

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: 针对卫星导航欺骗干扰检测问题, 提出一种基于LSTM的卫星导航欺骗干扰检测方法。通过分析欺骗干扰对接收机环路的影响, 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; 采用滑动窗口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, 以保持特征的时间关联性。基于得克萨斯大学奥斯汀分校公开的TEXBAT数据集进行实验, 实验结果表明, 相较于现有SVM方法, 所提方法将欺骗检测准确率提升了2.19%, 欺骗场景识别准确率达99.98%, 能有效解决导航欺骗检测和场景识别问题。

关键词: 卫星导航; 欺骗干扰; 滑动窗口处理; 长短期记忆神经网络

中图分类号: TN96, TP391

文献标志码: A

doi: 10.11959/j.issn.2096-6652.202517

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 410205, China

2. Xiangjiang Laboratory, Changsha 410205, China

Abstract: Facing the problem of satellite navigation spoofing interference detection, a satellite navigation spoofing interference detection method based on LSTM was proposed. Based on the analysis of the effect of spoofing interference on the receiver loop, the direct and indirect information in the tracking loop was selected as the spoofing detection feature parameters. The feature parameters were preprocessed using the sliding window, and the training and test sets were 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 with 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 network

0 引言

全球卫星导航系统 (global navigation satellite

system, GNSS) 在多个领域应用广泛, 但由于导航信号到达地面强度弱、体制结构公开等特点, GNSS容易受到干扰^[1]。根据干扰产生机理, GNSS

收稿日期: 2025-01-21; 修回日期: 2025-04-11

基金项目: 国家自然科学基金项目 (No.61976088); 湖南省重点研发计划项目 (No.2024AQ2033); 湖南省自然科学基金项目 (No.2024JJ9188, No.2025JJ90243); 湖南省教育厅科研基金项目 (No.21B0577)

Foundation Items: The National Natural Science Foundation of China (No.61976088), The Key Research and Development Plan Project of Hunan Province (No.2024AQ2033), The Natural Science Foundation of Hunan Province (No.2024JJ9188, No.2025JJ90243), The Scientific Research Foundation of Hunan Provincial Department of Education (No.21B0577)

干扰主要分为压制式和欺骗式两类^[2]。压制式干扰通过大功率信号覆盖目标频段，使接收机失锁，现有检测抑制技术相对成熟^[3-4]；欺骗式干扰则通过伪造卫星信号误导接收机输出错误信息^[5]，具有较强隐蔽性。其中，转发式欺骗存在信号时延特征，可通过时间校验、多相关峰检测等方法检测^[2-5]；生成式欺骗利用民用信号的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，隐蔽性和破坏性更强，严重威胁导航时空信息安全^[6]。

与非合作通信信号的检测和识别问题不同^[7]，卫星导航欺骗检测技术主要包括导航数据信息、空间处理、射频前端、基带数字信号处理、定位导航运算和机器学习6类方法^[2]，按照参数数量可分为单参数检测法和多参数检测法^[8]。单参数检测法包括基于信号质量监测（signal quality monitoring, SQM）、波达方向（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，具备精确识别和区分欺骗类别的能力^[9]。

机器学习算法能够利用多重参数建立分类模型，实现欺骗检测^[10]。Li等^[11]采用K最近邻（K-nearest neighbor, KNN）算法监测小时延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、预测数据类别和检测欺骗干扰，通过采集的GNSS数据集验证该方法在小时延欺骗场景下的检测性能优于传统多峰欺骗检测。倪淑燕等^[12]提出基于支持向量机（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数据集上验证了基于SVM的多参数检测方法可提高欺骗检测准确率。决策树（decision tree, DT）模型通过归纳已知数据对未知数据进行分类预测，是机器学习常用的分类器。Gallardo等^[13]采用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，实验结果表明，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模型表现出优异的检测性能。Pervysheva等^[14]综合多接收机信息，对DT、随机森林（random forest, RF）、梯度提升决策树

（gradient boosting decision tree, GBDT）、极限提升（extreme gradient boosting, XGBoost）树及引导聚集（bootstrap aggregating, Bagging）算法等模型的性能进行比较，并基于Jammertest 2023数据集进行实验，实验结果表明，RF模型的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（particle swarm optimization, PSO）算法训练多层感知机（multi-layer perceptron, MLP）模型，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^[16]提出一种基于卷积神经网络（convolutional neural network, CNN）的GPS反欺骗方法，以GPS卫星信号的DOA时间序列为输入，识别准确率达95%。Borhani-Darian等^[17]以互模糊函数（cross ambiguity function, CAF）图像为输入，采用并行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模型进行小型无人机导航欺骗检测，以定位信息与运动状态为特征检测量，在自建实验数据集上识别准确率达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，并通过学习数据的时序特征提高模型鲁棒性，基于自建的GNSS数据集进行实验，实验结果表明，LSTM在准确率与泛化能力上均优于决策树。盛孟刚等^[20]利用接收机钟差训练LSTM模型，并与MLP模型进行对比，结果表明LSTM在授时欺骗场景下的检测效果更佳。

综上所述，采用机器学习或深度学习方法进行卫星导航欺骗检测已成为当前的研究热点，其中特征参数的选取与处理方法对欺骗检测性能有直接影响。为进一步提升欺骗检测性能，本文从充分利用导航跟踪环路信息出发，将接收机跟踪环路输出的直接信息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，间接信息包括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。进一步地，采用滑动窗口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3个信号处理功能模块组成^[21]。当不存在欺骗时,接收机收到的信号中包括卫星信号和高斯白噪声,表示为:

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

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, 且有:

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

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、码相位和多普勒频移等信息, 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。

当信号进入跟踪环路后, 经混频器被分为同相(in-phase, I)支路和正交(quadrature-phase, Q)支路, I支路与Q支路输出结果分别为:

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

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

经过低通滤波器得到同相分量和正交分量, 分别为:

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

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

利用环路鉴别器处理同相分量和正交分量, 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数控振荡器(numerical controlled oscillator, 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, 假定在相干积分累积时间内未发生数据位跳变, 且码相位与多普勒频移的

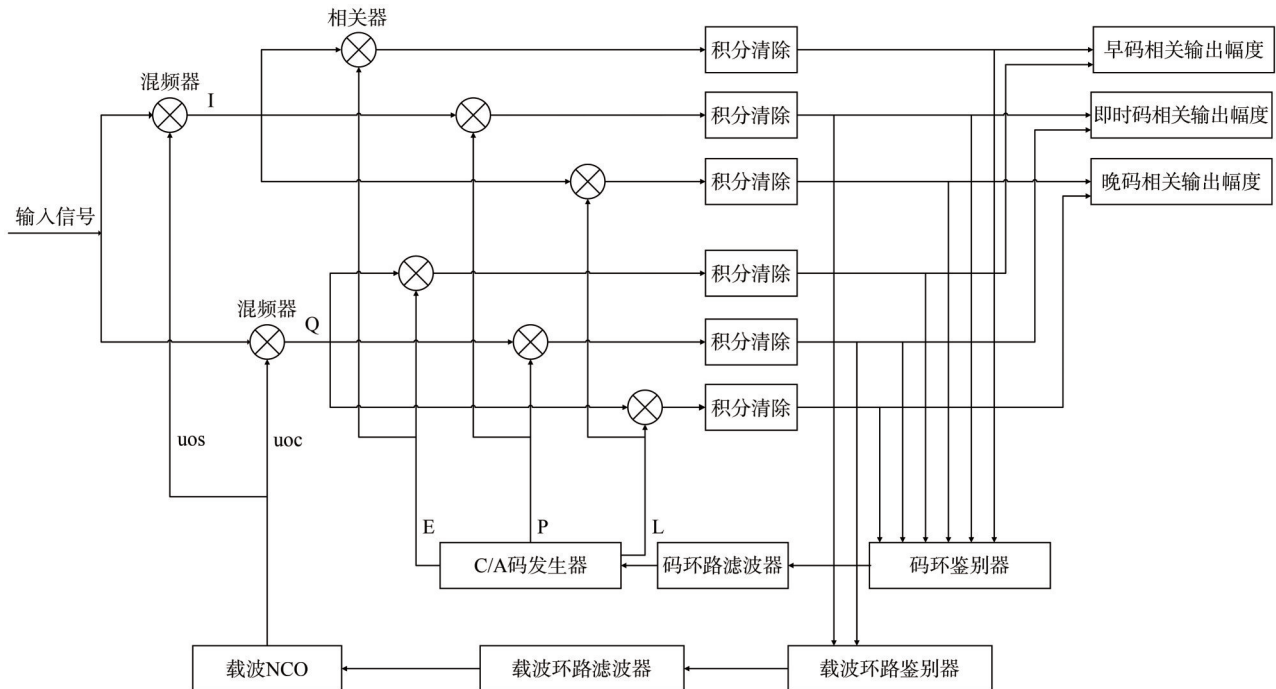


图1 跟踪环路结构

影响彼此独立^[4]，则相干积分输出分别为：

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

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

其中， I_p 、 Q_p 分别为同相相关器、正交相关器的输出； N_I 、 N_Q 分别为同相支路、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，接收机收到的信号中包含真实信号、欺骗信号和高斯白噪声^[22]，表示为：

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

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、载噪比和载波多普勒频移等。载波环输出的同相分量和正交分量分别为：

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

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

I支路和Q支路相关器输出分别为：

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

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

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，当欺骗信号与真实信号的码相位差减小至一个码片内时，欺骗信号使 $R(\tau)$ 的结果发生畸变^[3]。

1.3 欺骗检测特征参数选择

导航欺骗检测问题本质上属于分类问题，其中特征参数的选择与配置对欺骗检测性能具有显著影响。结合1.2节的分析结果可知，欺骗信号的注入会引起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信息发生变化。因此，有必要将这些跟踪环路输出的直接信息作为分类的特征参数。

同时，SQM作为检测GNSS多径信号和欺骗信号中常用的检测量，能够直观反映欺骗信号对跟踪环路相关峰的影响。通过处理跟踪环路相关器的早码、晚码和即时码输出，可得到各类SQM检测量。本文在不失一般性的前提下，选取Ratio、Delta、ELP和PCS共4类基础SQM检测量作为后续机器学习的特征参数。4类检测量分别表示为：

$$\text{Ratio} = \frac{E_1 + L_1}{2P_1} \quad (18)$$

$$\text{Delta} = \frac{E_1 - L_1}{2P_1} \quad (19)$$

$$\text{ELP} = \arctan\left(\frac{Q_E}{E_1}\right) - \arctan\left(\frac{Q_L}{L_1}\right) \quad (20)$$

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

其中， E_1 、 L_1 和 P_1 分别为同相相关器早码、晚码和即时码的输出； Q_E 和 Q_L 分别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。

综上所述，为充分利用基带信号处理信息，本文将跟踪环路输出的直接信息（如载波相位、码相位、载噪比和载波多普勒频移等）与SQM检测量共同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在处理长序列数据时易出现的梯度爆炸和梯度消失问题^[23]。LSTM采用非线性结构，具备优异的长序列数据处理能力。通过引入3个门控单元（输入门、遗忘门和输出门），LSTM能够选择性地保留或丢弃信息，并在信息传递过程中有效控制梯度的流动^[24]。由于欺骗行为对特征参数的影响具有时间相关性，即欺骗检测问题中的检测量表现为时间相关的长序列数据，因此本文选择LSTM模型用于卫星导航欺骗检测。LSTM单元结构如图2所示。

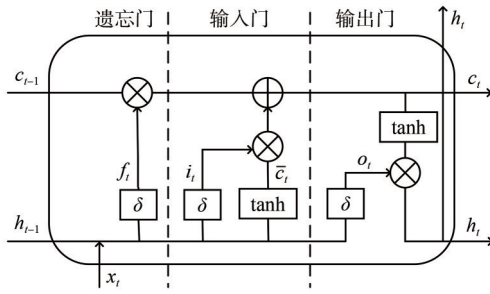


图2 LSTM单元结构

各状态更新计算式分别为：

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

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

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

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

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

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

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 分别为 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，本文构建了LSTM分类模型，该模型包括输入层、LSTM层、Dropout层、全连接层和输出层，整体结构如图3所示。

为提升模型的鲁棒性和泛化能力，本文在

LSTM层之后增加Dropout层。模型输入为预处理后的三维数据，输出为分类结果，其中，无欺骗记为0，有欺骗记为1。

2.2 数据滑动窗口预处理

数据预处理有助于提升数据质量，并减少噪声干扰。为提高模型的稳定性，并确保特征数据的均衡性，对原始数据进行标准化预处理，表示为：

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

其中， z 为原始数据特征值， μ 为特征均值， σ 为特征标准差， $\hat{z}$ 为标准化处理后的输出。为有效提取局部特征并保留全局趋势信息，结合时序数据的时间相关性和高维度特性，采用加窗技术将长时间序列分割为固定长度的子序列，并通过设定步长进行滑动处理，假定时间序列数据为：

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

设 w 为窗口长度， n 为步长，数据滑动窗口处理示意如图4所示。数据滑动窗口生成的子序列为：

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

其中， $i=1, n+1, 2n+1, \dots, (k-1)n+1$ ； k 为正整数。为适应导航数据的特性，本文将窗口长度设定为100、步长为1，滑动窗口生成的子序列作为LSTM的输入。每个输入序列包含当前时间点及其前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。滑动窗口处理方式能够有效捕捉并记忆整个时间窗口内的信息，常与LSTM模型联合使用，提升对时序特征的建模能力。

综上所述，基于LSTM分类算法的GNSS欺骗

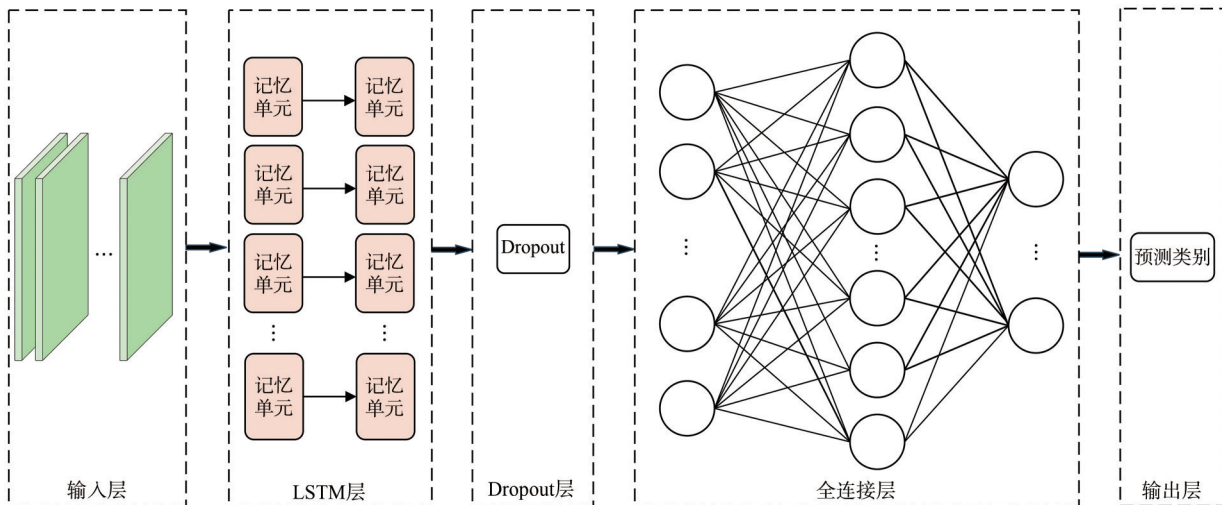


图3 LSTM分类模型

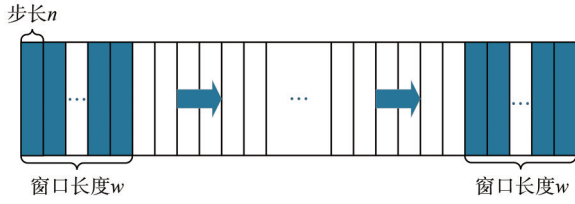


图4 数据滑动窗口处理示意

干扰检测流程如图5所示。

2.3 算法性能评估指标

基于多个指标评估检测性能，包括准确率、召回率、精确率和F1值。其中，准确率表示被正确预测的样本数占总样本数的比例。召回率表示实际属于某一类别的样本中，被成功预测为该类别的比例。精确率表示被预测为某一类别的样本中，实际属于该类别的比例。F1值为精确率和召回率的调和平均数，用于平衡精确率和召回率之间的关系。在多分类模型中，类别*i*的准确率、召回率、精确率和F1值分别为：

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

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

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

$$F1_i = \frac{2 \times \text{Precision}_i \times \text{Recall}_i}{\text{Precision}_i + \text{Recall}_i} \quad (34)$$

其中， Accuracy_i 为类别*i*的准确率， Recall_i 为召回率， Precision_i 为精确率。实际类别为*i*且被正确预测的样本数记为 TP_i ；实际类别非*i*但被预测为*i*的

样本数记为 FP_i ；实际类别非*i*且被正确预测的样本数记为 TN_i ；实际类别为*i*但被预测为非*i*的样本数记为 FN_i 。模型的整体性能通过各类别指标的均值进行评价，对每个类别分别计算准确率、召回率、精确率和F1值，然后取各项指标的平均值作为衡量模型整体性能的标准。

3 实验验证

本文实验的编程语言为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

本文实验所用数据集为美国得克萨斯大学奥斯汀分校无线电导航实验室公开发布的TEXBAT数据集。该数据集是当前研究GNSS欺骗检测的经典实验数据，包含8组欺骗场景和2组干净场景的真实采样数据，欺骗场景下TEXBAT数据集的主要参数设置见表1^[25]。

由于ds5~ds6为动态场景，多径干扰较严重，不利于实验结果对比，因此选择ds2、ds3、ds4和ds7数据集开展实验。为有效对比与评估实验结果，统一选取各数据集中同一颗卫星（PRN3）进行分析。

(1) 单检测量欺骗检测数据集

通过软件接收机对ds2、ds3、ds4和ds7数据集进行处理，分别计算PCS检测量，构建4类独立数据集。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。为保证训练集和测试集在类别分布上的均衡性，同

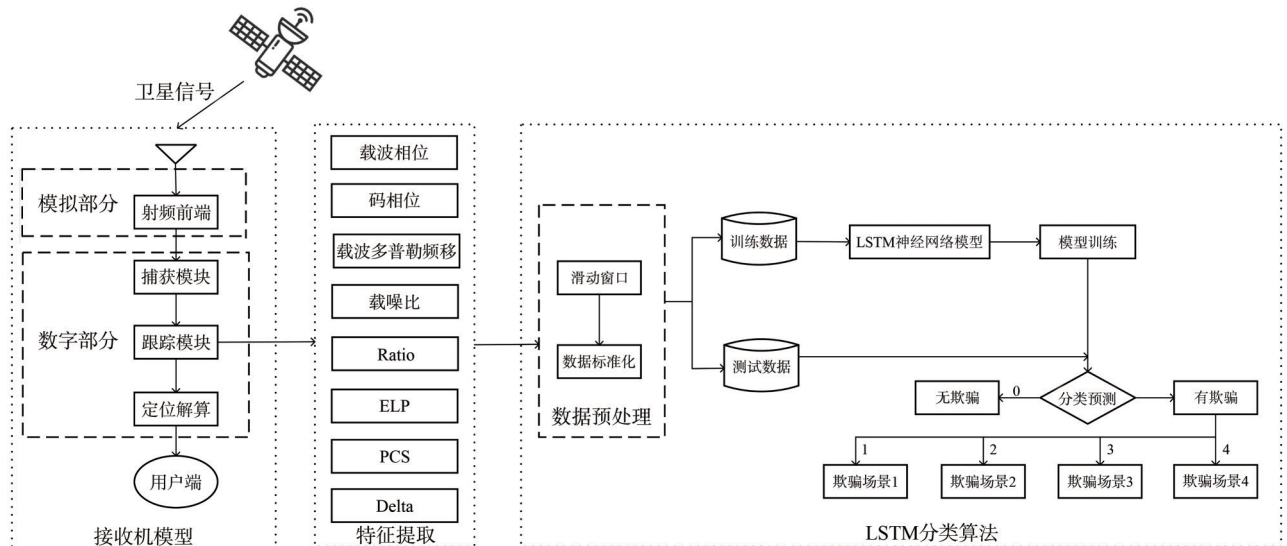


图5 基于LSTM分类算法的GNSS欺骗干扰检测流程

表1 TEXBAT数据集的主要参数设置

数据集	欺骗场景描述	欺骗种类	功率优势/dB	频锁状态	欺骗注入时间/s
ds1	静态瞬时跳变	N/A	N/A	失锁	100
ds2	静态大功率	时间	10.0	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

时兼顾数据的时序性,按照数据标签顺序划分数据集,训练集与测试集比例分别为80%与20%。单检测测量欺骗检测数据集如图6所示。



图6 单检测测量欺骗检测数据集

(2) 多检测测量欺骗检测数据集

针对ds2、ds3、ds4和ds7数据集进行独立处理,得到跟踪环路输出的载噪比、载波相位、码相位等直接特征,同时基于相关器输出构建PCS、Ratio、ELP等SQM检测测量作为间接特征。直接特征与间接特征共同构成多检测测量,数据集处理时段均选取0~450 s,特征输出间隔为10 ms,每个数据集包含45 000组数据,实验数据集由ds2、ds3、ds4和ds7数据集组成,共180 000组数据。训练集与测试集占比分别为80%与20%,多检测测量欺骗检测数据集如图7所示。

(3) 欺骗场景识别数据集

对clean、ds2、ds3、ds4和ds7数据集分别进

行处理,提取多检测测量特征。分别选取clean的0~450 s、ds2的100~300 s、ds3的100~300 s、ds4的100~300 s和ds7的110~310 s时段数据,共计125 000组。训练集与测试集占比分别为80%与20%,欺骗场景识别数据集如图8所示。

本文利用试错法^[26]确定LSTM模型超参数,以得到较优的结果,参数设置见表2。

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 欺骗检测实验

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

3.2.1 单检测测量欺骗检测

以PCS检测测量为研究对象,对比分析单SQM欺骗检测测量在各数据集上的性能。分别计算clean、ds2、ds3、ds4和ds7数据集中PRN3的PCS检测测量,结果如图9所示。

如图9(b)所示,无欺骗clean数据集的PCS检测测量值表现平稳。当受欺骗信号注入影响跟踪环路后,ds2的PCS检测测量在110 s处出现突变,相较于理论注入时刻(100 s)延迟10 s。相比之下,ds3和ds4的PCS检测测量分别在120 s和170 s发生明显突变,相较于理论欺骗注入分别延迟20 s和70 s。而ds7的PCS检测测量未出现明显波动。本文参考文献[27]的阈

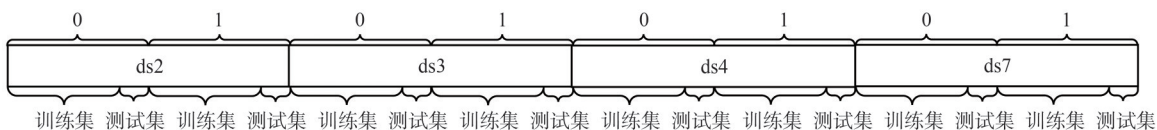


图7 多检测测量欺骗检测数据集

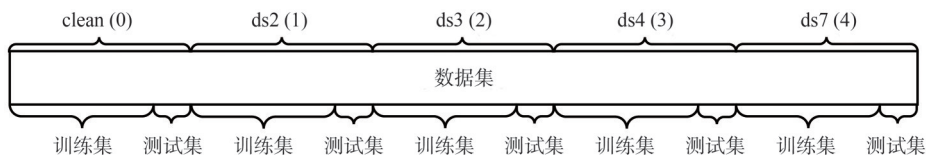


图8 欺骗场景识别数据集

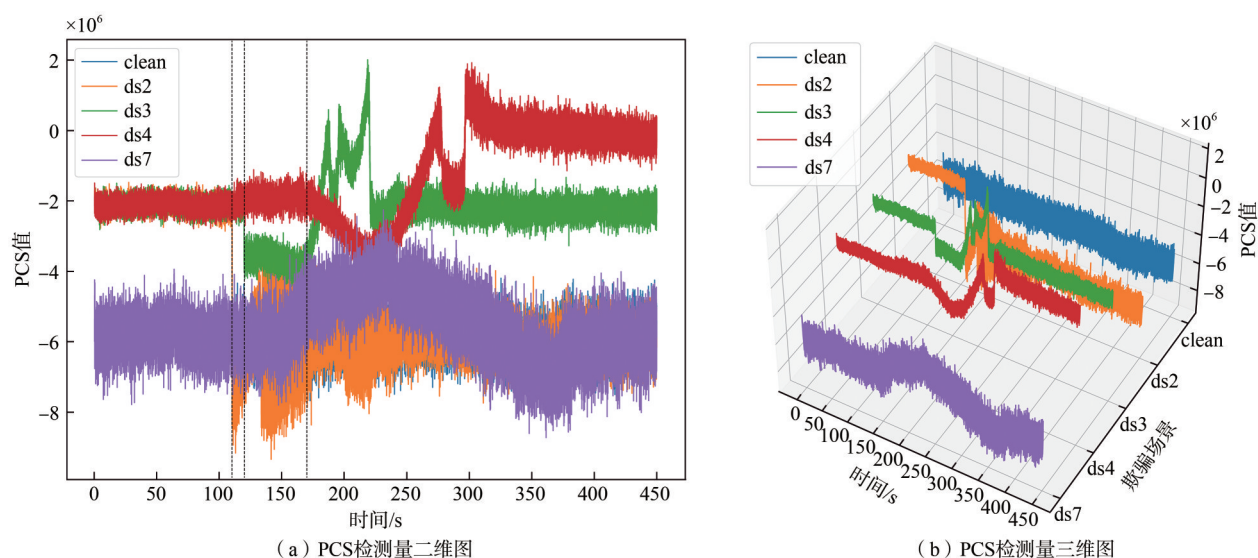


图9 不同场景下PCS检测量

值检测方法, 设置虚警率为10%, 检测概率变化如图10(a)所示。进一步地, 采用二元判决准则进行判断, 当检测概率大于50%时, 判定为存在欺骗干扰, 输出1; 当检测概率小于50%时, 判定为无欺骗干扰, 输出0, 判决结果如图10(b)所示。

如图10(b)所示, 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110 s及之后稳定保持为1; ds3数据集在120~220 s区间内判决结果主要为1, 但存在部分判定为0的离散位置; ds4数据集在200 s之后的判决结果主要为1, 同样存在类似判定为0的离散位置; ds7的判决结果波动较大, 仅在180 s与370 s判定为1, 且正确判定为1的频次较低, 表现出较高的漏检率。综合分析表明, 阈值检测法仅对ds2数据集的欺骗检测具有较低的漏检率和较高的

准确率, 而对ds3、ds4和ds7等数据集的欺骗检测在适用性和实时性方面均表现不佳。

基于3.1节构建的PCS单检测量欺骗检测数据集, 将有欺骗标记为1, 无欺骗标记为0, 本文采用KNN模型与LSTM模型进行训练和分类。不同数据集的LSTM模型测试集混淆矩阵如图11所示。

接下来, 分别计算阈值检测法、KNN分类法和LSTM方法的准确率, 结果见表3。由表3可见, 与文献[27]的阈值检测法和文献[5]的KNN分类法相比, 本文采用保持时序特征的PCS作为单特征检测量时, LSTM方法展现出更高的检测准确率。这一结果表明, 本文方法能够有效利用检测量的时序特性来提升检测性能。

在表3中, 3种方法在不同数据集上的检测性能存在明显差异。通过分析欺骗场景可知, ds2数

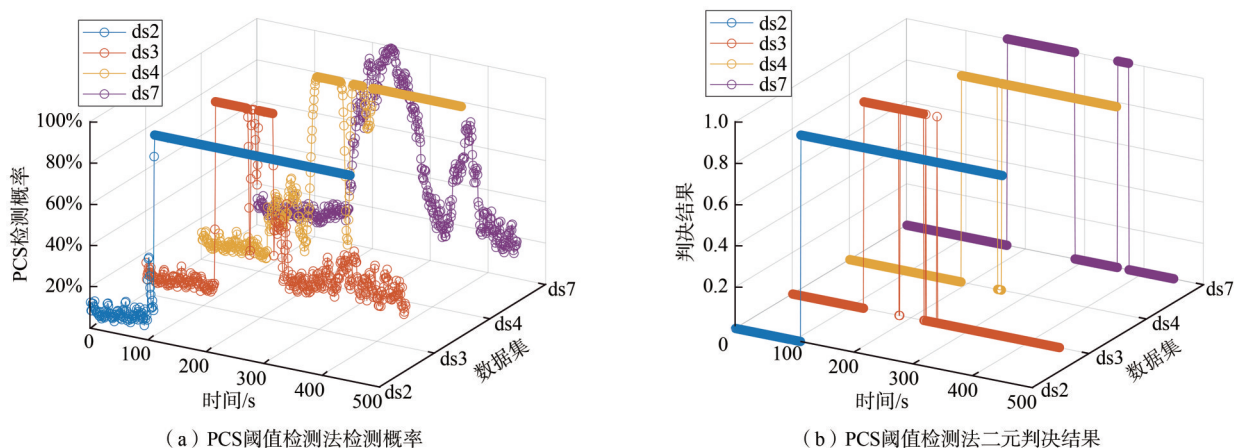


图10 不同场景下PCS阈值检测结果

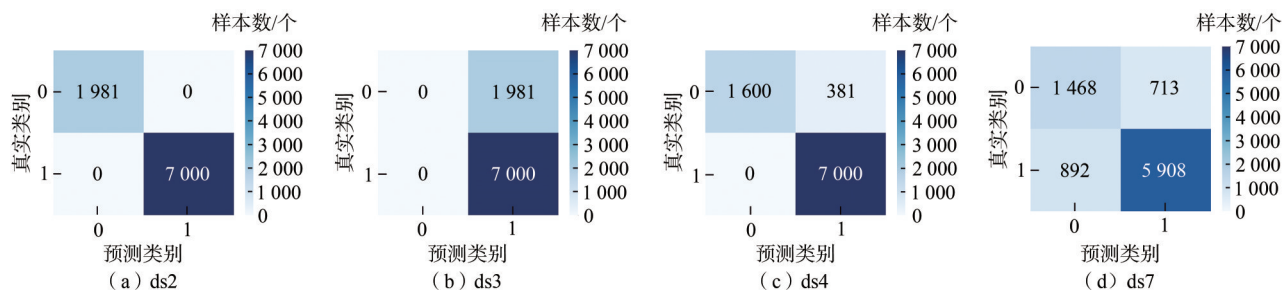


图11 不同数据集的LSTM模型测试集混淆矩阵

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%

据集采用大功率时间欺骗方式，欺骗注入时特征参数变化显著，因此较易检测到欺骗且检测准确率高。相比之下，ds3数据集采用小功率时间欺骗方式，ds4数据集为小功率地点欺骗，而ds7数据集的欺骗信号具有频率动态特性，这些特性使基于单检测量的方法难以准确识别欺骗，从而影响检测性能。此外，单一SQM检测量对于不同数据集的欺骗检测可能存在普适性不足的问题，为此本文进一步开展了多检测量实验研究。

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，将有欺骗标记为1，无欺骗标记为0，本文采用LSTM模型进行训练和分类。对测试集进行分类，得到的LSTM模型混淆矩阵如图12所示。

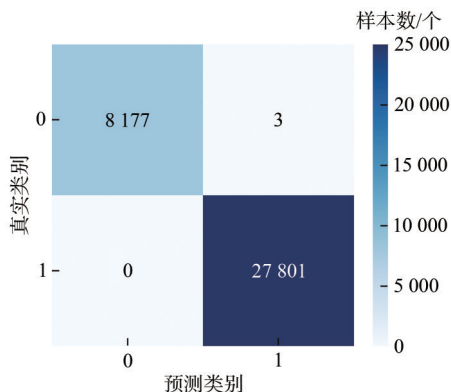


图12 LSTM模型混淆矩阵

在图12中，欺骗检测的正确分类数量显著高于错误分类数量。与使用单检测量特征相比，综合

多个检测量进行欺骗检测时，模型的分类准确率有显著提升。基于多检测量数据集训练LSTM模型后，分别对ds2、ds3、ds4和ds7数据集进行欺骗检测，结果如图13所示。

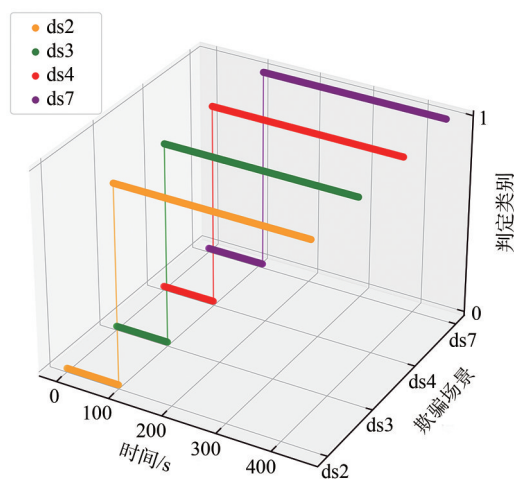


图13 不同场景下LSTM模型的检测结果

通过分析图13中4个数据集的欺骗检测结果可知，基于多检测量的LSTM模型检测到的欺骗时刻与表1中标注的欺骗开始时间基本一致，这表明本文方法具有良好的普适性和即时性。

表4总结了近期基于多检测量的欺骗检测相关研究成果，重点列出了特征参数、检测算法及其准确率等性能指标。

由表4可知，Sun等^[18]提出的PCA-CNN-LSTM方法通过融合多源数据实现99.49%的准确率，由于需要处理多传感器数据及相对复杂的算法，因此其计算资源要求较高。倪淑燕等^[12]以多个相关器的输出为检测量进行SVM检测，检测准确率达97.80%，但在不同欺骗场景下，性能存在一定差异性。Pervysheva等^[14]利用多接收机输出的位置、时钟及信号质量等参数构建RF模型，准确率为98.00%，但对多接收机协同工作和同步精度要求

表4 基于多检测量的欺骗检测方法

方法	特征参数	检测算法	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	97.80%
Pervysheva等 ^[14]	多接收机的位置、时钟信息及信号质量	RF	98.00%
Qi等 ^[19]	位移结果、运动状态特征	LSTM	97.60%
本文方法	跟踪环路信息	LSTM	99.99%

较高。Qi等^[19]以位移和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97.60%的检测准确率，但难以应对复杂轨迹欺骗。相比之下，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，且在多个数据集上均表现出良好的检测性能。相较于传统SVM方法^[12]，本文方法的欺骗检测准确率提高了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，若能识别欺骗攻击方式，将有助于制定更具针对性的防御策略。鉴于多检测量的LSTM模型表现出良好的检测性能，本文进一步验证其对不同欺骗场景的区分能力。

与二元分类的欺骗检测不同，欺骗场景识别本质上多元分类问题。需要说明的是，本节研究的欺骗场景对应ds2、ds3、ds4和ds7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场景；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ds7数据集的欺骗方式更复杂，牵引策略为载波同步。由于这4类数据集的欺骗策略存在差异性，因此可定义为4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模型进行训练和测试。训练集与测试集的损失值与准确率变化曲线如图14所示。

由图14(a)可以看出，随着迭代次数的增加，测试集的损失值呈下降趋势，且逐渐接近训练集的损失值，这表明模型未出现欠拟合现象。同时，测试集和训练集的损失值最终趋于收敛，相邻迭代次数的损失值差异小于0.05，说明模型也未出现过拟合现象。由图14(b)可以看出，模型的准确率在训练过程中逐渐收敛，最终稳定在99%左右。此外，在模型收敛后，本文计算得到模型的混淆矩阵，结果如图15所示。

由图15可以看出，LSTM多分类模型的误分类样本数量较少，且在不同类别上的分类表现较均衡。混淆矩阵计算结果显示，模型的平均准确率为99.98%，表明LSTM模型能够有效识别欺骗场景。为对比不同模型的性能，本文采用相同的训练集和测试集，分别对SVM、DT和KNN进行训练与评估。需要说明的是，为确保机器学习模型的最佳检测性能，本文基于网格搜索法^[26]确定超参数，具体见表5。

经过训练和测试后，得到各模型的多分类评价指标的均值，结果见表6。

由表6可以看出，采用RBF核函数的SVM模型分类准确率为89.01%，在对比机器学习模型中

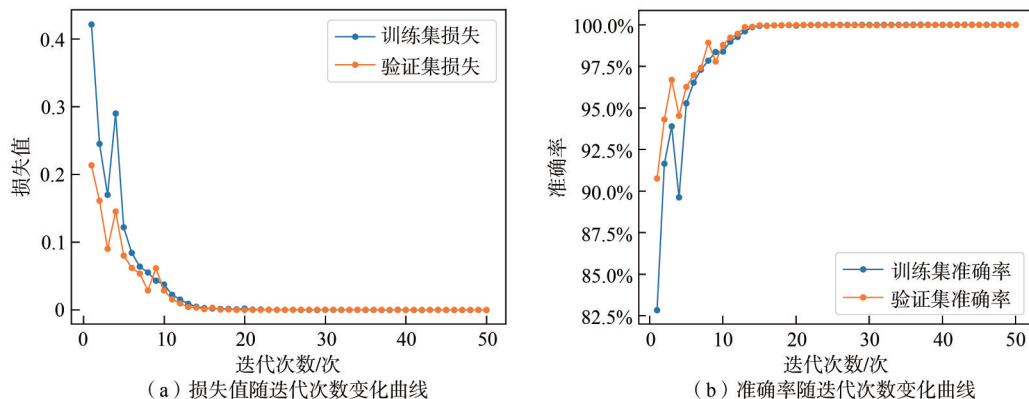


图14 损失值与准确率变化曲线

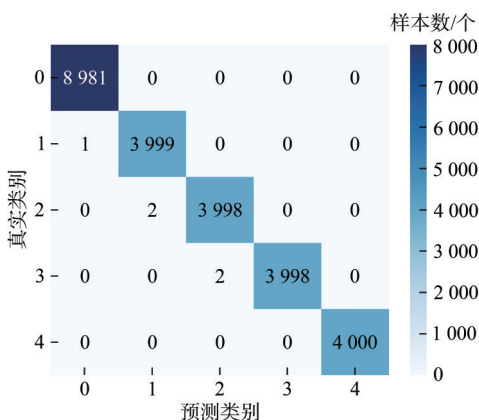


图 15 LSTM 多分类模型混淆矩阵

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%	89.10%	88.64%
KNN	85.43%	84.85%	85.36%	85.05%
DT	74.82%	72.01%	74.90%	72.73%
LSTM	99.98%	99.97%	99.97%	99.97%

表现最佳。与 SVM 模型相比，LSTM 模型在 4 项评价指标上均表现更佳。

实验结果表明，由于 GNSS 欺骗检测量具有时间相关性，基于 LSTM 模型能够有效解决 GNSS 欺骗检测和场景分类问题。

4 结束语

本文基于欺骗干扰对 GNSS 接收机基带跟踪环路影响的研究，通过分析 SQM 检测量在欺骗注入时的变化特征，成功解决了 LSTM 应用于欺骗检测与场景识别中的特征提取和时序数据处理问题。理论分析与实验结果表明，LSTM 算法不仅适用于欺骗检测，还能有效实现欺骗场景分类，主要研究成果如下。

(1) 在欺骗检测方面，采用保留时序特征的单一检测量时，LSTM 方法的检测准确率高于传统阈

值法和 KNN 分类法。综合利用保留时序特征的多检测量后，LSTM 方法的欺骗检测准确率进一步提升，并表现出更好的普适性。

(2) 在场景识别方面，基于保留时序特征的检测量进行多种欺骗场景识别，准确率达 99.98%。与传统机器学习方法相比，在准确率、召回率、精确率和 F1 值等各项指标上均表现更佳。

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(4): 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. Overview of GNSS spoofing jamming 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(2): 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(4): 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, 陈世淼, 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(5): 812-820.
NI S Y, CHEN S M, FU Q W, et al. Review on spoofing detection and mitigation of satellite navigation[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. Overview of 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] CHEN Z K, LI J Z, LI J, 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(5): 153-161.
ZHOU Y, WANG S L, YANG W, et al. Deceptive jamming detection of satellite navigation based on PSO-ELM[J]. Navigation Positioning and Timing, 2022, 9(5): 153-161.

[10] GHANBARZADE A, SOLEIMANI H. GNSS/GPS spoofing and jamming identification using machine learning and deep learning[EB]. arXiv

- preprint, 2025, arXiv: 2501.02352.
- [11] LI J Z, LI W Q, HE S F, et al. Research on detection of spoofing signal with small delay based on KNN[C]//Proceedings of the 2020 IEEE 3rd International Conference on Electronics Technology (ICET). Piscataway: IEEE Press, 2020: 625-629.
 - [12] 倪淑燕, 付琦玮, 陈世淼, 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(2): 24-31.
NI S Y, FU Q W, CHEN S M, et al. GNSS spoofing jamming multi-correlator detection method based on support vector machine[J]. Electronic Information Warfare Technology, 2025, 40(2): 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]. IEEE Access, 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]//Proceedings of the 2024 32nd Telecommunications Forum (TELFOR). Piscataway: IEEE Press, 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]//Proceedings of the 2020 25th International Computer Conference, Computer Society of Iran (CSICC). Piscataway: IEEE Press, 2020: 1-5.
 - [16] JAYAWEERA M. A novel deep learning GPS anti-spoofing system with DOA time-series estimation[C]//Proceedings of the 2021 IEEE Global Communications Conference (GLOBECOM). Piscataway: IEEE Press, 2021: 1-6.
 - [17] BORHANI-DARIAN P, LI H Q, WU P, et al. Detecting GNSS spoofing using deep learning[J]. EURASIP Journal on Advances in Signal Processing, 2024(1): 1-19.
 - [18] SUN Y C, YU M X, WANG L Y, et al. 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, 106(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(4): 86-91.
SHENG M G, SHENG S Y, DENG M, et al. The time spoofing detection method based on long short-term memory network[J]. GNSS World of China, 2024, 49(4): 86-91.
 - [21] 谢钢. GPS原理与接收机设计[M]. 北京: 电子工业出版社, 2017.
XIE G. GPS principles and receiver design[M]. Beijing: Publishing House of Electronics Industry, 2017.
 - [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(8): 2254-2262.
WANG W Y, GONG J, WANG J M. GNSS spoofing interference detection based on variance of SCB[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: 现状及展望[J]. 智能科学与技术学报, 2023, 5(2): 180-199.
HUANG J, TIAN Y L, DAI X Y, et al. Deep learning-based multi-modal trajectory prediction methods for autonomous driving: state of the art and perspectives[J]. Chinese 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(4): 456-465.
XU B W, BI J, YUAN H T, et al. Dynamic water quality warning with seasonal decomposition and long short-term memory network[J]. Chinese Journal of Intelligent Science and Technology, 2021, 3(4): 456-465.
 - [25] HUMPHREYS T, BHATTI J, SHEPARD D, et al. The Texas spoofing test battery: toward a standard for evaluating GPS signal authentication techniques[C]//Proceedings of the 25th International Technical Meeting of the Satellite Division of the Institute of Navigation. Piscataway: IEEE Press, 2012: 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(6): 122-135.
WANG L Y, SUN Y C, YU M X, et al. UAV GPS spoofing 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(3): 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, 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。



覃业梅 (1979-), 女, 博士, 湖南工商大学智能工程与智能制造学院教授, 主要研究方向为时间序列信号分析与预测。



廖一韪 (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, 湖南工商大学智能工程与智能制造学院讲师, 主要研究方向为中红外激光、光电信号检测及处理。