文章编号：2095-4980(2025)07-0655-08

面向有源配电台区电力设备的太赫兹指纹识别学习方法

岳　洋，张　磐，吴　磊，庞　超

(国网天津市电力公司 电力科学研究院，天津 300074)

摘　要：为提升对有源台区内海量分布式电力设备的安全管理能力，提出一种面向有源台区的电力设备太赫兹指纹识别防篡改与分簇联邦学习协同方法。首先通过特殊的工艺制作电力设备太赫兹标签，提供物理防伪基础；进而提出一种双分支多模态卷积神经网络识别设备指纹是否存在异常篡改；最后设计了一种分簇联邦学习(FL)训练方法，避免因隐私问题导致的防篡改识别模型的数据难以共享共用，并实现有源台区内多设备太赫兹指纹数据的分布式联合建模与高效协同训练。实验结果表明，本文所提方法的指纹识别精确度达到90%以上，比传统直方图相似度算法识别精确度提升了212%。本文所提方法在提高设备指纹识别精确度、增加训练效率和数据可用不可见等方面均具有显著优势，为电力设备的安全监测及预防攻击提供了新的技术路径。

关键词：有源配电台区；太赫兹设备指纹；联邦学习(FL)；设备识别

中图分类号：TN601　　**文献标志码：**A　　**DOI：**10.11805/TKYDA2025031

A terahertz fingerprint recognition learning method for power equipment in active distribution substations

YUE Yang，ZHANG Pan，WU Lei，PANG Chao

(Electric Power Research Institute，State Grid Tianjin Electric Power Company，Tianjin 300074，China)

Abstract：A terahertz fingerprint recognition and clustered Federated Learning(FL) collaboration method is proposed for anti-tampering protection of power equipment in power-supplied distribution areas, aiming to enhance the security management of massive distributed power devices within such areas. Firstly, specialized manufacturing techniques are employed to create terahertz tags for power equipment, providing a foundation for physical anti-counterfeiting. Then, a dual-branch multimodal convolutional neural network is introduced to detect abnormal tampering of device fingerprints. Finally, a clustered FL training method is designed to address data-sharing challenges caused by privacy concerns in anti-tampering recognition models, enabling distributed joint modeling and efficient collaborative training of terahertz fingerprint data across multiple devices in power-supplied distribution areas. Experimental results demonstrate that compared with traditional methods, the proposed approach improves recognition accuracy by 212% over the histogram similarity algorithm. Additionally, it significantly outperforms conventional image recognition algorithms in terms of fingerprint recognition accuracy, training efficiency, and ensuring data usability while maintaining privacy. Finally, the fingerprint recognition accuracy reaches more than 90%, which provides a novel technical pathway for security monitoring and attack prevention of power equipment.

Keywords：active distribution substations；terahertz device fingerprint；Federated Learning(FL)；equipment recognition

收稿日期：2025-02-08；**修回日期：**2025-04-09

基金项目：国网天津市电力公司科技资助项目(电科-研发　2023-41)

引用格式：岳洋,张磐,吴磊,等. 面向有源配电台区电力设备的太赫兹指纹识别学习方法[J]. 太赫兹科学与电子信息学报,2025,23(7):655-662. DOI:10.11805/TKYDA2025031.

Citation format：YUE Yang,ZHANG Pan,WU Lei,et al. A terahertz fingerprint recognition learning method for power equipment in active distribution substations[J]. Journal of Terahertz Science and Electronic Information Technology,2025,23(7):655-662. DOI:10.11805/TKYDA2025031.

随着智能电网向分布式能源高渗透方向演进，有源配电台区内不同厂家制造的光伏、充电桩等设备数量逐渐增加，保障台区内电力设备不受芯片篡改、信道监听等物理破解威胁对台区安全具有重要意义[1]。传统基于电子标签和加密认证的方式难以有效应对物理层攻击，而依赖集中式认证机制的方案又面临单点失效、隐私泄露和计算资源瓶颈等问题。近年来，太赫兹频段因其短波长、高分辨力及对非金属材料的穿透性，为设备指纹提取提供了独特的物理层特征，可有效抵御传统标签系统的伪造风险；同时，其频谱资源丰富，传输速率高，保密性强，易实现通信感知一体化等优势在未来具有优良的应用前景[2]，但现有基于单节点或局部特征建模的识别方法难以满足跨设备、跨台区的协同认证需求。由于数据存储和计算模式的分散性，现有模型的泛化能力受限，且由于设备指纹数据涉及敏感信息，集中式存储与处理会带来较大的隐私泄露风险[3]。因此，如何构建兼顾隐私保护、泛化能力和实时性的分布式设备身份认证方案，是智能电网安全领域亟需解决的问题。

针对上述挑战，已有研究从不同的角度提出了解决方案。研究者针对设备身份识别提出了基于物理不可克隆函数(Physical Unclonable Functions，PUF)的硬件特征提取[4]、射频指纹(Radio Frequency–DNA，RF–DNA)的无线信号鉴别[5]，以及结合光学特征的设备表面微结构分析[6]等方法。PUF 利用设备制造过程中的微小随机工艺偏差，确保设备特征难以复制，从而提供硬件级安全认证能力。但 PUF 的稳定性受环境因素影响较大，在电网设备复杂运行环境下可靠性有限。RF–DNA 通过分析无线信号的频谱特征进行设备识别，适用于无线通信场景，但在配电系统中，信号干扰和设备间的共模特性会降低其辨识能力。光学特征分析方法通过高精确度成像或光谱测量设备表面微结构，实现设备身份认证和伪造检测，能够提供较高的唯一性和抗伪造能力，但受限于环境光照条件，且难适用于远程非接触式认证。为进一步提升鲁棒性，多模态特征融合技术逐渐兴起。文献[7]提出一种基于多模态融合的端到端深度聚类旋转机械多传感器故障诊断方法，并设计了一种模态融合注意力机制，通过计算不同模态深度特征之间的亲和矩阵，实现模态特征的融合。文献[8]通过异步质询–响应机制实现身份验证解决方案，利用一次一密保证安全性。文献[9]通过基于 PUF 的协议保证身份安全，无需计算哈希函数或进行密钥交换，提升了计算经济性和安全性。但这些方法需在电力设备中添加专门的芯片并保障信号通路的完整，增加了中小厂商制造电力设备的成本并增加了实施统一安全标准的难度。

近年来，深度学习技术在电力设备识别领域取得显著进展。利用卷积神经网络(Convolutional Neural Network，CNN)挖掘数据局部特征并结合长短期记忆网络(Long Short Term Memory，LSTM)进行时序特征提取，以及结合生成对抗网络(Generative Adversarial Network，GAN)的数据增强策略，提高数据监测精确度。近期研究进一步引入迁移学习技术应对小样本问题[10]，或构建基于图神经网络的设备拓扑关系进行建模[11]。尽管如此，集中式训练模式需聚合多源数据，与电力企业数据主权边界形成冲突，导致实际部署可行性受限。为在保障数据隐私的同时提升模型性能，联邦学习(FL)在配电领域的应用逐渐增多。通过分布式训练机制，FL 能够使各参与方在本地保留数据，仅通过模型参数的交互完成协同学习，从而有效降低数据泄露风险。FL 已广泛用于负荷预测、协同调度等关键任务[12]，通过 FL，不同区域或主体能够在不共享原始数据的前提下，共同构建高效的预测与优化模型，促进配电系统的智能化和安全性提升[13]。文献[14]提出了一种融合区块链智能合约和同态加密的联邦学习方案。通过区块链和同态加密进一步增强客户端和服务器通信的安全性。文献[15]提出了一种基于具有依赖可分离卷积的卷积神经网络生成多标签分类联邦模型进行设备指纹的识别，在特征提取、泛化和收敛能力上实现了提升。但当前研究主要集中于电气量数据的分析，对太赫兹物理特征与联邦学习的深度融合尚缺乏系统性探索。特别是，现有 FL 模型在处理太赫兹指纹数据时面临适配性挑战，难以直接应对其高维、异构特性。目前的方法主要依赖预设参数进行客户端聚类，缺乏对数据分布和环境动态变化的自适应能力，导致在复杂配电台区拓扑结构不断演变的情况下，模型难以有效调整，进而影响学习效果与系统稳定性。因此，亟需一种创新性的方法，能够融合太赫兹物理层特征与 FL 技术，以提升电力设备身份认证的鲁棒性和泛化能力，确保智能电网环境下设备的安全接入和可信管理。为解决有源配电台区中电力设备的安全接入问题，本文提出一种有源配电台区内电力设备的太赫兹设备指纹联邦学习识别方法，实现设备指纹的获取和可靠认证，并打破不同设备之间的数据孤岛，实现数据可用不可见。

1 电力设备太赫兹指纹的生成方法和太赫兹标签工作原理

现有电力设备通常使用普通标签和射频识别(Radio Frequency Identification，RFID)标签进行外壳异动识别，攻击者只需将标签从原设备上剥离，再附着于非法设备，便能轻易绕过认证系统，使身份验证形同虚设。针对这一挑战，本文创新性地采用太赫兹标签防止此类篡改。根据麻省理工学院的研究[16]，使用掺杂金属颗粒的粘合剂制造标签，并通过亚太赫兹(sub–THz)波照射，可以在芯片–物品界面上产生独一无二的亚太赫兹波散射图

像，将该图像用于检测电力设备的异动，可实现物理上的身份防伪。电力设备太赫兹指纹的生成原理如图 1 所示。

本文利用这一技术构建电力设备防篡改太赫兹标签。有源台区内电力设备(如屋顶光伏逆变器、入户电表、电动汽车充电桩以及各类配电自动化设备)的表面标签粘合剂使用环氧树脂或硅胶与约 300 μm 大小的金属颗粒混合而成，并在设备首次通过认证后粘贴太赫兹标签。在设备首次投入使用时，使用太赫兹设备发射亚太赫兹波，金属颗粒在太赫兹波的照射下，会在设备表面形成独一无二的随机分布图案作为设备太赫兹指纹，对该指纹进行存储，即可为身份认证提供可靠的依据。一旦标签遭到剥离并重新粘贴，胶水中的金属颗粒分布将不可避免地发生变化，导致识别时的指纹变化。太赫兹设备指纹标签制造成本低廉，在电力设备分散且无人值守的有源台区，展现出巨大的应用潜力。

在识别设备中设置 2 个金属槽，标签将识别设备发射的亚太赫兹信号引导至金属槽 1(辐射槽)，随后这些信号被耦合至硅基板中。由于硅的介电常数较高，信号以基板模式波的形式传播。芯片表面下方的三维材料分布导致信号发生复杂的散射效应，其中部分散射波被金属槽 2(传感槽)捕获，并最终反向散射回读取器。芯片集成了多个辐射槽和传感槽，通过在频带内生成空间多样性的槽间耦合响应，形成电力设备的独特“设备指纹”。

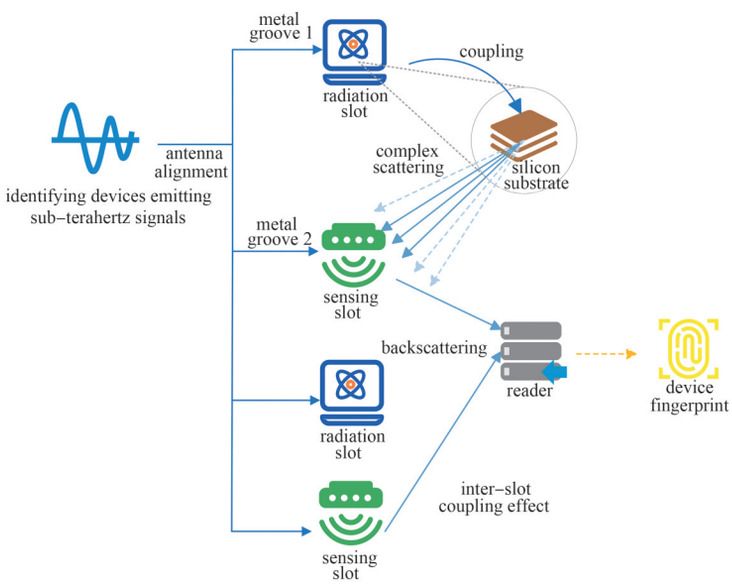

Fig.1 Generation principle of terahertz fingerprint of power equipment

图 1　电力设备太赫兹指纹的生成原理

2　基于双分支多模态卷积神经网络的太赫兹指纹识别方法

太赫兹设备指纹的独特性保障了设备安全，但由于电力设备运行时的振动、电磁力等因素，太赫兹设备指纹不可避免地会在设备的正常运行过程中发生细微的改变，该现象称为指纹漂移。为区分正常运行导致的电力设备指纹漂移和恶意攻击导致的设备异动，提出一种用于太赫兹指纹标签的本地设备异动识别方法，通过基于双分支多模态卷积神经网络(Dual-Branch CNN)进行本地指纹识别。

双分支卷积神经网络是近年来在图像处理任务中表现出色的深度学习架构，通过将不同类型的数据分别输入到不同的分支中处理。双分支卷积神经网络的核心思想是将输入数据的不同模态通过独立的分支进行处理，并最终融合各自的特征。本文输入数据由原始指纹图像和反射图像组成，因此将网络设计为两个分支：原始指纹图像分支用于处理原始指纹图像，反射图像分支用于处理反射图像。每个分支都由一系列卷积层、池化层和激活函数构成。

2.1　反射指纹图像分支

对于识别设备照射特种标签产生的太赫兹反射图像，采用二维卷积神经网络提取图像中的空间特征。假设输入的反射图像为 $\boldsymbol{x}_2$，其大小为 $h\times w$，即 $\boldsymbol{x}_2\in\mathbb{R}^{h\times w}$。

类似于质询波信号分支，首先进行卷积层设计。二维卷积操作用于提取图像的局部空间特征：

$$\boldsymbol{y}_2=\boldsymbol{W}_2\times\boldsymbol{x}_2+\boldsymbol{b}_2 \tag{1}$$

式中：$\boldsymbol{W}_2\in\mathbb{R}^{K_h\times K_w}$ 为二维卷积核，K_h 和 K_w 分别为卷积核的高和宽；$\boldsymbol{b}_2$ 为偏置项；$\boldsymbol{y}_2\in\mathbb{R}^{h'\times w'}$ 为卷积后的输出特征图，维度为 $h'\times w'$。

其次进行池化层设计。池化层用于减小特征图的空间维度，常使用最大池化操作：

$$\boldsymbol{p}_2=\mathrm{pool}\left(\boldsymbol{y}_2\right) \tag{2}$$

最后进行激活层设计。使用 ReLU 激活函数对卷积结果进行非线性变换：

$$\mathrm{ReLU}(\boldsymbol{y}_2)=\max(0,\boldsymbol{y}_2) \tag{3}$$

2.2 特征融合模块

在双分支卷积神经网络中，经过卷积层和池化层的特征将通过特征融合层进行融合。特征融合的目的是将不同输入的特征有效整合，以便网络可利用每种模态的信息进行最终的识别决策。使用加权融合的方式完成特征融合，通过权重调节分支的重要程度，融合过程为：

$$\boldsymbol{f}=\alpha_1\boldsymbol{p}_1+\alpha_2\boldsymbol{p}_2 \tag{4}$$

式中：$\boldsymbol{p}_1$为原始图像的特征；$\boldsymbol{p}_2$为反射图像特征；α_1和α_2为权重，$\alpha_1+\alpha_2=1$，可通过训练学习得到，α_1和α_2可根据模态的重要性自动调整；$\boldsymbol{f}$为融合后的特征向量，包含了从2个模态中提取的信息。

2.3 输出与置信度预测

融合后的特征$\boldsymbol{f}$将输入至全连接层，输出设备标签的置信度C。输出置信度的计算使用Softmax激活函数进行分类任务。

对于分类任务，Softmax函数将网络输出转化为概率分布：

$$C_i=\frac{\exp(f_i)}{\sum_{j=1}^{N}\exp(f_j)} \tag{5}$$

式中：C_i为第i类的预测概率；f_i为融合特征$\boldsymbol{f}$在第i类的输出。

2.4 训练与损失函数

网络的训练目标是最小化预测结果与真实标签之间的差异。采用交叉熵损失函数(Cross-Entropy Loss，CEL)用于分类任务。交叉熵损失函数CEL可按式(6)计算：

$$L_{\mathrm{CE}}=-\sum_{i=1}^{N}y_i\log C_i \tag{6}$$

式中y_i为真实标签的概率。

双分支多模态卷积神经网络的结构如图2所示，该结构可有效处理太赫兹波质询信号和反射图像，提取异构数据的高阶特征并进行融合。双分支卷积神经网络能够充分利用不同模态的数据特性，独立提取太赫兹质询波信号和反射图像的特征，最终通过融合操作得到更为综合的信息，提高了识别精确度，增加了系统的鲁棒性。

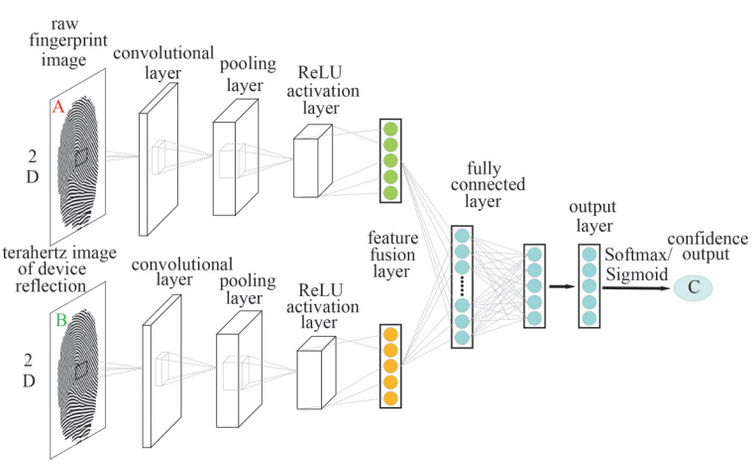

Fig.2 Structure of dual-branch multimodal convolutional neural network

图2 双分支多模态卷积神经网络结构

3 多设备协同训练的联邦学习神经网络训练方法

在有源台区内应用太赫兹设备指纹及识别方法的过程中，由于不同制造商、不同所有权等客观因素的存在，大量电力设备的太赫兹设备指纹识别模型无法共享共用，形成了数据模型孤岛，不利于指纹识别的快速学习，

对新型分类攻击也无法快速传递识别经验。因此，本文提出了用于多设备协同训练的联邦学习(FL)神经网络训练方法，并对模型参数相近的客户端进行分簇，通过计算各电力设备之间余弦相似度分出初始簇，并通过准确性验证将剩余客户端分簇，达到多设备聚类学习的效果。

FL是一种分布式机器学习方法，通过允许多个电力设备在本地训练并只共享模型更新，而非数据本身，有效保护了数据隐私。在FL中，每个客户端(电力设备)本地训练自己的模型，然后将其更新发送给中央服务器进行聚合。服务器端的聚合流程表示为：

$$\boldsymbol{W}_{t+1}=\sum_{k=1}^{K}\frac{n_k}{n}W_k^{(t+1)} \tag{7}$$

式中：$\boldsymbol{W}_k^{(t+1)}$为客户端k在第t轮训练后得到的模型参数；n_k为客户端k的样本量，n为所有客户端的总样本量；$\boldsymbol{W}_{t+1}$为全局模型的更新。

在传统的FL中，各客户端之间的模型更新是独立的，无法利用设备之间的相似性。本文提出的太赫兹设备指纹识别过程中，同类的太赫兹标签之间具有相似的图像尺寸和指纹特征。为提高训练效率和准确性，提出一种基于相似度分簇的多设备协同训练方法。该方法通过计算各客户端之间的相似性，并基于相似度进行分簇，从而使每个簇内的设备可共享更多的知识。

首先，定义每个设备k在训练中的模型参数为$\boldsymbol{w}_k$，通过计算各设备之间的余弦相似度$\cos(\theta_{ij})$度量模型参数的相似性：

$$\cos(\theta_{ij})=\frac{\boldsymbol{w}_i^{\mathrm{T}}\boldsymbol{w}_j}{\|\boldsymbol{w}_i\|\cdot\|\boldsymbol{w}_j\|} \tag{8}$$

式中$\boldsymbol{w}_i$和$\boldsymbol{w}_j$分别为设备i和设备j的模型参数。

通过计算所有设备之间的余弦相似度，可得到一个相似度矩阵$\boldsymbol{S}$，其中$\boldsymbol{S}_{ij}=\cos(\theta_{ij})$。对模型参数相似的客户端进行分簇，初始簇的划分基于所有客户端之间的余弦相似度矩阵$\boldsymbol{S}$。具体地，使用K-means聚类算法对设备进行初始分簇。设定簇数为L，并通过余弦相似度矩阵计算各客户端与簇中心的距离。

分簇过程可通过最小化簇内的总距离实现，目标函数为：

$$\min_{\{L_k\}}\sum_{k=1}^{L}\sum_{i\in C_k}\|\boldsymbol{w}_i-\boldsymbol{w}_k\|^2 \tag{9}$$

式中：L_k为第k个簇；$\boldsymbol{w}_k$为簇L_k的中心。

在多设备协同训练过程中，通过对客户端的模型参数进行相似度计算，并进行分簇，既保证了数据隐私，又使同一簇内的设备能够更高效地共享信息。

在每一轮联邦学习中，每个簇内的设备首先进行本地训练，计算出模型更新，并将其发送给中央服务器。中央服务器对各簇的模型更新进行聚合，计算出全局模型。最终，客户端根据聚合后的全局模型进行参数更新，完成一次联邦学习的训练过程。如图3所示。

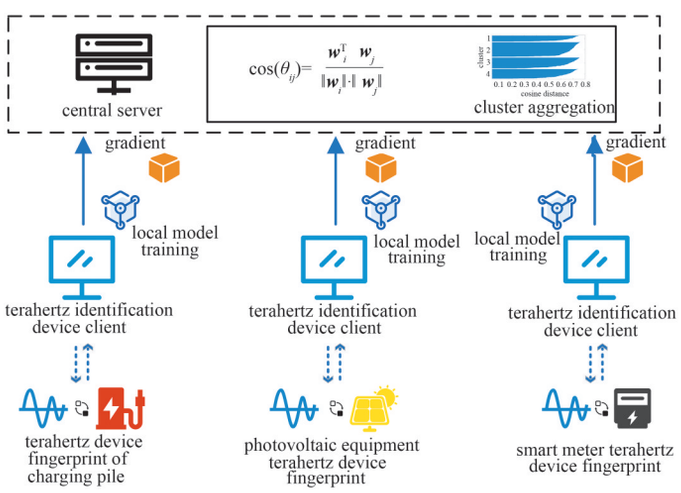

Fig.3 FL method for collaborative training of multiple devices in a power distribution area

图3 有源台区内多设备协同训练的联邦学习方法

4　仿真验证

对本文所提方法的识别精确度进行分析，并对联邦学习的算法性能进行验证和对比。

4.1 太赫兹指纹识别方法本地性能分析

精确度是衡量模型性能的一个关键指标。本文所设计的双分支卷积神经网络的输出为置信度，需为置信度确定阈值，本文中，置信度大于95%的太赫兹指纹被认为是未经篡改的指纹。精确度(Accuracy，A)计算如下：

$$A=\frac{n_{\mathrm{correct}}}{n_{\mathrm{total}}} \tag{10}$$

式中n_{correct}和n_{total}分别为正确分类的样本和样本

总数。

识别精确度曲线如图 4 所示，经过 3 000 轮左右的训练，在初始波动后精确度逐渐提高，最终趋于稳定并接近于 1(即 100%的识别精确度)。在 500~2 000 轮的训练过程中，随着训练轮数的增加，模型的精确度迅速上升。此时，神经网络通过调整权重和参数，逐步学会了任务中的基本模式和特征。这个阶段的快速提升表明网络对数据的学习能力较强，并在不断优化过程中表现出良好的收敛趋势。在训练的中间阶段(1 000~2 000 轮)，精确度曲线出现了一些波动，这种波动可能是由于模型在训练过程中遇到了局部最优解或振荡，网络在进行某些细节上的调整；或由于过拟合和欠拟合的交替作用，导致精确度表现不稳定。但总体而言，这些波动幅度较小，并没有显著影响精确度的整体上升趋势。当训练轮数接近 3 000 轮时，精确度的提升速度开始减缓，最终趋于稳定，并接近 1，表明神经网络已经收敛，基本达到了最佳的训练效果。精确度的平稳上升并最终稳定在一个较高的值，表明模型已经充分学习了任务中的特征，并且不再发生明显的过拟合现象。

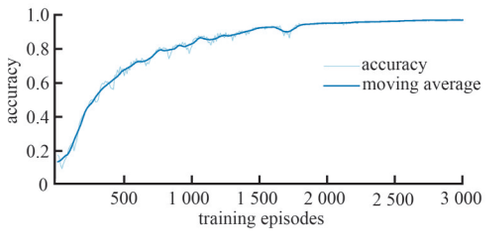

Fig.4 Terahertz fingerprint local recognition accuracy
图 4 太赫兹指纹本地识别精确度

综上所述，通过对双分支卷积神经网络在联邦学习环境下的太赫兹指纹识别训练过程进行分析可以发现，模型在初始阶段(约 500~2 000 轮)精确度迅速提升，说明本地模型较快地学习并掌握了指纹辨识所需的关键特征；此后本地模型在中间阶段(约 1 000~2 000 轮)出现小幅波动，主要归因于非独立同分布数据、模型聚合策略以及部分客户端在局部训练中的过拟合或欠拟合所导致的振荡；随着训练的持续进行，精确度曲线逐渐平稳并于约 3 000 轮时接近 1，表明本地模型已基本收敛并在本任务上达到理想的分类效果。整体而言，本地模型不仅能在短期内显著提升识别精确度，也能在后期有效克服训练过程中的波动并最终实现稳定、优异的识别性能。

4.2 联邦学习架构下太赫兹指纹识别方法性能分析

对联邦学习架构下太赫兹指纹识别方法进行性能分析。首先分析联邦学习聚类的性能，图 5 为联邦学习设备在不同区域中的聚类效果(图中的蓝色填充区域表示每个聚类内设备的集中程度，横坐标表示余弦距离，纵坐标表示不同的聚类(1~4，表示 4 个不同的聚类组)，每个聚类的形状代表了设备在该聚类中的分布情况。从图中可见，所有簇内设备的余弦距离主要分布在[0.1,0.6]区间，表明所提方法能有效将特征相似的设备归入同一聚类。其中，簇 1 的余弦距离分布最集中，主要小于 0.55，说明该簇内设备特征一致性最强；簇 3 和簇 4 的分布范围稍宽，延伸至 0.7 附近，可能存在更多特征差异。尽管不同簇的内部差异略有不同，但聚类边界清晰，各簇之间几乎无重叠，体现出良好的簇间可分性。整体来看，图 5 验证了所提方法具备较强的设备分簇能力，能够在保持簇内紧致性的同时确保簇间差异性，能够提升联邦模型的聚合质量与识别性能。

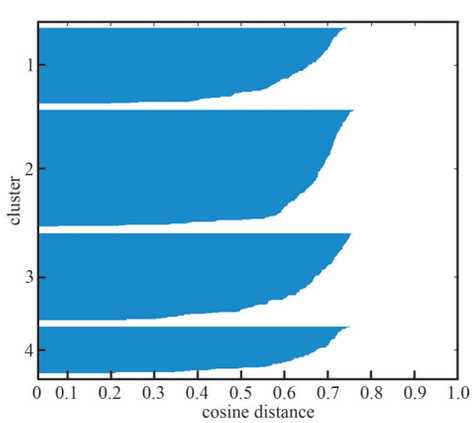

Fig.5 Device clustering effect of the proposed method
图 5 所提方法的设备分簇效果

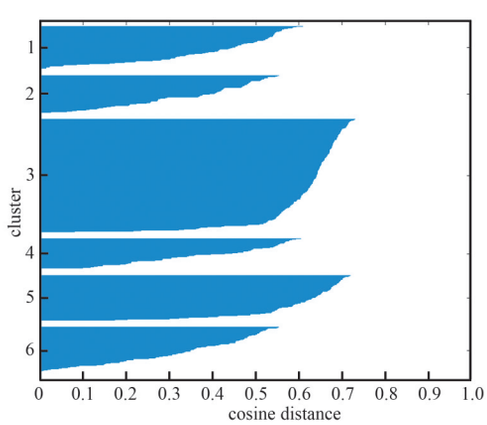

Fig.6 Discussion on the effect of different number of clusters
图 6 不同分簇数量的效果讨论

分析联邦学习中的分簇方法在通信开销与设备计算资源间的权衡关系，如图 6 所示。首先，在分簇规模与通信开销方面。当分簇数量增加(即每簇内设备数量减少)时，簇内设备数据分布趋于同质化，有助于提高模型的训练精确度，但同时也会增加联邦聚合的通信频率，导致通信开销增加；反之，若分簇规模较大，则通信次数有所减少，但簇内数据的异质性增加，可能会降低模型的收敛速度与精确度。其次，分簇规模也直接影响设备的

计算负载。当簇内设备数量减少时，每个设备需承担更多的本地计算任务以完成模型频繁迭代，因此会显著增加单设备的计算压力；相反，较大的簇规模可分摊计算负载，但可能会面临聚合模型精确度下降的问题。因此，在实际部署中需综合考虑通信带宽、网络稳定性和单个设备计算能力等实际因素，合理设计分簇规模与策略，以在通信成本和设备计算资源之间实现最优的权衡。

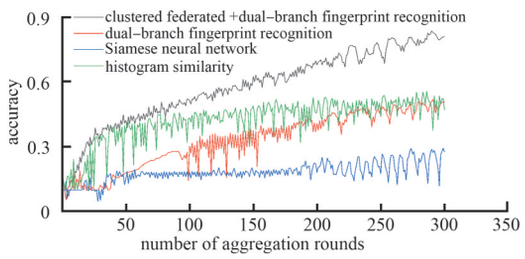

Fig.7 The accuracy of FL and its comparison with similar algorithms

图 7 联邦学习的精确度效果及与同类算法的对比

图 7 为 4 种不同模型在训练过程中的精确度变化。从这 4 条曲线可以看出，不同的模型在训练过程中的精确度提升存在明显差异。“分簇联邦+双分支指标识别”方法的精确度在训练初期呈现缓慢上升的趋势，但随着训练轮数的增加，精确度明显提升并趋于稳定。训练至约 100 轮时，精确度显著上升，接近 0.6；继续训练后，精确度稳定提高，并最终收敛至 0.9 左右，表明该方法具有很好的收敛性和较高的训练效果。整个训练过程较为平稳，几乎没有出现明显的波动，说明该方法的优化过程较为顺利，能够达到较高精确度。“双分支线性识别”方法在训练初期(约前 50 轮)精确度提升较为缓慢，初始精确度仅略高于 0.1；随着训练轮数的增加，在训练到约 100 轮时，精确度达到 0.4，之后的精确度提升变得更加平缓，其增长速度较“分簇联邦+双分支指标识别”方法要慢。尽管该方法最终在训练的后期收敛至较高的精确度，但整个过程的精确度提升幅度相对较小，可能存在一定的训练瓶颈，表明该模型可能需要进一步优化，或在面对数据的复杂性时，表现出一定的局限性。“Siamese 神经网络”在训练的初期(约前 100 轮)有较大的精确度波动，尤其在训练初期，精确度波动幅度较大，说明该方法可能在前期训练过程中对数据的相似性学习存在不稳定性。但随着训练的进行，精确度逐渐趋于平稳，并在接近 300 轮时收敛至约 0.6。这一趋势表明 Siamese 神经网络在学习相似度任务时表现出较强的灵活性和一定的学习能力，但其训练过程较为不稳定，可能需要更多的优化来提升模型的稳定性。“直方图相似度”方法的精确度在训练初期(大约前 100 轮)快速上升，在约 50 轮时，精确度接近 0.4，显示出较快的收敛速度，但训练后期(100~250 轮之间)，精确度的提升速度变缓，且出现了明显的波动，表明该方法可能在后期出现了过拟合或在局部最优解附近振荡。最后，精确度稳定在 0.6 左右，表明该方法尽管在初期表现优异，但在训练过程中受到一定的限制，难以进一步突破精确度的上限。

由此可见，采用“分簇联邦的双分支深度识别”模型在应对多样化的客户端数据时具有较强的学习能力与收敛稳定性，可在兼顾通信与计算资源的前提下取得优异的太赫兹指纹识别性能。

综合上述实验与分析可见，FL 架构下的分簇策略对于太赫兹指纹识别具有重要意义：一方面，合理的分簇能在设备相似性较高的簇内实现紧凑聚类，从而在非独立同分布环境下保证模型训练的有效性；另一方面，不同的分簇规模在通信开销与设备计算资源之间存在明显的差异性，需结合实际应用场景进行取舍，以最大化模型收益并尽量降低成本。

5　结论

本文提出的太赫兹指纹识别与分簇 FL 协同方法不仅有效提升了识别精确度，还解决了隐私保护和数据共享问题，为电力设备的安全监测和攻击预防提供了一条新技术路径，具有广阔的应用前景。未来的研究可进一步优化模型的稳定性和泛化能力，针对复杂环境下的抗干扰性能进行深入探索；同时，还需改进联邦聚合机制以提高数据融合效率和安全性，并探索太赫兹技术与其他先进感知技术的融合方案，以提升电力设备的安全管理水平。未来工作中，需在实际有源配电台区的环境中对本方法进行进一步验证，尤其是针对太赫兹传感器的部署和维护问题展开深入研究。如何在真实台区中平衡识别精确度、传感器寿命及运维投入，将是后续研究和实际应用亟需解决的关键挑战。

参考文献：

[1] HUANG Xiaoge,QIN Zhijun,LIU Hui. A survey on power grid cyber security:from component-wise vulnerability assessment to system-wide impact analysis[J]. IEEE Access, 2018(6):69023-69035. DOI:10.1109/ACCESS.2018.2879996.

[2] 陈智,刘轲,李玲香,等. 太赫兹通信感知一体化技术综述[J]. 中国科学(信息科学), 2024,54(5):1215-1235. (CHEN Zhi,LIU Ke,LI Lingxiang,et al. Survey of terahertz integrated communication and sensing technology[J]. Science in China(Information Sciences), 2024,54(5):1215-1235. DOI:10.1360/SSI-2023-0354.

[3] SHAH R,AMJADY N,BINTE N S,et al. Wildfire impacts on security of electric power systems:a survey of risk identification and

mitigation approaches[J]. IEEE Access, 2024(12):173047-173065. DOI: 10.1109/ACCESS.2024.3498036.

[4] 施江勇,高志远,刘天祎,等. 基于PUF的TPM架构设计与应用研究[J/OL]. 计算机工程与科学, 2024-11-01. http://kns.cnki.net/kcms/detail/43.1258.TP.20241101.1110.002.html. (SHI Jiangyong, GAO Zhiyuan, LIU Tianyi, et al. Design and application research of TPM architecture based on PUF[J]. Computer Engineering & Science, 2024-11-01. http://kns.cnki.net/kcms/detail/43.1258.TP.20241101.1110.002.html.)

[5] 陈梦迪,张巍,沈雷,等. 基于时频和双谱特征融合的DA-ResNeXt50射频指纹识别方法[J]. 电信科学, 2024,40(9):54-65. (CHEN Mengdi, ZHANG Wei, SHEN Lei, et al. DA-ResNeXt50 method for radio frequency fingerprint identification based on time-frequency and bispectral feature fusion[J]. Telecommunications Science, 2024,40(9):54-65.) DOI:10.11959/j.issn.1000-0801.2024208.

[6] 吴克迪. 光学隐身、纳米识别、超分辨成像的傅里叶分析与数值仿真[D]. 武汉:武汉大学, 2014. (WU Kedi. Fourier analysis and numerical simulation of optical invisibility, nanopatterns recognition, and super-resolution imaging[D]. Wuhan, China:Wuhan University, 2014.)

[7] 伍章俊,许仁礼,方刚,等. 一种面向旋转机械多传感器故障诊断的模态融合深度聚类方法[J]. 电子与信息学报, 2025,47(1):244-259. (WU Zhangjun, XU Renli, FANG Gang, et al. A modal fusion deep clustering method for multi-sensor fault diagnosis of rotating machinery[J]. Journal of Electronics & Information Technology, 2025,47(1):244-259.) DOI:10.11999/JEIT240648.

[8] ZHAO Guifen, LI Ying, DU Liping, et al. Asynchronous challenge-response authentication solution based on smart card in cloud environment[C]// 2015 2nd International Conference on Information Science and Control Engineering. Shanghai, China: IEEE, 2015:156-159. DOI:10.1109/ICISCE.2015.42.

[9] IDRISS T, BAYOUMI M. Lightweight highly secure PUF protocol for mutual authentication and secret message exchange[C]// 2017 IEEE International Conference on RFID Technology & Application(RFID-TA). Warsaw, Poland: IEEE, 2017: 214-219. DOI: 10.1109/RFID-TA.2017.8098893.

[10] 焦昊,赵佳伟,韦磊,等. 基于深度迁移学习的电力系统暂态状态估计[J]. 电力建设, 2025,46(1):97-106. (JIAO Hao, ZHAO Jiawei, WEI Lei, et al. Transient state estimation for power system based on deep transfer learning[J]. Electric Power Construction, 2025,46(1):97-106.) DOI:10.12204/j.issn.1000-7229.2025.01.009.

[11] 陈金杰,王一蕾,傅仰耿. 注意力融合机制和拓扑关系挖掘的异构图神经网络[J]. 福州大学学报(自然科学版), 2025,53(1):1-9. (CHEN Jinjie, WANG Yilei, FU Yanggeng. Heterogeneous graph neural network based on attention fused mechanisms and topology relation mining[J]. Journal of Fuzhou University(Natural Science Edition), 2025,53(1):1-9.) DOI:10.7631/ISSN.1000-2243.24019.

[12] 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.) DOI:10.13336/j.1003-6520.hve.20230765.

[13] 杨挺,张剑,蔡绍堂,等. 计及隐私数据保护的多虚拟电厂协同调度方法[J]. 天津大学学报(自然科学与工程技术版), 2024,57(8):836-846. (YANG Ting, ZHANG Jian, CAI Shaotang, et al. Collaborative scheduling method for multivirtual power plants considering privacy data protection[J]. Journal of Tianjin University(Science and Technology), 2024,57(8):836-846.) DOI:10.11784/tdxbz202306011.

[14] XU Yihang, MAO Yuxing, LI Simou, et al. Privacy-preserving federal learning chain for Internet of things[J]. IEEE Internet of Things Journal, 2023,10(20):18364-18374. DOI:10.1109/JIOT.2023.3279830.

[15] GAO Bo, YANG Fan, CUI Nan, et al. A federated learning framework for fingerprinting-based indoor localization in multibuilding and multifloor environments[J]. IEEE Internet of Things Journal, 2023,10(3):2615-2629. DOI:10.1109/JIOT.2022.3214211.

[16] LEE E, CHEN X B, ASHOK M, et al. 12.5 A packageless anti-tampering tag utilizing unclonable sub-THz wave scattering at the Chip-Item interface[C]// 2024 IEEE international solid-state circuits conference(ISSCC). San Francisco, CA, USA: IEEE, 2024:226-228. DOI:10.1109/ISSCC49657.2024.10454498.

作者简介:

岳　洋(1990-),男,硕士,工程师,主要研究方向为智能配电网技术.email:yang.yue@tj.sgcc.com.cn.

张　磐(1983-),男,硕士,正高级工程师,主要研究方向为配电自动化、智能配用电技术.

吴　磊(1985-),男,高级工程师,主要研究方向为智能配电网和继电保护技术.

庞　超(1995-),男,硕士,工程师,主要研究方向为智能配用电技术研究.