DOI:10.11784/tdxbz202506041

一种面向大规模电动汽车集群的隐私保护安全调度方法

杨　挺[1]，冯相为[1]，赵永生[2]，张　帅[2]，魏显鉴[3]
（1. 天津大学电气自动化与信息工程学院，天津 300072；2. 国网信息通信产业集团有限公司，北京 102206；
3. 国网天津市电力公司，天津 300450）

摘　要：大规模电动汽车集群参与的电动汽车-虚拟电厂（EV-VPP）无需额外投资即可提升对聚合分布式能源参与电网调频的能力．然而，其聚合调控依赖于 EV 位置和电池荷电状态等隐私信息，易削弱车主参与积极性并降低集群调控潜力．针对 EV 集群聚合过程中的隐私保护问题，本文提出一种强化安全保护的横向联邦强化学习（SEFRL）调度方法．首先，构建了基于马尔可夫过程的 EV-VPP 优化调度模型．其次，通过本地差分隐私扰动单个 EV-VPP 的原始上传数据，实现针对上层调度中心的数据安全防护．然后，通过 Kyber-AES 轻量级后量子加密方法保护联邦聚合数据，有效阻止通过对联邦学习梯度参数的监听而推演出原始隐私数据，实现信道的安全防护，并实现安全性和计算效率之间的平衡．最后，在改进 IEEE-33 节点系统中构建包括 EV 集群在内多种分布式能源参与的 EV-VPPs 协同调度系统验证所提算法性能．仿真表明，面对 Deep Leakage 推断攻击，所提 SEFRL 方法可以稳定保持联邦学习梯度参数反推演隐私数据的误差在 0.91 以上，保证真实数据无法获知，从而实现针对上层调度中心的数据保护．此外，隐私保护能力的提升增强了 EV 集群参与调度的积极性，系统整体调频成本相较于 EV 无序充电降低了 29.5%．

关键词：电动汽车集群；本地差分隐私；隐私保护；后量子加密
中图分类号：TM73　　**文献标志码**：A　　**文章编号**：0493-2137（2026）06-0586-09

Privacy-Preserving Secure Scheduling Method for Large-Scale Electric Vehicle Clusters

Yang Ting[1]，Feng Xiangwei[1]，Zhao Yongsheng[2]，Zhang Shuai[2]，Wei Xianjian[3]
（1. School of Electrical and Information Engineering，Tianjin University，Tianjin 300072，China；
2. State Grid Information & Telecommunication Group Co.，Ltd.，Beijing 102206，China；
3. State Grid Tianjin Electric Power Company，Tianjin 300450，China）

Abstract：The large-scale integration of electric vehicle（EV）clusters in virtual power plants（EV-VPPs）enhances the ability of these aggregated distributed energy resources to provide grid frequency regulation without requiring additional investment. However，controlling these systems relies on private information，such as EV locations and battery state of charge，which may undermine EV owners' willingness to participate and diminish the regulatory potential of the clusters. To address these privacy concerns during EV cluster aggregation this study proposes a security enhanced federated reinforcement learning（SEFRL）scheduling method. First，an optimal EV-VPP scheduling model is constructed based on a Markov decision process. Second，local differential privacy is applied to perturb the raw data uploaded by individual EV-VPPs，thereby safeguarding data privacy from the perspective of the upper-level scheduling center. Then，a lightweight postquantum Kyber-AES hybrid encryption scheme is introduced to secure the transmission of aggregated federated data，thereby effectively preventing the inference of raw private information through eavesdropping on gradient parameters while balancing security with computational efficiency. Finally，the

收稿日期：2025-06-30；**修回日期**：2025-09-15.
作者简介：杨　挺（1979—　），男，博士，教授，yangting@tju.edu.cn.
通信作者：冯相为，xwfeng@tju.edu.cn.
基金项目：国家重点研发计划资助项目（2022YFB2403900）；国家自然科学基金资助项目（62371338）.
Supported by the National Key Research and Development Program of China（No. 2022YFB2403900），the National Natural Science Foundation of China（No. 62371338）.

proposed method is validated using a coordinated scheduling system that integrates EV clusters with other distributed energy resources on a modified IEEE-33 bus system. The simulation results indicate that under deep leakage inference attacks, the SEFRL method maintains a stable error rate above 0.91 when back-calculating private data from federated learning gradients, thereby effectively protecting data from the upper-level scheduling center. Moreover, enhanced privacy protection increases EV-cluster participation in scheduling, resulting in a 29.5% reduction in overall system-frequency-regulation costs compared with uncoordinated charging strategies.

Keywords: electric vehicle (EV) cluster; local differential privacy; privacy preservation; postquantum encryption

随着电动汽车(electrical vehicle, EV)的保有量快速增加[1], EV 规模化聚合形成的大规模柔性负荷资源,对于电力系统削峰填谷能力的提升以及负荷曲线特性的改善具有重要作用,从而增强电网运行的稳定性与经济性[2].

大规模 EV 以集群形式参与的电动汽车-虚拟电厂(electric vehicle-participated virtual power plant, EV-VPP)能够在不增加额外投资的前提下提供超过其他类型虚拟电厂的分布式能源消纳能力,并在电网调频服务方面表现出巨大潜力[3].

然而, EV 的大量敏感数据对 EV-VPP 的隐私保护措施提出了更高要求. 面对 EV-VPP 内部优化调度和电网辅助服务响应的聚合需求,包含用户位置、电池荷电状态(state of charge, SoC)和 EV 运营数据在内的大量敏感数据被共享至 EV-VPP 调控平台,并进一步上传到上层调度中心(upper-level dispatching center, UDC)[4]. 在 EV-VPP 本地和电力市场的细粒度共享需求加剧了现有隐私保护机制的防护压力和数据泄露风险[5].

针对 EV 聚合过程中的隐私保护问题,学术界的研究主要集中在身份隐私、价格隐私及交互数据隐私的保护上. 文献[6]通过强化学习进行基于差分隐私的隐私预算自适应分配,从而根据需求智能调节隐私保护的强度. 文献[7]使用去中心化的多方安全计算来保护充电站聚合 EV 过程中的价格隐私数据. 而文献[8-9]分别通过对交互信息进行 Paillier 和 CKKS (Cheon-Kim-Kim-Song)同态加密来实现 EV 集群的隐私保护. 文献[10]通过设计基于 CL 签名和零知识证明的匿名凭证,实现 EV 接入过程的身份认证. 然而,对于 EV 聚合参与 VPP,进而参与电力市场的二级隐私保护机制,现有工作仍未能充分研究.

在上层调度中心聚合 EV-VPP 的数据交互场景下,联邦学习技术通过本地模型训练与梯度传输的模式来代替原始数据的直接交换,使得 EV-VPP 的隐私得到了一定程度的保护[11]. 但是近年来新型攻击技术的出现,导致在联邦学习架构下运行的 EV-VPP 仍然存在着隐私保护的薄弱点. 联邦学习后门攻击方法可以通过提炼恶意神经元在全局模型中插入攻击后门,推断攻击则可以通过截获通信梯度破解参与方的隐私数据[12]. 因此,对使用联邦架构的 EV 聚合过程中的隐私保护仍需研究.

此外, EV-VPP 与上层调度中心之间的 IEC 60870-5-104 等协议由于缺乏身份认证机制和高强度的加密保护,导致数据传输过程容易遭受外部攻击者的窃听和破解[13]. 攻击者获取多组梯度信息后,可以通过链式求导攻击破解原始数据或其关键特征,从而导致 EV-VPP 的隐私调度数据泄露,造成严重的安全隐患.

而 UDC 虽然是诚实的,但是可能会对 EV-VPP 参与单元的隐私数据好奇,并通过源推断攻击(source inference attack, SIA)等方法在不违反联邦学习协议的情况下窃取训练成员的隐私信息[14],因此聚合过程中 EV-VPP 针对 UDC 的隐私也需要保护.

针对上述挑战,本文提出一种强化安全保护的横向联邦强化学习调度方法. 通过针对上层调度中心窥探和外部攻击的双重防护,实现 EV 集群参与 EV-VPP 聚合的隐私保护. 首先构建了基于马尔可夫过程的 EV-VPP 优化调度模型,并提出一种基于 DTQN 的 EV-VPP 本地调频控制方法,解决调度过程中参与单元响应曲线的非线性和耦合性问题;然后,提出一种基于本地差分隐私的 EV-VPP 本地数据扰动方法,仅向上层调度中心共享梯度的统计特征而非原始数据,从而实现本地 EV 充电隐私数据的安全防护;最终,提出一种 Kyber 高级加密标准(advanced encryption standard, AES)后量子梯度加密方法,通过基于格理论 Kyber 算法实现密钥协商,并通过 AES 算法实现梯度高效加密,有效阻止对联邦学习梯度参数的推断攻击,实现信道安全防护.

1　EV-VPP 参与单元模型的构建

本节设计了 EV-VPP 的调控目标,并构建了基于马尔可夫过程的 EV-VPP 优化调度模型.

1.1　调控目标

首先构建 EV-VPP 的增量内部调度模型,其调控

目标是在考虑调频指令的功率平衡约束下最小化调度成本,即

$$\min C_{\text{EV-VPP}}=\sum_{t=1}^{T}\left(C_{\text{ind},t}+C_{\text{EV},t}+C_{\text{PV},t}+C_{\text{WP},t}+C_{\text{GT},t}+C_{\text{ES},t}+P_{\text{grid},t}E_t-G_t\right) \tag{1}$$

$$\sum_{i=1}^{N_{\text{f}}}\left(P_{\text{f},i,t}^{\text{base}}-\Delta P_{\text{f},i,t}\right)-\sum_{j=1}^{N_{\text{d}}}\left(P_{\text{d},j,t}^{\text{base}}+\Delta P_{\text{d},j,t}\right)=P_{\text{grid},t} \tag{2}$$

式中:$C_{\text{ind},t}$、$C_{\text{EV},t}$、$C_{\text{PV},t}$、$C_{\text{WP},t}$、$C_{\text{GT},t}$、$C_{\text{ES},t}$ 分别代表工业用户、电动汽车充电集群、分布式光伏、分布式风电、微型燃气轮机、储能单元在 t 时刻的调控增量成本;N_{d} 和 N_{f} 分别代表可调机组数量和柔性负荷数量;$P_{\text{d},j,t}^{\text{base}}$ 和 $\Delta P_{\text{d},j,t}$ 分别代表可调机组 j 的基准发电功率和调增量;$P_{\text{f},j,t}^{\text{base}}$ 和 $\Delta P_{\text{f},i,t}$ 分别代表柔性负荷 i 的基准负荷和调减量;$P_{\text{grid},t}$ 代表 EV-VPP 与外部电网的功率交换,内部可调机组发电量不足以满足负荷时为正,反之为负;E_t 代表 t 时刻向外部电网购电的分时电价;G_t 代表 t 时刻 EV-VPP 参与辅助服务的收益.

1.2 基于马尔可夫过程的 EV-VPP 优化调度模型

在 EV-VPP 系统中,调度过程需要考虑电动汽车的充、放电动作、工业用户的负荷及可调机组的发电波动等多种因素. 将这一调度过程建模为马尔可夫过程,可以将复杂的动态决策问题转化为状态、动作、奖励函数及其转移概率的组合,使问题具备可计算性,并能够利用强化学习等方法求取最优调度策略,从而在保证内部电力供应和参与辅助服务的同时,实现经济效益的优化.

(1) 调度状态:EV-VPP 的调度状态中包含了管理平台调度参与单元所需要的各项信息,以及上层调度中心下达的辅助服务指令、辅助服务收益和购电所需的信息. EV-VPP 的调度状态 s_t 定义为

$$s_t=\{s_{\text{pu}},P_{\text{ref},t},P_{\text{grid},t},E_t,G_t\} \tag{3}$$

式中 s_{pu} 代表 EV-VPP 参与单元在 t 时刻的状态集. 根据负荷和电源种类,具体可定义为

$$s_{\text{pu}}=\{s_{\text{ind},t},s_{\text{EV},t},s_{\text{PV},t},s_{\text{WP},t},s_{\text{GT},t},s_{\text{ES},t}\} \tag{4}$$

式中 $s_{\text{ind},t}$、$s_{\text{EV},t}$、$s_{\text{PV},t}$、$s_{\text{WP},t}$、$s_{\text{GT},t}$、$s_{\text{ES},t}$ 分别代表工业用户、电动汽车充电集群、分布式光伏、分布式风电、微型燃气轮机、储能单元在 t 时刻的状态集合,状态集合中分别包含参与单元各自的状态. 其中电动汽车的充电集群状态 $s_{\text{EV},t}$ 可定义为

$$s_{\text{EV},t}=\{N_t^{\text{EV}},c_t^{\text{avg}},\beta_t,P_t^{\text{ch}},P_t^{\text{dis}},\tau_t^{\text{dep}},\delta_t\} \tag{5}$$

式中:N_t^{EV}、c_t^{avg} 和 β_t 分别代表 t 时刻在线的电动汽车数量、平均 SoC 和总电池容量;P_t^{ch} 和 P_t^{dis} 分别代表 t 时刻的电动汽车充电集群的充电和放电功率;τ_t^{dep} 和 δ_t 分别代表 t 时刻的预计离网时间和总充电需求.

通过构建分时的状态变量集合,EV-VPP 的调度系统可以在不同状态下做出动态决策,以适应电网及市场的动态变化.

(2) 调度动作:在 EV-VPP 的调度过程中,调度平台需要基于当前状态选择适当的动作,以实现系统优化目标. t 时刻的动作具体定义为

$$a_t=\left\{P_{\text{ind,ac},t},\sum P_{\text{EV,ac},n,t},P_{\text{PV,ac},t},P_{\text{WP,ac},t},P_{\text{GT},t},P_{\text{ES},t},P_{\text{grid},t}\right\} \tag{6}$$

式中:$P_{\text{ind, ac}, t}$、$P_{\text{EV, ac}, n, t}$、$P_{\text{PV, ac}, t}$ 和 $P_{\text{WP, ac}, t}$ 分别代表在 t 时段内工业用户、第 n 个电动汽车充电子集群、光伏发电单元以及风力发电单元按指令接受调控后的实际负荷或出力;$P_{\text{GT}, t}$ 和 $P_{\text{ES}, t}$ 分别代表微型燃气轮机的出力以及储能单元的充电或者放电功率.

通过式(6)可知,动作空间的定义包括对 EV-VPP 内灵活负荷的功率调控指令和可调机组的出力调控指令,以及向电网购电的有功功率.

(3) 奖励函数:对于 EV-VPP,奖励函数的设计需要同时考虑调度目标的实现和约束条件的保持,同时还需考虑对智能体的学习引导效果.

$$r_t=-C_{\text{EV-VPP}}-L_t^{\text{ex}}-L_t^{\text{im}}-L_t^{\text{as}} \tag{7}$$

式中 L_t^{ex}、L_t^{im} 和 L_t^{as} 分别代表 t 时刻超出负荷跟踪能力、无法平衡内部供能需求和无法跟踪辅助服务指令的惩罚,在完成这 3 个约束时,L_t^{ex}、L_t^{im} 和 L_t^{as} 会变为正值施加奖励,辅助服务的收益在 EV-VPP 总成本 $C_{\text{EV-VPP}}$ 中计算.

(4) 状态转移函数:EV-VPP 的环境中有很多的随机因素,如电动汽车车主到达和出发时间不确定、分布式风电和光伏受随机天气因素影响以及辅助服务指令的随机性等,为了描述状态 s_t 转移到状态 s_{t+1} 到过程中的随机性,定义状态转移函数为

$$s_{t+1}=f(s_t,a_t,\xi_t) \tag{8}$$

式中 ξ_t 代表 EV-VPP 环境中的随机性因素.

2 强化隐私保护的多 EV-VPP 协同调度方法

本节提出了一种强化安全保护的横向联邦强化学习(security enhanced federated reinforcement learning, SEFRL)方法来解决调度中心聚合下的多 EV-VPP 分布式协同调度中的隐私保护问题.

调控架构由两个层级构成:聚合层只包含上层调度中心,负责对多个 EV-VPP 的梯度信息进行收集、聚合和协同优化调度;调度层由多个独立的 EV-VPPs 组成,每个 EV-VPP 通过运行深度 Transformer Q 网络独立决策、控制内部 EV 资源,并与 UDC 交互

聚合数据.

2.1　基于深度 Transformer Q 网络的 EV-VPP 本地调度方法

EV-VPP 系统作为分布式电动汽车与虚拟电厂协同运行的平台，其调度问题涉及多时间尺度的动态变化，具有明显的非线性和耦合特征，致使实时优化面临较大挑战. 本小节提出一种基于深度强化学习的深度 Transformer Q 网络（deep transformer Q-network，DTQN）算法来解决 EV-VPP 本地调度中时序耦合的复杂性和非线性调度问题.

在状态 s_t 下采取动作 a_t 后，管理平台收到奖励 r_t，EV-VPP 进入下一时段的状态 s_{t+1}，并形成经验样本 $\{s_t, a_t, r_t, s_{t+1}\}$，将经验样本存储至经验回放池，并使用经验回放对 Q 网络进行训练. 在训练开始阶段一定数量的随机动作后，样本缓冲池中已经积累了足够数量的样本，随后在训练时，从本地经验回放缓冲区中采样长度为 k 的历史经验集合，即采样序列，采样序列 $h_{t:t+k}$ 定义如下

$$h_{t:t+k}=\{o_t,o_{t+1},\cdots,o_{t+k-1}\} \tag{9}$$

式中 o_t 为 t 时刻的观察样本，EV-VPP 调度的系统状态通常是完全可观的，参与单元完全授权管理中心获取自己的状态信息，因此 o_t 等价于 s_t.

图 1 给出了基于深度 Transformer Q 网络的强化学习框架，首先从经验缓冲池中通过小批量（mini-batch）采样获得采样序列 $h_{t:t+k}$，经过采样嵌入层进行特征向量化，同时引入时间位置编码以增强序列的时序表示. 接下来，嵌入特征被输入到 4 层 Transformer 自注意力模块中提取状态间的复杂时序依赖关系. 在此基础上，模型通过分布式 Q 值头对每个可能动作的动作 Q 值分布进行估计，并计算目标 Q 值，进而通过最大值自变量（argmax）操作选择最优动作 a_t 作为当前时刻的调度决策.

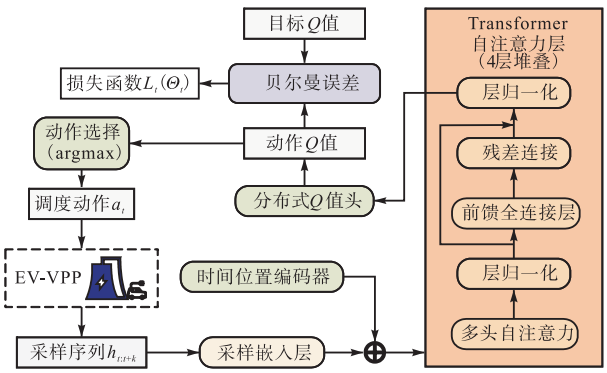


图 1　基于深度 Transformer Q 网络的强化学习框架

Fig.1　Reinforcement learning framework based on deep Transformer Q-networks

双 Q 网络中为了防止过拟合，只对动作网络进行更新，并每隔一定步长将动作网络的权重复制到目标网络. 以目标网络计算的 Q 值作为目标值，动作网络的损失函数 $L_t(\Theta_t)$ 定义为

$$L_t(\Theta_t)=E_{(\cdot)\sim\mathcal{D}}\left(y_t-Q(h_{t:t+k},a_t;\Theta_t)\right)^2 \tag{10}$$

式中：$\mathcal{D}$ 代表通过 mini-batch 采样的样本集合；$Q(h_{t:t+k},a_t;\Theta_t)$ 为经验样本通过动作网络输出的动作 Q 值，反映在当前策略下选择该动作后系统预期获得的累计奖励；优化损失函数 $L_t(\Theta_t)$ 时采用 t–1 时刻的网络参数计算 y_t，以保证计算过程中的参数稳定性，从而降低参数更新过程中的波动对训练效果的影响.

2.2　基于本地差分隐私的梯度数据扰动方法

在 EV-VPP 完成本地梯度的计算后，梯度的聚合过程还存在着数据被 UDC 窥探的隐私薄弱点. 本地差分隐私（local differential privacy，LDP）通过在本地添加扰动噪声，使得原始梯度免于推理攻击，扰动后上层调度中心只能获得梯度的统计特征而不是原始数据. 同时，梯度的统计特征也能支撑梯度分析、客户端聚类或分簇等聚合操作.

定义 1（ϵ-LDP）：给定一个随机算法 F 及其定义域 $D(F)$ 和值域 $R(F)$，当且仅当 F 对两个输入值 x_1 和 $x_2(x_1,x_2\in D(F))$ 计算得到相同的结果 $s(s\in R(F))$ 的概率满足下式时，随机算法 F 满足 ϵ-LDP

$$\frac{P[F(x_1)=s]}{P[F(x_2)=s]}\leqslant \mathrm{e}^{\epsilon} \tag{11}$$

式中 ϵ 为正实数，代表隐私预算.

在调度过程中，ϵ 越小，隐私保护程度越高，遭受推理攻击的可能性越小，但是较低的 ϵ 值会引入较大的数据扰动，可能降低数据精度和可用性.

在给出 ϵ-LDP 的准确定义后，需要将梯度的原始数据进行 LDP 扰动，本节使用拉普拉斯机制实现满足定义 1 的 LDP 扰动，拉普拉斯机制依赖于清晰的概率密度函数，其数学性质易于分析和证明，能够严格满足定义 1 并对 EV-VPP 的隐私梯度进行保护，同时，拉普拉斯机制可以自动校准噪声的幅度，从而在隐私保护和数据品质之间取得平衡.

首先定义一个拉普拉斯分布 $\mathcal{L}(\cdot)$ 为

$$\mathcal{L}(x\,|\,b)=\frac{1}{2b}\mathrm{e}^{-\frac{|x|}{b}} \tag{12}$$

式中 b 为拉普拉斯分布 $\mathcal{L}(\cdot)$ 的比例参数，则 t 时刻 EV-VPP 的叠加拉普拉斯 LDP 扰动后的扰动梯度 $\boldsymbol{\omega}_t^{\mathrm{LDP}}$ 计算式为

$$\boldsymbol{\omega}_t^{\mathrm{LDP}}=\boldsymbol{\omega}_t+\mathcal{L}(x\,|\,b)^d \tag{13}$$

式中 d 代表内部梯度 $\boldsymbol{\omega}_t$ 的维度.

为了保证 ϵ -LDP 的隐私保护效果,比例参数 s_{p} 计算式为

$$s_{\mathrm{p}}=\frac{\Delta\boldsymbol{\omega}}{\epsilon} \tag{14}$$

式中 $\Delta\boldsymbol{\omega}$ 代表梯度函数 $\boldsymbol{\omega}$ 的敏感度,$\Delta\boldsymbol{\omega}$ 定义为当 $\boldsymbol{\omega}$ 作用于任意两个相邻 EV-VPP 样本时 $\boldsymbol{\omega}$ 输出结果之间的最大差异为

$$\Delta\boldsymbol{\omega}=\max_{h_1,h_2\left|h_1\Delta h_2\right|=1}\left\|\boldsymbol{\omega}(h_1)-\boldsymbol{\omega}(h_2)\right\|_1 \tag{15}$$

式中 h_1 和 h_2 分别代表从 DTQN 样本集合 D 中采样的任意样本.

2.3 扰动梯度的 Kyber-AES 轻量级后量子加密方法

在对原始数据进行 LDP 扰动后,扰动梯度 $\boldsymbol{\omega}_t^{\mathrm{LDP}}$ 仍含有原始数据的统计特征信息,一旦未加密的数据受到外部攻击者的暴力破解,通过链式求导推断出的 EV-VPP 隐私数据统计特征仍会泄露参与单元的隐私. 因此,需要对 EV-VPP 和上层调度中心之间的信道进行加密.

本文提出了一种适用于 EV-VPP 联邦场景的 Kyber-AES 轻量级后量子加密方法. 在密钥协商阶段采用基于格理论的 Kyber 算法,使得密钥交换过程具备后量子安全性;在加密阶段采用 AES 算法对调度层 EV-VPPs 的本地梯度数据和聚合层的全局梯度数据进行高效对称加密,从而达到隐私安全性与计算经济性之间的平衡.

(1) Kyber 密钥协商阶段:首先,在密钥协商阶段,上层调度中心和 EV-VPPs 均运行 Kyber 密钥封装算法,实现后量子安全的会话密钥协商. EV-VPP 通过可信渠道获取上层调度中心的公钥种子,进而通过扩展函数 Sam 生成公开随机矩阵 $\boldsymbol{A}$,并采样随机向量 $\boldsymbol{r}$ 以及噪声项 e_1 和 e_2,随后计算

$$\boldsymbol{u}=C_q\left(\boldsymbol{A}^{\mathrm{T}}\boldsymbol{r}+\boldsymbol{e}_1,d_{\boldsymbol{u}}\right) \tag{16}$$

$$\boldsymbol{v}=C_q\left(\boldsymbol{t}_{\mathrm{P}}^{\mathrm{T}}\boldsymbol{r}+\boldsymbol{e}_2+\left\lceil\frac{q}{2}\right\rceil\boldsymbol{b},d_v\right) \tag{17}$$

式中:$C_q(\cdot,d_x)$ 表示压缩函数,即将输入向量进行模 q 操作并压缩到某个比特宽度(精度 d_x),其中 q 是模数,用于确保所有数值计算都在模环 Z_q 中进行,在 Kyber 算法中 q 取 3 329;$\boldsymbol{t}_{\mathrm{P}}=C_q(\boldsymbol{As}+\boldsymbol{e},d_t)$ 代表由 EV-VPP 私钥 $\boldsymbol{s}$ 生成的公钥组成部分,其中 $\boldsymbol{t}_{\mathrm{P}}^{\mathrm{T}}$ 代表 $\boldsymbol{t}_{\mathrm{P}}$ 的转置,$\boldsymbol{e}$ 是从离散高斯分布或中心化二项分布中采样得到的噪声向量;$\boldsymbol{b}$ 为封装时使用的比特串.

EV-VPP 通过上述过程获得密文 $\boldsymbol{c}=(\boldsymbol{u},\boldsymbol{v})$ 以及中间密钥 $\boldsymbol{K}_{\mathrm{m}}$ 后,结合随机哈希得出最终共享密钥 $\boldsymbol{K}$ 为

$$\boldsymbol{K}=H(\boldsymbol{K}_{\mathrm{m}},H(c)) \tag{18}$$

式中 $H(\cdot)$ 代表随机哈希函数.

随后,上层调度中心利用其私钥 $\boldsymbol{s}$ 对收到的密文 $\boldsymbol{c}$ 执行解封操作,从而恢复出与 EV-VPP 一致的对称密钥 $\boldsymbol{K}$. 通过 Kyber 算法中基于模块化带误差学习(learning with errors, LWE)难题的设计和 FO(Fujisaki-Okamoto)转换的引入,聚合层和调度层之间的会话密钥协商在经典和量子随机预言机模型下均能达到较高的安全性水平,从而实现后量子安全性.

(2) AES-256-GCM 高效加密阶段:在完成密钥协商之后,聚合层和调度层根据协商的高强度密钥采用 AES-256-GCM 算法完成扰动梯度的加密,AES-256-GCM 与原始 AES 算法相比,增加了 GCM 模式来提供数据的认证与完整性保护.

首先,为每次加密生成 96 位的随机初始向量 $\boldsymbol{N}$. 并将扰动梯度 $\boldsymbol{\omega}_t^{\mathrm{LDP}}$ 按 128 位块划分为 L 块,对每个 $\boldsymbol{\omega}_i$ 采用 AES-256 加密生成伪随机序列. 设计数器的值为 $u(i)$,则各块密文计算公式为

$$c_i=\boldsymbol{\omega}_i\oplus A_{\boldsymbol{K}}(\boldsymbol{N}\,\|\,\boldsymbol{u}(i)) \tag{19}$$

式中||表示串联操作 $A_{\boldsymbol{K}}(\cdot)$ 代表以密钥 $\boldsymbol{K}$ 为参数的 AES 加密函数. 整个扰动梯度数据的密文记为

$$C=c_0\,\|\,c_1\,\|\cdots\|\,c_{L-1} \tag{20}$$

在 GCM 模式中,利用 AES-256 生成的哈希子密钥 $H=A_{\boldsymbol{K}}(0^{128})$ 以及包含 EV-VPP 标识和训练轮次信息的附加认证数据(additional authenticated data, AAD)计算 GHASH 值,得到认证标签 T. 其中 GHASH 函数是 GCM 模式中用于计算 T 的哈希函数,通过在有限域 $G(2^{128})$ 内进行多项式乘法和累加,保证认证标签 T 的完整性.

其次,将初始向量 $\boldsymbol{N}$、密文 C 和认证标签 T 组合,构成加密梯度数据

$$\boldsymbol{c}_{\omega}=\{\boldsymbol{N},C,T\} \tag{21}$$

随后,上层调度中心在接收到 $\boldsymbol{c}_{\omega}$ 后,使用共享密钥 K 依次执行以下步骤:利用接收到的 $\boldsymbol{N}$、C 和事先约定的 AAD,重新计算认证标签 T':仅当 $T'=T$ 时,说明密文未被篡改,方可继续下一步;否则,拒绝解密并抛弃该扰动梯度数据.

验证通过后,对密文 C 进行 AES-CTR 解密,恢复原始梯度数据

$$\boldsymbol{\omega}_i=\boldsymbol{c}_i\oplus A_{\boldsymbol{K}}(\boldsymbol{N}\,\|\,u(i))$$
$$i=0,1,\cdots,L-1 \tag{22}$$

由此完成 LDP 扰动后梯度数据的密钥协商、加

密和解密. 在安全性方面，通过利用 Kyber 协商出的密钥 $\boldsymbol{K}$ 使系统具有了后量子安全性，同时 GCM 模式的应用可有效抵御包括窃听、篡改和重放等攻击.

在计算经济性方面，AES 算法在硬件（如 Intel AES-NI 硬件指令集扩展）支持下具有高性能特性，能够高效处理高频聚合下的大规模梯度加密任务.

2.4　考虑重要性的加权平均联邦聚合机制

由于在 EV-VPP 聚合场景下，每个 EV 接入的频率、充放电能力、数据量规模以及局部模型的收敛质量存在显著差异，传统联邦简单平均方法会导致聚合结果受到低质量或低贡献节点的干扰，进而降低全局模型的稳定性和预测精度. 因此，本文提出通过加权策略充分反映各个 EV-VPP 的实际贡献，从而提升聚合质量，加权联邦平均聚合函数设计为

$$\boldsymbol{\omega}_t^* = \sum_E \left(\frac{\lambda_m}{E} \boldsymbol{\omega}_t^{\mathrm{LDP}} \right) \tag{23}$$

式中：$\boldsymbol{\omega}_t^*$ 代表 t 时刻的全局梯度；λ_m 代表第 m 个 EV-VPP 的聚合权重；E 为 EVF-VPP 的数量.

3　基于改进 IEEE-33 节点系统的安全性分析和调度表现

本节基于改进 IEEE-33 节点系统，对所提 SEFRL 方法在 EV-VPP 调度中的安全和调度表现进行了分析.

3.1　改进 IEEE-33 节点系统仿真设置

为了验证 SEFRL 方法在 EV-VPP 调度中的安全性和有效性，基于改进 IEEE-33 节点系统与某地区调频辅助服务市场数据进行算例分析，模拟多个 EV-VPP 在上层调度中心下的协同调度.

图 2 展示了算例中基于改进 IEEE-33 节点的配电系统，设计了 3 个 EV-VPP 的仿真环境，以研究多类型灵活负荷与可调机组协同运行的优化调度策略. 3 个 EV-VPP 分别布置于馈线的起始端（EV-VPP 1）、中部负荷集中区（EV-VPP 2）以及末端负荷区（EV-VPP 3），各自独立管理并协调分布式光伏、风电、微型燃气轮机、储能单元、电动汽车充电集群和柔性工业负荷. 通过在节点 2、14、31 设置 EV 充电站，实现 EV-VPP 的构建，并充分利用 EV 的公共充电负荷，而通过私有桩进行充电的 EV 则被计入居民用电负荷内.

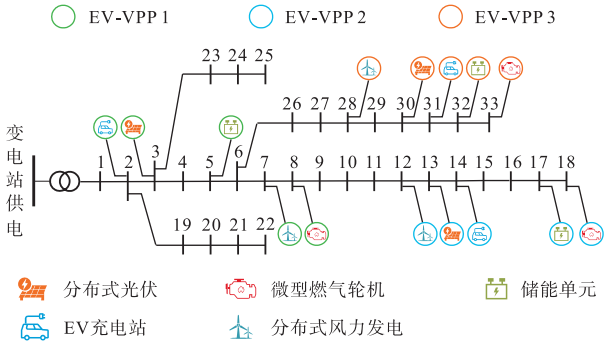


图 2　带有 EV-VPP 的改进 IEEE-33 节点系统

Fig.2　Improved IEEE 33-bus system with EV-VPPs

在本文算例中，EV-VPP 本地采用 DTQN 算法进行优化调度，采用 DTQN 架构可以利用 Transformer 结构强大的时序学习能力进行调度，从而保障 EV-VPP 的灵活负荷用能需求并降低运营成本.

算例中的联邦聚合参数和本地 DTQN 的算法参数由表 1 给出. 仿真采用的计算机配置有 Intel Core i7-13700 KF CPU 处理器，RAM 12 GB 内存和一个 NVIDIA RTX 4090 GPU，并配备 Ubuntu 22.04.3 LTS 操作系统，编程语言基于 Python 3.9，通过基于 Python 的 TensorFlow Federated（TFF）和 Vpplib 库进行联邦架构下 EV-VPP 的实现，通过 Pqcrypto 和 Cryptography 库进行加密算法的实现.

表 1　仿真参数设置

Tab.1　Simulation parameter settings

贪婪策略试错概率 ε	折扣系数	DTQN 注意力头数	DTQN 上、下文窗口长度 k	最大训练回合数 $I^{\max}$	mini-batch 长度	工业用户限停电的经济惩罚系数 $\delta_{m,x}^{\mathrm{IU}}$/(元/(kW·h))	EV 充电集群限停电的经济惩罚系数 $\delta_{m,x}^{\mathrm{EV}}$/(元/(kW·h))
0.85/0.10	0.992	8	25	10 000	128	11	2.2

3.2　面对 Deep Leakage 攻击模型的隐私性能分析

本节给出了所提 SEFRL 方法在面对专门针对联邦学习设计的 Deep Leakage 数据推断攻击时的隐私安全性能分析.

首先，根据联邦学习安全分析的经典假设，假设外部敌手具备完备的通信截获能力，即敌手可完全访问并获取联邦学习过程中传输的所有梯度信息. 基于这一假设，采用针对联邦学习设计的 Deep Leakage 模型，利用链式求导机制对截获的梯度数据进行反向推导，试图从中恢复出 EV-VPP 系统的原始隐私数据，以评估算法在真实敌手攻击场景中对隐私信息的保护能力.

为了衡量算法的隐私保护水平，采用梯度信息和敌手输入数据之间的互信息和敌手的推断误差来计算梯度数据对敌手的泄露. 两个数据之间的互信息值越小，表明数据之间的相关度越低，隐私信息的泄露程度就越小. 互信息 I^{MI} 定义为

$$I^{\mathrm{MI}} = E^{\mathrm{M}}(\boldsymbol{\omega}_t) + E^{\mathrm{M}}(\hat{\boldsymbol{\omega}}_t) - E^{\mathrm{J}}(\boldsymbol{\omega}_t, \hat{\boldsymbol{\omega}}_t) \tag{24}$$

式中：$E^{\mathrm{M}}(\cdot)$代表边缘熵计算函数，边缘熵描述某个变量单独存在时的信息量；$E^{\mathrm{J}}(\cdot)$代表联合熵计算函数，联合熵描述两个变量同时存在(即联合分布)时的整体信息量；$\hat{\boldsymbol{\omega}}_t$代表 t 时刻面对 EV-VPP 的原始梯度数据 $\boldsymbol{\omega}_t$时敌手的重构梯度数据.

对于梯度等连续随机变量 X 和 Y，其边缘熵 $E^{\mathrm{M}}(X)$和联合熵 $E^{\mathrm{J}}(X, Y)$定义为

$$E^{\mathrm{M}}(X) = -\int_{-\infty}^{\infty} p(x)\mathrm{lb}\ p(x)\ \mathrm{d}x \tag{25}$$

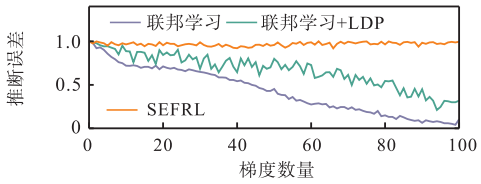
$$E^{\mathrm{J}}(X,Y) = -\iint p(x,y)\mathrm{lb}\ p(x,y)\ \mathrm{d}x\mathrm{d}y \tag{26}$$

式中：$p(x)$代表随机变量 X 的概率密度函数，即 X 在点 x 处的密度值；$p(x,y)$代表 X 和 Y 的联合概率密度函数，即 $X=x$、$Y=y$ 时的联合密度.

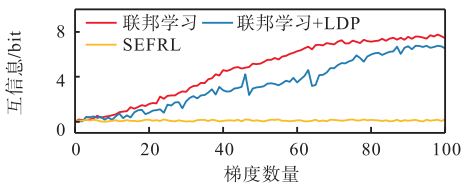
而推断误差用于衡量敌手通过攻击手段恢复或重构的数据序列与真实数据序列之间的差异程度. 推断误差值越大，表明敌手获得的数据与真实数据的偏离越显著，从而意味着隐私保护机制在抵御推断攻击方面的有效性越强. 推断误差 $\varepsilon^{\mathrm{inf}}$定义为

$$\varepsilon^{\mathrm{inf}} = (\boldsymbol{\omega}_t - \hat{\boldsymbol{\omega}}_t)^2 \tag{27}$$

图 3 给出了在 Deep Leakage 攻击模型下，所提方法与同类方法的隐私损失评估结果. 参与对比的有作为联邦学习代表算法的联邦平均算法(图中标注为联邦学习)、隐私增强型联邦学习经典范式 LDP-Fed(图中标注为联邦学习 + LDP)以及所提 SEFRL 方法.



(a) 推断误差与梯度数量的关系



(b) 互信息与梯度数量的关系

图 3 面对 Deep Leakage 数据还原的隐私损失评估

Fig.3 Privacy loss assessment in the face of Deep Leakage data reconstruction

图 3(a)展示了推断误差随敌手获取梯度数量的变化. 联邦平均算法的误差快速从 1.00 下降至约 0.10，说明在无防护情况下，Deep Leakage 攻击几乎可完全还原原始数据. 当梯度数量为 50 时，误差已降至约 0.40. 相比之下，联邦学习 + LDP 虽然也呈下降趋势，但误差始终高于无防护方案. 所提 SEFRL 方法的误差稳定在 1.00~0.91 之间，几乎不受梯度数量影响，推断误差始终大于 0.91 表明，即使在最优攻击条件下，重构出的数据序列中每个采样点的平均误差仍超过 0.954. 在梯度数量为 100 时，SEFRL 相较于联邦学习 + LDP 和联邦平均算法的防护效果分别提升了 856.1%和 212.7%. 这表明 SEFRL 能有效阻断攻击者利用梯度重建数据，实现高强度的推断防护.

互信息与敌手获得梯度数量的关系如图 3(b)所示，联邦平均算法在整个梯度增长过程中互信息持续上升，呈现出明显的线性增长趋势. 相比之下，联邦学习 + LDP 的互信息整体低于原始联邦学习，在梯度数量为 100 时互信息对比联邦平均算法降低了 12.3%. 所提 SEFRL 方法的互信息在整个梯度数量范围内始终保持在 1 bit 以下，表示敌手获得重构梯度数据 $\hat{\boldsymbol{\omega}}_t$后，仅减少对原始梯度数据 $\boldsymbol{\omega}_t$的 1 bit 不确定性，即一个开关量的不确定性. 此时，重构梯度数据对原始数据的恢复几乎没有帮助.

3.3 隐私保护提升对系统调频服务成本的影响分析

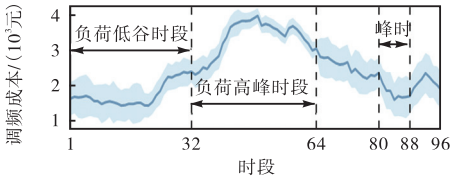
本节主要分析 EV 集群在 SEFRL 方法隐私保障下，其参与调控的积极性提升对改进 IEEE-33 节点系统调频服务成本的改善效果.

改进 IEEE-33 节点系统聚合多个 EV-VPP 与其他负荷共同参与辅助服务，其调频服务成本能够反映隐私保护增强对系统成本控制的影响.

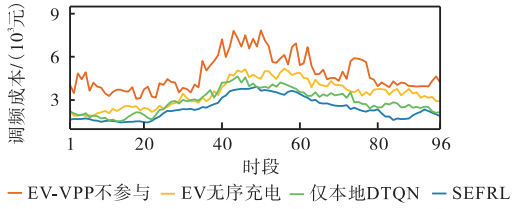
本节通过对比 SEFRL 方法在不同调度模式下的调频成本，起到类似消融实验的作用，以验证各环节的效果. 具体包括：①EV-VPP 不参与：参与单元独立响应调频，不通过 EV-VPP 聚合，用于评估因隐私顾虑放弃聚合的影响；②EV 无序充电：EV 充电集群不接受调控，采用最大功率无序充电，反映普通虚拟电厂在用户不参与下的调度效果；③仅本地 DTQN：各 EV-VPP 仅基于本地数据训练，不进行联邦聚合，用于分析在存在隐私威胁下，仅本地参与对调度性能的影响.

图 4 展示了所提出 SEFRL 方法在调频服务中的成本控制表现及不同调度模式下的对比效果，使用所提 SEFRL 方法消除隐私顾虑并提升参与单元的调控积极性后，改进 IEEE-33 节点系统在全时段内均表现出较低的调频成本，其平均成本均值为 2 431.4 元，对比 EV 无序充电和无联邦 DTQN，其平均成本均值分别降低了 29.5% 和 16.5%，验证了 EV 充电集群在

EV-VPP 中的作用，以及 EV-VPP 对比普通虚拟电厂的成本优势，同时也验证了联邦架构下打破数据孤岛带来的调度性能提升. 所提 SEFRL 方法对比 EV-VPP 不参与调频的情况，其平均成本大幅降低了 49.8%，表明所提 SEFRL 方法消除隐私顾虑后，EV 集群的分布式储能作用能够在改进 IEEE-33 节点系统的负荷平衡及频率调控方面节约大量成本.



（a）改进 IEEE-33 节点系统在 20 次实验中的调频成本波动



（b）不同参与积极性下的调频服务平均成本对比

图 4　参与积极性提升对调频服务成本的影响分析

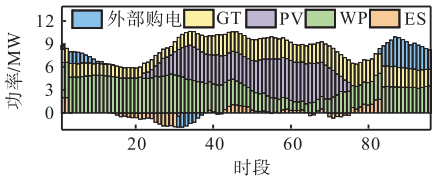
Fig.4　Analysis of the impact of increased participation enthusiasm on the cost of frequency regulation services

3.4　隐私保护提升对 EV-VPP 内部性能的影响分析

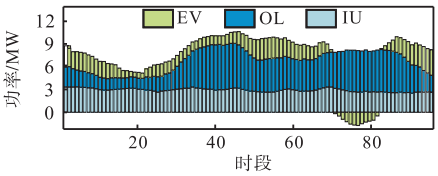
本节以 EV-VPP 3 为例，对 SEFRL 架构下 EV 集群充分参与情形的 EV-VPP 内部调度性能进行系统分析.

典型日内 EV-VPP 3 的调度结果如图 5 所示，详细给出了可调机组的出力情况、灵活负荷的波动情况以及外部购电的结果，图中：GT、PV、WP、ES 分别代表微型燃气轮机、分布式光伏、分布式风电和储能单元；EV、OL、IU 分别代表电动汽车充电集群、其他负荷和工业用户. 图 5(a)给出了可调机组的出力以及外部购电的调控结果，在负荷高峰时段(33 ~ 64 时段、80 ~ 88 时段)，外部购电的平均值仅为 0.298 8 MW. 购电行为主要集中在负荷低谷时段和平段，而在负荷高峰时段有长达 1.5 h 峰值超过 1.80 MW 的反向送电行为，这是由于所提 SEFRL 算法对 EV-VPP 3 的内部负荷进行了调控，从而大大降低了负荷高峰时段对电力系统稳定性的冲击，并根据上层调度中心的指令支撑系统调频.

图 5(b)展示了灵活负荷的调度结果. EV 充电负荷主要集中在高峰时段，而调控后在低谷时段达到了 1.64 MW，甚至比高峰时段高出 4.4%，表明 SEFRL 算法成功引导 EV 在低谷时段主动“谷充”，利用低价电能实现削峰填谷. 在 72 ~ 82 时段，EV 充电集群负荷均值为−1.100 MW，说明大量车辆通过 V2G 反向放电，有效缓解了电网压力. 工业用户和其他负荷因调度成本高，仅做小幅调整，以避免亏损.



（a）可调机组出力调度结果与外部购电情况



（b）灵活负荷在典型日内的调度结果

图 5　典型日内 EV-VPP #3 的调度结果

Fig.5　Dispatch results of typical intra-day EV-VPP #3

4　结　语

针对多 EV-VPP 在上层调度中心聚合下进行分布式协同调度导致的隐私泄露问题，本文提出了一种强化安全保护的横向联邦强化学习(SEFRL)方法. 所提 SEFRL 方法面对 Deep Leakage 推断攻击，可以稳定保持推断误差在 0.910 以上，表明即使面对最优攻击条件，仍能保持重构数据序列中每个采样点的平均误差超过 0.954. 并且通过所提 SEFRL 方法消除隐私顾虑后，EV-VPP 的平均调频成本降低了 29.5%，有效提升了调频效果.

随着电动汽车保有量的持续增长及其与电网双向互动能力的不断增强，未来研究可进一步面向电动汽车与多类可再生能源协同，构建统一、轻量化的隐私保护聚合体系.

参考文献：

[1] International Energy Agency(IEA). Global EV Outlook 2024[EB/OL]. https://www.iea.org/reports/global-ev-outlook-2024, 2025-04-05.

[2] 葛磊蛟，李元良，汪宇倩. 智能配电网态势感知实现效果综合评估模型[J]. 天津大学学报(自然科学与工程技术版)，2020，53(11)：1101-1111.
Ge Leijiao, Li Yuanliang, Wang Yuqian. Comprehensive evaluation model for situational awareness effects of

a smart distribution network[J]. Journal of Tianjin University(Science and Technology), 2020, 53(11): 1101-1111(in Chinese).

[3] 王明深，于 汀，穆云飞，等. 电动汽车能效电厂价格响应模型[J]. 天津大学学报(自然科学与工程技术版)，2016，49(12)：1320-1329.
Wang Mingshen, Yu Ting, Mu Yunfei, et al. A price response model for efficient power plant of electric vehicles[J]. Journal of Tianjin University(Science and Technology), 2016, 49(12): 1320-1329(in Chinese).

[4] Ledro M, Calearo L, Zepter J M, et al. Influence of realistic EV fleet response with power and energy controllers in an EV-wind virtual power plant[J]. Sustainable Energy Grids & Networks, 2022, 31: 100704.

[5] Ebrahimi M, Ebrahimi M, Shafie-Khah M, et al. EV-observing distribution system management considering strategic VPPs and active & reactive power markets[J]. Applied Energy, 2024, 364: 123152.

[6] Qiu R X, Liu X, Huang R, et al. Differential privacy EV charging data release based on variable window[J]. PeerJ Computer Science, 2021, 7: e481.

[7] Lu C B, Wu J M, Wu C Y. Privacy-preserving decentralized price coordination for EV charging stations[J]. Electric Power Systems Research, 2022, 212: 108355.

[8] 郭 静，顾智敏，朱道华，等. 隐私保护的电动汽车充电行为安全预测方法[J]. 电讯技术，2025，65(7)：1033-1041.
Guo Jing, Gu Zhimin, Zhu Daohua, et al. A secure charging behaviour forecasting method with privacy protection[J]. Telecommunication Engineering, 2025, 65(7): 1033-1041(in Chinese).

[9] Yu H, Zhang Y L, Qu J H, et al. A privacy-protected distributed operation method for flexible distribution networks with EV charging load clusters[J]. Energy, 2025, 327: 136409.

[10] 李元诚，胡柏吉，黄 戎. 基于匿名凭证与区块链的 V2G 网络电力交易隐私保护认证方案[J]. 通信学报，2025，46(5)：145-158.
Li Yuancheng, Hu Boji, Huang Rong. Privacy-preserving authentication scheme for electricity trading in V2G network using anonymous credential and blockchain[J]. Journal of Communications, 2025, 46(5): 145-158(in Chinese).

[11] 杨 挺，覃小兵，冯相为，等. 计及用户充电行为与隐私保护的联邦学习电动汽车短期充电负荷预测[J]. 高电压技术，2024，50(10)：4512-4519.
Yang Ting, Qin Xiaobing, Feng Xiangwei, et al. Short-term charging load prediction of federated learning electric vehicles after accounting for user charging behavior and privacy protection[J]. High Voltage Engineering, 2024, 50(10): 4512-4519(in Chinese).

[12] Sharma A, Marchang N. A review on client-server attacks and defenses in federated learning[J]. Computers & Security, 2024, 140: 103801.

[13] Csatár J, György P, Holczer T. Holistic attack methods against power systems using the IEC 60870-5-104 protocol[J]. Infocommunications Journal, 2023, 15(3): 42-53.

[14] Hu H S, Zhang X Y, Salcic Z, et al. Source inference attacks: Beyond membership inference attacks in federated learning[J]. IEEE Transactions on Dependable and Secure Computing, 2024, 21(4): 3012-3029.

(责任编辑：孙立华)