

基于“OODA 环”优化的卫星导航定位安全与 对抗应用研究

吴 鹏, 张启福, 魏鹏飞, 姚 远, 叶 菁
(甘肃酒泉十四支局 甘肃 735018)

摘要: 卫星导航定位设备的“生存”环境日益复杂、严峻, 各类电子对抗、干扰欺骗十分激烈, 人为干扰已成为卫星导航定位安全与对抗的重点。针对传统手段无法有效应对干扰复杂性、全面性、系统性的不足, 本文在分析“OODA 环”理论和实践转化的基础上, 结合复杂环境下“干扰-抗干扰”的整体对抗过程, 优化“OODA 环”运行, 将其与卫星导航定位安全与对抗应用进行耦合, 提出基于“环境感知-筛选隔离-检测识别-效能评估-策略规划-对抗反制-回访反馈-再感知”的卫星导航定位安全与对抗不定向循环链路, 并对拓展、映射的七个环节及关键技术进行分析、论证。通过引入“循环”和“不定向”两个概念, 不仅实现了周期性外循环和部分环节内循环的嵌套迭代和导向性传输的运行机制; 而且优化了内循环的自由度, 使得各环节互联且独立、循环但不定向, 有效增强了卫星导航定位安全与对抗的鲁棒性。本文的设计思路可加快实现循环链路的动态闭环, 提高对抗的整体效能, 在实践应用和技术论证中具有一定的参考价值。

关键词: 卫星导航定位; OODA 环; 安全与对抗; 压制式; 欺骗式; 不定向循环链路; 内循环

中图分类号: TN967.1 **文献标志码:** A **文章编号:** 2095-1000(2024)01-0091-09

DOI: 10.12347/j.ycyk.20230718001

引用格式: 吴鹏, 张启福, 魏鹏飞, 等. 基于“OODA 环”优化的卫星导航定位安全与对抗应用研究[J]. 遥测遥控, 2024, 45(1): 91-99.

Research about Application of OODA Ring Optimization in Satellite Navigation and Positioning Security and Countermeasures

WU Peng, ZHANG Qifu, WEI Pengfei, YAO Yuan, YE Jing
(Gansu Jiuquan 14th Branch, Gansu 735018, China)

Abstract: The living environment of satellite navigation and positioning equipment is increasingly complex and severe, all kinds of electronic countermeasures, interference and deception are very fierce, and man-made interference has become the focus of satellite navigation and positioning security and confrontation. In view of the shortcomings of traditional means to effectively deal with the complexity, comprehensiveness and systematization of interference, the paper, based on the analysis of OODA ring theory and practice transformation, combined with the overall counter process of interference and anti-interference in complex environment, optimized operation, coupled with satellite navigation and positioning security and counter, innovative satellite navigation and positioning security and counter non-directional circular link which is based on environment awareness, screening isolation, detection and recognition, performance evaluation, strategic planning, counter attack-return visit feedback, re-perception. The seven links of expansion and mapping are analyzed and demonstrated. By introducing the concepts of loop and undirected, the operation mechanism of nested iteration and guided transmission of cyclic outer loop and loop in link is not only realized, but also the freedom of the inner loop is optimized, so that links are interconnected and independent, and loop but not directed, effectively enhance the safety of satellite navigation and positioning and the robustness of confrontation. The design idea of the paper can accelerate the realization of the dynamic closed-loop loop of cyclic link, improve the overall efficiency of countermeasure, and has certain reference value in practical application and technology demonstration.

Keywords: Satellite navigation and positioning; OODA ring; Security and confrontation; Blanket jamming; Deception jamming; Non-directional circular link; Inner loop

Citation: WU Peng, ZHANG Qifu, WEI Pengfei, et al. Research about Application of OODA Ring Optimization in Satellite Navigation and Positioning Security and Countermeasures[J]. Journal of Telemetry, Tracking and Command, 2024, 45(1): 91-99.

0 引言

随着全球导航卫星系统的不断发展, 卫星导航定位作为一项革新技术, 已深度融入交通、航空航天、电力、金融等诸多领域, 极大地影响着人类的生产、生活。尤其是在一些高精尖行业的应用不可或缺, 不仅可为各类应用系统和平台提供精确的导航、定位、授时等服务, 而且可有效提升系统控制、多平台协同能力, 展现了“国之重器”的重要作用。

有发展就可能出现挑战, 伴随着导航对抗、授时干扰等理念的提出, 卫星导航定位的安全与对抗问题已成为各类应用的核心问题之一。近年来, 卫星导航定位设备被干扰、欺骗的情况比比皆是, 极大降低了导航定位性能。2017年, 20多艘在黑海作业的船只受到大规模诱骗攻击, 船载导航设备显示定位正常, 但实际位置偏差25海里(约为46 300米)^[1]。据报道, 依靠卫星导航的自动驾驶车辆的安全性也受到威胁。某地正常行驶的特斯拉Model3被坐标欺骗后, 直接失控, 在高速路上急刹车、急转弯。为此, 许多学者竞相开展安全与对抗方面的研究, 王旭旭研究了欺骗干扰检测、抑制技术, 提出基于信噪比和相对距离的检测方法, 以及正交干扰子空间的抑制方法^[2]。尹继东开展抗干扰技术分析, 对比了最小均方、功率倒置等自适应抗干扰算法的性能^[3]。姚旺对有源压制干扰、箔条干扰、欺骗干扰等机理和特性进行了研究, 从频域、空域提出相应对抗措施^[4]。

传统卫星导航定位的对抗研究注重在某项具体的干扰技术、检测方法、抗干扰算法等方面进行。然而在当前复杂环境的应用背景下, 卫星导航定位设备面临着全方位的安全威胁, 干扰的复杂性、全面性、系统性更加突出, 这就不能只关注于某项具体技术, 而要实现多个单项技术或系统的连贯和融合, 通过技术延伸和能量传递, 发挥卫星导航定位安全与对抗的整体效能, 以此形成一些符合实际的模式或机制。可见, 卫星导航定位安全与对抗从本质上来讲就是多系统叠加的机制对抗, 从环境感知、发现干扰、检测识别, 到制定策略、消除干扰的过程, 这是一个多个分

系统之间耦合连贯的机制。基于“OODA环”的应用, 立足于“观测-判断-决策-行动”的动态环路, 很好地契合了卫星导航定位安全与对抗的运行过程, 能更好地在保持各分系统独立性的基础上, 又不失连贯地形成闭环回路; 同时, 实现各分系统之间的能量传导和循环迭代, 涌现出超出“线性叠加”的“机制运行”能力。因此, 开展“OODA环”与卫星导航定位安全与对抗的耦合应用具有一定的价值。

1 “OODA环”理论与实践分析

“OODA环”理论是二十世纪七十年代由博伊德提出的一种闭环模型, 即观察(Observe)、判断(Orient)、决策(Decide)、行动(Act)等四个环节的循环^[5,6]。

“OODA环”的设计之初就是在对抗情况下, 通过观察目标、判断对手行为, 到准确评估, 并做出合理的决定, 以快速完成行动, 而行动后又回到最初的观察, 进而形成一个循环。

1.1 “OODA环”分析

“OODA环”的发展经历了从理念提出到实践验证再到拓展推广的过程。在实际应用中, “OODA环”的四个环节衔接运行、导向传输、融合互联, 如图1所示。

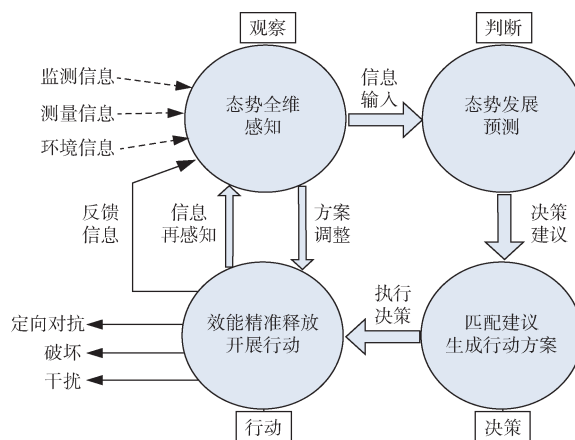


图1 “OODA环”循环运行示意图
Fig. 1 OODA loop operation diagram

① 观察环

属于“OODA环”的初始环节, 也是下一个

环路的溯源环节。通过专用传感器和技术对环境进行全维感知。采取监测、测量等方式,获取时域、频域、空域内各类系统和平台,以及非合作目标等环境因素产生的信息,并进行样本累积。依托大数据分析、处理技术,将获取的多维、多源、复杂数据进行快速整合,并充分挖掘有效信息,利用数据模型融合、数字化态势再生,为形势预判提供实时、可靠、准确的先验信息。

② 判断环

这一环节是通过对全维感知信息的推理判断,准确研判、评估对抗态势,并以此预测发展趋势。首先,结合先验信息的特征,通过对信息源的解释、整理和评估,以及威胁因素的分析,将有效信息转换成判断、决策所需支撑信息;其次,将支撑信息与现有数据库、知识库、人工思考及经验等进行全方位比较,形成具备优先级的决策建议。

③ 决策环

决策环是影响“OODA环”的核心因素。决策是在信任和理解判断结果后,综合评估不同优先级的决策建议,并结合自身实际,从中选择一个匹配度高且合理有效的建议,并以此进行推演验证,生成行动方案。同时,将此决策场景存储在决策数据库中,形成先验决策信息,以便在下一“OODA环”决策中进行调用、对比或迭代。

④ 行动环

这是“OODA环”效能精准释放环节。根据生成的行动方案,调配并指导各类对抗设备和技术力量,实现对目标的定向对抗、规避、破坏、干扰等不同对抗行动。同时,结合实时获取的最新观察信息,对态势进行更新,实现行动方案的自适应调整,以满足变化需要。相应的,对决策结果进行验证,若未达到既定效果,需要重新决策,接入新的“OODA环”,指导新的行动。

1.2 “OODA环”实践转化

在当前各类应用系统和平台信息化、智能化的大趋势下,“OODA环”理论得到了很好的完善和发展,其底层逻辑思维可融合在不同的应用场景中,使得各个独立的系统网络化关联在一起,在一定程度上展现了系统机制的运行模式^[7]。

凭借这种系统机制的优势,极大缩短了“OODA环”循环周期且提高了效能。一些学者为此进行了相关技术性论证。王太军提出了利用星

链等低轨星座的大容量、低时延和边缘计算能力,为“OODA环”快速响应提供技术支撑^[8]。孙盛智建立了“OODA环”模型,并评估了整体运行能力^[5]。顾灏冰基于延迟和阻断OODA快速闭环,提出智能博弈、以群制群等策略,开展了系统性对抗^[9]。

由此可见,“OODA环”具有一定的循环迭代、呈机制运行等特点,这与复杂环境下“干扰-抗干扰”的动态对抗过程十分契合。将“OODA环”应用于卫星导航定位安全与对抗中,可实现各类信息平台化感知、流程化传输、网络化循环,以及干扰源自主判断、评估,抗干扰策略自主生成、执行等连贯性过程,形成一个兼顾平台内循环和分系统间外循环的系统机制^[10]。

2 卫星导航定位干扰分析

卫星导航信号本身微弱,导航卫星轨道高度约22 000 km,卫星信号经传输消耗和大气延迟,到达地面功率仅仅约-160 dBW。卫星信号掩盖在自然噪声中,极易受到各类射频辐射的干扰。目前,对于卫星导航定位的干扰,主要有三个层面,从顶层而言就是对星干扰,直接干扰或者摧毁信号源;从中间层而言,就是对地面监控站的干扰,破坏导航电文校正、星地时间同步等;从底层而言,就是卫星接收机干扰,直接影响信号捕获、解调和解算的链路。

相比之下,对于卫星和地面监控站的干扰成本较大、难以实现,而对于接收机的干扰效果明显、易于实施,这就成了“干扰-抗干扰”博弈最为激烈的部分。其中,对于接收机的干扰主要是各类射频辐射,包括自然噪声、传感器射频辐射、人为干扰、电子对抗释能、民用设施辐射等,其中特异的人为干扰最为显著,是需要关注和研究的重点。

2.1 人为干扰的产生和分类

人为干扰是专门设计的,针对卫星导航信号的接收体制、信号结构和数据处理等流程中的薄弱环节而人为制造的指向性攻击,扰乱、破坏、诱导卫星导航定位设备无法定位或者错误定位。

人为干扰可按体制、样式、方式等三层进行分类。在体制上,可分为压制式、欺骗式和混合式干扰等三种^[11];在样式上,压制式干扰可分为窄带干扰和宽带干扰,欺骗式干扰可分为生成式干

扰和转发式干扰;在具体方式上,包括单频连续波干扰、窄带噪声干扰、窄脉冲干扰、噪声调幅干扰、噪声调频干扰、宽带脉冲干扰、宽带梳状谱干扰、线性扫频干扰、单天线生成式干扰、多天线生成式干扰、单源转发式干扰、多源转发式干扰^[12]等。如图 2 所示。

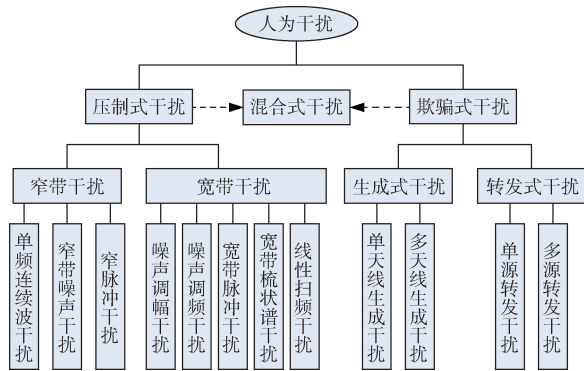


图 2 人为干扰的分类图

Fig.2 Man-made interference classification diagram

2.2 干扰作用机理分析

① 压制式干扰机理

利用大功率发射机,发射与卫星导航信号同频段的干扰信号,降低卫星导航信号信噪比,致使接收机无法捕获、锁定信号,从而丧失定位能力。其中,窄带干扰频谱宽度一般与导航信号带宽相近或者集中在几个较窄的频带上,干扰瞄准中心频点聚能,造成信号载波和码元丢失,无法解调伪码。宽带干扰是针对一定区域内所有卫星信号实施干扰,干扰频带覆盖几个或全部导航信号的频谱宽度,真实信号完全被淹没,导致接收机失锁。

② 欺骗式干扰机理

针对公开的卫星信号结构、接口协议等,利用专业手段和设备进行信号“仿真”、制造“伪卫星”或中继真实信号,产生与真实信号相似且功率略高的欺骗信号,使得接收机真假难辨,导致定位结果错误或偏离^[13]。其中,生成式干扰预先接收卫星信号,然后生成与其相关性最大的伪码信号,并对卫星星历、时钟参数进行篡改,以此产生相位滞后的欺骗信号。转发式干扰是将接收到的卫星信号经过延时处理、功率放大后传播,致使欺骗信号参与定位,导致定位偏离。

③ 混合式干扰机理

这是压制式和欺骗式干扰有效结合。首先,

通过大功率压制进行信息饱和,致使卫星信号被屏蔽或淹没,以此切断接收机与卫星之间的无线链路,迫使失锁重捕。在此期间,发射欺骗信号,构建虚假卫星系统,接收机被诱导锁定并错误定位,至此完成接收机的“接管”。这种组合干扰一般先压制,然后诱骗,隐蔽性和危害性很强。

综合可见,人为干扰成因比较复杂,干扰影响的不确定性较大,尤其是在复杂环境下,极易隐蔽和潜伏,加之其波形、功率和样式灵活多变,且压制式、欺骗式和混合式等多种干扰样式呈现出交织、组合的发展趋势,使得传统的对抗方法更加难以应对。

3 卫星导航定位安全与对抗链路设计及应用

对于卫星导航定位的安全与对抗,不能单纯地依靠某项技术或者手段,重点是解决“环境是什么、对抗要素是什么、干扰程度怎么样、采用什么抗干扰对策、实际如何应用”等系统性问题,即搭建安全与对抗的整体机制和架构。通过借鉴“OODA 环”成熟理论,对其进行优化设计,将原有四个环节扩展、映射于卫星导航定位安全与对抗“干扰-抗干扰”的整个链路,以此将系统性问题分解,通过系统平台化、平台信息循环聚合的模式,建立多级嵌套的对抗机制。

3.1 安全与对抗的不定向循环链路构建

这是融合“OODA 环”理论,将原有的“观察-判断-决策-行动”循环进行优化设计,将每个环节进行分解、拓展和映射,创新设计为“环境感知-筛选隔离-检测识别-效能评估-策略规划-对抗反制-回访反馈-再感知”的卫星导航定位安全与对抗不定向循环链路。这个设计将“OODA 环”的固定模式优化为安全与对抗链路的不定向循环模式。控制干扰从发现到检测到对抗,再到重新发现的整个循环回路,实现周期性外循环和部分环节内循环的网络化迭代输出。

这个理念重点在于引入“循环”和“不定向”两个概念,“循环”区分周期性外循环和部分环节内循环,也是整个链路的精髓所在,就是在循环中加强对干扰的理解、认知、对抗、重复理解的过程,并逐步提高理解、对抗的准确度和时效性;在安全与对抗不定向循环链路的七个环节中,环境感知、筛选隔离映射观察环,检测识别、效能

评估映射判断环，策略规划映射决策环，对抗反制映射行动环，回访反馈属于再感知的引导环，环环相扣又相对独立。“不定向”是不指定循环方向和周期，自适应地依据结果、输入条件、判断进行循环，是内外循环的灵活搭配；这样不仅发挥了外循环的固定性优势，而且优化了内循环运行的自由度。

总体设计思路为：第一环利用全维感知，实现环境信息样本累积；第二环对环境信息样本筛选隔离，保存有用信号；第三环提取特征参数，检测识别干扰模式；第四环建立效能评估指标，量化干扰估值；第五环结合相应准则和技术，制定抗干扰策略和方案，并内循环优化策略；第六环在机制运行层面进行对抗反制；第七环是将对抗情况向第三、四、五环回访反馈，实现迭代优化、循环闭合，如图3所示。

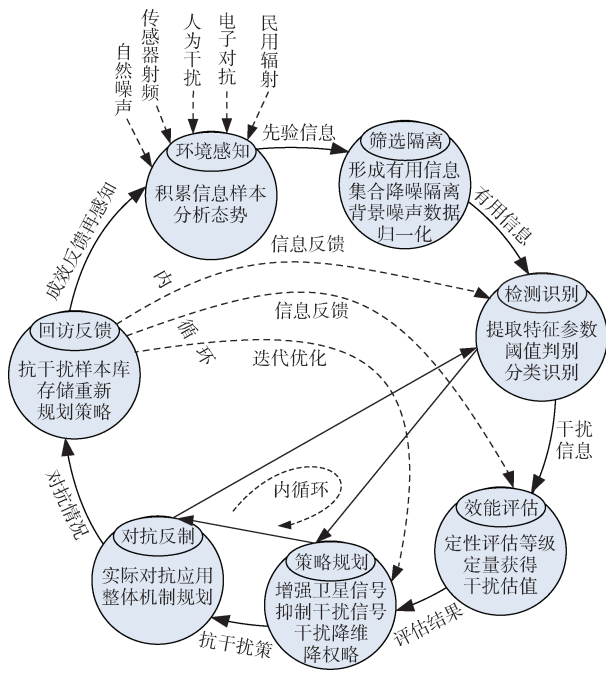


图3 安全与对抗不定向循环链路

Fig. 3 Security and countermeasures non-directional circular link

3.2 实际应用及关键技术分析

3.2.1 环境感知

了解和掌握卫星导航定位设备的“生存”环境是保障设备安全运行、进行干扰对抗的前提。这就要实现对环境的监测、感知。“生存”环境就是在卫星导航定位设备所处的时空区域内，各类系统运行产生的电子设备内部信号辐射，以及遭

遇的各种不同强度、不同频段、不同时空分布上的外部射频信号辐射的立体包围^[13]，主要包括传感器射频信号、人为干扰、电子对抗、民用设施辐射，以及电闪雷鸣、日凌等自然噪声。

环境感知就是搭建各类信息获取平台或系统之间异构的信息网，利用各种观察、监测设备和手段，获取丰富、全面的多源空间信息，作为环境信息样本进行累积，以此分析安全与对抗态势，为干扰判别提供丰富的先验信息和决策依据。

3.2.2 筛选隔离

利用环境感知所得信号的频率、功率、幅相、波形等特征，采用相关信号筛选技术和手段，将与卫星导航信号相关性较高的无线信号保留下来，包括卫星导航信号及人为干扰信号。将这些信号形成有用信息集合，作为干扰检测识别的信息输入。而把与卫星导航信号相关性较差的外部无线信号，诸如自然噪声、传感器射频信号、民用设施辐射信号，以及绝大部分的电子对抗等作为背景噪声进行降噪、隔离。同时，对有用信息集合进行归一化处理，实现不同源头、不同类别、不同量纲和数量级的卫星、干扰混合信号的标准化，转变为模型运算和数字化处理的形态。

3.2.3 检测识别

这是不定向循环链路中关键的枢纽环节，不仅承接外循环的干扰信号输入，而且是第五、六环的成果验证，通过第七环进行内循环反馈。目前，对干扰的检测识别主要是基于干扰信号的时域、频域、空域、能量域、组合域等特性，利用相应的干扰检测算法实现。下面就压制式和欺骗式干扰进行分析。

① 压制式干扰检测识别

对于压制式干扰，主要包括特征参数提取和分类识别两个过程。特征参数提取是获取干扰识别的判读信息，对卫星数据和干扰信息进行二次隔离；为确保干扰检测的敏感性，一般可选取空域二维角度、功率因子、频谱峰度系数、时域峰度系数、归一化频谱冲激部分标准差、FrFT能量聚集度、信号功率和时域波形峰值等8个特征参数。分类识别是对每个特征参数设定判别阈值，对干扰样本数据库、干扰频谱模板、人工经验等进行溯源^[14]，将有用信息集合逐层分解，将干扰信息逐个识别，以此形成“倒树状”层级识别网络，如图4所示。

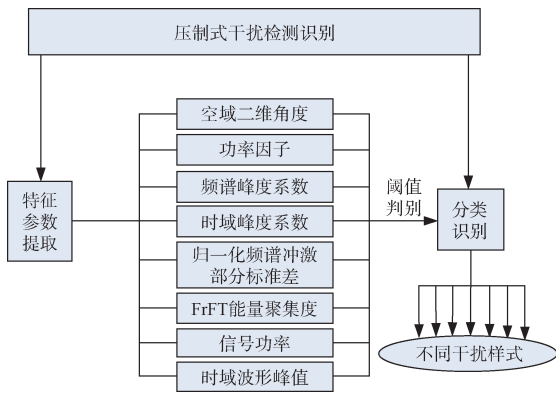


图4 压制式干扰检测识别

Fig. 4 Detection and recognition of blanket jamming

② 欺骗式干扰检测识别

目前的手段主要包括卫星信号功率检测、卫星信号波达角检测、一致性校验检测等^[12], 不同手段的立足点、难易程度和成效各不相同。本文结合实际, 提出一种多层次组合式检测识别方法, 分为四个层级, 即第一层特征参数提取, 第二层干扰检测, 第三层一致性校验判断, 第四层干扰样本识别。首先, 选取倒功率谱密度、相关峰值、多普勒频移、载噪比、空域分布、波达角、波达时间等7个量作为特征参数; 其次, 利用低功率谱密度、相关峰值判别, 检测干扰是否存在, 并“二分”出多路径效应; 然后, 借助多普勒频移、星历数据和时钟参数的一致性判断, “三分”出生成式和转发式; 最后, 利用波达角、波达时间和载噪比, “四分”出单天线和多天线、单源和多源等样式, 以此完成分类识别, 如图5所示。

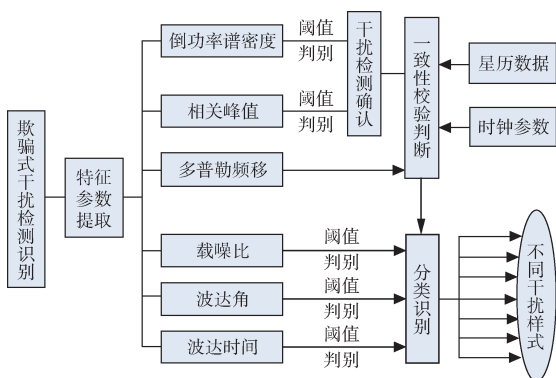


图5 欺骗式干扰检测识别

Fig. 5 Detection and recognition of deception jamming

3.2.4 效能评估

这是在检测识别基础上, 对干扰强度、幅度、广度等进行量化, 包括定性和定量两种方

式。定性是对干扰等级、性质的广义界定, 而定量是对干扰破坏程度的数字化评估。具体流程如下。

① 建立效能评估指标

立足信号捕获、信号跟踪、基带解调和定位解算等四个步骤, 建立表征干扰影响的评估指标, 主要包括平均捕获时间、捕获时间均方差、载波跟踪误差、码环跟踪误差、误码率、载噪比、测距误差、干信比、可见卫星数、DOP值、定位误差、信噪比等12个指标, 如图6所示。

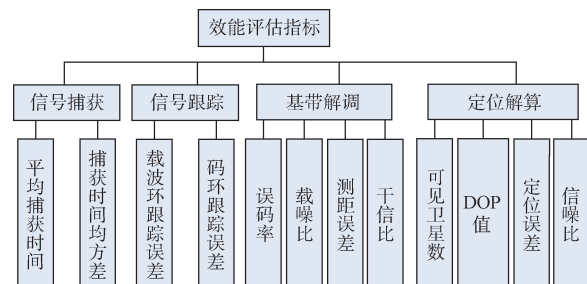


图6 效能评估指标

Fig. 6 Performance evaluation index

② 定性与定量评估

定性决定了干扰的整体性质、影响等级等, 可分四层进行设计, 即一级干扰、二级干扰、三级干扰、四级干扰。其中, 第一级干扰可采用普通的抗干扰技术处理, 后两级需要一定的抗干扰系统进行抑制, 第四级需要接入对抗机制, 通过抗干扰系统之间的网络化协同进行对抗。

定量是通过具体化参数、数字化指标来量化干扰的强度、范围。综合考虑评估指标的影响程度, 建立指标加权值矢量, 利用相应算法构建评估模型, 最终获得干扰估值。将此估值与定性等级进行匹配, 以此实现效能评估。

以欺骗式干扰为例, 假定干扰源的发射功率为 P_j , 发射天线增益为 G_j , 卫星导航定位接收机的天线增益为 G_T , 由此可得, 接收到的干扰信号功率为:

$$J = P_j + G_j + G_T + 2\Delta f - 20\ln(4\pi) - 2L_j \quad (1)$$

其中, Δf 表示无线电频率损耗, L_j 表示干扰源与卫星接收机之间距离引起的空间链路损耗。

此刻, 接收机接收到的信号为:

$$S_r(t) = X(t) + J(t) + n \quad (2)$$

由此可得:

$$S_r(t) = \sum_{i=1}^m A_i d_i(t - \tau_i) M_i(t - \tau_i) \cos(\omega_0 t + \varphi_i) + \sum_{j=1}^m A_j d_j(t - \tau_j) M_j(t - \tau_j) \cos(\omega_0 t + \varphi_j) + n(t) \quad (3)$$

其中, A_i 、 A_j 、 φ_i 、 φ_j 分别为卫星信号 S_i 和干扰信号 J_j 的幅度、相位, d_i 为第 i 颗卫星的卫星数据, τ_i 、 τ_j 为卫星信号和干扰信号的时延, M_i 、 M_j 分别为卫星信号和干扰信号的扩频序列, $n(t)$ 为高斯白噪声。

由此可通过干扰信号对接收机信号影响前后信号的信噪比损失来判断干扰的影响程度, 则有:

$$\gamma(t) = \frac{X(t)}{N} - \frac{S_r(t)}{N+J} \quad (4)$$

其中, $\gamma(t)$ 为信噪比损失, N 为卫星信号噪声, J 为干扰信号强度。

3.2.5 策略规划

这是在明确了干扰模式、干扰估值后, 在控制层面制定的对抗措施。须结合现有技术力量和对抗设备, 启动抗干扰响应机制, 自适应、优选匹配抗干扰策略和方案。同时, 与第三、六环实时内循环, 实现策略的迭代优化。

抗干扰总体策略可包括三个方面, 第一方面是增强卫星信号, 通过空域放大、同相叠加, 大大增强特定方向卫星信号; 目前主要应用自适应调零天线技术^[11], 利用阵列天线方向图合成, 使得主波束对准卫星信号, 常用的阵列形式有线性、圆形、矩形等。第二方面是抑制干扰信号, 利用空、时、频域滤波, 形成干扰信号空域零陷或反相消减^[14]; 这个通常与第一方面融合应用, 给每个阵元赋予最优权值, 控制阵列信号幅相, 以此实现主波束指向增强、干扰零陷。第三方面是干扰降维降权处理, 利用其他定位辅助手段, 降低干扰信号参与定位的权重, 逐渐减弱或消除其影响; 目前主要有一致性检测、惯导辅助、伪卫星技术等^[12]。

综合考虑总体策略的三个方面的内容, 下面重点对空时域自适应抗干扰技术、并行数字多波束抗干扰技术等进行分析。

① 空时域自适应抗干扰技术

空时域自适应处理技术是在空域调零天线技术的基础上, 通过在每个阵元后增加多级横向时延抽头, 并对每个时延抽头信号进行加权, 以此在阵元数已经固定的情况下, 大幅增加抗干扰自

由度^[11], 可有效提高抗宽带、窄带干扰的干扰比, 如图7所示。

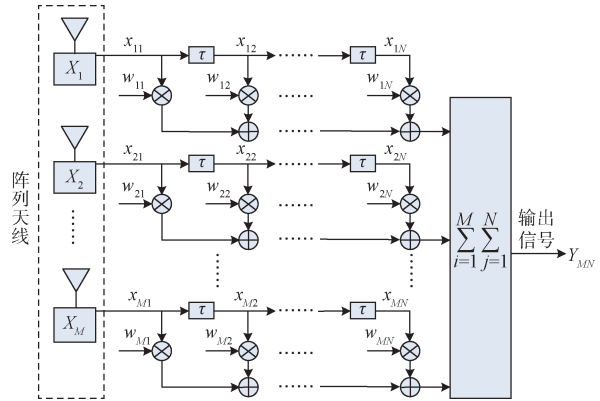


图7 空时域自适应处理结构

Fig. 7 Spatial time domain adaptive processing structure

图中的 x_{ij} ($i=1, 2, 3, \dots, M; j=1, 2, 3, \dots, N$)表示第 i 个阵元第 j 级时延抽头信号; τ 表示阵元的每个时延抽头长度; w_{ij} ($i=1, 2, 3, \dots, M; j=1, 2, 3, \dots, N$)表示第 i 个阵元第 j 级时延抽头信号所对应的加权值。

② 并行数字多波束抗干扰技术

这是解决自适应处理技术需要已知期望信号来向等先验信息才能进行干扰零陷的问题。首先, 将接收到的模拟中频信号转换为数字中频信号, 并通过傅里叶变换, 转换为频域数据; 然后, 利用可接收到的所有卫星信号的来波方向, 形成空域来波方向约束矩阵, 并联合信号的频域协方差矩阵, 生成每个波束的滤波加权值; 最后, 通过滤波加权值对频域数据进行空域滤波, 以此检测出信号的相关峰值, 形成卫星信号来波方向先验信息。通过这个处理, 可控制阵列天线合成波束指向, 并在非卫星信号来波方向形成空域零陷, 如图8所示。

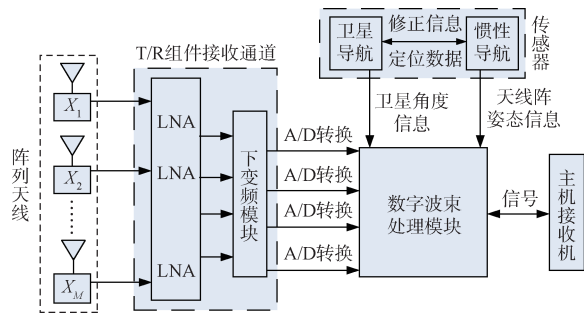


图8 数字多波束处理结构

Fig. 8 Digital multi-beam processing architecture

3.2.6 对抗反制

这是策略的“匹配”执行过程。结合不同应用场景, 将生成的抗干扰策略通过无线或者有线数据链向对抗系统交互信息, 对照干扰效能, 智能化选

择或指令式执行定向对抗、反干扰等不同策略, 消除干扰影响。通过对空域、时域、频域、组合域等不同抗干扰技术的分析, 可形成不同的对抗策略, 需结合实际需求进行合理调用, 如表 1 所示。

表 1 抗干扰策略分析
Table 1 Anti-interference strategy analysis

抗干扰策略	适用范围	优势	不足
时域抗干扰	窄带干扰	成本低, 体积小	只能处理与卫星信号相关性差的窄带信号
频域抗干扰	带宽有限的窄带干扰	成本低, 体积小, 干扰抑制能力强	不适用于宽带干扰
空域抗干扰	宽带及窄带干扰	能适应复杂环境, 抗干扰能力强	系统成本高, 抗干扰数受限于阵元, 抗干扰分辨率有限
空时域自适应抗干扰	宽带及窄带干扰	时延抽头增加了抗干扰自由度, 抗干扰能力强	系统成本高, 计算量较大
空频域自适应抗干扰	宽带及窄带干扰	可对宽带及窄带干扰联合处理, 形成多个频点的干扰零陷	复杂度高, 计算量较大
数字多波束抗干扰	宽带及窄带干扰	有效利用天线阵合成增益, 兼顾了干扰零陷和波束指向	复杂度高, 计算量较大, 需要惯导辅助

这个环节不只是一次循环的末端, 而是对抗干扰机制的检验和总结, 包括两个层面: 一是结合对抗结果, 形成出现问题、优化参数、调整策略、策略存储等信息响应机制, 更好地检验对抗质效; 二是整个机制建设规划, 反思对抗所需的支撑力量、防护设施、反制举措等多方面因素, 形成逆向信息反馈, 加强对抗系统和机制的整体性建设。

3.2.7 回访反馈

这是再感知的前提, 也是本次循环的成效反馈, 可以带着问题和缺陷在下一循环中进行优化、调整, 也可以形成模式记忆和样本积累, 从而在下一个循环进行调用。同时, 可将对抗结果直接反馈至第三、四、五环节进行内循环, 如干扰消除, 则保存本循环的流程和模式, 形成抗干扰样本库存储, 便于下次直接调用; 如干扰未消除或对抗不明显, 则需重新规划策略, 进行二次循环的对抗反制, 直至达到期望效果。

4 结束语

当前在面对“生存”环境日益恶劣且频谱化、信息多元化的复杂态势下, 卫星导航定位设备将经常处于干扰与抗干扰、欺骗与反欺骗、保安全与强对抗的应用场景中, 人为干扰的影响和威胁尤为突出。针对传统手段无法有效应对干扰复杂性、全面性、系统性的不足, 本文借鉴“OODA 环”理论, 在分析四个环节的特点及相互关联,

以及实践转化的基础上, 紧密结合卫星导航定位“干扰-抗干扰”的动态对抗需求, 对“OODA 环”进行优化设计, 与卫星导航定位安全与对抗应用进行耦合, 创新设计了包括环境感知、筛选隔离、检测识别、效能评估、策略规划、对抗反制、回访反馈等七个环节的卫星导航定位安全与对抗不定向循环链路, 具有创新性。还对七个环节进行细致分析, 实现了内外循环的嵌套迭代, 信息导向性传输, 以及各分系统和平台全机制运行。但是随着人为干扰的不断演变, 干扰对抗的时效性、自动化要求更高, 依靠人工和机械化的方式将面临一定挑战, 可考虑融合人工智能技术, 提高智能感知、自动识别、自主决策、主动对抗的能力^[15], 进一步提高卫星导航定位安全与对抗的整体效能。

参考文献

[1] 王月, 孙付平, 丛佃伟. GNSS 干扰感知与对抗决策方法研究[J]. 无线电工程, 2021, 51(10): 1048-1054.
WANG Yue, SUN Fuping, CONG Dianwei. Research on GNSS jamming sensing and countermeasure decision methods[J]. Radio Engineering, 2021, 51(10): 1048-1054.

[2] 王旭旭. 北斗欺骗干扰检测及抑制方法研究[D]. 杭州: 杭州电子科技大学, 2020.

[3] 尹继东, 冯雪峰. GNSS 抗干扰技术综述[J]. 电讯技术, 2020, 60(8): 989-998.
YIN Jidong, FENG Xuefeng. Overview of GNSS anti-interference technology[J]. Telecommunication Engineering,

- 2020, 60(8): 989-998.
- [4] 姚旺, 丛彦超. 海战场雷达末制导系统抗干扰技术研究[J]. 计算机测量与控制, 2021, 29(9): 152-155.
- [5] 孙盛智, 孟春宁, 郑高. 基于OODA环的海警装备作战能力评估[J]. 兵器装备工程学报, 2019, 40(5): 26-28.
SUN Shengzhi, MENG Chunling, ZHENG Gao. Assessment of combat capability of marine police equipment system based on OODA ring[J]. Journal of Ordnance Equipment Engineering, 2019, 40(5): 26-28.
- [6] REVAY M, LISKA M. OODA loop in command and control systems[C]//2017 Communication and Information Technologies (KIT), Vysoke Tatry, 2017: 1-4.
- [7] 李强, 王飞跃. 马赛克战概念分析和未来陆战场网信体制及其智能对抗研究[J]. 指挥与控制学报, 2020, 6(2): 87-93.
LI Qiang, WANG Feiyue. Conceptual analysis of mosaic warfare and systems of network-information systems for intelligent countermeasures and future land battles[J]. Journal of Command and Control, 2020, 6(2): 87-93.
- [8] 王太军, 唐鯽綦, 周超. "星链"在俄乌军事冲突中的应用探研[J]. 通信技术, 2022, 55(8): 1006-1013.
- [9] 顾灏冰, 田少华. 基于OODA环的马赛克战理念及关键技术分析[J]. 空天防御, 2021, 4(3): 65-69.
- [10] HUANG J M, GAO D P. Combat systems dynamics model with OODA loop[J]. Journal of System Simulation, 2012, 24(3): 561-181.
- [11] 王爽. GNSS压制式和欺骗式干扰抑制算法研究[D]. 沈阳: 沈阳航空航天大学, 2019.
- [12] 张伦东, 张超, 高扬骏. 卫星导航欺骗及检测(三): 基于辅助信息的欺骗检测[J]. 导航定位学报, 2021, 9(5): 13-19.
ZHANG Lundong, ZHANG Chao, GAO Yangjun. GNSS spoofing and detection(III): spoofing detection technology based on auxiliary information[J]. Journal of Navigation and Positioning, 2021, 9(5): 13-19.
- [13] 刘科等. GNSS欺骗与抗欺骗技术研究进展[J]. 江苏海洋大学学报, 2020, 29(4): 77-85.
- [14] 潘高峰, 王李军, 华军. 卫星导航接收机抗干扰技术[M]. 北京: 北京: 电子工业出版社, 2016, 4.
- [15] 黄东亮, 戴苏榕. 人工智能在OODA循环中的应用[J]. 航空电子技术, 2020, 51(2): 55-59.

[作者简介]

- 吴 鹏 1980年生, 本科。
- 张启福 1986年生, 硕士, 工程师。
- 魏鹏飞 1971年生, 本科, 高级工程师。
- 姚 远 1988年生, 本科, 工程师。
- 叶 菁 1974年生, 本科, 高级工程师。

(本文编辑: 潘三英)