

电力时间同步系统防欺骗抗干扰 检测技术及方法

刘铁强^{1,2,3,4}, 支春阳³, 柳林涛^{1,2}, 郝立芳³, 郭磊³, 杨双³

(1. 中国科学院大学, 北京 100049;

2. 中国科学院精密测量科学与技术创新研究院, 武汉 430071;

3. 深圳市远东华强导航定位有限公司, 石家庄 050081;

4. 中国电子科技集团公司第五十四研究所, 石家庄 050081)

摘要:为解决电力时间同步系统面临的复杂动态干扰与隐蔽欺骗威胁, 弥补传统防欺骗抗干扰技术适配性不足、缺乏综合检测的短板, 对适用于电力场景的抗干扰与防欺骗检测技术进行了研究; 采用基于盲信号分离与时空特征聚合网络的抗干扰识别算法(BSS-TSFANet)与多特征融合CNN-LSTM欺骗检测算法; BSS-TSFANet通过时频域虚拟多通道扩展与改进FastICA实现复合干扰的盲分离, 再经轻量化抗噪型TSFANet提取时空特征, 实现高精度干扰识别; CNN-LSTM算法经STFT时频转换、PCA降维后, 通过轻量化CNN与LSTM联合提取特征实现高精度欺骗检测; 经试验测试, BSS-TSFANet在干噪比-20 dB环境下对单一干扰平均识别准确率达96.78%, 对典型电力复合干扰的成分识别召回率达93.78%; CNN-LSTM算法对转发式与生成式欺骗的检测准确率分别达98.75%和99.95%; 两类算法均满足电力终端轻量化、实时性要求, 为智能电网电力时间同步系统提供了一体化抗干扰与防欺骗检测方案。

关键词: BSS-TSFANet; CNN-LSTM; 抗干扰; 防欺骗; 时间同步系统

Anti-Spoofing and Anti-Interference Detection Technologies and Methods for Power Time Synchronization Systems

LIU Tieqiang^{1,2,3,4}, ZHI Chunyang³, LIU Lintao^{1,2}, HAO Lifang³, GUO Lei³, YANG Shuang³

(1. University of Chinese Academy of Sciences, Beijing 100049, China;

2. Innovation Academy for Precision Measurement Science and Technology, Chinese Academy of Sciences, Wuhan 430071, China;

3. Shenzhen Far-East Huaqiang Navigation and Position Co., Ltd., Shijiazhuang 050081, China;

4. The 54th Research Institute of CETC, Shijiazhuang 050081, China)

Abstract: To address the complex dynamic interference and covert spoofing threats faced by power time synchronization systems, and to make up for the shortcomings of traditional anti-spoofing and anti-interference technologies such as poor adaptability and the lack of comprehensive detection capabilities, research is conducted on anti-interference and anti-spoofing detection technologies suitable for power scenarios. This paper presents a blind signal separation and temporal-spatial feature aggregation network-based anti-interference recognition algorithm (BSS-TSFANet) and a multi-feature fusion CNN-LSTM spoofing detection algorithm. The BSS-TSFANet achieves blind separation of composite interference via time-frequency domain virtual multi-channel expansion and an improved FastICA algorithm, and then extracts temporal and spatial features through a lightweight anti-noise TSFANet to realize high-precision interference recognition. For the CNN-LSTM algorithm, after short-time Fourier transform (STFT) for time-frequency conversion and principal component analysis (PCA) for dimen-

收稿日期:2026-03-09; 修回日期:2026-03-27。

作者简介:刘铁强(1984-),男,硕士,高级工程师。

引用格式:刘铁强,支春阳,柳林涛,等. 电力时间同步系统防欺骗抗干扰检测技术及方法[J]. 计算机测量与控制, 2026, 34(7): 59-67.

sionalities reduction, the lightweight CNN and LSTM are combined to extract features for high-precision spoofing detection. Experimental tests show that the BSS-TSFANet achieves an average recognition accuracy of 96.78% for single interference and a component recognition recall of 93.78% for typical power composite interference with an interference-to-signal ratio of -20 dB. The CNN-LSTM algorithm reaches the detection accuracies by 98.75% and 99.95% for replay spoofing and generative spoofing, respectively. Both algorithms meet the lightweight and real-time requirements of power terminals, providing an integrated anti-interference and anti-spoofing detection solution for power time synchronization systems in smart grids.

Keywords: BSS-TSFANet; CNN-LSTM; anti-interference; anti-Spoofing; time synchronization systems

0 引言

电力系统作为国家能源安全的重要基础设施,在建设智能电网的过程中,继电保护、柔性直流输电、电力市场交易以及新能源并网等业务领域的时间同步精度要求从毫秒级逐步达到微秒级乃至纳秒级^[1-2]。全球导航卫星系统(GNSS, global navigation satellite system),如北斗卫星导航系统(BDS, beidou navigation satellite system)、全球定位系统(GPS, global positioning system),凭借其全球覆盖、全天候服务、高精度授时优势,目前已经成为电力时间同步系统的主要授时方案之一,并已广泛应用于变电站、换流站及调度中心等场景^[3-4]。

然而,GNSS授时信号天然存在功率低、易受干扰的缺陷,在电力场景中面临压制式干扰和欺骗式攻击的双重威胁。此类威胁已多次引发电力时间同步系统失步、继电保护误动等安全事件,给电网稳定运行带来严峻挑战。

针对上述威胁,国内外学者已在授时信号抗干扰与防欺骗领域开展系列研究。抗干扰方面,传统非智能技术主要基于信号域处理,包括直接序列扩频(DSSS, direct sequence spread spectrum)、跳频(FHSS, frequency-hopping spread spectrum)、时域交织纠错编码等频域/时域方法^[5-6],以及自适应调零天线、空时自适应处理(STAP, space-time adaptive processing)等空域技术^[5,7],但前者对宽带干扰抑制能力有限且跳频同步开销较大,后者在电力变电站多反射环境中鲁棒性较差且计算复杂度高。近年来,基于强化学习的智能抗干扰技术成为研究热点,如文献[5]提出基于DDQN的抗干扰智能决策模型,文献[8]提出自适应特征值检测算法,文献[9]将近端策略优化算法应用于跳频电台,文献[10]提出基于时空特征聚合网络的压制干扰识别算法,但现有研究在多干扰源并发、复杂电磁环境适应性及抗干扰手段决策等方面仍存在不足。防欺骗方面,传统方法包括载噪比异常检测、多源比对、钟差检验等^[11-13],但易受多径效应影响、长期精度下降或受伪距噪声与时钟模型精度制约;基于数据驱动的智能方法如改进RCNN算法^[14]、LSTM网络^[15]、融合极限学习机

模型^[16]等,在欺骗检测准确率上取得显著成效,但对弱欺骗信号的检测精度仍显不足,且部分方法依赖高分辨率数据,电力终端硬件难以支撑。

综上所述,当前电力时间同步系统的抗干扰与防欺骗能力存在显著短板:抗干扰方面,传统扩频、跳频技术对动态干扰响应滞后,在低干噪比环境下效能骤降^[7];防欺骗方面,电力场景多采用简单的载噪比阈值检测,对弱欺骗信号的检测盲区大,误检率高达15%以上^[17]。因此,研究适用于电力场景的高鲁棒性、高精度抗干扰与防欺骗检测技术,已成为保障智能电网安全运行的迫切需求。

1 电力系统授时抗干扰防欺骗技术研究

1.1 技术应用现状

电力系统对授时抗干扰防欺骗技术的应用研究聚焦于设备优化与场景适配:文献[2]开展防欺骗和抗干扰设备试验,验证了在电力时间同步系统免受卫星欺骗及干扰的可行性,但未涉及算法层面的优化;文献[17]设计基于GNSS的电力授时接收机抗干扰模块,通过空频自适应滤波抑制工业干扰,但其仅针对压制干扰类型,无法处理欺骗干扰,适应性有限;文献[18]提出基于定向天线的北斗干扰源定位方法,可实现变电站周边干扰源的精确定位,但定位延迟大,无法满足实时防护需求;文献[19]提出智能电网接收机自主抗欺骗检测方法,通过电力系统内部时钟偏差校验,提升欺骗检测鲁棒性,但依赖电网内部多节点数据交互,兼容性较差。

当前,在电力时间同步系统应用的抗干扰防欺骗检测技术手段面临3个主要挑战:1)抗干扰算法对电力场景特有的动态干扰适用性不足,例如变电站内设备杂散辐射、突发脉冲干扰^[18];2)欺骗检测技术对弱信号与缓变型欺骗的识别能力有限,同时其硬件实现复杂,成本较高^[20];3)缺乏能够协同处理干扰与欺骗的综合防护方案,导致系统难以应对混合威胁。

1.2 技术适配性分析

考虑电力时间同步系统的独特属性,要求抗干扰防欺骗检测技术要满足3项关键需求:1)实时性:为支撑继电保护、自动化控制等关键业务,系统时间同步偏

差应满足毫秒级以下精度要求；2) 鲁棒性：技术必须足够强健，能应对变电站内工业设备杂散辐射、多径效应等构成的复杂电磁环境，对动态干扰与微弱欺骗信号均保持高检测精度；3) 轻量化：考虑到电力终端多为嵌入式设备，其计算与存储资源紧张，相关技术的硬件实现必须足够精简。

针对当前电力时间同步系统中存在的技术适配性与方案局限性，分析总结出 3 个层面的缺陷如下。

抗干扰技术层面：现有方法在电力场景下技术适配困难。传统扩频与调频技术在应对动态干扰时存在响应迟滞问题；智能强化学习算法虽具备动态决策能力，但其计算复杂度高，难以在资源有限的电力终端中部署；而自适应特征值算法虽在干扰检测方面表现良好，但缺乏相应的抗干扰决策机制，需与其他技术配合使用。

欺骗检测技术层面，同样存在适配性不足的问题。传统基于载噪比或钟差检验的方法对弱欺骗信号的识别精度有限；基于 CNN 的检测算法依赖高质量数据与 GPU 算力，在多数电力嵌入式终端中难以满足其运行条件；LSTM 类算法对生成式欺骗等新型攻击手段鲁棒性较弱。

系统集成层面：目前尚缺乏能够统一应对干扰与欺骗威胁的一体化解决方案。现有技术多孤立设计，导致电力系统需分别部署多套设备，不仅抬高了建设与运维成本，也带来系统兼容性的挑战。

为系统性解决上述缺陷，本研究将提出两类先进算法，分别针对抗干扰与欺骗检测在电力场景中的适配性进行优化，并通过模拟场景试验验证其有效性与可行性。

2 先进干扰欺骗检测算法设计

2.1 基于 BSS-TSFANet 的抗干扰识别算法

基于时空特征聚合网络的 GNSS 压制干扰识别算法在电力场景下的适用性存在明显局限。针对电力系统授时接收机面临的多源复合干扰挑战，提出一种融合盲信号分离（BSS，blind signal separation）与时空特征聚合网络（TSFANet，temporal-spatial feature aggregation network）的智能干扰识别算法，简称 BSS-TSFANet。该算法的核心思想是先分离、后识别、再决策，通过物理层信号解析与数据驱动深度特征提取的协同作用，实现对单一干扰的高精度分类和对复合干扰的有效解构。

2.1.1 算法整体框架

基于 BSS-TSFANet 的抗干扰识别算法的整体流程如图 1 所示。算法的输入为授时接收机射频前端输出的数字中频信号 $r(n)$ ，经过预处理后，依次通过盲信号分离、TSFANet 识别，输出干扰类型识别结果，通过

抑制策略匹配，选取最优抑制算法抑制干扰信号，最终输出干净的导航信号。

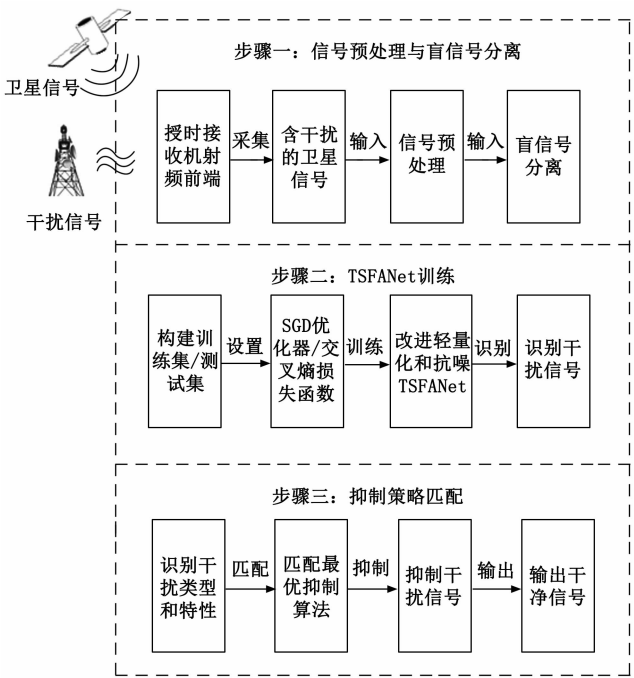


图 1 BSS-TSFANet 算法流程图

步骤一：信号预处理与盲信号分离

对接收信号 $r(n)$ 进行必要的预处理，然后送入盲信号分离模块。盲信号分离首先通过时频域虚拟多通道扩展将单通道观测信号转换为多通道虚拟观测矩阵，接着估计出源信号数目 N ，并分离出 N 个独立的信号分量 $\hat{s}_1(n), \hat{s}_2(n), \dots, \hat{s}_N(n)$ ，最后，根据功率阈值筛选出高功率的潜在干扰分量，滤除功率极低的噪声或微弱信号分量。

步骤二：TSFANet 训练

将每个分离出的分量 $\hat{s}_i(n)$ 计算 STFT 时频图像，划分出测试集和训练集，输入到改进的轻量化 TSFANet 中，输出每个分量的识别结果。并对所有分量的识别结果进行综合评估，判断干扰类型和功率。

步骤三：抑制策略匹配

根据识别出的干扰类型和特性，从预设的策略库中匹配最优的抑制算法，并触发执行，最后输出干净的导航信号。

2.1.2 盲信号分离（BSS）模块设计

实际授时接收机通常只输出单通道数字中频信号，而经典独立成分分析（ICA）要求观测信号数量不少于源信号数量。为解决单通道欠定盲分离问题，提出采用时频域虚拟多通道扩展方法，在时频域构造出多个虚拟观测信号，将单通道数据转化为多通道数据，从而满足 ICA 的可分离条件。

1) 时频域虚拟多通道构造:

对接收信号 $r(n)$ 进行短时傅里叶变换, 得到时频复矩阵 $\mathbf{R} \in \mathbb{C}^{T \times F}$, 其中 T 为时间帧数, F 为频率点数。通过引入时间延迟、频率平移等操作构造虚拟观测通道:

$$\begin{aligned} X_1(t, f) &= \mathbf{R}(t, f) \\ X_2(t, f) &= \mathbf{R}(t - \Delta t, f) \\ X_3(t, f) &= \mathbf{R}(t, f - \Delta f) \\ X_4(t, f) &= \mathbf{R}(t - \Delta t, f - \Delta f) \end{aligned} \quad (1)$$

其中: Δt 和 Δf 分别为时间延迟步长和频率平移步长。由此得到虚拟多通道观测张量 $X \in \mathbb{C}^{M \times T \times F}$, M 为虚拟通道数, 设置 $M=4$ 。将每个时频点 (t, f) 的 M 维向量视为一个观测样本, 构成数据集 $\{X_{tf} \in \mathbb{C}^M\}$ 。

2) 改进 FastICA 分离算法:

采用适用于复数域的 FastICA 算法对各时频点的观测向量进行分离。算法如下。

步骤一: 中心和白化

对观测数据 X 进行中心化和白化处理, 得到白化后的数据 $z = \mathbf{V}x$, 其中 $\mathbf{V}$ 为白化矩阵, 满足 $E\{zz^H\} = \mathbf{I}$ 。

步骤二: 独立性最大化迭代

使用负熵作为独立性度量 w , 通过固定点迭代求解分离向量目标函数为:

$$J(w) = [E\{G(|w^H z|^2)\} - E\{G(|v|^2)\}]^2 \quad (2)$$

其中: $G(u) = \log[\cosh(u)]$ 为非线性函数, v 为标准复高斯变量。采用牛顿迭代法更新 w :

$$w^+ = E\{zg(|w^H z|^2)\} - E\{g'(|w^H z|^2) | w^H z|^2\} w \quad (3)$$

其中: $g(u) = G'(u)$, $g'(u)$ 为其导数。迭代后需对 w^+ 进行正交化和单位化:

$$w = \frac{w^+}{\|w^+\|} \quad (4)$$

经过依次提取, 得到分离矩阵 $\mathbf{W}$, 计算出分离后的源信号估计 $y = \mathbf{W}^H z$ 。

步骤三: 时频域逆变换与信号重构

将分离出的各成分对应的时频矩阵 $\mathbf{Y}_k(t, f)$ 进行逆 STFT, 重构为时域信号分量 $\hat{s}_k(n)$ 。

步骤四: 干扰分量筛选

计算各分量的功率 $P_k = \frac{1}{N} \sum_n |\hat{s}_k(n)|^2$, 按降序排列。设置功率阈值, 将功率低于阈值的分量视为噪声、欺骗信号, 不予处理。保留高功率分量作为潜在干扰分量供 TSFANet 识别。

2.1.3 改进的 TSFANet 算法

改进的 TSFANet 结构保留了原 TSFANet 的双支路并行融合架构, 重点针对电力嵌入式终端的算力约

束, 开展了轻量化优化设计, 同时通过抗噪增强提升低干噪比环境下的识别鲁棒性。网络输入为干扰信号的时频图, 输出为干扰分类概率, 本次轻量化改进的核心轻量化设计与原始 TSFANet 的对比如下。

1) 空间特征聚合支路: 将原始残差块的标准卷积替换为深度可分离卷积, 参数量仅为标准卷积的 1/9 左右; 同时将 3 个卷积模块的输出通道数从原始的 32、64、128 缩减至 16、32、64, 在保留特征提取能力的同时大幅压缩参数规模。

2) 时间特征聚合支路: 将原始模型的双层 LSTM 结构替换为 BiGRU 结构, 隐藏层大小缩减至 128, 在保留双向时序依赖捕捉能力的前提下, 将时序模块参数量压缩至原始的 15% 以内。

3) 特征融合与分类模块: 简化全连接层设计, 剔除原始模型中维度为 512、256 的高维全连接层, 仅保留 2 层低维度全连接层完成分类, 进一步降低参数冗余。

4) 新增的双重抗噪注意力模块 (DANA, dual Anti-noise attention) 采用轻量化设计, 通道注意力 MLP 隐藏层维度仅为 8, 单模块参数量控制在 0.8 M 以内, 未给网络带来显著的参数与计算量增量。

(1) 空间特征聚合支路

空间特征聚合支路采用多层全局空间卷积模块 (GSCM) 堆叠而成, 每个 GSCM 由一个改进的残差卷积块和一个全局空间注意力 (GSA) 模块级联构成。

改进残差卷积块: 将原始残差块卷积连接替换为联合池化连接, 并在通道维度上将输入与输出堆叠, 实现特征图尺寸调整和通道扩展, 同时避免参数冗余和信息丢失。卷积层全部采用深度可分离卷积, 大幅降低计算量。深度可分离卷积将标准卷积分解为深度卷积和逐点卷积, 参数量约为标准卷积的 $\frac{1}{K^2}$, K 为卷积核大小。

全局空间注意力模块: 采用与原始 TSFANet 相同的 GSA 设计, 通过横向和纵向两个空间维度的全局平均池化和全局最大池化提取全局空间特征, 再经卷积融合生成与输入同形的权重矩阵, 实现对输入特征图的空间一通道联合加权。

(2) 时间特征聚合支路

时间特征聚合支路将时频图视为频率维度为特征、时间维度为序列的序列数据。采用双向门控循环单元提取时间特征, 以同时捕获前后向的时间依赖关系。设置隐藏层大小为 128, 层数为 1, 输出序列的最后一个时间步的隐藏层状态作为时间特征向量。

(3) 双重抗噪注意力模块

为提升模型在低干噪比环境下的鲁棒性, 在特征融

合前引入 DANA。DANA 模块由通道注意力子模块和空间注意力子模块串联组成, 具体如下。

通道注意力: 通过全局平均池化和全局最大池化分别聚合特征图的空间信息, 经共享的多层感知机生成通道权重, 与原始特征图相乘, 突出对分类贡献大的特征通道。

空间注意力: 沿通道轴进行平均池化和最大池化, 将结果拼接后通过卷积层生成空间权重图, 与特征图相乘, 突出信号区域、抑制噪声区域。

DANA 模块能有效增强模型对噪声干扰的抑制能力, 提升特征的可分性。

(4) 干扰信号分类

将空间支路输出的空间特征图经全局平均池化得到的空间特征向量 $f_s \in R^d$, 与时间支路输出的时间特征向量 $f_t \in R^d$ 拼接, 形成融合特征向量 $f = [f_s, f_t]$ 。随后通过两个全连接层得到最终分类概率 P 。

2.1.4 抑制策略匹配

对于第 i 个分离分量, 融合系数 λ 取 0.7, 融合后得到该分量的最终概率向量, 取最大值对应类别作为该分量的识别结果。

将识别为非欺骗类的信号分量及其估计频率, 供后续抑制算法使用。

通过识别出的干扰类型和参数, 自动加载对应的抑制算法并配置参数, 精准抑制干扰信号。干扰类型与抑制算法的策略库如表 1 所示。

表 1 干扰类型与抑制算法的策略库

序号	干扰类型	抑制算法
1	单音连续波干扰	自适应陷波滤波器
2	扫频干扰	时频域滤波
3	脉冲干扰	脉冲消隐
4	宽带噪声调频干扰	频域干扰抑制

2.2 基于多特征融合的 CNN-LSTM 欺骗检测算法

现有欺骗检测算法在电力系统的实际应用中面临两个主要瓶颈: 其一, 依赖单一类型的特征, 难以有效应对弱欺骗信号和生成式欺骗等复杂攻击模式; 其二, 高维特征对计算资源要求苛刻, 超出了当前电力终端嵌入式硬件的实时处理能力。

针对上述问题, 本文设计了一种融合多特征的 CNN-LSTM 欺骗检测算法。该算法首先利用短时傅里叶变换 (STFT) 结合主成分分析 (PCA) 对时频特征进行压缩降维, 再输入至 CNN 模块提取深层模式, 最后借助 LSTM 捕捉时序依赖关系。这一联合特征处理机制在提升检测精度的同时, 也增强了对电力终端硬件环境的适配性。

2.2.1 算法整体框架

CNN-LSTM 欺骗检测算法的整体框架如图 2 所示。

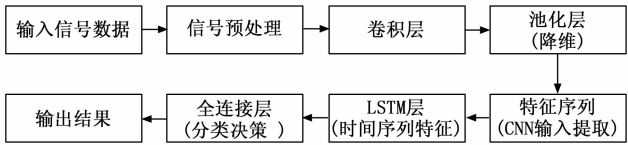


图 2 CNN-LSTM 欺骗检测算法整体框架

核心模块包括如下。

信号预处理模块: 采集 GNSS 信号的 I/Q 数据, 通过 STFT 转换为时频图, 结合 PCA 压缩特征维度。

CNN 特征提取模块: 利用轻量化 CNN 提取时频图的局部特征, 捕捉欺骗信号的时频异常。

LSTM 时序学习模块: 将 CNN 提取的特征序列输入 LSTM, 学习 GNSS 信号的长时序相关性, 识别欺骗导致的时序异常。

分类决策模块: 通过全连接层输出欺骗概率, 结合自适应门限判定是否存在欺骗。

2.2.2 信号预处理与特征压缩

2.2.2.1 时频图生成 (STFT)

GNSS 信号的 I/Q 数据为一维时序信号, 难以直接反映频率域的欺骗特征。采用短时傅里叶变换 (STFT) 将 I/Q 数据转换为时频图, 步骤如下。

分帧加窗: 将长度为 N 的 $\frac{I}{Q}$ 序列分为 K 帧, 帧长 $L=64$, 帧移 $S=32$, 采用汉宁窗抑制频谱泄漏, 窗函数为:

$$\omega(n) = 0.5 - 0.5\cos\left(\frac{2\pi n}{L-1}\right), n = 0, 1, \dots, L-1$$

(5)

傅里叶变换: 对每帧数据执行 FFT, 得到频率分辨率 $\nabla f = \frac{f_s}{L}$ ($f_s = 1$ MHz 为采样率), 频率范围为 $\left[0, \frac{f_s}{2}\right]$ 。

时频图构建: 将 K 帧的 FFT 结果按时间顺序排列, 构建维度为 $K \times \left(\frac{L}{2}\right)$ 的时频图, 其中 $K = \text{ceil}\left(\frac{(N-L)}{S}\right) + 1$, $\frac{L}{2}$ 为频率点数。

2.2.2.2 特征压缩 (PCA)

STFT 生成的时频图维度较高, 电力终端难以实时处理。采用主成分分析 (PCA) 压缩特征维度, 步骤为:

1) 数据标准化: 将时频图的每个频率点的幅值标准化至 $[0, 1]$, 公式为:

$$X_{\text{norm}}(k, f) = \frac{X(k, f) - X_{\min}(f)}{X_{\max}(f) - X_{\min}(f)} \quad (6)$$

2) 协方差矩阵计算: 计算 标准化后数据的协方差矩阵 $\Sigma = \frac{1}{K-1} X_{\text{norm}}^T X_{\text{norm}}$ 。

3) 主成分选择: 求解协方差矩阵的特征值与特征向量, 选择累计贡献率 $> 95\%$ 的前 M 个主成分, 将时频图维度从 $K \times \left(\frac{L}{2}\right)$ 压缩至 $K \times M$ ($M=8 \sim 16$)。

2.2.2.3 轻量化 CNN 特征提取模块

为适应电力终端的硬件资源约束, 设计轻量化 CNN 结构, 减少参数数量与计算复杂度, 轻量化设计策略包括: 采用小核卷积 (3×3), 减少参数数量; 减少卷积核数量 (16 个), 降低计算复杂度; 省略全连接层, 直接扁平化后输入 LSTM, 参数数量控制在 10^4 以内, 电力嵌入式终端可实时处理。

2.2.2.4 LSTM 时序学习模块

LSTM 模块负责学习 GNSS 信号的长时序相关性, 识别欺骗导致的时序异常, LSTM 层的核心门控机制包括如下。

遗忘门: 决定丢弃哪些细胞状态信息, 公式为:

$$f_t = \sigma(W_f \cdot [h_{t-1}, x_t] + b_f) \quad (7)$$

其中: W_f 为遗忘门权重, h_{t-1} 为上一时刻隐藏状态, x_t 为当前时刻输入, b_f 为遗忘门偏置, σ 为 sigmoid 函数。

输入门: 决定更新哪些细胞状态信息, 公式为:

$$i_t = \sigma(W_i \cdot [h_{t-1}, x_t] + b_i) \quad (8)$$

$$\bar{C}_t = \tanh(W_C \cdot [h_{t-1}, x_t] + b_C) \quad (9)$$

其中: i_t 为输入门激活值, $\bar{C}_t$ 为候选细胞状态。

细胞状态更新: 结合遗忘门与输入门, 更新细胞状态, 公式为:

$$C_t = f_t \odot C_{t-1} + i_t \odot \bar{C}_t \quad (10)$$

其中: $\odot$ 为元素积。

输出门: 决定输出哪些隐藏状态信息, 公式为:

$$O_t = \sigma(W_o \cdot [h_{t-1}, x_t] + b_o) \quad (11)$$

$$h_t = O_t \odot \tanh(C_t) \quad (12)$$

其中: h_t 为当前时刻隐藏状态, 作为 LSTM 层的输出。

2.2.2.5 自适应决策门限与损失函数

自适应决策门限: 传统固定门限对弱欺骗信号误检率高, 本文提出基于信号质量的自适应门限, 根据载噪比 C/N_0 动态调整门限 γ_{th} :

$$\gamma_{\text{th}} = 0.3 + 0.2 \cdot \exp\left(-\frac{C/N_0 - 25}{10}\right) \quad (13)$$

其中: $C/N_0 < 25$ dB Hz 时, $\gamma_{\text{th}} \approx 0.5$, 提高门限以减少误检; 25 dB Hz $\leq C/N_0 < 35$ dB Hz, γ_{th} 随 C/N_0

降低, 平衡误检与漏检; $C/N_0 \geq 35$ dB Hz, $\gamma_{\text{th}} \approx 0.3$, 降低门限以提高弱欺骗检测精度。

当算法输出的欺骗概率 $P_{\text{spoof}} > \gamma_{\text{th}}$ 时, 判定为存在欺骗; 反之则判定为无欺骗。

损失函数与优化器: 采用交叉熵损失函数 (BCE) 评估欺骗检测的分类误差, 公式为:

$$L = -\frac{1}{N} \sum_{i=1}^N [y_i \log(P_{\text{spoof},i}) + (1 - y_i) \log(1 - P_{\text{spoof},i})] \quad (14)$$

其中: y_i 为真实标签 (1=欺骗, 0=正常), $P_{\text{spoof},i}$ 为算法输出的欺骗概率, N 为样本数量。

优化器采用 Adam 优化器, 学习率 $lr=10^{-4}$, 权重衰减 $\text{weight_decay}=10^{-5}$, 避免过拟合。训练过程中采用早停策略 (Early Stopping), 当验证集损失连续 10 轮不下降时, 停止训练, 防止过拟合。

2.3 算法协同防护架构与工作机制

为实现干扰与欺骗复合威胁下的一体化防护, 解决两类算法独立运行时的协同适配问题, 提出“并行检测—分级响应—闭环验证”的双算法协同防护架构, 实现 BSS-TSFANet 抗干扰算法与 CNN-LSTM 欺骗检测算法的深度协同, 核心工作机制如下。

2.3.1 基础并行检测机制

正常工况下, 两类算法基于接收机输出的同一中频 I/Q 信号, 并行开展全时段实时检测, 无数据耦合导致的延迟累积:

1) BSS-TSFANet 算法持续对信号进行盲分离与干扰识别, 实时输出干扰类型、干噪比、干扰功率等状态参数, 同步完成干扰抑制策略的预匹配;

2) CNN-LSTM 欺骗检测算法同步对信号进行时频特征提取与欺骗概率计算, 基于自适应门限实时输出欺骗检测结果、欺骗类型与信号载噪比参数。

2.3.2 分级响应与协同处理策略

基于并行检测的结果, 针对 4 类典型场景设计分级响应机制, 实现复合威胁下的最优防护, 具体如下。

1) 无干扰、无欺骗场景: 两类算法均输出正常判定, 系统保持正常授时状态, 持续执行并行检测, 不触发任何防护动作。

2) 仅干扰、无欺骗场景: BSS-TSFANet 触发干扰告警, 基于识别出的干扰类型匹配对应抑制算法, 完成干扰抑制后输出干净信号至授时解算模块; CNN-LSTM 算法保持正常检测状态, 不触发告警。

3) 无干扰、仅欺骗场景: CNN-LSTM 算法触发欺骗告警, 立即输出异常信号至授时终端, 触发本地守时切换、钟差校验等防护动作, 锁定错误授时结果; BSS-TSFANet 保持正常检测状态, 不触发干扰抑制动作。

4) 干扰与欺骗同时存在场景: 采用“先干扰抑制、后欺骗验证”的串级协同策略, 首先由 BSS-TSFANet 触发干扰告警, 执行对应干扰抑制算法, 恢复信号载噪比与信噪比; 待干噪比恢复至 -10 dB 以上、信号质量满足欺骗检测要求后, 再由 CNN-LSTM 算法对抑制后的信号进行二次欺骗检测, 若检测到欺骗则触发对应防护动作, 若无欺骗则恢复正常授时。该策略可有效避免低信噪比环境下欺骗检测的高误检率问题, 同时确保复合威胁下的防护有效性。

2.3.3 极端工况冗余保护机制

针对变电站极端复杂电磁环境, 设计两项冗余保护机制, 保障系统运行稳定性, 具体如下。

1) 强干扰暂停机制: 当 BSS-TSFANet 检测到干噪比低于 -25 dB 、信号完全被压制时, 立即向 CNN-LSTM 算法发送暂停检测指令, 锁定欺骗检测结果, 避免无效检测导致的误告警; 同步触发授时终端切换至本地高稳晶振守时模式, 待信号质量恢复后, 重新启动并行检测。

2) 检测结果交叉验证机制: 当两类算法同时触发告警时, 系统自动记录干扰与欺骗的特征数据, 完成干扰抑制与欺骗检测后, 将处理后的信号参数与历史正常信号特征进行交叉比对, 验证防护动作的有效性, 避免误动作导致的授时中断。

2.3.4 系统集成适配设计

两类算法采用模块化设计, 可直接集成于现有电力时间同步终端的 FPGA+ARM 嵌入式硬件平台, 无需额外新增硬件设备: BSS-TSFANet 算法的盲信号分离模块与 TSFANet 推理模块部署于 FPGA 端, 实现信号预处理与干扰识别的硬件加速; CNN-LSTM 欺骗检测算法部署于 ARM 端, 实现轻量化实时推理; 两类模块通过内部高速总线完成参数交互与指令传输。

3 试验平台搭建与试验方案

为验证本文提出的 BSS-TSFANet 抗干扰算法与 CNN-LSTM 欺骗检测算法在电力时间同步系统中的有效性, 搭建试验平台并设计针对性的试验方案。

3.1 试验平台搭建

试验平台基于“GNSS 信号源—干扰/欺骗源—电力时间同步终端—监测系统”架构, 模拟变电站复杂电磁环境, 平台整体结构如图 2 所示, 各模块详细参数如表 2~4 所示。

GNSS 信号源—干扰/欺骗源—电力时间同步终端—监测系统基于中国电子科技集团公司第 54 研究所的“满天星”离散天线阵微波暗室搭建。

在“满天星”微波暗室半球波束内布置多个固定天

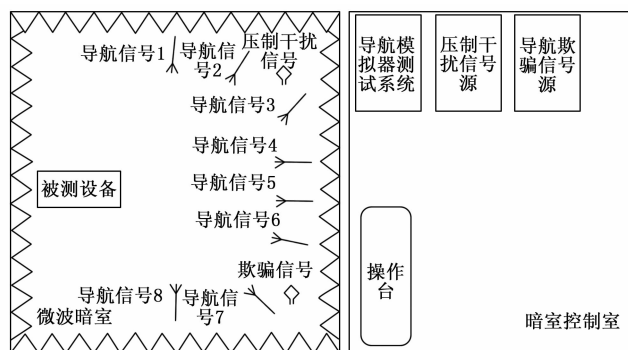


图 3 平台整体结构示意图

线, 通过实时选取最靠近轨迹点的固定天线发射卫星模拟信号达到模拟卫星运动轨迹功能。

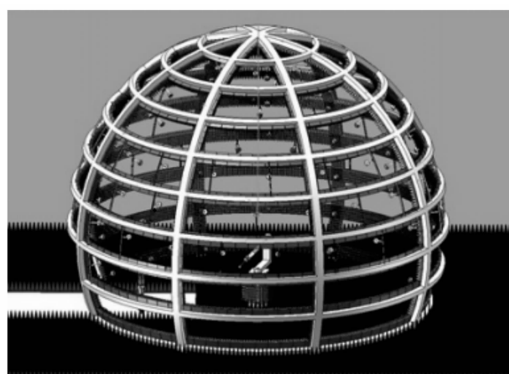


图 4 “满天星”离散天线阵微波暗室

主要测试设备由深圳市远东华强有限公司研制的 1 台 FH-NS9000 导航信号模拟器, 2 台 FH-NS3000 导航信号模拟器。

FH-NS9000 导航信号模拟器支持北斗、GPS、GLONASS、GALILEO 等四大卫星导航系统, 具备北斗三号 RNSS、RDSS、全球短报文联合仿真功能, 支持北斗三号系统恒包络输出, 具备星基、地基增强信号生成与数仿功能。支持组合导航和测试用惯性导航数据生成、结合场景仿真的欺骗干扰仿真以及输出信号正确性的自检功能。支持通过实时计算观测场景下的所有可视卫星仰角和方位角, 就近选取仰角和方位角差值最小的固定天线发射该可视卫星的模拟信号, 达到模拟全卫星星座的目的。

FH-NS3000 导航信号模拟器支持北斗、GPS、Galileo、GLONASS 系统任意三频点组合的导航信号的模拟仿真, 可重构为导航欺骗信号源和压制干扰信号源, 整机采用了低成本 1 U 机箱设计。

FH-NS3000 导航信号模拟器重构为导航欺骗信号源支持反无人机模式, 模拟电站附近常见的导航欺骗干扰信号。

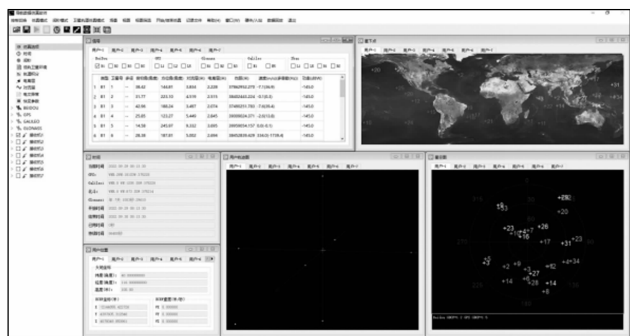


图 5 FH-NS9000 导航信号模拟器配置界面

FH-NS3000 导航信号模拟器重构为压制干扰信号源支持生成模拟单音、脉冲、扫频、梳状、宽带等常见的压制干扰信号。



图 6 压制干扰信号源配置界面

3.2 试验环境与参数配置

3.2.1 试验环境模拟

试验环境模拟电站复杂电磁环境，具体参数如下。

电磁环境：模拟电站内工业设备杂散辐射、突发脉冲干扰；

北斗信号参数：BDS B1I 信号（频率 1 561.098 MHz），信号功率 133 dBm；

压制干扰参数：干噪比（INR）范围 -20 dB；干扰类型包括单音（频率 1 561.098 MHz）、脉冲（周期 100 μ s）、扫频（扫频范围 1 550~1 570 MHz，周期 10 ms）、梳状波（8 个频点，间隔 0.5 MHz）、宽带（带宽为 4.092 MHz，BPSK 调制）；

欺骗干扰参数：欺骗类型包括转发式（延迟 50 ms）、生成式。设置场景 1：转发式，功率优势 0 dB，欺骗注入时间 100 s；设置场景 2：生成式，功率优势 0 dB，欺骗注入时间 100 s。接收机采样率为 5 Hz，观察时长 400 s。

3.2.2 算法参数配置

1) BSS-TSFANet 算法参数：

时频域虚拟通道数 $M=4$ ，时间延迟步长 $\Delta_t = 1$ 帧，频率平移步长 $\Delta f = 2$ 个频点；

FastICA 最大迭代次数 200，收敛容差 10^{-4} ；

干扰分量筛选功率阈值：低于最大功率 15 dB 的分量舍弃；

TSFANet 输入时频图尺寸：512 $\times$ 512；

空间支路：3 个 GSCM 模块，通道数分别为 16、32、64；

时间支路：BiGRU 隐藏层大小 128；

DANA 模块中通道注意力 MLP 隐藏层大小 8；

训练参数：优化器 Adam，学习率 0.001，批次大小 32，迭代轮数 100，早停耐心值 10；

训练集/验证集/测试集划分比例 7 : 2 : 1。

2) CNN-LSTM 算法参数：

I/Q 数据采样参数：采样率 1 MHz，序列长度 1 024 点，每帧数据重叠率 50%；

STFT 参数：帧长 $L=64$ ，帧移 $S=32$ ，汉宁窗；

PCA 参数：主成分数量 $M=8$ ；

训练参数：训练集/验证集/测试集划分比例 7 : 2 : 1，迭代次数 200 轮，批次大小 32；

早停策略：耐心值（Patience）= 10，即验证集损失连续 10 轮不下降则停止训练；

自适应门限参数：基础门限 0.3，调整系数 0.2，载噪比基准值 25 dB Hz。

3.3 试验结果

BSS-TSFANet 抗干扰算法分析：由表 2 可知，在干噪比 -20 dB 下，BSS-TSFANet 对 5 类典型压制干扰的平均识别准确率达到 96.78%，其中对单音连续波干扰识别率最高（98.2%）。表 3 显示，对于复合干扰，BSS 模块成功分离出各干扰成分，TSFANet 对各成分的识别召回率平均达 93.78%，验证了“先分离后识别”策略的有效性。在干噪比 -20 dB 信号条件下，BSS-TSFANet 仍能保持 85% 以上的识别准确率，体现出 DANA 模块的抗噪优势。算法单次推理时间约 25 ms，满足电力终端实时性要求。

表 2 单一干扰识别准确率（干噪比 -20 dB）

干扰类型	准确率/%
单音连续波	98.2
脉冲干扰	96.1
扫频干扰	96.8
梳状波	97.5
宽带	95.3
平均	96.78

表 3 典型复合干扰成分识别召回率（干噪比 -20 dB）

复合场景	干扰 1 成分 召回率/%	干扰 2 成分 召回率/%	干扰 3 成分 召回率/%	平均成分 召回率/%
单音+脉冲	98.1	96.5	—	97.3
扫频+宽带	94.3	92.8	—	93.55
单音+扫频+脉冲	92.1	90.5	88.9	90.5
总体平均				93.78

CNN-LSTM 欺骗检测算法分析：由表 4 可知，本文提出的 CNN-LSTM 算法在转发式欺骗场景下准确率达 98.75%，在生成式欺骗场景下达 99.95%，显著优于传统阈值检测法和单一 LSTM 方法。这得益于时频图与 PCA 特征压缩保留了关键欺骗特征，轻量化 CNN 有效提取局部异常，LSTM 捕捉了时序相关性，自适应门限进一步降低了弱欺骗的漏检率。算法参数量约 0.8 M，可在嵌入式平台实时运行。

表 4 不同场景的欺骗干扰检测准确率

	阈值检测 法/%	LSTM 方 法/%	CNN-LSTM 算 法/%
欺骗场景 1	44.75	78.25	98.75
欺骗场景 2	79.15	95.85	99.95

综上，两种算法分别解决了电力系统抗干扰与防欺骗的难题，且均具备轻量化、高精度的特点，可协同部署于电力时间同步终端。

4 结束语

本研究针对电力时间同步系统面临的压制干扰与欺骗信号威胁，提出了 BSSTSFANet 抗干扰识别算法与多特征融合 CNNLSTM 欺骗检测算法。BSSTSFANet 通过盲信号分离将复合干扰解构为独立分量，再经改进的轻量化 TSFANet 提取时空特征，实现了对单一干扰的高精度分类和对复合干扰的有效解构；CNNLSTM 算法利用 STFTPCA 联合降维与 CNNLSTM 深度特征提取，结合自适应门限，显著提升了对弱欺骗与生成式欺骗的检测能力。试验结果表明，两种算法在电力典型场景下均达到 96% 以上的准确率，且满足嵌入式终端的轻量化、实时性要求，为智能电网时间同步系统提供了一体化抗干扰与防欺骗技术方案。本研究提出的算法性能验证基于微波暗室的模拟电磁环境完成，仅覆盖了电力场景典型的干扰与欺骗类型，未在真实变电站的多径效应、动态杂散辐射、多源干扰并发的复杂现场环境中开展长期稳定性测试，算法的现场环境适配性有待进一步验证。

参考文献：

[1] 李 博，方 彤. 北斗卫星导航系统（BDS）在智能电网的应用与展望 [J]. 中国电力，2020，53（8）：107

- 116.
[2] 李秀彩，李文猛，何晓阳，等. 电力时间同步系统防欺骗和抗干扰设备试验研究 [J]. 电工技术，2023，（18）：202 - 206.
[3] 杨 帆. 基于北斗系统的嵌入式时钟同步技术及安全性分析研究 [D]. 天津：天津理工大学，2023.
[4] 杨斌杰. 基于多径信号的 GNSS 欺骗检测技术 [D]. 厦门：厦门大学，2022.
[5] 徐莫迟. 基于强化学习的测控链路抗干扰智能决策研究与实现 [D]. 成都：电子科技大学，2025.
[6] 陈 凤，李 聪，朱立东，等. 卫星通信干扰信号识别技术研究现状及展望 [J]. 太赫兹科学与电子信息学报，2024，22（3）：227 - 239.
[7] 张骏杨，楚鹰军. 卫星导航授时信号的抗干扰和欺骗检测技术综述 [J]. 现代传输，2020，（2）：56 - 65.
[8] 高田露. 基于矩阵特征值的 GNSS 干扰检测算法研究 [D]. 四川：中国民用航空飞行学院，2025.
[9] 何立爽. 超短波跳频电台抗灵巧干扰的关键技术研究 with 实现 [D]. 成都：电子科技大学，2025.
[10] 钟万福. 卫星导航系统电磁干扰智能识别技术研究 [D]. 山东：山东大学，2024.
[11] 马志奇，叶红军，魏 亮. 基于载噪比同步变化的北斗欺骗检测方法 [J]. 导航定位与授时，2024，11（1）：87 - 96.
[12] 陈建平，王旭旭，罗欣宇，等. 北斗欺骗干扰对电力授时的影响与对策分析 [J]. 浙江电力，2020，39（11）：34 - 39.
[13] 吴 果. 抗干扰卫星通信系统定时同步技术研究 [D]. 西安：西安电子科技大学，2018.
[14] 施俊龙. 基于改进 RCNN 算法的载波相位卫星导航欺骗信号检测技术 [J]. 海南热带海洋学院学报，2025，32（5）：106 - 112.
[15] 赵 慎，黄文娜，覃业梅，等. 一种基于 LSTM 的卫星导航欺骗干扰检测方法 [J]. 智能科学与技术学报，2025，7（2）：234 - 245.
[16] 王山亮. 基于 ELM 的卫星导航欺骗式干扰检测 [D]. 湘潭：湘潭大学，2022.
[17] 傅 宁，范金锋，杨 芳，等. 电力系统 GNSS 授时接收机抗干扰技术研究 [J]. 无线电工程，2020，50（1）：81 - 84.
[18] 陈 斌，陈真通，章坚武，等. 电网卫星授时系统中基于定向天线的北斗干扰源定位 [J]. 浙江电力，2021，40（2）：50 - 55.
[19] 周 斌，金贵红，吴育腾，等. 智能电网卫星导航接收机自主抗欺骗检测方法 [J]. 电力信息与通信技术，2023，21（11）：82 - 87.
[20] 孙天阳，刘文麒，王家星，等. 复杂电磁环境下的抗干扰 GNSS 授时终端设计 [J]. 导航与控制，2024，23（2）：62 - 71.