文章编号:1671-4598(2025)03-0054-09 DOI:10.16526/j.cnki.11-4762/tp.2025.03.007 中图分类号:TP355.1 文献标识码:A

基于改进 BiLSTM 的 ADS-B 信号欺骗检测方法研究

颜丽蓉，赵泽荣
（中国民用航空飞行学院，四川 广汉 618300）

摘要：随着智能交通系统的快速发展，ADS-B 技术作为一种先进的空中交通管理监控手段得到了广泛应用；然而，ADS-B 信号的开放性和易受攻击性使其成为潜在的欺骗攻击目标；为提升飞行安全并防止 ADS-B 系统遭受欺骗干扰，提出了一种基于深度学习的全向信标信号处理方法，用于检测 ADS-B 信号中的欺骗行为；该方法利用全向信标收集 ADS-B 信号数据并提取相关特征，随后通过 BiLSTM 深度学习模型对特征进行训练，实现在正常信号与欺骗信号之间的有效区分；结合焦点损失函数和贝叶斯优化算法对信号检测方法进行优化，并通过几何位置相关函数量化飞行状态误差；结果表明，模型的训练损失值和训练准确率分别达到了 0.25 和 98.15%，改进后的 BiLSTM 模型在分类性能上所有指标均超过了 99.50%；此外，研究方法在飞行速度、水平飞行方向和垂直飞行方向的检测误差分别仅为 0.01%、0.01%和 0.04%；对真实信号的检测显示，其飞行速度、水平和垂直方向的损失值均为 1，而欺骗信号在这些指标上的损失值误差分别为 15%、1%和 0.3%；综上所述，面向全向信标信号处理的深度学习 ADS-B 信号欺骗检测方法研究，有效实现了优异的检测准确率和鲁棒性，为民用航空安全领域提供了重要的技术支持与参考。

关键词：全向信标；ADS.B；信号欺骗检测；深度学习；BiLSTM

Study on Deception Detection Dethod for ADS-B Signals Based on Improved BiLSTM

YAN Lirong，ZHAO Zerong
（Civil Aviation Flight University of China，Guanghan 618300，China）

Abstract：With the rapid development of intelligent transportation systems，automatic dependent surveillance-broadcast (ADS-B) technology，as an advanced means of air traffic management and monitoring，is widely applied. However，the openness and vulnerability of ADS-B signals make it a potential target for deception attacks. In order to improve flight safety and prevent interference and deception，a deep learning based omnidirectional beacon signal processing method is proposed，which detects deception behavior in ADS-B signals. This method uses omnidirectional beacons to collect ADS-B signals and extract relevant features，and then trains the features through a bidirectional long short-term memory (BiLSTM) deep learning model to effectively distinguish between normal signals and deceptive signals. Optimize signal detection method by combining focus loss function and Bayesian optimization algorithm，and quantify flight state error through geometric position correlation function. The results show that the loss value and accuracy of the model training reach up to 0. 25 and 98. 15%，respectively. all indicators of the improved BiLSTM model are over 99.50% in the classification performance. In addition，the detection errors of the research method in flight speed，horizontal flight direction，and vertical flight direction are only 0.01%，0.01%，and 0.04%，respectively. The detection of real signals shows that the loss values of flight speed，horizontal and vertical directions are all 1，while the loss errors of deception signals on these indicators are 15%，1% and 0.3%，respectively. In summary，deep learning ADS-B signal deception detection methods for omnidirectional beacon signal processing effectively achieve high-quality detection accuracy and robustness，providing important technical support and reference for civil aviation safety.

Keywords：omnidirectional beacon；ADS-B；signal deception detection；deep learning；BiLSTM

收稿日期:2024-10-31； **修回日期**:2024-12-13。
基金项目:民航安全能力 SA 项目(ASSA2024/101);中央高效基本科研业务费专项资金资助项目(24CAFUC03071)。
作者简介:颜丽蓉(1976-),女,大学本科,工程师。
引用格式:颜丽蓉,赵泽荣.基于改进 BiLSTM 的 ADS-B 信号欺骗检测方法研究[J].计算机测量与控制,2025,33(3):54-62.

0　引言

随着社会经济的发展，越来越多的人选择乘坐飞机出行，客运流量和航班数量的增加对航空业的通信、监视和导航等技术提出了更高的要求[1]。自动相关监视-广播（ADS-B，automatic dependent surveillance-broadcast）作为现代航空交通管理的重要组成部分，通过实时广播飞机的位置、速度和高度等信息，显著提升了空中交通的安全性和效率[2]。此外，飞机的 ADS-B 系统可以实现飞机与飞机之间的信息互通，能够让飞行人员和空中管理人员采取相应地应对措施，从而可以避免某些人为管理失误造成的紧急冲突或其他一些不可抗拒因素导致的飞行计划冲突。近年来，随着中国民用航空事业的快速发展，空域内飞行器的数量大幅增加，导致飞行情况愈加复杂[3]。然而，ADS-B 技术存在信号无身份验证、信号未加密以及使用开放式广播等固有缺陷[4]。此外，ADS-B 系统的开放性使其容易受到各种欺骗攻击。其中，ADS-B 虚假欺骗攻击是一种典型的虚假欺骗攻击技术，其攻击原理是攻击者按照规定协议向空中数据链路发送与真实飞机 ADS-B 信号形式相似的虚假 ADS-B 信号，致使飞机控制员与地面监管人员将该虚假信号误认为是无人机真实信号。例如，文献[5] 学者的研究指出，依赖卫星定位技术的 ADS-B 和全球定位系统（GPS，global positioning system）可能成为欺骗攻击的目标。这类攻击的目的是通过向“受害者”的接收器插入错误信号，从而产生错误的定位或计时信息。攻击者可能试图插入虚假信息，以达到劫持或干扰空域监视安全的目的。此外，文献 [6] 等研究人员发现，在飞行员进行飞行状态估计的场景下，异步滤波器的设计特点可能会导致欺骗攻击和状态延迟等干扰信号的产生，进而影响飞行员的状态判断，可能会导致错误的航空决策，从而危及飞行安全。因此，开发一种有效的欺骗检测机制成为当前航空安全领域亟待解决的问题。近年来，深度学习作为一种强大的模式识别工具，已在多个领域取得显著成果。深度学习技术能够通过学习大量数据中的复杂特征来自动提取信息，具有较高的检测和分类能力。文献 [7] 等研究人员利用深度学习技术结合卡尔曼滤波器进行了欺骗干扰信号的检测，结果显示该方法的误报概率很低，证实了深度学习在信号欺骗检测中的高可行性。而文献 [8] 等研究人员也采用机器学习结合神经网络的方法进行了全球导航卫星系统（GNSS，global navigation satellite system）欺骗干扰检测，研究结果同样显示出可行性，验证了深度学习技术在该领域的有效性。因此，在这一背景下，研究创新性地利用深度学习技术结合全向信标信号处理，设计了一种面向全向信标信号处理的 ADS-B 信号欺骗检测方法。该方法采用双向长短期记忆网络（BiLSTM，bidirectional long short-term nemory）结构来进行时序信号处理，并结合飞行状态和飞行意图对欺骗信号进行判别，以期提高欺骗干扰信号的识别精度，为提升航空安全提供新的解决方案。

1　ADS-B 信号欺骗干扰原理

为了适应当前愈加复杂的空域环境，以实现更高效、安全的空中交通监视和管理，当前民用航空领域亟待解决 ADS-B 技术欺骗式干扰的局限。ADS-B 欺骗式干扰是指通过伪造或篡改飞机的位置、速度等关键信息，向其他飞机或地面基站广播虚假信息，从而干扰正常的空中交通管理的行为[9]。目前，欺骗式干扰主要有 3 种方式：删除真实信号、篡改真实信号以及注入虚假信号等[10]。其中删除真实信号的干扰方式通常是通过遮蔽、干扰或其他技术手段，阻止地面接收机接收真实的 ADS-B 信号。攻击者可以使接收机的信号接收失效，从而导致系统无法感知实际存在的飞行器信息。针对此攻击方式可以利用数据冗余和多站点接收的方法，来降低真实信号被删除的风险。篡改真实信号的干扰方式是通过拦截并修改原始 ADS-B 信号中的位置、速度等关键信息，将篡改后的信息重新广播，导致其他接收站获取到虚假的航迹数据。针对该攻击干扰方式，可以在接收端引入基于数据一致性的检测机制，通过比对历史轨迹与当前信息，来筛查出不符合正常轨迹特征的航迹点。注入虚假信号的干扰方式，一般是攻击者生成与真实 ADS-B 信号类似的广播信号，并向地面接收机或其他飞行器发送该虚假信息，制造不存在的虚假目标，从而干扰正常的空中交通管理针对此干扰方式可以引入基于信号物理特征的检测方法，分析信号到达时间、信号功率和调制特征等，来识别出不符合正常特征的信号源。这些干扰方式不仅威胁着空中交通管理的安全，还可能导致部分有效数据的丢失，给空中交通的安全性带来严重风险。信号欺骗干扰过程如图 1 所示。

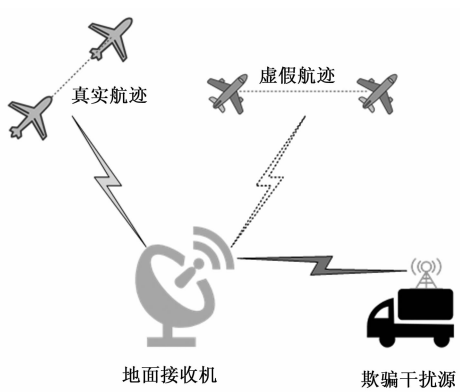


图 1　信号欺骗干扰过程

由图 1 所示，信号欺骗干扰过程中，欺骗干扰源会向地面接收机发送虚假的 ADS-B 信号，这些信号的报文格式和调制方式与真实信号相同，因此会使得地面接收机无法有效分辨，从而在交通管制系统的屏幕上显示出虚假的目标航迹。

2 ADS-B 信号欺骗检测方法

基于 ADS-B 技术的空中交通监视和管理系统中，接收到的信号包含了多种飞机的实时信息，主要涵盖了八种关键信息类型。这些信号的全面信息流使得空中交通管制中心能够有效追踪飞机位置、监控飞行状况，并管理空域安全。其中飞机的身份标识（Identification，ID）信息十分重要，是每架飞机独立的身份标识，主要是指飞机的航班号、注册码等。飞机 ID 信息可以识别特定飞机的基本数据，是空中交通管理的首要参数。而 ADS-B 系统能够获取飞机的实时空中坐标信息，包括了经度、纬度及高度等。该信息在空中交通监视和管理中至关重要，可以用于确定飞机在空中的精确位置，确保飞行路线的准确性和安全性。此外飞机的飞行状况信息里包含了飞机的姿态、航向及垂直速度等指标，可以反映飞机的当前飞行状态，例如是否处于上升、下降或平飞状态。这类信息可以帮助空中交通管制员快速判断飞机的飞行意图和状况变化。对于停留在地面的飞机，系统还会接收其地理位置信息。地面位置信息可以帮助机场地面管理人员跟踪停场飞机的位置，优化停机位和地面交通的管理。此外，ADS-B 系统还提供了飞机对地速度数据信息，这是通过地面雷达或机载传感器检测到的飞机飞行速度信息，该信息可以判断飞机运动特征和预测飞行轨迹。

此外 ADS-B 系统还包含了飞机运行状况信息、扩展间歇飞机身份信息和测试信息。飞机运行状况信息主要包括引擎状态、系统运行情况等，能够反映飞机的技术状况和运营状态，对于故障预警和突发情况处理有着关键作用。而扩展间歇飞机身份信息中包含着扩展的识别信息，以增强飞机身份的唯一性和安全性。例如，特定航线、飞行模式等信息便属于扩展间歇飞机身份信息，有助于更加细化地管理飞机信息。最后测试信息主要用于系统的自检与维护，包括信号测试、系统更新等内容，以确保 ADS-B 系统的稳定性和精确性。在针对虚假信号或真实信号的判别中，研究主要利用空中位置信息、飞行速度信息和飞行状况信息来综合考虑飞机的飞行基本情况和飞行意图，来更精确地进行欺骗信号的判别。地面接收机接收到的信号如式（1）所示。

$$s(t)=\sqrt{P}D(t)e^{j(\varphi+2\pi f_\theta t)}+a(t) \tag{1}$$

式（1）中，$s(t)$ 表示在 t 时刻接收到的信号，P 表示信号功率，a 表示高斯白噪声，D 表示基带信号，e 表示自然对数的底数，f_θ 表示载波频率，φ 表示初相位[11]。为了有效识别出真实信号和欺骗信号，研究引入了深度学习技术进行欺骗检测。深度学习是机器学习中的一类特殊方法，常用的网络结构包括了卷积神经网络（CNN，convolutional neural network）、递归神经网络（RNN，recursive neural network）和生成对抗网络（GAN，generative adversarial networks）这 3 种网络结构[12]。而长短期记忆（LSTM，long short-term memory）网络作为一种特殊变形的 RNN，可以对具有时序特征的数据进行分析[13]。虽然 LSTM 的网络结构能够有效学习长期依赖的信息，但该结构在处理序列数据时可能存在梯度消失的问题[14]。基于此，研究采用了 BiLSTM 结构来提高检测的准确性。BiLSTM 是 LSTM 的一种扩展结构，该网络结构的双向特征能够充分考虑到序列的前后文信息，可以有效捕捉序列中的长期依赖关系[15]。因此，研究利用深度学习技术中的 BiLSTM 来进行 ADS-B 信号欺骗检测方法设计。基于 BiLSTM 的 ADS-B 信号欺骗检测如图 2 所示。

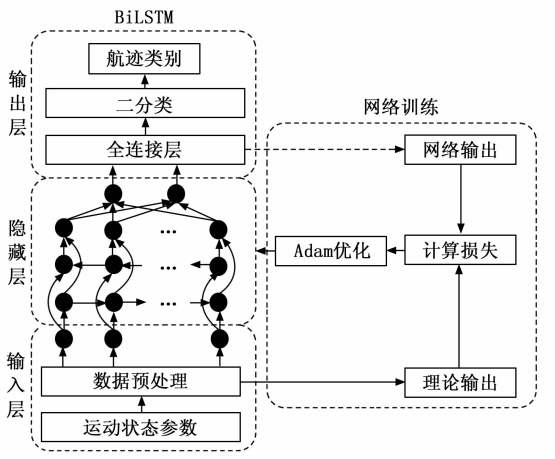


图 2 基于 BiLSTM 的 ADS-B 信号欺骗检测

由图 2 所示，基于 BiLSTM 的 ADS-B 信号欺骗检测方法基于的是 BiLSTM 的网络结构，主要分为输入层、隐藏层和输出层这三层结构。在该检测方法中，首先在输入层输入真实飞行器的运动状态参数，并对输入数据进行预处理等操作[16-17]。随后，数据进入 BiLSTM 的隐藏层进行训练，BiLSTM 的双向结构能够为输出层的每个节点提供完整的时序上下文信息。在经过训练后，提取出的 ADS-B 信号在时间上的变化特征将被输入到全连接层中，来进行真实航迹与虚假航迹的二分类处理，最终在输出层输出区分后的航迹类别[18]。此外，在隐藏层的训练过程中，研究采用了损失函数计算理论输出，并使用 Adam 优化算法进行优化，以实现更精确的分类效果。为了识别真实信号与虚假信号，研究聚焦于空中坐标信息、飞行速度信息和飞行状态信息等参数

来反映飞机的飞行基本情况和飞行意图，从而用于检测信号是否为欺骗信号。为了检测出真实航迹与虚假航迹，研究首先采集数据并制作出数据样本，接着从预处理后的信号中提取出关键特征数据，如空中坐标、飞行速度、飞行状态等。接着利用改进 BiLSTM 网络捕获信号在时间维度上的依赖关系，并通过反向传播算法优化网络参数，使得模型能够有效学习真实信号和欺骗信号之间的差异。最后利用焦点损失函数来度量预测结果与真实标签之间的差异，确保分类效果的精确度。此外，研究还采用 Adam 优化算法来调整网络的权重，以提高分类性能。

2.1　改进 BiLSTM 网络

2.1.1　引入焦点损失函数

研究的基于 BiLSTM 结构设计的信号欺骗检测方法能够有效实现 ADS-B 信号分类，为了能进一步提升检测精度和鲁棒性，研究针对分类过程中存在的难以区分样本以及误分类代价问题，利用焦点损失函数和贝叶斯优化算法来进行优化和改进。因为损失函数的作用是训练样本模型输出值与真实值之间的误差，然而在二分类问题中，传统损失函数的计算容易受到不稳定样本的影响，导致样本难以区分，从而会影响到真实信号与欺骗信号的分类精度[19]。为了解决这一问题，研究使用了焦点损失函数来替代传统损失函数。焦点损失函数是在交叉熵损失函数的基础上进行改进的，该函数通过引入调节参数和权重系数，具有解决样本不平衡、增加小数量目标类别权重以及强化分类错误样本权重等优点[20]。传统的交叉熵损失函数的表达式如式（2）所示：

$$CE(p,y)=\begin{cases}-\log(p), y=1\\ -\log(p), y=0\end{cases} \tag{2}$$

式（2）中，CE 表示传统的交叉熵损失函数，$y=1$ 表示稳定样本，$y=0$ 表示不稳定样本，p 表示模型预测样本为稳定样本的概率值。k 类样本正确预测的概率如式（3）所示：

$$p_t=\begin{cases}p, & y=1\\ 1-p, & y=0\end{cases} \tag{3}$$

式（3）中，p_k 表示 k 类样本正确预测的概率。由此可以得到预测 k 类样本的交叉熵损失函数，如式（4）所示：

$$CE(p,y)=CE(p_k)=-\log(p_k) \tag{4}$$

由式（4）可知，在飞行运动状态参数数据中，稳定样本的数量远远多于不稳定样本，导致绝大部分的损失值来自于稳定样本。这种情况下，稳定样本的总损失值在所有样本的总损失值中占据主要部分，导致模型更容易对稳定样本发生过拟合，无法有效关注不稳定样本所包含的信息，进而使得不稳定样本的误判率显著升高[21]。针对此问题，在代价敏感学习中解决样本不平衡的常用的方法是在交叉熵损失函数 CE 中引入误分类权重因子，对两类样本赋予不同的权重。权重系数的定义表达式如式（5）所示：

$$\alpha_k=\begin{cases}\alpha, & y=1\\ 1-\alpha, & y=0\end{cases} \tag{5}$$

式（5）中，α_k 表示权重系数，α 表示权重因子。含有权重因子的损失函数即被称为平衡焦点损失函数，平衡焦点损失函数的数学表达式如式（6）所示：

$$BCE(p_k)=-\alpha_k\log(p_k) \tag{6}$$

式（6）中，BCE 表示平衡焦点损失函数。平衡焦点损失函数仅是对交叉熵损失函数的简单扩展，在平衡焦点损失函数中，代表不同样本的权重系数平衡了稳定样本与不稳定样本的重要性，但未考虑重叠区域样本难分类的问题。非重叠区域样本是较为容易学习和分类的样本，故该区域样本的 p_k 值较大，损失值较小。虽然非重叠区域样本的损失值小，但此区域样本数量远大于重叠区域样本数量，故累加求和后此区域样本的加权损失值仍远大于重叠区域样本的加权损失值，导致重叠区域样本的信息被淹没，进而导致重叠区域样本无法被精准的分类。因此，仅依靠权重因子并不能解决上述问题。因此需要再加入调节参数来不断调节难易程度，当调节参数的值越大时，则表示差异程度越大。同时含有权重因子和调节系数的损失函数即被称为焦点损失函数，焦点损失函数的数学表达式如式（7）所示：

$$FL(p_k)=-\alpha_k(1-p_k)^{\gamma}\log(p_k) \tag{7}$$

式（7）中，FL 表示焦点损失函数，γ 表示调节参数。由式（7）可知，p_k 的值越接近 1，则交叉熵损失函数 FL 的值越小；反之则 FL 的值越大。当焦点损失函数 FL 中调节因子 γ 的值在 0 到 5 的取值范围内时，其具有动态调整样本损失值和平衡区域样本的权重特点。其中当某个样本被误分类时，其预测概率 p_k 较小，此时调节参数接近 1，使该样本的损失值几乎不受影响。而随着模型的迭代，模型会通过调整参数对该样本进行有效学习，使其 p_k 值逐渐增大。与此同时，调节参数会逐渐减小，导致该样本的损失值降低。通过这种动态变化，调节参数会自适应地调整梯度优化方向，促进模型在训练过程中更合理地分配注意力。此外，调节参数中的超参数会对非重叠区域样本的权重进行平滑调整，使模型更加关注重叠区域样本的学习。当调节参数取值为 0 时，焦点损失函数则退化为传统的交叉熵损失函数。调节参数的引入使得分类器能够更关注难分类样本，从而提高其分类精度。而权重系数的加入则有助于调节样本间的平衡度，从而可以避免影响易分类和难分类样本的损失计算[22]。

2.1.2　超参数调优

在引入焦点损失函数以提升 BiLSTM 结构在二分类任务中的表现后，为进一步降低误分类代价，研究采

用贝叶斯优化算法对模型进行进一步调整，以提高检测的准确性和稳定性。

贝叶斯优化算法是一种高效、灵活的黑盒优化算法，适用于非凸和高噪声问题[23]。在基于 BiLSTM 的 ADS-B 信号欺骗检测方法中，存在初始学习率、正则化系数、焦点损失函数引入的调节参数和权重系数等多个超参数。为了避免根据经验值设定超参数而导致性能欠佳，研究采用贝叶斯优化算法来进行超参数调优，以减少误分类的概率。基于贝叶斯改进的 BiLSTM 结构超参数调优流程如图 3 所示。

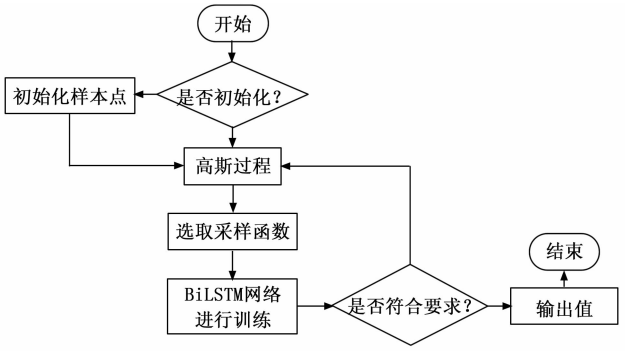


图 3 基于贝叶斯改进的 BiLSTM 结构超参数调优流程

由图 3 所示，在基于贝叶斯改进的 BiLSTM 结构超参数调优流程中，首先对 BiLSTM 网络模型进行初始化，如果尚未初始化则随机生成初始化的样本点。接着，利用模型训练的损失值进行高斯过程处理。然后，选取采样函数将新评估点输入 BiLSTM 网络进行训练，并得到训练后的输出值。在得到输出值后判断该输出值是否符合目标函数损失值的要求。如果符合，则输出该样本点及对应输出值并终止流程。如果不符合，则返回到高斯过程重新进行迭代。贝叶斯优化模型的数学表达式如式（8）所示：

$$P(f|D)=\frac{P(D|f)P(f)}{P(D)} \tag{8}$$

式（8）中，f 表示未知目标函数，D 表示参数和观测值的集合，$P(f|D)$ 表示未知目标函数的后验概率，$P(D|f)$ 表示未知目标函数的似然分布，$P(D)$ 表示边界是似然分布，$P(f)$ 表示先验概率[24]。贝叶斯优化目标如式（9）所示：

$$x_{\min}=\underset{x\in X}{\operatorname{argmin}} f(x) \tag{9}$$

式（9）中，$x_{\min}$ 表示优化后的超参数，$f(x)$ 表示优化前的目标函数。高斯分布过程如式（10）所示：

$$f(x_n)\sim GP(\mu(x_n),\boldsymbol{K}(x_n,x_n)) \tag{10}$$

式（10）中，$f(x_n)$ 表示超参数 x_n 的目标函数，n 表示超参数的数量，GP 表示高斯分布，$\mu(x_n)$ 表示 $f(x_n)$ 的数学期望，$\boldsymbol{K}$ 表示协方差矩阵[25]。协方差矩阵的数学表达式如式（11）所示：

$$\boldsymbol{K}=\begin{bmatrix} k(x_1,x_1) & (x_1,x_2) & \cdots & (x_1,x_n) \\ k(x_2,x_1) & k(x_2,x_2) & \cdots & k(x_2,x_n) \\ \cdots & \cdots & \cdots & \cdots \\ k(x_n,x_1) & k(x_n,x_2) & \cdots & k(x_n,x_n) \end{bmatrix} \tag{11}$$

由式（10）和（11）可得到联合高斯分布的表达式如式（12）所示：

$$\begin{bmatrix} f(x_n) \\ f(x_{n+1}) \end{bmatrix}\sim N\left(0,\begin{bmatrix} k & k \\ k^T & k(x_{n+1},x_{n+1}) \end{bmatrix}\right) \tag{12}$$

式（12）中，T 表示转置。由贝叶斯定量即可得到 $f(x_{n+1})$ 的后验概率如式（13）所示：

$$P(f(x_{n+1})\mid D_{n,x_{n+1}})=N(\mu_n(x_{n+1}),\sigma_n^2(x_{n+1})) \tag{13}$$

式（13）中，$P(f(x_{n+1})\mid D_{n,x_{n+1}})$ 表示 $f(x_{n+1})$ 的后验概率，通过不断迭代即可得到最优超参数的后验概率，从而可以指导搜索方向[26-27]。在利用改进的 BiLSTM 模型进行飞行运动状态参数的分类和识别后，为了减少由于极端情况引发的误差，并进一步提高判别精度，研究利用飞行速度、位置等局部信息，来构建更精确的几何位置相关函数。该损失函数可以量化计划飞行状态与目标飞行状态之间的误差，并可以通过数据间的相关度信息，来降低权值设定的主观性，从而可以获得更加稳定的损失函数值[28]。飞行速度的损失函数表达式如式（14）所示：

$$L_s(m)=\frac{\nu_r(m)}{\nu_p(m)}\in(0,+\infty) \tag{14}$$

式（14）中，$L_s(m)$ 表示第 m 处飞机的飞行速度损失函数，ν_r 和 ν_p 分别表示实际飞行速度和计划飞行速度，当 $L_s(m)$ 的值越接近 1 时则表示该飞机的实际飞行速度与计划飞行速度越接近[29]。水平飞行方向的损失函数表达式如式（15）所示：

$$L_H(m)=\cos(\varphi_H(m)-\psi_H(m))\in[-1,1] \tag{15}$$

式（15）中，$L_H(m)$ 表示第 m 处飞机的水平飞行方向的损失函数，ψ_H 和 φ_H 分别表示实际水平飞行方向和计划水平飞行方向，当 $L_H(m)$ 等于 1 时表明计划和实际的水平飞行方向具有高度一致性，而等于 -1 时则表明实际飞行方向正向着水平飞行的反方向行进。垂直飞行方向的损失函数表达式如式（16）所示：

$$L_V(m)=\cos(\varphi_V(m)-\psi_V(m))\in[-1,1] \tag{16}$$

式（16）中，$L_V(m)$ 表示第 m 处飞机的垂直飞行方向的损失函数，ψ_V 和 φ_V 分别表示实际垂直飞行方向和计划垂直飞行方向，同样 $L_V(m)$ 的值越接近 1 则表示计划和实际的垂直飞行方向越接近，$L_V(m)$ 等于 1 则表示飞行方向完整一致，等于 -1 则表示飞行方向完全相反。

3 实验

3.1 实验环境搭建

为了验证基于深度学习的 ADS-B 信号欺骗检测方

法的性能，研究搭建了仿真实验环境。实验系统环境为 Windows 10 64 位操作系统，仿真实验在 TensorFlow 深度学习框架下进行网络搭建，开发环境采用的是 Anaconda + TensorFlow + Spyder。硬件配置包括 NVIDIA Tesla C2075 显卡和 32 GB 内存。实验初始学习率设定为 0.01，最大迭代次数为 3 000 次，单次迭代的样本数量为 50 个，批处理大小为 128，正则化系数设置为 0.000 5。为了验证基于深度学习的 ADS-B 信号欺骗检测方法的性能，研究通过监测飞行速度、方向、几何位置误差等参数来确定。具体的实验环境和参数配置如表 1 所示。

表 1　实验环境和参数配置

实验环境	配置	参数	配置
系统环境	Windows10-64 bit	初始学习率	0.01
深度学习框架	TensorFlow	迭代次数	3 000 次
开发环境	Anaconda + TensorFlow + Spyder	批处理大小	128
显卡	NVIDIA Tesla C2075	正则化系数	0.000 5
内存	32 GB	迭代的样本数量	50 个

3.2　制作数据样本

由于实际中欺骗干扰信号较为罕见，因此在对 ADS-B 信号欺骗检测方法进行模型训练之前，首先需要收集并预处理来制作出数据样本。研究将地面接收机接收到的 ADS-B 信号作为真实数据，然后通过频率估计计算出偏频数据，再将偏频数据与位置信息相结合，从而生成与真实信号不同的虚假数据集。最后，研究随机选取出真实和虚假信号数据各 2 000 条，并按照 3∶7 的比例分为训练集和测试集。真实数据的信息集合如式（17）所示：

$$M_i = \{m_{ip1}, m_{ip2}, m_{iv1}, m_{iv2}, m_{ie1}, m_{ie2}\} \tag{17}$$

式（17）中，M_i 表示真实数据的第 i 秒的信号集合，m_{ip1} 和 m_{ip2} 表示接收到的两条位置信息，m_{iv1} 和 m_{iv2} 表示接收到的两条速度信息，m_{ie1} 和 m_{ie2} 表示接收到的两条事件驱动信息。频率估计的计算公式如式（18）所示：

$$f_i = f_0 + f_{di} + f_r + \bar{\delta_i} \tag{18}$$

式（18）中，f_i 表示第 i 条信号的估计频率，$\bar{\delta_i}$ 表示频率误差，f_0 表示载波频率，f_r 表示接收机固定频偏，f_{di} 表示多普勒频偏。估计频偏的数学表达式如式（19）所示：

$$\Delta f_i = f_i - f_0 \tag{19}$$

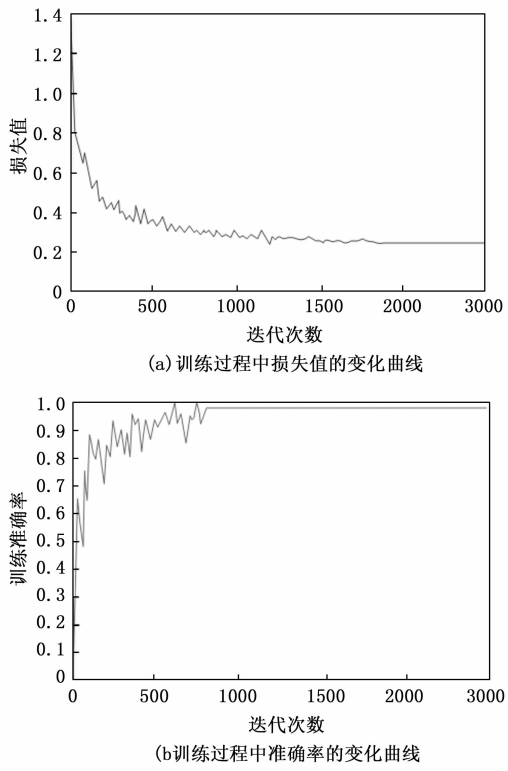
式（19）中，Δf_i 表示第 i 条信号估计频偏。将偏频数据与位置信息相拼接合成的虚假数据的信息集合如式（20）所示：

$$M'_i = \{(\Delta f_1, \Delta f_2, \cdots, \Delta f_{2n}), (lon_1, lon_2, \cdots, lon_{2n}), (lat_1, lat_2, \cdots, lat_{2n}), (alt_1, alt_2, \cdots, alt_{2n})\} \tag{20}$$

式（20）中，M'_i 表示虚假数据的第 i 秒的信号 $\alpha_i = \begin{cases} \alpha, & y=1 \\ 1-\alpha, & y=0 \end{cases}$ 集合，n 表示信号的数量，lon_{2n} 表示 $2n$ 条经度信息，lat_{2n} 表示 $2n$ 条纬度信息，alt_{2n} 表示 $2n$ 条高度信息。真实信号的频偏数据与飞机的飞行状态之间存在物理规律支持的映射关系。而虚假信号的频偏数据与飞行状态的关系缺乏物理规律的支撑，这使得它们在时间序列中表现出与真实信号不同的特征，从而虚假信号的映射关系与真实信号存在显著差异。因此能够有效制造出虚假的欺骗干扰信号数据，为后续的网络训练提供了支持。

3.3　网络训练与测试

为了验证基于深度学习的 ADS-B 信号欺骗检测方法的性能，研究首先进行了网络训练与测试。训练过程中的损失值和准确率变化趋势如图 4 所示。从图 4（a）可以看出，当迭代次数达到约 2 000 次时，损失值曲线趋于稳定，最终损失值收敛至 0.25。从图 4（b）可以看出，训练准确率在接近 800 次时趋于稳定，且最终达到了 98.15%的高准确率。综上，表明了该方法能够很好地识别真实信号与欺骗信号。



(a) 训练过程中损失值的变化曲线

(b训练过程中准确率的变化曲线

图 4　损失值与准确率的变化趋势

3.4　性能验证

为了进一步验证基于深度学习的 ADS-B 信号欺骗检测方法的性能，研究将所使用的改进 BiLSTM 模型

与其他先进的信号分类模型进行了对比分析，其他模型包括 LSTM、BiLSTM、支持向量机（SVM，support vector machine）、基于改进卷积神经网络-长短时记忆网络（CNN-LSTM，convolutional neural network-long short term memory network）模型以及基于改进注意力机制的长短时记忆网络（Attention-LSTM，attention mechanism-long short term memory network）模型等。不同模型的性能对比如表 2 所示。从表 2 中可以看出，在训练集中研究方法利用的改进 BiLSTM 模型在分类性能上非常优异，所有指标均在 99.50%以上。尤其在精确率、召回率和 F1 值等关键指标上，改进 BiLSTM 模型均表现出卓越的优势。从精确率来看，改进 BiLSTM 模型的精确率明显高于 LSTM、BiLSTM 和 SVM 等模型，同时也优于改进的 CNN-LSTM 和 Attention-LSTM 模型。在召回率方面，改进 BiLSTM 模型同样表现突出，显著超过了其他对比模型。而改进 BiLSTM 模型的 F1 值在所有对比模型中也是最高的，进一步证明了其在分类任务中的优越性能。综上所述，基于深度学习的 ADS-B 信号欺骗检测方法能够精确地区分真实信号和欺骗信号，具有高分类精确度和高鲁棒性。

表 2 不同模型的性能对比

数据集	模型	精确率/%	召回率/%	F1 值/%
训练集	改进 BiLSTM	99.98	99.85	99.63
	LSTM	97.51	97.68	98.05
	BiLSTM	99.30	99.31	99.35
	SVM	98.32	97.25	97.02
	改进 CNN-LSTM	99.05	99.11	99.34
	改进 Attention-LSTM	99.15	99.26	99.50
测试集	改进 BiLSTM	99.99	99.96	99.87
	LSTM	97.23	97.05	97.10
	BiLSTM	99.14	99.28	99.21
	SVM	98.01	97.13	96.84
	改进 CNN-LSTM	99.25	99.32	99.41
	改进 Attention-LSTM	99.48	99.56	99.50

不同检测方法的几何位置误差对比如图 5 所示。从图 5（a）可以看出，改进 BiLSTM 模型的飞行速度误差仅为 0.01%，而 LSTM、BiLSTM 和 SVM 模型的飞行速度误差分别为 1.50%、0.83%和 3.32%。研究方法相较于这 3 种模型分别缩小了 1.49%、0.82%和 3.31%。从图 5（b）可以看出，在水平飞行方向中，基于改进 BiLSTM 模型检测方法的误差同样仅为 0.01%，与其他 3 种方法的误差 1.23%、0.51%和 2.85%相比，分别减少了 1.22%、0.50%和 2.84%。从图 5（c）可以看出，基于改进 BiLSTM 模型检测方法在垂直飞行方向上的检测误差为 0.04%，而其他 3 种方法的误差为 2.08%、1.13%和 3.69%，分别降低了 2.07%、1.12%和 3.68%。综上可以看出，基于深度学习的 ADS-B 信号欺骗检测方法能够精确检测飞行器的实际飞行轨迹。

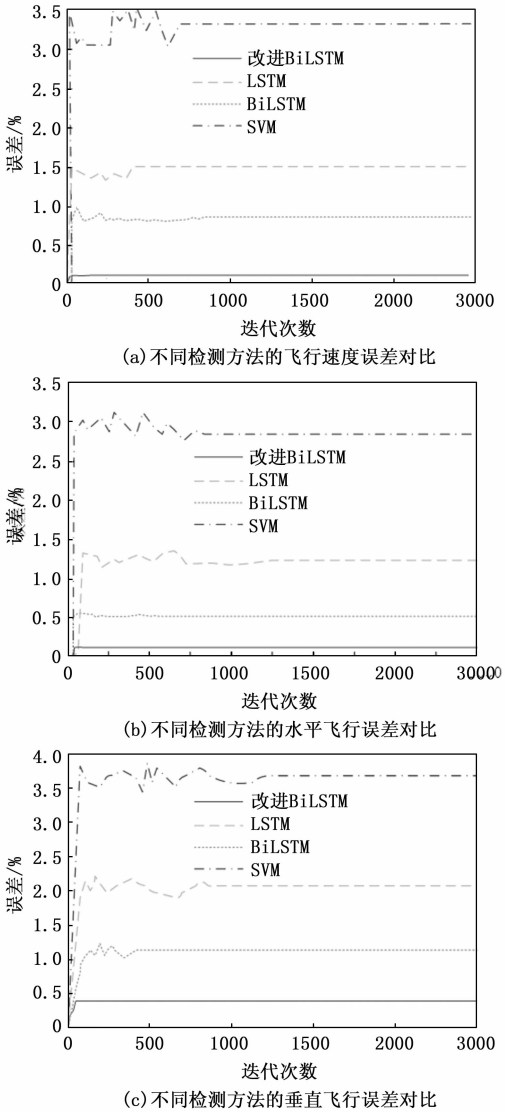
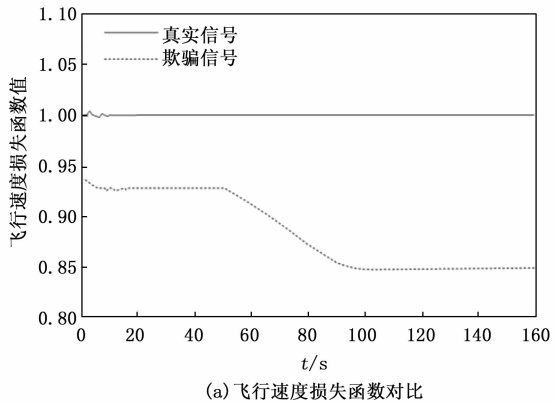


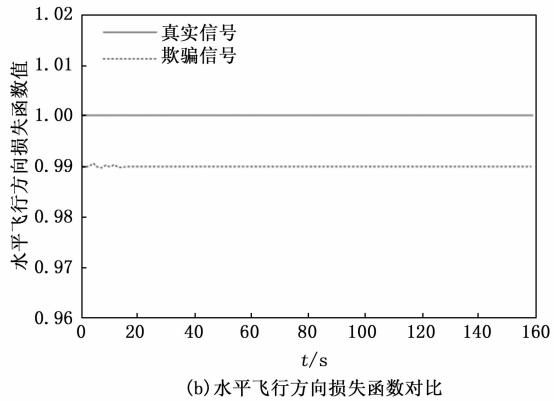
图 5 不同检测方法的几何位置误差对比

为了进一步验证基于深度学习的 ADS-B 信号欺骗检测方法的性能，研究将真实信号的飞行状态与欺骗信号的飞行状态在生成的虚假数据集中进行了对比验证。真实信号和欺骗信号的飞行状态一致性对比如图 6 所示。从图 6（a）可以看出，基于改进 BiLSTM 模型检测方法检测到的真实飞机信号的飞行速度损失函数值稳定为 1，说明该飞机的实际飞行速度与计划飞行速度几乎一致。而欺骗飞机信号的飞行速度损失函数值稳定在 0.85，与计划飞行速度产生了 15%的误差。从图 6（b）可以看出，真实信号的水平飞行方向的损失值同样稳定为 1，表明计划和实际的水平飞行方向完全一致，而欺骗信号的水平飞行方向的损失值为 0.99，虽然方向相

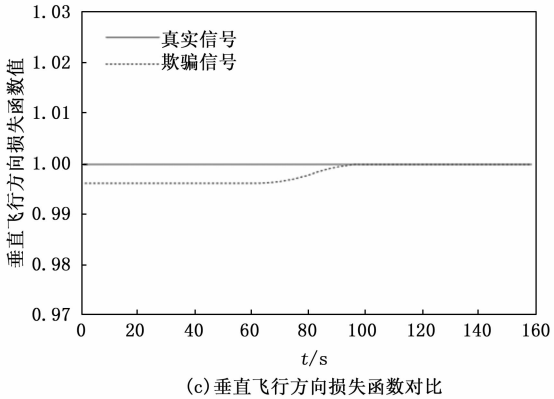
似，但仍存在 1%的误差。从图 6（c）可以看出，真实信号的垂直飞行方向的损失值同样稳定为 1，表明在垂直飞行方向上，实际和计划的飞行方向完全一致。而欺骗信号在 100 秒前的垂直飞行方向损失值为 0.997，100 秒后损失值增加到 1，说明前期欺骗信号的垂直飞行方向与计划存在 0.3%的误差，经过调整后方向调整到与计划飞行方向一致。综上可以看出，结合几何位置相关函数的 ADS-B 信号欺骗检测方法有效量化了飞行状态的误差，可以通过飞机的运行状态和飞行意图更精确地识别是否为欺骗信号。



(a) 飞行速度损失函数对比



(b) 水平飞行方向损失函数对比



(c) 垂直飞行方向损失函数对比

图 6　真实信号和欺骗信号的飞行状态一致性对比

4　结束语

随着 ADS-B 技术的应用，其低成本、高效率的优势得到了业内的广泛认可，然而虚假欺骗攻击已成为 ADS-B 技术面临的一大网络威胁。为了提升飞行安全，避免飞机遭受虚假欺骗攻击，研究利用深度学习技术结合全向信标信号，设计了一种基于改进 BiLSTM 的信号欺骗检测方法。该方法通过 BiLSTM 结构处理信号的时序特征，并结合焦点损失函数和贝叶斯优化算法进行改进，最后利用几何位置相关函数对飞机的飞行速度、位置等局部信息进行量化。结果显示，模型的训练损失值和训练准确率分别达到了 0.25 和 98.15%，表明该方法能够有效区分真实信号与欺骗信号。改进 BiLSTM 模型的分类性能指标均超过 99.50%，其中精确率、召回率和 F1 值分别达到了 99.98%、99.85%和 99.63%，展现了卓越的信号分类能力。此外，研究方法在飞行速度、水平飞行方向和垂直飞行方向的检测误差分别仅为 0.01%、0.01%和 0.04%，证明该方法能够精确检测飞行器的实际飞行轨迹。通过对真实飞机和欺骗飞机信号的检测结果分析可知，真实信号在飞行速度、水平飞行方向和垂直飞行方向上的损失值均为 1，表明实际飞行状态与计划一致，表现出极高的精度和鲁棒性。而欺骗信号的飞行速度、水平飞行方向和垂直飞行方向上的损失值误差分别为 15%、1%和 0.3%。综上所述，基于全向信标信号处理的深度学习 ADS-B 信号欺骗检测方法，能够高精度、稳定性地识别和区分真实信号与欺骗信号，有效保障了民用航空的飞行安全。然而，随着科技的发展，欺骗信号的形式也在不断演变。研究的方法并未涵盖所有类型的欺骗信号，因此研究的结果还不够全面，这方面还待进一步完善和改进。

为了应对未来更加复杂和多变的欺骗攻击，研究可以考虑从以下几个方面进行更深入的探讨。首先，未来研究可以将 ADS-B 信号与雷达、机载传感器等其他监视数据源进行融合讨论，这种多模态数据融合技术有助于在不同维度上进行验证，增强对欺骗信号的辨识能力。此外，因为在 ADS-B 信号的传输过程中，缺乏加密和身份验证机制导致使其易受到伪造和篡改攻击。所以未来可以探索在 ADS-B 协议中加入加密技术，通过数字签名、加密密钥等手段来提升信号传输的安全性，以确保信号的真实性。未来的空中交通监视将不仅限于识别常规信号，还应具备发现未知攻击模式的智能性，以应对日益复杂的空中威胁环境。

参考文献：

[1] 许　诚，程　强，赵　鹏，等. 基于人工智能的多模态雷达自适应抗干扰优化算法 [J]. 现代电子技术，2024，47 (7)：73－76.

[2] 刘拥军，马青松，杨　斌. 基于子空间相关运算的 GNSS 欺骗干扰检测研究 [J]. 海洋测绘，2023，43 (6)：56－60.

[3] KARNATI M，SEAL A，YAZIDI A，et al. LieNet：A

deep convolution neural network framework for detecting deception [J]. IEEE Transactions on Cognitive and Developmental Systems. 2021, 3: 14 (3): 971 - 984.
[4] ALASKAR H, SBAI Z, KHAN W, et al. Intelligent techniques for deception detection: a survey and critical study [J]. Soft Computing, 2023, 27 (7): 3581 - 3600.
[5] KOZOVIC D V, DURDEVIC DŽ. Spoofing in aviation: security threats on GPS and ADS-B systems [J]. Vojnotehnicki Glasnik/Military Technical Courier, 2021, 12: 69 (2): 461 - 85.
[6] REN B, KARIMI H R, YIN T, et al Asynchronous H∞ filtering for semi-Markov jump TS fuzzy systems within partial state delay and deception attack: Applied to aircraft - pilot state estimation [J]. Journal of the Franklin Institute, 2023, 360 (12): 9265 - 9289.
[7] LEONARDI M, SIRBU G. ADS-B crowd-sensor network and two-step Kalman filter for GNSS and ADS-B cyber-attack detection [J]. Sensors, 2021, 21 (15): 4992 - 4997.
[8] 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.
[9] 常浩伟，庞春雷，郭泽辉，等. 基于自适应免疫算法的欺骗信号检测方法 [J]. 系统工程与电子技术，2022，44 (8)：2419 - 2426.
[10] VAN HUYNH N, NGUYEN D N, HOANG D T, et al. Defeating super-reactive jammers with deception strategy: Modeling, signal detection, and performance analysis [J]. IEEE Transactions on Wireless Communications, 2022, 21 (9): 7374 - 7390.
[11] DERAKHSHAN A, MIKAEILI M, GEDEON T, et al. Identifying the optimal features in multimodal deception detection [J]. Multimodal Technologies and Interaction, 2020, 4 (2): 25 - 32.
[12] 程 擎，但诗芸，鲁合德. 高压线对机场全向信标及测距仪的电磁干扰分析 [J]. 电子测量技术，2021，44 (18)：13 - 18.
[13] KHANDKER S, TURTIAINEN H, COSTIN A, et al. Cybersecurity attacks on software logic and error handling within ADS-B implementations: Systematic testing of resilience and countermeasures [J]. IEEE Transactions on Aerospace and Electronic Systems, 2021, 58 (4): 2702 - 2719.
[14] FILIPPONE A, PARKES B, BOJDO N, et al. Prediction of aircraft engine emissions using ADS-B flight data [J]. The Aeronautical Journal, 2021, 125 (1288): 988 - 1012.
[15] VANCE N, SPETH J, KHAN S, et al. Deception detection and remote physiological monitoring: A dataset and baseline experimental results [J]. IEEE Transactions on Biometrics, Behavior, and Identity Science, 2022, 4 (4): 522 - 532.
[16] HABIBI MARKANI J, AMRHAR A, GAGNE J M, et al. Security establishment in ADS-B by format-preserving encryption and blockchain schemes [J]. Applied Sciences, 2023, 13 (5): 3105 - 3110.
[17] 傅金琳，赵申卫，邓福建，等. 多传感器导航中双天线基线欺骗干扰检测方法 [J]. 中国惯性技术学报，2022，30 (6)：820 - 825.
[18] GALLARDO-ANTOLIN A, MONTERO J M. Detecting deception from gaze and speech using a multimodal attention LSTM-based framework [J]. Applied Sciences, 2021, 11 (14): 6393 - 6402.
[19] DAVIDYAN J Y, HUELS B W, GISSEL J L. Two truths and a lie: introduction to deception detection [J]. Issues in Accounting Education, 2023, 38 (2): 85 - 93.
[20] 庞春雷，郭泽辉，吕敏敏，等. 基于 PNN 的北斗转发式欺骗干扰信号检测方法 [J]. 中国惯性技术学报，2021，29 (4)：554 - 560.
[21] ŞEN M U, PEREZ-ROSAS V, YANIKOGLU B, et al. Multimodal deception detection using real-life trial data [J]. IEEE Transactions on Affective Computing, 2020, 13 (1): 306 - 319.
[22] RUSENO N, LIN C Y, CHANG S C. Uas traffic management communications: the legacy of ADS-B, new establishment of remote id, or leverage of ADS-B-like systems [J]. Drones, 2022, 6 (3): 57 - 65.
[23] TEOH R, ENGBERG Z, SHAPIRO M, et al. The high-resolution Global Aviation emissions Inventory based on ADS-B (GAIA) for 2019 - 2021 [J]. Atmospheric Chemistry and Physics, 2024, 24 (1): 725 - 744.
[24] WARREN-WEST L S, JACKSON R C. Seeing the bigger picture: Susceptibility to, and detection of, deception [J]. Journal of Sport and Exercise Psychology, 2020, 42 (6): 463 - 471.
[25] 王文益，王沛菡. 基于捕获结果的 GNSS 欺骗式干扰检测 [J]. 信号处理，2021，37 (8)：1460 - 1469.
[26] KUMAR S G, CORRADO S J, PURANIK T G, et al. Classification and analysis of goarounds in commercial aviation using ADS-B data [J]. Aerospace, 2021, 8 (10): 291 - 298.
[27] 覃仕明，马 鹏. 基于 CNN-A-BiLSTM 的无刷直流电机故障诊断方法研究 [J]. 计算机测量与控制，2024，32 (9)：118 - 124.
[28] 李晓峰，邓 晔，乔淑君，等. 基于机械臂毫米波天线测试系统设计与实现 [J]. 计算机测量与控制，2024，32 (9)：21 - 26.
[29] 孙 晔，郭 琳. 基于传感器技术和 I-LSTM 算法的风电机设备运行故障检测及诊断研究 [J]. 计算机测量与控制，2024，32 (9)：51 - 57.