}^{t+1}]$ 和共性模型 $\omega_{i,\mathrm{c}}^{t+1}$，个性梯度向量 $\boldsymbol{g}_{i,\mathrm{p}}^{t}=[g_{i_1,\mathrm{p}}^{t},g_{i_2,\mathrm{p}}^{t},\cdots,g_{i_j,\mathrm{p}}^{t},\cdots,g_{i_m,\mathrm{p}}^{t}]$ 和共性梯度 $g_{i,\mathrm{c}}^{t}$：

$$\omega_{i_j,\mathrm{p}}^{t+1}=\omega_i^t-\eta g_{i_j,\mathrm{p}}^t \tag{10}$$

$$\omega_{i,\mathrm{c}}^{t+1}=\omega_i^t-\eta g_{i,\mathrm{c}}^t \tag{11}$$

$$g_{i_j,\mathrm{p}}^t=\nabla F_i(\omega^t;d_{i_j,\mathrm{p}}) \tag{12}$$

$$g_{i,\mathrm{c}}^t=\nabla F_i(\omega^t;d_{i,\mathrm{c}}) \tag{13}$$

式中：F 为损失函数；η 为学习率。其次，对训练模型得到的个性梯度向量 $\boldsymbol{g}_{i,\mathrm{p}}^t$ 和共性梯度 $g_{i,\mathrm{c}}^t$ 进行裁剪，用以约束梯度的灵敏度，如式(14)、(15)所示。

$$\bar{g}_{i_j,\mathrm{p}}^t=g_{i_j,\mathrm{p}}^t/\max(1,\|g_{i_j,\mathrm{p}}^t\|_2/C) \tag{14}$$

$$\bar{g}_{i,\mathrm{c}}^t=g_{i,\mathrm{c}}^t/\max(1,\|g_{i,\mathrm{c}}^t\|_2/C) \tag{15}$$

式中 C 为裁剪阈值。

再次，计算个性梯度灵敏度向量 $\Delta\boldsymbol{s}_{\boldsymbol{g}_{i,\mathrm{p}}}^t=[\Delta s_{g_{i_1,\mathrm{p}}}^t,\Delta s_{g_{i_2,\mathrm{p}}}^t,...,\Delta s_{g_{i_j,\mathrm{p}}}^t,...,\Delta s_{g_{i_m,\mathrm{p}}}^t]$。

$$\Delta s_{g_{i_j,\mathrm{p}}}^t=\max_{d_i,d_i'}\|g_{i_j,\mathrm{p}}^t(d_i)-g_{i_j,\mathrm{p}}^t(d_i')\|\le 2C \tag{16}$$

式中 d_i 与 d_i' 为临近数据集。

其次，通过主从博弈的方式确定个性化隐私预算 ε_i^t(博弈详见 3 节)，然后对裁剪后的个性梯度向量 $\bar{\boldsymbol{g}}_{i,\mathrm{p}}^t=[\bar{g}_{i_1,\mathrm{p}}^t,\bar{g}_{i_2,\mathrm{p}}^t,\cdots,\bar{g}_{i_j,\mathrm{p}}^t,\cdots,\bar{g}_{i_m,\mathrm{p}}^t]$ 施加个性化阶梯式 Laplace 噪声 $f_{\mathrm{Laplace}}[\ell\,|\,\Delta s_{g_{i_j,\mathrm{p}}}^t/(\varepsilon_i^t/\lambda_{i_j})]$(如式(17)所示)，实现对不同电力主体、不同程度敏感分量的差异化分层隐私增强。其中 $\lambda_{i_j}\in[0,1]$ 为个性分量隐私衰减因子，ℓ 为服从 Laplace 的随机变量取值。

$$\hat{g}_{i_j,\mathrm{p}}^t=\hat{g}_{i_j,\mathrm{p}}^t+f_{\mathrm{Laplace}}(\ell\,|\,\frac{\lambda_{i_j}\Delta s_{g_{i_j,\mathrm{p}}}^t}{\varepsilon_i^t}) \tag{17}$$

$$f_{\mathrm{Laplace}}(\ell|\frac{\lambda_{i_j}\Delta s_{g_{i_j,\mathrm{p}}}^t}{\varepsilon_i^t})=\frac{\varepsilon_i^t}{2\lambda_{i_j}\Delta s_{g_{i_j,\mathrm{p}}}^t}\exp(-\frac{\varepsilon_i^t}{\lambda_{i_j}\Delta s_{g_{i_j,\mathrm{p}}}^t}|\ell|) \tag{18}$$

最后，将扰动后的个性梯度向量 $\hat{\boldsymbol{g}}_{i,\mathrm{p}}^t=[\hat{g}_{i_1,\mathrm{p}}^t,\hat{g}_{i_2,\mathrm{p}}^t,\cdots,\hat{g}_{i_j,\mathrm{p}}^t,\cdots,\hat{g}_{i_m,\mathrm{p}}^t]$ 和未扰动的共性梯度 $\bar{g}_{i,\mathrm{c}}^t$ 上传至计量中心。

3）PUB-COFL 模型聚合。计量中心分别对个性模型向量 $\boldsymbol{\omega}_{\mathrm{p}}^{t+1}=[\omega_{1,\mathrm{p}}^{t+1},\omega_{2,\mathrm{p}}^{t+1},\cdots\omega_{j,\mathrm{p}}^{t+1},\cdots\omega_{m,\mathrm{p}}^{t+1}]$ 和全局共性模型 $\omega_{\mathrm{c}}^{t+1}$ 进行同级分量横向权重聚合，如式(19)、(20)所示。

$$\omega_{j,\mathrm{p}}^{t+1}=\omega_{j,\mathrm{p}}^t-\eta\sum_{i=1}^{n}\lambda_i^{t+1}\hat{g}_{i_j,\mathrm{p}}^t \tag{19}$$

$$\omega_{\mathrm{c}}^{t+1}=\omega_{\mathrm{c}}^t-\eta\sum_{i=1}^{n}\lambda_i^{t+1}\bar{g}_{i,\mathrm{c}}^t \tag{20}$$

式中：λ_i^{t+1}为聚合权重，由电力主体在联邦过程中的贡献度决定；在 t=0 时，$\omega_{\mathrm{p}}^t=\omega_{\mathrm{c}}^t=\omega$；当$t+1<T$时，计量中心将全局共性模型$\omega_{\mathrm{c}}^{t+1}$作为下一轮次联邦训练的预模型下发至各电力主体，以此进行迭代训练；当 t+1=T 时，计量中心下发全局共性模型ω_{c}^T至各电力主体，并对全局个性模型向量$\boldsymbol{\omega}_{\mathrm{p}}^T=(\omega_{1,\mathrm{p}}^T,\omega_{2,\mathrm{p}}^T,\cdots,\omega_{j,\mathrm{p}}^T,\cdots,\omega_{m,\mathrm{p}}^T)$和全局共性模型$\omega_{\mathrm{c}}^T$进行纵向权重集成式聚合，形成全局联合模型$\omega^T$，由此在保证计量中心侧模型准确性的同时，提高了其泛用能力，如式(21)所示。

$$\omega^T=\omega_{\mathrm{c}}^T+\sum_{j=1}^{m}\hbar_j\omega_{j,\mathrm{p}}^T \tag{21}$$

式中$\hbar_j$为全局个性模型聚合衰减因子，依据不同个性分量与共性分量的量级之比来逐级衰减聚合权重，以平衡个性模型在全局联合模型中的影响，如式(22)所示。

$$\hbar_j=\sum_{i=1}^{n}\tilde{\lambda}_i\rho_{i_j} \tag{22}$$

式中：ρ_{i_j}为电力主体 i 的个性分量 j 的极差与共性分量的极差在不同轮次下比值的平均，由电力主体向计量中心提供；$\tilde{\lambda}_i$为电力主体 i 在不同轮次下的平均聚合权重。

$$\rho_{i_j}=\frac{1}{T}\sum_{t=1}^{T}\frac{\Delta x_{i_j,\mathrm{p}}^t}{\Delta x_{i,\mathrm{c}}^t}=\frac{1}{T}\sum_{t=1}^{T}\frac{\|x_{i_j,\mathrm{p}}^t\|_\infty-\|x_{i_j,\mathrm{p}}^t\|_{-\infty}}{\|x_{i,\mathrm{c}}^t\|_\infty-\|x_{i,\mathrm{c}}^t\|_{-\infty}} \tag{23}$$

$$\tilde{\lambda}_i=\frac{1}{T}\sum_{t=1}^{T}\lambda_i^t \tag{24}$$

式中$x_{i_j,\mathrm{p}}^t$、$x_{i,\mathrm{c}}^t$分别为在第 t 轮联邦训练下，电力主体 i 的个性分量 j 采样序列与共性分量采样序列。

同理，电力主体将本地个性模型向量和全局共性模型进行纵向平均集成式聚合，形成本地联合模型ω_i^T，提升本地模型的个性化服务能力，如式(25)所示。

$$\omega_i^T=\omega_{\mathrm{c}}^T+\frac{1}{m}\sum_{j=1}^{m}\omega_{i_j,\mathrm{p}}^{T-1} \tag{25}$$

2 基于 DWT 的用户用电数据二维分解策略

为满足电力市场各主体对模型可用性与数据安全性的双重需求，本文提出一种基于 DWT 的用户用电数据处理方法。该方法利用小波变换在时频域的多尺度分析能力[28]，有效捕捉非平稳用电数据的多层次特征，以提升模型准确性；同时，通过对信号进行频域分解，分离出可共享的全局特征与高隐私风险的局部特征，从而为针对性隐私保护提供基础。具体而言，采用 DWT 将原始信号 $s(t)$逐层分解为高频细节系数 D 与低频逼近系数 A，以实现对用电数据特征的结构化提取，分解过程如下：

$$s(t)=C(t)+P(t)=A_\kappa+\sum_{j=1}^{\kappa}D_j \tag{26}$$

式中κ为 DWT 分解层数。

小波分解层数决定了信号分析的深度，各层分解结果对特征提取具有不同影响[29]。为在全局趋势表征与细节变化捕捉之间取得平衡，本文设定κ=3，分解原理如图 2 所示。最终，细节系数 $P(t)$由 D_1、D_2、D_3 构成，逼近系数由 A_3 构成。

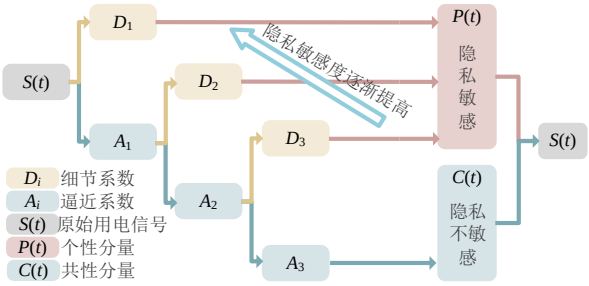

图 2 基于 DWT 的数据分解原理

Fig. 2 Principle of data decomposition based on DWT

原始信号为采样点为 96 的用户 1 天用电数据，分解示例如图 3 所示。下文分别从型态特征和隐私需求两个维度展开分析：

1）型态特征：①逼近系数 A 与原始用户用电数据有着相近的总体趋势；②细节系数 D_1、D_2、D_3 分别从不同分辨率刻画信号的局部波动；③各系数在量级上差异显著，且频率越高，量级越小。

2）隐私需求：①逼近系数(低频)主要反映由工休、昼夜等宏观因素驱动的长期趋势与周期变化[30]，属于共性特征，不易泄露个体行为，无需额外隐私增强；②细节系数(高频)则包含短期波动与

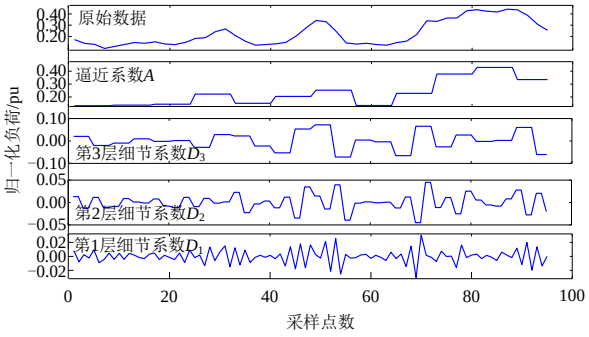

图 3 基于 DWT 的数据分解示例

Fig. 3 Example of data decomposition based on DWT

瞬变信号，常关联用户具体行为、生活习惯及电器使用模式等敏感信息[31-32]，极易泄露用户隐私，需进行隐私增强处理。

3　基于主从博弈的自适应隐私优化模型

本节在面向电力市场的联邦学习框架下，针对数据隐私保护与数据利用效率之间难以权衡的问题，构建了基于主从博弈的自适应隐私优化模型。通过博弈来优化隐私预算分配，确保整体的隐私保护水平和数据利用效率，推动电力主体积极参与数据共享，提高全局模型泛化能力，具体如图 4 所示。

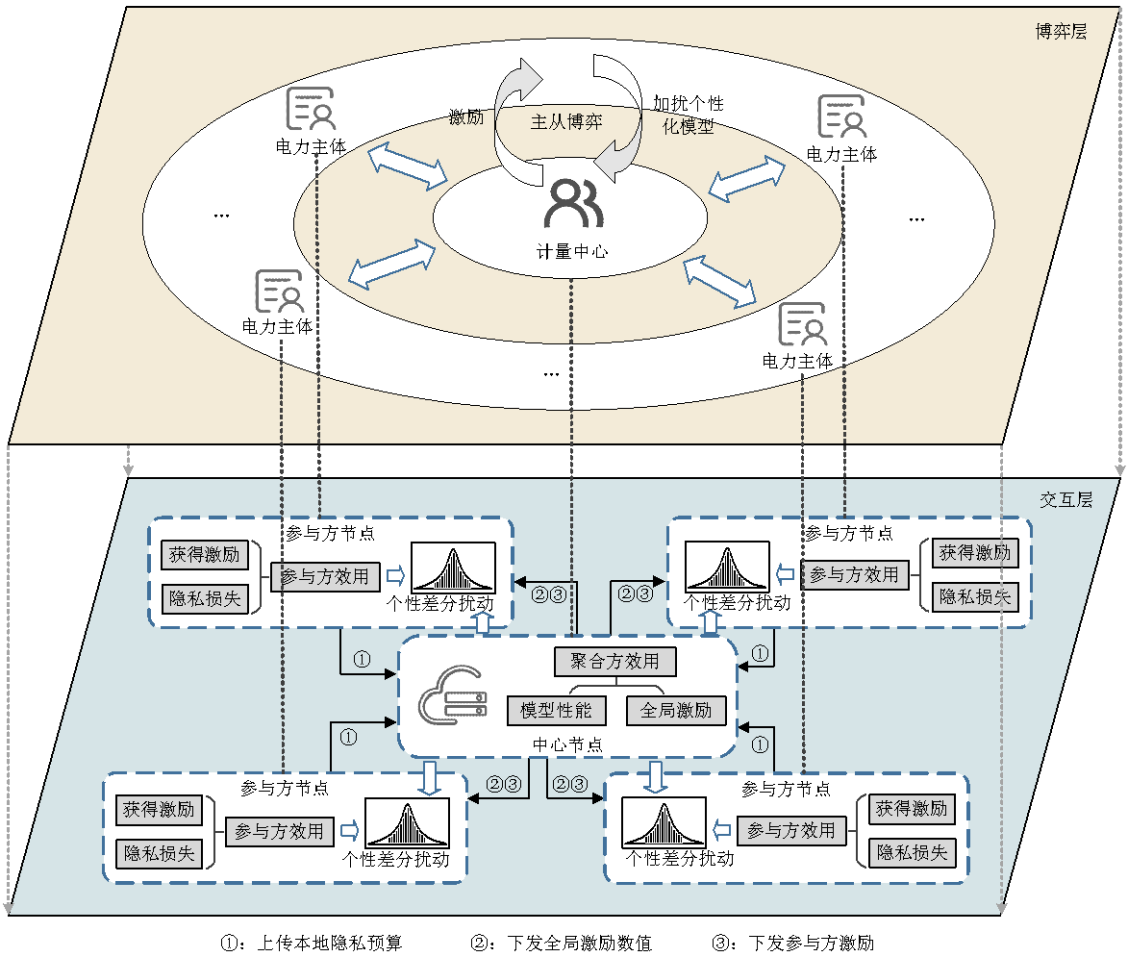

图 4　基于主从博弈的自适应隐私优化模型

Fig. 4　Adaptive privacy optimization model based on master-slave game theory

3.1　场景与假设基础

在电力市场数据交互场景下，各主体(包括中心节点与参与方)需遵循既定规范，其约束机制可有效抑制恶意攻击及破坏行为。基于此，本文采用“诚实但好奇”行为假设[33]：各主体均遵守协议与流程，不主动破坏系统，但存在窥探他人本地数据或信息的动机。在此假设下，主体因受规则约束而表现“诚实”，又因数据价值驱动而表现“好奇”，进而在既有安全框架内以理性方式追求自身利益最大化。为便于模型构建与分析，进一步假设所有参与主体均为完全理性的，且信息完全。

3.2　主从博弈模型

主从博弈以计量中心作为领导者设定全局激励，电力主体根据全局激励和自身隐私损失成本选择合适的隐私预算；计量中心在电力主体选择的隐私预算下，根据收益和成本选择合适的全局激励，从而在隐私保护和数据贡献之间达到平衡。通过多轮迭代，最终达到 Stackelberg 均衡。

1）计量中心效用定义。

①计量中心收益：在已知上传模型梯度有扰动的情况下，计量中心更希望得到电力主体加扰程度更低、性能更好的全局模型。考虑到隐私预算和模型性能成正相关，随着隐私预算增大，差分加扰程度减小的变化量逐渐变小，模型性能提升率逐渐变小并最终趋近于 0，即当隐私预算趋近无穷时，模型收益收敛于一个定值，满足边际递减性和收敛

性。因此，全局模型收益 E^{earn} 定义为

$$E^{\text{earn}}=\alpha_1\sum_{i=1}^{n}\lambda_i(1-\mathrm{e}^{-\alpha_2\varepsilon_i}) \tag{27}$$

式中：α_1, α_2>0；ε_i>0 为电力主体 i 所选择的隐私预算；$\lambda_i\in(0,1)$为电力主体 i 的联邦聚合权重。

②计量中心成本：此成本为本轮联邦计量中心对所有电力主体的全局激励 $I_{\max}$。

$$C^{\text{cost}}=I_{\max}=\sum_{i=1}^{n}I_i \tag{28}$$

式中 I_i 为计量中心对电力主体 i 的激励，为实现博弈的合理性，I_i>0。

③计量中心效用：定义为全局模型收益减去全局激励，如式(29)所示。

$$U=E^{\text{earn}}-C^{\text{cost}}=\alpha_1\sum_{i=1}^{n}\lambda_i(1-\mathrm{e}^{-\alpha_2\varepsilon_i})-\sum_{i=1}^{n}I_i \tag{29}$$

2）电力主体效用定义。

①电力主体收益：在已知全局激励 $I_{\max}$ 的情况下，考虑到隐私预算与加扰程度成负相关，电力主体收益 E_i^{earn} 定义为计量中心对电力主体的激励 I_i，如式(30)所示。

$$E_i^{\text{earn}}=I_i=I_{\max}\frac{\lambda_i\varepsilon_i}{\sum_{j=1}^{n}\lambda_j\varepsilon_j} \tag{30}$$

②电力主体成本：为满足本文所提的联邦学习框架，首先在拉普拉斯机制的 DP 下定义电力主体隐私损失。假设电力主体相邻数据集 x 和 x' 的查询结果为 $f(x)$ 和 $f(x')$，且满足 $|f(x)-f(x')|\le\Delta s_f$，将其代入拉普拉斯概率密度函数即可推出输出为 $y\in Y$ 的概率分布分别为 Pr[$f(x)$=y]和 Pr[$f(x')=y$]，如式(31)、(32)所示。

$$\Pr[f(x)=y]=\frac{1}{2b}\mathrm{e}^{-\frac{|y-f(x)|}{b}} \tag{31}$$

$$\Pr[f(x')=y]=\frac{1}{2b}\mathrm{e}^{-\frac{|y-f(x')|}{b}} \tag{32}$$

式中 $b=\Delta s_f/\varepsilon_i$。由库尔贝克-莱布勒(Kullback-Leibler，KL)散度衡量 2 个分布 P 和 Q 间的距离，KL 散度如式(33)所示。

$$D(P\|Q)=\mathop{\mathrm{E}}_{p\sim P}(\ln\frac{\Pr[P=p]}{\Pr[Q=q]}) \tag{33}$$

由此定义隐私损失函数 L，再将 Pr[$f(x)=y$]和 Pr[$f(x')=y$]代入 L 中[34]，如式(34)所示。

$$L=\ln(\frac{\Pr[f(x)=y]}{\Pr[f(x')=y]})=\ln(\exp(\frac{|y-f(x')|-|y-f(x)|}{b}))=\frac{|y-f(x')|-|y-f(x)|}{b}=\varepsilon_i\frac{|y-f(x')|-|y-f(x)|}{\Delta s_f} \tag{34}$$

由$[|y-f(x')|-|y-f(x)|]/\Delta s_f=\phi\le1$可知，隐私损失的最大值在 Laplace 机制下被ε_i 所约束，满足ε_i-DP 条件，如式(35)所示。

$$L_{\max}\le\varepsilon_i \tag{35}$$

由此可知，在该定义下隐私损失与隐私预算成线性关系，考虑到不同电力主体对本地数据的隐私价值评估不同，故电力主体隐私成本定义如下：

$$C_i^{\text{cost}}=\varphi_i\phi_i\varepsilon_i \tag{36}$$

式中：$\varphi_i>0$为电力主体隐私估值参数；$0<\phi_i<1$为隐私损失参数，满足$\phi_i=L_{\max}/\varepsilon_i$。

③电力主体效用：定义为电力主体收益减去电力主体成本，如式(37)所示。

$$U_i=E_i^{\text{earn}}-C_i^{\text{cost}}=I_{\max}\frac{\lambda_i\varepsilon_i}{\sum_{j=1}^{n}\lambda_j\varepsilon_j}-\varphi_i\phi_i\varepsilon_i \tag{37}$$

3.3 主从博弈求解策略

为实现在既定全局激励下计算电力主体最佳隐私预算的目的。首先进行电力主体效用函数 U_i 对隐私预算ε_i一阶偏导的求解，如式(38)所示。

$$\frac{\partial U_i}{\partial\varepsilon_i}=I_{\max}\lambda_i\frac{\sum_{j=1}^{n}\lambda_j\varepsilon_j-\lambda_i\varepsilon_i}{(\sum_{j=1}^{n}\lambda_j\varepsilon_j)^2}-\varphi_i\phi_i \tag{38}$$

考虑到只有电力主体效用大于 0 才可能参与联邦，如式(39)所示。

$$U_i=I_{\max}\frac{\lambda_i\varepsilon_i}{\sum_{j=1}^{n}\lambda_j\varepsilon_j}-\varphi_i\phi_i\varepsilon_i>0 \tag{39}$$

化简得到：

$$\frac{I_{\max}\lambda_i}{\sum_{j=1}^{n}\lambda_j\varepsilon_j}-\varphi_i\phi_i>0 \tag{40}$$

可得 $\lim\limits_{\varepsilon_i\to0}\partial U_i/\partial\varepsilon_i>0$。因此，由 $\varepsilon_i\to0$ 和 $\varepsilon_i\to\infty$ 时 $\partial U_i/\partial\varepsilon_i$ 的极限 $\lim\limits_{\varepsilon_i\to0}\partial U_i/\partial\varepsilon_i>0$，$\lim\limits_{\varepsilon_i\to\infty}\partial U_i/\partial\varepsilon_i<0$ 可知 $\partial U_i/\partial\varepsilon_i$ 一定与横坐标轴相交。

求解电力主体效用函数 U_i 对隐私预算 ε_i 的二阶偏导，如式(41)所示。

$$\frac{\partial^2 U_i}{\partial \varepsilon_i^{\,2}} = -2I_{\max}\lambda_i^{\,2}\frac{\sum_{j=1}^{n}\lambda_j\varepsilon_j - \lambda_i\varepsilon_i}{(\sum_{j=1}^{n}\lambda_j\varepsilon_j)^3} < 0 \tag{41}$$

由 $\partial^2 U_i/\partial\varepsilon_i^{\,2}<0$ 可知，$\partial U_i/\partial\varepsilon_i$ 在 $\varepsilon_i\in[0,\infty)$ 内恒递减，结合上诉条件可得 $\partial U_i/\partial\varepsilon_i$ 与横坐标有且仅有 1 个交点，即电力主体效用函数 U_i 存在唯一极大值，且该极大值不在 ε_i 取值范围的边界处，呈现出严格的凹函数特性，即电力主体可通过此博弈求出最优隐私预算 $\varepsilon_i^{*}\in(0,\infty)$ 使得电力主体收益最大化。

令 $\partial U_i/\partial\varepsilon_i=0$ 即可求得在既定全局激励下的电力主体选择隐私预算最优解 ε_i^{*}，如式(42)所示。

$$\varepsilon_i^{*} = \sqrt{\frac{\varphi_i\phi_i I_{\max}\sum_{j\neq i}\lambda_j\varepsilon_j}{\lambda_i}} - \frac{1}{\lambda_i}\sum_{j\neq i}\lambda_j\varepsilon_j \tag{42}$$

为实现在既定电力主体最优隐私预算 ε_i^{*} 下，计量中心计算最优全局激励的目的，首先求解计量中心效用函数 U 对全局激励 $I_{\max}$ 的一阶偏导。为简化计算，令 $-\alpha_2\sqrt{\varphi_i\phi_i I_{\max}\sum_{j\neq i}\lambda_j\varepsilon_j/\lambda_i}=\theta_i$，$(-\alpha_2/\lambda_i)\cdot\sum_{j\neq i}\lambda_j\varepsilon_j=\vartheta_i$，其中 $\theta_i<0$，$\vartheta_i<0$。式(42)被简化为

$$\varepsilon_i^{*} = -\frac{1}{\alpha_2}(\theta_i\sqrt{I_{\max}} - \vartheta_i) \tag{43}$$

将式(43)代入计量中心效用函数 U 并求其一阶偏导数，如式(44)所示。

$$\frac{\partial U}{\partial I_{\max}} = -\frac{\alpha_1}{2\sqrt{I_{\max}}}\sum_{i=1}^{n}\lambda_i\theta_i \mathrm{e}^{\theta_i\sqrt{I_{\max}}+\vartheta_i} - 1 \tag{44}$$

过程同上，由 $I_{\max}\to 0$ 和 $I_{\max}\to\infty$ 时 $\partial U/\partial I_{\max}$ 的极限 $\lim_{I_{\max}\to 0}\partial U/\partial I_{\max}>0$ 和 $\lim_{I_{\max}\to\infty}\partial U/\partial I_{\max}<0$ 可知 $\partial U/\partial I_{\max}$ 一定与横坐标轴相交。

计量中心效用函数 U 对全局激励 $I_{\max}$ 的二阶偏导如式(45)所示。

$$\frac{\partial^2 U}{\partial I_{\max}} = \frac{\alpha_1}{4(I_{\max})^{3/2}}\sum_{i=1}^{n}\lambda_i\theta_i e^{\theta_i\sqrt{I_{\max}}+\vartheta_i} - \frac{\alpha_1}{4I_{\max}}\sum_{i=1}^{n}\lambda_i\theta_i^{2}e^{\theta_i\sqrt{I_{\max}}+\vartheta_i} < 0 \tag{45}$$

计量中心效用函数 $U(I_{\max})$ 为凹函数，存在唯一极大值点，且该极大值不在 $I_{\max}$ 取值范围的边界处，即计量中心可通过此博弈解得最优全局激励 $I_{\max}^{*}\in(0,\infty)$ 使得计量中心收益最大化。

4　算例分析

本节实验在异常用电行为检测数据集上详细分析 PUB-COFL 的可行性，验证数据分解的合理性、主从博弈的收敛性以及 PUB-COFL 的性能。

4.1　实验设置

实验配置了 Intel(R) Xeon(R) Bronze 3 140 CPU，64GB RAM 和 RTX4 090 的硬件环境，软件环境为 Python3.9 和 Pytorch1.12.0。实验数据集采用异常用电行为检测数据集，此数据集来源于我国北方地区多家供电公司共 7 000 组用电用户时序电能数据，采集周期为 1 个自然日，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、比例缩减、削峰、下调、随机削减、置零、移峰类用电行为样本。为尽可能模拟不同程度的参与主体个性特征差异，实验利用狄利克雷分布策略将完整数据集划分到 5 个主体，实现对各主体随机分配不同大小本地数据集和不同用电类型标签比例的目标[35]，并将狄利克雷分布值设置为不同的值，以验证在不同数据统计异质性下所提框架的性能。

实验用长短期记忆网络(long short-term memory，LSTM)模型对异常用电行为检测数据集进行训练。在模型训练过程中，所有数据集被随机分割，其中训练样本集和测试样本集比例为 7:3。为更好地测试全局模型在各种情况下的泛用性，中心节点测试样本均等地包含了所有异常用电行为。

4.2　数据分解合理性分析

为更好地分析不同频率分量的“共性”与“个性”。实验通过引入“相关性”来将“频率”和“共/个性”这 2 个概念进行关联，并设计了 2 种情况的对比：1）同类型用电行为下，低频分量间相关性与高频分量间相关性的对比(图 5)；2）不同类型用电行为下，低频分量间相关性与高频分量间相关性的对比(图 6)。为化简实验并使结果更明显，本节仅对逼近系数 A_3(低频分量)和细节系数 D_1(高频分量)进行分析。考虑到数据集中各类型用电行为数据有着较强的标签化特征且数据样本庞大，本节采用抽样的思想，仅对部分用户进行了实验；在同类型用电行为上仅对正常用户进行了实验，其余类型实验结果类似。

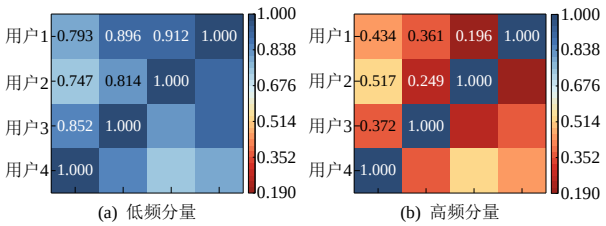

图 5 同类型用电行为下共性和个性分量 PCC

Fig. 5 PCC of common and individual components under the same type of electricity consumption behavior

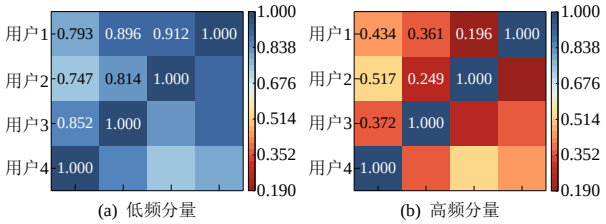

图 6 不同类型用电行为下共性和个性分量 PCC

Fig. 6 PCC of common and individual components under different types of electricity consumption behavior

图 5 示出了在同类型用电行为(正常用户)下，低频分量与高频分量的皮尔逊相关系数(Pearson correlation coefficient，PCC)。由图 5(a)可见，同类型用电行为低频分量间的 PCC 维持在 0.74 以上(PCC∈(–1,1)，且值越大相关性越强)，整体上呈现极强的相关性。而在图 5(b)中，同类型用电行为高频分量间的 PCC 相较于低频分量而言有不小的下降，其值主要在 0.2~0.5，整体上呈现弱相关性。这是因为低频分量捕获了用户用电行为中的普遍趋势，这些趋势在同类型用电行为上高度一致；而高频分量则包含了个体特有的波动和细节，即使在相同类型用电行为下，用户个体间相异的用电行为将导致细节和快速变化上的变异性增加。

图 6 示出了在不同类型用电行为下(包含正常用电行为和 6 种异常用电行为)，低频分量与高频分量的 PCC。由图 6(a)可见，不同类型用电行为低频分量间的 PCC 值主要集中在 0.2~0.6，整体上呈现弱相关状态。而在图 6(b)中，不同类型用电行为高频分量间的 PCC 主要集中在–0.4~0.4，分布跨越 0 值两侧，即分量间相关性方向存在不确定性，因此整体上不具备相关性。前者是因为即使在不同类型用电行为下，依然存在一些普遍趋势；后者是因为在不同类型用电行为下，用电行为特征的个体差异性被进一步放大，呈现波动特性的高频分量存在极大的不确定性。由上述实验结果可见，同/非同类型、低/高频与相关性呈现“象限化”关系(如图 7 所示)，从纵轴而言，随着分量的频率增加，相关性呈下降趋势；从横轴而言，随着用电行为类型增加，相关性呈下降趋势。

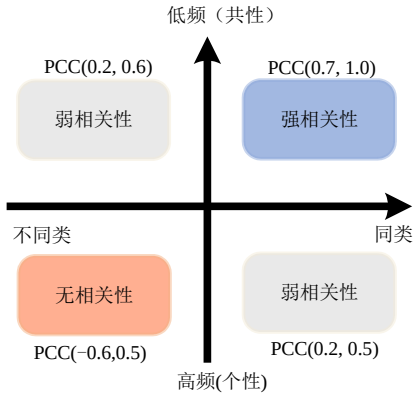

图 7 数据分量间相关性象限划分图

Fig. 7 Quadrant division diagram of correlation between data components

4.3 博弈收敛性分析

本节通过实验分析电力主体和计量中心效用函数的收敛性，验证了基于主从博弈的自适应隐私保护机制的可行性，如图 8 所示。为简化实验，分析电力主体效用 U_i 的收敛性时，假设电力主体估值参数与隐私损失参数为定值；分析计量中心效用 U 的收敛性时，假设电力主体均选择最优隐私预算。

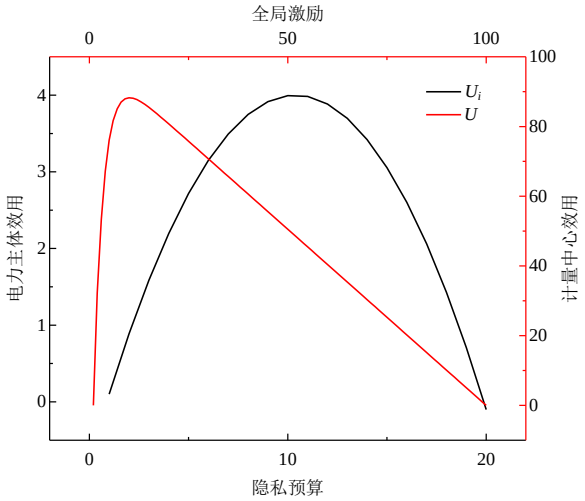

图 8 效用函数图

Fig. 8 Utility function diagram

对电力主体而言，当$\varepsilon_i<\varepsilon^*$时，效用 U_i 随着ε_i的增加而增加，这是因为当电力主体选择更大的隐私预算时将获得更多的激励，且所得到激励的增速大于隐私成本；当$\varepsilon_i=\varepsilon^*$时，电力主体效用 $U_i=U^*$达到极值，隐私成本与激励的增速相同；当$\varepsilon_i<\varepsilon^*$时，电力主体效用 U_i 随着ε_i 的增加而减少，隐私预算太大导致隐私风险急剧增加，在增速上激励难以弥补隐私成本。对计量中心而言，当 $I_{\max}<I^*_{\max}$ 时，效用 U 随着 $I_{\max}$ 的增加而急速增加，这是因为增加的激

励成本使得电力主体为提高自身收益而倾向于选择更大的隐私预算，从而有助于计量中心获取低扰动的模型参数以提高效用；当 $I_{max}=I^*_{max}$ 时，计量中心效用 $U_i=U^*$ 达到极值，激励成本与模型收益的增速相同；当 $I_{max}>I^*_{max}$ 时，计量中心效用 U 随着 I_{max} 的增加而逐步线性降低，这是因为满足边际效应的模型收益函数在激励成本 I_{max} 线性增加的过程中增速逐渐减低为 0，导致计量中心效用仅仅取决于激励成本。综上，效用函数 U_i 与 U 分别随着隐私预算和激励成本先增后减，呈现严格的凹函数特性，存在唯一极大值点 $U^*_i(\varepsilon^*_i)$和 $U^*(I^*_{max})$。

4.4　PUB-COFL 性能分析

实际电力场景中，不同电力主体所处的区域不同、所辖用户类型及比例不同等，导致其用电行为分布存在差异。考虑到相邻或具有相似经济、地理特征等区域之间的数据分布存在一定相似性；而在不同类型区域下，各电力主体间的数据分布存在较大差异，为了验证 PUB-COFL 方法在不同场景下的有效性和适应性，实验通过不同的数据分配策略来模拟上述实际场景。在不同非独立同分布(non-independently and identically distributed，Non-IID)程度下(其中 Non-IID 程度低和高分别对应狄利克雷分布值为 0.5 和 0.1)，分别从电力主体和计量中心的异常用电模型准确率上，将 PUB-COFL 与联邦平均、差分隐私联邦平均、联邦个性化、差分隐私联邦个性化算法进行对比分析。

1）联邦平均算法：计量中心将初始模型下发后，各电力主体利用本地数据进行本地模型训练，将参数上传至计量中心进行平均聚合，多轮迭代后得到全局模型。

2）差分隐私联邦平均算法：在联邦平均的基础上，融入差分隐私技术，即电力主体上传的参数中包含差分隐私噪声。

3）联邦个性化算法：先对自定义神经网络的基础层进行联邦平均算法，再对个性化层进行局部训练。

4）差分隐私联邦个性化算法：在联邦个性化算法的基础上，融入差分隐私技术，即电力主体上传的参数中包含差分隐私噪声。

实验结果对比如表 1 所示，首先对计量中心模型性能进行分析：当各主体数据集间的 Non-IID 程度较低时，联邦平均算法与联邦个性化算法的识别准确率分别为 93.24%和 92.83%，而在隐私增强的情况下，差分隐私联邦平均算法、差分隐私联邦个性化算法和 PUB-COFL 的识别准确率分别为 81.86%、81.67%和 83.81%，差分隐私联邦平均算法、差分隐私联邦个性化算法准确率非常接近且都低于 PUB-COFL，这是因为在低 Non-IID 情况下各主体间数据分布相似性高，其主体数据集“个性化”弱，因此全局模型差异不大，而在隐私增强上，差分隐私联邦平均算法与差分隐私联邦个性化算法采用统一的隐私预算，而 PUB-COFL 仅针对“个性”部分进行扰动，保留了大量原始共性部分；当各主体数据集间的 Non-IID 程度较高时，联邦平均算法与联邦个性化算法的识别准确率分别为 91.71%和 85.77%，差分隐私联邦平均算法、差分隐私联邦个性化算法和 PUB-COFL 的识别准确率分别为 76.92%、75.31%和 79.64%，原因是 PUB-COFL 在主要通过共性部分构建全局模型时考虑到了各主体的个性部分，使得全局模型在包含所有异常情况

表 1　联邦学习框架实验结果对比

Table 1　Comparison of experimental results of federated learning frameworks

算法	Non-IID 程度	识别准确率/%					
		主体 1	主体 2	主体 3	主体 4	主体 5	中心服务器
联邦平均算法	低	87.26	86.39	86.17	86.64	88.09	93.24
	高	82.37	82.45	82.42	83.12	81.78	91.71
差分隐私联邦平均算法	低	80.19	78.97	80.74	80.23	80.29	81.97
	高	72.28	71.16	73.38	72.17	71.73	76.92
联邦个性化算法	低	89.62	89.61	90.17	88.85	89.92	92.83
	高	87.31	88.85	87.42	86.97	86.71	85.77
差分隐私联邦个性化算法	低	82.83	82.06	81.33	82.49	83.32	81.67
	高	78.64	79.01	77.94	79.13	79.38	75.31
PUB-COFL (本文所提方法)	低	84.17	83.94	83.11	83.99	84.58	83.81
	高	80.93	82.05	81.29	80.73	80.74	79.64

的测试集上有着良好的泛用性。

其次，对各电力主体模型性能进行分析(以主体 1 为例)：当各主体数据集间的 Non-IID 程度较低时，联邦平均算法与联邦个性化算法的识别准确率分别为 87.26%和 89.62%，差分隐私联邦平均算法、差分隐私联邦个性化算法和 PUB-COFL 的识别准确率分别为 80.19%、82.83%和 83.81%；当各主体数据集间的 Non-IID 程度较高时，联邦平均算法与联邦个性化算法的识别准确率分别为 82.37%和 87.31%，差分隐私联邦平均算法、差分隐私联邦个性化算法和 PUB-COFL 的识别准确率分别为 72.28%、78.64%和 80.93%，这是因为个性化模型允许主体进行个性化优化，在数据分布差异不同的情况下，主体对全局模型进行不同程度的调整以更好地适应本地数据。

综上，PUB-COFL 在实现细粒度隐私增强的情况下，结合了传统联邦全局模型泛用性强和个性联邦主体模型适应本地特征的优点。对全局模型而言，PUB-COFL 相较于差分隐私联邦个性化算法有着更好的泛用性能；对主体本地模型而言，PUB-COFL 相较于差分隐私联邦平均算法有着对主体本地数据更好的适应性能，以上增益皆与主体间数据异构程度成正相关。

4.5 PUB-COFL 普适性分析

本节通过在爱尔兰数据集上进行对比分析，验证 PUB-COFL 在不同数据集上的普适性。此数据集包含爱尔兰 6 000 个用户 535 天的连续用电记录，采样间隔为 30 min。实验挑选 1 000 条用户的 1 日内用电数据，并进行了数据清洗和补充，形成 1 000 个正常用户 1 日内的用电数据样本，每条数据有 48 个采样点。在此样本上，通过基于数学建模表征[1]的方式生成包含 6 种异常用电行为等比分布的 6 000 条数据，将其与正常用户数据样本混合。

考虑到采集周期内数据采样点较少的问题，实验将 PUB-COFL 的数据分解层数设置为 2 层。为更好地测试全局模型在各种情况下的泛用性，中心节点测试样本均等地包含了所有异常用电行为。本节选择差分隐私联邦平均算法、差分隐私联邦个性算法与 PUB-COFL 进行对比分析，并在不同 Non-IID 程度下实验，以验证 PUB-COFL 方法在不同场景下的有效性和适应性，实验结果如表 2 所示。

表 2 联邦学习框架普适性实验分析

Table 2 Experimental analysis of the universality of federated learning framework

算法	Non-IID 程度	识别准确率/%					
		主体 1	主体 2	主体 3	主体 4	主体 5	中心服务器
差分隐私	低	78.39	79.52	80.44	79.35	78.16	80.24
联邦平均算法	高	69.46	70.55	72.72	73.02	69.43	76.90
差分隐私	低	81.22	79.94	81.93	82.82	81.25	80.52
联邦个性化算法	高	75.38	76.63	77.58	77.21	78.43	74.14
PUB-COFL	低	81.72	81.34	82.16	82.67	81.42	82.48
(本文所提方法)	高	75.33	77.65	76.84	78.45	77.21	77.57

首先对计量中心模型性能进行分析：当各主体数据集间的 Non-IID 程度较低时，差分隐私联邦平均算法、差分隐私联邦个性化算法和 PUB-COFL 的识别准确率分别为 80.24%、80.52%和 82.48%；当各主体数据集间的 Non-IID 程度较高时，差分隐私联邦平均算法、差分隐私联邦个性化算法和 PUB-COFL 的识别准确率分别为 76.90%、74.14%和 77.57%。其次，对各电力主体模型性能进行分析(以主体 1 为例)：当各主体数据集间的 Non-IID 程度较低时，差分隐私联邦平均算法、差分隐私联邦个性化算法和 PUB-COFL 的识别准确率分别为 78.39%、81.22%和 81.72%；当各主体数据集间的 Non-IID 程度较高时，差分隐私联邦平均算法、差分隐私联邦个性化算法和 PUB-COFL 的识别准确率分别为 69.46%、75.38%和 75.33%。

通过实验数据可知，主体数据集间的 Non-IID 程度较低时，相较于另外 2 个框架，PUB-COFL 的中心服务器模型性能更优，主体模型性能优于差分隐私联邦平均算法，与差分隐私联邦个性化算法接近；主体数据集间的 Non-IID 程度较高时，PUB-COFL 的中心服务器模型性能相较于差分隐私联邦个性化算法有较大提升，主体模型性能相比差分隐私联邦平均算法更优，与差分隐私联邦个性化算法接近。表明本文所提框架能有效提高中心服务器模型(全局模型)的泛用性和各主体模型(本地模型)的适应性，且本地适应性随数据采样点总体成正相关

趋势，这是因为小波分解在处理较长数据时，可以更精细地划分频率区间，使得分解出的细节分量能够更准确地捕捉其本地个性特征。由此可知，本文所提框架更适合于在一个周期内采样点数相对多的数据集。

5　结论

1）本文面向电力市场异常用电行为检测场景中个性化与泛化需求并存、数据共享与隐私保护需协同优化的问题，提出一种 PUB-COFL 框架。该框架引入基于小波变换的数据二维分解策略，实现了个性与共性、高敏感与低敏感特征的分离，进而支撑个性化本地建模与阶梯式隐私保护。

2）设计了一种计量中心与电力主体间的分量模型协同聚合机制，在保障模型泛用能力的同时提升了本地适应性能。

3）通过主从博弈动态优化隐私预算，并基于该预算对高频敏感分量实施了阶梯式差分加噪，从而在激励高质量数据共享的同时，显著降低了传统差分隐私中的加扰冗余。

4）仿真实验表明，所提框架在异常用电行为检测中，能够在实现更高效隐私保护的同时，显著提升全局模型的泛用性与本地模型的适应性。

参考文献

[1] 游文霞，梁皓，杨楠，等. 基于重采样和混合集成学习的不平衡窃电检测[J]. 电网技术，2024，48(2)：730-739.
YOU Wenxia，LIANG Hao，YANG Nan，et al. Class imbalanced electricity theft detection based on resampling and hybrid ensemble learning[J] . Power System Technology，2024，48(2)：730-739(in Chinese).

[2] 卿柏元，陈珏羽，李金瑾，等. 基于 CNN-LG 模型的窃电行为检测方法研究[J]. 湖南大学学报(自然科学版)，2022，49(8)：138-148.
QING Boyuan，CHEN Jueyu，LI Jinjin，et al. Research on detection method of electricity theft behavior based on CNN-LG model[J]. Journal of Hunan University(Natural Sciences)，2022，49(8)：138-148(in Chinese).

[3] RAZAVI R，GHARIPOUR A，FLEURY M，et al. A practical feature-engineering framework for electricity theft detection in smart grids[J]. Applied Energy，2019，238：481-494.

[4] 郭庆来，王博弘，田年丰，等. 能源互联网数据交易：架构与关键技术[J]. 电工技术学报，2020，35(11)：2283-2295.
GUO Qinglai，WANG Bohong，TIAN Nianfeng，et al. Data transactions in energy internet：architecture and key technologies[J]. Transactions of China Electrotechnical Society，2020，35(11)：2283-2295(in Chinese).

[5] 杨艺宁，张蓬鹤，夏睿，等. 基于 CT-GAN 的半监督学习窃电检测方法研究[J]. 湖南大学学报(自然科学版)，2024，51(6)：211-222.
YANG Yining，ZHANG Penghe，XIA Rui，et al. Research on semi-supervised learning detection method of electricity theft based on CT-GAN[J]. Journal of Hunan University (Natural Sciences)，2024，51(6)：211-222(in Chinese).

[6] 蒲天骄，张中浩，谈元鹏，等. 电力人工智能技术理论基础与发展展望(二)：自主学习与应用初探[J]. 中国电机工程学报，2023，43(10)：3705-3717.
PU Tianjiao，ZHANG Zhonghao，TAN Yuanpeng，et al. Theoretical primer and directions of electric power artificial intelligence (II)：self-directed learning and preliminary application[J]. Proceedings of the CSEE，2023，43(10)：3705-3717(in Chinese).

[7] 韩富佳，王晓辉，乔骥，等. 基于人工智能技术的新型电力系统负荷预测研究综述[J]. 中国电机工程学报，2023，43(22)：8569-8591.
HAN Fujia，WANG Xiaohui，QIAO Ji，et al. Review on artificial intelligence based load forecasting research for the new-type power system[J]. Proceedings of the CSEE，2023，43(22)：8569-8591(in Chinese).

[8] 孙晓燕，李家钊，曾博，等. 基于特征迁移学习的综合能源系统小样本日前电力负荷预测[J]. 控制理论与应用，2021，38(1)：63-72.
SUN Xiaoyan，LI Jiazhao，ZENG Bo，et al. Small-sample day-ahead power load forecasting of integrated energy system based on feature transfer learning[J]. Control Theory & Applications，2021，38(1)：63-72(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] MCMAHAN B，MOORE E，RAMAGE D，et al. Communication-efficient learning of deep networks from decentralized data[C]//Proceedings of the 20th International Conference on Artificial Intelligence and Statistics. Fort Lauderdale：PMLR，2017：1273-1282.

[11] WANG Yi，GAO Ning，HUG G. Personalized federated learning for individual consumer load forecasting [J]. CSEE Journal of Power and Energy Systems，2023：9(1)：326-330.

[12] GHOLIZADEH N，MUSILEK P．Federated learning with hyperparameter-based clustering for electrical load forecasting[J]．Internet of Things，2022，17：100470．

[13] ZHANG Weishan，CHEN Xiao，HE Ke，et al．Semi-asynchronous personalized federated learning for short-term photovoltaic power forecasting[J]．Digital Communications and Networks，2023，9(5)：1221-1229．

[14] DINH C T，TRAN N，NGUYEN J．Personalized federated learning with moreau envelopes[C]//Proceedings of the 34th International Conference on Neural Information Processing Systems．Vancouver，Canada：Curran Associates Inc.，2020：21394-21405．

[15] 焦润海，褚佳杰，李俊良，等．基于数据分解的多区域个性化联邦负荷预测方法[J].中国电机工程学报，2025，45(5)：1691-1703．
JIAO Runhai，CHU Jiajie，LI Junliang，et al．Personalized federated multi-region load forecasting method based on data decomposition[J]．Proceedings of the CSEE，2025，45(5)：1691-1703(in Chinese)．

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

[17] 纪守领，杜天宇，李进锋，等．机器学习模型安全与隐私研究综述[J]．软件学报，2021，32(1)：41-67．
JI Shouling，DU Tianyu，LI Jinfeng，et al．Security and privacy of machine learning models：a survey[J]．Journal of Software，2021，32(1)：41-67(in Chinese)．

[18] 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)．

[19] 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(CCS)．Vienna：Association for Computing Machinery，2016：308-318．

[20] 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．

[21] 雷诚，张琳，焦泽鑫．个性化语义敏感轨迹数据发布算法[J]．小型微型计算机系统，2024，45(12)：3002-3007．
LEI Cheng，ZHANG Lin，JIAO Zexin．Personalized semantic sensitive trajectory data publishing algorithm [J]．Journal of Chinese Computer Systems，2024，45(12)：3002-3007(in Chinese)．

[22] 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)．

[23] 顾永跟，李国笑，吴小红，等．预算约束下多任务联邦学习激励机制[J]．计算机工程，2024，50(5)：149-157．
GU Yonggen，LI Guoxiao，WU Xiaohong，et al．Incentive mechanism for multi-task federated learning under budget constraints[J]．Computer Engineering，2024，50(5)：149-157(in Chinese)．

[24] ZHAN Yufeng，LI Peng，WANG Kun，et al．Big data analytics by CrowdLearning：architecture and mechanism design[J]．IEEE Network，2020，34(3)：143-147．

[25] 王鑫，周泽宝，余芸，等．一种面向电能量数据的联邦学习可靠性激励机制[J]．计算机科学，2022，49(3)：31-38．
WANG Xin，ZHOU Zebao，YU Yun，et al．Reliable incentive mechanism for federated learning of electric metering data[J]．Computer Science，2022，49(3)：31-38(in Chinese)．

[26] 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 Zan，ZHANG Xiaoyan，YANG Shujie，et al．Adaptive incentive mechanism for privacy computing in federated compute first networks[J]．Chinese Journal of Computers，2023，46(12)：2705-2725(in Chinese)．

[27] 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 (iThings) and IEEE Green Computing & Communications (GreenCom) and IEEE Cyber，Physical & Social Computing(CPSCom) and IEEE Smart Data(SmartData) and IEEE Congress on Cybermatics (Cybermatics)．Melbourne：IEEE，2021：238-243．

[28] 周一辰，王书祥，李永刚，等．基于哈尔小波配点法的虚拟同步化电网动态仿真方法[J]．中国电机工程学报，2023，43(16)：6218-6232．
ZHOU Yichen，WANG Shuxiang，LI Yonggang，et al．Dynamic simulation method of virtual synchronized power grid based on haar wavelet collocation method[J]．Proceedings of the CSEE，2023，43(16)：6218-6232(in Chinese)．

[29] REIS A J R，DA SILVA A P A．Feature extraction via multiresolution analysis for short-term load forecasting [J]．IEEE Transactions on Power Systems，2005，20(1)：

189-198.

[30] 夏晓荣，胡鹏飞，王飞，等. 基于小波变换与优化 BP 神经网络的超短期光伏发电功率预测[J]. 电网与清洁能源，2024，40(10)：159-166.
XIA Xiaorong，HU Pengfei，WANG Fei，et al. Ultra-short-term photovoltaic power prediction based on wavelet transform and optimal BP neural networks [J]. Power System and Clean Energy，2024，40(10)：159-166(in Chinese).

[31] 臧海祥，陈玉伟，程礼临，等. 基于多尺度分量特征学习的用户级超短期负荷预测[J]. 电网技术，2024，48(6)：2584-2592.
ZANG Haixiang，CHEN Yuwei，CHENG Lilin，et al. User level ultra-short-term load forecasting based on multi-scale component feature learning[J]. Power System Technology，2024，48(6)：2584-2592(in Chinese).

[32] 刘科研，叶学顺，李昭，等. 基于多分辨率小波变换的配电网高阻接地故障检测方法[J]. 高电压技术，2023，49(10)：4247-4256.
LIU Keyan，YE Xueshun，LI Zhao，et al. Detection method of high impedance fault in distribution network based on multi-resolution wavelet transform[J]. High Voltage Engineering，2023，49(10)：4247-4256(in Chinese).

[33] 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).

[34] 方晨，郭渊博，王一丰，等. 基于区块链和联邦学习的边缘计算隐私保护方法[J]. 通信学报，2021，42(11)：28-40.
FANG Chen，GUO Yuanbo，WANG Yifeng，et al. Edge computing privacy protection method based on blockchain and federated learning[J]. Journal on Communications，2021，42(11)：28-40(in Chinese).

[35] LI Qinbin，DIAO Yiqun，CHEN Quan，et al. Federated learning on Non-IID data silos：an experimental study[C]//Proceedings of the 2022 IEEE 38th International Conference on Data Engineering(ICDE). Kuala Lumpur：IEEE，2022：965-978.

王路遥

在线出版日期：2025-08-27。
收稿日期：2024-11-01。

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)