DOI: 10.19783/j.cnki.pspc.250872

基于深度时空特征学习的直流微电网虚假数据注入检测方法

王 义[1,2]，罗胜耀[1,2]，唐 靓[3]，李忠文[1]，张世达[1,2]

(1. 郑州大学电气与信息工程学院，河南 郑州 450001；2. 河南省电力电子与电能系统工程技术研究中心，河南 郑州 450001；3. 国网镇江供电分公司，江苏 镇江 212000)

摘要：针对直流微电网中虚假数据注入攻击(false data injection attack, FDIA)隐蔽性强、难以精准检测的问题，提出一种基于深度时空特征学习的 FDIA 检测方法。首先，构建并行双分支检测模型。一支引入 Transformer 模块，利用自注意力机制提取全局信息与跨节点特征；另一支引入门控循环单元(gated recurrent unit, GRU)，捕捉量测数据中的时间依赖性与动态演化模式。其次，通过特征尺度对齐与自适应加权实现空间与时间表征的特征级融合，并配合归一化与残差抑制冗余与噪声。然后，将融合后的特征输入神经网络分类器，实现对多类型攻击的一体化检测。最后，在典型直流微电网场景下构建多类型攻击数据集并开展对比实验。结果表明，该方法各项指标整体优于对比模型，且表现出较强的鲁棒性与泛化能力。

关键词：直流微电网；虚假数据注入攻击；攻击检测；深度学习；Transformer-GRU

A false data injection detection method for DC microgrids based on deep spatiotemporal feature learning

WANG Yi[1,2], LUO Shengyao[1,2], TANG Liang[3], LI Zhongwen[1], ZHANG Shida[1,2]

(1. School of Electrical and Information Engineering, Zhengzhou University, Zhengzhou 450001, China; 2. Henan Provincial Engineering Technology Research Center of Power Electronics and Energy Systems, Zhengzhou 450001, China; 3. State Grid Zhenjiang Power Supply Company, Zhenjiang 212000, China)

Abstract: To address the strong stealthiness and low detectability of false data injection attacks (FDIAs) in DC microgrids, this paper proposes a FDIA detection method based on deep spatiotemporal feature learning. First, a parallel dual-branch detection model is constructed. One branch incorporates a Transformer module to extract global information and cross-node features through a self-attention mechanism, while the other branch adopts a gated recurrent unit (GRU) to capture temporal dependencies and dynamic evolution patterns in measurement data. Second, feature-scale alignment and adaptive weighting are employed to achieve feature-level fusion of spatial and temporal representations, supplemented by normalization and residual mechanisms to suppress redundancy and noise. Then, the fused features are fed into a neural network classifier to enable unified detection of multiple types of FDIA. Finally, a multi-type attack dataset is constructed under typical DC microgrid scenarios, and comparative experiments are conducted. The results demonstrate that the proposed method outperforms baseline models across overall evaluation metrics and exhibits strong robustness and generalization capability.

This work is supported by the Natural Science Foundation of Henan Province (No. 242300421167).

Key words: DC microgrid; false data injection attack; attack detection; deep learning; Transformer-GRU

0 引言

随着全球能源结构的转型与电力需求的持续增长，智能电网在现代电力系统中得到了日益广泛的应用。通过融合先进的通信技术、控制算法与分布式能源资源，智能电网正引导传统电网朝着更智能、可持续、更高效的方向发展[1]。在此背景下，作为智能电网的重要组成部分，微电网凭借其灵活的运行方式与分布式架构，在能源管理、可再生能源接入以及供电可靠性等方面展现出显著优势，因此在当代电力系统中扮演着日益关键的角色[2-3]。然而，

基金项目：河南省自然科学基金项目资助(242300421167)；国家自然科学基金项目资助(62203395)；中国博士后科学基金特别资助(2023TQ0306)；河南省青年人才托举工程项目资助(2025HYTP028)；中原科技创新青年拔尖人才项目资助

微电网的开放性以及其与网络–物理基础设施的深度融合，使其易受高级网络安全威胁的影响，尤其是虚假数据注入攻击(false data injection attack, FDIA)[4-5]。此类攻击通过篡改关键数据，可能导致状态估计失真，进而干扰能量调度与控制机制，严重威胁电网的稳定性与安全性[6-8]。因此，针对微电网设计鲁棒的 FDIA 检测与缓解策略，对于保障其安全稳定运行具有重要意义。

FDIA 常以隐蔽方式破坏系统运行，往往难以被及时发现。随着分布式能源资源的广泛部署，这一威胁愈加严峻，其根本原因在于微电网中数据采集与控制节点数量的急剧增加，显著增加了攻击面广度和检测任务的复杂性[9-10]。现有的 FDIA 检测方法主要可分为两大类：模型驱动方法与数据驱动方法[11-12]。模型驱动方法依赖于物理系统建模与状态估计，通过分析系统动态与状态方程识别异常[13]。例如，文献[14]提出了一种结合卡尔曼滤波与循环神经网络的 FDIA 检测方法，通过分离线性与非线性特征，并引入动态阈值以实现攻击识别。文献[15]将进化博弈理论框架与卡尔曼滤波相结合，利用支持向量机与 K 最近邻分类器检测不同类型的 FDIA，并通过纳什均衡分析制定最优防御策略。文献[16]引入基于集成经验模态分解的方法，利用从本征模态函数中提取的能量型指标区分不同攻击场景。文献[17]则提出了一种结合动态状态估计与未知输入观测器的 FDIA 检测与隔离策略，通过分析残差信号定位并隔离恶意行为。

尽管模型驱动方法在理论上能够实现较高的检测精度，但其在实际应用中常受到物理建模复杂性与测量不确定性等因素的限制。相比之下，数据驱动方法依托机器学习与深度学习技术，能够通过学习大量历史数据中的特征模式进行异常识别，因而受到越来越多关注[18-19]。例如，文献[20]提出了一种无监督的 FDIA 检测方法，将双图卷积自编码器与生成对抗网络相结合，提升了数据表示能力，并通过自适应阈值机制显著增强了检测性能。文献[21]针对孤岛运行的直流微电网，构建了一个数据驱动的网络攻击检测框架，通过强化学习模拟攻击者行为，并基于生成数据训练神经网络检测器。为应对面向分布式状态估计的新型攻击形式，文献[22]引入了一种能够捕捉系统测量时间相关性的深度学习模型，有效提升了对复杂攻击模式的识别能力。此外，文献[23]提出了一种基于预测区间的异常检测方案，通过优化生成的上下界实现快速识别系统异常行为，从而增强微电网的安全性。

综上所述，现有研究在 FDIA 检测方面已取得一定成效，有助于提升电网的网络安全性与系统稳定性。然而，当前方法在适用范围及对复杂攻击场景的适应能力等方面仍存在局限。为应对上述挑战，本文提出了一种针对直流微电网的 FDIA 检测策略。该方法基于微电网历史运行数据，采用并行双分支 Transformer-GRU 模型进行离线训练，从而实现系统资源的高效利用。训练完成后，该模型可实现对 FDIA 攻击的高精度、高效率识别，显著提升微电网的稳定性与安全性。在包含多个恒功率负载的直流微电网仿真系统中开展的仿真实验结果表明，所提方法能够有效识别各类攻击，提升系统的整体可靠性与安全水平。

1　系统建模与问题描述

1.1　直流微电网模型

考虑一个典型架构的直流微电网系统(direct current microgrid, DC MG)，其主要由滤波器、电力电子变换器、发电机、储能装置以及负载等关键部件构成，如图 1 所示。该直流微电网的电路拓扑结构如图 2 所示。根据电路拓扑图，整个直流微电网系统可被解耦为若干子系统，主要包括直流电源系统、恒功率负载(constant power load, CPL)系统以及储能系统(energy storage system, ESS)[24]。CPL 的状态方程可表示为

$$\dot{\boldsymbol{x}}_j = \boldsymbol{A}_j \boldsymbol{x}_j + \boldsymbol{d}_j h_j + \boldsymbol{A}_j^{\mathrm{s}} \boldsymbol{x}_{\mathrm{s}} \tag{1}$$

其中，$\boldsymbol{A}_j = \begin{bmatrix} -\dfrac{r_j}{L_j} & -\dfrac{1}{L_j} \\ \dfrac{1}{C_j} & 0 \end{bmatrix}$，$\boldsymbol{x}_j = [i_j \ v_j]$，$\boldsymbol{d}_j = \begin{bmatrix} 0 \\ -\dfrac{1}{C_j} \end{bmatrix}$，

$h_j = \dfrac{P_j}{v_j}$，$\boldsymbol{A}_j^{\mathrm{s}} = \begin{bmatrix} 0 & \dfrac{1}{L_j} \\ 0 & 0 \end{bmatrix}$，$\boldsymbol{x}_{\mathrm{s}} = [i_{\mathrm{s}} \ v_{\mathrm{s}}]$。

式中：r_j 和 L_j 分别表示从电源变换器到第 j 个 CPL 的线路电阻和滤波电感；C_j 表示第 j 个 CPL 的输入电容；i_j 和 v_j 分别表示第 j 个 CPL 中的电感电流和电

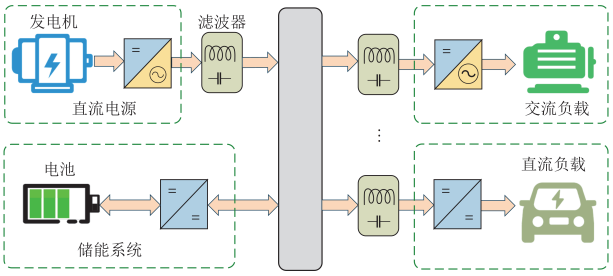


图 1　直流微电网系统

Fig. 1 DC microgrid system

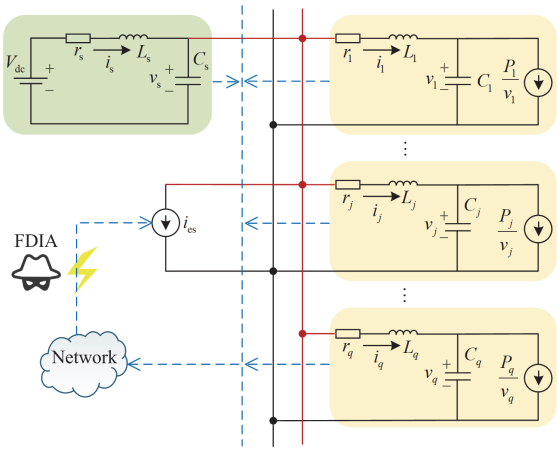


图 2 直流微电网简化系统结构图

Fig. 2 Simplified structural diagram of DC microgrid system

容电压；P_j 表示第 j 个 CPL 的负载功率；$j=1,2,\cdots,q$；i_s 和 v_s 分别表示 ESS 中的电感电流和电容电压。

此外，ESS 的状态方程可描述为

$$\dot{\boldsymbol{x}}_s=\boldsymbol{A}_s\boldsymbol{x}_s+\boldsymbol{b}_sV_{dc}+\boldsymbol{b}_{es}i_{es}+\sum_{j=1}^{q}\boldsymbol{A}_{cn}\boldsymbol{x}_j \tag{2}$$

其中，$\boldsymbol{A}_s=\begin{bmatrix}-\dfrac{r_s}{L_s} & -\dfrac{1}{L_s}\\ \dfrac{1}{C_s} & 0\end{bmatrix}$，$\boldsymbol{b}_s=\begin{bmatrix}\dfrac{1}{L_s}\\ 0\end{bmatrix}$，$\boldsymbol{b}_{es}=\begin{bmatrix}0\\ -\dfrac{1}{C_s}\end{bmatrix}$，$\boldsymbol{A}_{cn}=\begin{bmatrix}0 & 0\\ \dfrac{1}{C_s} & 0\end{bmatrix}$。

式中：r_s 和 L_s 分别表示储能系统中的线路电阻和滤波电感；C_s 表示电源变换器的输出电容；V_{dc} 表示直流电源电压；i_{es} 表示注入电流。

通过对 q 个 CPL 子系统与 1 个 ESS 子系统进行综合建模，整个 DC MG 系统的非线性动态方程可表示为

$$\dot{\boldsymbol{X}}=\boldsymbol{A}\boldsymbol{X}+\boldsymbol{D}\boldsymbol{H}+\boldsymbol{B}_{es}i_{es}+\boldsymbol{B}_sV_{dc} \tag{3}$$

式中：$\boldsymbol{X}=[x_1\ x_2\ x_3\cdots x_q\ x_s]$；$\boldsymbol{H}=[h_1\ h_2\ \cdots\ h_q]^{\mathrm{T}}$；

$$\boldsymbol{A}=\begin{bmatrix}\boldsymbol{A}_1 & 0 & \cdots & 0 & \boldsymbol{A}_1^s\\ 0 & \boldsymbol{A}_2 & \cdots & 0 & \boldsymbol{A}_2^s\\ \vdots & \vdots & & \vdots & \vdots\\ 0 & 0 & \cdots & \boldsymbol{A}_q & \boldsymbol{A}_q^s\\ \boldsymbol{A}_{cn} & \boldsymbol{A}_{cn} & \cdots & \boldsymbol{A}_{cn} & \boldsymbol{A}_s\end{bmatrix};\quad \boldsymbol{B}_{es}=\begin{bmatrix}0\\ \vdots\\ 0\\ \boldsymbol{b}_{es}\end{bmatrix};\quad \boldsymbol{D}=\begin{bmatrix}\boldsymbol{d}_1 & 0 & \cdots & 0 & 0\\ 0 & 0 & \cdots & 0 & 0\\ \vdots & \vdots & & \vdots & \vdots\\ 0 & 0 & \cdots & 0 & \boldsymbol{d}_q\\ 0 & 0 & \cdots & 0 & 0\end{bmatrix};\quad \boldsymbol{B}_s=\begin{bmatrix}0\\ \vdots\\ 0\\ \boldsymbol{b}_s\end{bmatrix}。$$

因此，DC MG 系统的状态空间方程可表示为

$$\begin{cases}\boldsymbol{x}(t+1)=f(\boldsymbol{x}(t),\boldsymbol{u}(t))+\boldsymbol{w}(t)\\ \boldsymbol{z}(t)=h(\boldsymbol{x}(t))+\boldsymbol{v}(t)\end{cases} \tag{4}$$

式中：$f(\cdot)$ 表示系统的状态转移函数；$h(\cdot)$ 表示量测函数；$\boldsymbol{x}(t)$ 表示系统的状态向量；$\boldsymbol{u}(t)$ 表示控制量；$\boldsymbol{w}(t)$ 和 $\boldsymbol{v}(t)$ 分别表示过程噪声和量测噪声。

1.2 FDIA 模型

FDIA 是一种常见的针对电力系统监控和控制的攻击方式，其基本原理是通过向系统中注入伪造的传感器数据，误导状态估计过程，进而破坏系统的正常运行[25]。在直流微电网系统中，虚假数据注入攻击通常通过篡改电流、电压等量测数据来实施。最大标准残差检验是坏数据检测的常用方法，用 $\boldsymbol{A}$ 表示攻击者在量测量中注入的 FDIA 向量，$\boldsymbol{\theta}$ 表示由 FDIA 引起的状态变量误差，则攻击后的残差 r_a 可以表示为

$$\begin{aligned}r_a&=\|\boldsymbol{z}_a-\boldsymbol{H}\boldsymbol{x}_a\|=\|(\boldsymbol{z}+\boldsymbol{A})-\boldsymbol{H}(\boldsymbol{x}+\boldsymbol{\theta})\|=\\ &\quad\|\boldsymbol{z}-\boldsymbol{H}\boldsymbol{x}+\boldsymbol{A}-\boldsymbol{H}\boldsymbol{\theta}\|\end{aligned} \tag{5}$$

式中：$\boldsymbol{z}_a$ 表示受攻击后的量测向量；$\boldsymbol{H}$ 表示量测矩阵；$\boldsymbol{x}_a$ 表示受攻击后的状态向量；$\boldsymbol{z}$ 表示原始量测向量；$\boldsymbol{x}$ 表示原始状态向量。

当 $\boldsymbol{A}=\boldsymbol{H}\boldsymbol{\theta}$ 时，则式(6)成立。

$$r_a=\|\boldsymbol{z}_a-\boldsymbol{H}\boldsymbol{x}_a\|=\|\boldsymbol{z}-\boldsymbol{H}\boldsymbol{x}\|<\tau \tag{6}$$

式中：τ 表示检测阈值。

由此可见，当攻击向量满足特定条件时，FDIA 能够避开检测机制，将虚假数据注入到系统中，从而误导状态估计和控制决策，造成系统运行的不稳定或安全隐患。

本文提出的 FDIA 包括 3 种类型，且均满足上述条件，接下来将对这 3 种攻击方式进行详细讨论与描述。

脉冲攻击：攻击者在一段时间内以脉冲的形式注入虚假数据 Δf_{a1}，可以表示为

$$f_a(t)=\begin{cases}\Delta f_{a1} & t\in[t_{ia},t_{fa}]\\ 0 & \text{其他}\end{cases} \tag{7}$$

式中：$f_a(t)$ 为攻击；t_{ia} 为攻击的初始时间；t_{fa} 为攻击的结束时间。

步进攻击：攻击者从特定时间开始，不断向系统注入虚假数据 Δf_{a2}，可以表示为

$$f_a(t)=\begin{cases}0 & t<t_{ia}\\ \Delta f_{a2} & t>t_{fa}\end{cases} \tag{8}$$

随机攻击：在随机时间，攻击者注入一个虚假数据 Δf_{a3}，可以表示为

$$f_{\mathrm{a}}(t)=\Delta f_{\mathrm{a3}} \tag{9}$$

2　基于 Transformer-GRU 的 FDIA 检测

2.1　Transformer-GRU 模型

为有效检测复杂多变的网络攻击行为，本文提出了一种名为 Transformer-GRU 的并行双分支深度时空特征学习模型，其整体架构如图 3 所示。该模型将 Transformer 与 GRU 模块并行集成，Transformer 模块用于从输入序列中提取空间特征，能够同时捕捉短期与长期依赖关系；而 GRU 模块则凭借其出色的短期记忆能力，在建模不规则攻击模式方面表现优越。

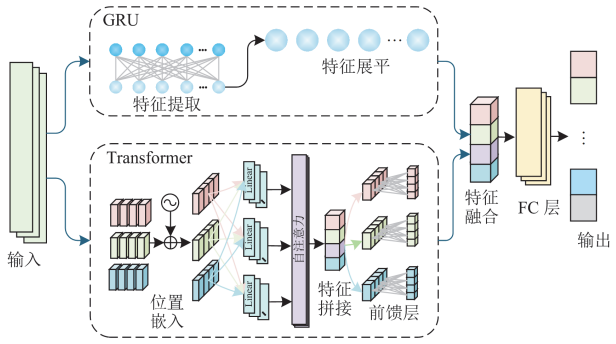


图 3　Transformer-GRU 模型结构图

Fig. 3 Architecture of the Transformer-GRU model

两分支在输出端先经线性层映射到相同维度并按时间步对齐，随后沿通道维进行拼接，经由带非线性激活的前馈网络完成加权融合；前馈层隐式学习门控，抑制冗余、突出判别性特征，并结合轻量残差与归一化稳定训练。融合后的联合表示进入分类头产生最终判别结果。基于归纳偏置互补与可优化性提升：Transformer 负责非局部依赖与跨节点交互的全局建模，GRU 提供局部平滑与时序记忆；双分支并行抽取特征，经前馈映射后融合输出，从而抑制冗余信息并凸显判别性特征。相较串行堆叠，并行后融合可减轻单一路径的信息衰减与偏置放大，更契合同时存在长程依赖与短期突发的攻击特征。通过融合两者的互补优势，所提出的模型在识别多样化且高度复杂的攻击行为方面表现出更强的能力，从而显著提升系统的鲁棒性与运行稳定性。

2.2　Transformer 模型

Transformer 是一种基于自注意力机制的神经网络结构，不依赖于循环神经网络(recurrent neural network, RNN)，能够高效捕捉全局依赖关系，并支持输入的并行处理，从而显著提升训练速度[26]。如图 4 所示，Transformer 的结构包括编码器、解码器及其连接层。

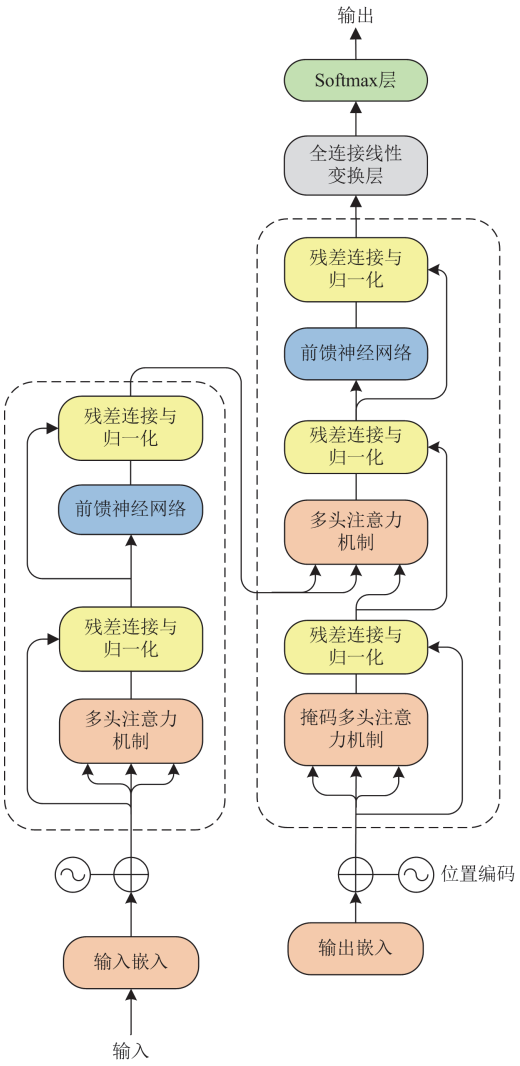


图 4　Transformer 结构

Fig. 4 Structure of the Transformer

自注意力机制是 Transformer 模型的核心，能够使模型在处理序列时建立输入各元素之间的相互关系。该机制通过将查询向量(query)映射到键–值对(key-value pairs)来实现，其计算公式为

$$\mathrm{Attention}(\boldsymbol{Q},\boldsymbol{K},\boldsymbol{V})=\mathrm{softmax}\left(\frac{\boldsymbol{Q}\boldsymbol{K}^{\mathrm{T}}}{\sqrt{d_{\mathrm{k}}}}\right)\boldsymbol{V} \tag{10}$$

式中：$\boldsymbol{Q}$、$\boldsymbol{K}$ 和 $\boldsymbol{V}$ 分别表示查询、键和值；d_{k} 为键的维度。softmax 函数确保权重归一化。在计算中，key-value 对应源语句，query 则为目标语句。

多头注意机制将自我注意分为几个“头”，能够同时关注输入序列的不同部分，从而获得不同的表示。每个注意力头通过学习不同的权重矩阵独立计算注意力，然后将这些结果连接起来并通过线性变换得到最终的输出。计算公式为

$$M(\boldsymbol{Q},\boldsymbol{K},\boldsymbol{V})=\mathrm{C}(H_{\mathrm{head}_1},H_{\mathrm{head}_2},\cdots,H_{\mathrm{head}_h})\boldsymbol{W}^{\mathrm{o}} \tag{11}$$

$$H_{\mathrm{head}_i}=A(\boldsymbol{Q}\boldsymbol{W}_i^{\mathrm{q}},\boldsymbol{K}\boldsymbol{W}_i^{\mathrm{k}},\boldsymbol{V}\boldsymbol{W}_i^{\mathrm{v}}) \tag{12}$$

式中：$\boldsymbol{W}^{\mathrm{o}}$、$\boldsymbol{W}_i^{\mathrm{q}}$、$\boldsymbol{W}_i^{\mathrm{k}}$、$\boldsymbol{W}_i^{\mathrm{v}}$为参数矩阵；C(·)为特征拼接算子；$A(\cdot)$为注意力函数；$H_{\mathrm{head}_i}$为每个注意力头的输出。

在攻击检测任务中，Transformer 架构凭借其强大的自注意力机制，能够有效捕捉恶意行为在长序列中的空间相关性，从而提升对复杂与潜伏性攻击的检测精度。

2.3 GRU 模型

门控循环单元是一种循环神经网络的变体，通过引入门控机制，有效缓解了梯度消失与爆炸问题。其结构主要包括两个核心门控：更新门与重置门，用于控制信息的流动并决定每个时刻隐藏状态的更新方式。

更新门：更新门控制前一时刻的隐藏状态应保留多少信息，并与当前输入结合生成新的状态。它有助于保留关键的历史攻击特征。

$$z_t=\sigma(\boldsymbol{W}_z\cdot[h_{t-1},x_t]) \tag{13}$$

式中：z_t为更新门的输出；$\boldsymbol{W}_z$为更新门的权重矩阵；h_{t-1}为上一时刻的隐藏状态；x_t为当前输入；$\sigma(\cdot)$为 sigmoid 激活函数。

重置门：重置门控制当前输入与过去隐藏状态的结合程度，用于决定在计算当前候选状态时应遗忘多少历史信息。它有助于 GRU 灵活应对突变或异常的攻击行为。

$$r_t=\sigma(\boldsymbol{W}_{\mathrm{r}}\cdot[h_{t-1},x_t]) \tag{14}$$

式中：r_t为重置门的输出；$\boldsymbol{W}_{\mathrm{r}}$为重置门的权重矩阵。

网络攻击通常具有明显的时间特性，如短时间内的突变或持续的异常模式。GRU 具备较强的短期记忆能力，能够有效跟踪这类动态变化，在应对不规则或突发性攻击时表现出良好的适应性与鲁棒性。图 5 给出了所提虚假数据注入攻击检测方法的整体流程框架。

3　仿真分析

3.1 实验设置

为确保仿真实验的完整性与有效性，本文选用一个典型的直流微电网系统作为测试模型。该系统由 3 个恒功率负载和 1 个电源组成，具有代表性与通用性，可有效模拟实际直流微电网的运行特性与行为。为保证实验的严谨性与可重复性，系统的具体参数如表 1 所示。

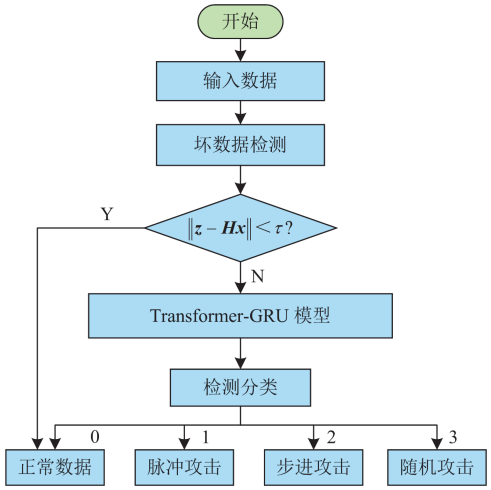


图 5 攻击检测流程图

Fig. 5 Attack detection flowchart

表 1 系统参数

Table 1 Parameters of the test system

区域	电阻/Ω	电感/mH	电容/μF	功率/W	电压/V
电源	1	17	550	—	200
CPL1	1.1	39.5	500	300	—
CPL2	1.1	39.5	500	300	—
CPL3	1.1	39.5	500	300	—

为构建本文所使用的数据集，基于第 1 节中给出的系统模型，搭建了直流微电网仿真模型。在此基础上，针对关键量测通道实施 3 类虚假数据注入：以各 CPL 支路的电感电流和电容电压以及储能支路电流等通道为对象，设计并施加了多种虚假数据注入攻击场景，包括脉冲攻击、步进攻击与随机攻击，3 种攻击细节如下。

脉冲攻击：在 $t=4\sim6$ s 对目标量测叠加方波脉冲，幅值约为 0.6 p.u.。

步进攻击：自 $t=4$ s 起施加固定偏置，幅值约为 0.2 p.u.，并持续至仿真结束。

随机攻击：全程叠加均值约为 0.10 p.u.的随机扰动，波动范围控制在±0.01 p.u.之内。

在正常运行与攻击条件下采集电压、电流等关键数据，从而形成 1 个覆盖全面的数据集。该直流微电网数据集包含：5200 条正常样本、4750 条脉冲攻击样本、4980 条步进攻击样本以及 5100 条随机攻击样本。数据集按照 70%用于训练、30%用于验证的比例进行划分，并在训练集与验证集中以相同比例随机分配攻击样本与正常样本，以保证模拟过程的公平性与结果的可靠性。

Transformer-GRU 并行集成模型利用直流微电网系统的检测数据进行训练，其架构设计包括两部

分：Transformer 和 GRU。Transformer 部分由 6 层堆叠而成，每层包含 512 个隐藏单元，并使用 8 个注意力头，通过多头自注意力机制和前馈神经网络捕捉输入序列的全局依赖关系。同时，GRU 部分由 2 层堆叠而成，每层包含 256 个隐藏单元，用于提取输入数据中的时序特征。这两个部分在训练过程中并行处理输入数据，其输出通过全连接层融合，生成最终的预测结果。在训练配置上，模型的批次大小为 128，训练过程设置为 250 个 Epoch，每个 Epoch 包含 1400 次迭代，总训练次数为 350 000 次。为加速模型收敛并提高性能，采用学习率衰减策略：初始学习率为 0.005，在前 150 个 Epoch 保持不变，随后每隔 50 个 Epoch 按衰减因子 0.1 更新学习率。通过这种策略有助于模型更快收敛，并表现出良好的泛化能力。

模型性能通过以下指标进行评估：准确率、精确率、召回率、F1 分数、混淆矩阵以及 ROC 曲线。准确率反映整体分类正确程度，精确率衡量被判为攻击的样本中实际为攻击的比例，召回率表示实际攻击中被成功识别的比例，F1 分数则在精确率与召回率之间进行平衡。混淆矩阵用于直观展示预测标签与真实标签之间的对应关系，揭示分类误差与偏差。ROC 曲线描绘了真阳性率与假阳性率之间的权衡，其下的面积(area under the curve, AUC)则反映模型整体的检测能力。

3.2 单一攻击场景

为全面评估所提方法的有效性，本研究首先在单一类型的网络攻击场景下进行初步分析，为后续复杂攻击条件下的性能评估奠定基础。具体而言，本文分别对 3 类攻击进行独立测试，以验证所提方法的检测能力，并与多种检测方法进行对比分析。相应的检测结果见图 6—图 8。

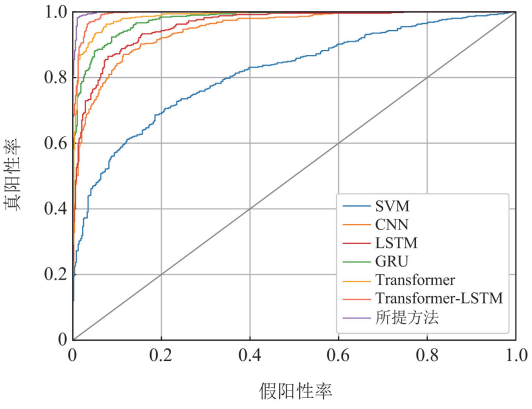


图 6 脉冲攻击下 ROC 曲线对比图

Fig. 6 Comparison of ROC curves under pulse attack

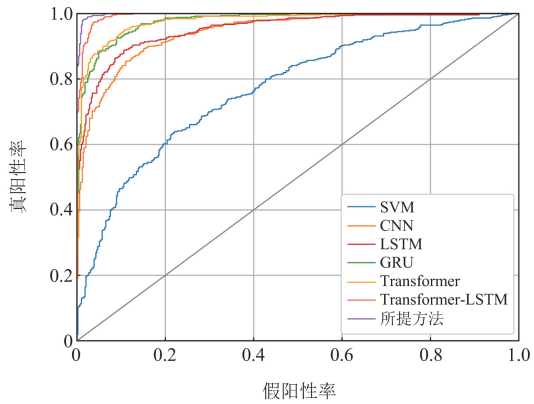


图 7 步进攻击下 ROC 曲线对比图

Fig. 7 Comparison of ROC curves under step attack

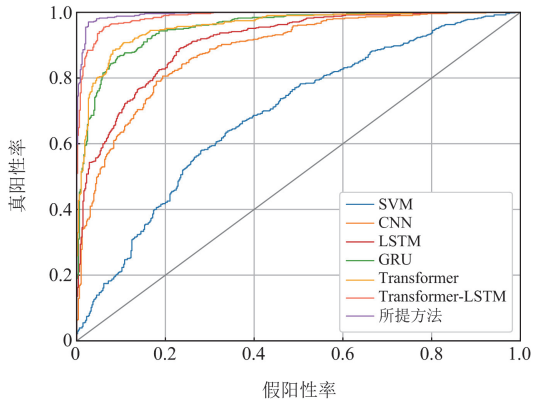


图 8 随机攻击下 ROC 曲线对比图

Fig. 8 Comparison of ROC curves under random attack

由图 6—图 8 可知，所提方法在 3 种单一攻击场景中均表现出优越的检测性能。相比其他方法，本文模型的 ROC 曲线在各场景下均更接近左上角，表明其具有更高的真阳性率和更低的假阳性率，从而展现出在面对脉冲、步进与随机攻击时的强判别能力。

表 2 通过 4 个评价指标准确率、精确率、召回率与 F1 分数对检测性能进行定量比较。在所有攻击类型下，所提方法在各项指标上均达到最高水平，显著优于对比模型。例如，在脉冲攻击条件下，所提方法的检测准确率达到 93.79%，F1 分数为 93.90%，体现了其出色的检测精度与强鲁棒性。

上述结果充分验证了所提检测策略在应对直流微电网各类虚假数据注入攻击时的有效性、可靠性及鲁棒性。

3.3 多重攻击场景

在验证所提模型在单一攻击场景下的检测性能后，进一步将分析扩展至 3 类攻击同时发生的多重攻击情形。该综合评估旨在验证所提检测方法在应

对复杂攻击模式下的有效性。下文将给出相应的仿真结果与性能指标，以进一步佐证所提方法的可行性。

表 2 FDIA 检测性能指标对比表

Table 2 Comparison of FDIA detection preformance indicator

	模型	准确率	精确率	召回率	F1 值
脉冲攻击	SVM	0.8076	0.6527	0.7501	0.7007
	CNN	0.7905	0.7985	0.7779	0.7890
	LSTM	0.8331	0.8109	0.8129	0.8146
	GRU	0.8464	0.8972	0.8470	0.8819
	Transformer	0.8725	0.9123	0.8692	0.8934
	Transformer-LSTM	0.9012	0.9301	0.8956	0.9157
	所提方法	0.9379	0.9484	0.9184	0.9390
步进攻击	SVM	0.7910	0.6413	0.7308	0.6778
	CNN	0.7833	0.7821	0.7668	0.7689
	LSTM	0.8146	0.7978	0.8021	0.8069
	GRU	0.8214	0.8806	0.8399	0.8692
	Transformer	0.8581	0.8944	0.8647	0.8801
	Transformer-LSTM	0.8863	0.9112	0.8835	0.9032
	所提方法	0.9298	0.9254	0.9007	0.9229
随机攻击	SVM	0.7646	0.6134	0.7175	0.6613
	CNN	0.7698	0.7745	0.7511	0.7571
	LSTM	0.8105	0.7823	0.7759	0.7976
	GRU	0.8111	0.8822	0.8254	0.8426
	Transformer	0.8492	0.8931	0.8490	0.8655
	Transformer-LSTM	0.8773	0.9098	0.8654	0.8850
	所提方法	0.9047	0.9216	0.8807	0.9036

图 9 展示了在多类型攻击同时发生的场景下，各种检测模型的 ROC 曲线。可以明显看出，所提模型的 AUC 值显著高于其他方法。同时，该模型在较宽范围的假阳性率条件下始终保持较高的真阳性率，充分体现出其在应对复杂、重叠攻击情形下的鲁棒性与可靠性。

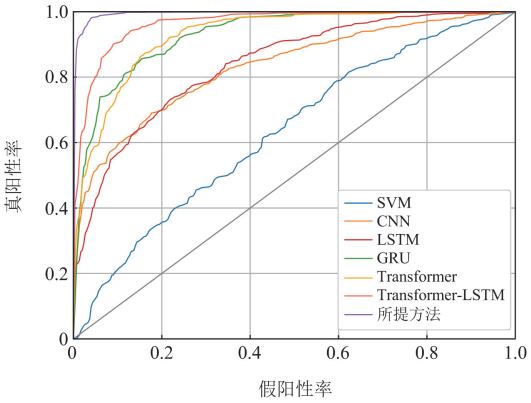


图 9 各类型攻击下 ROC 曲线对比图

Fig. 9 Comparison of ROC curves under multi-attacks

图 10 展示了在多重攻击场景下，4 种检测模型的混淆矩阵结果。可以观察到，所提方法在所有类别上均表现出更优的分类性能。对于 Class0(正常数据)、Class1(脉冲攻击)、Class2(步进攻击)以及 Class3(随机攻击)，所提模型的真正例数量明显高于其他模型，表明其具备更高的检测准确率和更低的误判率。相比之下，LSTM 与 CNN 在不同攻击类别之间存在更明显的混淆现象，GRU 和 Transformer 表现相当，Transforme-LSTM 虽表现相对较好，但在整体性能上仍不及所提模型。这些结果进一步验证了所提方法在复杂环境下区分多种攻击类型的优越性与可靠性。

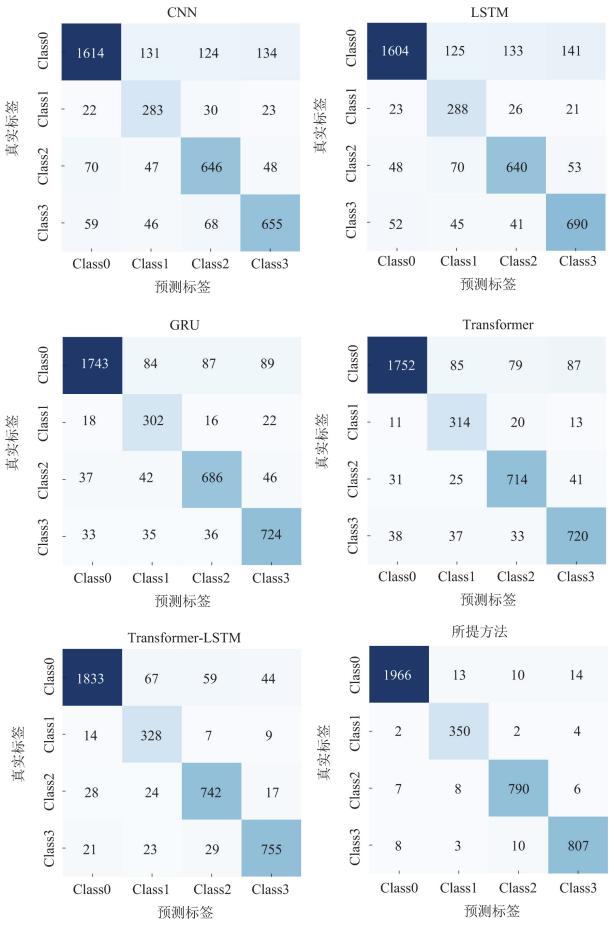


图 10 混淆矩阵对比图

Fig. 10 Comparison of confusion matrix

表 3 进一步列出了各检测模型在多重攻击下 4 项常用指标的性能评估结果。可以看到所提方法在各项指标上均表现最优，展现出较高的检测准确率，并在假阳性率与假阳性率之间实现了良好的平衡。这些结果验证了其在复杂多攻击场景中的鲁棒性与泛化能力。

由此可见，在多重攻击场景下，所提方法在检测性能方面优于对比模型，展现出极高的检测有效性。这进一步证明了所提方法在应对复杂攻击环境中的有效性与可靠性。

表 3 各模型性能评估结果

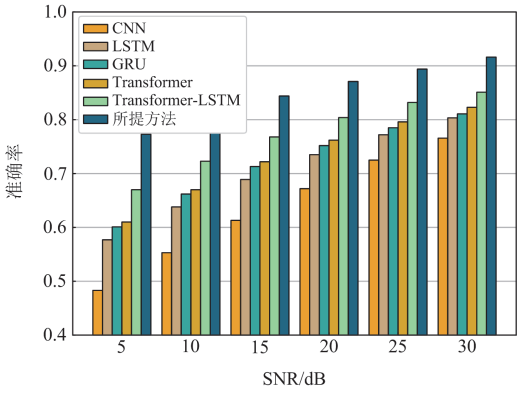
Table 3 Performance evaluation results of different models

模型	准确率	精确率	召回率	F1 值
SVM	0.7116	0.6228	0.7195	0.6661
CNN	0.7658	0.7690	0.7506	0.7559
LSTM	0.8034	0.7711	0.7830	0.7905
GRU	0.8508	0.8699	0.8211	0.8474
Transformer	0.8835	0.8912	0.8536	0.8719
Transformer-LSTM	0.9107	0.9038	0.8694	0.8863
所提方法	0.9362	0.9146	0.8846	0.9030

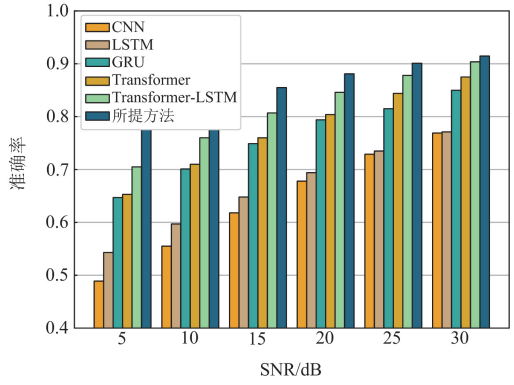
3.4 噪声影响分析

在实际的直流微电网运行中，电压与电流信号常受到测量噪声与外部干扰的影响，导致数据质量下降，从而影响基于深度学习的检测模型的性能。为评估所提模型在此类非理想条件下的鲁棒性，本文在前述仿真的基础上，引入不同强度的高斯白噪声，对原始干净数据集进行扰动扩展。以信噪比(signal-to-noise ratio, SNR)作为噪声强度的量化指标，选取 30 dB、25 dB、20 dB、15 dB、10 dB 和 5 dB 六个代表性信噪比水平，分别构建包含正常运行、脉冲攻击、步进攻击与随机攻击等场景的噪声测试集。所有模型均在无噪声数据上完成训练，仅在上述噪声测试集上进行性能评估。通过分析模型在不同噪声强度下的检测指标变化，揭示其性能退化趋势与抗噪能力。

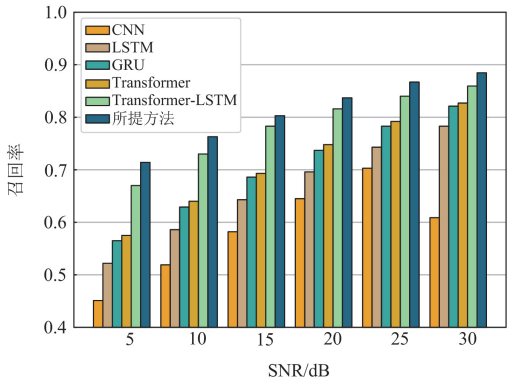
图 11 展示了各模型在不同信噪比条件下的检测性能，涵盖准确率、精确率、召回率与 F1 分数 4 项关键指标。随着 SNR 的降低，所有模型的检测性能均出现不同程度的下降。CNN 模型受噪声影响最为显著，在 5 dB 时各项指标大幅下滑，表明其抗噪能力较差。GRU 和 Transformer 表现相当，Transformer-LSTM 则表现出一定的鲁棒性，在中等强度噪声下仍能保持稳定的性能。相比之下，所提模型在所有 SNR 水平下均优于其他方法，得益于 Transformer 对全局上下文的建模能力与 GRU 对短期变化的敏感响应，其并行融合结构有效提升了模型在复杂攻击场景下的抗噪性与泛化能力。



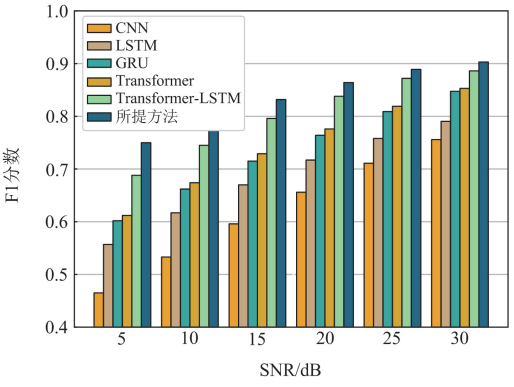
(a) 准确率



(b) 精确率



(c) 召回率



(d) F1分数

图 11 不同 SNR 条件下各模型的检测性能对比

Fig. 11 Comparison of detection performance of different models under different SNRs

图 12 与图 13 进一步给出了在两种代表性 SNR 条件下，各模型的 ROC 曲线与 AUC 值。在低噪声条件下，各类模型整体表现良好，均展现出一定的特征学习与分类能力。其中 CNN、LSTM、GRU、Transformer 和 Transformer-LSTM 的 AUC 分别为 0.819、0.863、0.910、0.891 和 0.957，而所提模型以 0.972 的 AUC 值取得最佳性能，显著优于上述对比模型，展现出更优的检测精度与泛化能力。在高

噪声环境下，各类模型的性能均出现不同程度的下降，其中 CNN 的性能下降最为显著(AUC 值为0.568)，表明其对噪声较为敏感。相比之下，GRU 和 Transformer 模型在噪声干扰下仍展现出一定的鲁棒性，而 Transformer-LSTM 的性能表现相对稳定。值得强调的是，所提方法在强噪声干扰下仍能保持最高的 AUC 值，且模型性能始终稳定优越，这进一步验证了其在强噪声环境下的可靠性。

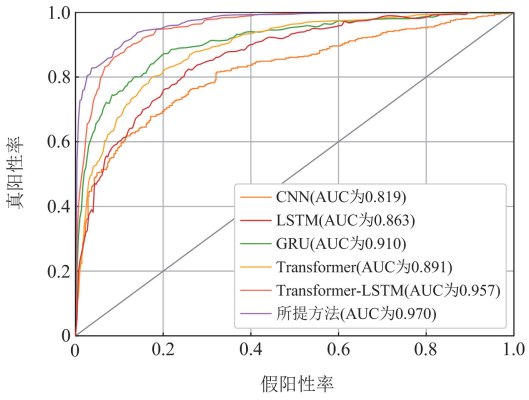


图 12 低噪声条件下各模型的 ROC 曲线

Fig. 12 ROC curves of different models under low noise conditions

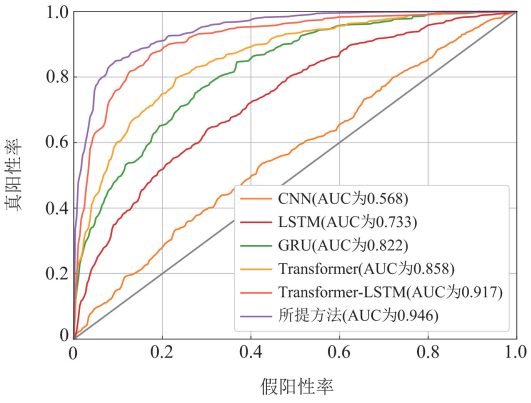


图 13 高噪声条件下各模型的 ROC 曲线图

Fig. 13 ROC curves of different models under high noise conditions

综上所述，所提模型在多种噪声条件下均展现出优越的检测性能与较强的鲁棒性。与其他基准模型相比，该模型在高噪声场景下性能退化最小，在低噪声环境中则保持较高的检测准确率。上述结果表明，所提方法具有良好的抗干扰能力与广泛的适应性，适用于复杂实际环境中的攻击检测任务。

4 结论

为应对微电网日益严峻的网络安全威胁，本文提出了一种基于深度时空特征学习的直流微电网虚假数据注入攻击检测策略。该方法基于深度学习技术，构建了一种并行双分支检测模型，将善于捕捉全局依赖关系的 Transformer 与在时序建模中高效稳健的 GRU 有机结合，从而实现对复杂攻击模式的精准识别。仿真结果表明，所提方法在多种攻击场景下均展现出较强的攻击识别能力和较低的误报率。此外，在不同信噪比条件下，该模型依然保持稳定的检测性能，尤其在高噪声环境中，模型仍能有效识别攻击模式，反映出其良好的鲁棒性与抗噪能力。

参考文献

[1] 杨杰, 郭逸豪, 郭创新, 等. 考虑模型与数据双重驱动的电力信息物理系统动态安全防护研究综述[J]. 电力系统保护与控制, 2022, 50(7): 176-187.
YANG Jie, GUO Yihao, GUO Chuangxin, et al. A review of dynamic security protection on a cyber physical power system considering model and data driving[J]. Power System Protection and Control, 2022, 50(7): 176-187.

[2] 曾君, 谭豪杰, 刘俊峰, 等. 基于状态势博弈的微电网能量管理优化算法研究[J]. 电力系统保护与控制, 2025, 53(5): 24-34.
ZENG Jun, TAN Haojie, LIU Junfeng, et al. Research on optimization algorithm of microgrid energy management based on a state potential game[J]. Power System Protection and Control, 2025, 53(5): 24-34.

[3] 刘浩, 王丹, 刘佳委, 等. 计及分布式水风光发电时空相关性的多微网协同优化策略[J]. 电力系统保护与控制, 2025, 53(13): 23-35.
LIU Hao, WANG Dan, LIU Jiawei, et al. Multi-microgrid collaborative optimization strategy considering spatiotemporal correlation of distributed hydro-wind-solar generation[J]. Power System Protection and Control, 2025, 53(13): 23-35.

[4] KODURU S S, MACHINA V S, MADICHETTY S, et al. Standalone deployment of two-fold deep neural network in distributed DC microgrid FDIA detection and mitigation scheme[J]. IEEE Journal of Emerging and Selected Topics in Industrial Electronics, 2024, 6(1): 201-214.

[5] 陈柏任, 夏候凯顺, 李梦诗. 基于数据驱动的电力系统虚假数据注入攻击防御框架的研究[J]. 电测与仪表, 2024, 61(12): 10-16.
CHEN Bairen, XIAHOU Kaishun, LI Mengshi. Research on defense framework for false data injection attacks in power system based on data-driven algorithm[J]. Electrical Measurement & Instrumentation, 2024, 61(12): 10-16.

[6] SAHOO S, YANG Yongheng, FREDE B. Resilient synchronization strategy for AC microgrids under cyber attacks[J]. IEEE Transactions on Power Electronics, 2020, 36(1): 73-77.

[7] MOHAMED A S, ARANI M F M, JAHROMI A A, et al. False data injection attacks against synchronization systems in microgrids[J]. IEEE Transactions on Smart Grid, 2021, 12(5): 4471-4483.

[8] ANNAVARAM D, MISHRA S, PULLAGURAM D. Resilient event-driven distributed control for DC microgrids against false data injection attacks[J]. IEEE Transactions on Smart Grid, 2024, 15(6): 5358-5372.

[9] 康文洋, 汤鹏志, 左黎明, 等. 基于 NB-IOT 的孤岛式微电网密钥协商协议研究[J]. 电力系统保护与控制, 2020, 48(5): 119-126.
KANG Wenyang, TANG Pengzhi, ZUO Liming, et al. Research on key agreement protocol for isolated microgrids based on NB-IOT[J]. Power System Protection and Control, 2020, 48(5): 119-126.

[10] DAI Jiahong, YANG Jiawei, WANG Yu, et al. Blockchain-enabled cyber-resilience enhancement framework of microgrid distributed secondary control against false data injection attacks[J]. IEEE Transactions on Smart Grid, 2023, 15(2): 2226-2236.

[11] 黄冬梅, 杨旭, 胡安铎, 等. 基于 CNN-BiGRU-XGBoost 的新型电力系统虚假数据注入攻击检测[J]. 电网技术, 2025, 49(5): 2119-2127.
HUANG Dongmei, YANG Xu, HU Anduo, et al. Detection of false data injection attack in new power systems based on CNN-BiGRU-XGBoost[J]. Power System Technology, 2025, 49(5): 2119-2127.

[12] LI Xueping, JIAO Wanzhou, HAN Qi, et al. Detection of FDIA in power grid based on hypergraph and attention mechanism[J]. IEEE Transactions on Smart Grid, 2025, 16(2), 1862-1871.

[13] LUO Xiaoyuan, LI Yating, WANG Xinyu, et al. Interval observer-based detection and localization against false data injection attack in smart grids[J]. IEEE Internet of Things Journal, 2020, 8(2): 657-671.

[14] WANG Yufeng, ZHANG Zhihao, MA Jianhua, et al. KFRNN: an effective false data injection attack detection in smart grid based on Kalman filter and recurrent neural network[J]. IEEE Internet of Things Journal, 2021, 9(9): 6893-6904.

[15] ZHANG Zhixun, HU Jianqiang, LU Jianquan, et al. Preventing false data injection attacks in LFC system via the attack-detection evolutionary game model and KF algorithm[J]. IEEE Transactions on Network Science and Engineering, 2022, 9(6): 4349-4362.

[16] ZHANG Jingqiu, SAHOO S, PENG J C, et al. Mitigating concurrent false data injection attacks in cooperative dc microgrids[J]. IEEE Transactions on Power Electronics, 2021, 36(8): 9637-9647.

[17] ALUKO A O, CARPANEN R P, DORRELL D G, et al. Real-time cyber attack detection scheme for standalone microgrids[J]. IEEE Internet of Things Journal, 2022, 9(21): 21481-21492.

[18] ZHANG Guangdou, LI Jian, BAMISILE O, et al. Spatio-temporal correlation-based false data injection attack detection using deep convolutional neural network[J]. IEEE Transactions on Smart Grid, 2021, 13(1): 750-761.

[19] 席磊, 白芳岩, 王文卓, 等. 基于海马优化深层极限学习机的电力信息物理系统 FDIA 检测[J]. 电力系统保护与控制, 2025, 53(4): 14-26.
XI Lei, BAI Fangyan, WANG Wenzhuo, et al. Cyber-physical power system FDIA detection based on seahorse optimized deep extreme learning machine[J]. Power System Protection and Control, 2025, 53(4): 14-26.

[20] FENG Hantong, HAN Yinghua, SI Fangyuan, et al. Detection of false data injection attacks in cyber physical power systems: an adaptive adversarial dual autoencoder with graph representation learning approach[J]. IEEE Transactions on Instrumentation and Measurement, 2023, 73: 1-11.

[21] WAN Yihao, DRAGIČEVIĆ T. Data-driven cyber attack detection of intelligent attacks in islanded DC microgrids[J]. IEEE Transactions on Industrial Electronics, 2022, 70(4): 4293-4299.

[22] MSOTAFA M, WENG Yang, KHALILI A, et al. Cyber-physical attack conduction and detection in decentralized power systems[J]. IEEE Access, 2022, 10: 29277-29286.

[23] ABDOLLAH K, SU Wencong, JIN Tao. A machine learning-based cyber attack detection model for wireless sensor networks in microgrids[J]. IEEE Transactions on Industrial Informatics, 2020, 17(1): 650-658.

[24] VAFAMAND A, MOSHIRI B, VAFAMAND N. Fusing unscented Kalman filter to detect and isolate sensor faults in DC microgrids with CPLs[J]. IEEE Transactions on Instrumentation and Measurement, 2021, 71: 1-8.

[25] 李卓, 谢耀滨, 吴茜琼, 等. 基于深度学习的电力系统虚假数据注入攻击检测综述[J]. 电力系统保护与控制, 2024, 52(19): 175-187.
LI Zhuo, XIE Yaobin, WU Xianqiong, et al. Review of deep learning-based false data injection attack detection in power systems[J]. Power System Protection and Control, 2024, 52(19): 175-187.

[26] 李云松, 张智晟. 考虑综合需求响应的 Transformer-图神经网络综合能源系统多元负荷短期预测[J]. 电工技术学报, 2024, 39(19): 6119-6128.
LI Yunsong, ZHANG Zhisheng. Transformer based multi load short-term forecasting of integrated energy system considering integrated demand response[J]. Transactions of China Electrotechnical Society, 2024, 39(19): 6119-6128.

收稿日期：2025-08-11；　修回日期：2025-11-11

作者简介：

王　义(1992—)，男，博士，副教授，研究方向为电力系统状态估计、新能源发电与智能微电网；E-mail: wangyi1414599008@163.com

罗胜耀(1999—)，男，硕士研究生，研究方向为电力系统动态状态估计；E-mail: lewuwo6@163.com

张世达(1992—)，男，通信作者，博士，助理研究员，研究方向为综合能源系统和电力系统规划运行。E-mail: zhangshida@zzu.edu.cn

(编辑　许　威)