分布式新能源场景下配电网虚假数据注入攻击检测

龚钢军[1]，张晓炜[1]，王路遥[1]，李璐含[1]，黄雨菲[1]，王浩淼[2]，扬爽[2]
（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 102206；
2. 国网辽宁省电力有限公司，沈阳市 110002）

摘　要：【目的】随着新型电力系统中分布式节点广泛接入配电网，频繁的数据交互增加了配电网遭受虚假数据注入攻击（false data injection attacks，FDIA）的风险。常规的数据驱动检测方法在挖掘数据特征时往往将所有数据作为一个整体，忽略了不同节点数据中的个性特征。针对这一问题，文章提出了一种基于最大信息系数的个性化联邦训练方法，用于分布式新能源场景下的虚假数据注入攻击检测。【方法】所提方法将检测模型部署在分布式边缘节点，提高了边缘节点的网络安全防护能力及本地数据隐私保护能力；通过应用多层神经网络进行个性化联邦训练，将其分为不同特征层来进行共性和个性特征分离，在分布式检测的基础上加强对异构节点数据的特征处理；考虑量测数据中的时间特征，通过引入最大信息系数深入挖掘数据中潜在的规律性特征，将分析结果融合个性化联邦训练，以提高对节点本身数据个性特征的提取能力。【结果】以含分布式新能源节点的园区数据为例进行仿真分析，所提方法相比传统联邦框架和不考虑相关性分析的检测方法，检测准确率、精确率、召回率和 F1 分数均有所提升；最大信息系数在处理周期性数据时具有较好的个性特征提取能力。【结论】所提方法增加了对数据共性和个性特征的分离和提取，在客户端数量较多时检测模型具有较快的收敛速率，更适合分布式新能源场景下的 FDIA 检测。

关键词：虚假数据注入攻击（FDIA）；分布式节点；个性化联邦学习；最大信息系数；数据安全
中图分类号：TM73；TP183　　**文献标志码**：A　　**文章编号**：1000-7229（2026）04-0016-12
DOI：10. 12204/j. issn. 1000-7229. 2026. 04. 002

Detection of False Data Injection Attacks on Power Distribution Networks in Distributed Renewable Energy Scenarios

GONG Gangjun[1], ZHANG Xiaowei[1], WANG Luyao[1], LI Luhan[1], HUANG Yufei[1]
WANG Haomiao[2], YANG Shuang[2]
（1. Beijing Engineering Research Center of Energy Electric Power Information Security（North China Electric Power University）, Beijing 102206, China; 2. State Grid Liaoning Electric Power Supply Co. , Ltd. , Shenyang 110002, China）

ABSTRACT: [**Objective**] With the extensive integration of distributed nodes in new power systems into distribution networks, frequent data interactions increase the risk of false data injection attacks（FDIA）on the distribution networks. Conventional data-driven detection methods tend to treat all data holistically when mining data features, usually ignoring individual characteristics in data from different nodes. To address this problem, this paper proposes a personalized federated training method based on maximum information coefficient for false data injection attack detection in distributed renewable energy scenarios. [**Methods**] The proposed method deploys the detection model in distributed edge nodes, which improves the network security protection and local data privacy protection of the edge nodes. Multi-layer neural networks subjected to personalized federated training are separated into distinct feature layers to decouple common and individual features, thereby enhancing the feature processing of heterogeneous node data on the basis of distributed detection. Considering the temporal features in the measurement data, the potential regular features in the data are deeply mined by introducing the maximum information coefficient, and the analysis results are fused into the personalized federated training in order to improve the ability of extracting the personality features of the nodes′ own data. [**Results**] The park data containing distributed renewable

基金项目：国家重点研发计划资助项目（2022YFB3105100）

energy nodes is taken as an example for simulation analysis, and the proposed method improves the detection accuracy, precision, recall, and F1 score compared to the traditional federated framework and the detection method that does not consider correlation analysis. Maximum information coefficient demonstrates better personality feature extraction when dealing with periodic data. [**Conclusions**] The proposed method enhances the separation and extraction of common and individual features of the data, and the detection model exhibits a faster convergence rate when there are a large number of clients, rendering it more suitable for FDIA detection in distributed renewable energy scenarios.

This work is supported by National Key R&D Program of China (No. 2022YFB3105100).

KEYWORDS: false data injection attack (FDIA); distributed nodes; personalized federated learning; maximum information coefficient; data security

0　引　言

随着大量分布式柔性资源接入配电网[1-2]，各业务主体之间的交互需求和数据流转需求急剧增加[3]，数据的频繁交互与流转带来了新的安全风险和隐私保护需求[4]。另外，随着“云大物移智”等数字技术在电力系统中的广泛应用，其面临的网络攻击风险也随之显著增加[5-6]，亟需开展配电网数据网络攻击防护方法研究，保障电力系统数据安全交互共享。

虚假数据注入攻击（false data injection attacks，FDIA）是常用的高威胁网络攻击手段[7]，其通过构建攻击向量篡改量测数据，引起调度中心对电网状态的误判，可直接对电网的运行稳定性造成影响[8]。2015年乌克兰多个区域电网受到恶意网络攻击[9]，攻击者采用恶意指令、恶意软件输送等方式进行协同攻击，导致乌克兰大规模停电。因此，网络攻击检测问题已成为学术研究焦点。目前，FDIA检测方法主要分为基于模型驱动和基于数据驱动两类：1）基于模型的检测方法依据电力系统参数信息和系统模型，通过分析特定时段内量测数据是否超出阈值，检测是否存在FDIA，主要包括状态估计[10]、物理特性[11]、图论[12]、矩阵论[13]等方法，但随着数字化技术不断发展，FDIA攻击手段变得更为隐蔽，模型驱动的检测方法难以适用于不断变化的攻击手段；2）基于数据驱动的检测方法不依赖于系统模型和参数信息，利用大数据分析和机器学习算法挖掘和学习数据特征，在面对变化的FDIA攻击手段时呈现出一定优势，常用的数据特征学习模型包括Transformer编码器[14]、求和检测器[15]、生成对抗网络[16]、卷积神经网络[17]等。总体来说，上述两类方法均属于集中式检测模式，均需将所有节点的原始数据汇聚到数据中心进行检测。

在分布式新能源飞速发展的背景下，“光储充放”分布式装置大量接入配电网，集中式检测模式在采集、传输、计算和存储能力方面面临极大挑战，且边缘节点的数据安全防护需求也愈发增强。因此，分布式检测模式应运而生。文献[18]提出了一种基于子网格的分布式FDIA检测框架，利用时空神经网络学习子网格级的代表性特征来表示数据间的时空关系，提高了系统并行计算的能力，但忽略了边缘节点的安全防护。为了在进行分布式检测的同时提高边缘节点的安全防护能力，许多学者将联邦学习（ederated learning，FL）运用到FDIA检测领域。文献[19-22]提出了基于联邦学习的端-边-云协同FDIA检测框架，通过设置边缘节点检测器来收集、存储和检测数据，将传统集中式检测模式转变为分布式检测模式。上述研究虽解决了集中式检测带来的数据中心计算能力瓶颈问题，但由于训练得到的模型是全局模型，缺乏对节点个性化特征的挖掘，也缺乏对个性化联邦学习（personalized federated learning，PFL）框架的研究分析。

个性化联邦学习允许每个参与方依据自己的数据或需求对模型进行调整，生成个性化模型[23]。已有学者将PFL应用到电力系统中，文献[24]构建了基于分量选择的PFL框架，用于不同区域的负荷预测；文献[25]通过上传部分而非全部模型参数的方式保留用户个性化差异，提高模型对单个用户的预测准确度，增强了算法在不平衡数据集上的适应能力。PFL在面对不同类型节点的异构数据时具有很好的应用效果，因此，对于包含大量分布式节点的配电网FDIA检测场景具有一定的适用性。

FDIA个性化检测模型构建时需要对节点历史数据进行特征提取。最大信息系数（maximal information coefficient，MIC）可以衡量不同变量之间的关联性[26]，能够提取不包含冗余信息的关键特征。在FDIA检测中，MIC常作为分类后的检测器[27]，通过衡量电力系统节点间互联关系强弱和MIC值的变化来判断节点是否受到攻击，降低误报率，提高模型检测效率[28]。本文从节点个性化特征提取的角度出发，利用MIC分析同一节点不同时段下数据间的相关性，将计算结果作为训练的部分输入融合进模型训练中。

综上，本文提出一种基于最大信息系数的个性

化联邦训练方法(correlation-personalized federated learning,co-PFL),采用分布式检测来应对分布式新能源场景中边缘节点抵御FDIA能力薄弱的问题。应用个性化联邦学习方法构建分布式的个性化检测模型,引入MIC对节点历史数据进行特征提取,增强个性化模型的检测能力。实验仿真表明,所提方法对具有明显个性特征的节点数据具有较好的特征提取能力和FDIA检测能力。

1 分布式新能源场景下虚假数据注入攻击检测模型

分布式新能源广泛接入配电网场景下,配电网中基于数据驱动的虚假数据注入攻击检测具有以下特点:

1)配电网拓扑结构和供电方式发生变化及信息交互更为频繁,配电网数据特征的复杂性提升,FDIA检测难度增加;

2)配电网中分布式节点增多,FDIA的攻击域变大,而节点本身缺乏较强的FDIA检测能力;

3)数据驱动的FDIA检测方法依赖于数据特征,建设时间较短的分布式新能源节点历史数据少,需从较少数据中挖掘更多可用特征。

针对以上特点,提出去中心化的分布式检测方法,利用联邦共享训练机制构建分布式检测模型,在特征提取过程中进行数据特征分离,提高检测模型的本地适用性。检测模型如图1所示,分为信息物理层、联邦学习层和特征提取层。层级间按配电网整体结构、中心服务器和边缘节点之间的联邦训练、联邦训练中数据特征提取方法不断细化分析,最终实现分布式的个性化FDIA检测功能。

1)信息物理层:描述分布式节点接入配电网后配电网物理形态和信息交互情况的变化。大量光伏、储能接入配电网中,产生了如光伏发电量、储能电量及运行状态等新数据类型,需求响应等场景下的信息交互也会增加数据特征的复杂性。同时,FDIA会出现在分布式节点数据采集和数据交互的过程中,更难以发现。

2)联邦学习层:侧重于中心服务器和边缘节点间的联邦训练过程。各参与方使用中心服务器初始化模型参数,基于本地数据进行模型训练。训练达到一定次数后上传一次本地模型参数,由中心服务器聚合后再次下发至参与方继续训练,直至模型收敛或达到参数交换次数要求。训练过程避免了本地数据的直接传输,降低了隐私泄露风险。

3)特征提取层:聚焦于数据特征,将多层的神经网络模型分为共性特征和个性特征两部分,通过个性化联邦学习和相关性分析实现数据共性和个性特征提取,得到个性化检测模型。

2 个性化联邦下虚假数据注入攻击检测

2.1 分布式场景下虚假数据注入攻击问题描述

分布式新能源广泛接入场景下,源网荷储间数据互动频繁,各类节点易遭受FDIA威胁,攻击者通过篡改数据对系统规划和运行造成影响。然而传统检测方法难以对FDIA进行有效检测。

传统检测错误数据的方法为残差检验,依据量测残差向量的欧氏范数是否超出预先设定的阈值来判断是否存在错误数据。错误数据的来源包括随机干扰、设备故障和受到攻击后的虚假数据。其中,部分FDIA无法通过残差检验检测出虚假数据。此类FDIA的攻击原理为在获取电力系统全部或部分配置信息(包括电网拓扑结构、线路参数、量测数据等)后,攻击者构建能绕过残差检验的攻击向量,具体描述如下。

分布式新能源场景下的系统模型表示为:

$$\boldsymbol{z}=\boldsymbol{z}^{c}+\boldsymbol{e} \tag{1}$$

式中:$\boldsymbol{z}$为系统收集到的量测向量,包括新能源发电及储能的功率、环境参数、开关状态等量测数据;$\boldsymbol{z}^{c}=h(\boldsymbol{x})$为状态$\boldsymbol{x}$下的真实值,$h(\cdot)$为量测函数向量;$\boldsymbol{e}$为满足高斯分布且均值为0的量测向量误差。此时,量测残差向量的欧氏范数为:

$$r=\left\|z-h(\boldsymbol{x})\right\| \tag{2}$$

令$\boldsymbol{c}=\hat{\boldsymbol{x}}_{a}-\hat{\boldsymbol{x}}$,遭受FDIA后被篡改的量测向量欧氏范数为:

$$r_{a}=\left\|z+\boldsymbol{a}-h\left(\hat{\boldsymbol{x}}_{a}\right)\right\|=\left\|z-h(\hat{\boldsymbol{x}})+\boldsymbol{a}-h(\boldsymbol{c})\right\|=\left\|r+\boldsymbol{a}-h(\boldsymbol{c})\right\| \tag{3}$$

式中:$\boldsymbol{a}$为攻击向量;$\hat{\boldsymbol{x}}$为状态变量的估计值;$\hat{\boldsymbol{x}}_{a}$为攻击后的状态变量估计值。

当攻击者掌握电力系统全部或部分配置信息时,精心设计出攻击向量$\boldsymbol{a}=h(\boldsymbol{c})$,此时系统残差未改变,FDIA无法通过残差检验检测出来。未能检测出的虚假数据会给电网稳定运行产生极大影响。例如,光伏发电输出功率数据遭到篡改,造成线路过载或停电;储能电量和开关状态遭到篡改,造成电网在使用储能进行削峰填谷时对设备状态误判等。

2.2 个性化联邦学习FDIA检测的可行性

联邦学习本质上是一种分布式的机器学习方法,在共同训练模型的同时保护了数据隐私安全。每个数据节点利用本地数据进行模型训练,将模型

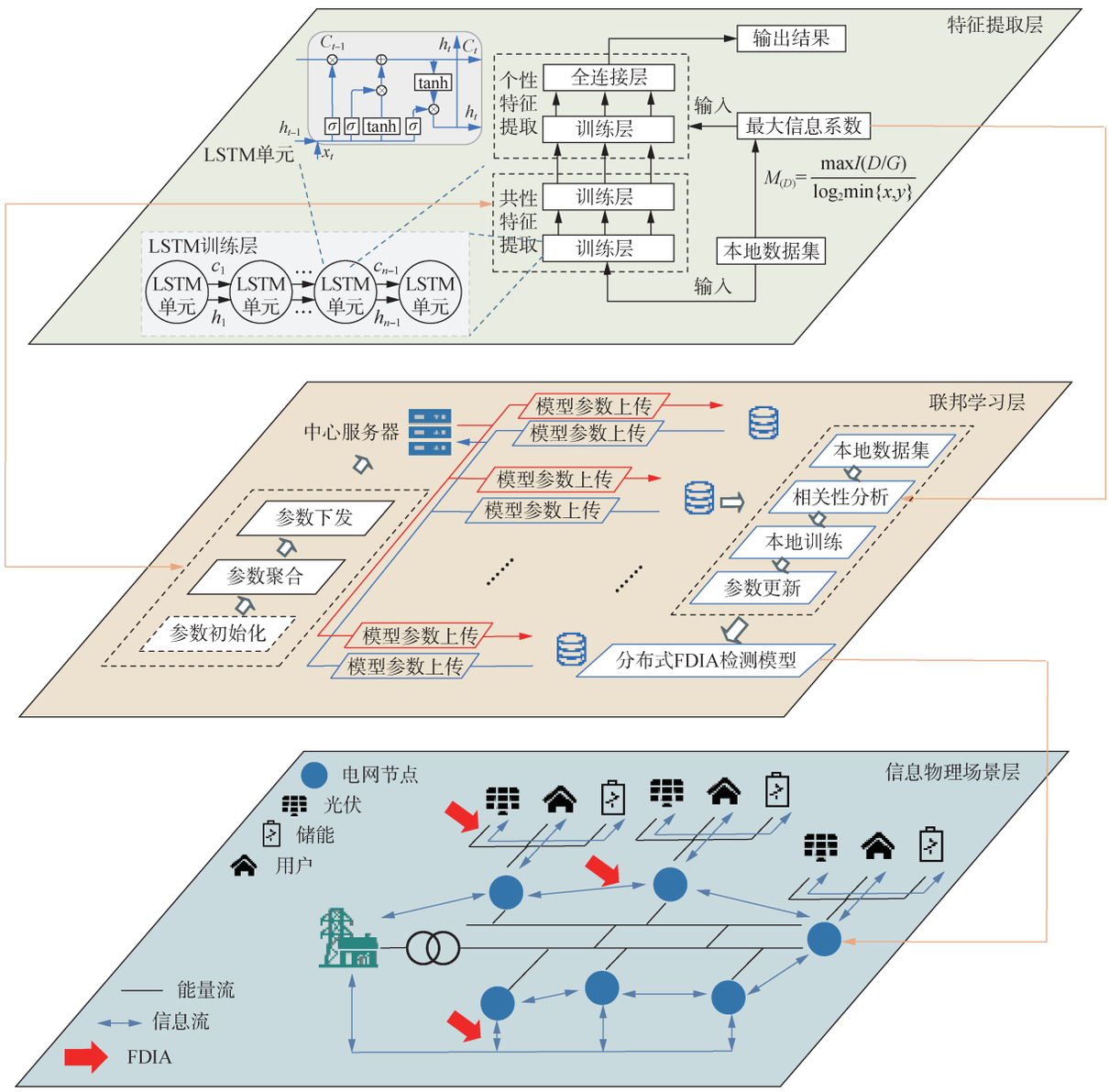


图 1　分布式新能源场景下 FDIA 检测模型

Fig. 1　FDIA detection model in distributed renewable energy scenarios

参数或梯度上传到中心服务器，聚合后下发给本地模型继续训练，模型达到最优时训练结束。由于原始数据不在训练过程中进行传递，因此联邦学习具有隐私保护效果。

传统联邦学习和个性化联邦学习的架构如图 2 所示。传统联邦学习训练得到的模型全局共享，难以兼顾共性特征较强的节点和个性特征较为明显的节点，不适用于分布式节点的异构数据。个性化联邦学习方法将节点处的模型进行分层，其中个性层不参与联邦的参数上传和下发，只交换共性层的模型参数，在检测模型中同时保留了不同节点间的共性特征和节点自身隐含的个性特征。保留个性特征的优势在于攻击方难以获取全部的本地数据和电网配置信息，无法对节点数据特征进行完全挖掘，构建

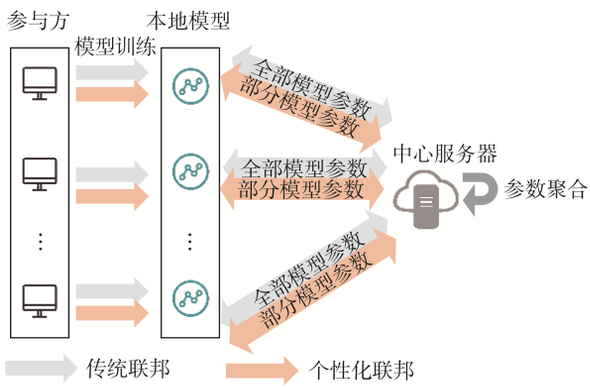


图 2　FL 和 PFL 架构对比

Fig. 2　Comparison of FL and PFL architectures

符合节点特征的攻击向量，其离群特性会更为明显，从而提高检测效率。

2.3 个性化检测模型构建

在分布式节点数据中，个性特征来自于用户用电习惯或者光伏、储能设备容量存在的差异性等，共性特征源于节点间的耦合关系和上级电网的统一规划。本文采用基于相关性分析的个性化联邦训练方法，使用多层长短期记忆网络（long short-term memory，LSTM）融合相关性分析方法进行共性和个性特征提取，在边缘节点构建个性化的分布式FDIA检测模型。检测模型训练框架如图3所示。

2.3.1 基于MIC的数据相关性分析

MIC是一种衡量两个变量间相关性的分析方法[26]，常用于机器学习的特征选择。其基本思想为：对于给定的数据集，将其构成的散点图划分为x行y列的网格，计算此时特征分布的互信息。保持x和y不变，采用不同的网格划分方案得出不同的互信息值，归一化后的互信息最大值即为MIC。计算方法如下：

$$M_{(D)}=\max_{xy<B(n)}\left\{L\left(D,x,y\right)/\log_2\min\left\{x,y\right\}\right\} \tag{4}$$

式中：$M_{(D)}$为计算出的MIC值；D为数据集；$L\left(D,x,y\right)$为互信息值；n为样本数量；$B(n)$为网络规格约束，通常设置为$n^{0.6}$。

MIC可以很好地衡量两个变量之间的关联性，而电网中具有物理连接的节点因为耦合关系，其数据会呈现较强的映射关系，因此在许多FDIA检测方法中，MIC常作为检测结果正常时的校验器，以减少误报的产生。在这些方法中，MIC用于分析不同节点间耦合关系强弱以判断是否受到攻击。如果从数据特征的角度出发，不同节点中存在差异化的潜在个性特征，利用MIC可以对这种特征进行提取，融合到个性化联邦训练中。

差异化的个性特征体现在：电网量测数据中的潜在特征与时间密切相关。当量测数据按一维时间序列进行排列时会呈现明显的波动，但是如果以二维的方式按不同时间尺度绘制数据，可以观察到数据中隐含的规律性。文献[29]以每周为时间尺度对电力用户用电量数据进行分析，发现了数据的分布规律，以此作为窃电用户的识别依据。在FDIA检测中，若节点受到攻击，量测数据中的规律性也会在一定程度上被弱化，这种变化可以作为数据是否受到FDIA的判断依据之一。

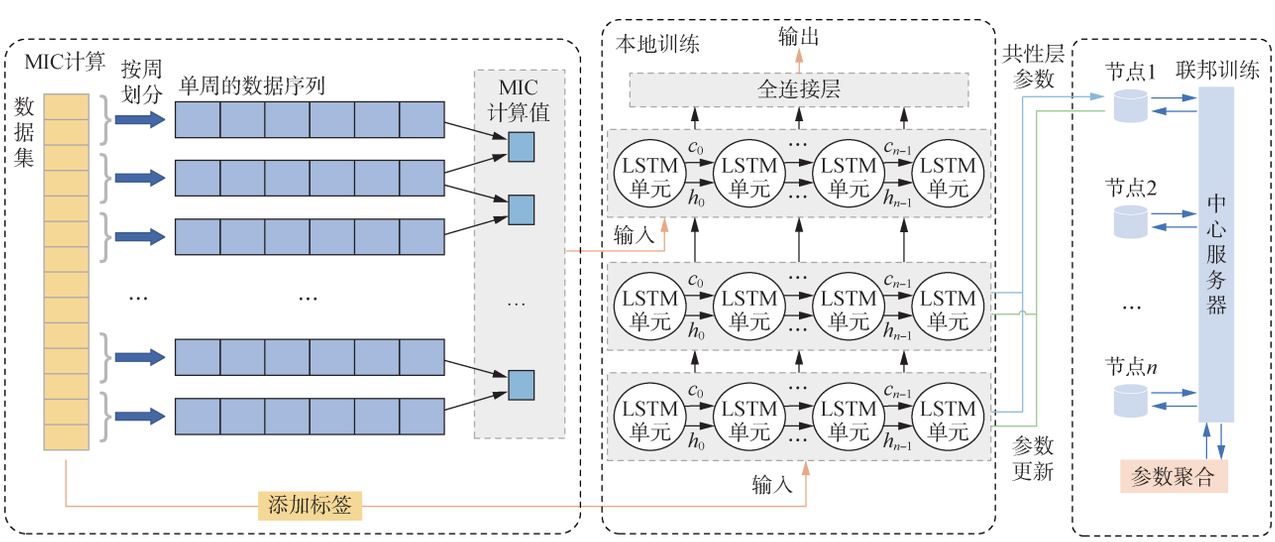
为了提取这种隐含的规律性特征，将节点的历史数据序列以某一时间尺度进行划分，计算得到一组可以呈现节点量测数据个性的特征值。此时MIC比较的对象不再是不同节点，而是将同一节点在不同时段的数据视为多个不同的变量，比较这些变量间的相关性。在同一时间尺度下，节点间的个性化差异体现在MIC值中。对于不同类型节点能够呈现其规律性的时间尺度不同，可以根据MIC在不同尺度下的分析结果选择最能代表该节点个性特征的时间尺度。MIC值计算方法如图3(a)所示。

2.3.2 个性化联邦训练模型构建和流程设计

基于个性化联邦的检测模型构建如下：

1)模型结构：训练使用的神经网络结构由3个训练层和一个全连接层组成，下层的两个训练层作为共性特征层，参与联邦训练；上层的一个训练层和全连接层作为个性特征层，用于处理相关性信息和输出分类结果，模型结构如图3(b)所示。

2)模型输入：检测模型的输入包括节点的本地



(a) MIC值计算方法　(b) 本地个性化联邦训练　(c) 联邦训练

图3 co-PFL训练模型

Fig. 3 co-PFL training model

数据、参与训练的虚假数据、标签和MIC计算值。标签用于指示数据类别。MIC计算值只作为个性特征层的输入，为保证模型输入的结构统一，将输入共性特征层中的MIC计算值设定为一个固定的弱相关值（MIC<0.6时视为弱相关[30]）。

3）聚合算法：常用的FedAvg聚合算法在面对异构节点数据时可能会存在收敛性不良等问题。为增强模型对异构数据的自适应性，采用FedAdam作为中心服务器端的聚合算法。FedAdam的优势在于：（1）可以根据历史训练的平均训练损失选择最佳超参数。对于不同地理位置下的分布式场景，节点类型和不同类型节点组成比例存在差异，此时可以自适应选择参数以达到最优训练效果。（2）超参数中引入τ作为算法自适应程度的调节参数，提供了更细粒度的适应性调整方法。

4）模型输出：检测模型输出为数据是否受到虚假数据注入攻击。将FDIA检测表述为真实数据和虚假数据的分类问题，训练得到一个可以判别数据中是否存在FDIA的分类器$g(\cdot)$：

$$g(X)=\begin{cases}1, & \text{存在FDIA}\\ 0, & \text{不存在FDIA}\end{cases} \tag{5}$$

模型训练步骤如下：

1）初始化：中心服务器初始化LSTM网络各层参数c_i、客户端学习率η_i、服务器学习率η、衰减常数β_1和β_2、适应性参数τ和v^{-1}、σ^{-1}，规定本地训练次数K和联邦训练次数P。初始化完成后中心服务器将网络参数下发至各客户端，同时各客户端使用本地数据计算MIC值。

2）本地训练：客户端根据接收的参数初始化本地模型，开始本地训练。每次训练中采用梯度下降法更新所有层参数。一轮训练共进行K次参数更新。

共性层输入如下：

$$\boldsymbol{X}_{\mathrm{c}}=\left[\boldsymbol{X}_{\mathrm{c}1},\boldsymbol{X}_{\mathrm{c}2},\cdots,\boldsymbol{X}_{ch},\cdots,\boldsymbol{X}_{cH}\right] \tag{6}$$

$$\boldsymbol{X}_{ch}=\left[\boldsymbol{u}_h,\boldsymbol{M}_{ch},T_{\mathrm{lable}}\right] \tag{7}$$

式中：$\boldsymbol{X}_{ch}$为h时刻的输入向量；$\boldsymbol{u}_h$为h时刻的量测数据向量；$\boldsymbol{M}_{ch}$为调整输入结构的补充向量，对应于个性层的MIC计算值，取值为0.5；T_{lable}为数据类别标签，$T_{\mathrm{lable}}=1$表示虚假数据样本，$T_{\mathrm{lable}}=0$表示真实数据样本。

个性层输入如下：

$$\boldsymbol{X}_{\mathrm{p}}=\left[\boldsymbol{X}_{\mathrm{p}1},\boldsymbol{X}_{\mathrm{p}2},\cdots,\boldsymbol{X}_{ph},\cdots,\boldsymbol{X}_{pH}\right] \tag{8}$$

$$\boldsymbol{X}_{ph}=\left[\boldsymbol{u}_h,\boldsymbol{M}_{ph},T_{\mathrm{lable}}\right] \tag{9}$$

式中：$\boldsymbol{X}_{ph}$为h时刻的输入向量；$\boldsymbol{u}_h$为h时刻的量测数据向量，与共性层一致；$\boldsymbol{M}_{ph}$为计算得到的MIC值。

3）参数上传：一轮训练完成后，各客户端计算本地模型共性层参数与中心服务器参数间的差值，将差值上传至中心服务器进行聚合。计算方法如下：

$$\Delta c_i^t=c_i^t-c_{\mathrm{s}}^t \tag{10}$$

式中：c_i^t为客户端i第t轮联邦训练前的参数；c_{s}^t为中心服务器第t轮更新前的参数。

4）参数聚合：中心服务器采用FedAdam作为聚合算法。计算方法如下：

$$c_{\mathrm{s}}^{t+1}=c_{\mathrm{s}}^t+\eta\sigma^t\Big/\sqrt{v^t}+\tau \tag{11}$$

$$\sigma^t=\beta_1\sigma^{t-1}+(1-\beta_1)\sum_{i\in I}\Delta c_i^t\Big/|I| \tag{12}$$

$$v^t=\beta_2 v^{t-1}+(1-\beta_2)\left(\sum_{i\in I}\Delta c_i^t\Big/|I|\right)^2 \tag{13}$$

式中：I表示客户端集合。

5）本地参数更新：中心服务器下发c_{s}^{t+1}至各客户端，客户端更新本地模型共性层参数，开启新一轮本地训练。当参数交换次数达到K时，结束训练。

2.4　算法复杂度分析

考虑到模型部署在边缘节点，高复杂度的算法对设备算力要求过高，因此对co-PFL进行复杂度分析，考虑个性化联邦学习服务器端、参数传输和客户端的时间复杂度总和。假设参数聚合算法的时间复杂度为t_{c}，联邦训练次数为P，则服务器端时间复杂度为$O(P\cdot t_{\mathrm{c}})$；假设参数传输的时间复杂度为t_{tr}，客户端数量为N，则参数传输时间复杂度为$O(P\cdot N\cdot t_{\mathrm{tr}})$；假设客户端训练时间复杂度为$t_{\mathrm{cl}}$，MIC计算复杂度为$t_{\mathrm{M}}$，联邦参数更新复杂度为$t_{\mathrm{u}}$，本地训练次数为$K$，则客户端时间复杂度为$N\cdot O(K\cdot t_{\mathrm{cl}}+P\cdot t_{\mathrm{u}}+t_{\mathrm{M}})$。总时间复杂度为$O\left(P\cdot t_{\mathrm{c}}+P\cdot N\cdot(t_{\mathrm{tr}}+t_{\mathrm{u}})+N\cdot(K\cdot t_{\mathrm{cl}}+t_{\mathrm{M}})\right)$。在实际实验过程中客户端训练时间远大于参数传输时间、参数聚合时间、客户端参数更新时间和MIC计算时间，基于以上假设，可以将总时间复杂度简化为$O(N\cdot K\cdot t_{\mathrm{cl}})$。传统联邦学习的算法复杂度为$O(N\cdot K\cdot t'_{\mathrm{cl}})$，其中$t'_{\mathrm{cl}}$为客户端训练时间。算法增加的时间复杂度只与本地训练时间有关。对于模型训练耗时的讨论将在3.3节展开。

3　算例分析

3.1　数据集构建

为验证所提方法的可行性，算例数据来源于中国北方某园区的数据集，该数据集由22个节点共32 716条数据组成，数据采集时间间隔为30 min，数据时长为4个月，包括用户用电量、光伏发电量、储能容量等电力数据。对于数据集中的缺失值采用插值

法对其进行恢复，如下式：

$$f(u_j)=\begin{cases}(u_{j-1}+u_{j+1})/2 & u_j\in\varnothing,u_{j-1},u_{j+1}\notin\varnothing\\0 & u_j,u_{j-1},u_{j+1}\in\varnothing\\u_j & u_j\notin\varnothing\end{cases}\tag{14}$$

式中：u_j表示用电量数据的值；$u_j\in\varnothing$表示对应时段的用电量数据值缺失。对于数据中可能存在的错误值，依据3σ准则减少异常值，如下式：

$$f(u_j)=\begin{cases}\mathrm{avg}(u)+2\mathrm{std}(u) & u_j>\mathrm{avg}(u)+2\mathrm{std}(u)\\u_j & u_j\leqslant\mathrm{avg}(u)+2\mathrm{std}(u)\end{cases}\tag{15}$$

式中：$\mathrm{avg}(u)$为u的平均值；$\mathrm{std}(u)$为u的标准差。为了保持不同数据间量纲的一致性，对所有数据进行归一化处理：

$$f(u_j)=[u_j-\min(u)]/[\max(u)-\min(u)]\tag{16}$$

式中：$\max(u)$、$\min(u)$分别为u中的最大值和最小值。

3.2 准确性分析

3.2.1 评估指标

采用准确率、精确率、召回率和F1分数作为模型性能评价指标。准确率A_c表示测试集中被正确分类的样本占所有样本的比例；精确率P_r表示测试结果为虚假数据的样本中被正确分类的样本比例；召回率R_e表示测试集中的虚假数据样本被正确分类的比例；F1分数S_c为精确率和召回率的调和均值。计算方法如下：

$$A_c=(T_p+T_n)/(T_p+T_n+F_p+F_n)\tag{17}$$

$$P_r=T_p/(T_p+F_p)\tag{18}$$

$$R_e=T_p/(T_p+F_n)\tag{19}$$

$$S_c=[(\alpha^2+1)P_rR_e]/[\alpha^2(P_r+R_e)]\tag{20}$$

式中：T_p、T_n分别表示被正确分类的虚假数据和真实数据量；F_p表示被错误分类为虚假数据的真实数据量；F_n表示被错误分类为真实数据的虚假数据量。F1分数中α通常取1。

3.2.2 不同模型准确性分析

为分析所提方法的模型检测效果，分别应用本地学习（local learning，LL）、集中学习（central learning，CL）、FL、支持向量机（support vector machines，SVM）、图卷积神经网络（graph convolutional networks，GCN）、co-PFL方法进行训练和检测。LL、CL、FL、co-PFL为同一模型（LSTM网络）在不同框架下的对比，SVM、GCN、co-PFL为同一联邦框架下不同检测模型的对比。在经过不同时间尺度的试验和分析后，用电、光伏、储能数据的时间尺度分别选择为一周、一日、一周。选取数据集中的10 000条数据进行模拟攻击[31]生成被篡改的数据，模拟幅值方差为$\sigma^2=0.06$的增量攻击，共42 716条数据样本，按照8∶2的比例随机选择样本作为训练集和测试集。数据攻击前后的最大标准化残差如图4所示，数据在受到攻击后残差值增大，但未超出常规检测阈值，仍无法通过状态估计检测出来。实验设置本地模型在每次本地更新期间训练100个epoch，客户端学习率设定为0.01，服务器学习率设定为0.01，min-batch为128，联邦通信轮次为20。评估结果如表1所示。

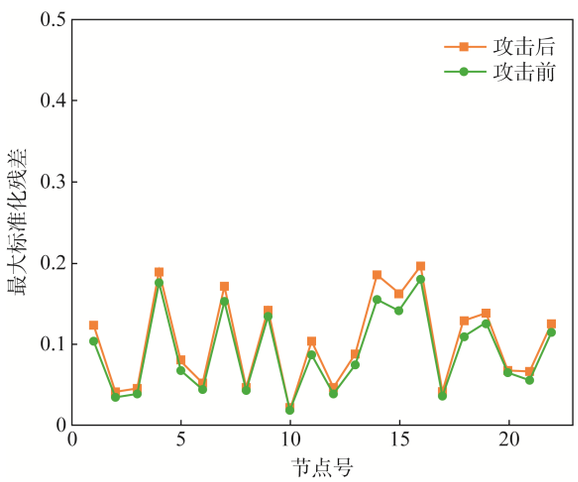


图4 各节点攻击前后的最大标准化残差

Fig. 4 Maximum standardized residuals before and after the attack on each node

表1 不同模型的评估结果

Table 1 Evaluation results of different models

检测模型	准确率	精确率	召回率	F1分数
LL	0.859 5	0.867 3	0.823 5	0.844 8
CL	0.866 9	0.875 3	0.831 9	0.853 0
FL	0.858 5	0.871 1	0.816 0	0.842 6
SVM	0.879 4	0.882 9	0.853 5	0.868 0
GCN	0.881 2	0.891 3	0.847 5	0.868 8
co-PFL	0.897 1	0.915 3	0.857 8	0.885 6

从表1可知，co-PFL方法的准确率、精确率、召回率、F1分数分别为0.897 1、0.915 3、0.857 8、0.885 6，其准确率相比LL、CL、FL、SVM、GCN分别提升了4.37%、3.48%、4.50%、2.01%、1.81%，说明该方法的总体训练效果明显优于其余几种训练方法。

对表1进一步分析，LL方法的准确率较低，原因在于缺乏对不同节点数据中共性特征的学习，且数据量少，学习效果较差。CL方法的准确率、精确率、召回率、F1分数为0.866 9、0.875 3、0.831 9、0.853 0，比FL方法分别高0.98%、0.49%、1.95%、1.23%，说明集中式训练方法可以得到较高准确率的全局模型，

但是需将所有原始数据进行汇集，数据在传输过程中存在网络安全风险；FL在构建分布式检测模型时，客户端进行本地训练后上传模型参数，避免了原始数据的直接传输，在降低传输成本的同时保护了本地数据的安全性和隐私性，但是降低了模型检测准确率。

co-PFL方法的准确率、精确率、召回率、F1分数比FL分别上升了4.50%、5.07%、5.13%、5.10%，这是因为co-PFL采用分层联邦方法和相关性分析对数据的共性特征和个性特征进行了分离，提高了特征学习效果，而FL则忽略了各客户端的个性特征。co-PFL方法的准确率相比SVM、GCN检测模型分别提升了2.01%、1.81%，这表明该方法在分布式新能源场景中具有较好的检测性能。

3.2.3　异构数据集准确性分析

为验证co-PFL方法在不平衡数据集下的表现，设置3种不同类型的数据集，如表2所示。数据集1为平衡数据集，数据集2代表数据量不同的情况，数据集3代表数据采样间隔不同的情况。分别应用FL和co-PFL方法进行建模，评估结果如图5所示。

表2　数据集设置

Table 2　Dataset settings

数据集编号	用电样本数	光伏样本数	储能样本数	FDIA样本数	总样本数量	采样间隔/min
1	10 000	3000	2000	5000	20 000	30
2	9000	2000	1000	3000	15 000	30
3	10 000	3000	2000	5000	20 000	60

由图5可知，在不同异构程度的数据集中，co-PFL方法的准确率均优于FL方法，且co-PFL的准确率稳定保持在较高水平，验证了该方法在高异构场景下的稳定性。

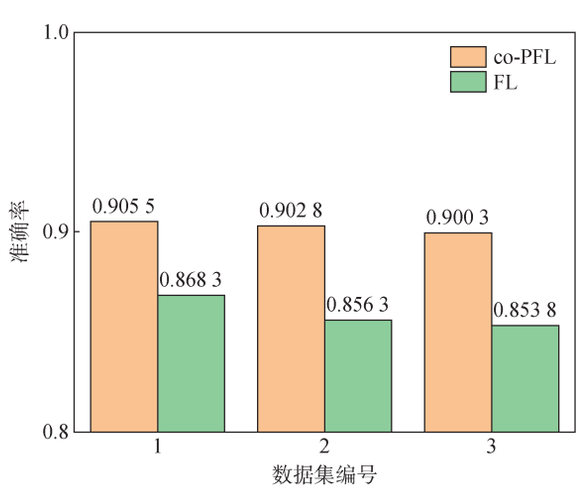


图5　不同数据集的准确率评估结果

Fig. 5　Accuracy evaluation results for different datasets

3.2.4　不同客户端数量准确性分析

为验证co-PFL方法的可扩展性，对不同客户端数量下模型检测准确率进行分析，如图6所示。从图中可以看出，客户端数较少时，模型检测准确率较低，随着客户端数增加，模型的准确率也随之提高，因此该方法具有较好的可扩展性。但是，在个性化联邦学习过程中，客户端数的增加也会带来系统开销的增大。本文的准确性分析实验选择客户端数为20以保证在一定程度准确率的基础上减少联邦过程中的通信开销。

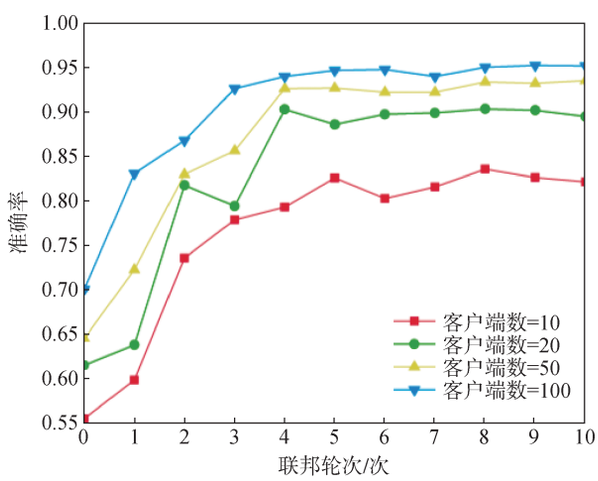


图6　不同客户端数量下模型检测准确率分析

Fig. 6　Model detection accuracy analysis with different number of clients

3.3　算法效率分析

记录3.2节中参与联邦训练的FL、SVM、GCN、co-PFL方法在训练和检测阶段的收敛过程，如图7所示。此外，为验证co-PFL方法在算法效率上的优越性，分别应用卷积神经网络（convolutional neural networks，CNN）、SVM、GCN在客户端数为10、20、50、100时进行联邦建模，模型的收敛时间如图8所示。

由图7可知，各检测模型在经过一定次数的联邦参数交换后可以收敛到最佳性能。其中，FL方法在12轮联邦训练后达到收敛，SVM、GCN方法在10轮后达到收敛，co-PFL方法在6轮后收敛达到最佳性能，收敛速度优于其他方法。

由图8可知，当客户端数量相同时，co-PFL的收敛耗时均小于其他常用模型。随着客户端数量的增加，各模型收敛耗时随之增加，co-PFL收敛时间的增加幅度相对较缓慢。当客户端数量较少时，SVM、GCN与co-PFL收敛时间较短，不同方法之间差距较小；当客户端数量较大时，co-PFL的收敛耗时明显小于其他常用模型。因此，该方法具有较好的训练效率。

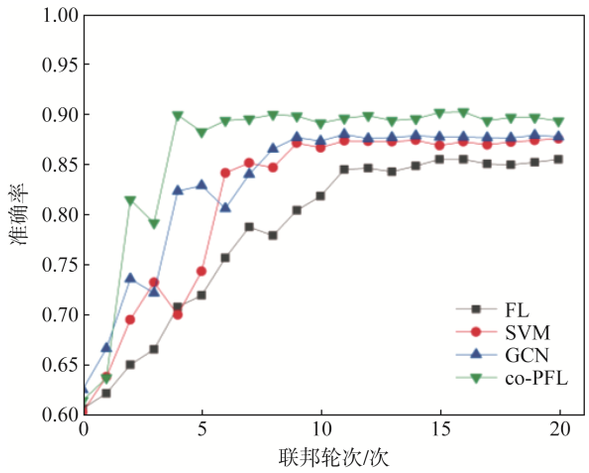


图7 训练和检测阶段各模型收敛过程

Fig. 7 Convergence process for each model in the training and detection phases

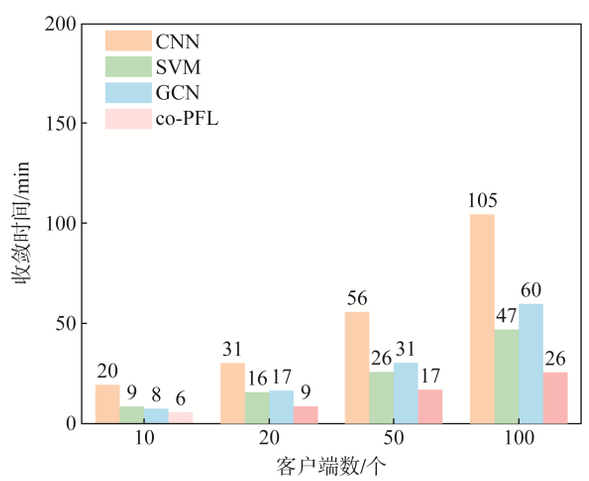


图8 不同客户端数量下各模型收敛时间比较

Fig. 8 Comparison of convergence time of each model with different number of clients

3.4 MIC效果分析

为验证MIC对数据时间周期性规律特征的提取效果，以用电量数据为例，选取1个节点连续4个月的用电量数据，按小时、日、周、月不同时间尺度从中随机选取连续时段数据，使用MIC对其进行相关性分析，分析结果如图9所示。

按周划分的数据MIC值在0.7~1.0之间，波动幅度较小，可以较好地呈现相关性，有利于提取用户个性特征；按小时划分的数据MIC值均小于0.3，说明对应时段内用电没有规律，因此数据间没有相关性或相关性很小；按日划分的数据MIC值在0.2~0.7之间，且波动幅度较大，未能体现用电规律；按月划分的数据MIC值在0.2~0.6之间，原因在于时间尺度大，不同月份的用电习惯受季节等因素影响较大，不适合作为特征提取的时间尺度。

以按周划分的数据为例，观察数据在受到攻击

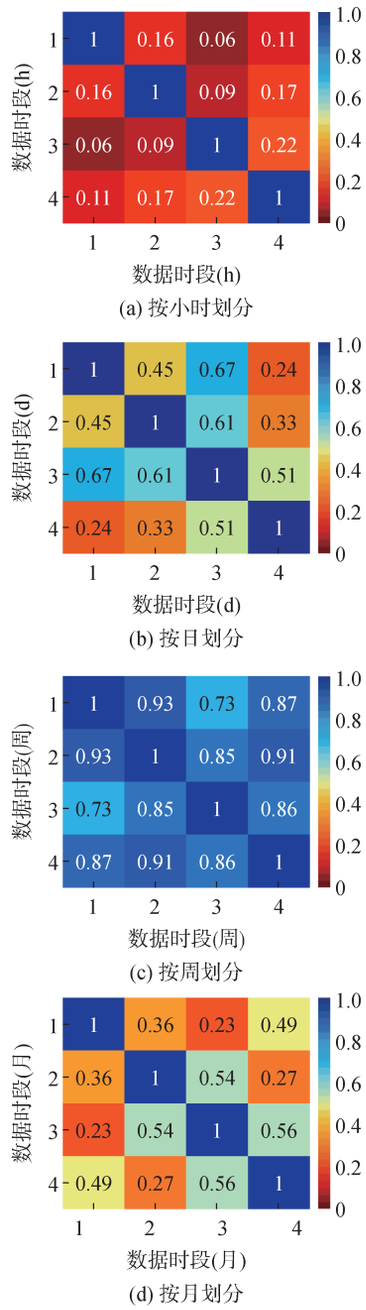


图9 不同时间尺度下的MIC热力图

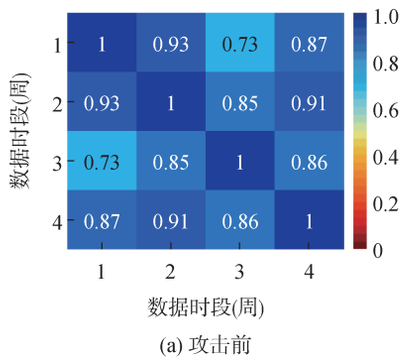
Fig. 9 Heat maps of MIC at different time scales

后的相关性变化。对其中第二周的数据进行模拟攻击，MIC分析结果热力图如图10所示。从图中可以看出，第二周数据与其他周数据之间的相关性与攻击前相比产生了明显变化，这种变化可用于对虚假数据的检测，原因在于攻击方不知道数据中的规律性，即每个用户的个性特征。

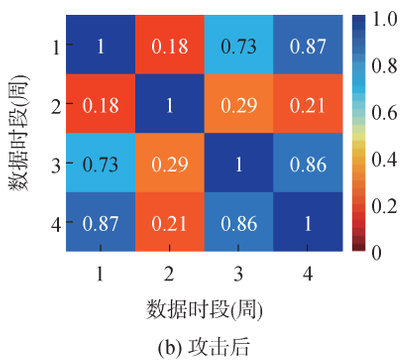
3.5 消融实验

3.5.1 相关性分析方法对比

为验证相关性分析方法对模型性能的影响，分别对用皮尔逊相关系数（pearson correlation coefficient，PCC）、斯皮尔曼相关系数（spearman



(a) 攻击前



(b) 攻击后

图 10　攻击前后的 MIC 热力图

Fig. 10　MIC heat maps before and after the attack

correlation coefficient，SCC）、MIC 作为相关性分析方法以及不使用相关性分析的个性化联邦进行对比分析。评估结果如表 3 所示。

表 3　不同相关性分析方法的评估结果

Table 3　Evaluation results of different correlation analysis methods

相关性分析方法	准确率	精确率	召回率	F1 分数
MIC	0.897 1	0.915 3	0.857 8	0.885 6
PCC	0.859 2	0.859 0	0.833 6	0.846 1
SCC	0.861 9	0.871 3	0.824 3	0.847 2
不使用相关性分析	0.842 8	0.867 5	0.780 7	0.821 8

从表中可以看出，在个性化联邦中加入相关性方法可以提高对 FDIA 的检测效果。同时，MIC 方法的准确率、精确率、召回率、F1 分数均优于 PCC 和 SCC。PCC 对非线性关系分析较差，SCC 更适合单调的非线性关系，MIC 更适合分布式新能源场景下带有周期性规律的数据特征提取。

3.5.2　数据规律特征对比

MIC 特征提取方法在面对周期性规律较强的数据时可以提高模型检测效果，而在处理周期性较弱的数据时不具有优势。为验证所提方法在处理规律较强数据时的优越性，将训练集中用电量数据的时间顺序打乱，构造在不同时间尺度下均不包含周期性规律的训练集，应用 MIC、PCC、SCC 和不使用相关性分析方法的检测模型进行实验，评估结果如表 4 所示。

表 4　无规律数据的评估结果

Table 4　Evaluation results for irregular data

相关性分析方法	准确率	精确率	召回率	F1 分数
MIC	0.818 9	0.854 2	0.798 6	0.825 4
PCC	0.812 1	0.925 4	0.706 5	0.801 3
SCC	0.800 8	0.832 4	0.787 0	0.809 0
不使用相关性分析	0.817 6	0.836 3	0.820 4	0.828 3

从表 3、4 中可以看出，在无规律的数据集中，MIC 未能体现出较好的性能，相比于不使用相关性分析方法的个性化联邦在性能上没有明显提升。因此，本文所提的检测方法更适合处理具有周期性规律的数据。

4　结　论

本文提出了基于个性化联邦和相关性分析的分布式虚假数据注入攻击检测方法。该方法利用分层联邦提取数据共性和个性特征，在边缘节点构建个性化 FDIA 检测模型以增强边缘节点的安全防护能力，同时引入 MIC 作为对数据中周期性规律的挖掘和提取，加强个性特征的提取效果。以含分布式新能源节点的园区数据为例验证所提方法的可行性。通过仿真分析得到以下结论：

1）本文提出的 co-PFL 检测方法相比于广泛使用的检测框架和检测模型，增加了对节点数据共性和个性特征的分离和提取，准确率相比 LL、CL、FL、SVM、GCN 分别提升了 4.37%、3.48%、4.50%、2.01%、1.81%，检测性能有所提升。

2）所提方法在训练和检测阶段收敛速率优于其他模型，在客户端数量较多时具有较快的收敛速率，更适合于分布式新能源场景下的 FDIA 检测。

3）在多层神经网络模型中的个性特征层加入 MIC，挖掘节点数据本身的周期性规律，提高了模型检测性能。但在不含周期性的数据集中没有表现出优势。

本文所提方法未考虑符合节点数据规律性特征的时间尺度自适应选择方法，如何针对不同的场景和业务特征选择合适的数据分析时间尺度是值得进一步研究的问题。

利益冲突声明（Conflict of Interests）：

所有作者声明不存在利益冲突。

作者贡献声明（Authors' Contributions）：

龚钢军提出论文研究方向，张晓炜设计研究方

案，王路遥进行对比实验分析，李璐含参与文献调研与整理，王浩淼、扬爽、黄雨菲参与论文写作和修订。所有作者均阅读并同意了论文终稿内容。

5 参考文献

[1] 席磊，王艺晓，熊雅慧，等. 基于改进深度极限学习机的电网虚假数据注入攻击定位检测[J]. 发电技术，2025，46(3)：521-531.
XI Lei，WANG Yixiao，XIONG Yahui，et al. Location detection of false data injection attacks in power grid based on improved deep extreme learning machine[J]. Power Generation Technology，2025，46(3)：521-531.

[2] 张玮，文国璐，罗仁军，等. 多源数据与配电网安全运行场景关联分析方法[J]. 电测与仪表，2025，62(10)：22-30.
ZHANG Wei，WEN Guolu，LUO Renjun，et al. Multi-source data correlation analysis method for secure operation scenarios of power distribution network[J]. Electrical Measurement & Instrumentation，2025，62(10)：22-30.

[3] 林裕新，陈楠，蔡建逸. 基于多源信息融合的配电网调度数据安全管控技术[J]. 电测与仪表，2024，61(6)：118-125，132.
LIN Yuxin，CHEN Nan，CAI Jianyi. Data security control technology for distribution network scheduling based on multi-source information fusion[J]. Electrical Measurement & Instrumentation，2024，61(6)：118-125，132.

[4] 席磊，熊雅慧，彭典名，等. 基于主成分分析-径向基神经网络算法的电网虚假数据注入攻击定位检测[J/OL]. 南方电网技术，2025：1-13.（2025-05-14）[2025-10-10]. https://link.cnki.net/urlid/44.1643.tk.20250513.1051.002.
XI Lei，XIONG Yahui，PENG Dianming，et al. Localization detection of false data injection attack on power grid based on principal component analysis-radial basis neural network algorithm [J/OL]. Southern Power System Technology，2025：1-13.（2025-05-14）[2025-10-10]. https://link.cnki.net/urlid/44.1643.tk.20250513.1051.002.

[5] 吴丽珍，张永朋，魏建平，等. 抵抗虚假数据注入攻击的综合能源系统弹性提升策略[J/OL]. 发电技术，2025：1-14.（2025-01-08）[2025-10-09]. https://link.cnki.net/urlid/33.1405.tk.20250108.0952.002.
WU Lizhen，ZHANG Yongpeng，WEI Jianping，et al. A comprehensive energy system resilience enhancement strategy to resist false dataInjection attacks [J/OL]. Power Generation Technology，2025：1-14.（2025-01-08）[2025-10-09]. https://link.cnki.net/urlid/33.1405.tk.20250108.0952.002.

[6] 席磊，曹利锋，宋浩杰，等. 基于残差生成对抗网络的电网虚假数据注入攻击防御方法[J]. 电网技术，2025，49(9)：3927-3936.
XI Lei，CAO Lifeng，SONG Haojie，et al. Defense method against false data injection attacks on power grids based on residual generative adversarial networks [J]. Power System Technology，2025，49(9)：3927-3936.

[7] 梁志宏，严彬元，洪超，等. 基于状态空间分解的电力系统虚假数据注入攻击检测与防御方法[J]. 南方电网技术，2025，19(6)：39-50.
LIANG Zhihong，YAN Binyuan，HONG Chao，et al. Detection and defense methods for false data injection attack in power systems based on state-space decomposition [J]. Southern Power System Technology，2025，19(6)：39-50.

[8] 席磊，田习龙，余涛，等. 基于相关特征-多标签级联提升森林的电网虚假数据注入攻击定位检测[J]. 南方电网技术，2024，18(5)：39-50，61.
XI Lei，TIAN Xilong，YU Tao，et al. Locational detection of false data injection attack in power grid based on relevant features multi-label cascade boosting forest [J]. Southern Power System Technology，2024，18(5)：39-50，61.

[9] 杨玉泽，刘文霞，李承泽，等. 面向电力SCADA系统的FDIA检测方法综述[J]. 中国电机工程学报，2023，43(22)：8602-8621.
YANG Yuze，LIU Wenxia，LI Chengze，et al. Review of FDIA detection methods for electric power SCADA system [J]. Proceedings of the CSEE，2023，43(22)：8602-8621.

[10] 常梦言，刘永慧. 虚假数据注入攻击下基于容积卡尔曼滤波的电力系统状态估计[J]. 电力科学与技术学报，2024，39(3)：10-18.
CHANG Mengyan，LIU Yonghui. State estimation of power system based on cubature Kalman filter under false data injection attacks [J]. Journal of Electric Power Science and Technology，2024，39(3)：10-18.

[11] PAL S，SIKDAR B，CHOW J H. Classification and detection of PMU data manipulation attacks using transmission line parameters [J]. IEEE Transactions on Smart Grid，2018，9(5)：5057-5066.

[12] JORJANI M，SEIFI H，VARJANI A Y. A graph theory-based approach to detect false data injection attacks in power system AC state estimation[J]. IEEE Transactions on Industrial Informatics，2021，17(4)：2465-2475.

[13] HUANG K K，XIANG Z L，DENG W F，et al. False data injection attacks detection in smart grid：a structural sparse matrix separation method [J]. IEEE Transactions on Network Science and Engineering，2021，8(3)：2545-2558.

[14] 席磊，和昀，李子豪，等. 基于Focal LossIM-Transformer的电网虚假数据注入攻击检测[J]. 南方电网技术，2025，19(6)：26-38.
XI Lei，HE Yun，LI Zihao，et al. False data injection attack detection based on focal LossIM-transformer[J]. Southern Power System Technology，2025，19(6)：26-38.

[15] YE D，ZHANG T Y. Summation detector for false data-injection attack in cyber-physical systems [J]. IEEE Transactions on Cybernetics，2020，50(6)：2338-2345.

[16] 夏云舒，王勇，周林，等. 基于改进生成对抗网络的虚假数据注入攻击检测方法[J]. 电力建设，2022，43(3)：58-65.
XIA Yunshu，WANG Yong，ZHOU Lin，et al. False data injection attack detection method based on improved generative adversarial network[J]. Electric Power Construction，2022，43(3)：58-65.

[17] 席磊，程琛，田习龙. 基于改进卷积神经网络的电网虚假数据注入攻击定位方法[J]. 南方电网技术，2025，19(1)：74-84.
XI Lei，CHENG Chen，TIAN Xilong. Improved convolutional neural network-based localization method for false data injection attacks on power grids [J]. Southern Power System Technology，

2025，19(1)：74-84.

[18] YIN X F，ZHU Y M，HU J K. A subgrid-oriented privacy-preserving microservice framework based on deep neural network for false data injection attack detection in smart grids[J]. IEEE Transactions on Industrial Informatics，2022，18(3)：1957-1967.

[19] LI Y，WEI X H，LI Y Z，et al. Detection of false data injection attacks in smart grid：a secure federated deep learning approach[J]. IEEE Transactions on Smart Grid，2022，13(6)：4862-4872.

[20] LI H J，DOU C X，YUE D，et al. End-edge-cloud collaboration-based false data injection attack detection in distribution networks[J]. IEEE Transactions on Industrial Informatics，2024，20(2)：1786-1797.

[21] KARIM M H，RANGANATHAN P. Edge-enabled AI for anomaly detection in distributed energy networks：a federated learning approach[C]//2024 56th North American Power Symposium (NAPS). IEEE，2024：1-7.

[22] ZHAO L，LI J M，LI Q，et al. A federated learning framework for detecting false data injection attacks in solar farms[J]. IEEE Transactions on Power Electronics，2022，37(3)：2496-2501.

[23] 孙艳华，王子航，刘畅，等. 个性化联邦学习的相关方法与展望[J]. 计算机工程与应用，2024，60(20)：68-83.
SUN Yanhua，WANG Zihang，LIU Chang，et al. Methods and prospects of personalized federated learning[J]. Computer Engineering and Applications，2024，60(20)：68-83.

[24] 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，I0005.
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，I0005.

[25] 高漪，周瑜，张安龙，等. 整县光伏下基于个性化联邦学习的光伏出力及负荷功率预测[J]. 电网技术，2023，47(11)：4629-4637.
GAO Yi，ZHOU Yu，ZHANG Anlong，et al. Personalized federated learning framework for countywide PV generation and load forecasting[J]. Power System Technology，2023，47(11)：4629-4637.

[26] RESHEF D N，RESHEF Y A，FINUCANE H K，et al. Detecting novel associations in large data sets[J]. Science，2011，334(6062)：1518-1524.

[27] 陶磊，罗萍萍，林济铿. 基于深度学习的直流微电网虚假数据注入攻击二阶段检测方法[J]. 中国电力，2024，57(9)：11-19.
TAO Lei，LUO Pingping，LIN Jikeng. Two-stage detection method for DC microgrid false data injection attack based on deep learning[J]. Electric Power，2024，57(9)：11-19.

[28] 李欣，易柳含，刘晨凯，等. 基于数据驱动的电力系统虚假数据注入攻击检测[J]. 智慧电力，2023，51(2)：30-37.
LI Xin，YI Liuhan，LIU Chenkai，et al. False data injection attacks detection in power system based on data-driven algorithm[J]. Smart Power，2023，51(2)：30-37.

[29] ZHENG Z B，YANG Y T，NIU X D，et al. Wide and deep convolutional neural networks for electricity-theft detection to secure smart grids[J]. IEEE Transactions on Industrial Informatics，2018，14(4)：1606-1615.

[30] 许越，李强，崔晖. 基于MIC-EEMD-改进Informer的含高比例清洁能源与储能的电力市场短期电价多步预测[J]. 电网技术，2024，48(3)：949-957.
XU Yue，LI Qiang，CUI Hui. Short-term multi-step price prediction for the electricity market with a high proportion of clean energy and energy storage based on MIC-EEMD-improved informer[J]. Power System Technology，2024，48(3)：949-957.

[31] YU J J Q，HOU Y H，LI V O K. Online false data injection attack detection with wavelet transform and deep neural networks[J]. IEEE Transactions on Industrial Informatics，2018，14(7)：3271-3280.

收稿日期：2025-05-23　**修回日期**：2025-10-11


龚钢军

作者简介：

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

张晓炜(2001)，男，硕士研究生，通信作者，主要研究方向为数据安全，E-mail：120232201278@ncepu.edu.cn；

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；

李璐含(2002)，女，硕士研究生，主要研究方向为数据安全；

黄雨菲(2004)，女，本科生，主要研究方向为电子信息；

王浩淼(1972)，男，本科，高级工程师，主要从事电力营销信息化工作；

扬爽(1981)，男，本科，高级工程师，主要从事电力营销信息化工作。

（编辑　曾文静）