DOI:10.20079/j.issn.1001-893x.230821004

卫星导航欺骗干扰检测与抑制技术综述*

倪淑燕[1a],陈世淼[1b],付琦玮[1b],毛文轩[1b],雷拓峰[1b],宋 鑫[2]

(1.航天工程大学 a.电子与光学工程系;b.研究生院,北京 101416;
2.军事科学院国防科技创新研究院,北京 100071)

摘 要:全球导航卫星系统(Global Navigation Satellite System,GNSS)欺骗式干扰具有隐蔽性强、危害性大的特点,对 GNSS 造成了严重的安全威胁。介绍了生成式和转发式欺骗干扰的原理和关键技术,总结了现有的欺骗式干扰检测方法和抑制方法,并从成本、性能、复杂度、研究重点等方面对现有技术进行了详细分析。以性能和成本为指标,对比分析了现有干扰攻击、检测和抑制方法。最后,对未来欺骗式干扰防御研究值得关注的问题进行了展望,以期为后续研究提供思路。

关键词:全球卫星导航系统(GNSS);欺骗式干扰;欺骗干扰检测;欺骗干扰抑制

开放科学(资源服务)标识码(OSID):

中图分类号:TN967 **文献标志码**:A **文章编号**:1001-893X(2024)05-0812-09

Review on Spoofing Detection and Mitigation of Satellite Navigation

NI Shuyan[1a],CHEN Shimiao[1b],FU Qiwei[1b],MAO Wenxuan[1b],LEI Tuofeng[1b],SONG Xin[2]

(1a.Department of Electronic and Optical Engineering;1b.Graduate School,Space Engineering University,Beijing 101416,China;
2.National Innovation Institute of Defense Technology,Academy of Military Sciences,Beijing 100071,China)

Abstract:The spoofing against the Global Navigation Satellite System(GNSS) has the characteristics of strong concealment and high harm,which threatens the security of GNSS.First of all,the principle and key technologies of self-consistent and replay spoofing are introduced.Secondly,the existing spoofing detection and mitigation methods are summarized and classified,and the existing technologies are analyzed in detail from the aspects of cost,performance,complexity and research focus.Thirdly,a comparative analysis is conducted on existing spoofing attacks,detection,and suppression methods based on performance and cost.Finally,the issues worthy of attention in spoofing defense in the future are prospected,in hope of providing ideas for follow-up related researches.

Key words:global navigation satellite system(GNSS);spoofing;spoofing detection;spoofing mitigation

0 引 言

全球卫星导航系统(Global Navigation Satellite System,GNSS)在军事和民用领域中的应用逐渐广泛,社会对于 GNSS 提供的定位、导航和授时(Positioning Navigation and Timing,PNT)服务的依赖性迅速增加,因此 GNSS 的安全性和稳定性也受到了极大的关注。由于导航信号强度弱、信号调制方式公开、部分导航数据可以预测等原因,GNSS 极易受到欺骗式干扰[1],这对于导航系统是致命的。欺骗式干扰是欺骗设备发出与真实导航信号相似的虚假导航信号,通过策略使得目标接收机将虚假导航信号误以为是真实导航信号,从而使目标接收机获取错误的定位、速度或时间信息。文献[2-3]介绍了近年来欺骗干扰成功的案例,对以上事件分析可

* 收稿日期:2023-08-21;修回日期:2023-11-09
通信作者:陈世淼 Email:1004591154@qq.com

以看出,导航干扰已经逐渐从阻碍接收导航信号的压制式干扰转变为入侵导航系统、篡改导航信息的欺骗式干扰。相比于压制式干扰,欺骗式干扰不易被发现,危害性更强。

为提升对欺骗式干扰防御的研究,并为学者提供研究思路,本文对现有的欺骗式干扰相关文献资料进行总结、归纳和分析。

1　欺骗式干扰攻击

1.1　生成式欺骗干扰

全球卫星导航系统产生的导航信号分为民用信号和军用信号,其固民用信号的伪码和导航电文完全公开,这就意味着完全可以根据需求通过软硬件模拟真实导航信号的产生。针对特定目标或者区域,发送生成的虚假导航信号,使得其获得错误的导航信息,这就是生成式欺骗干扰。根据欺骗设备的复杂程度和欺骗效果,可以将生成式欺骗干扰分为初级、中级和高级:初级生成式欺骗干扰的欺骗效果差,极易被检测;高级生成式欺骗干扰需要多天线协同工作,技术实现难度大,当前公开的文献主要围绕中级生成式欺骗干扰展开。对于欺骗设备来说,实现生成式欺骗干扰的难点是:①如何使欺骗信号进入到目标接收机的跟踪环路;②目标接收机被欺骗后,如何在不被发现的情况下诱导目标接收机的导航数据发生H　。

针对难点①,当前欺骗信号进入跟踪环路的方法分为公开欺骗和隐蔽欺骗两种:公开欺骗是指对目标接收机施加大功率压制式干扰,让目标接收机跟踪环路失锁,同时施加功率较高的欺骗信号,使得目标接收机在重捕获过程中捕获欺骗信号;隐蔽欺骗是指欺骗设备产生与目标接收机天线接收到的真实信号码相位和多普勒频移均匹配的虚假信号,在欺骗信号进入跟踪环路之前,欺骗信号的功率一直很小。在欺骗信号成功进入跟踪环路后,生成式欺骗信号提升信号幅值,并使其码相位和载波相位发生偏移,实现欺骗。该方法不需要压制式干扰和重新捕获,不易被检测,但对欺骗设备要求高。

针对难点②,在欺骗信号进入到接收机欺骗环路之后,欺骗目标可以通过故障检测器来判断是否被欺骗。故障检测器检测欺骗有两种方式:一是通过导航接收机的导航数据持续观察,若导航数据变化太大,超过设定阈值则判定其被欺骗;二是将导航接收机与惯性导航等其他导航方式相结合,对比不同导航方式的导航结果,若两者差值大于设定阈值,则判定被欺骗。对于以上问题,研究人员首先对欺骗目标的一个或者多个定位设备进行误差评估,在此基础上推导出可欺骗的位置集,将欺骗信号的定位结果限制在位置集内,从而防止被检测。

在进行生成式欺骗干扰的检测时可以从以下方面展开:欺骗信号的功率、载波多普勒频移、初始码相位差和载波相位差;欺骗信号进入跟踪环路后的环路参数;卫星导航与其他导航方式的定位结果差值的大小和变化规律。

1.2　转发式欺骗干扰

除了公开的民用导航信号外,还存在采用加密扩频码的军用导航信号和加密的民用导航信号两种类型无法自主生成的导航信号。而要想成功实现欺骗干扰,必须保证扩频码和导航数据的正确性。针对这种情况,可以通过转发式欺骗干扰来实现。欺骗设备首先接收真实的导航信号,根据目标欺骗位置对真实的导航信号增加适当的延迟,最后通过高增益发射机发送,实现对目标接收机的欺骗。

最简单的转发式欺骗设备具有一个接收天线,欺骗设备将接收到的真实信号加上时延再转发给目标接收机,时延包括转发欺骗设备处理信号的时延和从转发式欺骗设备天线到接收机天线的传输时延[4]。欺骗干扰中不同卫星的导航信号增加的时延相同,欺骗位置信息与转发式欺骗设备位置信息一致,目标接收机的时间将会比真实时间早。复杂的转发式欺骗设备具有多个接收机天线和多通道信号处理功能,欺骗设备可在每一个转发通道中调整信号的增益和幅值,从而独立控制每一个虚假导航信号的相对传输时延,产生任何可能的虚假位置信息,虚假的位置信息和时间信息具有相关性。

针对转发式欺骗干扰的产生,文献[5-7]分别对转发式欺骗干扰的功率、时延和多普勒频移的设置进行了详细研究;文献[8]分析了转发式欺骗干扰对不同运动状态接收机的信噪比、伪距差、定位偏差和信噪比的影响;文献[9-10]分析了转发式欺骗干扰对码速率、功率和 CMC(Code Minus Carrier)的影响,这对于研究转发式干扰检测具有参考意义。

表 1 对生成式和转发式欺骗干扰的优缺点和实现难易程度进行了对比分析,总的来说,两种干扰方式各有其固点,需要根据实际需求和使用环境来选择最合适的干扰方式。

表 1 生成式和转发式欺骗干扰对比分析

Tab.1 Comparison and analysis of generative and forwarding spoofing

干扰方式	优点	缺点	实现难度
生成式	可以有效欺骗卫星导航接收机，使其接收到错误的导航信息	需要知道卫星导航信号的详细信息，如信号结构、调制方式等	较难，需要具备信号处理、通信和卫星导航等相关领域的知识
转发式	不需要知道卫星导航信号的详细信息，易于实现较大范围的干扰覆盖	可能会对其他卫星导航接收机造成干扰，不适合用于精密干扰	较易，只需要对信号进行简单的接收和转发操作

2 欺骗式干扰检测

2.1 基于单天线接收机信号特征的欺骗干扰检测方法

欺骗检测方法研究初期，学者们通过寻找单天线接收机被欺骗后发生变化的信号特征来进行欺骗检测。由于欺骗信号无法完美模拟真实信号的功率，欺骗式干扰的加入会引起信号功率、噪声功率、载噪比等的变化。在捕获跟踪阶段，隐蔽欺骗策略下欺骗信号需要进入跟踪环路并缓慢增加功率、改变相位，这个过程会引起真实码和欺骗码相位之间的不对准和多个相关峰的出现。在欺骗信号进入跟踪环路后，如果隐蔽欺骗的欺骗信号变化过快或者欺骗策略为公开欺骗，会导致伪距、时间、测速结果、定位结果等信息的突然 H 。基于以上检测特征，将基于单天线接收机信号特征的欺骗干扰检测方法分类，如表 2 所示。

表 2 基于单天线接收机信号特征的欺骗干扰检测方法分类

Tab.2 Classification of spoofing detection methods based on signal features of single antenna receivers

应用阶段	检测方法	局限性
射频前端	AGC 增益监测[11]	仅对高功率欺骗信号有效
捕获阶段	信号功率监测[12]	仅对高功率欺骗信号有效
	载噪比监[13]测	载噪比变化易受环境影响
	多频点功率对比[14]	要求接收机具有多频定位功能
	相关峰个数检测方法[15]	要求接收机具有多相关器
跟踪阶段	信号质量监测[16]	检测效果受到真实信号和欺骗信号相关峰间隔的影响
	多普勒频率监测[17]	要求天线处于垂直往复运动状态
	不同频点的码相关一致性检验[18-19]	要求接收机具有多频定位功能
数据解算	钟差变化监测[20]	需要已知接收机运动状态
	接收机自主完整性监控[21]	仅在欺骗信号较少时有效

基于单天线接收机信号特征的欺骗干扰检测方法具有成本低、灵活高效的特点，是目前研究最多、应用最广的方法。将该方法与其他检测方法相结合，提高对多种欺骗干扰的检测概率，是未来的主要研究方向。

2.2 基于组合导航的欺骗干扰检测方法

惯性导航、视觉导航等导航方式不受欺骗干扰的影响，可将 GNSS 与其他导航方式相结合，通过不同导航方式的导航结果的差异来进行欺骗干扰检测，如果差异超过设定阈值，则判定为受到欺骗攻击。

惯性导航和 GNSS 组合可以通过对轨迹、加速度、位置等特征进行一致性检验，达到欺骗检测的目的：文献[22]将 GNSS 接收机估计的轨迹与 INS 得到的轨迹进行比较；文献[23]使用加速度计和 GNSS 接收机计算的加速度进行比较；文献[24]在 GNSS/INS 集成系统中使用基于残差的 RAIM 算法来检测欺骗；文献[25]通过紧密耦合的 GNSS/INS 集成系统结合扩展卡尔曼滤波器来检测欺骗；文献[26]提出了一种基于视觉/惯性/GNSS 定位耦合算法的欺骗检测方法，可有效检测偏差注入速度大于 1 m/s的欺骗干扰。不管是针对时间还是针对位置的欺骗干扰，被欺骗接收机的钟差都会发生异 | 化。文献[27]构造了芯片级原子钟辅助的欺骗检测模型，欺骗检测性能与时钟的时间保持能力呈正比。

基于组合导航的欺骗干扰检测方法对于转发式欺骗干扰检测效果较好。转发式欺骗干扰的信号滞后于真实信号，这会导致被欺骗设备的时间早于真实时间或者欺骗设备的位置偏离真实位置，通过组

合导航可以实现欺骗干扰检测。对于生成式干扰,该方法检测性能与欺骗信号的诱偏速度相关:如果欺骗信号诱偏过快,单位时间内H　超过其他导航方式的误差范围,则会被成功检测。同时,其他导航方式定位精度的增加会提高该方法的检测能力。

总的来说,基于组合导航的欺骗干扰检测方法的检测性能优于基于单天线接收机的检测方法,但是该方法需要额外的硬件,系统组成更加复杂。当前该方法的相关文献主要围绕寻找新的检测特征展开,后续应针对检测阈值的设置、多个差异特征联合检测和检测到欺骗后如何进行定位进行深入研究。

2.3　基于信号空间相关性的欺骗干扰检测方法

导航系统中多数导航卫星相对于地球坐标系处于运动的状态,接收机接收到的真实导航信号的方向也是处于动态变化的,当前常见的欺骗式干扰一般由同一欺骗设备产生,欺骗信号来自同一个方向,即使是具有多个发射天线的欺骗设备也难以模拟真实导航信号的方向性,所以欺骗信号的空间相关性明显高于真实信号。因此,许多学者以欺骗信号和真实信号来向不同以及来向不同引起的其他变量的不同为突破点进行欺骗信号的检测,根据天线或者接收机的数目不同可以分为多天线、双天线和旋转单天线 3 种不同的检测方法。

阵列天线广泛应用于导航压制式干扰的检测和消除,由于其能够实固波达方向估计和波束形成,许多学者基于阵列天线展开了欺骗式干扰的防御研究。文献[28]提出了一种使用阵列天线对解扩前信号进行欺骗干扰检测和抑制的方法。该方法利用原始基带信号,建立循环相关(Cyclic Correlation)矩阵,进行奇异值分解,通过进行循环相关特征值检验(Cyclic Correlation Eigenvalue Test,CCET)判定是否存在欺骗干扰,若存在欺骗干扰则通过特征向量建立投影子空间消除欺骗干扰。文献[29]一方面通过多天线计算导航信号的实际到达方向,一方面通过星历计算卫星的理论到达方向,根据理论值和真实值的差异来进行欺骗检测。文献[30]通过多天线的载波相位双差值检测欺骗式干扰,采用最小二乘法求解干扰方向矢量,进而构建其正交矩阵消除干扰。阵列天线在欺骗式干扰的检测和消除的应用上都有很好的性能,成本、复杂度和实时性是限制其广泛应用的主要原因。文献[31]利用多个接收机天线的位置信息推导出不同信号的到达角度差(Intersection Angle between Two Directions of Arrival,IA-DOA),基于 IA-DOA 的理想值与观测值进行广义似然比检验,实现了多来向欺骗干扰检测。

基于双天线的欺骗检测方法一般是通过单方向欺骗干扰在双天线下的某些信号特征与真实信号不同来进行的。文献[32]通过双天线接收机进行信号的载波相位双差测量,利用真实导航信号的载波相位双差值随着时间H　、欺骗信号的载波相位双差保持不变这一特性进行欺骗信号的鉴别,适用于静态欺骗场景。文献[33]针对基于接收机基线长度的欺骗干扰检测方法在短基线和低定位精度下检测性能差的问题,提出了基于双接收机的欺骗式干扰检测算法。文献[34]使用载波相位双差、星历数据和基线长度来估计基线向量,根据其误差平方和的统计特性进行假设检验,可以有效检测静态和动态环境下的单方向和多方向欺骗信号。此外,对于单方向的欺骗式干扰,还可以利用信号到达时间差和多普勒频差来进行欺骗检测。当前的基于双天线方法的检测效率与天线间的距离相关,距离越大检测成功率越高。许多设备对于天线架设有一定的空间限制,提高窄间距下的欺骗检测率能够增加双天线检测方法的普适性。

以上两种方法对于天线数目和相对位置的要求限制了其应固,许多学者采用旋转单天线的方法[35]测量接收到信号的空间相关性,实现欺骗干扰检测。文献[36]使用单个旋转天线进行空间功率测量,根据信号功率的变化曲线来进行欺骗检测。文献[35]利用改进概率神经网络对旋转天线的载波相位双差进行分类和处理,相比于传统方法有着更高的检测率。相对于多天线检测技术,旋转单天线检测方法具有复杂度低、适应性广的优点,但是天线的旋转会导致导航信号利用率的降低,对导航定位精度有一定的影响。

由于技术和成本的限制,当前实现的欺骗干扰均采用单一发射天线,即多个欺骗信号来自同一个方向,同时,基于信号空间相关性的欺骗干扰检测方法可有效检测具有一个发射天线的欺骗干扰,因此该方法为当前鲁棒性最好的检测方法。然而,该方法的实现对接收机天线的要求较高,天线的成本和体积空间限制了该方法的广泛应用,检测算法的复杂性也进一步增加了接收机的负担,如何降低成本和算法复杂度是当前检测方法的难点。此外,随着技术的发展,未来必定会面临多来向的欺骗干扰。当前,文献[31]能够实现多来向欺骗干扰的检测,但是当欺骗干扰来向与真实信号来向相差较小时检测性能下降,未来应当提高多来向欺骗干扰检测的性能。

2.4 基于机器学习的欺骗式干扰检测方法

欺骗干扰检测可以看作是二元分类问题,机器学习在二元分类问题上有着广泛的应用和较好的性能,许多学者使用机器学习来提高现有欺骗检测方法的性能。表 3 列举了当前使用机器学习的欺骗干扰检测算法。机器学习的应用能够实现多个特征参数的融合检测,如文献[41]将信号的载噪比、伪距、载波频率等信息同时作为特征参数来检测欺骗干扰,在提高检测成功率的同时增强了检测方法的鲁棒性,能更好地应对不同的欺骗干扰。

表 3 基于机器学习的欺骗式干扰检测方法

Tab.3 Spoofing detection methods based on machine learning

算法	输入特征参数	检测干扰类型	检测效果
改进概率神经网络[35]	旋转天线的载波相位双差	来自同一方向的欺骗式干扰	对欺骗信号的检测成功率可达 98.84%,检测时间不超过1 s
卷积神经网络[37]	信号捕获中的二维搜索矩阵	小延迟(0~2 个码片)欺骗干扰	对于延迟大于 0.5 码片的欺骗干扰可以达到 99.94% 的检测成功率
K 最近邻分类算法[38]	信号捕获中的二维搜索矩阵	小延迟(0~2 个码片)欺骗干扰	对于延迟大于 0.5 码片的欺骗干扰可以达到 99.95% 的检测成功率
支持向量机[39]	SQM 平均值和方差、C/N0 平均值和方差异、伪距定位残差、多普勒测速残差、时间钟差和时钟漂移等	中级生成式欺骗式干扰	在 TEXBAT 数据集中可以达到 93.97% 的检测成功率;在 OAKBAT 数据集中可以达到 97% 的检测成功率
支持向量机[40]	C/N0、伪距、载波多普勒频率、全载波相位、接收机时钟偏差、接收机时钟漂移等多个数据的互相关矩阵	生成式和转发式欺骗干扰	在文献进行验证的数据集中可以达到 97.72% 的检测成功率
多层感知神经网络[42]	钟差	时间同步攻击	优于传统的算法
支持向量机[43]	惯性导航系统和卫星导航系统的定位结果的距离	生成式和转发式欺骗干扰	在文献中设计的场景可以达到 95% 的检测成功率
概率神经网络[44]	载波相位双差观测值	来自同一方向的欺骗式干扰	对欺骗信号的检测成功率可达 98.51%,且耗时不超过0.1 s

从表 3 可知,相比于传统的欺骗式干扰检测算法,应用机器学习的检测方法有着更高的检测成功率,选择检测效果更好、计算量更小的模型和更有效的模型输入变量是该检测算法的主要研究方向。但是,检测的成功率会受到用于训练和验证的数据集的影响,将该方法应用于真实场景下可能无法达到文献所述的检测率。因此,在进行基于机器学习的欺骗式干扰检测方法研究时,建议采用标准数据集,可以参考德克萨斯大学奥斯汀分校无线电导航实验室提供的 TEXBAT 数据集和橡树岭国家实验室提供的 GPS 和 GALILEO 欺骗数据集 OAKBAT。

2.5 基于加密认证的欺骗干扰检测方法

军用导航信号长期以来一直受到密码防欺骗技术的保护,只有授权用户才能使用军用导航信号。当前许多学者通过密码学的加密认证技术对民用导航信号进行加密,使得导航信号难以被预测,并且接收机可以根据接收到的信号判断其完整性,从而更好地抵御欺骗攻击。根据加密认证方法和对象的不同可以将该方法分为导航消息认证(Navigation Message Authentication,NMA)、扩频码认证(Spreading Code Authentication,SCA)和组合认证方法。

基于加密认证的欺骗干扰检测方法的实现都需要对卫星信号进行修改,这对现有的已经定义的导航消息结构的全球导航卫星系统来说是不现实的。此外,由于加密认证中秘钥的传输一般通过存储在导航电文中,接收机获取完整的秘钥需要的时间较长,可能会达到分钟的量级。生成式欺骗干扰无法生成加密信号,故该方法可有效检测生成式欺骗干扰。转发式欺骗干扰不需要已知信号体制,但是会导致信号的延迟,因此,通过加密信号的时变性来实现转发式欺骗干扰的检测。NMA 和 SCA 技术的应用对象分别为导航消息和扩频码,但原则上专用于认证的信号分量也可以在其他对象插入,例如副载波或载波级别的不可预测特征、可变┆ 整形、跳频等。加密认证方法对于不同种欺骗式干扰均有很好的防御效果,选取认证速度快、占用资源小、鲁棒性

更强的认证方法是该方法主要研究方向。表 4 对不同的欺骗式干扰检测方法进行了总结和分析。

表 4　欺骗干扰检测方法性能对比分析

Tab.4 Comparative of performance of spoofing detection methods

分类方法		复杂度	性能	局限性
单天线接收机信号特征	AGC 监测	低	中	检测阈值需要自适应变化,仅对能量较高的干扰有效
	载噪比监测	中	中	低载噪比下检测性能较差
	SQM	中	高	计算量大,易受噪声影响
组合导航		高	高	需要额外的硬件
信号空间相关性	阵列天线	高	高	需要阵列天线且阵元间距小于波长的一半
	双天线	中	中	仅能够检测来自同一方向的欺骗干扰
	旋转单天线	高	中	接收机需要处于静止状态
机器学习		高	高	性能受到训练数据集的影响,检测实时性较差
加密认证	NMA	中	中	实现难度大,无法检测转发式干扰
	SCA	中	中	

3　欺骗式干扰抑制

3.1　信号重构

信号重构法是指在完成欺骗干扰检测后,获取欺骗干扰的码延迟、多普勒频率、载波相位和信号幅度,以此来重构欺骗信号,然后从原始中频导航信号中减去重构的欺骗信号,得到不含欺骗信号的导航信号,实现欺骗干扰抑制。文献[45]通过欺骗信号分类模块将跟踪的信号分为欺骗信号和真实信号,并基于欺骗信号信息进行信号重构和消除,然后重新检测处理后的信号,若存在欺骗信号则重新进行欺骗信号的重构和消除。文献[46]通过估算欺骗信号的幅度和相位来重构欺骗信号,将重构信号与延迟原信号对消,并通过定义干扰对消比(Interference Cancellation Ratio,ICR)进行了性能评估。从以上文献仿真结果发现,信号重构法的抑制效果好,但该方法需要持续、准确获取欺骗信号的信息,复杂性很高,实现难度大。

3.2　子空间投影

对于欺骗信号的所有参数进行准确估计的难度和运算量都很大,这限制了信号重构法的应用[47]。文献[48]提出了一种子空间投影方法,通过捕获跟踪来估计欺骗信号的载波频率和码相位,基于其 PRN 码的准正交性构建伪造信号的信号子空间,将接收到的信号正交投影到子空间上,抑制欺骗信号,从而实现对真实信号的捕获和跟踪。文献[49]通过参数估计法来估计欺骗信号的载波频率,具有更低的运算复杂度。与信号重构法相比,该方法减少了所需要的欺骗信号信息,具有更好的稳健性。但是,若欺骗信号与真实信号相位差少于一个码片,将失去抑制功能,说明该方法无法检测偏离较小的欺骗信号。

3.3　波束形成

自适应波束形成可以控制阵列天线的辐射方向图,抑制欺骗干扰源所在方向的欺骗信号,增强导航卫星方向的真实导航信号。波束形成技术与基于阵列天线的欺骗干扰检测技术同时使用,首先通过阵列天线获取基带信号并建立循环矩阵,根据特征值检验实现欺骗干扰检测,而后通过波束形成技术实现欺骗干扰的抑制和真实信号的增强。自适应波束形成在压制式干扰的抑制中有很多应用,算法也比较成熟,可直接应用于欺骗干扰抑制,并且可以同时实现压制式和欺骗式干扰的抑制。但是,随着干扰来向的增加,阵列天线需要进一步增加天线阵元的数目,因此设备的复杂性和高成本是限制其广泛应用的主要原因。

3.4　多相关器法

在接收机中引入多相关器结构,可以同时捕获和跟踪真实信号和欺骗,而后通过判定方法确认真实信号和排除欺骗信号,实现欺骗信号的检测和抑制。当在接收信号中存在多个信号时,在没有任何欺骗信号的先验知识的情况下,使用多相关器执行多信号跟踪。采用多径估计延迟锁相环(Multipath Estimating Delay Lock Loop,MEDLL)技术对基带信号进行处理,得到信号的幅度、传播延迟和载波相位,记作(τ_0,a_0,ϕ_0)和(τ_1,a_1,ϕ_1)[50],然后基于信号的幅度、传播延迟和载波相位的估计值,分别从原始基带信号中除去其中一组信号并对其进行跟踪,从而得到另一组信号的跟踪结果。

3.5　组合导航

前文介绍了基于组合导航的欺骗干扰检测方法,若判定卫星导航接收机被欺骗,则采用非卫星导航系统进行导航,实现欺骗干扰的抑制。该方法的本质是舍弃不可信的卫星导航结果,选用其他可信的导航结果。该方法的缺点在于需要多个导航系

统,成本较高,并且抑制后的定位精度取决于其他导航方式。

表 5 对不同欺骗式干扰抑制方法进行了总结和分析。

表 5 欺骗干扰抑制方法性能对比分析

Tab.5 Comparative analysis of performance of spoofing suppression methods

方法	复杂度	性能	局限性
信号重构	高	中	需要持续准确获取欺骗信号信息
子空间投影	中	好	欺骗信号和真实信号相位差少于一个码片时失效
波束形成	中	好	需要阵列天线且阵元间距小于波长的一半
多相关器法	低	中	计算量大且欺骗信号功率较大时将失效
组合导航	中	中	需要额外的硬件或传感器
直接定位法	中	中	低信噪比下性能差

4 攻击和检测技术对比分析

并非所有的防御措施都能够抵挡所有种类的欺骗攻击,同样,不同类型的欺骗攻击和防御技术的成本也存在差异。显然,在威胁方面,成本较低的攻击模式更有可能被使用,因为其所需设备和专业知识相对较少。因此,接收机应采用最经济的技术来抵御大部分低成本攻击。根据所需应用场景的安全要求和接收机的成本预算,设计者可进一步选择防御其他攻击模式。

为了给研究人员提供指导,本文根据成本对现有当前主流欺骗攻击方法进行排序,如表 6 所示。首先,以成本为依据对攻击和检测技术进行排序,在表中按照从左到右(攻击)和从上到下(检测)的成本增加的顺序排列,成本包括开发或硬件购买的成本、运行所需的专业知识以及操作的复杂性。针对不同的欺骗干扰检测方法列举了可以搭配进行的欺骗干扰抑制方法,同时也列举了不同欺骗干扰检测方法应对不同欺骗干扰攻击时的检测效果。

表 6 欺骗干扰攻击和检测技术分析

Tab.6 Analysis of spoofing attacks and detection

欺骗检测方法	检测效果									
	AGC 监测	载噪比监测	SQM	组合导航	双天线	阵列天线	旋转单天线	机器学习	NMA	SCA
转发式、单接收天线、单发射天线	~	~	~	~	√	√	√	~	×	×
生成式、单发射天线	√	√	√	√	√	√	√	√	√	√
生成式、单接收天线、单发射天线	~	~	~	~	√	√	√	~	√	√
转发式、多接收天线、单发射天线	~	~	~	~	~	~	√	~	×	×
生成式、多接收天线、多发射天线	~	~	~	~	~	~	~	~	√	√
转发式、多接收天线、多发射天线	~	~	~	~	~	~	~	~	×	×

注:√表示检测性能好,~表示检测性能适中或视情况而定,×表示性能差。

5 研究展望

在借鉴国内外研究成果的基础上,通过对比不同防御方法的性能,结合当前研究的发展趋势,建议在未来的研究中重点关注以下 5 个方面:

1)多种检测方法融合检测。当前不存在能够应对所有欺骗干扰的防御措施,许多检测方法仅针对特定的欺骗干扰。应深入研究多种欺骗检测技术的组合方法,深入集成不同的检测方法,提高欺骗检测的成功率。

2)基于阵列天线的防御技术。随着天线工艺的发展,限制阵列天线广泛应用的成本、体积等短板逐渐被克服。阵列天线具有灵活的波束合成能力和高增益辐射,使得其在压制式、欺骗式干扰领域都表现出优异的性能,能够同时实现干扰的检测和抑制。

3)将传统防御方法与机器学习结合。机器学习作为近年热点研究内容,在计算机视觉、模式识别等领域效果显著,将机器学习与传统检测方法结合能够有效提高检测效率和检测速度。

4)加强欺骗干扰抑制研究。欺骗式干扰的防御包括欺骗式干扰的检测和抑制,当前防御技术侧重于欺骗干扰的检测,然而检测到干扰但不能实现干扰的抑制不是我们想要的结果。因此,应当寻找新的干扰抑制方法或者提高现有抑制方法的抑制能力,提高被欺骗接收机的定位精度。

5)建立完善标准数据集。全球导航卫星系统欺骗发展越来越快,为方便学者展开欺骗干扰研究,

应当建立一套标准、完善的数据集。TEXBAT 数据集和 OAKBAT 数据集为当前领域内较为权威的数据集,但是上述数据集的建立并未考虑信号的来向,无法用于验证基于信号空间相关性的欺骗干扰检测方法。此外,当前并没有针对国产“北斗”导航系统的公开数据集,不利于“北斗”导航系统欺骗检测技术的发展。因此,应当建立完善的“北斗”导航数据集,推动“北斗”导航欺骗干扰检测技术研究的发展。

6　结束语

欺骗式干扰严重影响了卫星导航系统的安全应用,对欺骗式干扰展开防御研究刻不容缓。本文从欺骗式干扰攻击、检测和抑制 3 个方面对现有研究方法进行归纳和总结,指出了不同方法的性能和关键技术,并进行了横向对比分析,便于学者了解不同方法当前研究现状和研究重点,从而更好地开展深入的学术研究。

参考文献:

[1] MOSAVI M R, NASRPOOYA Z, MOAZEDI M. Advanced anti-spoofing methods in tracking loop[J]. Journal of Navigation, 2016, 69(4): 883-904.

[2] HARTMANN K, GILES K. UAV exploitation: a new domain for cyber power[C]//Proceedings of 2016 8th International Conference on Cyber Conflict. Tallinn: IEEE, 2016: 205-221.

[3] GREGORY P. EASA reports GNSS jamming/spoofing amid ukraine conflict[EB/OL]. (2022-03-18)[2023-08-08]. https://www.ainonline.com/aviation-news/air-transport/2022-03-18/easa-reports-gnss-jamming-spoofing-amid-ukraine-conflict.

[4] 赵香香,陈潇,郭旭强.一种针对用户 GNSS 时钟的转发式欺骗方法[J].电讯技术,2020,60(12):1415-1419.

[5] 史鹏亮,王晓宇,薛瑞.实施转发式 GNSS 欺骗干扰的功率控制策略研究[J].现代导航,2021,12(2):79-89.

[6] 毛虎,吴德伟,王永庆,等.对 GPS 接收机的转发欺骗干扰时延控制与运用策略分析[J].弹箭与制导学报,2019,39(5):147-153.

[7] BIAN S F, HU Y F, CHEN C, et al. Research on GNSS repeater spoofing technique for fake position, fake time & fake velocity[C]//Proceedings of 2017 IEEE International Conference on Advanced Intelligent Mechatronics. Munich: IEEE, 2017: 1430-1434.

[8] COULON M, CHABORY A, GARCIA-PENA A, et al. Characterization of meaconing and its impact on GNSS receivers[C]//Proceedings of the 33rd International Technical Meeting of The Satellite Division of The Institute of Navigation. Miami: ION, 2020: 3713-3737.

[9] BLUM R, DOTTERBOCK D, PANY T. Investigation of the vulnerability of mobile networks against spoofing attacks on their GNSS timing-receiver and developing a meaconing protection[C]//Proceedings of 2019 International Technical Meeting of The Institute of Navigation. Reston: ION, 2019: 345-362.

[10] 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 and Tutorials, 2020, 22(1): 249-291.

[11] AKOS D M. Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control(AGC)[J]. Navigation, 2012, 59(4): 281-290.

[12] JAFARNIA-JAHROMI A, BROUMANDAN A, NIELSEN J, et al. Pre-despreading authenticity verification for GPS L1 C/A signals[J]. Navigation, 2014, 61(1): 1-11.

[13] HU Y F, BIAN S F, CAO K J, et al. GNSS spoofing detection based on new signal quality assessment model[J]. GPS Solutions, 2018, 22(1): 1-13.

[14] DEHGHANIAN V, NIELSEN J, LACHAPELLE G. GNSS spoofing detection based on receiver C/No estimates[C]//Proceedings of the 25th International Technical Meeting of The Satellite Division of The Institute of Navigation. Nashville: ION, 2012: 2878-2884.

[15] HAN Y, ZHANG Q, LI C K, et al. Analysis of the influence of the loop filter in the phase locked loop on the output phase noise[C]//Proceedings of 2018 15th International Computer Conference on Wavelet Active Media Technology and Information Processing. Chengdu: IEEE, 2018: 185-189.

[16] SUN C, CHEONG J W, DEMPSTER A G, et al. Moving variance-based signal quality monitoring method for spoofing detection[J]. GPS Solutions, 2018, 22(3): 83-96.

[17] 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): 1655-1664.

[18] 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. Long Beach: ION, 2005: 1285-1290.

[19] 易曙明,游凌,李显.一种改进的民用 GPS 异步欺骗技术[J].电讯技术,2021,61(2):149-156.

[20] HWANG P Y, MCGRAW G A. Receiver autonomous signal authentication(RASA) based on clock stability analysis[C]//Proceedings of 2014 IEEE/ION Position, Location and Navigation Symposium. Monterey: IEEE, 2014: 270-281.

[21] SUN Y, FU L. A new threat for pseudorange-based RAIM: adversarial attacks on GNSS positioning[J]. IEEE Access, 2019, 7: 126051-126058.

[22] SWASZEK P F, PRATZ S A, AROCHO B N, et al. GNSS spoof detection using shipboard IMU measurements[C]//Proceedings of the 27th International Technical Meeting of the Satellite Division of The Institute of Navigation. Tampa: ION, 2014: 745-758.

[23] KWON K C, SHIM D S. Performance analysis of direct GNSS spoofing detection with accelerometers for constant velocity[J]. International Journal of Control, Automation and Systems, 2022, 20(8): 2749-2758.

[24] GAO Y J, LI G Y. A slowly varying spoofing algorithm avoiding tightly-coupled GNSS/IMU with multiple anti-

spoofing techniques[J].IEEE Transactions on Vehicular Technology,2022,71(8):8864-8876.
[25] TANIL Ç,KHANAFSEH S,JOERGER M,et al.An INS monitor to detect GNSS spoofers capable of tracking vehicle position[J].IEEE Transactions on Aerospace and Electronic Systems,2018,54(1):131-143.
[26] GU N Z,XING F,YOU Z.GNSS spoofing detection based on coupled visual/inertial/GNSS navigation system[J].Sensors,2021,21(20):1-6.
[27] 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.
[28] 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):1-5.
[29] APPEL M,KONOVALTSEV A,MEURER M.Joint antenna array attitude tracking and spoofing detection based on phase difference measurements[C]//Proceedings of the 29th International Technical Meeting of The Satellite Division of The Institute of Navigation.Portland:ION,2016:3018-3026.
[30] 崔建华,程乃平,倪淑燕.阵列天线抑制欺骗ɣ 航干扰信号方法研究[J].电子学报,2018,46(2):365-371.
[31] CHEN Z Y,LI H,WEI Y M,et al.GNSS antispoofing method using the intersection angle between two directions of arrival(IA-DOA) for multiantenna receivers[J].GPS Solutions,2022,27(1):1-11.
[32] JAHROMI A J,BROUMANDAN A,DANESHMAND S,et al.A double antenna approach toward detection classification and mitigation of GNSS structural interference[EB/OL].[2023-08-08].https://xueshu.baidu.com/usercenter/paper/show?paperid=1af697c2ffc6830176731ed021cf5aeb&site=xueshu_se.
[33] 陈世淼,倪淑燕,程凌峰,等.基于 IMM-KF 算法改进的欺骗式干扰检测算法[J].电讯技术,2024,64(4):559-566.
[34] CHEN J J,XU Y,YUAN H,et al.A new GNSS spoofing detection method using two antennas[J].IEEE Access,2020,8:110738-110747.
[35] CHANG H W,PANG C L,ZHANG L,et al.Rotating single-antenna spoofing signal detection method based on IPNN[J].Sensors,2022,22(19):1-9.
[36] WANG F,LI H,LU M Q.GNSS spoofing countermeasure with a single rotating antenna[J].IEEE Access,2017,5:8039-8047.
[37] LI J Z,ZHU X W,OUYANG M J,et al.Research on multi-peak detection of small delay spoofing signal[J].IEEE Access,2020,8:151777-151787.
[38] LIJ Z,LI W Q,HE S F,et al.Research on detection of spoofing signal with small delay based on KNN[C]//Proceedings of 2020 IEEE 3rd International Conference on Electronics Technology.Chengdu:IEEE,2020:625-629.
[39] CHEN Z K,LI J Z,LI J,et al.GNSS multiparameter spoofing detection method based on support vector machine[J].IEEE Sensors Journal,2022,22(18):17864-17874.
[40] SEMANJSKI S,SEMANJSKI I,DE WILDE 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):1-6.
[41] OROUJI N,MOSAVI M R.A multi-layer perceptron neural network to mitigate the interference of time synchronization attacks in stationary GPS receivers[J].GPS Solutions,2021,25(3):84-89.
[42] PANICE G,LUONGO S,GIGANTE G,et al.A SVM-based detection approach for GPS spoofing attacks to UAV[C]//Proceedings of 2017 23rd International Conference on Automation and Computing.Huddersfield:IEEE,2017:1-11.
[43] 庞春雷,郭泽辉,吕敏敏,等.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.
[44] SHEPARD D P,HUMPHREYS T.Straight talk on anti-spoofing securing the future of PNT disruption[J].GPS World,2012,13(1):31-34.
[45] BROUMANDAN A,JAFARNIA-JAHROMI A,LACHAPELLE G.Spoofing detection,classification and cancelation(SDCC) receiver architecture for a moving GNSS receiver[J].GPS Solutions,2015,19(3):475-487.
[46] 孙迅,吴兆军,聂裕平.一种新的卫星导航欺骗干扰抑制方法[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.哈尔滨:中国卫星导航学会,2018:28-32.
[47] 张佳琪,李归,姚元,等.基于 GNSS 多通道跟踪接收机的阵列反欺骗方法[J].电讯技术,2023,63(6):817-825.
[48] HANS,CHEN L,MENG W X,et al.Improve the security of GNSS receivers through spoofing mitigation[J].IEEE Access,2017,5:21057-21069.
[49] 卢丹,白天霖.利用信号重构的全球导航卫星系统欺骗干扰抑制方法[J].电子与信息学报,2020,42(5):1268-1273.
[50] SHANG X Y,SUN F P,ZHANG L D,et al.Detection and mitigation of GNSS spoofing via the pseudorange difference between epochs in a multicorrelator receiver[J].GPS Solutions,2022,26(2):37-44.

作者简介:

倪淑燕 女,1981 年生于河北清河,2010 年获博士学位,现为副教授,主要研究方向为卫星导航抗干扰、航天测控通信、电路与系统等。

陈世淼 男,1997 年生于河南南乐,2020 年获硕士学位,现为博士研究生,主要研究方向为卫星导航欺骗干扰检测技术。

付琦玮 女,1998 年生于天津,2021 年获学士学位,现为硕士研究生,主要研究方向为卫星导航抗干扰技术。

毛文轩 男,2000 年生于山西运城,2022 年获学士学位,现为硕博连读研究生,主要研究方向为卫星导航欺骗干扰检测技术。

雷拓峰 男,1998 年生于陕西西安,2019 年获学士学位,现为硕博连读研究生,主要研究方向为卫星信号处理和信道编码技术。

宋 鑫 男,1995 年生于山西临汾,2022 年获博士学位,现为助理研究员,主要研究方向为卫星信号处理和高动态载波同步。