利用机器学习的GNSS欺骗检测综述

周雅兰,宋晓鸥
武警工程大学 信息工程学院,西安 710086

摘 要:近年来,随着全球卫星导航的重要性日益突出,欺骗检测成为热点研究问题。机器学习作为一种低成本的方法,具有自动从复杂数据中学习规律的能力,并且已在物联网欺骗检测中取得较好的效果,因此越来越多的研究将其用于GNSS欺骗干扰检测。从基于机器学习进行GNSS欺骗检测的基本流程出发,阐述了利用机器学习进行GNSS检测的数据采集和预处理。根据机器学习在欺骗检测中发挥的作用,将基于机器学习的GNSS欺骗检测分为基于信号分类以及基于信息验证的机器学习GNSS欺骗干扰检测两大类进行归纳与总结。最后,根据现有研究问题提出了对未来发展方向的展望。

关键词:机器学习;神经网络;全球卫星导航系统(GNSS);欺骗检测;欺骗干扰
文献标志码:A **中图分类号:**TP391 doi:10.3778/j.issn.1002-8331.2401-0330

Overview of GNSS Spoofing Detection Using Machine Learning

ZHOU Yalan, SONG Xiao'ou
School of Information Engineering, Engineering University of PAP, Xi'an 710086, China

Abstract: In recent years, with the increasing importance of global satellite navigation, deception detection has become a hot research issue. As a low-cost method, machine learning has the ability to automatically learn rules from complex data, and has achieved good results in the Internet of things spoofing detection. Therefore, more and more studies have used it for GNSS spoofing detection. Firstly, starting from the basic process of GNSS spoofing detection based on machine learning, the data acquisition and preprocessing of GNSS detection using machine learning are described. Then, according to the role of machine learning in spoofing detection, GNSS spoofing detection based on machine learning is divided into two categories: GNSS spoofing detection based on signal classification and GNSS spoofing detection based on information verification. Finally, according to the existing research problems, the prospect of future development direction is put forward.

Key words: machine learning; neural network; global navigation satellite system (GNSS); spoofing detection; spoofing jamming

随着全球卫星导航系统(global navigation satellite system,GNSS)的不断发展,其应用领域也不断扩展,在无人驾驶[1-2]、无人作战[3-4]、精密制导[5-6]等需要精确定位授时信息的民用及军事领域发挥着主导作用。然而,导航卫星距离地面两万至三万千米,导航信号到达终端接收机时十分微弱。并且,民用信号系统不加密且信号频点和格式对外公开。这些因素导致卫星导航信号极易受到人为恶意干扰,使终端用户无法获得正确的定位、导航和授时信息,造成军事行动失败或者交通设施瘫痪甚至人员伤亡等严重后果。其中,欺骗干扰通过转发真实的卫星导航信号或者生成与真实卫星导航信号高度相似的虚假欺骗信号使用户接受机获得错误的定位、导航和授时信息,达到干扰的目的。随着软件无线电的发展,欺骗干扰的方式越来越复杂,也更加隐蔽、更具威胁性。

根据检测原理的不同,传统的欺骗检测方法可以分为三类[7]:第一类是基于检测信号特征的异常变化。例如通过检测真实卫星信号与欺骗信号的功率、载噪比、到达方向、多普勒频移等特征的不同来检测欺骗干扰。这类方法利用接收机输出以及天线阵等,从统计的角度进行假设检验,设置门限检测欺骗干扰。然而随着欺骗干扰方式越来越复杂多变,这类检测方法难以对所有的欺骗场景进行建模,适应性较差。第二类是基于信号中的加密信息。这类欺骗检测方法需要修改信号结构或导航电文结构,在民事应用的实际情况中难以实现。第

基金项目:国家自然科学基金(61801516)。
作者简介:周雅兰(2001—),女,硕士研究生,CCF学生会员,研究方向为卫星导航信号检测、机器学习;宋晓鸥(1983—),通信作者,女,博士,副教授,研究方向为卫星导航信号处理、认知无线电,E-mail:15129290085@163.com。
收稿日期:2024-01-22 **修回日期:**2024-05-20 **文章编号:**1002-8331(2024)17-0062-12

三类利用系统中其他导航的辅助检测。通常将GNSS结果与惯性导航或者视觉导航结果进行一致性检验,以此检测欺骗干扰。这类检测方法需要额外的硬件设备,例如惯性测量单元,适用场景不广泛[8]。

机器学习神经网络可以自适应地学习输入-输出关系。它不需要指定数学模型、初始条件、噪声模型或它们的统计量[9]。作为一种数据驱动的方法,机器学习具有自动从数据中学习规律的能力,可以根据新的数据适应新的欺骗干扰方式。并且机器学习模型可以利用多层神经网络结构进行多层级的特征提取,提高特征表达能力。同时由于机器学习强大的数据处理能力,进行欺骗检测的时间进一步缩短,在无人驾驶、精确制导等需要实时检测的实际应用场景具有重要意义。目前,已经有许多研究及论文将机器学习用于卫星导航欺骗检测并成为一种趋势[10-12]。然而,现有的卫星导航欺骗检测综述[13-18]侧重于传统的欺骗检测方式,如信号功率检测、信号质量检测、信号到达角测量等方法,并未结合最新文献对基于机器学习的卫星导航欺骗检测进行系统地总结。因此,本文根据是否借助外部设施辅助,分基于信号分类以及信息验证两部分对基于机器学习的欺骗检测方法进行分析,以期对未来机器学习在GNSS欺骗检测中的应用提供参考。

1　数据采集与处理

利用机器学习的GNSS欺骗检测基本流程如图1所示:首先采集数据并对其进行预处理,而后采用合适的机器学习模型并进行参数选择与调优,将处理好的数据输入到机器学习模型中进行欺骗检测,最后根据检测结果响应应对措施。

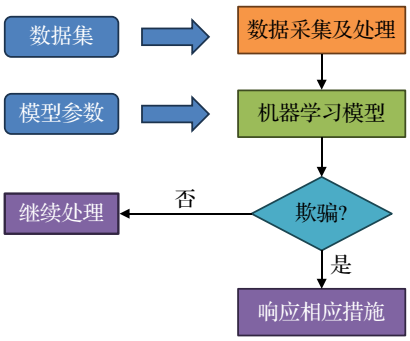


图1　机器学习欺骗检测流程图

Fig.1　Machine learning-based spoofing detection flow chart

1.1　数据采集

数据是影响机器学习模型欺骗检测性能的关键因素,当前用于机器学习欺骗检测研究的数据集可分为人工数据集和公开数据集。

人工数据集是在研究中根据所研究内容对GNSS信号进行采集和特征提取,通常利用软件无线电构建GNSS接收机。在文献[19]中,研究人员用一个通用的软件无线电外设单元构建GPS接收机,采集GPS信号并进行特征提取,用以研究无人机系统上的欺骗检测。提取的13个特征如表1所示,在文献[19-27]中多次用于无人机系统上的欺骗检测技术研究。

表1　13个特征列表

Table 1　List of 13 features

特征	缩写
载噪比(carrier to noise ratio)	C/N0
即时相关器幅度(prompt correlator)	PC
超前相关器幅度(early correlator)	EC
滞后相关器幅度(late correlator)	LC
即时同相分量(prompt in-phase component)	PIP
即时正交分量(prompt quadrature component)	PQP
跟踪载波多普勒(tracking carrier doppler)	TCD
载波多普勒(carrier doppler)	DO
载波相位环(carrier phase cycles)	CP
周内时(time of the week)	TOW
接收机时间(receiver time)	RX
伪距(pseudorange)	PD
伪随机噪声(pseudorandom noise)	PRN

实时采集GNSS信号在时间和金钱方面的成本很高并且极易出错,研究者为了便于研究创建并公开发布了GNSS欺骗信号数据集,如表2所示。

GATEMAN[28]数据集是在由欧盟资助的GATEMAN(GNSS navigation threats management)项目框架内进行的欺骗检测的实验室验证中生成的,模拟了对飞行中飞机的简单欺骗(即欺骗信号与真实信号没有实现同步),由于硬件生成器的限制只对GPS L1和Galileo E1进行了仿真。TEXBAT是由德克萨斯大学奥斯汀分校无线电导航实验室开发的公开数据集,共记录了从简单

表2　公开欺骗数据集

Table 2　Public spoofing datasets

数据集	年份	信号	欺骗场景	欺骗类型
GATEMAN	2018	GPS L1、Galileo E1	动态	简单欺骗
TEXBAT	2012 2016	GPS L1	静态、动态	简单欺骗、中级欺骗、复杂欺骗
OAKBAT	2020	GPS L1、Galileo E1	静态、动态	简单欺骗、中级欺骗
Fgi-Spoofrepo	2024	GPS L1、Galileo E1、GPS L5、Galileo E5a	静态	简单欺骗、中级欺骗
Mendeley Data	2024	GPS L1、GPS L5、Galileo E1、Galileo E5a、BeiDou B1、BeiDou B2、QZSS L1、QZSS L2、GLONASS L1、GLONASS L2	静态	—

到复杂8个欺骗场景,其中包括6个静态场景和2个动态场景,此外还包括动态和静态的2个“干净”(无欺骗)数据。TEXBAT[29-30]是目前公认的权威GNSS欺骗数据集,为欺骗检测技术的研究提供了重要基础。OAKBAT数据集[31]由美国橡树岭国家实验室发布,在TEXBAT的框架下重现了前6个场景,并提供了更详细的元数据及上下文信息以便用户更好地分析和使用数据集,甚至在此基础上创建自己的数据集。除此之外,OAKBAT还记录了Galileo E1信号在相应场景下的数据,进一步丰富了TEXBAT数据集。然而,这两个数据集都缺乏对L较低波段如GPS L5和Galileo E5a的记录,而检测L较低波段的欺骗脆弱性也十分重要。因此,在2024年芬兰地理空间研究所公布了包括对GPS L1、Galileo E1、GPS L5h和Galileo E5a信号记录的欺骗数据集Fgi-Spoofrepo[32],并使用基于MATLAB的开源软件定义接收器FGI-GSRx对数据集进行分析。同年,由云南大学信息科学与工程学院公布的欺骗数据集Mendeley Data[33]记录了包括北斗二代在内5个星座的共8个信号波段的数据,填补了之前公开欺骗数据集没有北斗信号记录的空白,有助于推进对北斗欺骗信号检测技术的研究。

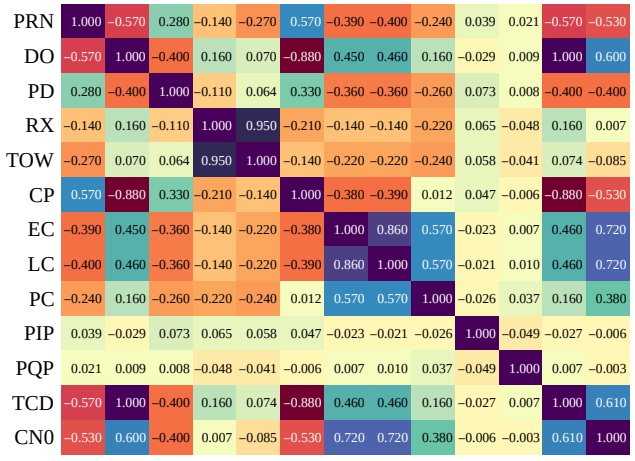
1.2　数据预处理

采集的数据大多是不规范的,如果直接输入到机器学习模型中进行检测不仅会加大计算量,还不能得到最佳的检测结果。因此,在数据输入机器学习模型之前通常需要对其进行清洗和准备。根据所采集的数据以及检测方法的不同,对数据进行预处理的方式不尽相同。但综合基于机器学习的GNSS欺骗检测文献发现,对GNSS数据预处理方式主要为数据归一化、特征提取以及非平稳数据修正。

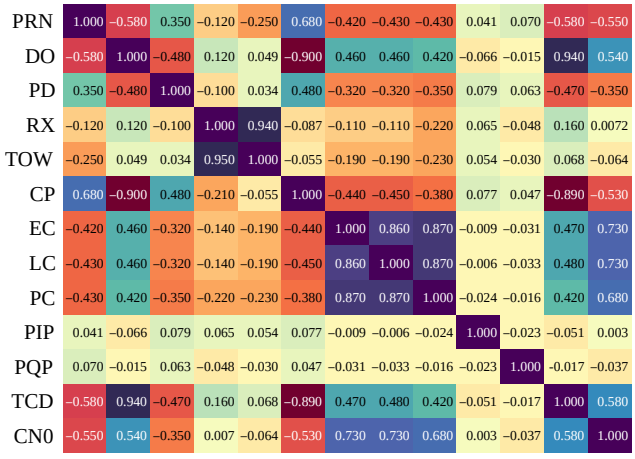
在多场景、多源头采集到的GNSS数据往往量纲不统一,不便于后续数据的处理甚至还会影响模型的收敛速度。归一化可以对数据进行量纲统一,将数据压缩至[0,1]范围内,以便后续处理。目前,在利用机器学习进行GNSS欺骗检测研究中使用的数据归一化方法为:Z-score和min-max。

数据集中往往存在具有很强相关性的特征,如果不通过筛选同时作为模型输入,则会大大降低模型性能[20]。由此可知,选择适合的特征输入对于提高机器学习模型检测欺骗信号的性能至关重要。目前,用于计算特征相关性的算法有皮尔逊相关性[22,34]和斯皮尔曼相关性[19,21,35-36],通过计算相关系数来量化特征之间的相关程度。图2所示分别为利用皮尔逊相关性和斯皮尔曼相关性对表1所示13个特征进行相关性计算的结果。

机器学习算法无法处理非平稳数据;一个正确的学习模型需要一个静态的关系。因此,需要将服从非平稳



(a)皮尔逊相关性



(b)斯皮尔曼相关性

图2　13个特征相关性热力图

Fig.2　Correlation heatmap of 13 features

分布的特征,使用差分将数据转换为平稳数据。这个过程涉及到计算样本之间的连续差异,如式(1)所示:

$$R=\frac{x_{i+1}-x_i}{n_{i+1}-n_i} \tag{1}$$

其中,R为瞬时变化率,n_i和n_{i+1}为两个样本之间的距离,即为1。现有基于机器学习欺骗检测的数据预处理

表3　现有研究数据预处理方法

Table 3　Data pre-processing of exist research

文献及年份	数据归一化		特征提取		非平稳数据修正
	min-max	Z-score	斯皮尔曼相关性	皮尔逊相关性	
文献[37]:2023	√				
文献[22]:2022	√		√		
文献[27]:2024		√			
文献[35]:2023			√		
文献[38]:2020				√	
文献[25]:2022	√			√	√
文献[24]:2022	√		√		√
文献[19]:2021			√		√

方法如表3所示。

2 基于机器学习的GNSS欺骗检测

GNSS信号分类方法利用机器学习分类器技术来区分欺骗信号和真实信号,而GNSS信息验证方法则利用基于机器学习的位置识别技术来证明GNSS位置的真实性。

2.1 基于信号分类的机器学习欺骗检测

基于信号分类的机器学习欺骗检测将检测过程视为分类任务,通过欺骗信号与真实信号在信号特征方面的特征差异,从数据中提取相应特征输入机器学习模型进行分类,进而完成欺骗检测。

从接收机接收到GNSS信号到解算出定位导航结果的信号处理过程中,欺骗信号的出现会引起基于信号功率、基于信号到达特征、基于信号相关峰和基于导航解算结果的五类特征差异,如表4所示,提取特征时接收机射频前端、基带信号处理模块、解调解码模块和位置速度时间(position velocity-time,PVT)模块会输出中间级别的观测值和信号参数,可提取相关特征输入机器学习模型进行信号分类。在基于信号相关峰的差异中,信号质量监测(signal quality monitoring,SQM)技术是由于欺骗信号与真实卫星信号相互作用,在跟踪阶段引起相关峰值失真,通过检测信号相关峰值的异常来检测欺骗信号,包括Ratio、Delta等不同形式的度量值。互模糊函数(cross ambiguity function,CAF)可以通过计算多普勒频率和码延迟的相关性来发现欺骗信号的存在:当欺骗信号存在时CAF图像中会出现多个峰值,而当只有真实信号存在时则只能观察到单个峰值。

表4 由欺骗信号引起的特征差异

Table 4 Differences characteristics induced by spoofing signal

差异类别	差异特征	相关文献
基于信号功率的差异	C/N0	文献[39-40]
	接收功率	文献[41-42]
基于信号到达特征的差异	DOA	文献[43]
基于信号相关峰的差异	SQM	文献[41,44-45]
	CAF	文献[46-48]
基于中间观测值的差异	伪距、多普勒频移、载波相位	文献[9,34,49-50]

基于信号分类的机器学习欺骗检测将从接收机各模块中提取的多种信号特征参数作为输入,训练各种机器学习模型进行分类以完成欺骗信号检测。目前,用于GNSS欺骗检测的机器学习模型主要分为三类:传统有监督机器学习模型、无监督机器学习模型以及深度学习模型。

2.1.1 传统有监督机器学习模型

传统机器学习算法是指在深度学习兴起之前的机器学习模型,而有监督模型则是指由带有正确标签的数据训练的模型。如表5所示,在GNSS欺骗检测中常见的传统有监督机器学习模型包括支持向量机(support vector machine,SVM)、K最近邻(K-nearest neighbor,KNN)算法、决策树(decision trees,DT)及在其基础上发展出来的集成树模型。

SVM是在特征空间中寻找一个最优超平面,使其能够区分两类数据并且使各类数据中离超平面最近的点与超平面的距离之和最大,其中离超平面最近的样本点称为支持向量。由此可得,SVM是一种线性分类器,但是通过引入核函数将数据映射到更高维的特征空间,SVM也能处理非线性分类问题。文献[38,51]在实验以及真实数据集上验证了SVM在欺骗检测上的有效性。文献[49]提出了一种基于SVM的多参数联合检测,提取了SQM、C/N0等多个特征用于训练SVM模型,与传统的单参数检测方法相比,检测性能显著提升。参数与核函数的选择和SVM的检测性能密切相关。文献[22]比较了线性SVM、C-SVM和Nu-SVM在欺骗检测上的性能,其中C-SVM为常用的经典SVM,Nu-SVM将C-SVM中的参数"C"改为"Nu"以控制支持向量的个数,其结果表明Nu-SVM的检测性能更好。SVM的检测性能可以通过选择合适的核函数得到提升,如:线性核函数、多项式核函数、RBF(radial basis function)核以及Sigmoid核函数。文献[8]通过分析改进的SQM等特征,提出了一种基于SVM的欺骗检测方法,并比较了不同核函数的检测性能,在该研究中使用RBF核作为核函数时检测性能最高。而文献[52]利用K-fold分析用于无人机欺骗检测的机器学习模型,结果表明使用多项式核的SVM模型优于决策树、随机森林以及朴素贝叶斯模型。

KNN根据距离待测样本最近的K个样本所属的类别对待测样本进行分类。KNN算法训练时间短,流程简单明了,易于实现。在文献[53]中,KNN被用于检测识别多峰欺骗干扰,仿真结果证明了该方法优于传统的多峰欺骗检测。但是由于该模型需要存储所有的训练数据,对内存要求较大,并且因为需要计算输入数据到

表5 传统有监督机器学习模型比较

Table 5 Comparison of traditional supervised ML models

算法	相关文献	优点	局限性	适用场景
SVM	文献[8,22,38,51-52]	仅依据支持向量进行分类,不太容易过拟合;鲁棒性强	在样本量过大,核函数映射维度非常高时,计算量大;对参数、核函数敏感	适用于高维小规模数据集
KNN	文献[22,44,53-55]	结构简单明了,易于训练;检测精度高	计算要求高;对K值敏感	适用于小规模数据集
DT及集成树	文献[19,56-58]	可解释性强;不需要额外的数据预处理	容易过拟合;对异常点敏感	适用于大规模数据集

所有训练数据之间的距离,检测时间可能会较长,因此该模型面对较复杂的欺骗干扰检测性能并不是很好。文献[44]中KNN模型的检测概率只有77.291%,不如检测概率达到99.3247%的神经网络模型。在文献[22,54-55]中,KNN与SVM、神经网络、决策树等其他模型同时被用于欺骗检测,结果显示KNN并不是最优检测模型。

决策树(decision trees,DT)的基本思想就是递归地构建一个树状结构,将一个大的分类问题分为若干的小的分类问题,直到这些子分类问题可以被简单地解决。近年来,很多在DT基础上衍生出来的基于树结构的集成学习模型也被用于检测GNSS欺骗干扰:随机森林(random forest,RF)、梯度提升决策树(gradient boosting decision trees,GBDT)、adaptive boost(AdaBoost)、extreme gradient boosting(XGBoost)以及light gradient boosted machine(LGBoost)。其中,随机森林是以决策树为基学习器的Bagging集成模型,用投票法来组合多个决策树的输出结果。而GBDT是以决策树为基学习器的Boosting模型,使用梯度下降算法让来自先前树的误差最小化。AdaBoost是以单层决策树为基学习器的Boosting模型,在训练过程中增加了错分样本的权重,同时给错误率低的决策树赋予话语权;XGBoost在GBDT的基础上利用并行化、树剪枝和正则化来避免过拟合;LGBoost在XGBoost的基础上采用单边梯度采样和基于互斥特征的特征捆绑降低了计算复杂度。基于树结构机器学习模型不需要对数据进行额外的特征预处理,并且基于集成的树结构模型在分类型性能上得到了很大的提升,因此在GNSS欺骗信号检测中也有较多应用。文献[56]将选取的伪距等8个GPS信号特征输入3个不同的AdaBoost模型进行欺骗信号检测,结果显示gentle AdaBoost检测准确率最高,为97.04%。文献[19]比较了RF、GBDT、XGBoost和LGBM这4种基于树结构模型的性能,最后XGBoost在准确率、检测时间和占用内存方面都优于其他模型。文献[57]利用基于树的模型和RBF核的SVM等其他模型检测SCER欺骗攻击,根据仿真结果,基于决策树的分类器和提出的特征提取方法,模型在40~50 dBHz的载噪比范围内获得了大于98.48%的准确率,优于其他模型。同样,在文献[58]提出的PERDET欺骗检测方法中采用线性核的支持向量机(SVM)、RBF核的SVM、K最近邻(KNN)、RF、GBDT和XGBoost共6种机器学习算法对所选特征数据集进行学习。通过对这些模型的结果进行比较发现,在综合分类结果上,RF和XGBoost模型是6种分类器中最优的。

2.1.2 无监督机器学习模型

有监督机器学习模型已经在GNSS欺骗检测领域展现出了良好的发展趋势,但是其有效性依赖于训练数据集中各种攻击类型的获取与标注,因此在实际应用中存在局限性。针对这一局限性,一些研究将GNSS欺骗检测视为异常检测,利用无监督机器学习模型,无须各种攻击类型数据的标签,通过输入探究输入数据的内在关系来完成对真实信号与欺骗信号的分类,能够在实际应用中有效检测出新的欺骗信号。文献[59]提出了一种结合基于密度的应用和噪声空间聚类(density-based spatial clustering of applications and noise,DBSCAN)算法的改进接收机自主完好性监测(receiver autonomous integrity monitoring,RAIM)欺骗检测方法,然而这种方法在处理高维数据集时往往表现不佳。文献[60]提出一种基于无监督机器学习模型的高斯混合模型(Gaussian mixture models,GMM)算法,通过对未受欺骗的GPS信号进行聚类来检测欺骗攻击,但是当存在大量缺失值时会影响其检测性能。文献[50]提出了一种基于无监督模型独立森林(isolation forest)的卫星导航欺骗信号检测方法,通过使用每个数据的聚合度来确定检测分数,从而确定是否为异常数据进而检测欺骗,但当数据集较大时其检测性能下降。

除此以外,一些生成式神经网络如自编码器(Auto-Encoder,AE)和生成对抗网络(generative adversarial network,GAN)也常被用作无监督欺骗检测。文献[41,61]将变分自编码器(variational AutoEncoder,VAE)用于欺骗检测,通过学习真实信号的潜在分布来检测欺骗信号。文献[61]将无监督算法与有监督算法在检测欺骗性能上作比较,结果表明无监督算法在未知数据上优于有监督算法。文献[62]通过发动机的射频指纹(radio frequency fingerprints,RFFs)来构建类噪声特征,然后将卷积自编码器(convolutional autoencoder,CAE)用于异常检测,在实验中得到了99.7%以上的准确率。文献[63]将一种基于BiGAN的GAN框架用作单类分类器,进行GNSS欺骗检测,并在实验中与AE、VAE等六种分类器比较得到了最高的检测准确率。文献[64]提出了一种基于GAN和卫星星座指纹的欺骗检测框架,利用GAN学习卫星星座指纹的聚合表示并以此识别、清除欺骗信号,该方法规避学习算法运行过程中的对抗干扰问题,鲁棒性更好。

2.1.3 深度学习模型

随着硬件计算能力的提升,深度学习由于不需要复杂的特征工程以及较强的适应性在GNSS欺骗检测领域的应用也越来越多。根据现有研究,用于欺骗检测的深度学习模型主要为:多层感知机(multilayer perceptron,MLP)、卷积神经网络(convolutional neural network,CNN)、长短时记忆网络(long short-term memory,LSTM),其比较如表6所示。

MLP由多个感知机连接而成,是深度学习最基础的神经网络模型。文献[44]提出了一种基于MLP的GPS欺骗检测方法,并在GPS的软件接收机的仿真实验

表6 深度学习模型比较

Table 6 Comparison of deep learning models

算法	相关文献	优点	局限性	适用场景
MLP	文献[42,44,65]	结构简单,在简单数据集上能取得较好的性能	对于复杂的欺骗数据集没有足够的鲁棒性,需要大量的训练欺骗数据以避免过拟合	适用于处理一维矢量数据以及不具有显著空间结构的问题
CNN	文献[39,46,66-68]	可以自动提取特征,还具有参数共享、局部连通性、多层结构等优点	对欺骗数据序列的适应性较差,捕获全局欺骗信息的能力有限	适用于二维或者图像类欺骗数据
LSTM	文献[7,34,69-71]	能够利用过去的输入数据进行未来的预测	需要更多的计算资源和动手训练,容易出现梯度消失和梯度爆炸等问题	适合处理具有序列性质的欺骗数据

中验证了其有效性。文献[42]利用粒子群优化算法(particle swarm optimization,PSO)训练MLP用于GNSS欺骗检测,并在仿真中与基于贝叶斯的分类器相比得到了更好的检测结果。但是这些方法并没有在通用数据集上进行验证,不利于与其他方法进行比较。文献[65]利用MLP检测无人机上的欺骗攻击,分别在TEXBAT和MAVLINK数据集上得到了83.23%和99.93%的准确率,并于LSTM比较证明了其检测性能更好。

CNN包括输入层、卷积层、池化层、全连接层以及输出层,本质是由MLP发展而来,对图像分类任务特别有效。文献[66]提出了一种基于CNN的GPS欺骗检测方法,通过无人机在飞行过程中记录的数据训练,通过实验实现了对欺骗攻击的高精度检验,但是只对训练过的攻击类型有效。文献[39]将一维CNN用于无人机上的欺骗攻击检测,实现了检测的轻量级以及高效节能,并在飞行测验中与SVM相比证明了其更好的检测性能。文献[67]针对捕获阶段难以检测出小时延(0~2个码片)欺骗信号的问题,采用了基于CNN的检测方法。根据实验仿真结果,当欺骗信号与真实卫星信号的码片相位差大于0.5时,基于CNN的方法取得了较高的检测精度。文献[46]将捕获阶段获得的CAF图像作为输入,分别利用CNN和MLP进行分类来检测欺骗信号的存在,实验表明在复杂的场景下,CNN的检测性能优于MLP。文献[68]将文献[46]提出的方法与基于GMM的聚类方法相连接,GMM负责确定峰值(即信号)的数量和位置。由于CAF图像的尺寸较大,通过CAF图像检测的计算成本较大、时间较长,因此文献[48]提出了潜在语义分析(latent semantic analysis,LSA)的降维算法来对CAF图像进行降维,而后分别利用CNN与MLP进行检测,缩短了检测时间,降低了计算成本。

LSTM是一种常用的处理序列数据的循环神经网络(recurrent neural network,RNN)模型。文献[69]结合线性回归和LSTM来预测最佳无人机路线来检测欺骗,并增强对GPS欺骗信号的敏感性。文献[7]利用LSTM对采集的飞行数据进行学习,依据初始状态预测后续的飞行轨迹并据此检测欺骗攻击。文献[34]利用过去的多普勒测量值来训练LSTM网络并通过预测GNSS信号的多普勒频移来判断是否存在欺骗。文献[70]在接收机信号捕获阶段通过分析和利用欺骗攻击的时序特征,利用LSTM神经网络设计了一种欺骗检测和攻击方式识别算法,并通过测试证明其有效性。文献[35]提出了一种PCA-CNN-LSTM模型用于小型无人机上的欺骗检测,主成分分析(principal component analysis,PCA)和CNN用于数据预处理和重要特征提取,而后利用LSTM进行进一步的处理和建模从而检测欺骗攻击,通过多种模型的融合获得了更好的检测性能。

2.1.4 机器学习分类模型总结归纳

将机器学习用于欺骗信号检测弥补了传统方法建模难、计算复杂等问题,本小节将用于信号分类的机器学习模型分为传统有监督机器学习模型、无监督机器学习模型以及深度学习模型三类,如表7所示,对三类模型进行总结归纳。

(1)传统机器学习模型与深度学习模型对比:传统的机器学习方法对数据质量和特征选择的要求较高,并且超参数需要事先人工选择,而深度学习模型可以自动学习从原始数据中提取特征,无须人工设计;传统机器学习模型简单,因此训练速度快、可解释性强、计算成本小,而深度学习模型需要大量数据,因此计算成本高、实时性低;但是传统的机器学习模型应用较单一,准确率低且易受干扰,深度学习模型从原始的欺骗数据输入映射到最终的欺骗检测输出,这使得深度学习模型能够适应复杂的欺骗数据集,并在欺骗检测任务上取得更好的准确率,适应性强。

表7 机器学习模型比较

Table 7 Comparison of machine learning models

算法	优点	局限性	适用场景
传统有监督机器学习模型	训练速度快、可解释性强、计算成本小	应用单一、准确率低、易受干扰、难以处理高维数据	适用于数据规模较小且实时性要求高的场景
无监督机器学习模型	无须数据标签、工作量小	可解释性弱、检测精度不高	适用于欺骗数据标签难以获得的场景
深度学习模型	适应性强、能够自动提取特征、分类精度高	可解释性低、计算成本高、实时性低	适用于大规模欺骗数据集

(2)有监督与无监督机器学习模型比较:有监督机器学习算法通过对比输出与输入数据的标签进行训练,检测精度高,在欺骗信号分类方面已经有了很好的发展。但是有监督模型要求带有标签的数据,这在无法获得带标签攻击数据时无法进行,并且有监督机器学习方法通常只对训练过的攻击类型检测有效,不能精确检测出未知的欺骗信号。无监督机器学习直接对输入数据进行内在分析,无须标注标签,并且对未知的欺骗信号类型同样有效。

(3)传统机器学习模型与深度模型融合:深度学习通过大量的数据来学习高级特征,从而实现端到端的自主学习,而一个性能良好的深度学习模型往往需要很高的单元数、隐藏层数或特征数,这使得计算成本大大加大。而传统的机器学习模型虽然计算成本小,但却存在“维数灾难”。因此,可以将传统机器学习模型与深度学习模型融合起来:利用机器学习模型进行特征提取与数据预处理,而后利用深度学习进行进一步检测,这样不仅可以增强深度学习的可解释性,也可以减轻深度学习模型的计算压力。

2.2 基于信息验证的机器学习欺骗检测

基于信号分类的欺骗干扰检测在信号层面对接收到的GNSS真实信号与欺骗信号进行区分来检测欺骗干扰,但是由于接收信号受环境和电离层的影响,此类方法的检测精度会降低。作为一种欺骗检测方法的补充,也可以通过比较由GNSS计算的位置、速度等信息和由备选辅助设施的位置、速度等信息检测欺骗干扰,即如图3所示的基于信息验证的GNSS欺骗检测。需要GNSS精确定位的设备如无人机、智能手机、自动驾驶汽车等通常配备摄像头等视觉传感器和加速度计、陀螺仪、磁力计等惯性传感器(inertial MeasUrement unit,IMU)以及Wi-Fi,因此可以通过融合传感器的数据或者结合移动蜂窝网络的信息进行基于信息验证的GNSS欺骗检测。但是在传统的基于信息验证的欺骗干扰检测方法中,无论是基于传感器融合辅助还是基于外部信号辅助的方法都存在相应的局限性。随着机器学习的发展,许多研究将机器学习方法用于基于信息验证的欺骗干扰检测方法,来弥补后者的缺陷并提高检测复杂欺骗攻击的性能。

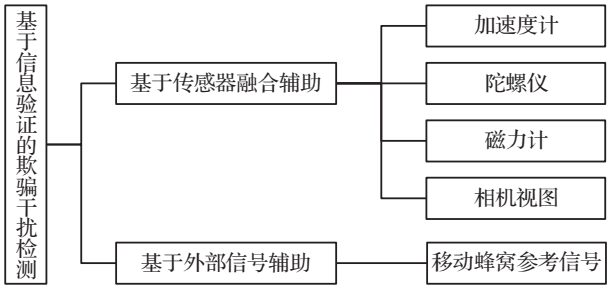


图3 基于信息验证的GNSS欺骗检测

Fig.3 Information verification-based GNSS spoofing detection

2.2.1 传感器融合辅助方法

一般来说,攻击者很难改变设备的相机视图来进行位置欺骗,因此惯性导航系统(inertial navigation system,INS)中相机实时拍摄的航拍图像可以作为一种外带的位置信息验证,与基于GNSS位置的公用历史卫星图像进行一致性对比来检测GNSS欺骗干扰。然而这种信息验证的方法由于天气、季节变换等因素的影响使实施航拍图像与历史卫星图像之间在分辨率、亮度等特征方面存在较大差异,使欺骗检测难度加大,延长了欺骗检测的时间。卷积神经网络(CNN)在图像识别、分类等方面展现出强大的性能,因此文献[71]提出了基于CNN模型图像匹配算法的欺骗检测算法,在100 ms的时间内检测GPS欺骗干扰的成功率约为95%。

除了视觉传感器外,加速度计、陀螺仪、磁力计等惯性传感器(IMU)的位置、速度等信息也通常与基于GNSS的位置、速度等信息进行对比来检测GNSS欺骗攻击。现有文献通常考虑两种检测方法:一种是直接比较IMU与GNSS的测量值;另一种是将二者进行融合,并将融合过程的异常检测为欺骗干扰。第一种称为直接比较法,对基于IMU和GNSS的加速度估计、位置估计、旋转速度估计等信息进行了比较。然而,由于比例因子和非正交性误差,IMU提供的位置速度等信息可靠性较差,并且误差随着时间累积,因此直接比较法需要随着时间进行阈值参数的微调。第二种方法通常应用卡尔曼滤波进行融合,融合过程中卡尔曼新息的统计量用于检测可能存在的欺骗干扰,然而卡尔曼滤波需要的计算量通常较大。由此,机器学习可以作为一种比较或融合IMU和GNSS测量值的更简单的方法。文献[72]将在一组真实和受欺骗的轨迹下获得的从GNSS和IMU上测量速度的差值作为输入训练一个神经网络(NN)来检测欺骗攻击,与Neyman-Pearson检验和直接比较法进行了比较,获得了更低的错误概率。文献[73]将GNSS数据点和IMU数据点之间的欧氏距离作为SVM的输入,利用SVM对GNSS和IMU测量值进行融合来检测欺骗干扰。文献[58]提出了PERDET方法,利用机器学习的方法,基于传感器之间的互补性来弥补传感器的误差等不足,选择了加速度计,陀螺仪,磁力计,GPS和气压计作为输入进行欺骗干扰检测。

长短期记忆网络(long short-term memory,LSTM)作为一种经典的机器学习模型,主要用于解决异常检测和时序预测等问题。因此,LSTM根据设备传感器的输出对设备的位置、速度等信息进行预测,将预测信息与基于GNSS的信息进行比较来检测欺骗干扰,避免了基于IMU随时间累积的误差的影响。文献[7]利用LSTM根据IMU的信息预测路径,与GNSS给出的路径进行比较检测欺骗干扰。文献[74]以多个低成本车载传感器

的数据作为输入,利用深度强化模型预测了车辆在两个连续时间点内的移动距离,与基于GPS计算的移动距离比较,检测欺骗干扰的准确率达到了99.99%到100%。文献[75]利用LSTM提出了一种基于对无人驾驶车辆位置预测的欺骗检测策略。文献[76]提出了DeepPOSE,一种利用移动设备上的运动传感器来估计车辆位置并进一步检测GPS欺骗干扰的深度学习模型。文献[77]加速度计、转向角传感器、速度传感器等低成本传感器的数据输入LSTM模型,用于预测位置偏移进而检测欺骗攻击,并使用公开可用的真实世界本田研究院驾驶数据集验证了方法的有效性。

2.2.2 外部信号辅助方法

除了利用基于传感器数据的INS进行辅助定位来检测GNSS欺骗干扰外,基于移动定位系统(mobile positioning system,MPS)的外部定位技术也可以用于验证GNSS位置信息的真实性。文献[78]提出一种基于5G基站的欺骗检测方法,该方法利用从多个5G基站收集的接收信号强度(received signal strength,RSS)来推断无人机的位置从而进行基于位置信息验证的欺骗干扰检测。但是该方法采用三角测量定位技术,要求至少三个基站同时工作才能达到理想的欺骗干扰检测精度。为了使无人机在不能同时被三个基站同时覆盖的情况下仍能够达到理想的欺骗检测效果,文献[79]和[80]在此基础上分别在边缘服务器上引入深度神经网络和深度集成网络实现了无人机在3个、2个或者1个基站情况下的实时欺骗检测,以无人机与基站之间的路径损耗作为输入,输出欺骗出现的可能性。但是该方法需要收集来自不同基站的路径损耗数据,可能造成网络拥堵。

尽管上述基于移动蜂窝网络定位方法在欺骗检测方面被验证是有效的,但是在城市峡谷中,建筑物复杂密集且不规则,电磁传播环境复杂,此类方法无法在无人机上精确检测出欺骗干扰。文献[81]利用3D无线电地图和机器学习方法来检测蜂窝连接无人机的GPS欺骗攻击。这些方法都是基于单个无人机进行欺骗检测,每个无人机一个检测程序,当一个大型无人机群与一个基站连接时,可能会导致检测系统出现拥塞。文献[82]提出了一种基于GNN的蜂窝连接无人机蜂群GPS欺骗检测方法,通过比较蜂群GPS拓扑信息和通信拓扑之间的差异来检测蜂群的GPS欺骗攻击,对于由10架无人机组成的无人机集群,使用Intel Core 1.6 GHz处理器,GNN检测欺骗干扰的准确率超过90%,计算时间小于10 ms。

表8从数据来源、分析层面、计算位置、硬件设施四个方面,对GNSS信号分类、传感器数据融合和蜂窝信号分析三类基于机器学习的GNSS欺骗检测方法进行了对比。

3 未来发展趋势

随着计算能力的不断提升,机器学习已经成为GNSS欺骗检测领域的研究热点。现依据机器学习在GNSS欺骗检测方面可提升的问题提出对未来发展趋势的展望。

(1)针对检测时延与可靠性问题。目前欺骗检测研究大多是在单个样本的基础上进行,但单次检测结果不总是可靠,既无法控制虚警概率也不能尽量缩短检测时延。受序列检测的启发,未来可研究的一个途径是训练样本视为时间序列,进而开发一个检测模型,在一个时间窗口内进行欺骗检测,单次检测器可作为预警生成器,通过序列检测的算法将单次检测的信息聚合起来,提高检测结果的可靠性。而目前序列检测中存在一种流行的算法是最快检测算法,可实现一定虚警约束下的最小时延。同时,将人工智能算法与传统方法的结合能在一定程度上增加检测模型的可解释性,也是未来的一大研究趋势。

(2)针对检测实时性问题。随着GNSS导航的应用领域越来越广泛,对GNSS欺骗检测实时性要求高的场景也越来越多。目前关于GNSS欺骗检测的研究大都是根据采集的数据进行训练,属于离线欺骗检测,而应用于动态欺骗攻击的在线欺骗检测系统的开发和应用将成为未来发展的趋势。

(3)针对模型轻量化问题。目前用于复杂多变的机器学习模型往往是大型的:它需要很高的单元数、隐藏层数或特征数。这转化为保存模型和移动数据所需的计算需求、内存带宽和存储量的持续增加。而这对于无人机等小型设备终端往往难以实现。因此未来发展将需要在模型复杂度和计算存储资源之间进行权衡,降低检测模型的复杂度,设计轻量化检测模型。

(4)针对数据标签获得问题。在机器学习中,数据是训练模型的关键组成部分。在基于机器学习的欺骗检测中,当测试分布与训练数据略有不同时机器学习模型的解释性能和泛化性能大大降低。然而在实际应用中,带有标签的各种欺骗攻击数据往往难以获得,这使

表8 基于机器学习欺骗检测方法对比

Table 8 Comparison of ML-based spoofing detection methods

检测方式	数据来源	分析层面	计算位置	硬件设施
GNSS信号分类	GNSS信号	信号	GNSS接收机	GNSS接收机
传感器数据融合	传感器数据	信息	设备终端	不同传感器
蜂窝信号分析	蜂窝信号	信息	边缘服务器	单个或多个基站

得机器学习模型在训练过程中往往存在过拟合现象。而数据增广与生成可以使用多种方法来增加数据的数量和多样性,根据专业知识描述训练样本,从而根据现有数据集生成虚拟数据集形成虚实结合的数据集来扩充现有数据集,使训练模型更具泛化能力,解决标签难获得造成的模型过拟合问题。

(5)针对模型适应性问题。在现有基于机器学习的GNSS欺骗检测方法对训练过的欺骗攻击检测性能较好,而对于未训练过的欺骗检测检测精度不高。而在现实情况中几乎不可能获得所有的欺骗攻击数据,为了提高模型的适应性,迁移学习可以提升现有模型检测未知欺骗攻击的能力。同时迁移学习可以让模型通过已有的标记数据向未标记数据迁移,降低模型对数据集样本量的需求。

4 结束语

本文从利用机器学习进行GNSS欺骗干扰检测的基本步骤出发,详细阐述了在相关研究中存在的相关数据集以及数据预处理方法。而后,根据机器学习在GNSS检测中发挥的作用分基于信号分类以及基于信息验证的机器学习GNSS检测进行分析与总结。最后,思考了关于检测时延与可靠性、检测实时性、模型轻量化、数据标签难获得以及模型适应性的问题,并提出了相应的发展趋势。

参考文献:

[1] JOUBERT N, REID T G R, NOBLE F. Developments in modern GNSS and its impact on autonomous vehicle architectures[C]//Proceedings of the 2020 IEEE Intelligent Vehicles Symposium, 2020: 2029-2036.

[2] JING H, GAO Y, SHAHBEIGI S, et al. Integrity monitoring of GNSS/INS based positioning systems for autonomous vehicles: state-of-the-art and open challenges[J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(9): 14166-14187.

[3] LYU C, ZHAN R. Global analysis of active defense technologies for unmanned aerial vehicle[J]. IEEE Aerospace and Electronic Systems Magazine, 2022, 37(1): 6-31.

[4] LYU X, HU B, WANG Z, et al. A SINS/GNSS/VDM integrated navigation fault-tolerant mechanism based on adaptive information sharing factor[J]. IEEE Transactions on Instrumentation and Measurement, 2022, 71: 1-13.

[5] GROVES P D, LONG D C. Combating GNSS interference with advanced inertial integration[J]. Journal of Navigation, 2005, 58(3): 419-432.

[6] CELIS R D, CADARSO L. GNSS/IMU laser quadrant detector hybridization techniques for artillery rocket guidance[J]. Nonlinear Dynamics, 2018, 91(4): 2683-2698.

[7] WANG S, WANG J, SU C, et al. Intelligent detection algorithm against UAVs' GPS spoofing attack[C]//Proceedings of the 2020 IEEE 26th International Conference on Parallel and Distributed Systems, 2020: 382-389.

[8] ZHU X, HUA T, YANG F, et al. Global positioning system spoofing detection based on support vector machines[J]. IET Radar, Sonar & Navigation, 2022, 16(2): 224-237.

[9] BOSE S C. GPS spoofing detection by neural network machine learning[J]. IEEE Aerospace and Electronic Systems Magazine, 2022, 37(6): 18-31.

[10] SIEMURI A, KUUSNIEMI H, ELMUSRATI M S, et al. Machine learning utilization in GNSS—use cases, challenges and future applications[C]//Proceedings of the 2021 International Conference on Localization and GNSS, 2021: 1-6.

[11] DANG Y. Machine learning based GNSS spoofing detection and mitigation for cellular-connected UAVs[D]. Helsinki: Aalto University, 2023.

[12] SIEMURI A, SELVAN K, KUUSNIEMI H, et al. A systematic review of machine learning techniques for GNSS use cases[J]. IEEE Transactions on Aerospace and Electronic Systems, 2022, 58(6): 5043-5077.

[13] JUNZHI L, WANQING L, QIXIANG F, et al. Research progress of GNSS spoofing and spoofing detection technology [C]//Proceedings of the 2019 IEEE 19th International Conference on Communication Technology, 2019: 1360-1369.

[14] MENG L, YANG L, YANG W, et al. A survey of GNSS spoofing and anti-spoofing technology[J]. Remote Sensing, 2022, 14(19): 4826.

[15] 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.

[16] 张鑫. 卫星导航欺骗干扰信号检测技术综述[J]. 全球定位系统, 2018, 43(6): 1-7.
ZHANG X. Overview of satellite navigation spoofing signal detection technology[J]. GNSS World of China, 2018, 43 (6): 1-7.

[17] 刘清秀, 程玉, 王国栋, 等. 北斗卫星导航欺骗与抗欺骗技术现状探讨[J]. 导航与控制, 2021, 20(4): 24-32.
LIU Q X, CHENG Y, WANG G D, et al. Discussion on detection and anti-deception technology of Beidou satellite navigation[J]. Navigation and Control, 2021, 20(4): 24-32.

[18] BIAN S, JI B, HU Y. Research status and prospect of GNSS anti-spoofing technology[J]. Scientia Sinica Informationis, 2017, 47(3): 275-287.

[19] AISSOU G, SLIMANE H O, BENOUADAH S, et al. Tree-based supervised machine learning models for detecting GPS spoofing attacks on UAS[C]//Proceedings of the 2021 IEEE 12th Annual Ubiquitous Computing, Electronics &

Mobile Communication Conference, 2021: 649-653.

[20] TALAEI KHOEI T, ISMAIL S, SHAMAILEH K A, et al. Impact of dataset and model parameters on machine learning performance for the detection of GPS spoofing attacks on unmanned aerial vehicles[J]. Applied Sciences, 2022, 13(1): 383.

[21] KHOEI T T, AISSOU G, AL SHAMAILEH K, et al. Supervised deep learning models for detecting GPS spoofing attacks on unmanned aerial vehicles[C]//Proceedings of the 2023 IEEE International Conference on Electro Information Technology, 2023: 340-346.

[22] AISSOU G, BENOUADAH S, EL ALAMI H, et al. Instance-based supervised machine learning models for detecting GPS spoofing attacks on UAS[C]//Proceedings of the 2022 IEEE 12th Annual Computing and Communication Workshop and Conference, 2022: 208-214.

[23] KHOEI T T, GASIMOVA A, AHAJJAM M A, et al. A comparative analysis of supervised and unsupervised models for detecting GPS spoofing attack on UAVs[C]//Proceedings of the 2022 IEEE International Conference on Electro Information Technology, 2022: 279-284.

[24] GASIMOVA A. Performance comparison of weak and strong learners in detecting GPS spoofing attacks on unmanned aerial vehicles (UAVs)[D]. Grand Forks: University of North Dakot, 2022.

[25] GASIMOVA A, KHOEI T T, KAABOUCH N. A comparative analysis of the ensemble models for detecting GPS spoofing attacks on UAVs[C]//Proceedings of the 2022 IEEE 12th Annual Computing and Communication Workshop and Conference, 2022: 310-315.

[26] KHOEI T T, ISMAIL S, KAABOUCH N. Dynamic selection techniques for detecting GPS spoofing attacks on UAVs [J]. Sensors, 2022, 22(2): 662.

[27] ESHMAWI A A, UMER M, ASHRAF I, et al. Enhanced machine learning ensemble approach for securing small unmanned aerial vehicles from GPS spoofing attacks[J]. IEEE Access, 2024, 12: 27344-27355.

[28] LOHAN E S, FERRE R M, RICHTER P, et al. GNSS navigation threats management on-board of aircraft[J]. INCAS Bulletin, 2019, 11(3): 111-125.

[29] HUMPHREYS T, BHATTI J, SHEPARD D, et al. The texas spoofing test battery: toward a standard for evaluating GPS signal authentication techniques[J]. Proceedings of the 25th International Technical Meeting of the Satellite Division of the Institute of Navigation, 2012: 3569-3583.

[30] HUMPHREYS T. TEXBAT data sets 7 and 8[EB/OL]. (2016-02-26) [2024-01-29]. https://rnl-data. ae. utexas. edu/datastore/texbat/texbat_ds7_and_ds8.pdf.

[31] ALBRIGHT A, POWERS S, BONIOR J, et al. A tool for furthering GNSS security research: the oak ridge spoofing and interference test battery[C]//Proceedings of the 33rd International Technical Meeting of the Satellite Division of the Institute of Navigation, 2020: 3697-3712.

[32] ISLAM S, BHUIYAN M Z H, LIAQUAT M, et al. An open GNSS spoofing data repository: characterization and impact analysis with FGI-GSRx open-source software-defined receiver [EB/OL]. (2024-03-12)[2024-04-09]. https://www.research-square.com/article/rs-4021306/v1.

[33] WANG X, YANG J, HUANG M, et al. GNSS interference and spoofing dataset[J]. Data in Brief, 2024, 54: 110302-110316.

[34] CALVO-PALOMINO R, BHATTACHARYA A, BOVET G, et al. Short: LSTM-based GNSS spoofing detection using low-cost spectrum sensors[C]//Proceedings of the 2020 IEEE 21st International Symposium on "A World of Wireless, Mobile and Multimedia Networks", 2020: 273-276.

[35] SUN Y, YU M, WANG L, et al. A deep-learning-based GPS signal spoofing detection method for small UAVs[J]. Drones, 2023, 7(6): 370.

[36] NAYFEH M, LI Y, SHAMAILEH K A, et al. Machine learning modeling of GPS features with applications to UAV location spoofing detection and classification[J]. Computers & Security, 2023, 126: 103085.

[37] ALAMI E H, HALL K, RAWAT D B. Comparative study of machine learning techniques for detecting GPS spoofing attacks on mission critical military IoT devices[C]//Proceedings of the 2023 IEEE International Conference on Communications Workshops, 2023: 512-517.

[38] SEMANJSKI S, SEMANJSKI I, WILDE D W, et al. Use of supervised machine learning for GNSS signal spoofing detection with validation on real-world meaconing and spoofing data—part I[J]. Sensors, 2020, 20(4): 1171.

[39] SUNG Y H, PARK S J, KIM D Y, et al. GPS spoofing detection method for small UAVs using 1D convolution neural network[J]. Sensors, 2022, 22(23): 9412.

[40] FERRE M R, FUENTE D L A, LOHAN E S. Jammer classification in GNSS bands via machine learning algorithms[J]. Sensors, 2019, 19(22): 4841.

[41] IQBAL A, AMAN M N, SIKDAR B. A deep learning based induced GNSS spoof detection framework[J]. IEEE Transactions on Machine Learning in Communications and Networking, 2024, 2: 457-478.

[42] 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, 2020: 1-5.

[43] HUANG C, CHEN Z, PENG X, et al. A GNSS spoofing detection method based on CNN-DOA[C]//Proceedings of the China Satellite Navigation Conference, 2024: 402-414.

[44] SHAFIEE E, MOSAVI M R, MOAZEDI M. Detection of

spoofing attack using machine learning based on multi-layer neural network in single-frequency GPS receivers[J]. Journal of Navigation, 2018, 71(1): 169-188.

[45] IQBAL A, AMAN M N, SIKDAR B. Machine learning based time synchronization attack detection for synchrophasors[C]// Proceedings of the 2023 IEEE Global Communications Conference, 2023: 2251-2256.

[46] 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, 2020: 3241-325.

[47] LI J, ZHU X, OUYANG M, et al. GNSS spoofing jamming detection based on generative adversarial network[J]. IEEE Sensors Journal, 2021, 21(20): 22823.

[48] ZARRINNEGAR K, TOHIDI S, MOSAVI M R, et al. Improving cross ambiguity function using image processing approach to detect GPS spoofing attacks[J]. Iranian Journal of Electrical and Electronic Engineering, 2023, 19(1): 2584.

[49] CHEN Z, LI J, LI J, et al. GNSS multiparameter spoofing detection method based on support vector machine[J]. IEEE Sensors Journal, 2022, 22(18): 17864-17874.

[50] ZUO S, LIU Y, ZHANG D, et al. Detection of GPS spoofing attacks based on isolation forest[C]//Proceedings of the 2021 IEEE 9th International Conference on Information, Communication and Networks, 2021: 357-361.

[51] 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, 2019: 1-6.

[52] SHAFIQUE A, MEHMOOD A, ELHADEF M. Detecting signal spoofing attack in UAVs using machine learning models[J]. IEEE Access, 2021, 9: 93803-93815.

[53] LI J, LI W, HE S, 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, 2020: 625-629.

[54] PARDHASARADHI B, YAKKATI R R, CENKERAMADDI L R. Machine learning-based screening and measurement to measurement association for navigation in GNSS spoofing environment[J]. IEEE Sensors Journal, 2022, 22(23): 23423-23435.

[55] QIN W, DOVIS F. Situational awareness of chirp jamming threats to GNSS based on supervised machine learning[J]. IEEE Transactions on Aerospace and Electronic Systems, 2022, 58(3): 1707-1720.

[56] LI J, CHEN Z, RAN Z, et al. The GNSS spoofing detection method based on AdaBoost[C]//Proceedings of the 2023 6th International Symposium on Autonomous Systems, 2023: 1-6.

[57] 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.

[58] WEI X, WANG Y, SUN C. PerDet: machine-learning-based UAV GPS spoofing detection using perception data[J]. Remote Sensing, 2022, 14(19): 4925.

[59] ZHANG K, TUHIN R A, PAPADIMITRATOS P. Detection and exclusion RAIM algorithm against spoofing/replaying attacks[C]//Proceedings of the International Symposium on GNSS 2015, 2015: 81-90.

[60] FENG Z, SEOW C K, CAO Q. GNSS anti-spoofing detection based on Gaussian mixture model machine learning [C]//Proceedings of the 2022 IEEE 25th International Conference on Intelligent Transportation Systems, 2022: 3334-3339.

[61] IQBAL A, AMAN M N, SIKDAR B. Machine and representation learning based GNSS spoofing detectors utilizing feature set from generic GNSS receivers[J]. IEEE Transactions on Consumer Electronics, 2024, 70(1): 574-583.

[62] ZHANG X, HUANG Y, TIAN Y, et al. Noise-like features-assisted GNSS spoofing detection based on convolutional autoencoder[J]. IEEE Sensors Journal, 2023, 23(20): 25473-25486.

[63] BREWINGTON J, KAR D. UAV GPS spoofing detection via neural generative one-class classification[C]//Proceedings of the 24th International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing, 2023: 492-497.

[64] ROY D, MUKHERJEE T, RIDEN A, et al. GANSAT: a GAN and satellite constellation fingerprint-based framework for GPS spoof-detection and location estimation in GPS deprived environment[J]. IEEE Access, 2022, 10: 45485-45507.

[65] JULLIAN O, OTERO B, STOJILOVIĆ M, et al. Deep learning detection of GPS spoofing[C]//Proceedings of the Machine Learning, Optimization, and Data Science, 2022: 527-540.

[66] ABDULLAYEVA F, VALIKHANLI O. Development of a method for detecting GPS spoofing attacks on unmanned aerial vehicles[J]. Problems of Information Technology, 2022, 13(1): 3-8.

[67] LI J, ZHU X, OUYANG M, et al. Research on multi-peak detection of small delay spoofing signal[J]. IEEE Access, 2020, 8: 151777-151787.

[68] BORHANI-DARIAN P, LI H, WU P, et al. Detecting GNSS spoofing using deep learning[J]. EURASIP Journal on Advances in Signal Processing, 2024(1): 14.

[69] MENG L, YANG L, REN S, et al. An approach of linear regression-based UAV GPS spoofing detection[J]. Wireless Communications and Mobile Computing, 2021: 1-16.

[70] ZHANG G, MENG W, MA X, et al. LSTM network based

spoofing detection and recognition in a GNSS receiver[C]// Proceedings of the China Satellite Navigation Conference, 2020: 613-622.

[71] XUE N, NIU L, HONG X, et al. DeepSIM: GPS spoofing detection on UAVs using satellite imagery matching[C]// Proceedings of the Annual Computer Security Applications Conference, 2020: 304-319.

[72] GUIZZARO C, FORMAGGIO F, TOMASIN S. GNSS spoofing attack detection by IMU measurements through a neural network[C]//Proceedings of the 2022 10th Workshop on Satellite Navigation Technology, 2022: 1-6.

[73] PANICE G, LUONGO S, GIGANTE G, et al. A SVM-based detection approach for GPS spoofing attacks to UAV[C]// Proceedings of the 2017 23rd International Conference on Automation and Computing, 2017: 1-11.

[74] DASGUPTA S, GHOSH T, RAHMAN M. A reinforcement learning approach for global navigation satellite system spoofing attack detection in autonomous vehicles[J]. Transportation Research Record: Journal of the Transportation Research Board, 2022, 2676(12): 318-330.

[75] DASGUPTA S, RAHMAN M, ISLAM M, et al. Prediction-based GNSS spoofing attack detection for autonomous vehicles[J]. arXiv: 2010.11722, 2020.

[76] JIANG P, WU H, XIN C. DeepPOSE: detecting GPS spoofing attack via deep recurrent neural network[J]. Digital Communications and Networks, 2022, 8(5): 791-803.

[77] DASGUPTA S, RAHMAN M, ISLAM M, et al. A sensor fusion-based GNSS spoofing attack detection framework for autonomous vehicles[J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(12): 23559-23572.

[78] DANG Y, BENZAID C, SHEN Y, et al. GPS spoofing detector with adaptive trustable residence area for cellular based-UAVs [C]//Proceedings of the 2020 IEEE Global Communications Conference, 2020: 1-6.

[79] DANG Y, BENZAID C, YANG B, et al. Deep learning for GPS spoofing detection in cellular-enabled UAV systems [C]//Proceedings of the 2021 International Conference on Networking and Network Applications, 2021: 501-506.

[80] DANG Y, BENZAID C, YANG B, et al. Deep-ensemble-learning-based GPS spoofing detection for cellular-connected UAVs[J]. IEEE Internet of Things Journal, 2022, 9(24): 25068-25085.

[81] DANG Y, KARAKOC A, NORSHAHIDA S, et al. 3D radio map-based GPS spoofing detection and mitigation for cellular-connected UAVs[J]. IEEE Transactions on Machine Learning in Communications and Networking, 2023, 1: 313-327.

[82] DANG Y, KARAKOC A, JÄNTTI R. Graphic neural network based GPS spoofing detection for cellular-connected UAV swarm[C]//Proceedings of the 2023 IEEE 97th Vehicular Technology Conference, 2023: 1-6.