doi:10.19306/j.cnki.2095-8110.2020.04.016

卫星导航欺骗式干扰抑制技术研究与分析

刘　鹏，陈思源，任婵婵，刘盛典

（航天恒星科技有限公司，北京 100095）

摘　要：为避免欺骗式干扰对卫星导航构成重大威胁，研究了卫星导航欺骗式干扰抑制技术。首先，根据欺骗式干扰产生原理和实施方式将其分为四类，之后论述了国内外欺骗式干扰和欺骗式干扰抑制技术的研究现状，调研了国内外主要研究机构针对欺骗式干扰抑制采取的技术措施，进一步按照适用接收机的类型对技术进行了分类，并对各类技术对于四类干扰的抑制效果进行了逐一对比分析。在此基础上，展望了未来欺骗式干扰抑制技术的发展趋势，对从事该项技术的研究者具有一定的参考借鉴价值。

关键词：卫星导航；欺骗式；抗欺骗；研究现状；发展趋势

中图分类号：TN972.3　　**文献标志码**：A　　**开放科学（资源服务）标识码（OSID）**：

文章编号：2095-8110(2020)04-0123-08

Research and Analysis of Anti-Spoofing Technology for Satellite Navigation

LIU Peng, CHEN Si-yuan, REN Chan-chan, LIU Sheng-dian

(Space Star Technology Co., Ltd., Beijing 100095, China)

Abstract: To avoid the major threat spoofing poses to satellite navigation, anti-spoofing technology of satellite navigation is studied. Initially, four categories of spoofing are presented according to its principle and implementation. Then the research status of spoofing and anti-spoofing technology is discussed, technical measures adopted by major research institutes are investigated. Further the technology is classified according to the types of applicable receivers, and the spoofing suppression effects of various technologies are compared and analyzed. On this basis, the development trend of anti-spoofing technology in the future is prospected, which provides a reference to the researcher who is engaged in this technology.

Key words: Satellite navigation; Spoofing; Anti-spoofing; Research status; Development trend

0　引言

卫星导航是一种重要的卫星应用形式，在政治、经济、科学和军事等各项人类活动中得到了广泛应用。卫星导航系统以人造卫星作为导航台，可以为全球陆、海、空、天的各类军民载体，提供全天候、24h 连续高精度的三维位置、速度和时间信息[1]。在为人类活动提供便利的同时，由于工作空间中复杂的电磁干扰环境，卫星导航系统本身存在的一些问题逐渐暴露出来。由于国际电信联盟（International Telecommunication Union，ITU）对地面接收卫星信号功率密度的限制，致使地面接收到

收稿日期：2019-05-30；**修订日期**：2019-06-18

基金项目：装发共用技术（41411010302）

作者简介：刘鹏（1980-），男，硕士，高级工程师，主要从事导航信号处理、导航电子对抗方面的研究。E-mail：Liup_st@126.com

的卫星导航信号相当微弱，很容易受到各种类型射频干扰的影响。因此，干扰抑制技术已经成为保证卫星导航接收机正常工作的必备手段[2]。

导航接收机所受干扰分为无意干扰和有意干扰两种。对于民用导航接收机，主要的干扰形式为无意干扰；而对于军用导航接收机而言，主要考虑的干扰形式为有意的人为干扰。从技术角度出发，有意干扰又可以分为两类：一是压制式干扰，二是欺骗式干扰[2]。压制式干扰通过发射干扰信号以压制在导航接收机前端的导航卫星信号，使导航接收机接收不到导航卫星信号，从而导致卫星导航接收机无法正常工作，其表现为捕获时间变长甚至无法捕获、卫星信号载噪比下降、同时接收的卫星数减少、导航定位精度下降及失锁等问题。欺骗式干扰是使接收机在看似正常工作的条件下，让虚假的卫星信号以强于真实导航信号的形式，优先控制导航接收机的跟踪环，使接收机锁定错误的卫星信号继而解算出虚假的导航数据，计算出错误的位置、速度和时间信息。根据干扰机理，基本的欺骗式干扰可以分为生成式干扰与转发式干扰两种。压制式干扰和欺骗式干扰均会对导航信号的观测量精度和定位精度造成一定影响，甚至在采取抗干扰措施的情况下，仍然无法完全消除影响。

相比压制式干扰，欺骗式干扰具有较强的隐蔽性，因此不易被发现，可获得良好的干扰效果[3]。针对压制式干扰抑制技术，目前国内外已开展了深入研究，相关技术已在导航接收机中得到大量应用。相对而言，国内外对欺骗式干扰抑制技术的研究起步稍晚。随着伊朗诱捕美国无人机等一系列有影响事件的发生，近年来，欺骗式干扰抑制技术逐渐成为卫星导航应用领域的研究热点，国内外科研机构对此开展了大量研究工作。

本文针对卫星导航欺骗式干扰抑制技术开展相关研究，论述了国内外欺骗式干扰抑制技术的研究现状，以及研究中采用的技术手段，并按照适用接收机的类型对技术进行了分类，对各类技术的干扰抑制效果进行了对比分析。在此基础上，分析了未来欺骗式干扰抑制技术的发展趋势，以期能够对该领域的后续研究产生一定的参考借鉴价值。

1 欺骗式干扰分类及工作原理

欺骗式干扰是干扰抑制技术的作用对象，不同的干扰抑制技术适用的干扰类型不同，研究欺骗干扰机理是开展欺骗式干扰抑制研究的基础，因此有必要对欺骗式干扰信号的主要类型及其工作原理进行研究。

欺骗式干扰的基本形式包含转发式和生成式两种，在此基础上，又可以衍生出其他干扰类型，本文重点介绍了中间媒介伪造以及多系统协同复杂欺骗，这两种衍生类型可认为是生成式干扰的扩展。

1.1 欺骗干扰类别

1.1.1 转发式欺骗干扰

转发式欺骗是利用高增益的天线接收视线范围内的导航卫星信号，通过延迟和功率变换，从射频端向干扰区域内播发，其工作原理如图 1 所示。

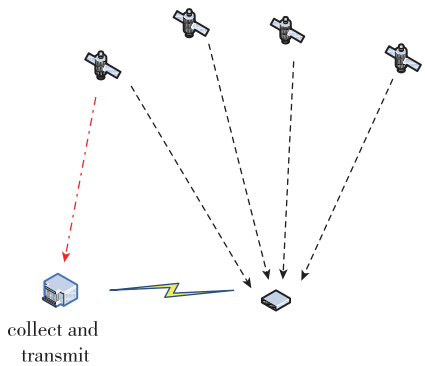

图 1 转发式欺骗示意图

Fig. 1 Repeater spoofing diagram

此种欺骗方式的实现方式较为简单，不需要解析导航信号的结构，且对于加密的导航信号依然有效，因此国内外的研究较多。该欺骗样式的弊端在于，在接收机端，欺骗信号的时延一定滞后于真实信号，欺骗信号欲有效地接管接收机通道并产生欺骗效果，往往需要首先发送强功率压制式干扰，使被欺骗接收机的正常跟踪状态被打断，迫使其重新捕获信号。这一特点将利于接收机检测欺骗。

1.1.2 生成式欺骗干扰

简单的自主生成式欺骗可以用全球导航卫星系统(Global Navigation Satellite System，GNSS)模拟信号源配合射频天线来实现，其工作原理如图 2 所示。

这种欺骗方式可以通过设置信号源参数，生成任意卫星号的伪造信号，但较难与欺骗区域内的真实卫星信号保持一致或者同步。因此，此种欺骗方式也需要通过压制干扰，或提高伪造信号功率的方法，使欺骗信号能够有效地进入接收机跟踪通道，而这种异常的高功率信号也将为欺骗的检测提供

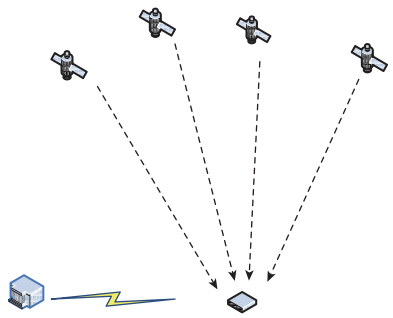

图 2　自主生成式欺骗示意图

Fig. 2　Self-generated spoofing diagram

机会。另外，由于需要事先知道信号格式，该类型通常仅适用于对公开导航信号进行欺骗。

1.1.3　中间媒介伪造欺骗干扰

中间媒介伪造式欺骗干扰同时使用导航接收机与信号发生器，因此该种欺骗设备也被称为 Receiver-Spoofer。导航接收机用于跟踪视线范围内的所有真实卫星信号，并实时提供真实信号的载波多普勒、伪码延迟、导航电文及时间信息，这些信息将被传递给信号发生器，信号发生器结合欲欺骗目标接收机的位置和速度信息，产生接近于真实信号的欺骗信号，其工作原理如图 3 所示。

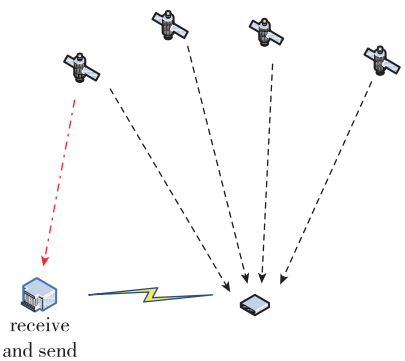

图 3　中间媒介伪造式欺骗示意图

Fig. 3　Intermediate spoofing diagram

中间媒介伪造式欺骗可以在不打断接收机跟踪状态的情况下，隐蔽地完成欺骗过程，因而不易被发现，干扰抑制难度较大。该欺骗样式主要存在 2 个缺点：1）需要事先获取目标接收机的位置和速度等信息，具有一定难度；2）欺骗信号作用范围较小。

1.1.4　多系统协同复杂欺骗干扰

更为高级的欺骗方式，是利用多个协同的设备和天线，联合发送伪造信号，用于伪造来波方向等信号的空域特征，可以对阵列天线接收机实施有效欺骗，如图 4 所示，多个干扰设备的协同是这种欺骗的关键所在。

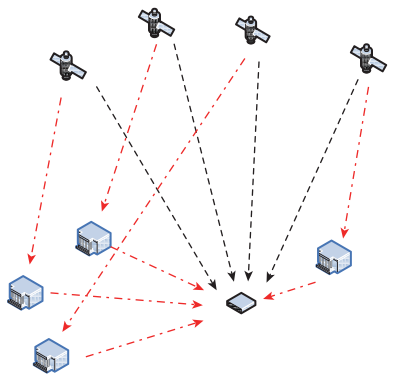

图 4　多系统协同复杂欺骗示意图

Fig. 4　Multi-system cooperative complex spoofing diagram

这种欺骗样式的技术要求非常高，实现难度很大。从相关文献来看，该欺骗样式目前还只停留在理论概念阶段，但预计未来有望成为重要的干扰样式，特别是在军事对抗领域。

1.2　欺骗效果分析

各类欺骗样式对比总结如表 1 所示。不同的欺骗方式所需要的成本、技术难度、效果（抗反欺骗能力）各有不同，各种欺骗方法的适用范围差别也较大。

表 1　欺骗方式总结对比

Tab. 1　Spoofing method summary and contrast

欺骗样式	难度	成本	覆盖区域	干扰效果	适用范围
转发式	小	低	大	一般	大范围欺骗
生成式	较大	高	大	较好	大范围欺骗
中间媒介伪造	很大	很高	小	好	小范围欺骗，针对特定目标
多系统协同复杂	极大	极高	小	极好	小范围欺骗，针对特定目标

这里的欺骗范围指达到相应欺骗样式预期欺骗效果的范围，对于中间媒介伪造和多系统协同复杂欺骗这些针对特定目标的复杂欺骗，在施加过程中也会对一定范围内的设备产生影响。欺骗式干扰的影响范围主要受干扰施加平台和干扰功率等因素影响。对于大范围远距离欺骗式干扰，相对于地面干扰平台，升空干扰平台更具优势，例如直升机、专用电子对抗飞机、无人驾驶飞机、系留气球、卫星等。

2　导航欺骗干扰抑制技术研究

2.1　国外研究现状分析

国外对导航欺骗干扰抑制技术的研究起步较

早，早在 2001 年，美国运输部就评估了全球定位系统(Global Positioning System，GPS)的脆弱性对交通运输设施的影响，并首次表达了对于欺骗式干扰威胁的担忧。美国国家运输系统中心在提交给国家运输部的技术报告文件中概要地论述了关于 GPS 的欺骗式干扰以及抗欺骗式干扰技术，阐述了基于欺骗式干扰的信号特征判别的抗欺骗式干扰方法[4]。

受伊朗捕获美国无人机事件的影响，近年来卫星导航欺骗式干扰抑制技术得到快速发展。该事件发生于 2011 年 12 月，一架由美国生产的 RQ-170 哨兵无人侦察机在入侵伊朗领空 250km 时被捕获。伊朗尚未公开其捕获方案，比较可信的捕获过程为：首先屏蔽无人机的通信链路，切断其与地面控制中心的联系；同时利用压制式干扰使其无法正常接收真实 GPS 卫星信号，迫使其进入纯惯性导航状态；这时利用转发欺骗式干扰技术，把错误信息包装成看起来可靠的 GPS 信号，通过欺骗无人机海拔和经纬度数据，使其降落在指定地点，而整个过程中无需破解无人机与指控中心的远程控制及通信信号。

受此事件影响，国外开展了大量卫星导航欺骗式干扰抑制技术的研究工作，其中美国处于领先地位，主要研究机构包括美国的德州大学奥斯汀分校(University of Texas at Austin)、罗德岛大学(University of Rhode Island)、加拿大的卡尔加里大学(University of Calgary)，以及韩国的国立首尔大学(Seoul National University)等。

美国德州大学奥斯汀分校是国外较早开展欺骗干扰与干扰抑制技术研究的工作机构，该校在欺骗干扰机理和干扰抑制技术研究方面开展了大量工作。欺骗干扰机理研究方面，2012 年 6 月，Todd E. Humphreys 教授领导的无线电导航实验室开展了 2 项公开的测试研究，评估欺骗式干扰对于民用无人机和智能电网的影响，结果表明，它们都很容易受到欺骗式干扰的影响[5]；2013 年 7 月，该实验室还通过现场实验，用欺骗式干扰成功地控制了一艘船偏离航线[6]；2014 年，他们又成功地欺骗了一架无人机，控制了它的飞行位置[7]。

干扰抑制技术研究方面，实验室研究人员对关于加密认证的欺骗式干扰检测技术在民用接收机中的应用进行了详细的分析和讨论[8-9]。目前，GNSS 运营机构通过在各系统在电文格式设计中均存在的预留字节上加入电文加密认证，从而使接收机可以准确地区分出真实卫星信号和生成式欺骗干扰信号。但这样的区分需要解码到电文阶段才能判断是否是干扰，并且意味着整个系统电文的修改，这将是一个浩大的工程。而且这种方法只能区分生成式欺骗干扰，而转发式欺骗干扰将包含电文的加密认证信息，从而无法对其进行有效抑制。此外，他们还提出了结合惯性导航设备的欺骗式干扰检测技术[10-11]，该方法同时适用于转发式干扰与生成式干扰，但对受限于成本和体积等因素的、不依赖于其他辅助设备的导航设备不可行。

此外，美国罗德岛大学的研究人员提出了利用 2 个以上接收机的定位结果差异来进行转发式欺骗干扰的检测[12]，然而这种方法需要多个独立的接收机分别进行定位。加拿大卡尔加里大学的研究人员提出了利用阵列天线中不同阵元间的信号相关值异常来检测欺骗式干扰[13]，然而这种方法仅可用于检测单个高功率的转发式欺骗干扰；他们还研究了采用 GNSS、惯性导航和里程计一致性检验来检测欺骗式干扰的方法[14]，需要借助较多辅助设备。俄罗斯的 Sergery Lyusin 等研究了通过定位结果检测和估计欺骗式干扰的方法[15]。韩国国立首尔大学的 Beomju Shin 等推算出欺骗过程方程，可以计算欺骗过程中欺骗信号的码相位，并评估欺骗信号成功的可能性[16]。在对前人研究工作进行总结的基础上，德州大学奥斯汀分校的 Mark L. Psiaki 等对可能的欺骗模式和已有的抗欺骗式干扰方式进行了总结，归纳出涵盖多天线、惯导辅助、信号加密等 13 种组合的抗欺骗方法[17]。工程应用方面，2017 年 11 月 GPSdome 公司推出了无人机 GPS 抗干扰和抗欺骗天线模块 GPSdome 1.0-T，该模块可保护无人机和其他自主设备上基于 GPS 的计时系统免受干扰和欺骗。2018 年 5 月，美高森美公司发布了选择可用性防欺骗模块的全新 SyncServer S650 SAASM 服务器产品，为国防市场中包括卫星通信和国防作战基础设施等关键任务电子系统和仪器仪表应用的同步提供了一个高度安全、准确、灵活的时间和频率平台。

2.2 国内研究现况分析

相比国外，国内对卫星导航欺骗式干扰的研究起步稍晚，但随着我国自主北斗导航系统建设的快速推进，近年来受到了越来越高的重视。国内主要研究机构包括清华大学和国防科技大学、上海交通

大学以及北斗开放实验室等单位。

欺骗干扰机理研究方面，海军工程大学的研究人员对生成式欺骗干扰的类型和特点进行了一定的分析[18]；国防科技大学和上海交通大学的研究人员基于卫星导航模拟仿真技术，构建了生成式欺骗干扰仿真评估平台，对虚假信号牵引目标接收机跟踪环路的功率需求及对定位的影响进行了分析[19-20]；西安电子科技大学的研究人员对转发式干扰的作用机理及影响进行了分析[21]。北斗开放实验室在 2016 年的第七届中国卫星导航学术年会上发布了全国首套诱骗式民用反无人机系统—ADS2000，可通过全面干扰、压制、欺骗甚至接管无人机核心导航系统实现对黑飞无人机管控的捕获。信息工程大学的何婷等对 GNSS 转发式欺骗干扰算法进行了改进，指出 GNSS 多天线转发式欺骗干扰在实际应用中，当干扰机与目标机距离大于一定范围时，将引起目标机钟差突跳，导致欺骗信号容易被检测和识别。为此提出了干扰机阵列按照正六边形网型布设，可实现目标区域的无缝覆盖，并且灵活易拓展[22]，但这种改进方式需要多台干扰机，且干扰目标区域有限。

干扰抑制技术研究方面，海军工程大学的研究人员对基于加密认证的欺骗式干扰检测技术进行了分析[23]，其结论与德州大学奥斯汀分校的结论相似，该方法仅适用于生成式欺骗干扰，无法对转发式欺骗干扰进行有效抑制；解放军理工大学的研究人员分析了基于到达时间检测的抗转发式干扰方法[24]，该方法基于转发干扰信号到达时间落后于真实信号的假设，因此仅适用于转发式欺骗干扰；清华大学的研究人员提出了利用捕获阶段多峰检测和跟踪阶段信号质量监测算法将观测量分类，并结合信号完好性监测算法检验区分欺骗信号与真实信号，以及捕获阶段码多普勒和载波多普勒一致性检测法等[25-26]。其中，捕获阶段多峰检测算法仅适用于转发式干扰，跟踪阶段信号质量监测算法适用于生成式干扰，信号完好性监测仅能检测一颗导航星的欺骗信号。将三种方法进行结合，可以获得较为理想的欺骗干扰抑制效果，但该方法基于单天线，对于利用方向信息进行欺骗的多系统协同复杂欺骗干扰抑制效果较差。上海交通大学的战兴群研究了通过检测多普勒频差(Detect Doppler Difference，DFD)检测单天线欺骗式干扰的方法，指出在接收机随机运动时，2 颗真实卫星信号之间的 DFD 为非线性的，单天线欺骗信号为线性，并建立 DFD 模型将检测欺骗式干扰转化为检测序列线性问题[27]，这种抑制方法仅针对单天线欺骗式干扰，不能应对复杂的多系统协同欺骗。此外，北京环球信息应用开发中心的研究人员分析了利用单天线时域卡尔曼滤波对欺骗式干扰进行抑制的方法[28]；哈尔滨工业大学的罗德巳对基于分块粒子滤波的改进型自主完好性监测抗欺骗式干扰方案进行了研究[29]；南京大学的徐瑞对采用 GNSS/INS 松耦合位置融合和位置速度融合时，惯性测量单元(Inertial Measurement Unit，IMU)对欺骗式干扰的补偿进行了评估[30]；北京航空航天大学的孙超研究了多种度量标准的信号质量监测(Signal Quality Monitoring，SQM)欺骗式干扰检测方法[31]；中国民航大学的张瑞华等针对生成式欺骗干扰结合阵列天线技术与矢量跟踪环路，提出了一种基于矢量跟踪环路的欺骗干扰检测和抑制方法[32]。虽然都对已有算法进行了一定程度的改进，但也无法对四种欺骗干扰样式进行完全抑制。

2.3　导航欺骗干扰抑制技术的分类

在导航接收机的实际应用中，干扰抑制技术的实现往往受到接收机具体形态的影响，以上调研的各项技术并不是对于所有接收机都能适用。例如文献[10]和文献[11]提到的干扰抑制技术需要利用惯性辅助信息，不能适用于单独利用卫星导航进行定位的设备；文献[13]提到的干扰抑制技术需要利用阵列天线中不同阵元间的信号相关值，不能适用于利用单天线工作的设备。可见，在对干扰抑制技术进行研究时，必需考虑接收机的具体产品形态。因此，本文根据接收机的产品形态对导航欺骗干扰抑制技术进行了分类。

接收机的产品形态主要受到安装载体的体积和功耗等因素的影响。为了便于开展干扰抑制技术研究，本文按照天线形态和是否有外部辅助信息将导航接收机分为单天线接收机、阵列天线接收机以及惯性信息辅助接收机三种，相应的干扰抑制算法按照适用接收机的不同也分为三种。

根据上述分类准则，本文调研的各项国内外研究技术分类结果如表 2 所示。

表 2 欺骗干扰抑制技术分类

Tab. 2 Classification of anti-spoofing method

适用类别	单天线接收机	阵列天线接收机	惯性信息辅助接收机
干扰抑制技术	[8][9][15][18][19][20][22][23][25][26][27][28][29][31]	[12][13][24][32]	[10][11][14][30]

需要说明的是，阵列天线接收机和惯性信息辅助接收机可以认为是单天线接收机的扩展，通常适用于单天线接收机的算法也能适用于另外两种接收机，但适用于阵列天线接收机和惯性信息辅助接收机的算法对单天线接收机并不适用。

2.4 干扰抑制效果分析

如图 5 和图 6 所示，本文介绍了四种欺骗式干扰样式，以及三种干扰抑制技术类别。

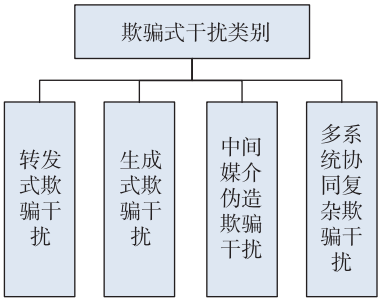

图 5 欺骗式干扰类别

Fig. 5 Category of spoofing

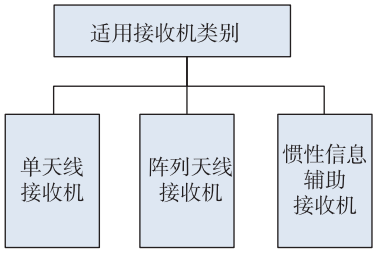

图 6 干扰抑制技术适用接收机类别

Fig. 6 Receiver category of anti-spoofing technology

根据研究现状分析，常见的检测和抑制欺骗式干扰的方法主要包括：加密认证、多峰检测、信号质量检测、定位结果检测、多普勒一致性检测等可用于各种接收机的方法；涉及信号来向检测等阵列天线接收机特有方法；以及需要惯导辅助等仅用于惯性辅助接收机的方法。

根据理论分析，对三类干扰抑制方案对四种干扰样式的抑制效果进行了评估，结果如表 3 所示。其中√表示可以较好的抑制，～表示能抑制某些情况，×表示不能抑制。需要说明的是，适用于单天线接收机的欺骗干扰抑制技术通常也能用于其他两类接收机，本文为了便于比较，表 3 中假设阵列天线和惯性辅助接收机仅采用了引入阵列方向信息和惯性辅助信息后的增量技术手段。

表 3 欺骗式干扰方式与抗欺骗式干扰方案关系

Tab. 3 Relationship between spoofing and anti-spoofing schemes

欺骗式干扰样式	欺骗式干扰抑制技术类别						
	单天线					阵列天线	惯性信息辅助
	加密认证	多峰检测	信号质量检测	定位结果检测	多普勒一致性检测		
生成式	√	～	～	～	×	√	√
转发式	×	√	～	～	×	√	√
中间媒介伪造	√	×	√	～	√	√	√
多系统协同复杂	√	×	√	～	√	×	～

其中，定位结果检测方法不受欺骗形式的限制，但仅能在欺骗卫星信号数较少时起作用。通过分析可见：

1）单一通用技术对欺骗式干扰抑制效果有限，仅可抑制某类或某些情况下的欺骗式干扰，综合多种技术对欺骗式干扰具有较好的效果，对于转发式干扰，当前应用通常要求可以抑制转发延时不小于 1.5 码片的干扰；

2）多天线方案通过检测欺骗式干扰来向识别干扰，不能识别可以伪造来向的多系统协同复杂干扰；

3）惯性信息辅助抗欺骗方案可以在捕获跟踪定位各阶段进行信号一致性检测，利用惯性信息作为基准可抑制更多的欺骗式干扰样式；

4）阵列天线接收机和惯性辅助接收机干扰抑制效果更优，但与单天线接收机相比，其体积、功耗及成本均会明显增加。

3 发展趋势分析

通过上述对国内外卫星导航欺骗式干扰抑制技术的研究情况，结合应用需求分析，本文认为卫星导航欺骗式干扰抑制技术主要有以下发展趋势：

(1)多源融合欺骗式干扰抑制技术

卫星导航定位精度高,但作为一种非自主导航手段,必然面临干扰的问题,与以惯性导航为代表的自主导航手段相结合是提升抗干扰能力的有效手段。近年来,随着以 Micro-PNT 为代表的小型化自主导航传感器的发展,两者结合必然能够更好的融合发展。

(2)高精度差分定位与干扰抑制技术的结合

欺骗干扰通常与压制干扰相结合,两者均会对导航卫星的伪距和载波相位观测量精度造成一定影响,这种影响对于高精度的差分定位接收机影响较大。因此,研究低失真干扰抑制算法,减小干扰抑制时对伪距和载波相位等观测量的影响,具有显著的应用价值。

(3)欺骗式干扰与压制式干扰联合抑制技术

当前的卫星导航接收机设计中,欺骗式干扰与压制式干扰的抑制算法基本是独立的,如何在设计上将二者有效融合,相互提升各自的干扰抑制效果,实现 1+1>2 的效果,也是未来需要重点考虑的研究方向。

(4)高集成度、低功耗的工程应用需求

工程应用中,对卫星导航设备的功耗和体积等技术指标提出了越来越高的要求,高集成度和低功耗一直是卫星导航接收机的发展趋势。随着卫星导航射频和基带芯片的研制,接收机的集成度大为提升,功耗大幅下降,导航接收机小型化是未来工程应用的研究重点与难点。

4　总结

欺骗式干扰抑制技术是当前卫星导航应用领域的重要发展方向,本文对卫星导航欺骗式干扰抑制技术进行了研究,论述了国内外欺骗式干扰抑制技术的研究现状,调研了国内外主要研究机构针对欺骗式干扰抑制采取的技术措施,进一步按照适用接收机的类型对技术进行了分类,并对各类技术的干扰抑制效果进行了对比分析。在此基础上,展望了未来欺骗式干扰抑制技术的发展趋势,对从事该项技术的研究者具有一定的参考借鉴价值。

参考文献

[1] 谢钢 . GPS 原理与接收机设计 [M]. 北京: 电子工业出版社, 2017.
Xie Gang. Principles of GPS and receiver design[M]. Beijing: Publishing House of Electronics Industry, 2017(in Chinese).

[2] 吴仁彪, 王文益, 卢丹, 等 . 卫星导航自适应抗干扰技术[M]. 北京: 科学出版社, 2015.
Wu Renbiao, Wang Wenyi, Lu Dan, et al. Adaptive interference mitigation in GNSS[M]. Beijing: Science Press, 2015(in Chinese).

[3] 刘鹏, 王盾, 陈耀辉, 等 . 导航电子对抗技术的研究现状及发展趋势[C]// 第九届中国卫星导航学术年会, 2018: 210-214.
Liu Peng, Wang Dun, Chen Yaohui, et al. Research status and development trend of GNSS electronic warfare[C]// Proceedings of 9th China Satellite Navigation Conference, 2018: 210-214(in Chinese).

[4] Volpe J. Vulnerability assessment of the transportation infrastructure relying on the global positioning system [J]. The Journal of Navigation, 2003, 56(2): 185-193.

[5] Shepard D P, Bhatti J A, Humphreys T E, et al. Evaluation of smart grid and civilian UAV vulnerability to GPS spoofing attacks[D]. The University of Texas at Austin, 2012.

[6] Bhatti J, Humphreys T E. Hostile control of ships via false GPS signals: demonstration and detection [J]. Navigation, 2017, 64(1): 51-66.

[7] Kerns A J, Shepard D P, Bhatti J A, et al. Unmanned aircraft capture and control via GPS spoofing[J]. Journal of Field Robotics, 2014, 31(4): 617-636.

[8] Humphreys T E, Bhatti J A, Shepard D P, et al. The texas spoofing test battery: toward a standard for evaluating GPS signal authentication techniques[C]// Proceedings of 25th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2012). Nashville, TN, 2012: 3569-3583.

[9] Wesson K D, Rothlisberger M P, Humphreys T E. A proposed navigation message authentication implementation for civil GPS anti-spoofing[C]// Proceedings of 24th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2011). Portland, OR, 2011: 3129-3140.

[10] Jafarnia-Jahromi A, Lin T, Broumandan A, et al. Detection and mitigation of spoofing attack on a vector based tracking GPS receiver[C]// Proceedings of International Technical Meeting of the Institute of Navigation, 2012: 1-11.

[11] Nielsen J, Broumandan A, Lachapelle G. GNSS spoofing detection for single antenna handheld receivers [J]. Annual of Navigation, 2011, 58(4): 335-344.

[12] Swaszek P F, Hartnett R J. Spoof detection using multiple COTS receivers in safety critical applications [C]// Proceedings of 26th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2013). Nashville, TN, 2013: 2921-2930.

[13] Nielsen J, Broumandan A, Lachapelle G. Method and system for detecting GNSS spoofing signals[P]. US Patent, No. 7952519, 2011.

[14] Broumandan A, Lachapelle G. Spoofing detection using GNSS/INS/odometer coupling for vehicular navigation[J]. Sensors, 2018, 18(5): 1305.

[15] Sergey L. Detection and elimination of GNSS spoofing signals with PVT solution estimation: Moscow(RU)[R]. US 2019/0129041 A1, 2019.

[16] Shin B, Park M, Jeon S, et al. Spoofing attack results determination in code domain using a spoofing process equation[J]. Sensors, 2019, 19(2): 293.

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

[18] Cheng X J, Cao K J, Xu J N, et al. Analysis on forgery patterns for GPS civil spoofing signals[C]// Proceedings of International Conference on Computer Sciences and Convergence Information Technology. IEEE, 2009: 353-356.

[19] 黄龙，吕志成，王飞雪．针对卫星导航接收机的欺骗干扰研究[J]．宇航学报，2012，33(7):884-890.
Huang Long, Lyu Zhicheng, Wang Feixue. Spoofing pattern research on GNSS receivers[J]. Journal of Astronautics, 2012, 33(7): 884-890(in Chinese).

[20] 严凯．GNSS 脆弱性仿真评估平台技术研究[D]．上海：上海交通大学，2013.
Yan Kai. Research on GNSS vulnerability simulation and assessment platform technology[D]. Shanghai: Shanghai Jiaotong University, 2013(in Chinese).

[21] 曹艳霞，田斌．GPS 转发干扰模式的研究[J]．电子科技，2006(4)：67-70.
Cao Yanxia, Tian Bin. Study of a novel retransmitted jamming of GPS receivers[J]. Electronic Science and Technology, 2006(4): 67-70(in Chinese).

[22] 何婷．GNSS 转发式欺骗干扰方法的改进[J]．测绘通报，2019(4)：71-74.
He Ting. Improvement of the method of GNSS relationship deception interference mode[J]. Bulletin of Surveying and Mapping, 2019(4): 71-74(in Chinese).

[23] Cheng X J, Xu J N, Cao K J, et al. An authenticity verification scheme based on hidden messages for current civilian GPS signals[C]// Proceedings of 4th International Conference on Computer Sciences and Convergence Information Technology (ICCIT'09). 2009: 345-352.

[24] 赵新凯，郭晶．基于欺骗式干扰的卫星导航抗干扰方法研究[C]// 北京地区高校研究生学术交流会，2008.
Zhao Xinkai, Guo Jing. Research on anti-jamming method of satellite navigation based on deceptive jamming [C]// Proceedings of Beijing University Graduate Academic Exchange, 2008(in Chinese).

[25] Tao H, Li H, Lu M. A GNSS anti-spoofing method based on the cooperation of multiple techniques[C]// Proceedings of 6th China Satellite Navigation Conference, 2015: 205-215.

[26] Yuan D, Li H, Lu M. GNSS spoofing mitigation based on joint detection of code Doppler and carrier Doppler in acquisition[C]// Proceedings of 5th China Satellite Navigation Conference, 2014: 763-774.

[27] Tu J, Zhan X, Zhang X, et al. Low-complexity GNSS anti-spoofing technique based on Doppler frequency difference monitoring[J]. IET Radar Sonar & Navigation, 2018, 12(9): 1058-1065.

[28] Tang B, Dai W, Xie W, et al. A new method for the estimation of GPS repeater jamming based on coloured noise Kalman filter[J]. The Journal of Navigation, 2011, 64: 141-150.

[29] 罗德巳．基于粒子滤波的 GNSS 抗欺骗式干扰研究[D]．哈尔滨：哈尔滨工业大学，2014.
Luo Desi. Research on GNSS anti-spoofing scheme based on particle fliter[D]. Harbin: Harbin Institute of Technology, 2014(in Chinese).

[30] Xu R, Ding M, Qi Y, et al. Performance analysis of GNSS/INS loosely coupled integration systems under spoofing attacks[J]. Sensors, 2018, 18(12):4108.

[31] Sun C, Cheong J W, Dempster A G, et al. GNSS spoofing detection by means of signal quality monitoring (SQM) metric combinations[J]. IEEE Access, 2018(6): 66428-66441.

[32] 张瑞华，贾琼琼，吴仁彪．利用矢量跟踪环路的欺骗干扰检测与抑制方法[J]．信号处理，2018，34(6)：62-70.
Zhang Ruihua, Jia Qiongqiong, Wu Renbiao. Spoofing detection and suppression method by utilizing vector tracking loop[J]. Journal of Signal Processing, 2018, 34(6): 62-70(in Chinese).