计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2023,32(4):94−103 [doi: 10.15888/j.cnki.csa.009012]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于注意力机制的 CNN-LSTM 的 ADS-B 异常数据检测①

刘　浪, 时宏伟

(四川大学 计算机学院, 成都 610065)
通信作者: 时宏伟, E-mail: shihw001@126.com

摘　要: 广播式自动相关监视 (ADS-B) 是民航新一代空中交通管理系统的重要组成部分, 由于协议没有数据加密和认证, 导致容易受到数据攻击. 为了准确检测 ADS-B 数据攻击, 基于 ADS-B 数据的时序性, 提出了一种基于注意力机制的卷积神经网络-长短期记忆网络 (convolutional neural networks-long short-term memory, CNN-LSTM) 异常数据检测模型. 首先, 利用 CNN 提取 ADS-B 数据的特征, 然后以时序形式将特征向量输入到 LSTM 中, 最后使用注意力机制进行网络参数优化, 实现对 ADS-B 数据的预测, 通过计算预测误差, 来进行异常检测. 实验表明, 该模型能够很好地检测出模拟的 4 种类型的异常数据, 与其他机器学习方法相比, 具有更高的准确率和 *F*1 分数.

关键词: 广播式自动相关监视; 异常检测; 卷积神经网络 (CNN); 长短期记忆网络 (LSTM); 注意力机制

引用格式: 刘浪,时宏伟.基于注意力机制的 CNN-LSTM 的 ADS-B 异常数据检测.计算机系统应用,2023,32(4):94–103. http://www.c-s-a.org.cn/1003-3254/9012.html

ADS-B Anomaly Detection Based on Attention Mechanism for CNN-LSTM

LIU Lang, SHI Hong-Wei

(College of Computer Science, Sichuan University, Chengdu 610065, China)

Abstract: Automatic dependent surveillance-broadcast (ADS-B) is an important part of the new generation air traffic management system of civil aviation. As the protocol does not have data encryption and authentication, it is vulnerable to data attacks. To accurately detect ADS-B data attacks, based on the timing of ADS-B data, this study proposes a convolutional neural networks-long short-term memory (CNN-LSTM) anomaly detection model based on attention mechanism. Firstly, CNN is adopted to extract the features of ADS-B data, and then the feature vectors are input into the LSTM in the form of time series. Finally, the attention mechanism is applied to optimize the network parameters to realize the prediction of ADS-B data, and the anomaly detection is carried out by calculating the prediction error. Experiments show that the model can well detect four types of abnormal data and has higher accuracy and *F*1 score than other machine learning methods.

Key words: automatic dependent surveillance-broadcast (ADS-B); anomaly detection; convolutional neural network (CNN); long short-term memory (LSTM); attention mechanism

空中交通管理 (air traffic management, ATM) 系统是一个利用通信、导航和监视技术来管理空域和确保航空器的空中交通安全和秩序的系统. 随着空域密度的日益增加, 一次监视雷达 (primary surveillance radar, PSR)、二次监视雷达 (secondary surveillance radar, SSR) 和广域多向定位 (wide area multilateration, WAM) 等技术已经无法满足未来空中交通管理的发展需求. 与传统的技术手段相比, 广播式自动相关监视 (automatic

① 收稿时间: 2022-08-29; 修改时间: 2022-09-27; 采用时间: 2022-09-30; csa 在线出版时间: 2022-11-29
CNKI 网络首发时间: 2022-11-30

dependent surveillance-broadcast, ADS-B) 技术具有数据精度高、建设成本低、维护方便等优势, 已经成为空中交通管理系统的重要组成部分[1,2], 数据安全方面更加不应被忽视.

ADS-B 采用单向广播的方式传播数据, 接收端能够轻易地获取报文信息, 但却无法验证消息的准确性和可靠性, 这会导致容易受到窃听、干扰、删除、注入和修改等类型的攻击威胁. 相关研究已经证明了 ADS-B 系统存在安全漏洞[3,4]. 因此, 随着空中交通的不断发展以及 ADS-B 技术的进一步普及, 快速地检测出上述类型攻击下形成的异常数据, 将有助于安全航空环境的建设.

在其他的研究中, 对于 ADS-B 数据的安全问题已经提出来很多的方法, 可以分为非机器学习方法和机器学习方法两类. 非机器学习方法主要有 4 种解决方案, 分别是加密技术、物理层信息、多点定位和数据融合. 加密技术在无线网络的通信安全领域是一种使用广泛的保证数据安全可靠传输的手段. 在之前的研究中, 通过使用对称密钥[5]、消息验证码[6]、非对称密钥[7] 和签名[8] 加密 ADS-B 数据或生成额外的安全信息. 攻击者发起攻击之前对 ADS-B 数据进行安全保护, 虽然可以有效地防止窃听等攻击[9], 但由于密钥管理的复杂性, 以及需要对标准的 ADS-B 协议进行修改, 导致加密在空中交通管理系统中难以得到应用. ADS-B 数据在通信过程中会附加一些物理层信息, 可以通过这些物理层信息来进行异常检测. 根据接收信号强度与距离的负相关关系[10]、分析具有特定 ADS-B 应答器的两个 ADS-B 消息之间的时间分布[11] 来检测 ADS-B 数据的异常. 但是当攻击者通过统计分析获取物理层信息, 来构造虚假数据进行注入攻击时, 就很难检测出异常数据. 多点定位技术是通过将到达时间差计算出的位置与解调后的位置进行比较, 来识别 ADS-B 数据是否受到攻击[12,13]. 作为空中交通管理系统的一种备份技术, 多点定位技术需要设备较多, 成本高、工作机制较为复杂, 工作覆盖范围受限, 需要多个地面站协同工作, 实际应用范围受限, 主要部署在机场和主要航线上. 还可以利用 ADS-B 数据和传统的 PSR 数据、SSR 数据[14–16]、WAM 数据[17] 进行融合分析, 来检查 ADS-B 数据是否合法. 当 ADS-B 数据与其他监控数据的差值超过阈值时, 可以检测到异常数据. 但由于时间同步和监视精度的差异, 基于数据融合的方法存在局限性和不足, 实际应用受限. 由于 ADS-B 数据是典型的时间序列数据, 具有时间依赖性, 过去的数据暗示了现在或将来数据发展变化的规律, 具有趋势性、周期性和不规则性. 随着机器学习的不断发展, 可以通过一些深度学习方法, 对 ADS-B 时间序列数据进行重构或者预测, 来进行异常检测. 例如, 使用 RNN 来进行 ADS-B 数据异常检测[18]; 使用 LSTM 对 ADS-B 数据进行训练来检测数据的合法性[19]; 使用 LSTM 编解码器模型重构 ADS-B 数据, 通过分析重构误差来检测数据异常[20]; 使用 Seq2Seq 模型重构 ADS-B 数据, 利用重构误差来进行异常检测[21]; 分别使用 BiGRU[22]、变分自编码器[23] 对 ADS-B 数据进行数据重构, 然后使用 SVDD 来分析重构值与真实值之间的差值进行异常检测. 利用高斯差分法获取位置数据的细节信息, 然后利用 LSTM 模型对位置数据进行重构, 利用重构误差检测异常数据[24].

在当前的研究中, 基于深度学习的方法能够在不改变 ADS-B 协议框架的基础上, 基于已有的航迹信息, 检测出数据是否存在异常. 于是, 我们基于深度学习方法, 提出了一种检测 ADS-B 异常数据的解决方案. 模型首先利用 CNN 处理 ADS-B 数据, 然后将处理后的数据以时序形式的特征向量输入到 LSTM 网络中, 最后使用注意力机制进行参数优化, 实现对 ADS-B 数据的预测, 计算预测值与真实值之间的可决系数. 输入正确的 ADS-B 数据, 可决系数将在一定的范围内, 若输入的数据包含异常, 可决系数将变小, 达到异常检测的目的. 在本文中, 实验使用的异常数据是指经过一定规则操作后的模拟攻击数据.

1 相关工作

1.1 ADS-B

ADS-B 是利用空地、空空数据通信完成交通监视和信息传递的一种航行新技术, 如图 1 所示. 具有数据更新率快、信息丰富、精度高、成本低、支持信息共享等优点. 根据相对于航空器的信息传递方向, 机载 ADS-B 应用功能可分为发送 (OUT) 和接收 (IN) 两类.

ADS-B OUT 是指航空器向外发送信息, 机载发射机以一定的周期发送航空器的各种飞行信息, 是机载 ADS-B 设备的基本功能. 地面系统通过接收机载设备发送的 ADS-B OUT 信息, 监视空中交通状态. ADS-B 发送的航空器水平位置一般源于 GNSS 系统, 具有比雷达设备更高的监视精度.

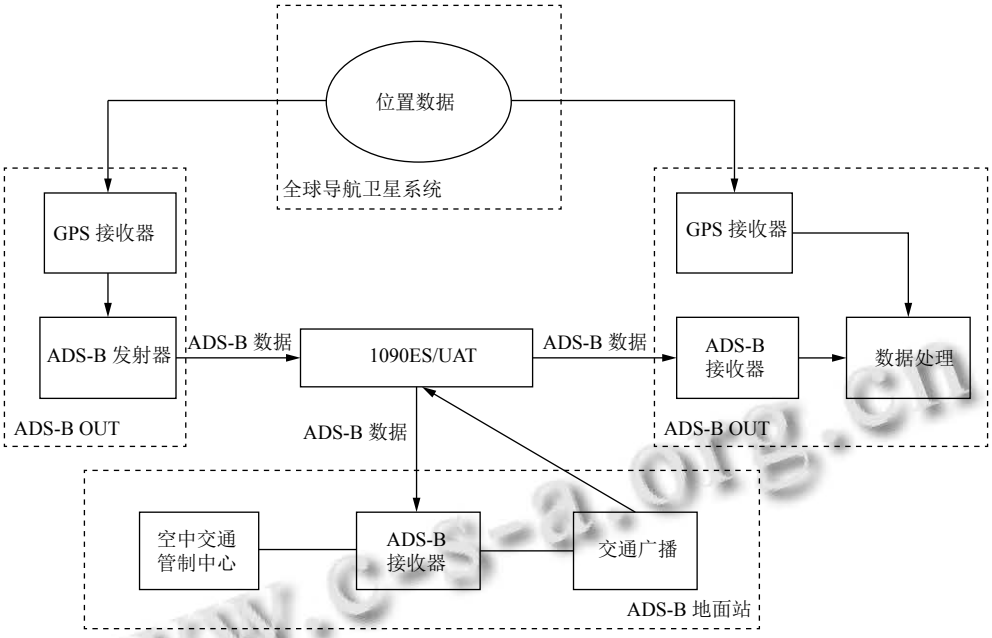


图 1 ADS-B 系统结构

ADS-B IN 是指航空器接收其他航空器发送的 ADS-B OUT 信息或地面服务设施发送的信息, 为机组提供运行支持. ADS-B IN 可使机组在驾驶舱交通信息显示设备 (cockpit display of traffic information, CDTI) 上“看到”其他航空器的运行状况, 从而提高机组的空中交通情景意识.

1.2 ADS-B 受攻击的类型

ADS-B 系统以明文格式来广播数据, 使飞机容易受到以下 5 种类型的数据攻击.

(1) 窃听: 由于缺乏信息加密和以广播的方式传播, 使得攻击者能够轻易地通过设备进行窃听, 从而使攻击者能够掌握我方的飞行信息[25], 是其他攻击的基础.

(2) 干扰: 普遍存在于所有的无线通信方式中, 攻击者通过在 1 090 MHz 频率上发送高功率的干扰信号来实现攻击[26]. 或是通过发送一些易识别的简单攻击数据, 降低 ADS-B 系统的可靠性, 扰乱空中交通管理系统.

(3) 消息注入: 利用 ADS-B 系统没有认证机制, 攻击者通过 ADS-B 发射器发送生成的 ADS-B 消息, 来实现攻击. 由于攻击消息的注入, 使得空中交通管理系统中出现了大量的虚假航迹, 影响系统的正常工作.

(4) 消息删除: 使飞机航迹在空中交通管理系统中消失, 但由于需要严格的时间同步, 单一的消息删除很容易在 SSR 或 WAN 的支持下检测到.

(5) 消息修改: 通过向实际的 ADS-B 数据中注入偏差来实现, 一般通过消息删除和消息注入来实现. 符合飞行规则的消息修改, 会使空中交通管理系统对飞机航迹产生错误的判断, 严重影响空中交通安全和秩序.

2 模型

由于 ADS-B 是典型的多特征时间序列数据, 预测当前时刻的特征信息需要考虑过去一段时间的数据. 因此, 本文选择使用深度学习的方法来分析飞行路线和检测异常, 这种方法不需要修改 ADS-B 系统当前的协议架构, 并且能够自主、独立地分析 ADS-B 消息来进行异常检测.

2.1 卷积神经网络 (CNN)

CNN 可以通过对数据逐层卷积和池化来操作数据. 其中卷积层利用权重共享和局部连接对输入数据进行卷积提取深层特征. 池化层通过一定的规则, 对卷积层处理后的数据进行池化操作, 减少参数量, 保留主要特征, 防止过拟合.

CNN 能够很好地提取出数据的隐藏特征, 并逐层融合, 生成高层抽象特征. 但因为其缺乏记忆功能, 不具备对时间序列数据中的时间相关性的要求. 因此, 本文将 LSTM 网络与之结合, 将 CNN 的输出作为 LSTM 的输入.

2.2 长短时记忆神经网络 (LSTM)

递归神经网络 (recursive neural network, RNN) 是最早用于时间序列预测的机器学习模型之一. 而 LSTM 则是 RNN 的一个改进版本, 能够很好地解决 RNN 存在的梯度消失问题. LSTM 通过引入门控结构控制信息传递的路径, 从而有效的记忆保存时序数据特征. LSTM 的单元结构如图 2 所示.

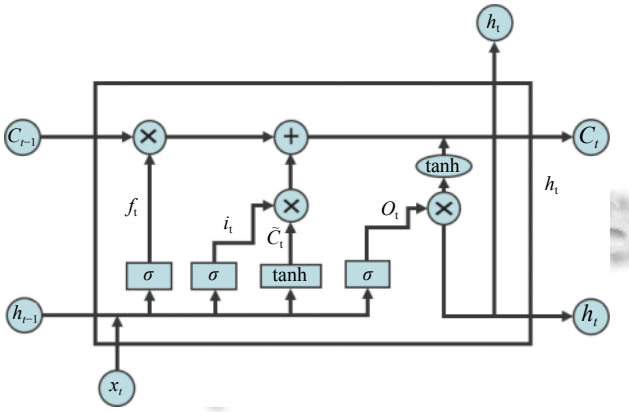


图 2 LSTM 单元结构

LSTM 的循环单元结构主要包括遗忘门f_t、输入门i_t和输出门o_t这 3 个门控结构.

LSTM 的计算过程如下.

(1) 遗忘门

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

其中, f_t代表遗忘门的输出; W_f代表系数; b_i代表偏倚.

(2) 输入门

$$i_t = \sigma(W_i \cdot [h_{t-1}, x_t] + b_i) \tag{2}$$

$$\tilde{C}_t = \tanh(W_C \cdot [h_{t-1}, x_t] + b_C) \tag{3}$$

其中, i_t和$\tilde{C}_t$分别是σ激活函数和tanh激活函数的输出; W_i、W_C代表线性关系系数; b_i、b_C代表偏倚量.

细胞状态:

$$C_t = f_t \odot C_{t-1} + i_t \odot \tilde{C}_t \tag{4}$$

其中, C_t代表细胞的状态; $\odot$代表哈达玛积.

(3) 输出门

$$o_t = \sigma(W_o \cdot [h_{t-1}, x_t] + b_o) \tag{5}$$

$$h_t = o_t \odot \tanh(C_t) \tag{6}$$

其中, o_t代表输出门的输出; h_t代表隐藏层的输出.

LSTM 特殊的门控结构可以控制时间序列数据特征的保留与遗忘, 但在单独处理长时间序列时, 仍然会出现丢失重要特征的可能. 因此, 本文采用首先通过 CNN 处理时间序列数据, 然后将输出作为 LSTM 网络的输入, 从而提高模型的预测的精度.

2.3 注意力机制 (Attention)

分析 ADS-B 数据得知, 航迹序列长度一般相对较长, 最长的航迹包含了超过了 2 000 条 ADS-B 数据, 引入注意力机制, 能够很好地提高模型的预测能力.

注意力机制能够将模型的注意力放在需要重点关注的时间序列数据上, 减少其他数据的权重. 使用注意力机制能够将更大的权重分配给重要数据, 提高模型精度, 能够改进 CNN-LSTM 因数据过长而忽略重要信息的情况, 有效地提高预测模型的准确性[27].

2.4 基于注意力机制的 CNN-LSTM 模型

LSTM 具有不错的记忆非线性时间序列数据的能力, ADS-B 数据又是典型的非线性时序数据, 因此我们选择 LSTM 作为基准模型. 但 LSTM 在特征提取方面的不足, 可能造成重要特征的丢失, 因此我们使用 CNN 对输入的 ADS-B 数据先进行特征提取, 然后将输出作为 LSTM 的输入. 本文首次将 CNN-LSTM 模型用于 ADS-B 异常数据的检测中, 为避免重要数据的丢失, 还将注意力机制引入模型, 避免由于时序数据过长导致的重要信息丢失的情况. 模型结构如图 3 所示, 共分为 5 层: 输入层、CNN 层、LSTM 层、注意力层、输出层. ADS-B 数据输入模型后, 经过 CNN 层提取特征, 将输出作为 LSTM 层的输入, 在注意力层的帮助下, 进行数据预测, 最后经过输出层将结果输出.

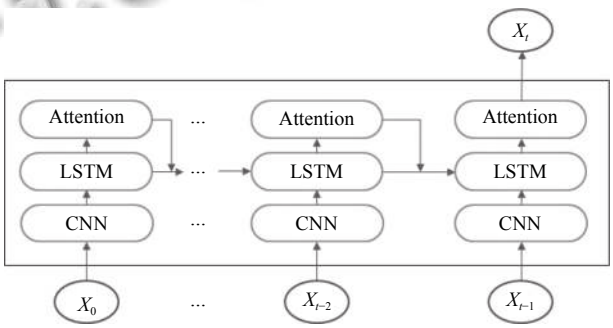


图 3 基于注意力机制的 CNN-LSTM 模型结构

模型每层的叙述如下.

(1) 输入层. 对长度为n的 ADS-B 数据进行预处理, 将其作为该模型的输入, 表示为$X = [X_1, \cdots, X_{k-1}, X_k, \cdots, X_n]^{\mathrm{T}}$.

(2) CNN 层. CNN 层主要用于提取时间序列数据的特征, 包括 1 层卷积层、1 层池化层. 卷积层为一维

卷积, 使用*ReLU*激活函数, 池化层采用最大池化方法. 将时间序列数据通过 CNN 层, 通过*Sigmoid*激活函数得到的输出$H_C=[h_{C_1},\cdots,h_{C_{t-1}},h_{C_t},\cdots,h_{C_j}]^{\mathrm{T}}$的表示如下:

$$C=ReLU(X\otimes W_1+b_1) \tag{7}$$

$$P=\max(C)+b_2 \tag{8}$$

$$H_C=Sigmoid(P\times W_2+b_3) \tag{9}$$

其中, C为卷积层输出; P为池化层输出; W_1、W_2为权重; b_1、b_2、b_3为偏差; $\otimes$是卷积运算.

(3) LSTM 层. 建立 LSTM 层, 将 CNN 层输出H_C的时间序列输入 LSTM 层, 输出h_t表示如下:

$$h_t=LSTM(H_{C,t-1},H_{C,t}),\ t\in[1,i] \tag{10}$$

其中, h_t为t时刻的输出.

(4) 注意力层. 将 LSTM 的输出h_t作为注意力层的输入, 将权重以概率的方式进行分配, 计算出权重矩阵. 注意力层权重的表示如下:

$$e_t=u\tanh(wh_t+b) \tag{11}$$

$$a_t=\frac{\exp(e_t)}{\sum_{j=1}^{t}e_j} \tag{12}$$

$$s_t=\sum_{t=1}^{i}a_th_t \tag{13}$$

其中, b为偏置系数; u、w为权重系数; e_t为注意力层的概率分布; s_t表示注意力层t时刻的输出.

(5) 输出层. 该层的计算公式如下:

$$\hat{y}_t=Sigmoid(w_os_t+b_o) \tag{14}$$

其中, $\hat{y}_t$为t时刻的输出; w_o为权重; b_o为偏差.

3 实验分析

为了评估提出的方法, 结合常见的攻击威胁类型, 本文进行了一系列的实验. 在一部分数据集中分别模拟可能受到的攻击威胁类型, 构造测试集中的异常数据, 使用本文的模型以及一些对比模型来检测异常数据, 通过模型预测值与真实值之间的可决系数, 对不同的特征设置不同的阈值, 可决系数低于阈值的, 可认定为异常 ADS-B 数据.

3.1 数据收集

实验使用的数据可公开获取, 来自飞常准 ADS-B 网站 (https://flightadsb.variflight.com), 抽取了成都双流机场进出场飞机的 6 298 条航迹数据组成数据集. 其中 5 398 条航迹数据作为训练样本, 900 条航迹数据作为测试样本. 其中每条航迹的 ADS-B 数据在 200–2 800 条之间, 包含飞机的起飞、巡航和降落等全部阶段. 每条 ADS-B 数据包含时间 (Time)、协调世界时 (UTC Time)、飞机注册号 (anum)、航班号 (fnum)、高度 (height)、速度 (speed)、航向角 (angle)、经度 (longitude)、纬度 (latitude) 等信息.

3.2 模拟攻击数据

为了评估模型的性能, 表 1 描述了本文的测试集构建过程, 900 条测试样本按照正负样本比 6:1 构建测试集, 对于其中的负样本分别使用干扰、修改、删除和注入 4 类常见攻击下的 10 种攻击方法, 包括速度信息删除、高度信息删除、航向角信息删除、速度高斯噪声、路线替换、航向角转向、高度偏移 (+)、高度偏移 (−)、速度偏移 (+)、速度偏移 (−). 每种攻击方式得到一个测试集, 得到 10 种测试集分别测试 10 种攻击下模型的异常检测能力.

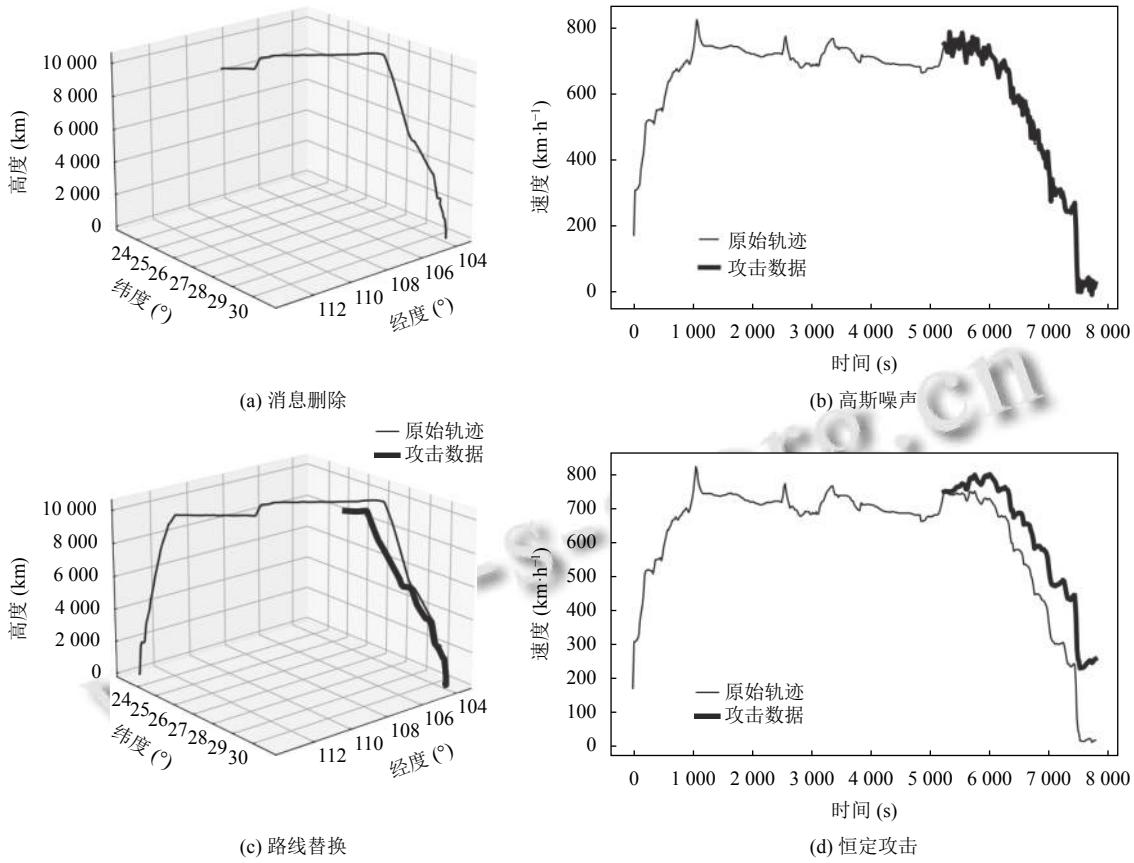
表 1 模拟攻击方法

攻击类型	数据操作	攻击方法
消息删除	速度删除	删除ADS-B数据中前15%的速度信息.
	高度删除	删除ADS-B数据中前15%的高度信息.
	航向角删除	删除ADS-B数据中前15%的航向角信息.
干扰	速度高斯噪声	对原始的ADS-B数据中速度信息添加(0, 20)的高斯噪声
消息注入	路线替换	使用另一条航迹的ADS-B数据替换当前飞机的ADS-B数据.
消息修改	航向角转向	使原始的ADS-B数据中的航向角信息改为与原始值相反的值.
	高度偏移(+)	以120 m为单位, 逐渐增加ADS-B信息的高度数据. 将第1个时刻的高度数据增加120 m, 第2个增加240 m, 依此类推.
	高度偏移(−)	类似于高度偏移(+), 以120 m为单位, 逐渐减少ADS-B信息的高度数据.
	速度偏移(+)	以15 km/h为单位, 逐渐增加ADS-B信息的速度数据. 将第1个时刻的速度数据增加15 km/h, 第2个增加30 km/h, 依此类推.
	速度偏移(−)	类似于速度偏移(+), 以15 km/h为单位, 逐渐减少ADS-B信息的速度数据.

选取一组包含 370 条 ADS-B 数据的航迹, 具体的攻击数据生成方法如下.

(1) 消息删除. 如图 4(a) 所示, 删除掉航迹信息的前 15% 数据.

(2) 干扰. 如图 4(b) 所示, 前 265 条数据不做修改, 对后 105 条数据的速度信息添加含有高斯噪声的 ADS-B 报文.



(a) 消息删除 (b) 高斯噪声

(c) 路线替换 (d) 恒定攻击

图 4 模拟数据攻击

(3) 消息注入. 如图 4(c) 所示, 前 265 条数据不做修改, 将另一架航迹的后 105 条 ADS-B 数据注入.

(4) 消息修改. 如图 4(d) 所示, 前 265 条数据不做修改, 第 266 条数据的速度增加 15 km/h, 第 267 条数据的速度增加 30 km/h, 依次类推.

3.3 数据预处理

对于实验所需的数据, 需要进行一定的预处理操作, 以便于模型能够更好地学习.

3.3.1 数据缺失值处理

ADS-B 数据具有一定的丢包率, 在进入模型训练前需要对 ADS-B 数据进行预处理操作. 本文采用插值方法对丢失的 ADS-B 数据进行补全, 具体操作如图 5 所示. 如果在t_k时刻 ADS-B 数据x_k丢失, 则数据x_k的计算如下:

$$x_k = x_{k-1} + \frac{x_{k+1} - x_{k-1}}{t_{k+1} - t_{k-1}} \times (t_k - t_{k-1}) \tag{15}$$

使用基于注意力机制的 CNN-LSTM 模型分别对原始 ADS-B 数据、数据预处理后的 ADS-B 数据进行预测, 分析预测值与真实值之间的可决系数, 图 6(a) 和图 6(b) 表示了数据预处理前后高度特征的可决系数分布情况变化, 图 6(c) 和图 6(d) 表示了数据预处理前后速度特征的可决系数分布情况变化, 可以看出经过预处理操作后, ADS-B 数据两种特征的可决系数都得到了明显的提高. 其中, 高度特征的可决系数大于 0.9 的数据占比由 69.34% 提高到 93.09%, 速度特征的可决系数大于 0.8 的数据占比由 51.03% 提高到 75.90%. 可以看出, 对实验数据进行预处理操作, 能够降低 ADS-B 数据缺失对实验结果的影响, 有助于模型对 ADS-B 数据进行预测分析, 提高模型的检测精度.

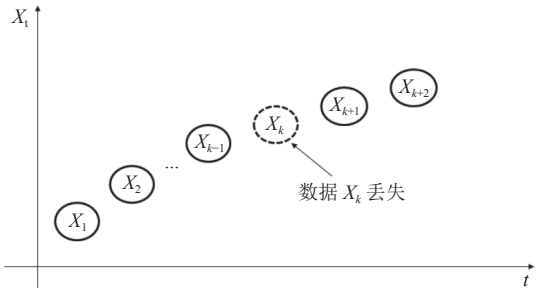
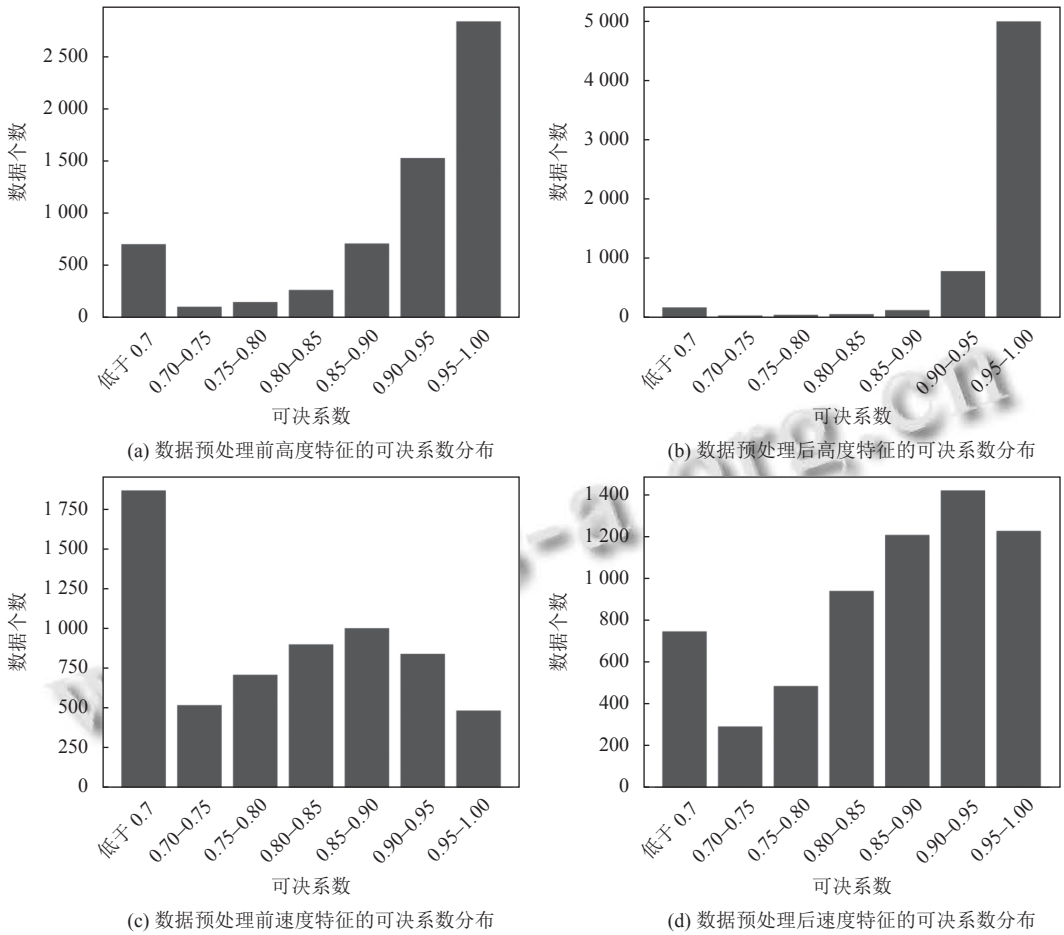


图 5 缺失值处理



(a) 数据预处理前高度特征的可决系数分布 (b) 数据预处理后高度特征的可决系数分布

(c) 数据预处理前速度特征的可决系数分布 (d) 数据预处理后速度特征的可决系数分布

图 6 数据预处理前后 ADS-B 数据预测值与真实值的可决系数分布

3.3.2 归一化操作

在实验中, 本文选取经度、纬度、高度、速度、航向角分别作为训练特征. 为了后续数据处理的方便以及加快模型收敛速度, 本文对数据采用归一化操作. ADS-B 数据是时间序列数据$D=[D_1,D_2,\cdots,D_k,\cdots,D_m]$, 归一化方程如下:

$$X_k=\frac{D_k-\min(D)}{\max(D)-\min(D)} \tag{16}$$

其中, D_k表示时间序列D的第k个数据, $\min(D)$表示D的最小值, $\max(D)$表示D的最大值.

对 ADS-B 数据$D=[D_1,D_2,\cdots,D_k,\cdots,D_m]$进行归一化操作, 得到时间序列$X=[X_1,X_2,\cdots,X_k,\cdots,X_m]$.

3.4 评价指标

3.4.1 阈值设置

本文对于模型预测值与真实值之间的比较, 采用可决系数, 计算公式如下:

$$R^2=1-\frac{\sum_i(\hat{y}^{(i)}-y^{(i)})^2}{\sum_i(\bar{y}-y^{(i)})^2} \tag{17}$$

其中, $\hat{y}^{(i)}$表示模型在i时刻的预测值, $y^{(i)}$表示模型在i时刻的真实值, $\bar{y}$表示真实值的平均值. R 方值的结果表示模型的预测值和真实值之间距离, 通过对不同的特征设置不同的阈值, 来反映模型对于异常数据的检测能力.

3.4.2 模型评估

表 2 描述了样本分类结果. *TP* (true positive) 是指正确分类的正样本数, *FN* (false negative) 是指错误分类的负样本数, *FP* (false positive) 是指错误分类的正样本数, *TN* (true negative) 是指正确分类的负样本数. 为了评估模型的效率, 本文采用召回率 (*TPR*)、检测率 (*TNR*)、准确率 (*Acc*) 和 *F*1 分数 (*F*1) 作为评价指标, 具体定义如下.

表 2 样本分类结果

真实情况	判定结果	
	正样本	负样本
正样本	*TP*	*FN*
负样本	*FP*	*TN*

(1) 召回率 *TPR*, 它表示所有正类样本中, 有多少被正确分类, 即正确分类的正样本数占正样本总数的比例.

$$TPR=\frac{TP}{TP+FN} \tag{18}$$

(2) 检测率 *TNR*, 它表示所有负类样本中, 有多少被正确分类, 即正确分类的负样本数占负样本总数的比例.

$$TNR=\frac{TN}{FP+TN} \tag{19}$$

(3) 准确率 *Acc*, 它表示样本正确分类的百分比, 即正确分类的样本总数占总样本数的比例.

$$Acc=\frac{TP+TN}{TP+FP+TN+FN} \tag{20}$$

(4) *F*1 分数 (*F*1), 它是用来衡量二分类问题模型精确度的一种指标, 是准确率和召回率的调和平均数.

$$F1=\frac{2TP}{2TP+FP+FN} \tag{21}$$

3.5 实验结果

本次实验运行环境及参数配置: 电脑 CPU 为 2.40 GHz, 内存为 8 GB, 操作系统为 Windows 10, 运算平台为 CUDA 11.0, 编程语言为 Python 3.7. 实验中经过反复测试, 基于注意力机制的 CNN-LSTM 模型中, CNN 层采用 ReLU 激活函数, 其中卷积层有 32 个卷积核, 大小设置为 1×3, 步长为 1, 池化层使用最大池化. LSTM 层的滑动窗口大小为 15, 单元数为 64, 训练次数 (epochs) 为 50, 批尺寸 (batch_size) 为 16, Dropout 比率为 0.2, 采用的损失函数为均方误差 (MSE).

本文采用基于注意力机制的 CNN-LSTM 模型进行异常数据检测, 对于不同的特征, 设置了不同的阈值. 表 3 列出了异常数据检测的结果, 可以看出:

(1) 在召回率结果上, 模型在航向角信息删除攻击下为 82.9%, 在其他攻击下均为 91% 以上.

(2) 在检测率结果上, 模型在航向角信息删除和路线替换攻击下分别为 61.4% 和 60.4%, 在其他攻击下均为 90% 以上.

(3) 在准确率结果上, 模型在航向角信息删除攻击下为 80.2%, 在其他攻击下均在 92% 以上.

(4) 在 *F*1 分数结果上, 模型在航向角信息删除攻击下为 0.88, 在其他攻击下均在 0.95 以上.

(5) 可以看出在大多数类型的攻击下, 模型都能够很好地检测出异常数据, 在高度偏移 (+/−)、速度偏移 (+/−) 4 种攻击下, 检测率均能达到 100%, 召回率和准确率也在 98% 以上, *F*1 分数超过 0.99, 表明模型能够很好地处理这几种类型的攻击.

(6) 模型在航向角信息删除攻击下, 召回率为 82.9%、检测率为 61.4%; 在航向角信息转向攻击下, 召回率为 91.9%, 检测率为 96.9%, 说明航向角信息相对其他信息的时间相关性相对较弱.

表 3 基于注意力机制的 CNN-LSTM 模型的异常检测结果

评价指标	速度信息删除	高度信息删除	航向角信息删除	速度高斯噪声	路线替换	航向角转向	高度偏移 (+)	高度偏移 (−)	速度偏移 (+)	速度偏移 (−)	平均值
召回率 (%)	98.5	98.3	82.9	93.2	97.5	91.9	98.2	98.2	98.7	98.7	95.61
检测率 (%)	90.0	95.0	61.4	94.4	60.4	96.9	100.0	100.0	100.0	100.0	89.80
准确率 (%)	97.4	97.9	80.2	93.4	92.8	92.5	98.4	98.4	98.9	98.9	94.88
*F*1分数	0.985	0.988	0.880	0.961	0.960	0.956	0.991	0.991	0.994	0.993	0.970

通过计算, 在这 10 种攻击下, 使用基于注意力机制的 CNN-LSTM 模型进行 ADS-B 异常数据检测, 平均召回率为 95.61%, 平均检测率为 89.8%, 平均准确率为 94.88%, 平均 *F*1 分数为 0.97.

3.6 对比实验及分析

此外, 为了验证模型性能, 本文选择了 7 种深度学习模型作为对比, 来检测在以上 10 种攻击下产生的异常数据. 包括 LSTM 模型、GRU 模型、基于注意力机制的 LSTM 模型、基于注意力机制的 GRU 模型、LSTM 编解码器模型、CNN-LSTM 模型和 CNN-GRU 模型进行对比实验. 表 4 给出了各模型和基于注意力机制的 CNN-LSTM 模型的召回率、检测率、准确率和 *F*1 分数的平均值. 可以看出:

(1) LSTM 模型和 GRU 模型的召回率、检测率、

准确率和 *F*1 分数较低. 这是因为这两种模型没有充分考虑 ADS-B 数据作为典型时间序列数据的相关特性.

(2) 将注意力机制引入到 LSTM 模型和 GRU 模型中, 可以发现模型的召回率、检测率、准确率和 *F*1 分数均得到了提升. 但是幅度并不大, 以 *F*1 分数为例, LSTM 模型和 GRU 模型分别提升了 0.8%、2.8%.

(3) 将 CNN 网络与 LSTM 模型、GRU 模型相结合, 相比较引入基于注意力机制, 模型的召回率、检测率、准确率和 *F*1 分数提升幅度更大. 以 *F*1 分数为例, LSTM 模型和 GRU 模型分别提升了 23.9%、6.3%.

(4) 与基于注意力机制的 LSTM 模型和 CNN-LSTM 模型相比, 基于注意力机制的 CNN-LSTM 模型的异常数据检测性能更好. 这是由于 CNN 网络能够有效提取数据特征, 引入注意力机制则能将网络权重分配到数据的重点区域, 解决由于 ADS-B 数据过长而忽略重要信息的情况, 提高检测精度.

(5) 与 LSTM 编解码器模型相比, 基于注意力机制的 CNN-LSTM 模型的异常数据检测性能更好. 因为 LSTM 编解码器模型忽略了 ADS-B 数据作为典型的跨时非线性依赖数据的分布特点, 基于注意力机制的 CNN-LSTM 模型具有更好的适应性, 异常数据检测效果更好.

表 4 各模型异常检测均值

评价指标	LSTM	GRU	基于注意力机制的LSTM	基于注意力机制的GRU	LSTM编解码器	CNN-LSTM	CNN-GRU	基于注意力机制的CNN-LSTM
召回率 (%)	59.9	74.2	60.7	74.8	82.3	92.3	86.2	95.6
检测率 (%)	91.1	88.8	91.6	91.5	87.6	86.5	83.4	89.8
准确率 (%)	63.8	76.0	64.6	77.2	83.0	91.5	85.8	94.9
*F*1分数	0.742	0.840	0.748	0.864	0.889	0.919	0.893	0.970

4 结论与展望

本文结合 ADS-B 数据的时间序列特点, 提出了基于注意力机制的 CNN-LSTM 模型, 用于异常数据检测, 将实验结果与其他 7 种模型进行对比. 结果表明基于注意力机制的 CNN-LSTM 模型的异常数据检测能力更好, 平均召回率达到 95.6%, 平均检测率达到 89.8%, 平均准确率达到 94.9%, 平均 *F*1 分数达到 0.97.

在未来的工作中, 将分 3 个方面继续努力: 第一, 将采用多特征学习的方法, 使模型的检测更加合理; 第二, 计划引入飞行规则, 通过验证数据的合理性, 辅助模型进行异常数据检测; 第三, 将结合常见攻击类型, 尝试采取更多类型的攻击, 以检测模型应对复杂攻击的能力.

参考文献

1 Li TY, Wang BH, Shang FT, *et al*. Dynamic temporal ADS-B data attack detection based on sHDP-HMM. Computers & Security, 2020, 93: 101789. [doi: 10.1016/j.cose.2020.101789]

2 邓晓波, 王飞, 杨光曜. 机载 ADS-B 技术现状与发展趋势. 航空工程进展, 2021, 12(1): 121–128. [doi: 10.16615/j.cnki.1674-8190.2021.01.016]

3 Costin A, Francillon A. Ghost in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices. Las Vegas: EURECOM, 2012. 1–10.

4 Schäfer M, Lenders V, Martinovic I. Experimental analysis of attacks on next generation air traffic communication. Proceedings of the 11th International Conference on Applied Cryptography and Network Security. Banff: Springer, 2013. 253–271. [doi: 10.1007/978-3-642-38980-1_16]

5 Yang HM, Zhou QX, Yao MX, *et al*. A practical and compatible cryptographic solution to ADS-B security. IEEE Internet of Things Journal, 2019, 6(2): 3322–3334. [doi: 10.1109/JIOT.2018.2882633]

6 Kacem T, Barreto A, Wijesekera D, *et al*. ADS-Bsec: A novel framework to secure ADS-B. ICT Express, 2017, 3(4): 160–163. [doi: 10.1016/j.icte.2017.11.006]

7 Lee SH, Kim YK, Han JW, *et al*. Protection method for data communication between ADS-B sensor and next-generation air traffic control systems. Information, 2014, 5(4): 622–633. [doi: 10.3390/info5040622]

8 Baek J, Hableel E, Byon YJ, *et al*. How to protect ADS-B: Confidentiality framework and efficient realization based on staged identity-based encryption. IEEE Transactions on Intelligent Transportation Systems, 2017, 18(3): 690–700. [doi: 10.1109/TITS.2016.2586301]

9 Wesson KD, Humphreys TE, Evans BL. Can cryptography secure next generation air traffic surveillance? http://radionavlab.ae.utexas.edu/images/stories/files/papers/adsb_for_submission.pdf. (2014-03-20).

10 Strohmeier M, Lenders V, Martinovic I. Intrusion detection for airborne communication using PHY-layer information. Proceedings of the 12th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment. Milan: Springer, 2015: 66–77. [doi: 10.1007/978-3-319-20550-2_4]

11 Strohmeier M, Martinovic I. On passive data link layer fingerprinting of aircraft transponders. Proceedings of the 1st ACM Workshop on Cyber-physical Systems-security and/or PrivaCy. Denver: ACM, 2015. 1–9. [doi: 10.1145/2808705.2808712]

12 Monteiro M. Detecting malicious ADS-B broadcasts using wide area multilateration. Proceedings of 2015 IEEE/AIAA 34th Digital Avionics Systems Conference (DASC). Prague: IEEE, 2015. 1–28. [doi: 10.1109/DASC.2015.7311579]

13 颜可壹, 吕泽均, 时宏伟, 等. 基于 TDOA/TSOA 的 ADS-B 系统防欺骗技术. 计算机应用研究, 2015, 32(8): 2272–2275. [doi: 10.3969/j.issn.1001-3695.2015.08.007]

14 Zhang T, Wu RB, Lai R, *et al*. Probability hypothesis density filter for radar systematic bias estimation aided by ADS-B. Signal Processing, 2016, 120: 280–287. [doi: 10.1016/j.sigpro.2015.09.012]

15 王布宏, 罗鹏, 李腾耀, 等. 基于粒子群优化多核支持向量数据描述的广播式自动相关监视异常数据检测模型. 电子与信息学报, 2020, 42(11): 2727–2734. [doi: 10.11999/JEIT190767]

16 王振昊, 王布宏. 基于 SVDD 的 ADS-B 异常数据检测. 河北大学学报 (自然科学版), 2019, 39(3): 323–329. [doi: 10.3969/j.issn.1000-1565.2019.03.015]

17 Cho T, Lee C, Choi S. Multi-sensor fusion with interacting multiple model filter for improved aircraft position accuracy. Sensors, 2013, 13(4): 4122–4137. [doi: 10.3390/s130404122]

18 Nanduri A, Sherry L. Anomaly detection in aircraft data using Recurrent Neural Networks (RNN). Proceedings of 2016 Integrated Communications Navigation and Surveillance. Herndon: IEEE, 2016. 5C2-1–5C2-8. [doi: 10.1109/ICNSURV.2016.7486356]

19 Li TY, Wang BH, Shang FT, *et al*. Online sequential attack detection for ADS-B data based on hierarchical temporal memory. Computers & Security, 2019, 87: 101599. [doi: 10.1016/j.cose.2019.101599]

20 Habler E, Shabtai A. Using LSTM encoder-decoder algorithm for detecting anomalous ADS-B messages. Computers & Security, 2018, 78: 155–173. [doi: 10.1016/j.cose.2018.07.004]

21 丁建立, 邹云开, 王静, 等. 基于深度学习的 ADS-B 异常数据检测模型. 航空学报, 2019, 40(12): 323220. [doi: 10.7527/S1000-6893.2019.23220]

22 罗鹏, 王布宏, 李腾耀. 基于 BiGRU-SVDD 的 ADS-B 异常数据检测模型. 航空学报, 2020, 41(10): 323878. [doi: 10.7527/S1000-6893.2020.23878]

23 Luo P, Wang BH, Li TY, *et al*. ADS-B anomaly data detection model based on VAE-SVDD. Computers & Security, 2021, 104: 102213. [doi: 10.1016/j.cose.2021.102213]

24 Wang ES, Song YS, Xu S, *et al*. ADS-B anomaly data detection model based on deep learning and difference of Gaussian approach. Transactions of Nanjing University of Aeronautics and Astronautics, 2020, 37(4): 550–561. [doi: 10.16356/j.1005-1120.2020.04.006]

25 McCallie D, Butts J, Mills R. Security analysis of the ADS-B implementation in the next generation air transportation system. International Journal of Critical Infrastructure Protection, 2011, 4(2): 78–87. [doi: 10.1016/j.ijcip.2011.06.001]

26 Wilhelm M, Martinovic I, Schmitt JB, *et al*. Short paper: Reactive jamming in wireless networks: How realistic is the threat? Proceedings of the 4th ACM Conference on Wireless Network Security. Hamburg: ACM, 2011. 47–52. [doi: 10.1145/1998412.1998422]

27 姚越, 刘达. 基于注意力机制的卷积神经网络-长短期记忆网络的短期风电功率预测. 现代电力, 2022, 39(2): 212–218. [doi: 10.19725/j.cnki.1007-2322.2021.0108]

(校对责编: 牛欣悦)