Website：ycyk.brit.com.cn

卫星导航接收机欺骗攻击及防护综述

石善斌[1]，赵丙风[2]
（1 北京跟踪与通信技术研究所 北京 100094；
2 中国电子科技集团公司第五十四研究所 石家庄 050081）

摘要：本文主要研究卫星导航欺骗干扰技术与欺骗防护技术，首先介绍欺骗干扰的生成方式、欺骗干扰实施策略与播发策略，并从欺骗威胁、实现难度、防护难度等多方面给出现有欺骗技术的对比分析。其次从信号体制、终端处理技术、辅助信息校验技术等三个层面介绍现有欺骗防护技术，并从欺骗适应性、实现需求、实现难度、实现效果等几方面给出防护技术对比分析。在此基础上，研究在面对不同欺骗攻击时接收机的欺骗防护框架，对于评估导航接收机的防护能力有借鉴意义。

关键词：卫星导航；接收机；欺骗干扰；欺骗防护技术；欺骗防护框架
中图分类号：TN973; TN965 **文献标志码：**A **文章编号：**2095-1000(2024)02-0075-08
DOI：10.12347/j.ycyk.20230808001
引用格式：石善斌，赵丙风. 卫星导航接收机欺骗攻击及防护综述[J]. 遥测遥控，2024，45(2)：75–82.

Analysis on Spoofing Attack and Anti-spoofing Framework of GNSS Receiver

SHI Shanbin[1], ZHAO Bingfeng[2]
（1. Beijing Institute of Tracking and Telecommunications Technology, Beijing 100094, China;
2. 54th Research Institute of China Electronics Technology Group Corporation, Shijiazhuang 050081, China）

Abstract: This paper focuses on the spoofing and anti-spoofing technology and protection of GNSS receiver. Firstly, the signal generation and spoofing implementation strategies are introduced, and several aspects such as spoofing threat implementation difficulty and protection difficulty are compared and analyzed. Secondly, an analysis of anti-spoofing technologies is discussed from three aspects: signal system, receiver signal processing technology and auxiliary information verification technology. A comparative analysis of anti-spoofing technologies is provided from the aspects of spoofing adaptability, implementation requirements, implementation difficulty, and effectiveness. Based on these, the anti-spoofing framework of GNSS receiver is proposed to deal with different spoofing attacks, which has significant reference for evaluating the spoofing procetion ability of GNSS receivers.

Keywords: GNSS; Receiver; Spoofing; Anti-spoofing technology; Anti-spoofing framework
Citation: SHI Shanbin, ZHAO Bingfeng. Analysis on Spoofing Attack and Anti-spoofing Framework of GNSS Receiver[J]. Journal of Telemetry, Tracking and Command, 2024, 45(2): 75–82.

0 引言

卫星导航以其高精度、全天时、全天候、大范围、低成本的特点，已成为国家经济社会发展不可或缺的重要手段，对资源利用、环境保护、公共服务等方面的发展产生了深刻影响。随着导航系统应用范围的不断扩展，导航信号容易受到干扰的问题也逐渐暴露，卫星导航抗干扰的重要性日益凸显。

对卫星导航系统的干扰主要分为压制干扰与欺骗干扰两类。压制干扰是指干扰信号的强度远高于导航信号强度，导致接收机性能降低或者失去正常工作能力的干扰方式。欺骗干扰是指发射与真实信号高度相似的虚假导航信号或转发真实信号，以欺骗或诱导接收设备，使其忽略正确卫星信号而在虚假信号下工作的干扰方式。欺骗干扰功率需求低，隐蔽性好，具有较强的生存能力。从某种程度上来讲，欺骗干扰带来的危害比压制干扰更为严重。欺骗干扰通过产生虚假电文或增加信号延迟产生虚假信息，使接收机无意识的锁

收稿日期：2023-08-08；修回日期：2023-11-20

定在欺骗信号上，得到错误的导航定位结果，达到干扰接收机的目的。

国外关于欺骗干扰的关注与研究起步较早[1]，并在加密认证技术[2,3]、接收机信号处理技术[4−9]、外来辅助信息检测技术[10,11]等多种抗欺骗技术研究方面取得了成果。国内对欺骗干扰的研究起步于2005 年[12]，此后清华大学[13]、北京航空航天大学[14−16]、国防科技大学[17−19]、电子科技大学[20,21]等高校以及其他科研院所[21−29]先后开展相关研究并取得了一定的进展。欺骗与抗欺骗技术是矛与盾的关系，可以应对所有欺骗的抗欺骗方法是不存在的，而能欺骗所有导航设备的欺骗技术也是不存在的，两者都必须有一定的前提条件。

本文基于目前欺骗及其防护技术研究进展，梳理了不同欺骗方法及其实施策略、欺骗防护技术；在此基础上，尝试根据应对欺骗攻击的能力，确定接收机欺骗防护等级，并针对卫星导航系统现有各类军、民用户所存在的欺骗安全隐患，提出相应的欺骗防护措施与建议。

1 欺骗干扰技术分析

1.1 信号生成方式

根据干扰信号生成方式，欺骗式干扰分为生成式欺骗干扰与转发式欺骗干扰。

1.1.1 生成式欺骗

生成式欺骗干扰直接将扩频码、射频载波和导航数据比特等信息复制，改变部分信息产生欺骗信号，欺骗信号与真实信号近似，使目标接收机受欺骗信号影响得到错误的结果，达到欺骗目标接收机的目的，实现框架如图 1(a)所示。

生成式欺骗有两种[25]：1)直接生成式欺骗，由导航信号模拟源直接产生欺骗信号，因与真实卫星信号不同步，易被识别；2)存储生成式欺骗，欺骗源根据接收真实信号的先验信息，辅以雷达等其他手段获得目标接收机的位置，同步产生精准的欺骗信号，在实现上更复杂，欺骗能力也更强。

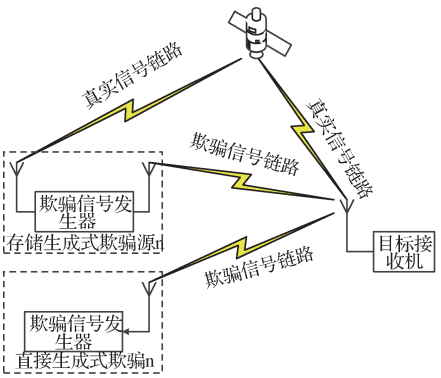
生成式欺骗要掌握伪码结构、导航电文等全部信息，因此生成式欺骗仅限于公开信号。使欺骗信号与真实信号保持尽可能多的相似信号参数，是生成式欺骗干扰实施成功的必要条件，主要包括码相位、多普勒频率、信号强度、导航电文、载波相位等。

1.1.2 转发式欺骗

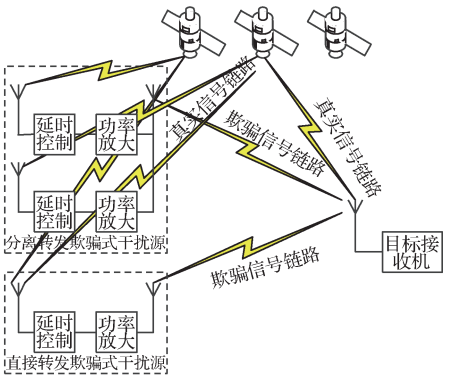
转发式欺骗是在接收到真实的信号后，添加特定的延时[18]，进行适当的功率放大[15]，选择全部或者部分卫星的信号[14],向目标干扰区域内转发，以达到欺骗目标接收机的目的，如图 1(b)所示。

转发式欺骗干扰分为两种[19]：① 直接转发式欺骗，对真实卫星信号进行接收、放大后直接通过发射天线辐射出去，不添加选择性延迟，实现简单；② 分离转发式欺骗干扰，即将接收的真实信号进行分离，对不同卫星信号添加合理的延时控制，以形成伪星座来实施欺骗干扰。

转发式欺骗干扰的优势是无需掌握信号伪码、信号结构，从而对授权和公开信号均适用。转发式欺骗的硬件方案，包括前端和后端两部分，前端实现真实卫星信号的接收、延时和放大，后端完成对转发信号的发射，可采用空域隔离的方法避免信号发射端对接收端的干扰。转发式欺骗成功的关键是添加合理的转发时延与功率放大。



（a）生成式欺骗干扰
（a）Generative deception jamming



（b）转发式欺骗干扰
（b）Repeater deception jamming

图 1 欺骗原理框图

Fig. 1 Spoofing schematic diagram

1.2　干扰策略分析

1.2.1　干扰实施策略

将欺骗信号注入到目标接收机的策略有两种[4,19,20]：入侵式和牵引式。入侵式指在目标接收机的捕获阶段实施欺骗信号的直接侵入；牵引式指在目标接收机跟踪阶段实施欺骗信号的环路牵引式侵入。

入侵式欺骗有直接入侵与先压制后入侵两种。直接入侵需要在目标开机捕获前完成信号发射才能有效实施欺骗，该方法可行性较差。先压制后入侵则先通过压制干扰阻塞目标对于真实信号的接收状态，同时播发欺骗信号，由于欺骗信号功率高于真实信号，欺骗信号就会在重捕中入侵目标接收机。

牵引式欺骗则避免了压制式干扰导致的目标接收机失锁现象，通过跟踪牵引实现信号的诱偏。牵引式欺骗通过产生与真实信号伪码相位存在相对滑动且信号功率稍高的欺骗信号，从而在伪码相对运动过程中自动实现相位匹配并通过其功率优势牵引目标接收机。

1.2.2 干扰播发策略

依据干扰机平台数和干扰机通道数不同实现不同的欺骗效果。一是单站单场景欺骗，设备形态最简单，可快速布站，实现扰乱特定区域目标的定位结果[27]；二是单站多场景欺骗，通过设计欺骗场景实现对目标的轨迹引导式欺骗，目标接收机按照场景设计轨迹运动[16]；三是多站独立欺骗，多个转发式干扰站独立工作，实现对区域目标的定位扰乱的欺骗效果；四是多站组网欺骗，多个天线所播发的欺骗干扰信号可通过组网的方式形成一个共同的欺骗场景[4]。

单站播发欺骗使用一个发射天线播发或转发欺骗信号，实现复杂度低，但因欺骗信号来自同一方向，易被检测识别，失去欺骗效果；多站播发的欺骗，增加了目标接收机的检测难度，也增加了欺骗设备实现难度，尤其是多站组网欺骗实施代价极大。

1.3　欺骗技术比较

针对文献中研究较多的几种欺骗技术，表1简要从欺骗的生成方式、欺骗能力、实施策略、实施限制、欺骗威胁、实现难度、防护难度等方面给出了常见欺骗技术的对比。

目前，对于欺骗研究主要集中于增加欺骗威胁和提升防护难度两个方面，由表1可知，欺骗威

表1　欺骗干扰技术对比

Table 1　Comparison of spoofing technologies

欺骗技术		欺骗能力	实施策略	实施限制	欺骗威胁	实现难度	防护难度
单站单场景	直接生成式	位置与时间可设置，面向区域目标，干扰解算结果	入侵式引导式	与真实信号不同步，易造成目标解算结果跳变	中	低	中
	直接转发式	可欺骗授权信号接收机，干扰一定区域内的目标定位结果	入侵式	欺骗控制不灵活，需要增大欺骗信号功率，仅能使用入侵式实施欺骗，引入信号延时	低	低	低
单站多场景	存储生成式	信号与真实信号更接近，攻击隐秘性强，可实现区域特定目标轨迹引导	入侵式引导式	单天线发射隐藏性不足，易被阵列天线检测识别，技术门槛高，硬件复杂度较高	高	高	高
	分离转发式	通过合理延时控制、选星控制、功率控制实现对特定授权目标的轨迹引导	入侵式	需要分离卫星信号，单天线发射易被阵列天线检测识别，通道时延控制复杂	中	中	中
多站独立	分离转发式	多发射天线增加隐秘性，对区域目标实现定位扰乱，多站增加了干扰的鲁棒性	入侵式	欺骗控制不灵活，需要增大欺骗信号功率，仅能使用入侵式实施欺骗，引入信号延时	高	中	中
多站组网	存储生成式	信号与真实信号更接近，攻击隐秘性强，可实现区域特定目标轨迹引导，实现对阵列天线接收机的干扰	入侵式引导式	设备实现复杂度极高，仅针对特定目标	高	极高	高
	分离转发式	可通过合理的延时控制及选择实现授权信号的轨迹引导，实现对阵列天线目标接收机的干扰	入侵式	设备实现复杂度极高，仅针对特定目标	高	极高	高

胁和防护难度高的欺骗技术实施难度一般也高，对目标接收机带来的威胁也更大。

2 欺骗防护技术分析

2.1 防护技术介绍

2.1.1 信号体制

信号体制抗欺骗干扰方法包括电文加密与扩频伪码加密。利用加密信息无法被伪造的特性，对导航伪码或卫星播发的导航电文进行加密实现欺骗防护，是对抗生成式欺骗干扰最有力的手段[2]。

对所有电文加密或对伪码加密，需要修改信号体制，代价过高。此外可利用导航电文的预留信息位实现部分电文加密[3]，但现有导航信号的电文数据率低、预留电文空间小，限制了该方法的应用。

2.1.2 终端处理技术

终端处理技术的欺骗防护手段可以分为天线处理技术、基带处理技术以及信息处理技术。

1. 天线处理技术

① 针对真实信号与欺骗信号来向不同，利用空域滤波实现欺骗消除，适用于干扰信号功率高于底噪的欺骗场景[21]。

② 通过天线间载波相位差进行到达角检测，适用于单站发射的欺骗检测,无需修改接收机的信号处理算法[5]，还可通过载波相位双差算法检测欺骗干扰，再利用载波相位双差、子空间投影和波束形成理论抑制干扰信号[28]。

③ 合成孔径天线阵检测方法，需要在天线运动过程中对所有的真实与欺骗信号同时进行捕获和跟踪处理，并将所有跟踪结果进行两两组合检测欺骗信号[6]，该方法需要修改接收机信号处理算法，并且实现复杂度明显提高，使得该技术的实用化受到了限制。

④ 通过对欺骗信号的重构实现欺骗干扰消除[7]，利用阵列天线或者多接收机联合实现欺骗检测，接收机根据接收信号估计欺骗信号参数，继而重构欺骗信号，在中频信号中消除重构的欺骗信号，得到仅包含真实信号与噪声的中频信号。

⑤ 欺骗信号源定位技术，利用接收机组网，在网络节点内的不同位置测量得到真实信号条件下和欺骗干扰条件下的接收机钟差，得到欺骗干扰源到达不同位置接收机的距离差，结合双曲线交叉定位原理确定欺骗干扰位置，将其摧毁而实现根源性的干扰消除[9]。

2. 基带处理技术

基于基带信号处理技术的抗欺骗方法是国内外学者研究的热点，主要有以下几种方法：

① 通过多相关检测算法实现欺骗信号的检测与识别。信号捕获是时频二维的相关搜索过程，在信号捕获过程中检测到多个相关峰，则一定存在欺骗干扰。

② 斜率检测技术[8]。作为多相关峰检测的补充，利用相关斜率检测实现欺骗信号的检测。

③ 功率检测技术。对于陆基的欺骗干扰来说，欺骗信号 CN0 会因传播距离变化而显著波动，故可通过 AGC 的异常调整实现欺骗检测[4]；依据卫星的周期性，特定位置的真实信号 CN0 可作为先验信息，欺骗信号一般高于真实信号，当接收 CN0 与先验 CN0 之差超过阈值时，则可能存在欺骗信号[23]。

④ 伪距一致性检测方法。同一卫星不同频点信号的伪距观测值接近，其伪距差值超过门限后可判定当前卫星存在欺骗[25]；两台接收机进行伪距双差，消除大气传播误差后，若结果大于阈值，则当前卫星为欺骗信号[17]。

⑤ 多普勒检测方法。当特定卫星多普勒观测量出现大的波动，或者信号短暂失锁重捕后多普勒观测量出现跳变时，则当前环境存在欺骗干扰。

3. 信息处理技术

① 解算结果一致性检测方法[25]。在接收机出现信号未失锁而解算结果有跳变，或信号短暂失锁重定位后解算结果出现跳变，亦或解算得到的位置信息、速度信息、加速度信息与定位间隔不匹配，则当前存在欺骗干扰。

② 信息合理性检测方法[25]。利用储存的正确电文解算卫星历书信息，预测可见星，对于接收的不可见星可以判定为欺骗信号；基于接收的卫星星历、钟差、健康状态等信息，对导航电文进行合理的预测，与当前接收电文信息进行对比确认，如有差异，则当前存在欺骗干扰。

③ RAIM 检测算法。利用欺骗信号对解算结果的影响把受欺骗的卫星检测并剔除[24]；基于时域差分将载波多普勒检测与 RAIM 算法结合进行欺骗干扰识别[22]，以提高 RAIM 在欺骗干扰检测领域的适应范围；同时可利用真实信号的冗余度，采用

遍历检测的方法，识别并剔除多个欺骗干扰信号[13]。

2.1.3　辅助信息校验技术

基于辅助信息检测技术的抗干扰方法，引入外部辅助传感器。如惯性测量单元 IMU、高精度芯片级原子钟 CSAC、里程计、气压计等，用于提供辅助位置和时间信息，通过监测多个GNSS观测值和测量值的相互关系的方法，可以对欺骗攻击进行有效检测[10]。外部辅助传感器具备全自主导航能力，不受欺骗干扰的影响，这是将其导航输出作为参考用于欺骗检测的基础。同时，还可以利用多径估计延迟锁定环路来配合INS/GNSS组合导航环路模式，实现对引导式欺骗干扰的识别[26]。

2.2　防护技术比较

近30年间国内外对卫星导航信号的抗欺骗技术开展了大量的研究，表2简要给出了常用抗欺骗技术的适应性、实现需求、实现难度、实现效果的对比。

表2　欺骗防护技术对比

Table 2　Comparison of anti-spoofing technologies

防护技术			对欺骗的适应性	实现需求	实现难度	实现效果
信号体制		信息加密	针对公开信号欺骗干扰	修改信号体制	高	好
		伪码加密	针对公开信号欺骗干扰	修改信号体制	高	好
终端处理技术	天线处理技术	空域滤波	欺骗信号功率高于背景噪声	使用阵列天线	中	中
		到达角检测/载波相位双差	单站播发欺骗源	阵列天线或多天线接收机	高	好
		合成孔径天线阵	单站播发欺骗源	多通道测量	高	好
		欺骗信号重构消除	真实信号可识别未被淹没	阵列天线配合多通道接收机，算法估计欺骗信号参数	极高	好
		欺骗信号源定位技术	单站欺骗信号或多站组网发射欺骗信号	多接收机组网，算法估计多欺骗信号时延	极高	好
	基带处理技术	多相关峰检测	转发式欺骗	实现多相关峰搜索	低	好
			生成式欺骗	实现多相关峰搜索	低	中
		斜率检测	欺骗信号延迟小于1.5码片	增加相关器	低	中
		CN0检测技术	欺骗信号功率高于真实信号	多跟踪通道	低	好
		伪距一致性	欺骗信号造成伪距不一致	增加伪距校验算法	低	好
		多普勒检测	欺骗信号造成多普勒跳变或者载波与伪码多普勒不一致	增加多普勒校验算法	低	好
	信息处理技术	解算结果一致性	欺骗信号导致解算结果跳变	增加PVT解算后检验算法	低	中
		信息合理性检测	电文未加密，欺骗信号修改了电文比特，或播发了不可见卫星	增加电文校验算法	低	中
		RAIM检测	欺骗信号造成的解算残差较大，仅有单个欺骗信号	——	低	好
			欺骗信号造成的解算残差较大，有多个欺骗信号	增加多星RAIM检测算法	中	好
辅助信息校验			——	需要增加额外的辅助信息来源，增加对应的检测算法	高	好

3　接收机欺骗防护体系

卫星导航欺骗防护问题是国内外的研究热点。各类学者从不同的层面阐述了欺骗干扰的检测、识别等方法，形成诸多技术成果。下面从抗欺骗防护能力的角度，给出抗欺骗防护框架。

3.1　欺骗攻击分类

参考经典的欺骗攻击分类[1]，并结合当前公开文献中研究涉及的欺骗模式与种类[29]，表3给出了欺骗攻击分类。

表3中从上到下欺骗实施复杂度依次递增，但欺骗威胁也依次变大。从欺骗实施目的看，无非特定与区域目标的结果扰乱、特定目标的轨迹引导两种，欺骗方可根据欺骗目的与实施难度综合考虑选择合适欺骗技术以成功实施欺骗。其中，简单模拟欺骗、简单转发欺骗因实施简单的特点，

表 3 欺骗攻击分类

Table 3 Classification of spoofing attack

分类	欺骗描述	典型欺骗技术
I类 简单模拟欺骗	基于已有信号模拟源技术，以较小的代价实现对扰乱区域目标或者特定目标的定位结果扰乱，仅针对公开信号，一般采用入侵式实施欺骗，欺骗设备成本低，实现难度低，欺骗源架设迅速，防护难度低	单站单场景直接生成式欺骗
II类 简单转发欺骗	基于已有信号转发器，对所有卫星信号施加相同的延迟，目标接收机解算结果为转发器接收天线布站位置，可欺骗公开信号和授权信号，实现简单，设备成本低，欺骗源架设迅速，防护难度低	单站单场景直接转发式欺骗
III类 单天线收发欺骗	以目标接收无感的方式实现对特定目标的轨迹引导，或对区域目标的扰乱，需要获取目标接收机相位中心的相对位置与相对运动信息，仅针对公开信号，欺骗设备成本高，实现技术难度高，隐秘性强，防护难度高	单站多场景存储生成式欺骗
IV类 多天线收发欺骗	在单天线收发欺骗的基础上增加多站组网发射，形成包含欺骗信号的伪星座，增加目标接收机防护难度，仅针对公开信号，欺骗设备成本高，实现难度极高，防护难度高	多站组网存储生成式欺骗
V类 多通道转发欺骗	以多处理通道实现对接收卫星信号的分离，对不同卫星施加不同延时控制，以单天线发送模式、多天线独立发送模式或多天线组网发送模式完成信号转发，实现对区域目标的结果扰乱或对特定目标的轨迹引导，可欺骗公开信号和授权信号，欺骗实现复杂，设备成本高，欺骗防护难度较高	单站多场景分离转发式欺骗 多站独立分离转发式欺骗 多站组网分离转发式欺骗

研究较少；单天线收发欺骗、多通道转发欺骗因其欺骗威胁大，实施难度相对较低，成为目前国内外学者研究的重点；多天线收发欺骗因其仅能针对公开信号故暂时未有大量研究。

3.2 欺骗防护框架

卫星导航的目的是获取可信的PVT解算结果，一般接收机对于当前是否存在欺骗、存在何种形式欺骗是没有先验信息的，需要接收机采取必要的技术手段实现对当前环境中欺骗信号的检测与识别，以保障其解算结果可信度。不同平台使用的卫星导航接收机硬件状态不尽相同，可利用的欺骗防护技术也不尽相同，依据欺骗防护可以达到的结果，表4给出几种不同平台下接收机可用的欺骗防护技术。

由表4可以看出：① 无论何种导航接收设备，基于接收机自身的信息处理技术是进行欺骗检测并给出告警信息的有效手段，基带信号处理技术是识别欺骗并给出正确解算结果的重要手段；

表 4 欺骗防护策略

Table 4 Classification of spoofing attack

可用技术描述			防护结果			
			A 不能告警 结果不正确	B 能够告警 结果不正确	C 能够告警 结果正确	D 能够告警结果正确 能够定位欺骗源
应用平台	I	单天线接收设备	未采取任何防护 信息处理技术	信息处理技术 辅助信息校验	信息加密 伪码加密 合成孔径天线阵 基带处理技术 RAIM检测技术	——
	II	阵列天线接收设备	未采取任何防护 信息处理技术	到达角检测技术 信息处理技术 辅助信息校验	信息加密 伪码加密 空域滤波 欺骗重构消除 基带处理技术 RAIM检测技术	——
	III	组网使用接收设备	未采取任何防护 信息处理技术	信息处理技术 辅助信息校验	信息加密 伪码加密 基带处理技术 RAIM检测技术	欺骗信号源定位技术

② 利用接收自身硬件增加天线处理技术、辅助信息检测技术、多接收机组网等是提高欺骗防护能力的有效手段；③ 对于以公开信号为目标的多天线收发欺骗，常规处理技术多数失效，通过信号体制加密使其退化为转发式欺骗是防护该类型欺骗的关键。

因为接收机本身并不能保证解算结果的正确性，所以对于接收机的防护等级需要通过考核来认证。对于智能手机、智能穿戴、共享单车等大众消费领域应用，无需考核或者根据需求通过B级即可；对于通信基站、电力监测、铁路列车控制、工程测绘、海事应用等有其他定位手段的行业应用，至少应通过B级欺骗防护等级考核；对于自动驾驶、车联网、民航进近、金融医疗等对时间、速度、位置信息比较敏感的行业应用，应要求设备通过C级欺骗防护等级考核；对于军事应用，应要求设备至少通过C级欺骗防护等级考核，特殊情况可要求达到D级欺骗防护能力。

4 结束语

本文首先梳理当前欺骗干扰实施的信号生成方式、干扰实施策略和干扰实施条件分析，在此基础上，从信号体制、终端处理技术、辅助信息校验技术几方面简要梳理了欺骗防护技术，对常用欺骗防护技术做了对比分析，根据欺骗干扰的能力给出了欺骗防护等级划分与建议。最后给出了欺骗防护框架，对于后续评估导航接收终端的欺骗防护能力有借鉴意义。

参考文献

[1] HUMPHREYS T E, LEDVINA B M, PSIAKI M L, et al. Assesing the spoofing threat: Development of a portable GPS civilian spoofer[C]//Proceedings of the 21th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+2008), 2008: 2314-2325.

[2] WESSON K D, ROTHLISBERGER M P, HUMPHREYS T E. Practical cryptographic civil GPS signal authentication[J]. Navigation, 2012, 59(3): 177-193.

[3] WILDE W D, SLEEWAEGEN J M, BOUGARD B, et al. Authentication by polarization: a powerful anti-Spoofing Method[C]//Proceedings of the 31th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+2018), 2018: 3643-3658.

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

[5] MONTGOMERY P Y, HUMPHREYS T E, LEDVINA B M. A multi-antenna defense: Receiver-autonomous GPS spoofing detection[J]. Inside GNSS, 2009, 4(2): 40-46.

[6] NIELSEN J, BROUMANDAN A, LACHAPELLE G. GNSS spoofing detection for single antenna handheld receivers[J]. Navigation, 2012, 58(4): 335-344.

[7] STENBERG N, AXELL E, RANRAKOKKO J, et al. GNSS spoofing mitigation using multiple receivers[C]//2020 IEEE/ION Position, Location and Navigation Symposium (PLANS), 2020: 555-565.

[8] WESSON K D, SHEPARD D P, BHATTI J A, et al. An evaluation of the vestigial signal defense for civil GPS anti-spoofing[C]//Proceedings of the 24th International Technical Meeting of the Satellite Division of The Institute of Navigation, 2011.

[9] BROUMANDAN A, JAFARNIA-JAHROMI A, DANESHMAND A, et al. A network-based GNSS structural interference detection, classification and source localization [C]//Proceedings of the 2015 International Technical Meeting of the Institute of Navigation, 2015: 3358-3369.

[10] SEMANJSKI A, MULS A, SEMANJSKI I. Use and validation of supervised machine learning approach for detection of GNSS signal spoofing[C]//2019 International Conference on Localization and GNSS (ICL-GNSS), 2019: 1-6.

[11] KUJUR B, KHANAFSEH S, PERVAN B. Detecting GNSS spoofing of ADS-B equipped aircraft using INS [C]//2020 IEEE/ION Position, Location and Navigation Symposium (PLANS), 2020: 548-554.

[12] 杨景曙, 曾芳玲, 盛琥, 等. 通过区域映射实现诱导的GPS 干扰系统[J]. 电子学报, 2005, 33(6): 1036-1038.
YANG J S, ZENG F L, SHENG H, et al. A jamming system through section mapping for GPS navigation[J]. Acta Electronica Sinica, 2005, 33(6): 1036-1038.

[13] LI J F, LI H, PENG C X, et al. Research on the random traversal RAIM method for anti-spoofing applications [C]//Proceedings of the 10th China Satellite Navigation Conference, 2019: 593-605.

[14] 史鹏亮, 靳文鑫, 吴舜晓. 实施转发式GNSS欺骗干扰的选星方法研究[J]. 北京理工大学学报, 2019, 39(5): 524-531.
SHI P L, JIN W X, WU S X. Research on satellite selection algorithm of gnss repeater deception jamming[J]. Transactions of Beijing Institute of Technology, 2019,

39(5): 524-531.

[15] 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, 4(2): 79-89.
SHI P L, WANG X Y, XUE R. Research on power control strategy of gnss repeater deception jamming[J]. Modern Navigation, 2021, 4(2): 79-89.

[16] 史鹏亮, 王晓宇, 薛瑞 . 无人机位置欺骗诱导策略[J]. 国防科技大学学报, 2021, 43(2): 40-46.
SHI P L, WANG X Y, XUE R. Induction strategy for unmanned aerial vehicle position spoofing[J]. Journal of National University of Defense Technology, 2021, 43(2): 40-46.

[17] 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 against repeater deception jamming detection algorithm based on pseudo-range information[J]. Systems Engineering and Electronics, 2017, 39(11): 2393-2398.

[18] 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.
HANG L, LYU Z C, WANG F X. Spoofing pattern research on GNSS receivers[J]. Journal of Astronautics. 2012, 33(7): 884-890.

[19] 庞晶, 倪少杰, 聂俊伟, 等 . GNSS 欺骗干扰技术研究[J]. 火力与指挥控制, 2016, 41(7): 1-4, 9.
PANG J, NI S J, NIE J W, et al. An overview to GNSS spoofing technologies[J]. Fire Control & Command Control, 2016, 41(7): 1-4,9.

[20] 陈碧, 郭承军 . GPS 欺骗干扰过程研究[J]. 科技通报, 2016, 32(10): 165-169.
CHEN B, GUO C J. Study on GPS spoofing pattern process[J]. Bulletin of Science and Technology, 2016, 32(10): 165-169.

[21] 李亚斌, 郭承军, 田忠 . 基于调零技术的GPS抗欺骗干扰研究[J]. 电光与控制, 2017, 24(1): 37-40.
LI Y B, GUO C J, TIAN Z, et al. Null-steering based anti-spoofing for civilian GPS[J]. Electronics Optics & Control, 2017, 24(1): 37-40.

[22] WEI Y M, LI H, PENG C X, et al. Time domain differential RAIM method for spoofing detection applications [C]//Proceedings of the 10th China Satellite Navigation Conference, 2019: 606-614.

[23] 曹可劲, 彭煊坤, 李豹, 等 . 基于信噪比测量的欺骗干扰检测方法[J]. 计算机测量与控制, 2016, 24(4): 29-32.
CAO K J, PENG X K, LI B, et al. A method of spoofing jamming detection based on SNR measurement[J]. Computer Measurement & Control, 2016, 24(4): 29-32.

[24] HAN S, LUO D S, MENG W X, et al. Antispoofing RAIM for dual-recursion particle filter of GNSS calculation[J]. IEEE Transactions on Aerospace and Electronic Systems, 2016, 52(2): 836-851.

[25] 王璇, 唐斌, 郑冲, 等 . 卫星导航接收机欺骗与反欺骗技术综述[C]//第十二届中国卫星导航年会论文集, 2021: 2-6.

[26] 柯晔, 吕志伟, 周玟龙, 等 . GNSS/INS 紧组合的新息优化抗差估计欺骗检测算法[J]. 中国惯性技术学报, 2022, 30(2): 272-280.
KE Y, LYU Z W, ZHOU W L, et al. Innovation optimal robust estimation spoofing detection algorithm of tightly coupled GNSS/INS integration[J]. Journal of Chinese Inertial Technology, 2022, 30(2): 272-280.

[27] 胡彦逢, 边少锋, 纪兵, 等 . 卫星导航对抗之欺骗与反欺骗技术探讨[C]//第七届中国卫星导航学术年会论文集, 2016.

[28] 崔建华, 程乃平, 倪淑燕 . 阵列天线抑制欺骗式导航干扰信号方法研究[J]. 电子学报, 2018, 6(2): 365-371.
CUI J H, CHENG N P, NI S Y. Research on spoofing suppressing method using antenna array for navigation signal[J]. Acta Electronica Sinica, 2018, 6(2): 365-371.

[29] 刘洋 . 惯性/卫星组合导航欺骗检测关键技术研究[D]. 西安: 西北工业大学, 2019.

[作者简介]

石善斌　1979年生，博士，助理研究员。

赵丙凤　1988年生，硕士，高级工程师。

(本文编辑：潘三英)