DOI: 10.13382/j.jemi.B2206167

基于 TimeGAN-LSTM 的无人机 GPS 欺骗干扰检测模型*

王路阳 孙一宸 于明鑫 李天放 董明利
(北京信息科技大学仪器科学与光电工程学院 北京 100192)

摘 要:针对无人机易受 GPS 欺骗干扰的问题,提出一种基于长短时记忆法(LSTM)的无人机全球定位系统(GPS)欺骗干扰检测模型。为了提高模型训练精度,首先利用时序生成对抗网络(TimeGAN)对训练数据集进行了数据增强工作,弥补了训练数据量的不足,还对比了增强数据集与原始数据集的性能差距。然后搭建了 LSTM 模型,在仿真实验下 TimeGAN+LSTM 模型获得的准确率、精确率、召回率和 F1 值分别为 98.08%、98.55%、98.07% 和 98.31%。最后与传统机器学习模型进行比较,对比结果证明,提出的欺骗干扰检测模型拥有更好的性能指标。该模型可实现对无人机 GPS 欺骗干扰信号的有效检测。

关键词: 无人机;GPS 欺骗干扰检测;深度学习;TimeGAN;LSTM
中图分类号: TN973 **文献标识码**: A **国家标准学科分类代码**: 510.40

UAV GPS spoofing detection model based on TimeGAN-LSTM

Wang Luyang Sun Yichen Yu Mingxin Li Tianfang Dong Mingli
(School of Instrument Science and Opto-Electronics Engineering, Beijing Information Science and Technology University, Beijing 100192, China)

Abstract: To address the problem that unmanned aerial vehicle (UAV) is vulnerable to GPS spoofing, an UAV GPS spoofing detection model based on long short-term memory (LSTM) is proposed. In order to improve the training accuracy of the model, the training dataset was firstly enhanced using time series generative adversarial networks (TimeGAN) to compensate for the lack of training data and to compare the performance difference between the enhanced dataset and the original dataset. The LSTM model was then built, and experimental results show that the accuracy, precision, recall and F1 value trained by the TimeGAN+LSTM model under simulation experiments are 98.08%, 98.55%, 98.07% and 98.31%. Finally, the comparison with the traditional machine learning model proves that the proposed spoofing detection model has better performance metrics. The model can achieve effective detection of UAV GPS spoofing signals.

Keywords: UAV; GPS spoofing detection; deep learning; TimeGAN; LSTM

0 引 言

近年来无人机发展迅速,在民用和军用领域应用广泛,民用领域包括物流[1-2]、物联网[3-4]、智慧城市应用[5]、地质测绘、灾害管控和紧急救援[6]等,值得一提的是,由于近几年新冠疫情在全球流行,无人机也被用于人群监控、公共场所消毒,以抑制新冠肺炎的流行和传播[7]。根据高盛公司的报告,截止至 2020 年,消费者无人机出货量已达到 780 万台,收入达到 33 亿美元。作为对比,2014 年商用无人机领域的出货量仅为 45 万台,收入为 7 亿美元,商业分析预测到 2025 年,全球无人机市场将增加到 500 多亿美元。此外,无人机还被应用于各种军事活动中,例如监视、目标跟踪、空对地战斗等,从 2017 年~2021 年,美国在无人机上的军费开支也逐年上升。可以肯定的是,无人机将在未来的社会中起到重要的作

收稿日期: 2022-12-29 Received Date: 2022-12-29
*基金项目:北京市教委科技计划一般项目(KM202011232007)、高校学科人才引进计划(D17021)、北京信息科技内涵发展项目(2019KYNH204)资助

用,有关无人机的技术也将快速发展[8-9]。

尽管无人机具有很多优点,但它们也存在安全隐患,即使是警用和军用的专业无人机也不可避免的存在一些安全漏洞[10],蓄意攻击者可能会利用这些安全漏洞发起攻击,无人机会被远程关闭、劫持甚至失控坠毁[11]。无人机的安全漏洞主要来自于其非常依赖全球定位系统(global positioning system, GPS)进行定位和导航,使得攻击者可伪造 GPS 信号来间接控制无人机[12],这与 GPS 信号极易被伪造和干扰息息相关[13-14]。攻击者往往使用功率更高的虚假 GPS 信号,再添加一些噪声信号以掩盖真实信号。由于大部分干扰设备都可以实时与 GPS 卫星时钟同步,所以无人机很容易锁定虚假的 GPS 信号,这时攻击者再操纵干扰设备不断发送虚假信号或者不断增加信号传播时延,从而使无人机偏离原有航线。

近几年,无人机被攻击与欺骗的事件不断增多,针对 GPS 的干扰与如何限制干扰的研究也逐渐增多。攻击者实施攻击时会采用不同的硬件与软件,实现对无人机攻击的方式有一定的差异化,但是攻击原理大多类似,基本分为两类:压制式与欺骗式。

压制式干扰(Jamming)指的是对一定范围内的无人机或其他使用 GPS 的设备发射大功率射频信号,使得真实信号完全淹没在射频干扰信号中,致使无人机丧失部分或者全部正常工作的能力[15-16]。对于没有搭载抗干扰技术的无人机而言,压制式干扰的影响往往是毁灭性的。在没有 GPS 定位的情况下,无人机的飞行方向和速度都将不受控制,很可能出现坠毁炸机的情况。但是由于压制式干扰的工作原理简单,针对其进行反制措施也比较容易,例如设定在无人机没有定位信号情况下不同的应对策略,所以现如今压制式干扰也不常被攻击者使用。

欺骗式干扰(Spoofing)[17-19]可以理解为对目标导航信号的拦截和重播,与压制式干扰不同,欺骗式干扰的功率水平与真实信号类似或者略高一点,信号格式与频谱结构与真实信号基本一样,目的在于扰乱无人机内部 GPS 接收器的码同步电路。欺骗式干扰相对于压制式干扰,被检测和预防的可能更小,目前主要分为两类:转发式欺骗干扰和生成式欺骗干扰[20]。

为了保护无人机免受各类针对 GPS 的攻击,减小对无人机飞行过程中的威胁,近几年也衍生了不同种类的反欺骗技术[21-23],用来最大程度检测 GPS 信号欺骗。

2016 年,Mead 等[24]开发了一种名为沙箱的硬件,用于监测 GPS 边界信号的异常波动,Ransathan 等[25]提出了一种可以检测出 GPS 攻击者位置的方法。2018 年,Kang 等[26]提出了一种使用单天线功率测量的方法,根据 GPS 年历与星历数据的波达角(direction of arrival, DOA)与测量的 DOA 之间的差异,检测欺骗信号。上述方法已被证明具有较好性能,但是共同的缺点是需要特殊的硬件设备,这明显会增加无人机的重量和成本。反欺骗系统不应具有较大的使用功率,这会严重影响无人机的续航里程,因此关于 GPS 反欺骗的传统方法都不适合轻便的无人机。

在针对无人机的反欺骗研究中,研究者建立了很多反欺骗机制,常用的检测信号攻击的手段有入侵检测系统(intrusion detection system, IDS)。2013 年,Mitchell 等[27]设计了一种 IDS 系统,根据固定阈值定义了信号的分类规则来分类欺骗信号和真实信号。2017 年,Sedjelmaci 等[28]也利用 IDS 系统设计了一种检测无人机网络异常威胁的方案,其中用来分类的阈值更加精细,但是基于固定阈值分类欺骗信号和真实信号的方法还是有很大的局限性,无法抵御更高级的欺骗攻击。2019 年,Eldosouky 等[29]建立了一种基于协作定位技术的 Stackelberg 博弈模型,在模型中,无人机操作员是防御者,GPS 欺骗者是攻击者,考虑攻击者与防御者相互作用的动态效果来实施反欺骗手段,但是仅限于博弈算法与概念,并不是反欺骗的实际技术手段。同年,Tedeschi 等[30]提出了一种基于组合导航的 JAM-ME 的辅助导航系统,当无人机检测到干扰攻击时,它会切换到 JAM-ME 模式,利用干扰信号定位干扰机,然后利用其位置计算与无人机的相对距离,建立辅助导航系统。

近几年随着计算机技术的发展,有关机器学习及其衍生技术也逐渐应用于各个领域,同样的,也有很多研究者利用机器学习更为灵活而精准的决策机制,应用于无人机反欺骗领域。2019 年,Semanjski 等[31]利用支持向量机(support vector machine, SVM)提出了一种检测全球导航卫星系统(global navigation satellite system, GNSS)欺骗信号的方法。同年,Arthur 等[32]使用 SVM 建立了一个轻量化 IDS 系统,能保证欺骗信号的高检测率。2021 年,Shafique 等[33]提出了一种基于 SVM 的无人机欺骗信号检测机制,并且对比了其他几种机器学习方法,还加入训练数据的特征分析,保证欺骗检测模型的准确率。虽然在无人机 GPS 反欺骗领域中,采用机器学习方法相较于传统方法性能表现更为优异,但是所使用的机器学习算法较为简单,而无人机真实飞行环境复杂,往往需要更高级的算法对其进行处理,如深度学习方法,文献[33]中也提到深度学习是该领域未来的发展方向。

在无人机反欺骗领域,近两年也逐渐出现深度学习方法的应用。2020 年,Borhani-Darian 等[34]讨论了深度学习方法在 GNSS 欺骗检测中的应用,涉及到一个多层感知器(multi-layer perceptron)和两类卷积神经网络(convolution neural networks),并且在模拟数据上进行了性能验证。2021 年,Jayaweera[35]提出了一种使用卷积神经网络的 GPS 反欺骗技术,使用 GPS 卫星信号的 DOA 时间序列作为输入,准确率可以达到 95%。有关无人机

反欺骗领域的解决方案会更多的应用到深度学习,并且研究者们的相关工作还未完全展开,使用的训练数据集多为公开或仿真数据集且输入特征维度较少。

本文提出了一种无人机 GPS 欺骗干扰检测模型,使用复合翼无人机采集真实环境中的欺骗干扰数据,采用皮尔逊相关系数进行数据降维、特征筛选,利用时序生成对抗网络(time series generative adversrial networks, TimeGAN)进行数据增强,建立基于深度学习长短时记忆法(long short-term memory, LSTM)的欺骗干扰检测模型,采用 K 折交叉验证法与混淆矩阵中二级指标:准确率、精确率、召回率和三级指标 F1 值作为评估方法,得到的结果与几种经典的机器学习模型进行了对比。

本文的主要贡献如下:1) 提出一种基于 LSTM 的无人机 GPS 欺骗检测模型,其中欺骗干扰数据集是使用无人机采集的真实数据集。2) 利用 TimeGAN 对数据集进行数据增强工作。3) 与主流的几种机器学习模型进行了对比,证明深度学习模型 LSTM 对本文工作的优越性。

1　数据采集与预处理

1.1　硬件系统

如图 1 所示,本文选用纵横大鹏公司的复合翼无人机 CW-10Ⅱ 作为实验采集数据的无人机。复合翼无人机相比旋翼无人机,飞行状态更加稳定、迅速,飞行过程中受到环境因素的干扰相比旋翼无人机也更小,且复合翼无人机具有固定翼没有的旋翼起飞功能,这使得数据采集更加安全、便捷,为后续数据分析提供了良好的基础。

图 1　CW10-Ⅱ 复合翼无人机

Fig. 1　CW10-Ⅱ composite wing UAV

CW-10Ⅱ 具体参数如下:续航时间 90 min,抗风能力 6 级,实验时起飞高度为 100 ~ 150 m,飞行速度为 23 m/s,同时也有 12 kg 的起飞重量与 2 kg 的任务载荷。

欺骗干扰实验选用的湖南矩阵电子科技公司某型号干扰机如图 2 所示。该干扰机具体参数如下:信号功率动态范围大于 40 dB,信号干扰范围为全向 360°,半径可调节范围为 0~300 m,可以提供 16 通道 GPS:L1 规模的欺骗信号,能满足实验时所需的复杂电磁测试环境。

图 2　湖南矩阵科技有限公司某型号干扰机

Fig. 2　Hunan matrix technology Co., Ltd. a model of jammer machine

1.2　数据采集

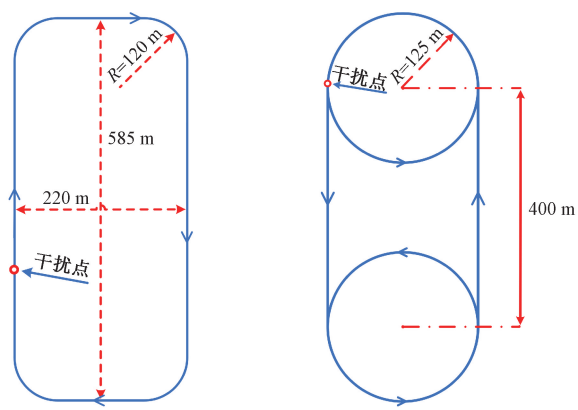
为了保证无人机采集干扰数据时不受环境因素影响,实验需要在天气良好的情况下采集数据,实验时的具体天气情况如表 1 所示。

表 1　外场实验天气情况

Table 1　Weather conditions for field experiments

日期	天气	气温/℃	风速
2021. 12. 27	晴	-8	3 级
2021. 12. 28	晴	-5	3 级
2021. 12. 29	晴	-5	4 级

无人机飞行路径设置为直线、圆形、弧形等不同形状的飞行路径,实验时的飞行路径和干扰机位置如图 3 所示。



(a) 实验飞行路径1　(b) 实验飞行路径2

(a) Experimental flight path 1　(b) Experimental flight path 2

图 3　实验飞行路径

Fig. 3　Experimental flight path

无人机执行飞行任务时会设置不同的飞行状态,一般分为匀速飞行和变速飞行,具体干扰情况与飞行状态如表 2 所示。干扰机干扰模式为定向 GPS 欺骗干扰,偏移速度为 2~3 m/s。

表 2　无人机飞行计划

Table 2　UAV flight plan

日期	干扰情况	飞行路径
2021. 12. 27	否	路径 1
2021. 12. 27	是	路径 1
2021. 12. 28	是	路径 2
2021. 12. 28	否	路径 2
2021. 12. 29	是	路径 1
2021. 12. 29	是	路径 2

1.3　数据预处理

采集的真实数据样本需要对数据进行清洗与筛选，在去除明显和无人机飞行状态、干扰状态无相关性的数据后，剩余 36 个特征数据，每个特征包括 1 824 项数据值，其中无人机受到干扰时的样本为 785 项，正常飞行数据为 1 039 项，36 个特征数据名称及对应含义如表 3 所示。

表 3　特征名称及含义

Table 3　Feature name and meaning

特征名称	特征含义
gpsPdop	GPS 位置精度
gpsNumSv	GPS 卫星数
Itow	GPS 时间
gpsSec	GPS 走秒
P_Sol_Status	GPS 导航解算状态
Avionics Temp	电路板温度
Cmd	动力指令
Lat	纬度
Lon	经度
H	高度
Tas	空速测量值
Eu[0]	滚转欧拉角
Eu[1]	偏航欧拉角
Eu[2]	俯仰欧拉角
Pqr[0]	*X* 轴角速度
Pqr[1]	*Y* 轴角速度
Pqr[2]	*Z* 轴角速度
InertVNED[0]	北向地速
InertVNED[1]	东向地速
InertVNED[2]	地向速度
Compass	罗盘
Acc[0]	*X* 轴加速度
Acc[1]	*Y* 轴加速度
Acc[2]	*Z* 轴加速度
XaccBias[0]	*X* 轴加速度偏差
YaccBias[0]	*Y* 轴加速度偏差
ZaccBias[0]	*Z* 轴加速度偏差
XMagField	*X* 磁场强度
YMagField	*Y* 磁场强度
ZMagField	*Z* 磁场强度
Static Press	静压
Dynamic Press	动压
Air Height	飞机气压高度
SouthWind	南风
WestWind	西风
Spoofing	欺骗干扰

之后根据数据采集时记录的干扰时间，对采集数据进行欺骗干扰数据标注，无人机受到干扰时的数据标注为 Spoofing = 1，未受干扰的数据标注为 Spoofing = 0，这部分工作也为后续建模提供了输入与输出的特征数据。然后分析数据相关性，相关性分析采用皮尔逊相关系数，如式(1)所示：

$$r_{x,y}=\frac{\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i-\bar{x})^2}\sqrt{\sum_{i=1}^{n}(y_i-\bar{y})^2}} \tag{1}$$

式中：n 为样本容量，x_i 和 y_i 为本项工作中设置的输入和输出，$\bar{x}$ 和 $\bar{y}$ 为输入与输出平均值。

通过皮尔逊相关系数方法筛选出了与欺骗干扰(Spoofing)相关的 15 个特征数据，数据包括：gpsNumSv(GPS 卫星数)、P_Sol_Status(GPS 导航解算状态)、cmd(动力指令)、Lat(纬度)、Lon(经度)、InertVNED[0](北向地速)、InertVNED[1](东向地速)、InertVNED[2](地向速度)、XaccBias(*X* 轴加速度偏差)、YaccBias(*Y* 轴加速度偏差)、ZaccBias(*Z* 轴加速度偏差)、AirHeight(飞机气压高度)、WWest(西风速度)、WSouth(南风速度)、Acc[1](*X* 轴加速度)、Spoofing(欺骗干扰)。前 15 个特征数据作为无人机 GPS 欺骗干扰检测模型的输入，而 Spoofing 作为输出，皮尔逊相关系数可视化热图如图 4 所示。

1.4　TimeGAN 增强数据

为解决因训练样本数据量小引起的模型过拟合或欠拟合问题，本文采用 TimeGAN 模型对欺骗数据进行扩充。TimeGAN 是生成对抗网络(generative adversrial networks，GAN)的分支[36]，结合了无监督学习的灵活性和监督训练提供的控制，允许对网络进行更精细的动态调整。一般 GAN 的主体为一个对抗模块，对抗模块由两个神经网络组成：生成器(Generator)和鉴别器(Discriminator)，使用这两个神经网络通过生成数据和真实数据不断对比，优化生成数据质量，其中式(2)为评估生成器和鉴别器的价值函数：

$$\mathcal{L}_U=\mathbb{E}_{s,x_{1:t}\sim p}\left[\|s-\tilde{s}\|_2+\sum_t\|x_t-\tilde{x}\|_2\right] \tag{2}$$

式中：$s,x_{1:t}$ 为原始数据集，$\tilde{s},\tilde{x}$ 为原始数据集的重构形式，p 为原始数据对应的条件分布。

TimeGAN 网络除了具有一般 GAN 的对抗模块，还有一个自编码模块[37]。自编码模块主要作用是数据降维，该模块有内嵌函数(embedding function)和恢复函数(recovery function)构成的两个神经网络，两者由隐藏函数连接，内嵌函数通过隐藏函数(latent codes)将数据转换为 $h(h\in\mathcal{H})$，之后输入给鉴别器进行数据选择，再由恢复函数进行逆变换，最终输出增强后的数据集。在

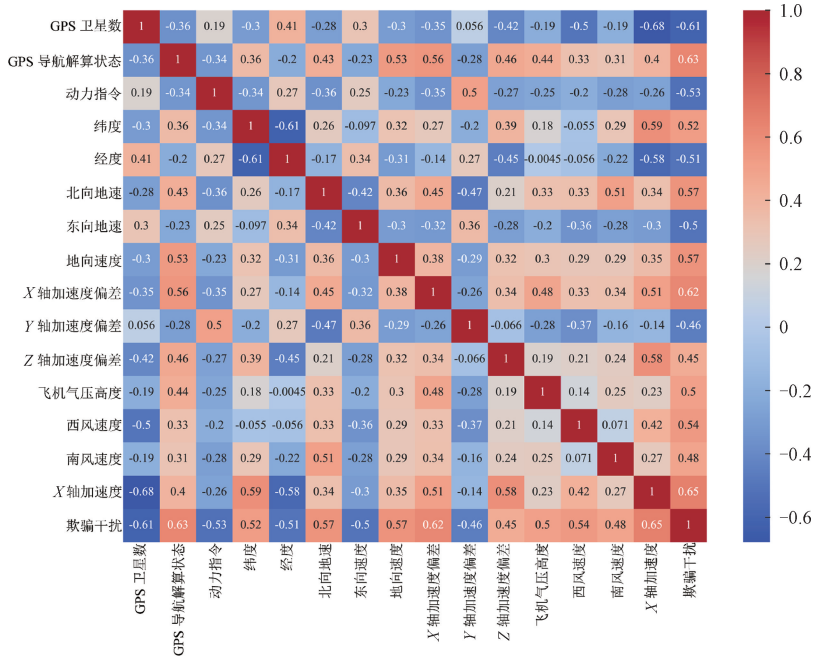


图 4　数据相关性热图

Fig. 4　Data correlation heat map

TimeGAN 中，由式(3)评估内嵌函数和恢复函数组成神经网络：

$$\mathcal{L}_R = \mathbb{E}_{x_1:t\sim p}\left[\sum_t \| x_t - r(e)(x_t)) \|_2\right] \tag{3}$$

式中：r 是恢复函数，e 是内嵌函数。

生成与时间相关的数据对于 GAN 本来就很困难，尤其是输入数据还具有多特征长序列的特点。为了将数据间的时间关系引入到学习架构中，TimeGAN 使用了基于自回归学习算法的监督损失函数，以便 GAN 网络能够引入时间条件概率，TimeGAN 生成数据的示意图如图 5 所示。

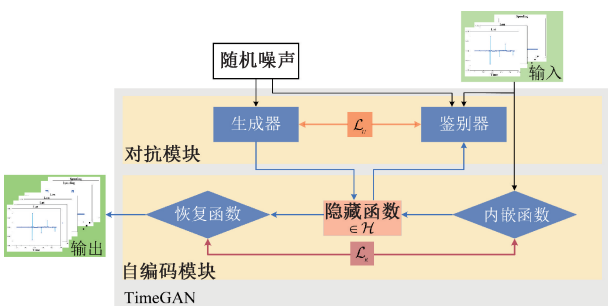


图 5　TimeGAN 生成数据示意图

Fig. 5　TimeGAN generate data schematic

本文中采集的真实数据集均为时序数据，它是由无人机在飞行过程中传感器每秒反馈的参数组成的，所以数据集中的数据具有多特征时序长序列的特点，因此采集的真实数据集非常符合 TimeGAN 增强数据的适用范围。

在原始数据集输入 TimeGAN 训练前还需对数据进行一定步长 n 的切片，使数据变成三维数据。这个过程可看作对数据进行不同程度的分组，而生成过程便是以每一个分组的数据进行训练生成，这样的预处理也将决定扩充数据的倍数。由于原始数据集大小不同，不同的切片数量也将一定程度上决定扩充数据集的质量。本文中所用到的切片数分别为 5、10、24，对应扩充后还原成二维后的每个特征包含的数据的样本容量为 9 095 条、18 190 条、43 656 条，其中，步长 $n=5$ 时，TimeGAN 切片处理数据示意图如图 6 所示。

对数据切片后，会统一对数据进行归一化处理[38]，这有益于减少模型训练时间，提升训练精度。选用的归一化方法为最大最小值归一化，如式(4)所示，缩放范围为(0,1)，相比于均值标准化，最大最小值归一化更适合于时序数据以及最值较少的数据。

$$x' = \frac{\bar{x} - \min(x)}{\max(x) - \min(x)} \tag{4}$$

式中：$\bar{x}$ 为样本平均值，$\min(x)$ 为样本容量中自变量 x 的最小值，$\max(x)$ 为样本容量中自变量 x 的最大值。

最后，为了保证切片后数据的相对独立性，在数据生成之前，会将已经分割好的切片数据打乱顺序，输入 TimeGAN 中生成数据。

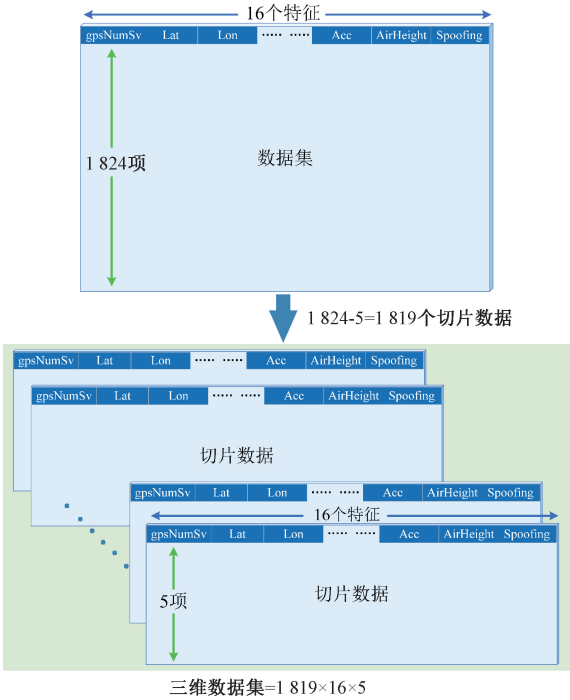


图 6　TimeGAN 切片数据处理示意图

Fig. 6　TimeGAN data slicing processing schematic

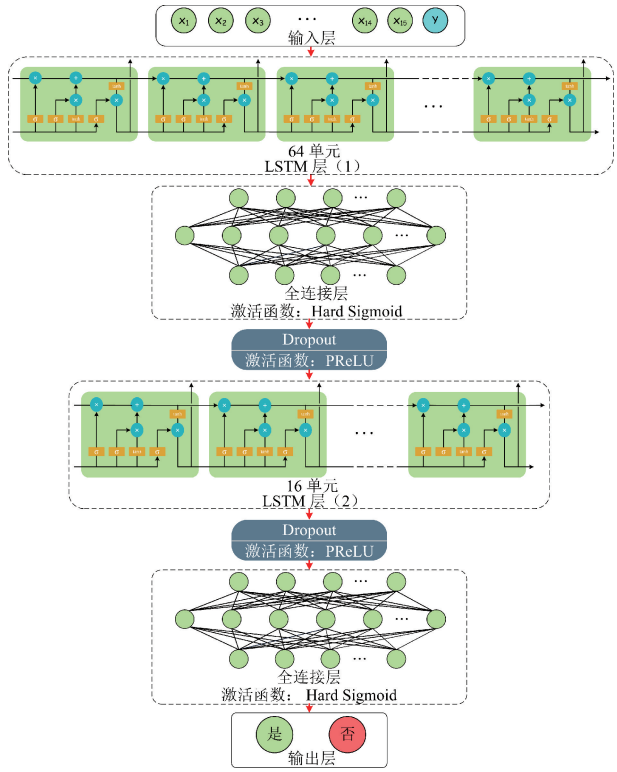


图 7　无人机 GPS 欺骗检测模型结构

Fig. 7　UAV GPS spoofing detection model structure diagram

2　建立无人机欺骗干扰模型

LSTM 在处理和预测时间序列相关的数据方面要优于大部分神经网络，而本文中模型的训练数据集全部为时序数据。由于 LSTM 本身具有的复杂非线性结构，使得 LSTM 适合构造大型深度神经网络，并且处理系统的异常检测也有较为优异的性能，在本文工作中，需要根据无人机输入的特征数据对无人机受干扰状态进行分类，也属于系统的异常检测。LSTM 加全连接层（Dense）的搭配也常用于时序数据的分类工作。因此选用 LSTM 作为本文搭建无人机 GPS 信号欺骗检测模型的深度学习模型。模型中包括两个 LSTM 层，两个 Dropout 层及两个全连接层，整体结构如图 7 所示。为了优化模型性能，提升模型鲁棒性和泛化性，在每个 LSTM 层后搭配了 Dropout 层，还使用了全连接层作为分类器提升模型分类性能，并且对应调整了各自的激活函数，模型的特征输入为预处理后的 15 个特征，输出特征 Spoofing 的值，也就是无人机的受干扰状态（是否被干扰）。

2.1　LSTM 神经网络

LSTM 是一种特殊的循环神经网络（recurrent neural network，RNN）模型，由于标准的 RNN 存在梯度消失或者梯度爆炸的问题，为了解决这些问题衍生出了 LSTM[39]，一个普通的 LSTM 单元由一个记忆单元、输入门、输出门和遗忘门组成，其中还包括 Sigmoid 和 Tanh 激活函数，它将时间序列数据的时间相关性存储在记忆单元中来进行处理，LSTM 的每个神经元可由式（5）~（10）描述。

$$\boldsymbol{X}=\begin{bmatrix}h_{t-1}\\ x_t\end{bmatrix} \tag{5}$$

$$f_t=\sigma(\boldsymbol{W}_f\cdot\boldsymbol{X}+b_f) \tag{6}$$

$$i_t=\sigma(\boldsymbol{W}_i\cdot\boldsymbol{X}+b_i) \tag{7}$$

$$o_t=\sigma(\boldsymbol{W}_o\cdot\boldsymbol{X}+b_o) \tag{8}$$

$$c_t=f_t\odot c_{t-1}+i_t\odot\tanh(W_c\cdot X+b_c) \tag{9}$$

$$\boldsymbol{h}_t=o_t\odot\tanh(c_t) \tag{10}$$

式中：$W_i, W_f, W_o\in\mathbb{R}^{d\times 2d}$ 为加权矩阵，$b_i, b_f, b_o, \in\mathbb{R}^{d}$ 为 LSTM 在训练期间要学习的偏差值，分别为输入门、遗忘门和输出门的偏差，σ 为 Sigmoid 激活函数，tanh 为 Tanh 激活函数，$\odot$ 为逐元素乘法，x_t 为 LSTM 单元的输入，$\boldsymbol{h}_t$ 为隐藏层向量。

2.2　模型训练

在本文中模型训练与评估采用端到端整体训练的方法。采用的语言为 Python 3.9、深度学习框架为 Keras 2.9.0、GPU 为 Nvidia GTX 1080 Ti、CPU 为 Intel Core i7-10700K、操作系统为 Windows 10。

训练过程中需要使用激活函数来提高模型精度。激活函数的作用是向模型中引入一些非线性参量，这样可

以避免模型中单纯的线性组合,因为模型在真实环境中遇到的情况可能更加复杂多样,数据之间的关系往往不是线性可分的,通过激活函数引入的非线性参量让数据能够更好的被分类。

式(11)为模型中 Dropout 层搭配的激活函数 PReLU,PReLU 相比于 ReLU 进行了一定的参数修正,式(12)为激活函数 ReLU,两种激活函数如图 8 所示,与 Dropout 层搭配,能更好地防止模型的过拟合。

$$\mathrm{ReLU}=\begin{cases}x & x>0\\ 0 & x\leqslant 0\end{cases} \tag{11}$$

$$\mathrm{PReLU}=\begin{cases}x & x>0\\ ax & x\leqslant 0\end{cases} \tag{12}$$

式中:a 为一个不为 0 的常数。

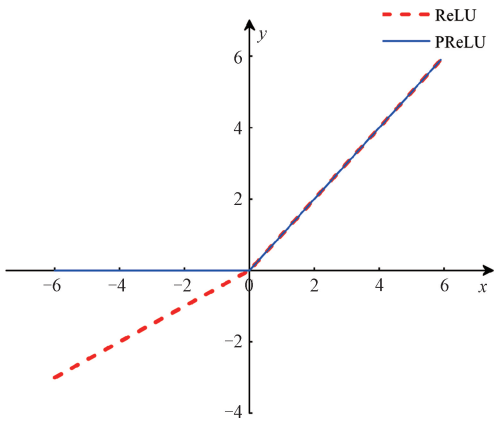


图 8　ReLU 与 PReLU 函数图

Fig. 8　ReLU and PReLU function diagram

式(13)为激活函数 Sigmoid,式(14)为全连接层使用的激活函数 Hard Sigmoid,在二分类工作中 Sigmoid 激活函数相比于其他激活函数更具优势,而 Hard Sigmoid 相对于 Sigmoid 进一步提升了计算效率,在保证模型性能的前提下使模型训练更加迅速,两个全连接层提升了整个模型的鲁棒性,两种激活函数如图 9 所示。

$$\mathrm{Sigmoid}=\frac{1}{1+\mathrm{e}^{-x}} \tag{13}$$

$$\mathrm{Hard-Sigmoid}=\begin{cases}0 & x<-2.5\\ 0.2x+0.5 & -2.5\leqslant x\leqslant 2.5\\ 1 & x>2.5\end{cases} \tag{14}$$

本文提出的 LSTM 模型结构与参数信息,包括模型每层的输出维度和参数数量如表 4 所示。

整体模型的超参数,如迭代次数(Epochs)、学习率(learning rate)等对提升模型精度起着至关重要的作用。训练时使用试错法寻找最优超参数,如表 5 所示,并使用 Adam 优化器以确保训练模型时不存在过拟合或欠拟合等问题。损失函数选用二元交叉熵(binary crossentropy),对于二分类问题效果会更好,式(15)为二元交叉熵。

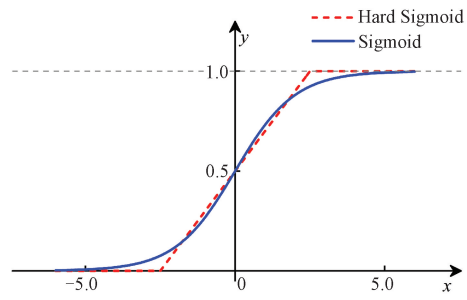


图 9　Sigmoid 与 Hard-Sigmoid 函数图

Fig. 9　Sigmoid and Hard-Sigmoid function diagram

表 4　LSTM 模型摘要

Table 4　LSTM model summary

层结构	输出维度	参数数量
LSTM (1)	(1,64)	20 480
Activation	(1,64)	/
Dropout	(1,64)	/
Dense (1)	(16)	5 200
LSTM (2)	(1,16)	5 184
Activation	(1,16)	/
Dropout	(1,16)	/
Dense (2)	(2)	152

$$Loss=-\frac{1}{N}\sum_{i=1}^{N}y_i\log(p(y_i))+(1-y_i)\cdot\log(1-p(y_i)) \tag{15}$$

式中:y_i 为[0,1]二元标签,$p(y_i)$ 是输出属于 y 标签的概率。

表 5　LSTM 模型超参数

Table 5　LSTM model hyperparameters

超参数名称	值
Dropout (1)	0.5
Dropout (2)	0.5
Batch size	4
Epochs	100
Learning rate	0.001

3　结果及分析

3.1　评估方法

混淆矩阵是一个二维矩阵,多用于评价分类器的优劣,是用于评价分类模型中的一种常见方法,其中 4 种计算模型性能指标包括正样本预测正确数目(true positive, TP)、正样本预测错误数目(false positive, FP)、负样本预测正确数目(true negative, TN),负样本预测错误数目(false negative, FN),混淆矩阵如表 6 所示。

表 6　混淆矩阵

Table 6　Confusion Matrix

	预测为真实信号	预测为欺骗信号
实际为真实信号	TP	FN
实际为欺骗信号	FP	TN

在评估模型性能时，为了使评估结果更加直观，通常会根据混淆矩阵计算二级指标：准确率、精确率、召回率，和三级指标 F1 值，从而更加直观的看出模型性能。

准确率（Accuracy）通常是最常见的评价指标，其含义为分类正确的样本数目占全部样本数目的百分比，准确率如式（16）所示。

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \tag{16}$$

精确率（Precision）是指预测结果为正样本中含有真实正样本的数目，精确率如式（17）所示。

$$\text{Precision} = \frac{TP}{TP + FP} \tag{17}$$

召回率（Recall）是指样本容量中的正样本预测正确的数目，召回率如式（18）所示。

$$\text{Recall} = \frac{TP}{TP + FN} \tag{18}$$

由于精确率和召回率有时候会出现负相关的情况，所以需要引入 F1 值来进一步评价模型性能，F1 值是由精确率和召回率计算得到的，是两者的加权调和平均，F1 值如式（19）所示。

$$\text{F1} = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{19}$$

3.2　K 折交叉验证

在评估机器学习与深度学习的模型性能时，通常会用到 K 折交叉验证法，这是一种重采样方法，用于在有限的数据样本中评估机器学习模型。此外，在使用 K 折交叉验证法时，不会随机打乱数据集，保证时序数据之间的时间信息不会丢失，并且在评估属于最大似然估计法的模型时还能避免因为训练次数导致的精度不一致问题。

对于具体的 K 值选择，要根据数据集的情况来确定，通常情况下 K 值越大意味着对数据集训练与测试越充分，但也并不意味着 K 值越高越好，因为对于时序数据来说，过高的 K 值可能会抵消数据之间的时间信息。

在本文中为了保证训练出的模型能更好地适应无人机真实的飞行环境、得到的验证结果更具有说服力，在 K 折交叉验证中使用的验证集均为 1.3 节中提到的原始数据集，样本容量为 1 824 项，所以为了保证模型拥有较好性能，选择 $K=5$，这样平均每份验证集约为 365 项数据，再将剩余 4 折原始数据使用 TimeGAN 进行数据扩容后作为模型的训练集，在充分测试数据的同时也能较好的保有数据之间的时间信息。

本文选用的 5 折交叉验证法示意图如图 10 所示，首先将真实数据集顺序分为 5 个部分，分别命名为 1 折、2 折、3 折、4 折和 5 折。使用 TimeGAN 对每一部分数据集分别进行扩充，分别为生成 1、生成 2、生成 3、生成 4 和生成 5。

每次训练时，选择其中一个原始数据集作为验证集，剩余的数据集作为训练集。例如，第 1 次训练时，利用 5 折作为验证集，其余的真实数据集与扩充数据集作为训练集，以此类推，重复 5 次。

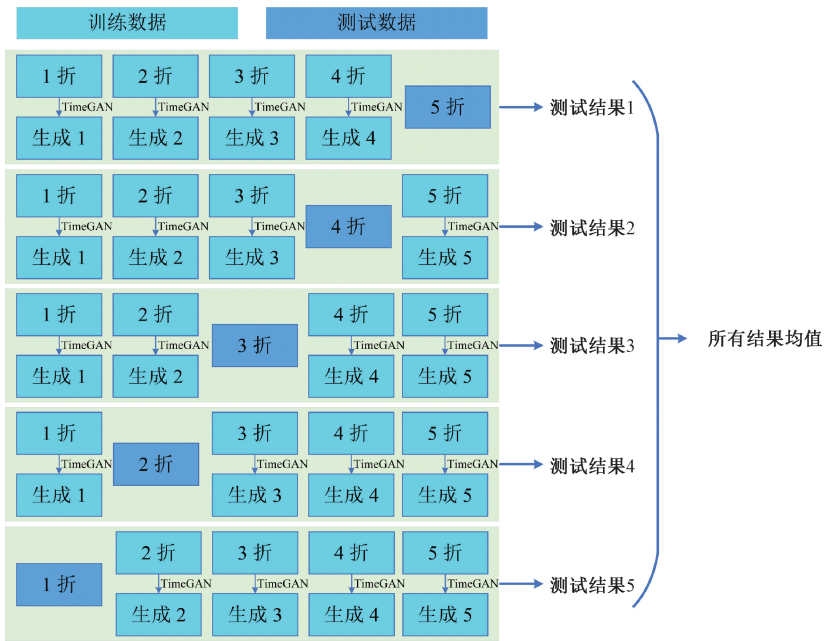


图 10　K 折交叉验证图

Fig. 10　K-fold cross-validation method schematic

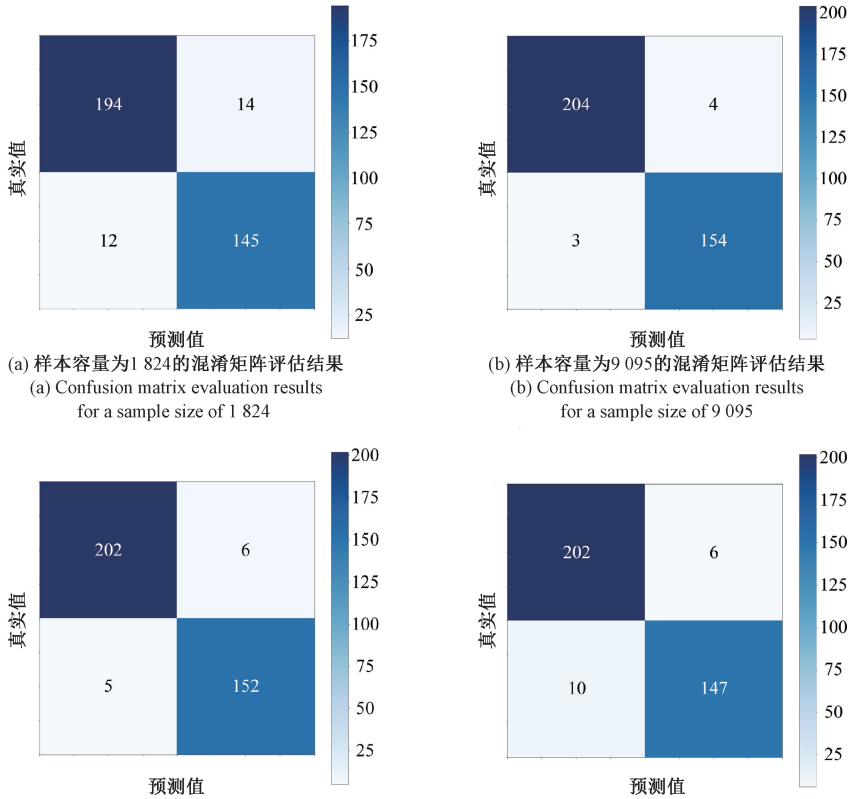
训练完成后,将 5 折交叉验证法得到的混淆矩阵对应元素进行平均,得到 TP、FP、TN、FN 的平均值(TP)、(FP)、(TN)、(FN),利用混淆矩阵均值结果评估模型性能。

3.3　评估结果

在评估 LSTM 模型性能时,选择 5 折交叉验证法的验证集均为原始数据集的平均分配,且数据顺序未经过随机打乱,这是为了保留原始数据集中的时间信息,同时还能测试模型在原始数据集中的泛化和表征能力。在测试 LSTM 模型时还会对 1.4 节中 TimeGAN 生成的 3 种不同样本容量(9 095、18 190、43 656)的数据集分别进行评估。

作为对比,还需测试 LSTM 模型在样本容量为 1 824 的原始数据集中的表现,评估方法与指标保持一致。

本文中使用 5 折交叉验证法评估 4 种样本容量的 LSTM 模型的混淆矩阵评估结果如图 11 所示。



(a) 样本容量为1 824的混淆矩阵评估结果
(a) Confusion matrix evaluation results for a sample size of 1 824

(b) 样本容量为9 095的混淆矩阵评估结果
(b) Confusion matrix evaluation results for a sample size of 9 095

(c) 样本容量为18 190的混淆矩阵评估结果
(c) Confusion matrix evaluation results for a sample size of 18 190

(d) 样本容量为43 656的混淆矩阵评估结果
(d) Confusion matrix evaluation results for a sample size of 43 656

图 11　4 种样本容量的 LSTM 模型混淆矩阵评估结果

Fig. 11　Confusion matrix evaluation results for LSTM models with 4 sample sizes

由实验产生的混淆矩阵结果对比可得,提出的 LSTM 模型对无人机 GPS 欺骗干扰信号做到有效识别的同时,对正确信号的误识别概率也能得到控制,而经过数据增强后的结果中 FP 与 FN 都得到了较好的控制。由混淆矩阵计算的二级指标准确率、精确率、召回率与三级指标 F1 值的均值结果如表 7 所示。

由实验结果可得,在验证集完全相同的情况下,经过数据增强后的数据集的模型性能表现均好于样本容量为 1 824 项的真实数据集,且模型性能有了显著的提升,这说明用 TimeGAN 增强数据集的方式确实能够提升 LSTM 模型性能,方法具有可行性。

表 7　LSTM 模型 4 种指标评估结果 s

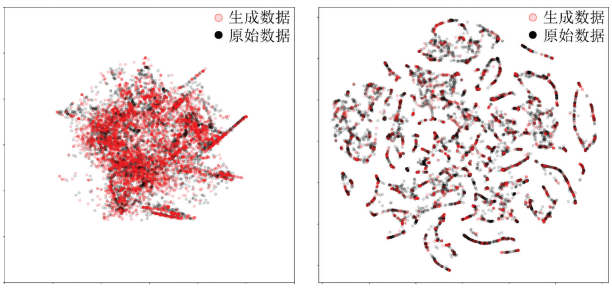
Table 7　Results of the evaluation of the four metrics of the LSTM model

样本容量	准确率/%	精确率/%	召回率/%	F1 值/%
1 824	92.88	94.17	93.27	93.72
9 095	98.08	98.55	98.07	98.31
18 190	96.99	97.58	97.12	97.35
43 656	95.62	95.28	97.12	96.19

在增强数据集的评估结果中,样本容量为 9 095 项的数据集相比于其他两种样本容量的数据集,模型综合表现最好。样本容量为 18 190 项的数据集的表现也要好于样本容量为 43 656 项的数据集,这证明在 1.4 节中

提到的切片数量会影响数据集质量,生成数据集的样本容量变大的同时,数据质量也会变差。

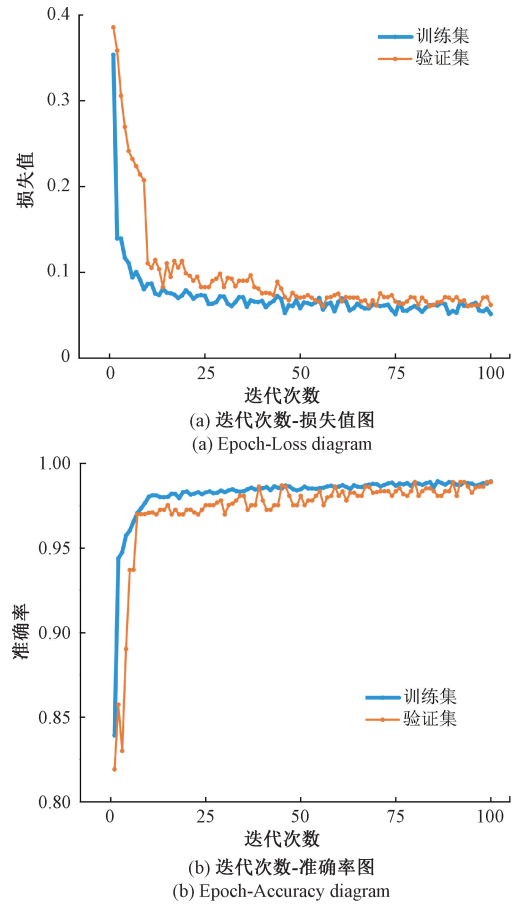
基于以上对增强数据集的对比与评估,选择样本容量为 9 095 的数据集作为训练 LSTM 模型以及后续对比几种机器学习的训练集。为了评估生成数据集质量,还使用了可视化主成分分析(principal components analysis, PCA)与 T 分布随机近邻嵌入(T-distribution stochastic neighbour embedding, T-SNE)绘制出生成数据与原始数据的分布情况对比,更能直观看出生成数据和原始数据的近似程度,两种实验的分布可视化示意图如图 12 所示,可以观察到使用 TimeGAN 生成的数据集与原始数据分布区域相仿,重叠程度较好。



(a) PCA实验结果　(b) TSNE实验结果
(a) PCA Experimental results　(b) TSNE Experimental results

图 12　生成数据与原始数据分布可视化示意图

Fig. 12　Visualization of the distribution of the generated data and the original data



(a) 迭代次数-损失值图
(a) Epoch-Loss diagram

(b) 迭代次数-准确率图
(b) Epoch-Accuracy diagram

图 13　LSTM 模型训练图

Fig. 13　LSTM model training diagram

利用样本容量为 9 095 项的数据集训练 LSTM 模型时的迭代次数-损失值图和迭代次数-准确率图如图 13(a)所示,由训练结果曲线可知,验证集中的损失值开始随着迭代次数的增大而急剧下降,并且趋近于训练集中的损失值,说明模型没有出现欠拟合情况,而后续迭代次数的增长,验证集和训练集的损失值也趋于收敛,相邻迭代次数的跳变幅度小于 0.05,证明模型没有出现过拟合情况。而图 13(b)中能也看出最终得到的准确率结果在训练过程中趋于收敛,准确率在 98% 附近,模型性能优异。

使用 TimeGAN 增强数据集训练的 LSTM 模型,在未打乱顺序的原始数据验证集中有较高的性能指标,也能说明该模型可以在真实环境中有优异的表现,具有较好的泛化能力。

3.4　机器学习模型性能对比

本文选择的深度学习模型 LSTM 对时序数据处理具有优异的性能,而机器学习对于处理二分类问题也已经非常成熟,所以本文也选择了 3 种经典的机器学习模型作为对比:SVM、朴素贝叶斯(naive Bayes, NB)、决策树(decision tree, DT)。

SVM 是一种通过学习训练集中的不同特征的数据,将预测分为不同类别的分类器,是一种十分经典的机器学习模型,随着 SVM 不断发展,较为常用的有 4 种核函数:Sigmoid、Linear、rbf、Poly,本文针对这 4 种不同的核函数会依次实验,验证其性能。

NB 是一个条件概率模型,是利用概率统计知识进行分类的算法,其优点就是能使用较少的参数和训练数据达到相对优秀的性能,但是面对复杂情况,这可能也是其缺点,但 NB 依旧是主流的分类器,在大部分情况下表现的很好。

DT 是一种监督学习技术,用于分类和回归问题非常成熟,多数情况下还是用作分类问题,是一种树状结构的分类器,分为根节点和叶节点,根据输入不同的特征数据,决策树给出不同的分类结果(是或否),来判断是否生成子树继续分类,对于本文中的多特征数据输入的二分类问题,具有适用性。

实验中采用与 LSTM 模型同样的训练集与测试集分别对 SVM、NB、DT 3 种机器学习模型进行训练与评估,在训练机器学习模型时,选择网格搜索法(grid search)确定每个机器学习最优的超参数,以发挥各种模型的最佳性能,经过网格搜索法筛选后的机器学习模型超参数如

表 8 所示。

表 8　机器学习超参数

Table 8　Machine learning hyperparameters

模型	核函数	超参数	
SVM	Sigmoid	C = 100	gamma = 1
	Linear	C = 100	gamma = 1
	rbf	C = 1 000	gamma = 0.01
	Poly	C = 10	degree = 3
NB	–	–	
DT	–	criterion = entropy	splitter = best
		max_depth = 15	max_leaf_nodes = None

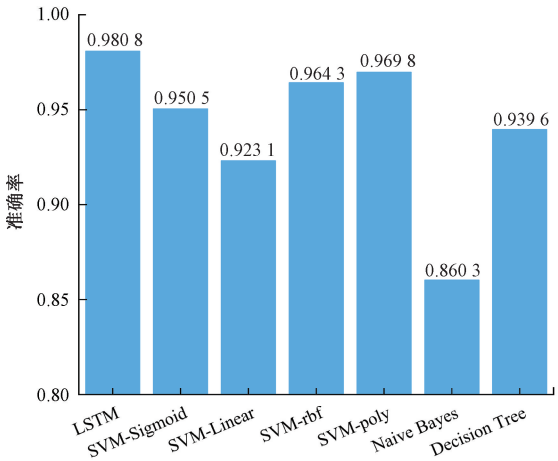
针对以上几种机器学习的 5 折交叉验证的均值结果如表 9 所示。由实验结果可以看出，对于没有超参数的 NB 来说，处理真实数据集中相对复杂的分类问题，模型性能是不如能通过超参数调节的机器学习模型的，在本文工作中表现最好的机器学习模型为使用 Poly 核函数的 SVM。

表 9　机器学习 4 种指标评估结果

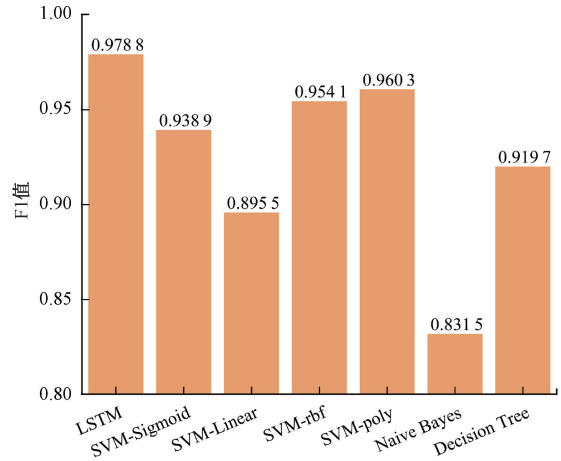
Table 9　Results of the evaluation of the four metrics of the machine learning　(%)

机器学习种类	核函数	准确率	精确率	召回率	F1 值
SVM	Sigmoid	95.05	92.27	95.56	93.89
	Linear	92.31	93.02	86.33	89.55
	rbf	96.43	93.75	97.12	95.41
	Poly	96.98	96.38	95.68	96.03
NB	/	86.03	82.18	84.17	83.15
DT	/	93.96	93.33	90.65	91.97

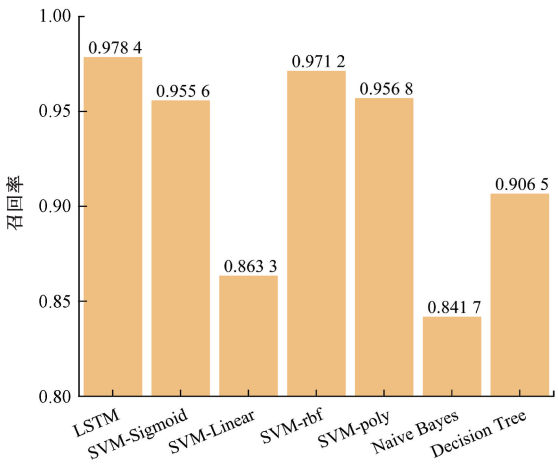
LSTM 模型与几种机器学习模型在相同的训练集与测试集中得到的 4 种评估指标结果的对比如图 14 所示，可以验证得到本文提出的 LSTM 模型相对于机器学习模型具有更优异的性能，在 4 项指标中表现均为最好，不会出现明显的跳变，鲁棒性更好。LSTM 模型相比于几种机器学习模型每一项最优的指标中：准确率高 1.1%、精确率高 1.55%、召回率高 0.72%、F1 值高 1.85%。



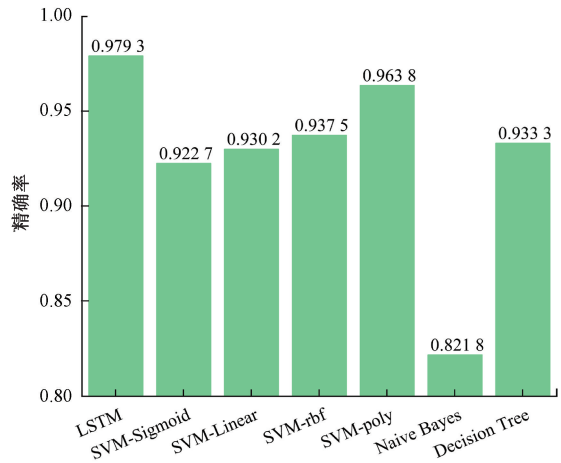
(a) LSTM 模型与几种机器学习准确率对比
(a) LSTM model with several machine learning accuracy comparison



(b) LSTM 模型与几种机器学习精确率对比
(b) LSTM model with several machine learning precision comparison



(c) LSTM 模型与几种机器学习召回率对比
(c) LSTM model with several machine learning recall comparison



(d) LSTM 模型与几种机器学习 F1 值对比
(d) LSTM model with several machine learning F1-score comparison

图 14　LSTM 模型与几种机器学习模型性能对比

Fig. 14　Performances comparison of LSTM models with several machine learning models

相比于几种机器学习模型,LSTM 结构更为复杂,并且每个 LSTM 层之后都有对应的全连接层,由于最终需要解决的是二分类问题,所以跟随全连接层的激活函数 Hard-Sigmoid 也能帮助提升模型性能,全连接层后的 Dropout 层加激活函数 ReLU 能抑制模型在训练过程中的过拟合现象,并且有一定几率过滤掉上层迭代后的产生的异常数据。

对于二分类问题,虽然机器学习训练时间短,解决方案也比较成熟,但是本文中使用的多特征时序数据作为输入训练集的二分类问题,其数据集具有维度高,组成复杂的特点,在这种情况下,具有多层神经网络的深度学习 LSTM 模型作为解决方案取得的效果显然更好。

4　结　论

本文提出了一种检测无人机 GPS 欺骗干扰信号的深度学习 LSTM 模型,实现对无人机接收到的欺骗信号与真实信号的有效分类。首先使用皮尔逊相关系数方法从多个维度的真实数据中选出和欺骗干扰相关性较强的特征数据,作为模型的输入量。其次,使用 TimeGAN 对时序的真实数据集进行数据增强。在训练 LSTM 模型时使用了 K 折交叉验证法,并且分别采用混淆矩阵及其二级指标准确率、精确率、召回率和三级指标 F1 值来评估模型性能。结果表明提出的 LSTM 模型比传统的机器学习模型在本文工作中表现更好,具有很好的鲁棒性和泛化能力。

在未来,为了进一步改善所提出的方法,之后的工作可以尝试更多的深度学习模型,比如近年来比较热门的 TransFormer 模型,相比于 LSTM 模型其具有两个主要的优势:非顺序数据处理和多头注意力机制。非顺序数据处理意味着模型在训练过程中可以进行数据集的整段或整体处理,而非顺序处理,也就表明其并不依赖于之前处理数据的信息,所以可以大幅缩短处理数据的时间,而多头注意力机制则用于计算数据之间的相似性得分,从而帮助模型在训练的过程中得到数据之间的相似性关系,更好的提高预测或分类的精度。

在本项工作取得进展后,还可以在判断无人机受到干扰后的下一步指令做更多开拓性的研究,例如无人机在禁用 GPS 模块后,利用惯性导航系统反馈的数据做飞行路径规划,这类工作可能会用到更多的回归模型与算法加以分析预测。

参考文献

[1] ŠKRINJAR J P, ŠKORPUT P, FURDIĆ M. Application of unmanned aerial vehicles in logistic processes [C]. Proceedings of the International Conference on New Technologies, Development and Applications, Springer, 2018: 359-366.

[2] HASSIJA V, CHAMOLA V, GUPTA V, et al. A survey on supply chain security: Application areas, security threats, and solution architectures [J]. IEEE Internet of Things Journal, 2020, 8(8): 6222-6246.

[3] VASHISHT S, JAIN S, AUJLA G S. MAC protocols for unmanned aerial vehicle ecosystems: Review and challenges [J]. Computer Communications, 2020, 160: 443-463.

[4] LIU Y, DAI H N, WANG Q, et al. Unmanned aerial vehicle for internet of everything: Opportunities and challenges [J]. Computer Communications, 2020, 155: 66-83.

[5] GARG P, CHAKRAVARTHY A S, MANDAL M, et al. Isdnet: Ai-enabled instance segmentation of aerial scenes for smart cities [J]. ACM Transactions on Internet Technology (TOIT), 2021, 21(3): 1-18.

[6] GUVENC I, KOOHIFAR F, SINGH S, et al. Detection, tracking, and interdiction for amateur drones [J]. IEEE Communications Magazine, 2018, 56(4): 75-81.

[7] CHAMOLA V, HASSIJA V, GUPTA V, et al. A comprehensive review of the COVID-19 pandemic and the role of IoT, drones, AI, blockchain, and 5G in managing its impact [J]. IEEE Access, 2020, 8: 90225-90265.

[8] 彭艺, 唐剑, 杨青青, 等. 基于强化学习的应急无人机通信中继选择策略[J]. 电子测量与仪器学报, 2022, 36(7): 9-15.
PENG Y, TANG J, YANG Q Q, et al. Relay selection strategy for emergency UAV communication based on reinforcement learning [J]. Journal of Electronic Measurement and Instrumentation, 2022, 36(7): 9-15.

[9] TAN X G, ZHANG G M. Research on surface defect detection technology of wind turbine blade based on UAV image[J]. Instrumentation, 2022, 9(1): 41-48.

[10] RODDAY N M, SCHMIDT R D O, PRAS A. Exploring security vulnerabilities of unmanned aerial vehicles [C]. Proceedings of the NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium. IEEE, 2016: 993-994.

[11] ALLADI T, CHAMOLA V, SIKDAR B, et al. Consumer IoT: Security vulnerability case studies and solutions [J]. IEEE Consumer Electronics Magazine, 2020, 9(2): 17-25.

[12] PSIAKI M L, HUMPHREYS T E. GNSS spoofing and detection [J]. Proceedings of the IEEE, 2016, 104(6): 1258-1270.

[13] FAN X, DU L, DUAN D. Synchrophasor data correction under GPS spoofing attack: A state estimation-based approach [J]. IEEE Transactions on Smart Grid, 2017, 9(5): 4538-4346.

[14] TROGLIA G M, TRUONG M D, MOTELLA B, et al. Hypothesis testing methods to detect spoofing attacks: A test against the TEXBAT datasets [J]. GPS Solutions, 2017, 21(2): 577-589.

[15] GAO G X, SGAMMINI M, LU M, et al. Protecting GNSS receivers from jamming and interference [J]. Proceedings of the IEEE, 2016, 104(6): 1327-1338.

[16] VAN DEN BERGH B, POLLIN S. Keeping UAVs under control during GPS jamming [J]. IEEE Systems Journal, 2018, 13(2): 2010-2021.

[17] BROUMANDAN A, SIDDAKATTE R, LACHAPELLE G. An approach to detect GNSS spoofing [J]. IEEE Aerospace and Electronic Systems Magazine, 2017, 32(8): 64-75.

[18] LIU Y, LI S, FU Q, et al. Analysis of Kalman filter innovation-based GNSS spoofing detection method for INS/GNSS integrated navigation system [J]. IEEE Sensors Journal, 2019, 19(13): 5167-5178.

[19] HE L, LI H, LU M. Dual-antenna GNSS spoofing detection method based on Doppler frequency difference of arrival [J]. GPS Solutions, 2019, 23(3): 1-14.

[20] GROSS J N, KILIC C, HUMPHREYS T E. Maximum-likelihood power-distortion monitoring for GNSS-signal authentication [J]. IEEE Transactions on Aerospace and Electronic Systems, 2018, 55(1): 469-475.

[21] WU Z, ZHANG Y, YANG Y, et al. Spoofing and anti-spoofing technologies of global navigation satellite system: A survey [J]. IEEE Access, 2020, 8: 165444-165496.

[22] MORALES-FERRE R, RICHTER P, FALLETTI E, et al. A survey on coping with intentional interference in satellite navigation for manned and unmanned aircraft [J]. IEEE Communications Surveys & Tutorials, 2019, 22(1): 249-291.

[23] KHAN S Z, MOHSIN M, IQBAL W. On GPS spoofing of aerial platforms: A review of threats, challenges, methodologies, and future research directions [J]. PeerJ Computer Science, 2021, 7: e507.

[24] MEAD J, BOBDA C, WHITAKER T J. Defeating drone jamming with hardware sandboxing [C]. Proceedings of the 2016 IEEE Asian Hardware-Oriented Security and Trust (AsianHOST), IEEE, 2016: 1-6.

[25] RANSATHAN A, ÓLAFSDÓTTIR H, CAPKUN S. Spree: A spoofing resistant GPS receiver [C]. Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking, 2016: 348-360.

[26] KANG C H, KIM S Y, PARK C G. Adaptive complex-EKF-based DOA estimation for GPS spoofing detection [J]. IET Signal Processing, 2018, 12(2): 174-181.

[27] MITCHELL R, CHEN R. Adaptive intrusion detection of malicious unmanned air vehicles using behavior rule specifications [J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2013, 44(5): 593-604.

[28] SEDJELMACI H, SENOUCI S M, ANSARI N. A hierarchical detection and response system to enhance security against lethal cyber-attacks in UAV networks [J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2017, 48(9): 1594-1606.

[29] ELDOSOUKY A, FERDOWSI A, SAAD W. Drones in distress: A game-theoretic countermeasure for protecting UAVs against GPS spoofing [J]. IEEE Internet of Things Journal, 2019, 7(4): 2840-2854.

[30] TEDESCHI P, OLIGERI G, DI PIETRO R. Leveraging jamming to help drones complete their mission [J]. IEEE Access, 2019, 8: 5049-5064.

[31] SEMANJSKI S, MULS A, SEMANJSKI I, et al. Use and validation of supervised machine learning approach for detection of GNSS signal spoofing [C]. Proceedings of the 2019 International Conference on Localization and GNSS (ICL-GNSS), IEEE, 2019: 1-6.

[32] ARTHUR M P. Detecting signal spoofing and jamming attacks in UAV networks using a lightweight IDS [C]. Proceedings of the 2019 International Conference on Computer, Information and Telecommunication Systems (CITS), IEEE, 2019: 1-5.

[33] SHAFIQUE A, MEHMOOD A, ELHADEF M. Detecting signal spoofing attack in UAVs using machine learning models [J]. IEEE Access, 2021, 9: 93803-15.

[34] BORHANI-DARIAN P, LI H, WU P, et al. Deep neural network approach to detect GNSS spoofing attacks [C]. Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020), 2020: 3241-3252.

[35] JAYAWEERA M. A Novel deep learning GPS anti-spoofing system with DOA time-series estimation [C]. 2021 IEEE Global Communications Conference (GLOBECOM), IEEE, 2021: 1-6.

[36] YOON J, JARRETT D, VAN DER SCHAAR M. Time-series generative adversarial networks [J]. Advances in Neural Information Processing Systems, 2019, 32.

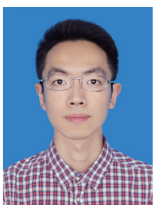
[37] BAASCH G, ROUSSEAU G, EVINS R. A conditional generative adversarial network for energy use in multiple

buildings using scarce data [J]. Energy and AI, 2021, 5: 100087.

[38] IOFFE S, SZEGEDY C. Batch normalization: Accelerating deep network training by reducing internal covariate shift [C]. Proceedings of the International Conference on Machine Learning, PMLR, 2015: 448-456.

[39] 陶镛泽, 胡佳成, 施玉书,等. 基于 LSTM 的矩形纳米光栅 AFM 图像复原方法[J]. 仪器仪表学报, 2021, 42(7): 50-57.
TAO Y Z, HU J CH, SHI Y SH, et al. AFM image restoration method of rectangular nano grating based on LSTM [J]. Chinese Journal of Scientific Instrument, 2021, 42(7): 50-57.

作者简介



王路阳,2020 年于南京农业大学获得学士学位,现为北京信息科技大学仪器科学与光电工程学院在读硕士研究生,主要研究方向为无人机 GPS 信号欺骗检测。
E-mail: wangluy@126.com

Wang Luyang received B. Sc. degree from Nanjing Agriculture University in 2020. Now he is a M. Sc. candidate at School of Instrument Science and Opto-Electronics Engineering in Beijing Information Science and Technology University. His main research interest includes UAV GPS signal spoofing detection.

孙一宸,2017 年于西安工业大学获得学士学位,2021 年于北京信息科技大学获得硕士学位,现为北京工业大学博士研究生,主要研究方向为红外成像处理算法和衍射深度神经网络增强算法。
E-mail: sunyichen@emails.bjut.edu.cn

Sun Yichen received his B. Sc. degree from Xi′an Technological University in 2017 and M. Sc. degree from Beijing Information Science and Technology University in 2021. Now he is a Ph. D. candidate at Beijing University of Technology. His main research interests include infrared imaging processing algorithms and diffractive deep neural network enhancement algorithms.

于明鑫,2010 年北京理工大学获得硕士学位,2015 年北京理工大学获得博士学位,现为北京信息科技大学副教授,主要研究方向为机器学习理论与应用、智能微系统轻量化算法、计算机视觉。
E-mail: yumingxin@bistu.edu.cn

Yu Mingxin received his M. Sc. degree in 2010 from Beijing Institute of Technology and Ph. D. degree in 2015 from Beijing Institute of Technology. Now he is an associate professor in Beijing Information Science and Technology University. His main research interests include theory and application of machine learning, lightweight algorithms for intelligent microsystems, computer vision.

李天放,2019 年于北京化工大学获得学士学位,现为北京信息科技大学仪器科学与光电工程学院在读硕士研究生,主要研究方向为红外成像。
E-mail: litianfang@bistu.edu.cn

Li Tianfang received his B. Sc. degree from Beijing University of Chemical Technology in 2019. Now he is M. Sc. candidate at School of Instrument Science and Opto-Electronics Engineering in Beijing Information Science and Technology University. His main research interest includes infrared imaging.

董明利(通信作者),1986 年和 1989 年于合肥工业大学分别获得学士和硕士学位,2009 年于北京理工大学获得博士学位,现为北京信息科技大学教授,北京信息科技大学仪器科学与光电工程学院院长,主要研究方向为光电与视觉检测。
E-mail: dongml@bistu.edu.cn

Dong Mingli (Corresponding author) received her B. Sc. and M. Sc. degree from Hefei University of Technology in 1986 and 1989, and Ph. D. degree in 2009 from Beijing Institute of Technology. Now she is a professor in Beijing Information Science and Technology University and the dean of School of Instrument Science and Opto-Electronics Engineering in Beijing Information Science and Technology University. Her main research interests include optoelectronic and visual inspection.