

一种基于LSTM的卫星导航欺骗干扰检测方法

赵慎^{1,2}, 黄文娜¹, 覃业梅^{1,2}, 廖一霏¹, 杨玲玲¹

(1. 湖南工商大学智能工程与智能制造学院, 湖南 长沙 410205;

2. 湘江实验室, 湖南 长沙 410205)

摘要: 面向卫星导航欺骗干扰检测的问题, 本文提出一种适用于长短期记忆神经网络 (Long Short-term Memory, LSTM) 检测欺骗干扰的特征参数选取及数据处理方法。基于欺骗干扰对接收机环路的影响分析, 选取跟踪环路中的直接与间接信息作为欺骗检测特征参数; 利用滑窗技术对特征参数进行预处理, 并按时间序列构建训练集和测试集, 以保证特征的时间关联性。基于美国德克萨斯大学奥斯汀分校的TEXBAT数据集进行实验, 相较于现有SVM方法, 本文方法可将欺骗检测的准确率提高2.19%, 且欺骗场景识别的准确率达99.98%, 可有效解决导航欺骗的检测和场景识别问题。

关键词: 卫星导航; 欺骗干扰; 滑窗处理; 长短期记忆神经网络

中图分类号: TN96, TP391

文献标志码: A

A Satellite Navigation Spoofing Interference Detection Method Based on LSTM

ZHAO Shen^{1,2}, HUANG Wenna¹, QIN Yemei^{1,2}, LIAO Yifei¹, YANG Lingling¹

1. School of Intelligent Engineering and Intelligent Manufacturing, Hunan University of Technology and Business, Changsha Hunan 410205, China

2. Xiangjiang Laboratory, Changsha, Hunan 410205, China

Abstract: Facing the problem of satellite navigation spoofing interference detection, this paper proposes a feature parameter selection and data processing method applicable to the detection of spoofing interference by Long Short-term Memory (LSTM) neural network. Based on the analysis of the effect of spoofing interference on the receiver loop, the direct and indirect information in the tracking loop is selected as the spoofing detection feature parameters; the feature parameters are preprocessed using the sliding window technique, and the training and test sets are constructed according to the time series to ensure the temporal relevance of the features. Based on the experiments conducted on the TEXBAT dataset from the University of Texas at Austin, this paper's method can improve the accuracy of spoofing detection by 2.19% and spoofing scene recognition by 99.98% compared to the existing SVM methods, which can effectively solve the problem of navigation spoofing detection and scene recognition.

Key words: satellite navigation, spoofing interference, sliding window processing, long and short-term memory neural networks

收稿日期: XXXX-XX-XX; 修回日期: XXXX-XX-XX

基金项目: 国家自然科学基金 (NO.61976088) 项目; 湖南省重点研发计划项目 (NO.2024AQ2033); 湖南省自然科学基金 (NO.2024JJ9188); 项目湖南省教育厅科研基金 (NO.21B0577) 项目

Foundation Items: National Natural Science Foundation of China (No.61976088), Key Research and Development Program of Hunan Province (No.2024AQ2033), National Natural Science Foundation of Hunan Province (No.2024JJ9188), Scientific Research Foundation of Hunan Provincial Education Department (NO.21B0577)

0 引言

全球卫星导航系统 (Global Navigation Satellite System, GNSS) 在军事与民用领域都有广泛的应用, 而由于导航信号到达地面强度弱、体制结构公开等原因, 使得 GNSS 极易受到干扰^[1]。按照干扰产生机理的不同, GNSS 干扰主要包括压制式和欺骗式干扰^[2]。压制式干扰通过大功率信号覆盖目标频段致使接收机失锁, 现有检测抑制技术相对成熟^[3-4]; 欺骗式干扰通过伪造卫星信号误导接收机输出错误信息^[5], 具有较强的隐蔽性。其中转发式欺骗存在信号时延特征, 可通过时间校验、多相关峰检测等简易方法检测^[2-5]; 生成式欺骗利用民用信号公开特性模拟虚假导航信息, 能诱导接收机跟踪环路锁定欺骗信号, 具有更强的隐蔽性和破坏性, 严重威胁导航时空信息安全^[6]。

区别于非合作通信信号的检测/识别问题^[7], 卫星导航欺骗检测技术包括基于导航数据信息、空间处理、射频前端、基带数字信号处理、定位导航运算结果和机器学习等六类^[2]。按照参数数量可分为单参数检测法和多参数检测法^[8]。单参数检测方法包括基于信号质量监测 (Signal Quality Monitoring, SQM)、空间信号来向 (Direction Of Arrival, DOA) 信息和射频前端自动增益控制 (Automatic Gain Control, AGC) 参数等^[2]; 多参数检测法综合利用多重参数信息, 具备精准识别并区分欺骗类别的能力^[9]。

机器学习算法能够将多重参数作为特征, 建立分类模型, 实现欺骗检测^[10]。Li 等^[11]利用 K 最近邻 (K-Nearest Neighbor, KNN) 算法, 监测小延迟欺骗场景下跟踪环路相关峰的数量变化和相位差, 计算测试数据 K 个最近邻点所属类别的发生频率, 预测数据类别, 检测欺骗干扰, 通过采集的 GNSS 数据集验证该方法在小延迟欺骗场景下优于传统多峰欺骗检测。不同于 KNN 算法, 倪淑燕等^[12]提出采用支持向量机 (Support Vector Machine, SVM) 的欺骗检测方法, 利用多相关器的输出构建特征参数, 在 TEXBAT 数据集上进行实验, 结果证明基于 SVM 的多参数检测方法可提高欺骗检测准确率。决策树 (Decision Trees, DT) 模型归纳已知数据, 对未知数据分类预测, 是机器学习常用的分类器。Gallardo 等^[13]利用 DT 模型和径向基函数 (Radial Basis Function, RBF) 核的

SVM 识别安全代码估计与重放 (Secure Code Estimation and Replay, SCER) 欺骗攻击, 根据信号功率谱密度、相关峰的高斯拟合参数和相位差等特征, 在公开数据集上进行实验, 结果证明机器学习算法提高了检测 SCER 欺骗攻击的准确率, 且在高信噪比条件下 DT 模型具有优异的检测性能。Pervysheva 等^[14]综合多接收机信息, 比较 DT、随机森林 (Random Forest, RF)、梯度提升决策树 (Gradient Boosting Decision Trees, GBDT)、极限提升树 (Extreme Gradient Boosting, XGBoost) 及装袋算法 (Bootstrap Aggregating, Bagging) 的模型性能, 基于 Jammertest 2023 数据集进行实验, 结果表明 RF 模型准确率优于其他模型。随着硬件处理能力的提升, 深度学习在 GNSS 欺骗检测领域逐渐得到应用^[10]。Tohidi 等^[15]采用粒子群优化算法 (Particle Swarm Optimization, PSO) 训练多层感知机 (Multi-layer Perceptron, MLP) 模型, 并分析多径信号在欺骗检测中的影响, 利用信号功率和相关函数变化等特征区分干扰信号、欺骗信号、多径信号和无干扰信号, 与贝叶斯分类器相比, 检测准确率提升了约 4%。Jayaweera 等^[16]提出了基于卷积神经网络 (Convolutional Neural Networks, CNN) 的 GPS 反欺骗方法, 利用 GPS 卫星信号的 DOA 时间序列作为输入, 识别准确率达 95%。Borhani-Darian 等^[17]将互模糊函数 (Cross Ambiguity Function, CAF) 图像作为输入, 利用并行 CNN 模型检测欺骗信号, 在中/高信噪比下, 检测性能优于传统算法。Sun 等^[18]采用 PCA-CNN-LSTM 模型实施小型无人机导航欺骗检测, 以定位信息与运动状态作为特征检测量, 基于自建的实验数据集, 识别准确率达 99.49%。Qi 等^[19]以定位结果和惯性传感器数据为特征参数, 构建 LSTM 欺骗检测模型, 并通过学习数据时序特征提高模型鲁棒性, 利用自建的 GNSS 数据集进行实验, 表明 LSTM 的准确率与泛化能力均优于决策树。盛孟刚等^[20]利用接收机钟差训练 LSTM 并与 MLP 对比, 结果表明 LSTM 在授时欺骗场景下检测效果更优。

综上, 采用机器/深度学习方法进行卫星导航欺骗检测, 是当前的研究热点, 其中, 特征参数的选取与处理方法直接影响欺骗检测的性能。从充分利用导航跟踪环路信息提高欺骗检测性能出发, 本文将接收机跟踪环路输出的直接和间接信息作为特征输入参数, 直接信息包括载噪比、载波相位、码

相位和载波多普勒频移, 间接信息为 Ratio、超前滞后相位差 (Early-late Phase, ELP)、Delta、功率检测与 SQM 融合 (Power Combined with SQM, PCS) 等 SQM 检测量, 进一步通过滑窗技术对特征参数进行预处理, 并按时间序列构建 LSTM 的训练集和测试集, 实现导航欺骗识别和场景分类。

1 GNSS 欺骗检测特征参数选择

1.1 GNSS 跟踪环路模型

接收机由射频前端处理、基带数字信号处理和定位导航解算三个信号处理功能模块组成^[21]。不存在欺骗时, 接收机接收到的信号中包含卫星信号和高斯白噪声

$$x(t) = x_r(t) + w(t) \quad (1)$$

其中, $x_r(t)$ 为卫星信号, $w(t)$ 表示均值为 0、方差为 σ^2 的高斯白噪声, 且

$$x_r(t) = \sqrt{P_r} C_r(t - \tau_r) D_r(t - \tau_r) \exp[j2\pi(f_{IF} + f_r)t + j\varphi_r] \quad (2)$$

其中, P_r 、 C_r 和 D_r 分别为信号功率、伪随机扩频码和导航信息数据比特电平值; τ_r 、 f_r 和 φ_r 分别为码相位、载波多普勒频移和载波相位; f_{IF} 为导航信号的载波中心频率。

为实现载波和扩频码同步, 同时得到载波相位、码相位、多普勒频移等信息, 基带数字信号处理中的跟踪环路一般设计为图 1 所示的结构。

信号进入跟踪环路经过混频器分为同相 (In-phase, I)、正交 (Quadrature-phase, Q) 支路, I

支路与 Q 支路输出结果为

$$I(n) = D_r(n) \cos(w_{IF}n) \cos(w_{IF}n + \varphi_r) = \frac{1}{2} D_r(n) \cos(\varphi_r) + \frac{1}{2} D_r(n) \cos(2w_{IF}n + \varphi_r) \quad (3)$$

$$Q(n) = D_r(n) \cos(w_{IF}n) \sin(w_{IF}n + \varphi_r) = \frac{1}{2} D_r(n) \sin(\varphi_r) + \frac{1}{2} D_r(n) \cos(2w_{IF}n + \varphi_r) \quad (4)$$

经过低通滤波器得到同相分量和正交分量

$$I(n) = \frac{1}{2} D_r(n) \cos(\varphi_r) \quad (5)$$

$$Q(n) = \frac{1}{2} D_r(n) \sin(\varphi_r) \quad (6)$$

利用环路鉴别器处理两路信号得到相位差, 本地载波与接收信号载波相位差为

$$\Delta\varphi = \arctan \frac{Q(n)}{I(n)} \quad (7)$$

根据相位差调整本地载波 NCO 使本地载波与输入信号载波相位对齐。与载波环类似, 早码、晚码和即时码的 I/Q 支路分别与本地产生的伪随机码进行相关运算, 当接收机锁定时, 接收信号与本地产生的信号频率完全相同, 假定相干积分累积时间内未发生数据位跳变, 且码相位和多普勒频移的影响相互独立^[4], 相干积分输出

$$I_p(n) = \sqrt{P_r} D_r(n) R(\hat{\tau}) \cos \varphi_r + N_I \quad (8)$$

$$Q_p(n) = \sqrt{P_r} D_r(n) R(\hat{\tau}) \sin \varphi_r + N_Q \quad (9)$$

其中, I_p 、 Q_p 分别为同相、正交相关器的输出; N_I 、 N_Q 分别为同相、正交支路的噪声; $\hat{\tau}$ 为真实信号与本地生成信号的码相位差; $R(\hat{\tau})$ 为真实信号

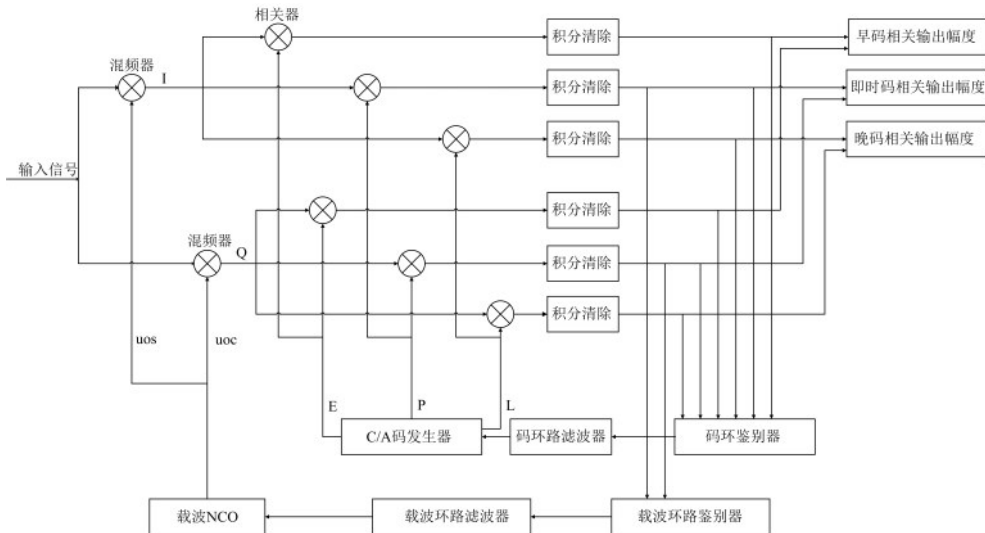


图 1 跟踪环路

与本地生成信号的互相关函数,以 GPS L1 频段为例,表达式为:

$$R(\hat{\tau}) = \begin{cases} 1 - |\hat{\tau}|, & |\hat{\tau}| \leq 1 \\ 0, & |\hat{\tau}| > 1 \end{cases} \quad (10)$$

1.2 欺骗信号影响分析

当存在欺骗时,接收机接收到的信号中包含真实信号、欺骗信号和高斯白噪声^[22]

$$x(t) = x_r(t) + x_s(t) + w(t) \quad (11)$$

其中, $x_s(t)$ 为欺骗信号。由欺骗式干扰原理可知, $x_s(t)$ 与 $x_r(t)$ 结构相似, 表示为

$$x_s(t) = \sqrt{P_s} C_s(t - \tau_s) D_s(t - \tau_s) \exp[j2\pi(f_{IF} + f_s)t + j\varphi_s] \quad (12)$$

其中, P_s 、 C_s 和 D_s 分别为信号功率、伪随机扩频码和导航信息数据比特电平值; τ_s 、 f_s 和 φ_s 分别为码相位、载波多普勒频移和载波相位; f_{IF} 为导航信号的载波中心频率。根据 GNSS 跟踪环路模型, 欺骗信号的注入会引起跟踪环路输出信息的变化, 如载波相位、码相位、载噪比、载波多普勒频移等。载波环输出的同相分量和正交分量分别为

$$I(n) = \frac{1}{2} D_r(n) \cos(\varphi_r) + \frac{1}{2} D_s(n) \cos(\varphi_s) \quad (13)$$

$$Q(n) = \frac{1}{2} D_r(n) \sin(\varphi_r) + \frac{1}{2} D_s(n) \sin(\varphi_s) \quad (14)$$

I/Q 支路相关器输出为

$$I_P(n) = \sqrt{P_r} D_r(n) R(\hat{\tau}) \cos \varphi_r + \sqrt{P_s} D_s(n) R(\hat{\tau}) \cos \varphi_s + N_I \quad (15)$$

$$Q_P(n) = \sqrt{P_r} D_r(n) R(\hat{\tau}) \sin \varphi_r + \sqrt{P_s} D_s(n) R(\hat{\tau}) \sin \varphi_s + N_Q \quad (16)$$

相关运算后的互相关函数为

$$R(\tau) = R(\hat{\tau}) + R(\tilde{\tau}) \quad (17)$$

其中, $R(\tilde{\tau})$ 为欺骗信号与本地生成信号的互相关函数, 欺骗信号与真实信号码相位差减小至 1 个码片内时, 欺骗信号使 $R(\tau)$ 的结果畸变^[3]。

1.3 欺骗检测特征参数选择

导航欺骗检测问题本质上是分类问题, 其中特征参数的选择和配置对欺骗检测的性能有着显著的影响。结合 1.2 节分析, 欺骗信号的注入会改变跟踪环路输出的载波相位、码相位、载噪比和载波多普勒频移等, 故有必要选择这些跟踪环路输出的直接信息作为分类的特征参数。

同时, 作为检测 GNSS 多径和欺骗中普遍采用的检测量, SQM 直观反映欺骗信号对跟踪环路相关峰的影响。通过对跟踪环路相关器早码、晚码和即时码输出进行处理, 得到各类 SQM 检测量。不失一般性, 本文选取 Ratio、Delta、ELP、PCS 等四类基础 SQM 检测量为后续机器学习的特征参数。此四类检测量分别表示为

$$\text{Ratio} = \frac{E_I + L_I}{2P_I} \quad (18)$$

$$\text{Delta} = \frac{E_I - L_I}{2P_I} \quad (19)$$

$$\text{ELP} = \arctan\left(\frac{Q_E}{E_I}\right) - \arctan\left(\frac{Q_L}{L_I}\right) \quad (20)$$

$$\text{PCS} = |Y_E| + |Y_L| - 2|Y_P| \quad (21)$$

其中 E_I 、 L_I 和 P_I 为同相相关器早码、晚码和即时码的输出; Q_E 和 Q_L 为正交相关器早码和晚码的输出; Y_E 、 Y_L 和 Y_P 分别为早码、晚码和即时码的相关输出幅度。

综上, 为充分利用基带信号处理信息, 本文将载波相位、码相位、载噪比和载波多普勒频移等跟踪环路输出的直接信息与 SQM 检测量作为欺骗检测的特征参数。

2 基于 LSTM 的 GNSS 欺骗检测算法

2.1 LSTM 算法

LSTM 是一种特殊的循环神经网络 (Recurrent Neural Network, RNN), 旨在解决传统 RNN 处理长序列数据时出现的梯度爆炸和消失的问题^[23]。LSTM 采用非线性结构, 具有优异的长序列数据处理能力。通过引入三个门控单元 (输入门、遗忘门和输出门), 允许选择性地保留或丢弃信息, 并且在传递信息时控制梯度的流动^[24]。欺骗对特征的影响与时间相关, 即欺骗检测问题中的检测量表现为时间相关联的长序列数据, 故选择 LSTM 用于检测卫星导航欺骗。LSTM 单元结构如图 2 所示。

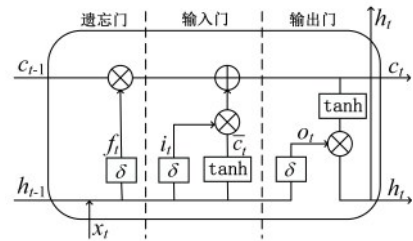


图2 LSTM 单元结构

各状态更新方程为

$$i_t = \delta(W_i[h_{t-1}, x_t] + b_i) \quad (22)$$

$$f_t = \delta(W_f[h_{t-1}, x_t] + b_f) \quad (23)$$

$$o_t = \delta(W_o[h_{t-1}, x_t] + b_o) \quad (24)$$

$$\bar{c}_t = \tanh(W_c[h_{t-1}, x_t] + b_c) \quad (25)$$

$$c_t = f_t \odot c_{t-1} + i_t \odot \bar{c}_t \quad (26)$$

$$h_t = o_t \odot \tanh(c_t) \quad (27)$$

其中, i_t 、 f_t 和 o_t 分别为输入门、遗忘门和输出门 t 时刻的值; $\bar{c}_t$ 和 c_t 为 t 时刻记忆单元的中间量和状态量; w_i 、 w_f 、 w_o 和 w_c 分别为不同状态单元对应的权重矩阵; b_i 、 b_f 、 b_o 和 b_c 分别为不同状态单元下对应的偏置矩阵; $\odot$ 表示对应元素相乘; h_t 为 t 时刻隐藏层的输出; δ 为 sigmoid 激励函数; $\tanh$ 为双曲正切函数。

针对导航欺骗检测问题的特点, 构建的 LSTM 分类模型包括 2 个 LSTM 层、1 个 Dropout 层和 1 个全连接层, 整体结构如图 3 所示。

为提升模型的鲁棒性及泛化能力, 在 LSTM 层后增加 Dropout 层, 模型输入为预处理后的三维数据, 输出为分类类别, 其中无欺骗表示为 0, 有欺骗表示为 1。

2.2 数据滑窗预处理

数据预处理可提升数据质量, 并减少噪声干扰。为提高模型的稳定性, 确保特征数据的均衡性, 对数据进行标准化预处理

$$\hat{z} = \frac{z - \mu}{\sigma} \quad (28)$$

其中, z 为原始数据特征值; μ 为特征均值; σ 为特征标准差; $\hat{z}$ 为标准化处理后输出。为有效提取局部特征, 保留全局趋势信息, 基于时序数据的时间相关性和高维度性, 采用加窗技术将长时间序列分

割为固定长度的子序列, 并通过给定步长进行滑动处理, 假定时间序列数据为

$$X = \{x_1, x_2, x_3, \dots, x_t\} \quad (29)$$

w 为窗口长度, n 为步长, 滑窗处理如图 4 所示。

滑窗生成的子序列为

$$W_i = \{x_i, x_{i+1}, x_{i+2}, \dots, x_{i+w-1}\}, i = 1, n+1, 2n+1, \dots \quad (30)$$

为适应导航数据特点, 窗口长度设定为 100、步长为 1, 滑窗生成的子序列作为 LSTM 的输入。每个输入序列包含当前时间点及之前 99 个时间点的特征值, 整个输入序列的标签由子序列中最后一个时间点的标签确定, 滑动窗口处理能够有效捕捉和记忆整个时间窗口内的信息, 常与 LSTM 结合应用。

综合以上分析, 基于 LSTM 分类算法的 GNSS 欺骗干扰检测流程如图 5 所示。

2.3 算法性能评估指标

基于多个指标评价检测性能, 包括准确率、召回率、精确率、F1 值。其中, 准确率为被正确预测的样本数占总样本数的比例; 召回率为实际属于某个类别的样本中, 成功被预测为该类别的比例; 精确率为被预测为某一类别的样本中, 实际为该类别的样本的比例; F1 值为精确率和召回率的调和平均数, 用来平衡精确率和召回率。多分类模型中类别 i 的准确率、召回率、精确率和 F1 值分别为

$$\text{Accuracy}_i = \frac{TP_i + TN_i}{TP_i + FN_i + FP_i + TN_i} \quad (31)$$

$$\text{Recall}_i = \frac{TP_i}{TP_i + FN_i} \quad (32)$$

$$\text{Precision}_i = \frac{TP_i}{TP_i + FP_i} \quad (33)$$

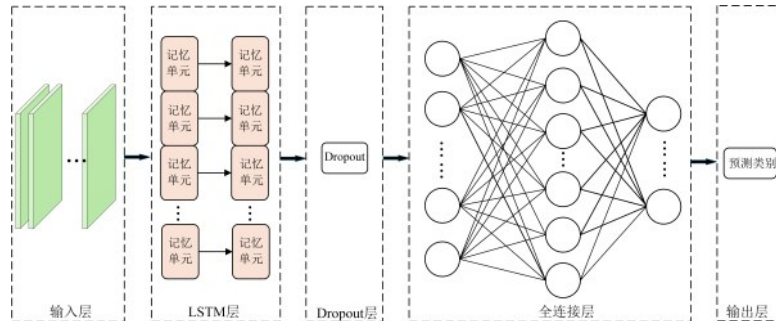


图3 LSTM分类模型

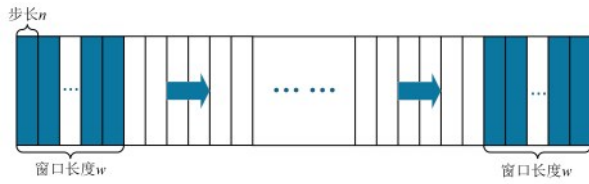


图4 数据滑窗处理示意图

$$F1_i = \frac{2 \times Precision_i \times Recall_i}{Precision_i + Recall_i} \quad (34)$$

其中, TP_i 为实际为类别 i 且预测为类别 i 的样本数; FP_i 为实际不是类别 i 但预测为类别 i 的样本数; TN_i 为实际不是类别 i 且预测为非类别 i 的样本数; FN_i 为实际为类别 i 但预测为非类别 i 的样本数。模型的整体评价指标为每个类别的评价指标均值, 对每个类别分别计算准确率、召回率、精确率和 F1 值, 计算各个指标平均值, 以此作为模型整体性能的衡量标准。

3 实验验证

实验中语言为 python3.8、深度学习框架为 pytorch1.10.2、GPU 为 NVIDIA RTX A6000、CPU 为 Intel Core i9-13900k、操作系统为 Windows 10。

3.1 实验数据集及模型参数设置

实验采用美国德克萨斯大学奥斯汀分校无线电导航实验室公开的 TEXBAT 数据集。该数据集是目前研究 GNSS 欺骗的经典实验数据, 包含八组欺骗场景和两组干净场景的真实采样数据, TEXBAT 数据集的欺骗场景设置如表 1 所示^[25]。

由于 ds5-ds6 为动态场景, 其多径干扰不利于实验结果对比, 故选择 ds2、ds3、ds4、ds7 四个数

表 1 TEXBAT 数据集主要参数

数据集	欺骗场景描述	欺骗种类	功率优势/dB	频锁状态	欺骗开始时间/s
ds1	静态瞬时跳变	N/A	N/A	失锁	100
ds2	静态大功率	时间	10	失锁	100
ds3	静态功率匹配	时间	1.3	锁定	100
ds4	静态功率匹配	地点	0.4	锁定	100
ds5	动态大功率	时间	9.9	失锁	100
ds6	动态小功率	地点	0.8	锁定	100
ds7	静态功率匹配	时间	N/A	锁定	110
ds8	静态功率匹配	时间	N/A	锁定	110

据集实施实验。均选用各数据集中的同一颗星 (PRN3) 进行分析, 以有效对比评估实验结果。

(1) 单检测量欺骗检测数据集。通过软件接收机对 ds2、ds3、ds4、ds7 数据集进行处理, 分别计算 PCS 检测量, 构成四类独立的数据集。每类数据集包含 45 000 组 PCS 数据, 其中无欺骗数据为 10 000 组, 有欺骗数据为 35 000 组。为确保训练和测试数据集中类别分布均衡, 同时兼顾数据时序性, 按照数据标签, 顺序划分数据集, 训练集与测试集占比分别为 80% 与 20%。四类独立数据集构成如图 6 所示。

(2) 多检测量欺骗检测综合数据集。对 ds2、ds3、ds4、ds7 数据集独立处理, 得到跟踪环路输出的载噪比、载波相位、码相位等直接特征, 同时根据相关器输出构建 PCS、Ratio、ELP 等 SQM 检测量为间接特征。直接特征与间接特征构成多检测量, 数据集处理时段均选取 0-450s, 特征输出间隔为 10ms, 每个数据集包含 45 000 组数据, 实验数

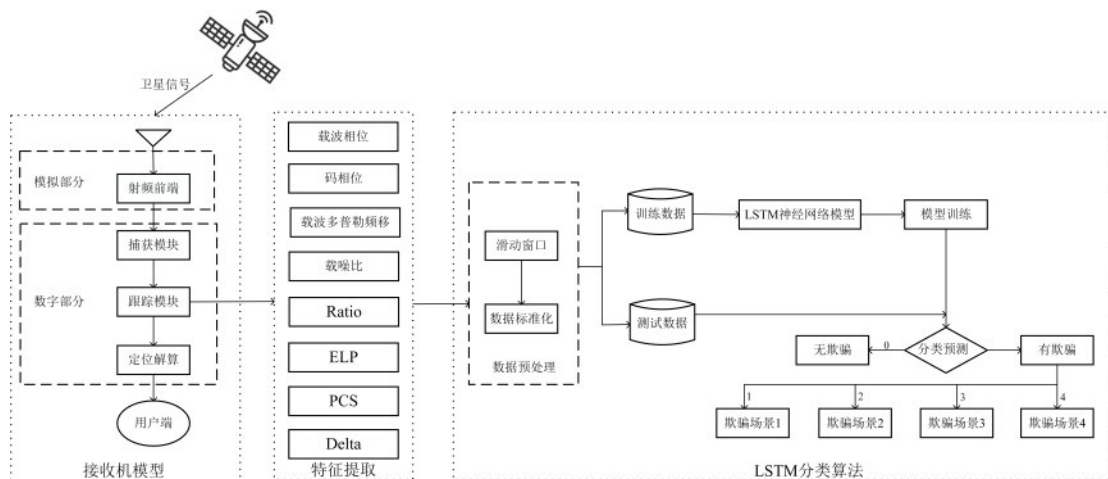


图5 LSTM分类算法的GNSS欺骗干扰检测流程

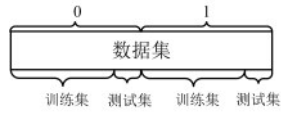


图6 单检测量欺骗检测数据集

数据集由 ds2、ds3、ds4、ds7 数据集联合组成，共 180 000 组。训练集与测试集占比分别为 80% 与 20%，数据集构成由图 7 所示。

(3) 欺骗场景识别数据集。对 clean、ds2、ds3、ds4、ds7 数据集分别处理，得到多检测量。分别选取 clean 的 0-450s、ds2 的 100-300s、ds3 的 100-300s、ds4 的 100-300s、和 ds7 的 110-310s 时段的数据，共 125 000 组。训练集与测试集占比分别为 80% 与 20%，数据集构成如图 8 所示。

利用试错法^[26]确定 LSTM 模型参数，以得到较优的结果，参数设置如表 2 所示。

3.2 欺骗检测实验

为验证应用 LSTM 实施 GNSS 欺骗检测的有效性，本节开展两类实验：(1) 对数据集中的单检测量进行欺骗检测，对比阈值检测法^[27]、KNN 分类法^[5]与 LSTM 方法的优劣；(2) 利用多检测量，评估 LSTM 进行欺骗检测的性能。

表 2 LSTM 模型超参数

参数名称	实验设置
Batch size	32
Dropout	0.5
优化器	Adma 优化算法
学习率	0.001
损失函数	交叉熵损失函数

3.2.1 单检测量欺骗检测

以 PCS 检测量为例，探讨单 SQM 欺骗检测量在各数据集上的适用性。分别计算 clean、ds2、ds3、ds4、ds7 数据集中 PRN3 的 PCS 检测量，结果如图 9 所示。

由图 9 (b) 可见，无欺骗 clean 数据集的 PCS 检测量值表现平稳。受欺骗信号注入对环路的影响，ds2 的 PCS 检测量在 110s 处突变，比理论注入时刻 (100s，见表 1) 晚 10s；与之相比，ds3 和 ds4 的 PCS 检测量分别在 120s 和 170s 表现出明显突变，比理论欺骗注入分别晚 20s 和 70s；而 ds7 的 PCS 检测量未表现明显波动。基于文献[27]中阈值检测方法，设置虚警率为 10%，检测概率变化曲线如图 10 (a) 所示。进一步，基于二元判决，当检测概率大于 50% 时，判定存在欺骗干扰，输出为

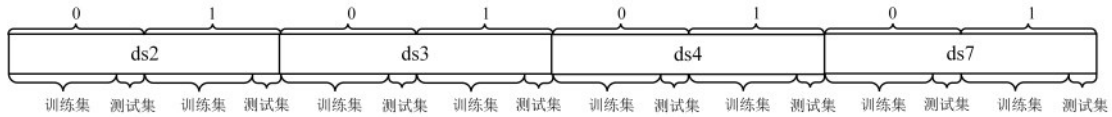
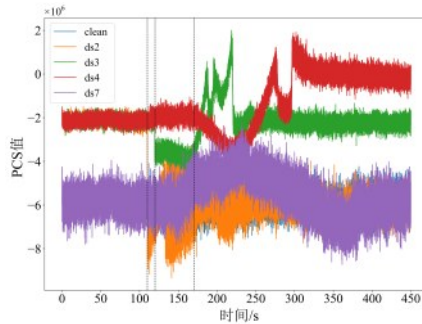


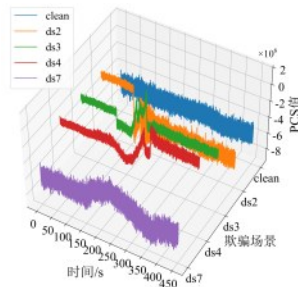
图7 多检测量欺骗检测数据集



图8 欺骗场景识别数据集



(a) PCS检测量二维图



(b) PCS检测量三维图

图9 不同场景下PCS检测量变化图

1; 当检测概率小于 50% 时, 判定无欺骗干扰, 输出为 0, 判决结果曲线如图 10 (b) 所示。

由图 10 (b) 可见, 针对不同欺骗数据集, 阈值检测法的欺骗检测结果存在显著差异。ds2 数据集的判决结果在 110s 及之后时稳定保持为 1; ds3 数据集在 120s-220s 的判决结果为 1, 且存在部分判定为 0 的离散位置; ds4 数据集在 200s 之后的判决结果为 1, 且存在类似判定为 0 的离散位置; ds7 的判决结果存在较大波动, 分别在 180s 与 370s 判定为 1, 且准确判别为 1 的频次较少, 漏检率较高。综合以上结果可见, 应用阈值检测法实施欺骗检测, 仅对 ds2 数据集表现出较低的漏检率、较高的准确率, 而对 ds3、ds4 和 ds7 等数据集中的欺骗检测效果的适用性和实时性均不佳。

基于 3.1 节构建的 PCS 单检测量欺骗检测数据集, 将有/无欺骗分别标记为 1/0, 采用 KNN 模型与 LSTM 模型进行训练和分类。各数据集中 LSTM 模型测试集分类的混淆矩阵如图 11 所示。

分别计算阈值检测法、KNN 分类法和 LSTM 方法的准确率, 结果如表 3 所示。

由表 3 可见, 与文献[27]中的阈值检测法和文献[5]中 KNN 分类法相比, 以保持时序特征的 PCS 为单特征检测量, LSTM 方法准确率均高于前两者, 表明本文方法可利用检测量的时序特性, 实现

表 3 不同数据集的检测准确率

欺骗场景	阈值检测法	KNN 分类法	LSTM 方法
ds2	97.78%	97.81%	100%
ds3	44.67%	73.77%	77.94%
ds4	78.89%	80.81%	95.76%
ds7	54.01%	70.39%	82.13%

检测性能的提升。

同时表 3 中结果表明, 对于不同数据集, 以上三种方法的检测性能均存在差异性。通过分析欺骗场景可知, ds2 数据集欺骗方式为大功率时间欺骗, 欺骗注入时, 特征参数变化显著, 较易检测到欺骗, 检测准确率高; 与之相比, ds3 数据集为小功率时间欺骗, ds4 数据集为小功率地点欺骗, ds7 数据集中欺骗信号具有频率动态特性, 使得基于单检测量的检测方法难以准确识别欺骗, 进而影响检测性能。此外, 对于不同数据集的欺骗检测问题, 单一 SQM 检测量可能存在普适性不足的问题, 为此进一步开展多检测量实验研究。

3.2.2 多检测量欺骗检测

基于 3.1 节构建的多检测量欺骗检测综合数据集, 将有/无欺骗标记为 1/0, 采用 LSTM 模型进行训练与分类。对测试集分类, 得到的混淆矩阵如图 12 所示。

由图 12 可见, 欺骗检测分类正确的数量远大

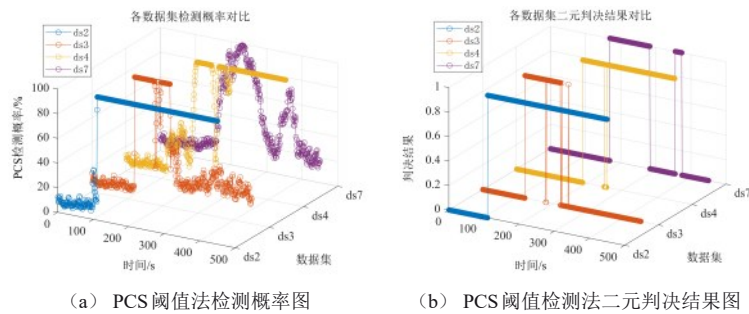


图 10 不同场景下 PCS 阈值检测结果图

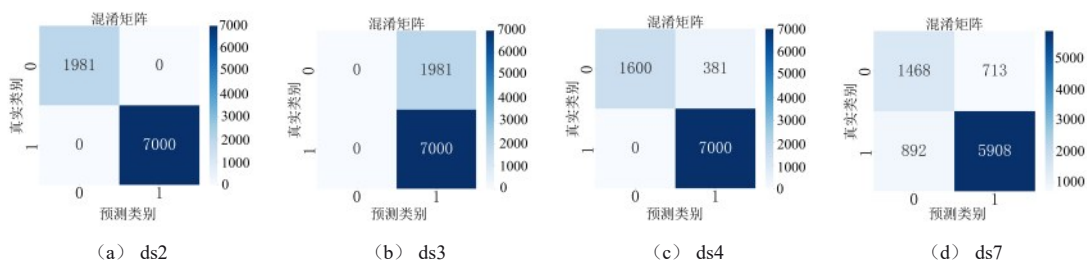


图 11 不同数据集的 LSTM 模型测试集混淆矩阵

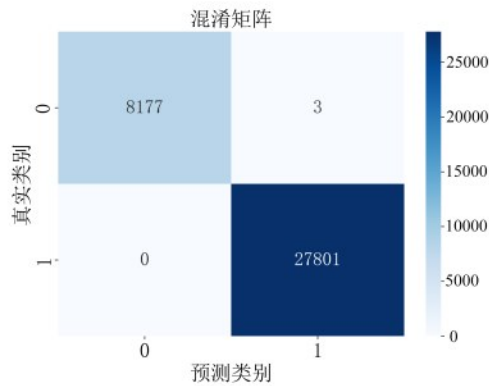


图 12 LSTM 模型混淆矩阵

于分类错误的数量。相较于利用单检测量特征，综合多个检测量实施检测欺骗时，模型分类的准确率表现出显著提升。利用多个检测量的数据集，实施 LSTM 模型训练，并分别对 ds2、ds3、ds4 和 ds7 数据集实施欺骗检测，结果如图 13 所示。

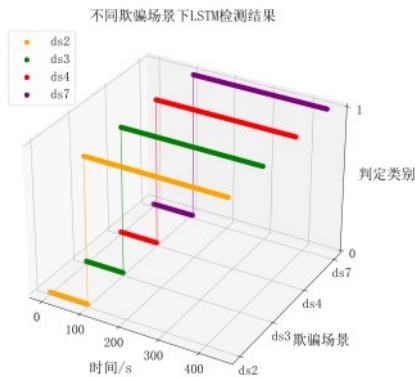


图 13 不同场景下 LSTM 模型的检测结果

分析图 13 中四个数据集的欺骗检测结果可见，多检测量的 LSTM 模型所检测的欺骗时刻与表 1 中欺骗注入时间基本一致，表明所提方法具备较好的普适性和即时性。

进一步，表 4 总结了近期关于“基于多检测量的导航欺骗检测”部分成果，并着重对比列出了特征参数、检测算法及其准确率性能等。

由表 4 可见，Sun 等提出的 PCA-CNN-LSTM 方法融合多源数据，准确率为 99.49%，由于需处理多传感器数据及相对复杂的算法，其计算资源要求高；倪淑燕等以多个相关器的输出为检测量，实施 SVM 检测，检测准确率为 97.8%，针对不同的欺骗场景，其检测性能表现出一定的差异性；Pervysheva 等利用多个接收机输出的位置、时钟及信号质量等参数构建 RF 模型，准确率为 98%，要求多接收机协同工作，同步精度要求高；Qi 等以位移与加速度等少量特征为检测量，基于 LSTM 模型，在低特征维度条件下实现 97.6% 的检测准确率，不能适用于复杂轨迹欺骗。与上述方法相比，本文方法仅需单个导航接收机的跟踪环路信息，对检测设备要求较低，且在多个数据集上检测性能表现好。相较于传统 SVM 方法^[12]，所提方法的欺骗检测准确率高出 2.19%。

3.3 欺骗场景分类及模型对比

在欺骗检测与抑制问题中，若具备识别欺骗攻击方式的能力，则可制定更具针对性的抗欺骗措施。鉴于多检测量的 LSTM 模型较优的检测性能，进一步验证其对欺骗场景的区分能力。

与欺骗检测的二元分类相比，欺骗场景识别本质是多元分类问题。需要说明的是，本小节所指欺骗场景，对应 ds2、ds3、ds4 和 ds7 四种不同欺骗数据集。其中，ds2 数据集为静态大功率的时间欺骗场景，ds3 数据集为静态功率的时间欺骗场景；ds4 数据集为静态功率匹配的位置欺骗；ds7 数据集与 ds3 数据集类似，均为静态功率的时间欺骗场景，区别在于其欺骗方式更为复杂，牵引策略为载波同步。鉴于该四类数据集的欺骗策略的差异，故可将之定义为四类欺骗场景。

基于 3.1 节构建的欺骗场景识别数据集，将 clean、ds2、ds3、ds4 和 ds7 数据集的数据分别标记为 0、1、2、3、4，采用 LSTM 模型进行训练与测试。训练集与测试集的损失值与准确率变化曲线

表 4

基于多检测量的欺骗检测方法

方法提出者	特征参数	算法	准确率/%
Sun 等 ^[18]	导航定位参数、运动状态特征、传感器数据	PCA-CNN-LSTM	99.49
倪淑燕等 ^[12]	多个相关器输出值	SVM	97.8
Pervysheva 等 ^[14]	多接收机的位置、时钟信息及信号质量	RF	98
Qi 等 ^[19]	位移结果、运动状态特征	LSTM	97.6
本文方法	跟踪环路信息	LSTM	99.99

如图 14 所示。

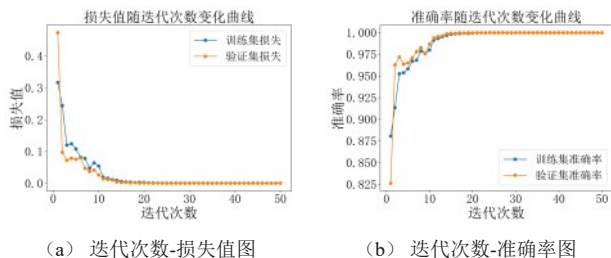


图 14 损失值与准确率随迭代次数变化曲线图

由图 14 (a) 可见, 随着迭代次数的增加, 测试集的损失值呈现下降趋势, 且逐渐趋近于训练集的损失值, 表明模型未出现欠拟合; 同时, 测试集和训练集的损失值趋于收敛, 相邻迭代次数的损失值差异小于 0.05, 表明模型未出现过拟合。由图 14 (b) 可见, 准确率在训练过程中趋于收敛, 最终结果在 99% 附近。进一步, 在模型收敛时, 得到模型的混淆矩阵, 如图 15 所示。



图 15 LSTM 多分类模型混淆矩阵

由图 15 可见, LSTM 多分类模型误分类样本数较少, 分类表现均衡。由混淆矩阵得准确率均值为 99.98%, 表明 LSTM 模型具备识别欺骗场景的能力。分别对 SVM、DT、KNN 采用相同的训练集与测试集, 进行训练与评估, 以对比各模型的性能。需要指出的是, 为确保机器学习模型的检测性能, 论文基于网格搜索法^[26]确定其中的超参数, 超参数结果如表 5 所示。

经过训练和测试后, 得到各模型的多分类评价指标的均值, 结果如表 6 所示。

由表 6 可见, 采用 RBF 核函数的 SVM 的分类准确率为 89.01%, 在选用的几种机器学习模型中表现最佳。与 SVM 模型相比, LSTM 的 4 项指标均表现更佳。

综合以上两类实验结果可知, 由于 GNSS 欺骗

表 5 机器学习模型超参数

模型	超参数
SVM	C=100
	Kernel:RBF
	Gamma:scale
DT	Min_samples_leaf=1 Max_depth=15 Criterion:gini
KNN	Metric:euclidean
	Neighbors:11 Weights:distance

表 6 机器模型分类评价指标

模型	准确率/%	召回率/%	精确率/%	F1 值/%
SVM	89.01	88.28	89.1	88.64
KNN	85.43	84.85	85.36	85.05
DT	74.82	72.01	74.9	72.73
LSTM	99.98	99.97	99.97	99.97

检测的时间相关性, 基于 LSTM 模型可有效解决 GNSS 欺骗检测和场景分类问题。

4 结论

本文在研究欺骗干扰对 GNSS 接收机基带跟踪环路影响的基础上, 分析 SQM 检测量随欺骗注入的变化, 解决了 LSTM 用于欺骗检测与场景识别时的特征提取和时序数据处理问题。理论分析和实验表明, LSTM 算法不仅可适用于欺骗检测, 亦可应用于欺骗场景的分类。

(1) 利用保留时序特征的单一检测量, LSTM 方法对欺骗检测的准确率高传统阈值法和 KNN 分类法; 综合利用保留时序特征的多个检测量, LSTM 方法的欺骗检测准确率得到进一步提升, 且具备良好的普适性。

(2) 将保留时序特征的检测量用于多种欺骗场景的识别, 其准确率达 99.98%。与传统机器学习相比, 准确率、召回率、精确率、F1 值均表现更佳。

参考文献:

- [1] 赵慎, 胡勇, 李世玲, 等. 基于 PCS 与 Ratio 融合的 GNSS 欺骗检测方法研究[J]. 全球定位系统, 2024, 49(04): 99-106.
ZHAO S, HU Y, LI S L, et al. Research on GNSS Spoofing Detection Method Based on PCS and Ratio Fusion[J]. Global Positioning System, 2024, 49(4): 99-106.
- [2] 周彦, 王山亮, 杨威, 等. GNSS 欺骗式干扰检测综述[J]. 计算机工程与应用, 2022, 58(11): 12-22.
ZHOU Y, WANG S L, YANG W, et al. Survey on GNSS Spoofing In-

- terference Detection[J]. Computer Engineering and Applications, 2022, 58(11): 12-22.
- [3] 赵慎, 胡勇, 李世玲, 等. 绝对同相支路输出的 GNSS 欺骗检测[J]. 导航定位与授时, 2024, 11(02): 83-92.
ZHAO S, HU Y, LI S L, et al. GNSS Spoofing Detection with Absolute In - Phase Branch Output [J]. Navigation Positioning and Timing, 2024, 11 (2): 83-92.
 - [4] 赵慎, 廖一霏, 李世玲, 等. 多相关器联合功率 GNSS 欺骗干扰检测方法研究[J]. 全球定位系统, 2024, 49(04): 66-74.
ZHAO S, LIAO Y F, LI S L, et al. Research on Multi-Correlator Joint Power GNSS Spoofing Interference Detection Method[J]. Global Positioning System, 2024, 49(4): 66-74.
 - [5] 倪淑燕, 陈世森, 付琦玮, 等. 卫星导航欺骗干扰检测与抑制技术综述[J]. 电讯技术, 2024, 64(05): 812-820.
NI S Y, CHEN S M, FU Q W, et al. Survey on Satellite Navigation Spoofing Interference Detection and Suppression Techniques[J]. Telecommunication Engineering, 2024, 64(5): 812-820.
 - [6] 周雅兰, 宋晓鸥. 利用机器学习的 GNSS 欺骗检测综述[J]. 计算机工程与应用, 2024, 60(17): 62-73.
ZHOU Y L, SONG X O. Survey on GNSS Spoofing Detection Using Machine Learning[J]. Computer Engineering and Applications, 2024, 60(17): 62-73.
 - [7] 赵慎, 戴卫华, 周开军, 等. 基于间隔自相关的跳频跳时信号突发检测[J]. 电子学报, 2024, 52(12): 3985-3993.
ZHAO S, DAI W H, ZHOU K J, et al. Frequency Hopping/Time Hopping Signal Burst Detection Based on Interval Autocorrelation[J]. Acta Electronica Sinica, 2024, 52(12): 3985-3993.
 - [8] Z. CHEN, J. LI, J. LI, et al. GNSS Multiparameter Spoofing Detection Method Based on Support Vector Machine[J]. IEEE Sensors Journal, 2022, 22(18): 17864-17874.
 - [9] 周彦, 王山亮, 杨威, 等. 基于 PSO-ELM 的卫星导航欺骗式干扰检测[J]. 导航定位与授时, 2022, 9(05): 153-161.
ZHOU Y, WANG S L, YANG W, et al. Satellite Navigation Spoofing Detection Based on PSO-ELM[J]. Navigation Positioning and Timing, 2022, 9(5): 153-161.
 - [10] GHANBARZADE Ali, SOLEIMANI Hossein. GNSS/GPS Spoofing and Jamming Identification Using Machine Learning and Deep Learning[J]. ArXiv abs/2501.02352, 2025, (): n. pag.
 - [11] J. LI, W. LI, S. HE, Z. DAI, Q. FU. Research on Detection of Spoofing Signal with Small Delay Based on KNN[J]//2020 IEEE 3rd International Conference on Electronics Technology (ICET), Chengdu, China. New York: IEEE, 2020: 625-629.
 - [12] 倪淑燕, 付琦玮, 陈世森, 等. 基于支持向量机的 GNSS 欺骗式干扰多相关器检测方法[J]. 电子信息对抗技术, 2025, 40(02): 24-31.
NI S Y, FU Q W, CHEN S M, et al. A Multi-Correlator Detection Method for GNSS Spoofing Interference Based on Support Vector Machine[J]. Electronic Information Warfare Technology, 2025, 40(02): 24-31.
 - [13] GALLARDO F, YUSTE A P. SCER Spoofing Attacks on the Galileo Open Service and Machine Learning Techniques for End-User Protection[J]. Journal of Navigation, 2020, 8: 85515-85532.
 - [14] PERVYSHEVA Y, KÄPPI J, SYRJÄRINNE J, et al. Multi - Receiver Ensemble Machine - Learning Techniques for GNSS Spoofing Detection with Generalisability Approach [C]//2024 32nd Telecommunications Forum (TELFOR). Belgrade, Serbia, 2024. New York: IEEE, 2024: 1 - 4.
 - [15] TOHIDI S, MOSAVI M R. Effective Detection of GNSS Spoofing Attack Using A Multi-Layer Perceptron Neural Network Classifier Trained by PSO[C]//2020 25th International Computer Conference, Computer Society of Iran (CSICC), Tehran, Iran. Tehran: CSICC, 2020: 1-5.
 - [16] JAYAWEERA M. A Novel deep learning GPS antispoofing system with DOA time-series estimation[C]//2021 IEEE Global Communications Conference (GLOBECOM), Madrid, Spain. Madrid: IEEE, 2021: 1-6.
 - [17] BORHANI-DARIAN P, LI H, WU P, et al. Detecting GNSS spoofing using deep learning[J]. EURASIP Journal on Advances in Signal Processing, 2024(14): 1-19.
 - [18] SUN Y, YU M, WANG L, 等. A Deep-Learning-Based GPS Signal Spoofing Detection Method for Small UAVs [J]. Drones, 2023, 7 (6): 370.
 - [19] Qi X, Sato T, Wen Z, et al. GNSS Spoofing Detection Using Multiple Sensing Devices and LSTM Networks[J]. IEICE Transactions on Communications, 2023, E106-B(12), 1372-1379.
 - [20] 盛孟刚, 盛思缘, 邓敏, 等. 基于长短期记忆网络的授时欺骗检测方法[J]. 全球定位系统, 2024, 49(04): 86-91.
SHENG M G, SHENG S Y, DENG M, et al. Timing Spoofing Detection Method Based on Long Short-Term Memory Network[J]. Global Positioning System, 2024, 49(4): 86-91.
 - [21] 谢钢. GPS 原理与接收机设计[M]. 电子工业出版社: 201701.436.
XIE G. GPS Principles and Receiver Design[M]. Beijing: Publishing House of Electronics Industry, 201701.436.
 - [22] 王文益, 龚婧, 王金铭. 基于 SCB 方差的 GNSS 欺骗式干扰检测算法[J]. 系统工程与电子技术, 2021, 43(08): 2254-2262.
WANG W Y, GONG J, WANG J M. GNSS Spoofing Interference Detection Algorithm Based on SCB Variance[J]. Systems Engineering and Electronics, 2021, 43(8): 2254-2262.
 - [23] 黄峻, 田永林, 戴星原, 等. 基于深度学习的自动驾驶多模态轨迹预测方法: 现状 & 展望[J]. 智能科学与技术学报, 2023, 5(02): 180-199.
HUANG J, TIAN Y L, DAI X Y, et al. A Survey on Multi-Modal Trajectory Prediction Methods for Autonomous Driving Based on Deep Learning[J]. Journal of Intelligent Science and Technology, 2023, 5(2): 180-199.
 - [24] 许博文, 毕敬, 苑海涛, 等. 基于季节性分解与长短期记忆网络的水质动态预警[J]. 智能科学与技术学报, 2021, 3(04): 456-465.
XU B W, BI J, YUAN H T, et al. Water Quality Dynamic Early Warning Based on Seasonal Decomposition and Long Short-Term Memory Network[J]. Journal of Intelligent Science and Technology, 2021, 3(4): 456-465.
 - [25] Humphreys T, Bhatti J, Shepard D P, et al. The Texas Spoofing Test Battery: Toward a Standard for Evaluating GPS Signal Authentication Techniques[C]//2012 ION GNSS Conference, 2012, 25: 3569-3583.
 - [26] 王路阳, 孙一宸, 于明鑫, 等. 基于 TimeGAN-LSTM 的无人机 GPS 欺骗干扰检测模型[J]. 电子测量与仪器学报, 2023, 37(06): 122-135
WANG L Y, SUN Y C, YU M X, et al. UAV GPS Spoofing Interference Detection Model Based on TimeGAN-LSTM[J]. Journal of Electronic Measurement and Instrumentation, 2023, 37(6): 122-135.
 - [27] 王璐, 张林杰, 吴仁彪. 功率监测与 SQM 融合的 GNSS 欺骗干扰检测[J]. 信号处理, 2023, 39(03): 505-515.
WANG L, ZHANG L J, WU R B. GNSS Spoofing Interference Detection by Power Monitoring and SQM Fusion[J]. Signal Processing, 2023, 39(3): 505-515.

[作者简介]



赵慎 (1983-), 男, 博士, 湖南工商大学智能工程与智能制造学院副教授, 电信与通信工程系主任, 主要研究方向为导航时空信息安全, 智能无线感知。



黄文娜 (2001-), 女, 湖南工商大学智能工程与智能制造学院硕士生, 主要研究方向为导航时空信息安全。



博士,
湖南

覃业梅 (1979-), 女, 工商大学智

能工程与智能制造学院教授, 智能科学与技术系主任, 主要研究方向为时间序列信号分析与预测。



廖一霏 (2000-), 女, 湖南工商大学智能工程与智能制造学院硕士生, 主要研究方向为导航时空信息安全。



杨玲玲 (1993-), 女, 博士, 湖南工商大学讲师, 主要研究方向为中红外激光技术、光电信号检测及处理。