计算机工程与应用
*Computer Engineering and Applications*
ISSN 1002-8331,CN 11-2127/TP

# 《计算机工程与应用》网络首发论文

题目： GNSS 欺骗式干扰检测综述
作者： 周彦，王山亮，杨威，易炯，张世仓，蔡成林
网络首发日期： 2022-02-28
引用格式： 周彦，王山亮，杨威，易炯，张世仓，蔡成林．GNSS 欺骗式干扰检测综述[J/OL]．计算机工程与应用．
https://kns.cnki.net/kcms/detail/11.2127.TP.20220227.0944.002.html

# GNSS 欺骗式干扰检测综述

周彦[1]，王山亮[1]，杨威[2]，易炯[2]，张世仓[3]，蔡成林[1]
1.湘潭大学 自动化与电子信息学院，湖南 湘潭 411105
2.长沙海格北斗信息技术有限公司，长沙 410003
3.中国航空工业集团公司雷华电子技术研究所，江苏 无锡 214000

**摘 要：**近年来，随着卫星导航系统在军事监测、精细农业、交通监控、资源勘探、灾害评估等领域的广泛应用，提高卫星导航系统的安全性和鲁棒性成为研究的热点。本文首先介绍了卫星导航欺骗式干扰的原理与分类，根据卫星信号从生成到最终实现定位导航这一过程和基于统计学层面将当前的欺骗式干扰检测技术分成基于导航数据信息、基于空间处理、基于射频前端处理、基于基带数字信号处理、基于定位导航运算结果和基于机器学习等六大类，并对每类采用的检测方法进行性能对比，最后从实时检测和综合检测两个方面对未来的欺骗式干扰检测进行展望。

**关键词：**卫星导航；欺骗式干扰检测；欺骗式干扰；安全性；导航数据
文献标志码：A 中图分类号：TP31 doi：10.3778/j.issn.1002-8331.2201-0055

## Overview of GNSS Spoofing Jamming Detection

ZHOU Yan[1], WANG Shanliang[1], YANG Wei[2], YI Jiong[2], ZHANG Shicang[3], CAI Chenglin[1]

1. School of Automation and Electronic Information, Xiangtan University, Xiangtan, Hunan 411105, China
2. Changsha HaigeBeidou Information Technology Co. Ltd, Changsha, Hunan 410003, China
3. Leihua Electronic Technology Research Institute of Aviation Industry Corporation of China, Wuxi, Jiangsu 214000, China

**Abstract:** In recent years, with the wide application of satellite navigation systems in military monitoring, precision agriculture, traffic monitoring, resource exploration, disaster assessment and other fields, improving the safety and robustness of satellite navigation systems has become a research hotspot. This paper first introduces the principle and classification of satellite navigation deceptive jamming. According to the process from the generation of satellite signals to the final realization of positioning and navigation, and based on the statistical level, the current deceptive jamming detection technology is divided into navigation data information based, space processing based, Based on six categories: radio frequency front-end processing, baseband digital signal processing, positioning and navigation calculation results, and machine learning, the performance of the detection methods used in each category is compared. Deceptive jamming detection looks ahead.

**Key words:** satellite navigation; spoofing jamming detection; spoofing jamming; safety; navigation data

**基金项目：**航空科学基金(20200020114004)，湖南省高新技术产业科技创新引领计划项目(2020GK2036)，国家自然科学基金(61773330)。
**作者简介：**周彦(1978－)，男，博士，教授，研究方向为多传感器信息融合、视觉导航、机器视觉等，E-mail：yanzhou@xtu.edu.cn；王山亮(1995－)，男，硕士研究生，研究方向为卫星导航干扰检测；蔡成林(1969－)，男，博士，教授，研究方向为卫星导航、无线通信。

全球卫星导航系统（Global Satellite Navigation System, GNSS）通常意义上泛指所有的导航卫星系统，包括全球的、区域的和增强的系统。目前世界上有四种主要的 GNSS 系统，分别是美国的 GPS、俄罗斯的 GLONASS、欧盟的 Galileo 以及我国自主建设、独立运行的北斗卫星导航系统（BDS）。其主要思想就是通过位于空间的导航卫星发射无线电导航信号实现终端设备的导航、定位与授时功能[1]。

卫星导航系统已经成为人们日常生活和工业活动中不可缺少的一部分。如今，卫星导航系统已服务于交通[2,3]、电力[4]、金融[5]、通信[6]、农林牧渔[7-10]等各行各业，并赋能各行业提质升级，这显示出 GNSS 巨大的应用价值。然而，GNSS 设备的使用在使公众的生活更加便利的同时，也带来了一定的潜在威胁。由于导航卫星距离地面 2 万~3 万千米，导航信号到达地面时非常微弱。因此，GNSS 终端非常容易受到有意或无意的干扰。而正是由于干扰的存在，使得接收终端无法工作或者即使捕获、锁定卫星信号，解算出来的位置、速度、时间（PVT）结果精度也会很低。更甚者，当不法分子利用发射设备发射虚假的导航信号并被接收终端捕获时，接收终端最终解算出虚假的导航授时信息，严重情况下会将导致社会关键基础设施瘫痪、军事行动失败等后果。

近些年，全球频频发生的卫星干扰事件也证明了 GNSS 信号的脆弱性。2011 年 12 月，伊朗军方利用 GPS 欺骗设备成功捕获一架美军隐形无人侦察机 RQ-170[11]。2017 年 6 月 22 日至 24 日期间，在黑海作业的 20 多艘船只受到了所谓的大规模诱骗攻击，其 GPS 导航系统错误地将船舶定位在了距航行位置数英里外的机场。2019 年 11 月，北约多国联合部队举办的三叉戟军事演习期间，芬兰北部地区以及东北部地区 GPS 信号出现了明显的干扰情况，使得大批民航客机上的航电设备受到干扰滞留机场无法起飞，芬兰空军原本的军事演习计划也受到了很大的影响。

由以上列出的事件不难想象，有针对性地进行卫星欺骗导航的后果往往不堪设想。而且随着软件定义无线电技术和开源导航模拟软件的不断发展，欺骗的实施成本和技术门槛也逐步降低。因此，卫星导航欺骗式干扰检测的研究对卫星导航安全、可靠地提供服务具有十分重要的意义。

## 1 卫星导航欺骗式干扰原理及分类

根据欺骗信号生成方式的不同，目前欺骗式干扰主要分为两类，即生成式欺骗干扰和转发式欺骗干扰。

生成式欺骗干扰是在已知民用码的产生方式前提下，自主发射与真实卫星信号相似的欺骗信号，然后通过发射模块辐射到目标接收机，目标接收机在捕获到欺骗信号后，通过真实信号与欺骗信号的相关峰的相对运动，欺骗信号相关峰借由功率优势逐渐将真实信号相关峰剥离跟踪环路，随后被目标接收机锁定，从而得到错误的伪距测量值，解算得到错误的 PVT 信息，达到欺骗目的。因为干扰源不依赖 GPS 系统，所以隐蔽性很强，同时干扰源可以根据自身的需求对各项参数进行调整，灵活度高，但实施的成本相对较高，此外，对于信号结构不公开的军码，可行性不高，这也限制了其应用范围。产生式欺骗干扰模型如图 1 所示。

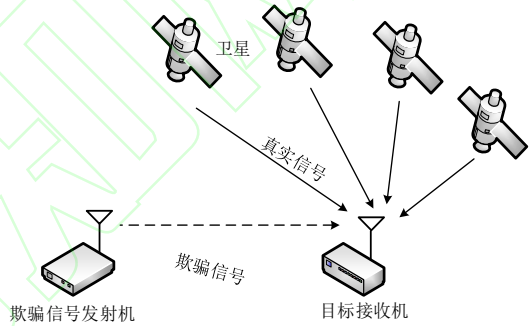


**图 1 生成式欺骗干扰模型**

Fig.1 Model of generative spoofing jamming

转发式欺骗干扰就是干扰机通过自身天线接收真实的卫星信号，然后经过适当的延迟和功率放大后发射出去。在这一过程中，干扰机不需要伪码进行码相关及方程解算处理，所以不受军码加密的限制，可以应用于对军用信号的欺骗干扰，且实施成本相对较低。但相比于生成式欺骗干扰，转发式欺骗干扰信号有个突出的特征，就是干扰信号到达目标接收机的时延一定大于真实信号到达目标接收机的时延。此外，转发式欺骗干扰只能通过改变伪距测量值来实现，其控制性相对较差。转发式欺骗干扰模型如图 2 所示。

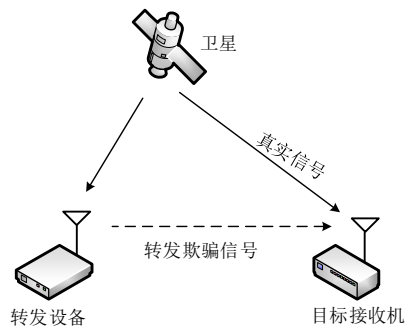


**图 2 转发式欺骗干扰模型**

Fig.2 Model of forward spoofing jamming

## 2 欺骗式干扰检测技术研究现状

卫星信号从产生到最终实现导航定位一般经历如下过程：卫星生成导航卫星信号，经过大气层之后辐射到天线，天线将电磁波转换成高频电流，通过接收机射频前端处理模块后变成数字中频信号，经过基带数字信号处理模块后得到 GPS 测量值和导航电文，最后进行解算后实现定位导航[12]。如图 3 所示。

近些年，国内外众多高校和研究机构在欺骗干扰以及欺骗信号对接收机的影响方面做了很多的研究，同时也提出了许多的欺骗干扰信号检测方法。根据卫星信号从生成到最终实现导航定位这一过程的变化和基于统计学层面，将检测方法大致归纳为六类，即基于导航数据信息的欺骗式干扰检测、基于空间处理欺骗式干扰检测、基于射频前端欺骗式干扰检测、基于基带数字信号处理欺骗式干扰检测、基于定位导航运算结果欺骗式干扰检测和基于机器学习的欺骗式干扰检测。

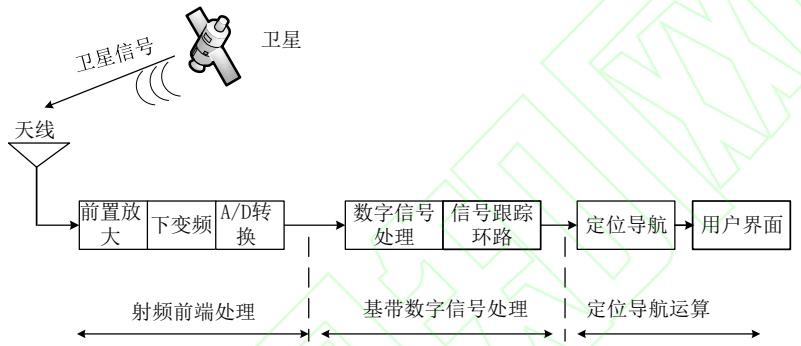


**图 3 卫星信号历经图**

Fig.3 Satellite signal ergodic map

### 2.1 基于导航数据信息的欺骗式干扰检测

基于导航数据信息的欺骗干扰检测方法主要是对信号导航信息进行加密处理，通过添加类似于密码学里的信号加密特征，从而使攻击者很难获得并改变卫星信号里的导航信息，大大增强信息的安全性。由于军码在设计之初就已经进行了加密处理，故而信号加密一般针对民用信号。早在 2003 年 Scott 在文献[13]中就提出了对民用信号进行加密认证这一思想。根据从数据层面和信号层面将信号加密认证分为两类，即扩频码验证（SCA）、导航信息认证（NMA）。

SCA 就是在 GNSS 的伪码上调制一个加密的安全码[14]，通过校验伪码上的不可预测的特征，来验证伪码码片的真实性。如文献[15]利用超音速码加密民用信号;文献[16]用短序列扩频安全码修改导航信息。因为除非欺骗方预先获取到加密信息，否则很难准确预测到伪码码片，故而这类方法安全性很高，但需要改变标准信号协议。此外，对接收机也要进行改造，改造后的接收机需要有一个附加的缓冲区来存储接收到的射频信号，同时还需要一个独立的高精度的同步时钟[17]，成本较高。

NMA 一般通过生成和验证加密数字签名算法，使用受控的密钥对 GNSS 导航数据进行标识[18]。NMA 的实现方式主要有两种：即数字签名技术和延迟的对称密钥传输协议技术。数字签名技术能够提供简单且标准的数据认证方式。一般的数字签名算法有 RSA 和 DSA 算法，但此类算法会造成数据开销较大的问题。为此，文献[19]使用椭圆曲线数字签名算法（ECDSA）解决数字签名引起的数据开销问题。文献[20]提出了一种比 ECDSA 更优的认证方案。延迟的对称密钥传输协议技术是建立在单向哈希链基础上实现的。当前属于此类协议的有两种：即时间效应流丢失容错认证（TESLA）和高效多链流签名（EMSS）。TESLA 通过密钥延迟发布技术将最初的对称加密模型变为非对称加密模型,其需要发送方和接收方预先同步时钟。文献[21]就 TESLA 协议进行修改，以便让所有卫星使用单一密钥链。EMSS 使用的是一连串的哈希链，同时对最后一个哈希链数字签名，该方法不需要时钟同步，但要求接收机同时接收数字签名和哈希值。为了安全可靠，NMA 一般对整个导航信息进行加密，这就需要修改导航信号的接口规范，给应用带来了很大不便[22]。

值得一提的是，文献[23]将扩频码加密和导航电文加密结合起来，利用分组密码算法加密验证消息，用非对称加密算法和密码杂凑算法生成签名，同时使用扩频调制技术将其隐藏在导航信息中，最终成功检测欺骗攻击。文献[24]提出一种卫星和接收机之间的

双向身份认证和通信会话密钥协商的加密认证方案，可以抵御转发式欺骗干扰，不增加额外的卫星和接收机硬件成本，但是需要地面控制中心参与其中。

民用卫星信号的信号加密技术的实施，虽然可以保证用户的安全可靠，不容易上当受骗，且接收方的授权应用程序可以避免接收方的额外硬件开销，但要做到这一点却非常困难。因为加密信息是一项庞大的工程，需要由国家层面对整个卫星导航信号体制进行更改，成本相对较高，对接收方也需要进行一些改进。对于目前数量极其庞大的 GNSS 民用接收机来说，该技术的应用在短期内很难实现。此外，由于转发式欺骗干扰并没有改变导航数据的比特位，故而仅仅通过信号加密认证来应对转发式欺骗干扰往往是不可行的，可以结合非电文加密技术中的到达时检测技术，来提高接收机的安全性。

对于导航电文加密技术和扩频码加密技术的比较如下表所示：

**表 1　NMA 和 SCA 性能比较**

Table 1 Performance comparison of NMA and SCA

| 技术名称 | 实现方式 | 优点 | 缺点 | 适用场景 |
|---|---|---|---|---|
| 扩频码验证 | 伪码上调制一个加密的安全码 | 相比于 NMA，具有更高的安全性 | 改变了标准信号协议；需要对接收机结构进行改造，成本高；对转发式欺骗干扰的检测效果很低 | 生成式欺骗干扰、调零干扰、前向估计攻击 |
| 导航信息认证 | 通过生成和验证加密数字签名的算法，使用受控的密钥对 GNSS 导航数据进行标识 | 不改变信号调制方式；不需要改变接收机硬件结构；计算量增加较少 | 需要修改导航信号的接口规范；对转发式欺骗干扰的检测效果很低 | 生成式欺骗干扰、调零干扰 |

## 2.2 基于空间信息处理的欺骗式干扰检测

欺骗式干扰源通常从同一天线发射多个欺骗信号，而真实信号则从不同方向的不同卫星发射，如图 4 所示。因此，可以利用空间处理技术来估计接收信号的空间特征，并识别那些空间相关的信号[25]。由于卫星的空间几何信息几乎不可能被模仿，因此信号的来向检测是当前实现欺骗干扰检测最有效的方法之一。

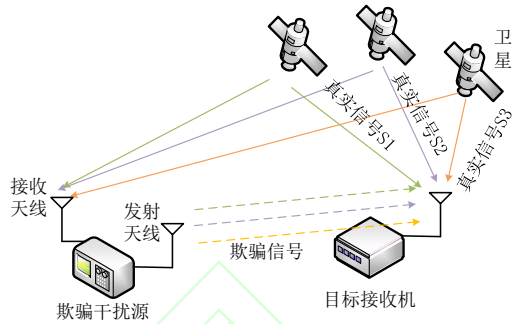


**图 4　真实/欺骗信号空间信息图**

Fig.4　Real/spoofed signal spatial infographic

鉴于此，文献[26]和[27]通过单天线接收机在运动过程中不同历元时刻相关器的输出来进行欺骗干扰检测。但是此类方法一般都需要接收机进行大量地计算处理，且需要对接收机算法进行大量修改，这无疑加大了接收机的负荷，于是有人就提出将天线进行简单的改造，即让其旋转起来，通过对天线匀速旋转条件下接收机输出载波相位测量值的处理，实现欺骗干扰信号的到达角检测，无需修改接收机信号处理算法[28]。但无论是基于固定单天线还是经过改造后的旋转单天线，其都有一个很大的弊端，即只能运用于固定安装在已知位置的场景，为了解决这一问题，张鑫等[29]提出了基于旋转双天线的检测方案，通过将两个阵元的输出序列作差，消除平动项的影响，这样就具备了在移动载体上进行欺骗干扰检测的能力。当欺骗信号单一或者通过位于不同空间位置的天线发射出来时，以上检测方案就会失效，针对此情形，文献[30]提出了一种利用双天线和干涉仪对 GPS 载波信号进行方位角估计的方法，从而实现欺骗干扰检测，但是增加的干涉仪同样也增加了检测成本。文献[31]采用两个低成本的固定的 GNSS 天线形成基线矢量，然后将载波相位双差数据与星历数据相结合求出基线向量，继而实现干扰检测。但是该检测方法要求两根 GNSS 天线固定，这是其应用范围大打折扣，无法适用于动态场景。此外，利用天线阵列也可以实现对单一欺骗信号或来自多方向欺骗信号的检测，通过天线阵列彼此之间已知的空间关系对欺骗信号形成制约，从而很容易实现来自不同发射天线的欺骗干扰检测，同时也能将欺骗干扰信号消除[32-34]。文献[35]提出一种基于阵列天线的卫星和欺骗器到达方向(DoA)估计的欺骗探测技术,采用压缩感知的正交匹配追踪(OMP)方法，在样本数量较少的情况下,精确估计所有 PRN 信号的 DoA，并对所有 PRN 信号的 DoA 估计结果进行欺骗检测。该方法在复杂的欺骗场景中仍有较好的检测效果。

基于空间处理的欺骗干扰检测方法，一般来说，接收天线数量少，接收机在处理时就要进行大量计算，同时最后的检测效果相对于多天线的也较差，应用范围有限。当增加接收天线数量时，虽然会提升检测效果，但相应的也提高了系统硬件成本，此外通过采用特殊性能的天线[36]也可以实现欺骗干扰的有效检测，但特制天线的使用也提升了整个检测系统的成本，不便于大范围推广使用。基于信号空间几何信息的检测方法的比较如下表所示：

**表 2　信号空间几何信息的检测方法比较**

Table 2　Comparison of detection methods of signal spatial geometric information

| 天线信息 | | 性能比较 | | |
|---|---|---|---|---|
| 天线数量 | 天线运动状态 | 优点 | 缺点 | 适用范围 |
| 单天线 | 运动 | 结构简单，可操作性高；成本低 | 检测效果较差 | 适用于简单的欺骗攻击 |
| 双天线 | 静止 | 成本相对适中，不需要对天线进行改造；检测效果较好 | 适用范围较窄，无法应用于运动场景 | 适用于静态欺骗场景 |
| | 运动 | 适用范围广 | 需要对天线进行改造 | 静态和动态场景均可以适用 |
| 天线阵列 | 天线间相对静止 | 既可以检测出欺骗信号，又可以将欺骗信号消除 | 成本高昂；复杂度高 | 适用于对实时性要求不高的场景 |

## 2.3 基于射频前端处理的欺骗式干扰检测

接收机射频前端处理模块通过天线接收所有可见 GNSS 卫星信号，经前置滤波器和前置放大器的滤波放大后，再与本机振荡器产生的本振信号进行混频而下变频成中频信号，最后经模数转换后将中频信号转换成离散时间的数字中频信号[12]。

接收机射频前端一般都会有自动增益控制（AGC）来用于调整射频前端增益，以使模数转换（ADC）的输入电平在一定范围内保持稳定。在无干扰情况下，AGC 的增益值只会在很小的范围内变化，但是当有功率较大的欺骗干扰信号进入射频前端时，AGC 的增益就会出现较大的波动，于是就可以依据此特征来进行欺骗干扰检测[37]。AGC 增益部分不涉及数字信号处理过程，因此鲁棒性较强，且具有较低的计算复杂度。但是该方法对于像逐步拉偏式这种功率精密控制的欺骗式干扰漏检率会很高。

## 2.4 基于基带数字信号处理欺骗式干扰检测

基带数字信号处理模块通过处理射频前端所输出的数字中频信号，复制出与接收到的卫星信号相一致的本地载波和本地伪码信号，从而实现对 GNSS 信号的捕获与跟踪，并且从中获得 GNSS 伪距和载波相位等测量值以及解调出导航电文[12]。一般来说，当存在欺骗干扰时，欺骗信号和真实信号在经过基带数字信号处理后，其在接收信号强度、信号质量、多普勒频移一致性、信号到达时间等方面会有比较显著的差异，因此通过合适的检测方案将其差异识别出来即可实现欺骗干扰检测。

### 2.4.1 接收信号强度检测

接收信号强度检测是单天线接收机常用的方法，一般是在信号解扩后进行检测。其主要研究思路是当存在欺骗式干扰时，接收到的卫星信号在绝对功率、载噪比（C/N0）、L1/L2 功率比出现异常，通过检测是否出现异常来检测是否存在欺骗式干扰。

绝对功率检测：即通过检测接收到的绝对功率是否远远大于设定的卫星信号真实功率的阈值来发现欺骗信号。由于欺骗干扰机和目标接收机之间的路径损耗变化很大，所以从欺骗干扰机角度，估计在目标接收机上施加足够的信号强度所需的发射功率，同时又不过分超过真实 GPS 信号的功率是一件困难的事[38]。因此，接收一个绝对功率大大高于预期的真实 GPS 信号功率的欺骗干扰信号是检测欺骗攻击的简单而直接的方法[39]。但是对于比较复杂精确的逐步拉偏式欺骗干扰和多径效应，如果仅仅检测信号绝对功率，则漏警率会非常高，检测效果很差。对此，文献[40]提出了一种总信号能量检测的方法，通过建立能分别反映信号分量功率和噪声底面电平的新检测量，实现干扰检测，在欺骗干扰和真实信号的接收强度非常接近的情况下，该方法仍能很好地工作，但是该方法还是无法有效应对多径效应。

C/N0 检测：一般情况下，欺骗干扰装置发射的信号功率会高于实际卫星信号的功率。当有大功率欺骗信号攻击 GPS 接收机时，接收机接收到的 C/N0 可能会突然变化。该方法通过持续监测 C/N0 的变化，查找可能是攻击迹象的异常变化，从而发现是否存在欺骗干扰信号[41]。同样地，该方法对于比较复杂精确的逐步拉偏式欺骗干扰的检测效果很差。

L1/L2 功率对比度检测：是基于接收机可以同时监测 GPS 中 L1 和 L2 信号的功率，而低精度的欺骗设

备可能只能欺骗 L1 信号中的干扰,因此，通过检测 L1 和 L2 的功率电平异常差异或 L2 信号是否存在，就有可能检测到是否存在欺骗干扰信号[42]。然而，大多数民用接收机无法同时监测 L1 和 L2 波段，这限制了该检测技术的应用范围。基于信号幅度的检测方法性能比较如下所示：

**表 3　信号强度检测方法比较**

Table 3　Comparison of signal strength detection methods

| 欺骗检测方法 | 特征差异 | 实现难度 | 场景适用性 |
|---|---|---|---|
| 绝对功率检测 | 欺骗信号具有更高的信号功率 | 低 | 中等 |
| C/N0 检测 | 欺骗信号具有更高的载噪比 | 低 | 中等 |
| L1/L2 功率对比度检测 | 欺骗信号 L1 和 L2 功率有差异 | 中等 | 低 |

### 2.4.2 信号质量检测

信号质量检测(SQM)技术是基于欺骗干扰信号与真实卫星信号的相互作用，导致跟踪相位相关峰值失真，通过对 GNSS 接收机跟踪环路中早码、即时码和晚码相关器的输出值进行计算,识别相关函数的形变。SQM 一般通过检测相关峰的不对称性或相关峰的异常尖锐和平坦这两个指标来监测信号相关峰可能的失真和异常[43]，其对应的检测算法分别是 Delta 算法和 Ratio 算法[44]。当前主要通过监测相关峰在时域和频域上对真实信号和欺骗信号进行分析，找出差异特征，最终实现检测。

在时域上，针对小时延欺骗信号检测问题上，文献[45]在捕获阶段获取二维搜索矩阵，并利用卷积神经网络实现欺骗干扰信号的识别,最终实验得出在 0.5 个码片及以上的欺骗与真实卫星信号码相位差下，可以有效识别欺骗信号。针对大时延欺骗信号和小时延欺骗信号检测问题上，文献[46]提出了一种信号捕获阶段的联合检测方案，通过检测相关峰的个数实现对大时延转发式欺骗干扰的检测，利用相关峰的半高宽（FWHM）实现对小时延欺骗信号的检测。文献[47]提出一种检测码跟踪环中过零点 S 曲线偏差（SCB）方差值变化的中级欺骗干扰检测方法。文献[48]提出一种通过多个相关器测量自相关函数变形的检测方法。对于以上采用的标量跟踪结构，SQM 可以根据相关峰重叠对相干积分结果的影响有效检测欺骗干扰。但是，当重叠不存在时，这些方法是无效的。对此文献[49]采用矢量跟踪结构对所有接收信号进行联合跟踪，发现无论是否存在重叠，相干积分结果都会受到欺骗干扰的影响，从而最终实现干扰检测。

在频域上，文献[50]利用 GPS 卫星信号的码相关特性和转发信号的时延特性，提出了一种基于 FFT 的卫星信号转发式欺骗干扰检测方法，此方法可以有效识别转发延迟不小于 1.5 个码片的欺骗干扰信号。文献[51]依据接收机捕获结果中伪码相关峰呈现三角形的特点，提取相关三角形两侧斜率值，并结合快速傅里叶变换（FFT）快速捕获算法，提出基于伪码相关峰斜率正负跳变和斜率峰值等间隔分布的转发式干扰检测方法。

信号质量检测因其简单性和有效性而在多径检测和欺骗检测中备受青睐,但是其检测效果受到真实信号与欺骗信号相关峰间隔有关,而且当干扰源采用压制式干扰时，欺骗信号占据跟踪环路，此时欺骗信号在与真实卫星信号相互作用后,欺骗信号凭借功率优势使得相关峰的失真很小，从而出现漏检的情形，故而一般采用多种策略协同检测，先检测是否有压制式干扰，确定没有后,再分别采用针对大时延欺骗信号和小时延欺骗信号的检测方法，从而提升整个检测方案的完整性，但如果采用直接将多种欺骗检测结果相或的方法,则检测性能将会随着某一种检测器性能下降而下降[52]。因此，如果发现某一个检测器性能误差超过门限,则在融合过程中剔除该检测方案,从而可以保证当一种检测方法失效不会影响融合后的整体性能。

### 2.4.3 多普勒频移一致性检测

多普勒频移是由卫星和接收机间的相对运动造成的，其计算公式如下：

$$f_d = \frac{(\boldsymbol{v} - \boldsymbol{v}^{(s)}) \cdot \boldsymbol{I}^{(s)}}{\lambda} \quad (1)$$

其中，$f_d$：多普勒频移；$\boldsymbol{v}$：接收机的速度；$\boldsymbol{v}^{(s)}$：卫星的运行速度；$\boldsymbol{I}^{(s)}$：卫星在接收机处的单位观测矢量；$\lambda$：波长。

由式(2)分析可知,在 GNSS 信号穿过电离层后，载波多普勒频移与伪码多普勒频移应该保持一致性，即两个频率之比应该为一个常数。然而，欺骗干扰信号往往无法保持这两个参数的一致性，文献[53]据此进行欺骗干扰检测。文献[54]指出可以根据接收机的高度和速度估计多普勒频移的变化。如果接收机遇到欺骗干扰，则多普勒频移的变化会发生异常。文献[55]提出了一种联合利用 GNSS 信号传递的导航信息和接收机垂直往复运动引起的波状多普勒变化的欺骗检测

方法，此方法既能检测单天线欺骗干扰，又能应对多天线欺骗干扰。文献[56]利用载波相位观测和导航信息精确估计一对固定天线的到达频率差，根据观测结果是否与预测结果相一致来判别是否有欺骗干扰。

### 2.4.4 信号到达时间检测

根据 1.2 中转发式欺骗干扰原理可以看到，当使用转发设备对 GNSS 信号进行接收并转发后，目标接收机接收到的欺骗信号必然与真实信号在时间维度上有一定延迟，故可以根据这一特征来检测是否有欺骗信号的入侵。针对信号到达时间的检测方案主要探讨分析伪码和数据位的时间延迟[14,57,58]和 L1/L2 信号的相对时间延迟[38]。利用信号到达时间进行卫星导航欺骗干扰检测，通常对固定位置接收机等有一定效果，对于动态场景其适用性有待提高。

## 2.5 基于定位导航结果的欺骗式干扰检测

卫星信号经过基带数字信号处理模块载波解调和伪码解扩后，得到导航电文同时在解调解扩的过程中，还会得到伪距、速度等信息。有些学者就从这些定位导航结果信息出发，提出一系列检测算法。

Xiao 等[59]利用伪距单差结合方差分析技术通过分析不同信号伪距单差均值的一致性来检测欺骗信号，但是其检测性能受热噪声方差、接收机之间的基线长度以及卫星个数的影响，为此，Liu 等[60]通过双接收机的伪距双差、卫星与载体的距离双差以及卫星钟差双差计算得到误差值，基于误差值的明显差异性实现对信号的检测与判别。Tao 等[61]从速度角度出发，依据多普勒测量和伪距测量都与接收机的速度有关，采用两种计算速度的方法来检验多普勒频移和伪距测量的一致性。Jeong 等[62]通过监测修正伪距和估计距离之间的差异变化来检测欺骗信号，但是该检测方法仅适用于使用地基增强系统(GBAS)数据的系统。

利用其他高精度辅助设备测得的数据信息来与 GNSS 接收机测得数据信息进行一致性比较是另一部分学者的研究思路。

接收机终端之所以容易被恶意干扰，主要是因为其接收的卫星信号易受到电磁干扰。因此，通过引入不受电磁影响的高精度设备，将其测得的数据信息与接收机终端解算的结果进行比对这一思路应运而生。目前可由于辅助检测的设备有很多，如惯性导航系统（INS）、芯片级原子钟、加速度计等。

INS 是一种不依赖于外部信息、也不向外部辐射能量的自主式导航系统。其能够在短时间内提供高精度、高稳定性的导航参数[63]。这些性质恰恰可以用来辅助欺骗干扰检测。文献[64]通过欺骗信号与真实信号在空间几何关系的差异，建立了在正常环境和欺骗场景下伪距/载波相位双差数学模型，并将接收机实际测得的双差观测值与 INS 数据计算的双差观测值进行比对，从而判别是否受到干扰。针对载波相位单差技术无法应用于运动载体，载波相位双差检测技术对多阵元发射的欺骗信号或单路欺骗信号失效这一问题，文献[65]利用干扰源与真实卫星到天线阵距离上的差异这一特征，提出一种惯导辅助的三元天线阵欺骗干扰检测技术，通过运动载体在某一时间段内运动一段距离即可进行欺骗干扰检测。文献[66]通过研究 GNSS 欺骗干扰对 INS/GNSS 的卡尔曼滤波协方差、新息序列和惯性传感器偏差估计的影响，给出了一种基于新息序列和惯性传感器偏差欺骗检测的方案。文献[67]将统计学中的广义似然比应用到干扰检测中，通过对 GNSS 和 IMU 的测量模型进行分析，设计了欺骗干扰检测模型，构建了假设性检验模型，并通过广义似然比检验来实现最终的检测。上述检测方案都是在干扰信号拉偏程度大于纯惯导误差漂移的情形下，最终的检测效果差强人意，但是当遇到不易被 INS 识别的逐步诱导式精细拉偏时，其检测效果就显得不尽人意，针对这一情形，文献[68]从速度和位置两种惯性信息出发，研究了位置欺骗和速度欺骗对伪距测量和伪距率测量带来的影响，并结合 INS 短时间位置误差传播模型，分析了真实信号和欺骗信号下伪距和伪距率变化的一致性关系，并构造了时间序列模型来实现信号的判别。

商业化芯片级原子钟产品具有小体积、高稳定度、低功耗等特点，这些优点也使其在欺骗干扰检测中大放异彩[69]。文献[70]从时间维度进行欺骗检测，通过分析欺骗干扰对接收机时间的影响，针对先压制后欺骗干扰的欺骗模式，基于真实信号和欺骗信号下的钟差预测误差分布，构造了芯片级原子钟辅助的欺骗检测模型。

加速度计因为具有良好的偏差稳定性，且成本很低，不受电磁干扰，因此在欺骗干扰检测中可以作为辅助设备。文献[71]通过比较加速度计输出信息与 GPS 输出信息的差异，提出了一种加速度计辅助的 GNSS 欺骗检测算法，该算法能有效检测出由于欺骗干扰引起的加速度参数异常变化。

虽然这些辅助设备能在欺骗检测中起着举足轻重的作用，但是在实际应用中还要考虑诸多其他因素，如 INS 系统所用的时钟、加速度计和陀螺仪等元件具有无法消除的系统误差，因此，随着工作时间的累积，

其误差累积越来越大[72]，导致 INS 系统无法用于长时间的欺骗干扰检测。一般将 INS 与 GNSS 相结合，在 GNSS 信号良好时，接收 GNSS 信息用于修正 INS 的计算结果。芯片级原子钟虽然有着优异的检测效果，但是其造价相当昂贵，不适合大范围普及。

## 2.6 基于机器学习的欺骗式干扰检测

近年来，机器学习在信息安全、医药学、生物学、金融市场、公共交通、制造业等众多行业和领域扮演着日益重要的角色[73]。鉴于机器学习具有快速处理大量数据、分析提取有效信息等优点，一些研究人员将机器学习引入到卫星导航欺骗式干扰检测中，通过机器学习算法学习输入特征间的差异，从而将欺骗信号和真实信号区分开来，实现欺骗式干扰检测。目前基于机器学习的欺骗式干扰检测方法有 E. Shafiee 等[74]提出了用多层神经网络训练进行欺骗干扰检测；L. Junzhi 等[75]探讨了将生成对抗网络（GAN）应用于欺骗干扰检测的可行性并在文献[76]中通过网络中欺骗干扰和抗欺骗干扰的对抗学习，成功实现了对小时延欺骗干扰信号的检测。考虑到传统的检测算法大多仅利用一个参数检测欺骗干扰，具有一定的局限性，卢丹等[77]提出一种融合布谷鸟搜索算法和分类支持向量机的多参数欺骗干扰检测算法；针对载波相位差分检测技术中存在的模糊度解算复杂和虚警率高的问题，庞春雷等[78]提出一种基于概率神经网络（PNN）的检测方法；Xu 等[79]提出了一种多通道一维全卷积神经网络故障检测方法。

机器学习方法因其具有模型鲁棒性强、泛化能力高、自动表征复杂多元非线性关系等特点，在信号检测中大放异彩，但根据机器学习中“没有免费的午餐”定理，没有算法能够完美地解决所有问题，在针对具体问题时，需要采用合适的机器学习算法，才能达到比较好的效果。

下面对以上各种欺骗干扰检测技术进行总结：

**表 4 欺骗干扰检测技术比较**

Table 4 Comparison of deceptive jamming detection methods

| 类别 | 检测类型 | 检测方法 | 依据 | 实现难度 | 检测效果 | 场景适应性 |
|---|---|---|---|---|---|---|
| 基于导航数据信息 | 加密认证 | 扩频码验证 | 欺骗干扰源几乎不可能准确预测到伪码码片 | 高 | 高 | 高 |
| | | 导航信息认证 | 欺骗干扰源几乎不可能生成对应真实信号的数字签名 | 高 | 高 | 高 |
| 基于空间信息处理 | 信号到达方向检测 | 运动单天线 | 欺骗式干扰源通常从同一天线发射多个欺骗信号，而真实信号则从不同方向的不同卫星发射 | 低 | 中 | 中 |
| | | 双天线 | | 中 | 中 | 中 |
| | | 天线阵列 | | 高 | 高 | 高 |
| 基于射频前端 | 自动增益控制检测 | 自动增益控制异常变化 | 功率较大的干扰信号进入时会引起自动增益控制的异常变化 | 低 | 低 | 低 |
| | 接收信号强度检测 | 绝对功率 | 欺骗信号有更大的功率 | 低 | 中 | 高 |
| | | 载噪比 | 欺骗信号有更高的载噪比 | 低 | 中 | 中 |
| | | L1/L2 功率比 | 一般欺骗干扰源无 L2 信号 | 中 | 低 | 低 |
| 基于基带数字信号处理 | 信号质量检测 | 相关峰数量 | 欺骗信号的进入会使得相关峰数量增加 | 低 | 低 | 低 |
| | | 相关峰形状 | 欺骗信号与真实信号相关峰重叠，产生畸变 | 中 | 中 | 中 |
| | 多普勒频移检测 | 多普勒频移一致性 | 欺骗信号很难让载波多普勒频移与伪码多普勒频移保持一致性 | 中 | 中 | 中 |
| 基于定位导航结果 | 信号到达时间 | 伪码和数据位时间延迟 | 欺骗信号与真实信号在时间维度上有一定延迟 | 中 | 低 | 低 |
| | | L1/L2 信号相对时间延迟 | 一般欺骗干扰源无 L2 信号 | 中 | 低 | 低 |
| | 与其他设备的一致性检测 | 与惯导、芯片级原子钟等不受电磁干扰的高精密设备的一致性检测 | 欺骗信号的存在使得结算结果不一致 | 高 | 高 | 高 |
| | 伪距、速度等一致性检测 | 真实信号与欺骗信号的伪距和速度模型构造 | 欺骗信号与真实信号的解算结果模型不同 | 中 | 中 | 中 |
| 统计学层面 | 机器学习 | 机器学习算法构造 | 欺骗信号与真实信号之间的特征有差异 | 低 | 中 | 高 |

## 3、GNSS 欺骗干扰检测技术研究趋势

### 3.1 实时检测

目前针对欺骗信号干扰检测的方法基本上是非实时的，一般采集相关信息后进行事后处理以完成欺骗信号干扰检测。这对于像汽车、飞机、轮船导航等实时性要求极高的应用场景就显得力不从心，故而一方面可以从优化算法和实验方案等角度提升接收机处理速度，达到实时检测的目标；另外，检测与对抗（或决策）形成闭环，对于增强系统可靠性具有重要作用，是未来的研究方向之一。

### 3.2 融合检测

通过第 2.4 节对当前的欺骗干扰检测研究现状分析归纳可以看出，目前大部分欺骗干扰检测方法通过在某一特定场景下，真实信号与欺骗干扰信号在某一方面的差异来实现欺骗干扰检测，而像文献[80]-[82]这样多方案协同检测的检测方案少之又少。针对特定场景的单一特征检测可能检测效果很好，而当将其应用到其他场景时，该方法缺乏复杂环境适应性，其检测效果就不尽如人意。因此，综合检测是一个可行的理想的发展方向，可以通过将几个干扰检测方案进行融合，实现综合检测，并不断进行整个检测系统的完善，使其更具通用性。但目前实现综合检测的难题主要有：干扰信号具有很大的未知性，无法提前预知，当采用多方案相或的协同检测时，虽然在环境的适应性上提高了，但最终的检测效果会下降，因此如何平衡适应性和最后检测效果是一个值得考虑的问题；另外多方案融合检测相应的增加了冗余计算量，对接收机有更高的硬件要求。

## 参考文献


[1]HOFMANN B, LICHTENEGGER H, WASLE E. GNSS-global navigation satellite systems: GPS, GLONASS, Galileo and More[M].Berlin:Springe,2008.

[2]CAI B G, WU B Q, LU D B. Survey of performance evaluation standardization and research methods on GNSS-based localization for railways[J]. 电子学报：英文版，2020, 29(1):12.

[3]WU Y H, ZHENG M H, HE W, et al. Intelligent vehicle safety system based on BeiDou satellite navigation system[J]. IET Intelligent Transport Systems, 2019, 13(6):967-974.

[4]徐纵,黄陆明,李博,俞文慧,雷振洲,王佳琳.采用北斗卫星导航系统的超高压变电站 GIS 变形监测精度分析[J].浙江电力,2021,40(4):101-107.

XU Z, HUANG L M, LI B, et al. Analysis of GIS deformation monitoring accuracy of ultra-high voltage substation using Beidou satellite navigation system[J]. Zhejiang Electric Power, 2021,40(4):101-107.

[5]徐明.北斗卫星导航系统在金融押运行业的设计与实践[J].金融科技时代,2017(9):41-43.

XU M. Design and practice of Beidou satellite navigation system in financial escort industry[J]. Fintech Era, 2017(9):41-43.

[6]卢天增,甄卫民,马宝田,刘少林,谭帅.基于 GNSS 与网络通信融合定位的隔离者管理系统的设计与实现[J].全球定位系统,2021,46(4):45-51.

LU T Z, ZHEN W M, MA B T, et al. Design and implementation of isolator management system based on GNSS and network communication fusion positioning[J]. Global Positioning System, 2021,46(4):45-51.

[7]姚洋,郭承军. 北斗卫星导航系统在精准农业中的应用研究[C]. 第十二届中国卫星导航年会论文集——S01 卫星导航行业应用, 2021:110-113.

YAO Y, GUO C J. Application research of Beidou satellite navigation system in precision agriculture[C]. Proceedings of the 12th China Satellite Navigation Conference——S01 Satellite Navigation Industry Application, 2021:110-113.

[8]胡鸿. 北斗卫星导航系统和高分一号在天保工程森林管护中的应用研究[D].中国林业科学研究院,2018.

HU H. Application research of Beidou satellite navigation system and Gaofen-1 in forest management and protection of natural protection project[D]. Chinese Academy of Forestry Sciences, 2018.

[9]“北斗”应用之现代牧业[J].太空探索,2017(4):17.

"Beidou" Application of modern animal husbandry[J]. Space Exploration, 2017(4):17.

[10]王超,康萌,张宇,张淼.北斗导航技术在渔业生产定位中的运用[J].黑龙江水产,2020,39(6):26-27.

WANG C, KANG M, ZHANG Y, et al. Application ofBeidou navigation technology in fishery production positioning[J]. Heilongjiang Fisheries,2020,39(6):26-27.

[11]O'HANLON B W, PSIAKI M L, BHATTI J A, et al. Real-time GPS spoofing detection via correlation of encrypted signals[J]. Navigation, 2014, 60(4): 267-278.

[12]谢钢. GPS 原理与接收机设计[M]. 北京:电子工业出版社. 2009, 7: 1-13.

XIE G. GPS Principle and receiver design[M].Beijing: Electronic Industry Press. 2009,7: 1-13.

[13]SCOTT L. Anti-spoofing & authenticated signal architecture for civil navigation systems[C]. 16th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GPS/GNSS 2003), Portland, OR, 2003.

[14]LO, SHERMAN L, DAVID E, et al. Signal authentification, A secure civil GNSS for today[J]. Inside GNSS, 2009.

[15]POZZOBON, OSCAR, GAMBA, et al. Supersonic GNSS authentication codes[C]. Proceedings of the 27th International Technical Meeting of the Satellite Division of The Institute of Navigation(ION GNSS+ 2014), Tampa, Florida, 2014: 2862-

2869.
[16]KUHN M G. An asymmetric security mechanism for navigation signals[J]. Springer Berlin Heidelberg, 2004.
[17]MARGARIA D, MOTELLA B, ANGHILERI M, et al. Signal structure-based authentication for civil GNSSs: recent solutions and perspectives[J]. IEEE Signal Processing Magazine, 2017, 34(5):27-37.
[18]KERNS J, WESSON K D, HUMPHREYS T E. A blueprint for civil GPS navigation message authentication[C]. 2014 IEEE/ION Position, Location and Navigation Symposium - PLANS 2014, 2014:262-269.
[19]申成良，郭承军. 民用 GNSS 信号电文加密认证技术研究[C].第九届中国卫星导航学术年会论文集——S03 卫星导航信号及抗干扰技术, 2018:6.
SHEN C L, GUO C J. Research on encryption and authentication technology of civil GNSS signal message[C]. Proceedings of the 9th China Satellite Navigation Conference——S03 Satellite Navigation Signal and Anti-jamming Technology. 2018: 6.
[20]GHORBANI K, OROUJI N, MOSAVI M R. Navigation message authentication based on one-way Hash Chain to mitigate spoofing Attacks for GPS L1[J]. Wireless Personal Communications, 2020, 113(6).
[21]HERNANDEZ I F, RIJMEN V, GRANADOS G S, et al. A Navigation message authentication proposal for the Galileo open service[J]. Navigation, 2016, 63(1):85-102.
[22]WESSON K, ROTHLISBERGER M, HUMPHREYS T. Practical cryptographic civil GPS signal authentication[J]. John Wiley & Sons, Ltd,2012,59(3):1-10.
[23]WU Z, ZHANG Y, LIU R. BD-II NMA&SSI: An scheme of anti-Spoofing and open BeiDou II D2 navigation message authentication[J]. IEEE Access, 2020,8:23759-23775.
[24]郭军,孙家奇,李顶伦.一种新型 GNSS 加密认证方案的分析与设计[J].通讯世界,2020,27(6):125-126.
GUO J, SUN J Q, LI D L. Analysis and design of a new GNSS encryption authentication scheme[J]. Communication World, 2020,27(6):125-126.
[25]ALI J J, ALI B, JOHN N, et al. GPS vulnerability to spoofing threats and a review of anti spoofing techniques[J]. International Journal of Navigation and Observation,2012.
[26]NIELSEN J, BROUMANDAN A, LACHAPELLE G. Spoofing detection and mitigation with a moving handheld receiver[J]. GPS World,2010.
[27]BROUMANDAN, ALI J J, DEHGHANIAN V, et al. GNSS spoofing detection in handheld receivers based on signal spatial correlation[C]. Proceedings of the 2012 IEEE/ION Position, Location and Navigation Symposium, 2012:479-487.
[28]张鑫,陈华明,黄仰博,张国柱,欧钢.利用旋转天线载波相位双差进行欺骗干扰检测技术[J].武汉大学学报(信息科学版),2016,41(4):529-534.
ZHANG X, CHEN H M, HUANG Y B, et al. Deception interference detection technology using rotating antenna carrier phase double difference[J]. Journal of Wuhan University (Information Science Edition), 2016,41(4):529-534.
[29]张鑫.卫星导航欺骗干扰信号仿真与检测关键技术研究[D].国防科学技术大学,2014.
ZHANG X. Research on key technologies of simulation and detection of satellite navigation deception jamming signals[D]. National University of Defense Technology,2014.
[30]JUNHO O, HYOUNGMIN S. Direction of arrival estimation of GNSS signal using dual antenna[J]. Journal of Positioning, Navigation, and Timing, 2020,9(3):215-220.
[31]CHEN J J, XU T, YUAN H. A New GNSS spoofing detection method using two antennas[J]. IEEE ACCESS, 2020,8: 110738-110747.
[32]ZHANG J Q, CUI X W, XU H L, et al. A two-stage interference suppression scheme based on antenna array for GNSS jamming and spoofing[J]. Sensors,2019,19(18):
[33]FAN G W, GAN X L, YU B G, et al. Adaptive spoofing suppression algorithm for GNSS based on multiple antennas array[J]. Sensors, 2020,20(4): 21-30.
[34]YANG Q, ZHANG Y, TANG C K. A combined anti jamming and antispoofing algorithm for GPS Arrays[J]. INTERNATIONAL JOURNAL OF ANTENNAS AND PROPAGATION, 2019.
[35]LEE Y S, YEOM J S, NOH J H, et al. A novel GNSS spoofing detection technique with array antenna-based multi-PRN diversity[J]. Journal of Positioning, Navigation, and Timing, 2021, 10(3):169-177.
[36]KANG C H, KIM S Y. Adaptive complex-EKF-based DOA estimation for GPS spoofing detection[J]. IET Signal Processing,2018,12(2):
[37]AKOS D M. Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC)[J]. Navigation, 2012,5(4):281-290.
[38]WEN H, HUANG P Y R, DYER J, et al. Countermeasures for GPS signal spoofing[C]. Proceedings of the 18th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS '05), Long Beach, Calif, USA, 2005: 1285–1290.
[39]JAHROMI, ALI B, ALI N, et al. GPS spoofer countermeasure effectiveness based on signal strength, noise power, and C/N0 measurements[J]. International Journal of Satellite Communications and Networking, 2012.
[40]HU Y, BIAN S, CAO K, et al. GNSS spoofing detection based on new signal quality assessment model[J]. GPS Solutions, 2018, 22(1):28.
[41]ELEZI E, ÇANKAYA G, BOYACI A, et al. A detection and identification method based on signal power for different types of electronic jamming attacks on GPS signals[C]. 2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC),2019:1-5.
[42]DEHGHANIAN V, NIELSEN J, LACHAPELLE G. GNSS spoofing detection based on receiver C/N0 estimates[J]. proceedings of international technical meeting of the satellite division of the institute of navigation, 2012.
[43]张伦东,张超,高扬骏.卫星导航欺骗及检测（二）：基于接收机改进的欺骗检测[J].导航定位学报,2021,9(4):1-10.
ZHANG L D, ZHANG C, GAO J Y. Satellite navigation deception and detection: improved deception detection based on receiver[J]. Journal of Navigation and Positioning, 2021, 9(4):

1-10.
[44]PHELTS, ENGE R, PER K. Multi correlator techniques for robust mitigation of threats to GPS signal quality[D]. Stanford University. 2001.
[45]LI J, ZHU X, OUYANG M, et al. Research on multi-peak detection of small delay spoofing signal[J]. IEEE Access, 2020, PP(99):1-1.
[46]张国利,丁继成,张尧.基于 GNSS 信号时延特征的转发式欺骗干扰检测算法[J].无线电工程,2019,49(7):626-630.
ZHANG G L, DING J C, ZHANG Y. Repetitive deception jamming detection algorithm based on GNSS signal time-delay characteristics[J]. Radio Engineering, 2019,49(7):626-630.
[47]王文益,龚婧,王金铭.基于 SCB 方差的 GNSS 欺骗式干扰检测算法[J].系统工程与电子技术,2021,43(8):2254-2262.
WANG W Y, GONG J, WANG J M. GNSS deceptive jamming detection algorithm based on SCB variance[J]. System Engineering and Electronic Technology, 2021,43(8):2254-2262.
[48]KHAN, AM, AHMAD. Global navigation satellite systems spoofing detection through measured autocorrelation function shape distortion[J]. Int J SatellCommun Network. 2021; 1- 9.
[49]ZAHNG X R, LI H, YANG C, et al. Signal quality monitoring-based spoofing detection method for global navigation satellite system vector tracking structure[J]. IET Radar, Sonar & Navigation,2020,14(6):
[50]李娟丽,梁立明,张骅.一种 GPS 信号转发欺骗干扰检测技术[J].现代导航,2017,8(4): 253-256.
LI J L, LIANG L M, ZHANG Y. A GPS signal forwarding spoofing jamming detection technology[J]. Modern Navigation,2017,8(4): 253-256.
[51]赵香香,李亚平. 基于伪码相关峰斜率等间隔分布的转发式干扰检测方法[C].第十届中国卫星导航年会论文集——S11 抗干扰与反欺骗技术.2019:5.
ZHAO X X, LI Y P. Forwarding interference detection method based on equal interval distribution of pseudo-code correlation peak slope[C]. Proceedings of the 10th China Satellite Navigation Conference——S11Anti-jamming and Anti-spoofing Technology.2019:5.
[52]范广腾,李献斌,王建.基于检测器性能实时评估的欺骗检测融合算法[J].哈尔滨工业大学学报,2020,52(5):165-170.
FAN G T, LI X B, WANG J. Deception detection fusion algorithm based on real-time evaluation of detector performance[J]. Journal of Harbin Institute of Technology, 2020, 52(5): 165-170.
[53]QI W, ZAHNG Y, LIU X. A GNSS anti-spoofing technology based on doppler shift in vehicle networking[C]. 2016 International Wireless Communications and Mobile Computing Conference (IWCMC), 2016:725-729.
[54]张国利,张尧,田野.基于 DOD 和 PTD 的北斗欺骗式干扰检测技术研究[J].应用科技,2019,46(2):35-41.
ZHANG G L, ZHANG Y, TIAN Y. Research on Beidou deception jamming detection technology based on DOD and PTD[J]. Applied Technology, 2019,46(2):35-41.
[55]HE L, LI H, LU M Q. Global navigation satellite system spoofing detection technique based on the doppler ripple caused by vertical reciprocating motion[J]. IET Radar, Sonar & Navigation,2019,13(10).
[56]HE L, LI H, LU M Q. Dual-antenna GNSS spoofing detection method based on doppler frequency difference of arrival[J]. GPS Solutions, 2019, 23(3):78.
[57]HUMPHREYS T E, LEDVINA B M, PSIAKI M L, et al. Assessing the spoofing threat: development of a portable GPS civilian spoofer[C]//International Technical Meeting of the Satellite Division of the Institute of Navigation. 2008.
[58]LO S C, ENGE P K. Authenticating aviation augmentation system broadcasts[C].Proceedings of the IEEE/ION Position, Location and Navigation Symposium (PLANS ’10),Indian Wells, Calif, USA, 2010: 708–717.
[59]肖岭,唐小妹,李柏渝等.GNSS 双接收机抗欺骗技术[J].国防科技大学学报,2016, 38(3):45-49.
XIAO L, TANG X M, LI B Y, et al. GNSS dual receiver anti-spoofing technology[J]. Journal of National University of Defense Technology, 2016, 38(3): 45-49.
[60]刘科,吴文启,唐康华等.基于伪距信息的 GNSS 双接收机抗转发式欺骗干扰检测算法[J].系统工程与电子技术, 2017, 39(11): 2393-2398.
LIU K, WU W Q, TANG K H, et al. GNSS dual-receiver anti-repeating spoofing interference detection algorithm based on pseudo range information[J]. System Engineering and Electronic Technology, 2017,39(11):2393-2398.
[61]TAO H, WU H L, LI H, et al. GNSS spoofing detection based on consistency check of velocities[J]. Journal of Engineering,2019.
[62]JEONG S K, KIM M C, LEE J Y. CUSUM-based GNSS spoofing detection method for users of GNSS augmentation system[J]. International Journal of Aeronautical and Space Sciences, 2020(prepublish):
[63]邹昆.惯性/卫星组合导航系统不组合问题浅析[J].航空科学技术,2013(4):49-51.
ZOU K. Analysis of the non-combination problem of inertial/satellite integrated navigation system[J]. Aeronautical Science & Technology, 2013(4):49-51.
[64]LIU Y, LI S H, XIAO X. INS-aided GNSS spoofing detection based on two antenna raw measurements[J]. Gyroscopy and Navigation,2016,7(2):
[65]范广腾,黄仰博,伍微等.惯导辅助的三元天线阵欺骗干扰检测算法[J].国防科技大学学报,2017,39(2):91-95.
FAN G T, HUNAG Y B, WU W, et al. Inertial navigation-aided three-element antenna array deception jamming detection algorithm[J]. Journal of National University of Defense Technology, 2017,39(2):91-95.
[66]LIU Y, LI S H, Fu Q W, et al. Impact assessment of GNSS spoofing attacks on INS/GNSS integrated navigation system[J]. Sensors (Basel, Switzerland),2018,18(5):
[67]CECCATO M, FORMAGGIO F, LAURENTI N, et al. Generalized likelihood ratio test for GNSS spoofing detection in devices with IMU[J]. IEEE Transactions on Information Forensics and Security, 2021, PP(99):1-1.
[68]武智佳,吴文启,刘科等.基于 INS/GNSS 紧耦合组合的逐

步诱导式欺骗检测算法研究[J].导航定位与授时, 2019, 6(1): 7-13.
WU Z J, WU W Q, LIU K, et al. Research on step-by-step induced deception detection algorithm based on INS/GNSS tightly coupled combination[J]. Navigation Positioning and Timing, 2019,6(1):7-13.
[69]郭平,赵建业.芯片级原子钟在 Micro-PNT 中的应用[J].数字通信世界,2018(12):13-14+2.
GUO P, ZHAO J Y. Application of chip-level atomic clock inMicro-PNT[J]. Digital Communication World, 2018(12): 13-14+2.
[70]刘洋,李四海,付强文等.芯片级原子钟辅助的惯性/卫星组合导航系统欺骗检测方法[J].中国惯性技术学报, 2019, 27(5): 654-660.
LIU Y, LI S H, FU Q W, et al. Chip-level atomic clock assisted inertial/satellite integrated navigation system deception detection method[J]. Journal of Chinese Inertial Technology, 2019, 27(5):654-660.
[71]LEE J H, KWON K C, AN D S, et al. GPS spoofing detection using accelerometers and performance analysis with probability of detection[J]. International Journal of Control, Automation and Systems,2015,13(4):
[72]姜雪梅,车转转.惯性导航系统标定滤波方法研究[J].航空科学技术,2018,29(1):46-52.
JIANG X M, CHE Z Z. Research on calibration filtering method of inertial navigation system[J]. Aeronautical Science & Technology,2018,29(1):46-52.
[73]何晓骁,姚呈康.人工智能等新技术在航空训练中的应用研究[J].航空科学技术,2020,31(10):7-11.
HE X X, YAO C K. Research on the application of new technologies such as artificial intelligence in aviation training[J]. Aeronautical Science & Technology, 2020,31(10):7-11.
[74]SHAFIEE E, MOSAVI M R, MOAZEDI. Detection of spoofing attack using machine learning based on multi-layer neural network in single-frequency GPS receivers[J]. Science Letter,2018:
[75]LI J Z, LI W Q, FU Q X, et al. Research progress of GNSS spoofing and spoofing detection technology[C]. 2019IEEE 19th International Conference on Communication Technology (ICCT), 2019:1360-1369.
[76]LI J Z, ZHU X, OUYANG M, et al. GNSS spoofing jamming detection based on generative adversarial network[J]. IEEE Sensors Journal, 2021, PP(99):1-1.
[77]卢丹,殷亚强.基于 CS-C-SVM 的多参数 GNSS 欺骗干扰检测[J/OL].信号处理:1-10[2022-01-18].
LU D, YIN Y Q. Multi-parameter GNSS spoofing jamming detection based on CS-C-SVM[J/OL]. Signal Processing: 1-10 [2022-01-18].
[78]庞春雷,郭泽辉,吕敏敏,张良,翟丁,张闯.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.
PANG C L, GUO Z H, LV M M, et al. Beidou relaying spoofing jamming signal detection method based on PNN[J]. Chinese Journal of Inertial Technology,2021,29(4):554-560.
[79]XU H W, LIAN B W. Fault detection for multi-source integrated navigation system using fully convolutional neural network[J]. IET Radar, Sonar & Navigation,2018,12(7):
[80]JEONG S, LEE J. Synthesis algorithm for effective detection of GNSS spoofing attacks. Int. J. Aeronaut. Space Sci. 21, 251–264 (2020).
[81]TU J X, ZHAN X Q, CHEN M L, et al. GNSS intermediate spoofing detection via dual-peak in frequency domain and relative velocity residuals[J]. IET Radar, Sonar & Navigation,2020,14(3):
[82]金磊,曾富华,王娜.信息辅助快速捕获的抗欺骗干扰技术[J].指挥与控制学报,2020,6(1):81-86.
JIN L, ZENG F H, WANG N. Anti-spoofing and jamming technology for information-assisted rapid capture[J]. Journal of Command and Control, 2020,6(1):81-86.