引文格式:王月,孙付平.卫星导航对抗性能与效能评估研究发展分析与思考[J].武汉大学学报(信息科学版),2026,51(4):633-656.DOI:10.13203/j.whugis20240314

Citation: WANG Yue, SUN Fuping. Analysis and Reflections on the Research Development of Performance and Effectiveness Evaluation for Satellite Navigation Countermeasures[J]. Geomatics and Information Science of Wuhan University, 2026, 51(4):633-656.DOI:10.13203/j.whugis20240314

卫星导航对抗性能与效能评估研究发展分析与思考

王 月[1] 孙付平[1]

1 信息工程大学地理空间信息学院,河南 郑州,450001

摘 要:全球导航卫星系统(global navigation satellite system, GNSS)是当今世界各大国竞相角逐的威慑力量和大国标志。面对日益严峻的GNSS安全应用威胁,卫星导航对抗逐渐得到各国的重视。目前,国际上卫星导航对抗研究主要集中于GNSS干扰与抗干扰相关理论、技术与装备等领域,对GNSS干扰与抗干扰性能与效能评估的研究相对薄弱,存在评估指标零散、权重可信度不高、已有效能评估方法不适用、性能评估无法有效支撑效能评估等难题,需要集中智慧、创新思维,寻找破解这些难题的办法。首先,明确了卫星导航对抗的内涵,并结合现有的评估分类将卫星导航对抗评估定义为卫星导航对抗性能评估与效能评估两类;随后,分析评述了国内外在这两类研究领域的发展思路、创新成果、测试应用以及一些值得关注的发展动向;最后,总结归纳了研究历程不同阶段的技术特征和成功经验,对照分析了卫星导航对抗评估研究的发展局限,并依据具体国情提出了4个方面的对策和建议,涉及研究思路、研发重点和事项安排等方向性议题,旨在抛砖引玉、深入交流,为决策部门部署下一步工作提供参考。

关键词:GNSS;卫星导航对抗;指标体系;性能评估;效能评估;多属性决策;动态博弈

中图分类号:P228 **文献标识码**:A **收稿日期**:2024-12-07

DOI:10.13203/j.whugis20240314 **文章编号**:1671-8860(2026)04-0633-24

Analysis and Reflections on the Research Development of Performance and Effectiveness Evaluation for Satellite Navigation Countermeasures

WANG Yue[1] *SUN Fuping*[1]

1 School of Geospatial Information, Information Engineering University, Zhengzhou 450001, China

Abstract: **Objectives**: Global navigation satellite system (GNSS) serves as both a strategic deterrent capability and a symbol of national strength among major powers worldwide. With the security environment surrounding GNSS applications becoming increasingly severe, satellite navigation countermeasures have attracted growing attention from many countries. In recent years, research in this field has mainly focused on theories, technologies, and equipment related to GNSS jamming and anti-jamming. By comparison, studies on the performance evaluation and efficacy assessment of GNSS jamming and anti-jamming remain relatively limited. A number of prominent problems still exist, including fragmented evaluation indicators, limited systematicity in evaluation frameworks, insufficient credibility of indicator weighting, the limited applicability of existing effectiveness evaluation methods, and the inability of performance evaluation results to effectively support efficacy assessment. These issues highlight the urgent need to integrate collective expertise and develop innovative approaches to overcome current bottlenecks in satellite navigation countermeasure evaluation. The conceptual connotation of satellite navigation countermeasures is clarified, and the current state of evaluation research in this field is systematically examined. On this basis, major limitations in existing re-

基金项目:国家自然科学基金(42330113)。

第一作者:王月,博士,讲师,主要从事卫星导航对抗评估理论与方法研究。wangyplaxd@163.com

通信作者:孙付平,博士,教授。sun.fp@163.com

search are identified, and feasible directions for future development are proposed in accordance with practical national needs. **Methods:** First, the connotation and scope of satellite navigation countermeasures are explicitly clarified. By combining this understanding with existing evaluation taxonomies, satellite navigation countermeasure evaluation is categorized into two major types that are performance evaluation and effectiveness evaluation. Performance evaluation is conducted by establishing evaluation models and testing methods to quantitatively assess satellite navigation countermeasures, thereby obtaining quantitative results and supporting performance optimization. Effectiveness evaluation, in contrast, is carried out by using operations research methods to determine indicator weights and optimize alternative schemes, thereby obtaining the optimal solution, formulating response strategies, and improving protective benefits. In this framework, performance evaluation serves as the basis for effectiveness evaluation. Based on this classification, domestic and international research in both categories is reviewed and analyzed from multiple perspectives, including development ideas, technological approaches, representative innovations, testing and application, and emerging trends worthy of attention. Through comparative analysis, the evolution of relevant evaluation methods is further examined, and their main characteristics at different stages of development are summarized. **Results:** The analysis indicates that the theoretical and methodological research on performance evaluation and effectiveness evaluation of satellite navigation countermeasures can be accomplished through the successive implementation of these two types of evaluation, given their interaction and continuity. However, existing studies have mainly focused on partial performance evaluation under a single interference source or a single confrontation scenario, resulting in a rather limited evaluation perspective. Comprehensive evaluation and optimal decision-making for multiple confrontation scenarios and multiple interference patterns have not yet been adequately addressed. Consequently, a number of problems remain, including fragmented indicator systems, incomplete performance evaluation models, low credibility of indicator weighting, the limited applicability of effectiveness evaluation methods, insufficient coordinated treatment of dynamic complexity, fuzziness, and randomness, and the lack of validation and feedback mechanisms. These limitations ultimately prevent performance evaluation from effectively supporting effectiveness evaluation and, in turn, hinder the effective protection benefits of satellite navigation systems. **Conclusions:** In light of these findings and with due consideration of specific national conditions, four categories of countermeasures and suggestions are proposed. These recommendations involve research concepts, development priorities, and task arrangements among other strategic issues. The overall purpose is to encourage further discussion and deeper academic exchange, promote the transition from fragmented indicator-based analysis to more systematic and application-oriented evaluation thinking, and provide useful references for decision-making departments in planning future work on satellite navigation countermeasures. By strengthening both performance evaluation and efficacy assessment in an integrated manner, the scientific foundation and practical support for GNSS confrontation capability development can be further improved.

Key words: GNSS; satellite navigation countermeasures; index system; performance evaluation; effectiveness evaluation; multi-attribute decision-making; dynamic game

全球导航卫星系统(global navigation satellite system, GNSS)是国家重要的空间基础设施,大量应用于国民经济的核心领域,日益成为保障现代社会大系统实时动态安全运行的战略基础资源。由于系统本身的脆弱性和易干扰性,目前各相关国家都在不遗余力地推进卫星导航系统的性能完善和技术升级,力图取得制信息权的优势。因此,在保证己方有效利用卫星导航信息的同时阻止敌方使用该信息,就成为各相关国家在导航领域争夺的焦点。1997年,为了稳固全球定位系统(global positioning system, GPS)在高科技时代日益增长的优势,美国正式提出了卫星导航对抗的概念[1]。2020年,美国提出了“下一代国防太空体系架构”的概念,将下一代太空体系建设的军事需求明确指向了导弹抗干扰和卫星导航对抗[2-3];2021年,中国则将下一代北斗卫星导航系统(BeiDou satellite navigation system, BDS)的发展方向对准更泛在的综合定位导航授

时,建立国家时空体系,实现导航与通信深度融合,军事需求明确指向卫星导航对抗[4-5]。因此,卫星导航对抗现已从保障GNSS的安全应用发展成渗透空天、网络、电子等诸多领域的综合攻防战,是取得制信息权的关键。

卫星导航对抗是电子对抗行动在导航应用领域的集中呈现,其核心是保护和阻止,常分为卫星导航侦察、卫星导航攻击以及卫星导航防御三大类,包括软毁伤与硬毁伤技术、用户端防御与系统端防御技术、干扰信号监测与目标侦察技术等。GNSS是卫星导航对抗的主体,导航信号频率固定且下行链路信号微弱,使得GNSS干扰易发、频发,GNSS抗干扰研究成为热点,卫星导航对抗现已从毁伤与抗毁伤的大国较量逐渐聚焦至GNSS干扰与抗干扰的攻防对抗。其中,GNSS干扰包括压制干扰和欺骗干扰,GNSS抗干扰包含用户端抗干扰与系统端抗干扰。用户端抗干扰技术相比于系统端抗干扰更容易施行,而欺骗干扰相比于压制干扰实现难度大,危害更加严重,但隐蔽性更好,能实现对目标精准控制。20世纪以来,GNSS干扰的案例不胜枚举。例如,伊朗诱捕美军RQ-170哨兵无人机,黑海船只受到了大规模的欺骗干扰[6-7];俄乌战争期间俄方频繁采用压制干扰,如克拉苏哈-4系统,令乌方制导武器命中率大幅降低,并影响了机载预警和控制系统等;为应对俄方干扰威胁,乌方利用无人机优先摧毁俄方导航对抗装备,莫斯科市区因此频繁遭遇无人机袭击[8]。上述事件使得GNSS安全应用获得了更多关注。为有效应对不断增长的安全威胁、保障GNSS的安全应用,相关单位先后搭建了卫星导航对抗系统框架以推进其中的技术发展,又陆续研发并测试了导航对抗装备与各类搭载平台,以保障系统安全应用。

为科学衡量卫星导航对抗的测试效果、装备性能与算法优劣,从而有效牵引对抗技术的成熟化与装备的体系化升级,亟需系统性地深入开展卫星导航对抗评估研究。实现有效评估不仅有利于GNSS内部系统的更新与外部设施的维护,还能扩大己方防护效益并帮助作出最优决策。现有评估研究主要归为两类[9]:(1)卫星导航对抗性能评估,通过确定评估模型与检测方法开展性能评估,以得到量化结果、完成性能优化;(2)卫星导航对抗效能评估,通过运筹学方法完成指标定权与方案择优,以得到最优解,给出应对策略且扩大防护效益。其中,性能评估是效能评估的基础。然而,卫星导航对抗系统框架成形不久,相关的研究不多,且现有研究仍处于单一场景、单一干扰源的分项性能评估阶段,缺少系统的效能评估研究且现有的效能评估方法不适用,导致未能形成一套完整的卫星导航对抗性能与效能评估指标体系与综合评估方法。

因此,本文以中国BDS安全防护的重大需求为牵引,分析并思考卫星导航对抗性能与效能评估的理论与方法研究发展,支撑不同信息对抗情形下最优决策的实现与动态博弈分析,以提升BDS对抗干扰威胁的安全防护能力。

1　卫星导航对抗及其评估研究的发展概况

1.1　卫星导航对抗概况

根据用户部分、地面部分、空间部分等卫星导航系统的组成及导航信号频率固定且下行链路信号微弱等特点,卫星导航对抗技术可归为3类,即卫星导航侦察、卫星导航攻击和卫星导航防御,其组成如图1所示。此外,因GNSS干扰事件易发、频发,且卫星导航对抗又多聚焦于GNSS干扰与抗干扰,故本文主要针对GNSS干扰与抗干扰开展性能与效能评估研究。

1)卫星导航侦察。利用侦察设备搜索、截获、识别、定位和分析空中辐射的电磁能量,以掌握对方辐射源的技术特性、生存能力、威胁程度和部署变动等情报的电子技术[10]。对攻击方而言,侦察是对任务目标的识别、跟踪和其威胁程度的确定,典型技术包括任务目标特征识别、任务目标拦截、任务目标定位[11]等。对防御方而言,导航侦察主要是对攻击方生成或转发的干扰信号的感知,主要技术包括干扰检测技术、干扰识别与分类技术、干扰源探测与干扰源定位技术[12]等。对硬毁伤系统而言,侦察是对预警卫星和预警飞行系统等预警系统侦察能力的衡量,即探测能力、跟踪定位能力、预报能力、预警任务完成能力、自主运行能力、信息传输能力和生存抗毁能力等[13]。而安全态势感知技术是对脆弱性、容灾性、威胁性和稳定性等能力的性能评估。

2)卫星导航攻击。从攻击对象来看,相比于系统端,对GNSS用户端实施攻击容易得多。从攻击手段来看,可分为硬摧毁、赛博攻击和软毁伤。硬摧毁主要利用高功率微波、强电磁脉冲等物理方式和各种类型的导弹等装备对GNSS设备及导航系统包含的基础设施和卫星等造成不

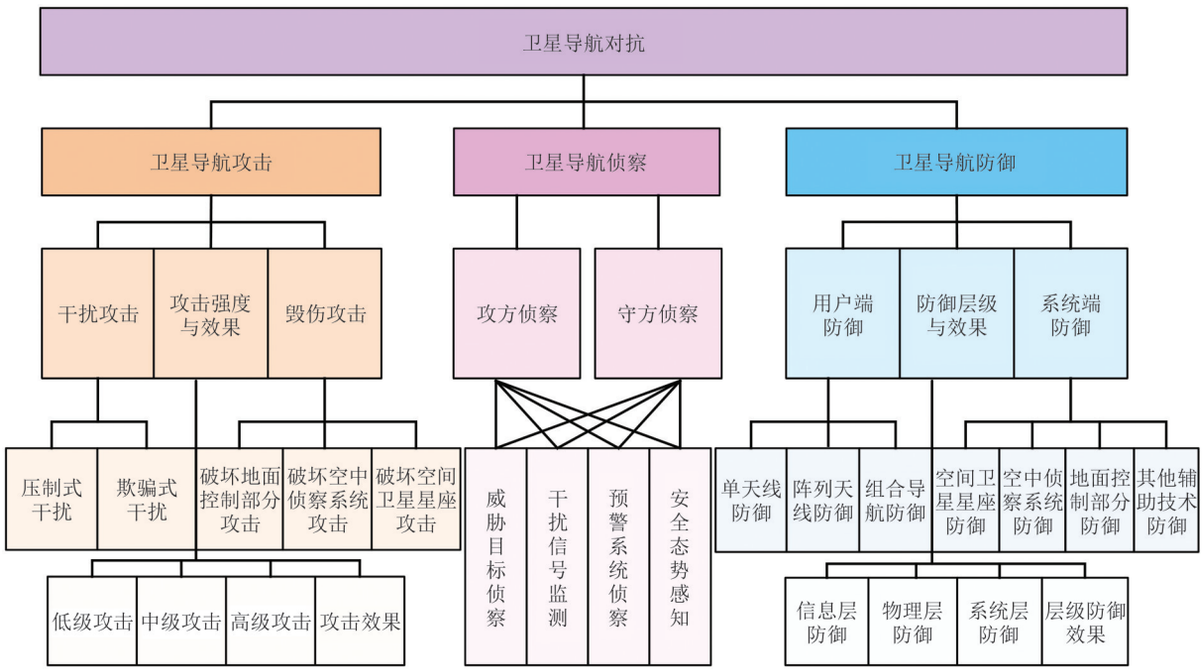
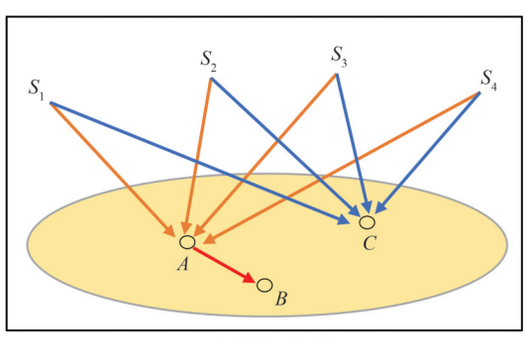


图1 卫星导航对抗的基本组成

Fig. 1 Basic Components of Satellite Navigation Countermeasures

可逆的损毁[14]。赛博攻击主要通过网络蠕虫、计算机病毒等低级攻击、中级攻击和高级攻击逐步入侵、破坏GNSS包含的智能设备和信息传输链路等[15]。软毁伤即GNSS干扰技术,是本文研究的主要攻击手段,利用有意干扰使GNSS无法正常工作,包括压制式干扰和欺骗式干扰,前者按照干扰信号的带宽分为窄带干扰与宽带干扰等[16],后者包括基于卫星导航模拟器的欺骗技术、转发式欺骗技术和较复杂的生成式欺骗方式等。其中,欺骗式干扰实现难度大,危害更加严重,但隐蔽性更好,能实现对目标的精准控制[17]。

以危害严重及实现难度大的GNSS欺骗技术为例进行扩展说明。根据技术实现的特点,GNSS欺骗技术可分为3类[1-2]:(1)初级欺骗技术,即基于卫星导航模拟器的欺骗技术,是较容易实现的生成式欺骗方式。(2)中级欺骗技术,即转发式欺骗技术,其干扰原理如图2所示,在欺骗实施的过程中,位于A点的欺骗干扰设备接收到导航信号并转发给位于B点的接收机,从而将其欺骗到预设位置C点。该类欺骗的难点在于对接收到的导航信号进行高精度时延控制与参数调制处理等,从而穿透接收端的信号处理与鉴别机制。(3)高级欺骗技术,为较复杂的生成式欺骗方式,其干扰原理如图3所示。在欺骗实施的过程中,欺骗信号的相关峰与真实信号的相关峰之间会发生交替的相对运动,欺骗信号相关峰凭借其功率优势逐渐将真实信号相关峰从跟踪环路



S_i:卫星发射的导航信号

A:欺骗干扰设备 B:导航接收机 C:预设的欺骗位置

图2 转发式欺骗的干扰原理

Fig. 2 Jamming Principle of Repeater Deception

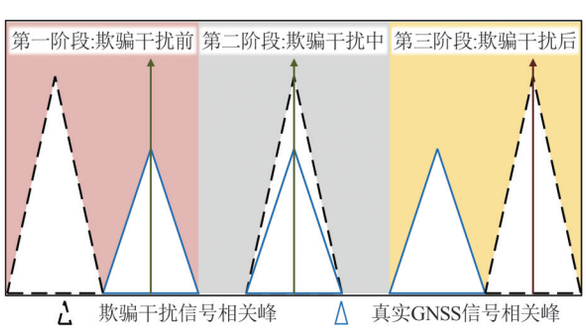


图3 生成式欺骗的干扰原理

Fig. 3 Jamming Principle of Generative Deception

中拖拽剥离,最终实现对环路的控制,该过程的实现难点主要在于欺骗触发条件与欺骗策略设计。生成式欺骗信号的码相位超前真实信号,因此不会被当作多径信号,故隐蔽性更佳。文献[18-19]使用初级欺骗技术完成欺骗接收机的实验并验证

了该技术的可行性;为提高中级欺骗的实现效果,文献[20-21]针对中级欺骗的实现难点深入分析了影响效果的时延、定位误差、选星方法等并提出了相应的解决方案;文献[22-23]针对高级欺骗的实现难点分别在欺骗信号无缝地接替真实信号的锁定条件和结合无人机动力学模型的欺骗策略上作出了贡献。从初级欺骗技术到高级欺骗技术,欺骗技术的隐蔽性逐级变强、技术成本变高、实现难度和抗欺骗难度逐级提升。

3)卫星导航防御。在系统设计层面,通过采用军民码信号频谱分离与重构、功率增强以及电文与伪码加密等技术,能够有效提升系统的综合防御能力。相较于这些需要在系统端进行全局性升级的防御手段,针对用户接收终端的强化技术则具有更易实施和部署的优势。对硬毁伤的防御是对空间段、空中段、地面段等基础设施进行电磁防护,常用技术包括滤波、屏蔽、隐身、接地及元器件加固等[24]。对赛博攻击的防御是对信息层、物理层和系统层进行安全防护设计,常用技术为各种攻击与异常检测、攻击传播路径和异常影响轨迹分析、安全策略与全局调度策略制定等[25]。对软毁伤攻击的防御技术即GNSS抗干扰技术,是本文研究的主要防御手段,包括抗压制干扰技术和抗欺骗干扰技术。其中,对窄带干扰的抗干扰技术包括但不限于时域窄带抑制、变换域抑制技术和码辅助技术等,对宽带干扰的抗干扰技术包括但不限于功率倒置算法、波束形成算法和空时联合抗干扰技术等[26];抗欺骗干扰技术包括基于信号特征的抗欺骗技术和基于辅助信息的抗欺骗技术。

以实践需求迫切的GNSS抗欺骗技术为例进行扩展说明。随着导航欺骗技术的发展,GNSS抗欺骗技术根据技术应用的特点主要分为3类[17]:(1)特殊抗欺骗技术,为基于导航信号加密认证的抗欺骗技术,仅在特定服务或增值服务中应用;(2)常规抗欺骗技术,为基于信号特征的抗欺骗技术,从绝对功率监测、多普勒频率信息与星历信息一致性检测、信号品质检测到空间处理技术[27],成果丰富;(3)新型抗欺骗技术,为基于辅助信息的抗欺骗技术,利用惯性导航、视觉定位等非卫星导航手段与卫星导航结果的比较实现检测。文献[28]提出基于多普勒频差的GNSS多天线阵检测欺骗攻击方法并验证了方法的有效性;文献[29]利用惯性导航系统监测器构建的评估模型检测出导航欺骗干扰并验证了其攻击效果;文献[30]提出基于视觉传感器的协同导航方式,利用未受欺骗的无人机位置确定受欺骗的无人机位置。从特殊抗欺骗技术到常规抗欺骗技术,应用场景与范围变广、抗欺骗手段变多;从常规抗欺骗技术到新型抗欺骗技术,欺骗消除程度变大,定位结果更可靠,接收机的布设与使用限制减少、成本变低,但研究成熟度却变低了。

1.2　评估研究发展概况

性能表示系统或事物执行其功能或提供其功能服务的能力、水平或质量,这种能力的大小、水平的高低、质量的好坏可用一系列的性能指标来度量,在某种意义上可把性能看成是系统或事物的固有属性或特征[31]。军事装备的效能在GJB 1364—1992中的定义是指在规定的条件下达到规定使用目标的能力。其中,规定的条件指的是环境条件、时间、人员、使用方法等因素,规定使用目标指的是所要达到的目的,能力则是指达到目标的定量或定性程度[32]。效能是一个抽象概念,随着研究角度的不同具有不同的具体内涵,可通过效率、效果、效益来衡量。虽然不同领域对效能的定义略有差异,但其核心是针对系统,目标是通过综合评估得到效果与效益,最终实现决策。

性能评估是效能评估的基础,完成两类评估才可视为实现完整评估。评估的研究进展具体为:评估指标作为衡量性能变化对评估对象实施能力影响的重要标准而存在,完成评估指标体系搭建后,评估方法的选取显得尤为重要。效能评估方法有很多,具体分类如图4所示。早期多采用单一评估方法,随着人工智能的发展与应用,评估方法现已从层次分析法(analytic hierarchy process, AHP)、熵权法(entropy weigh, EW)分别与模糊综合评判法(fuzzy comprehensive assessment, FCA)融合的定量评估[33],组合赋权方法(combination assigning method, CAM)与FCA融合的定量评估,AHP、EW、CAM分别与灰色关联分析方法(grey relational analysis, GRA)融合的定量评估[34],逐渐发展到多维度、多功能评估方法联合智能改进的定量评估。对于卫星导航对抗系统,上述评估方法广泛应用于实现导航定位的陆海空各类机动平台、精密制导的巡航导弹和精确制导导弹等相关装备的性能评估,以及野外机动部队的定位、支持到救援行动等任务实施效果评估,研究成果推动了装备升级、提升了任务成功率、辅助了最优决策实现。

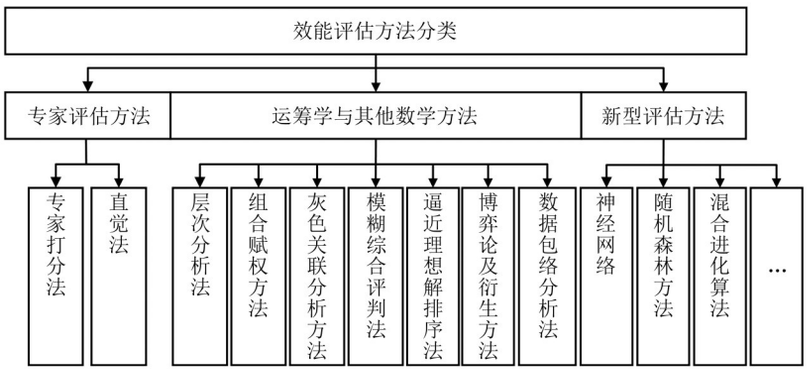


图4 效能评估方法的分类

Fig. 4 Classification of Effectiveness Evaluation Methods

FCA根据附加条件和模糊数学的原理,基于评估标准与评估指标,经过模糊变换后对待评估对象计算一级、二级评判矩阵进行总体评判,再据此排序择优[34]。作为因素识别和解析工具的GRA也是一种效能评估方法,应用于主客观信息集成的多属性决策研究[35]。AHP则是一种将评估过程中的影响因素分成目标-准则-方案等层次的主观决策方法[36],技术路线如图5所示。

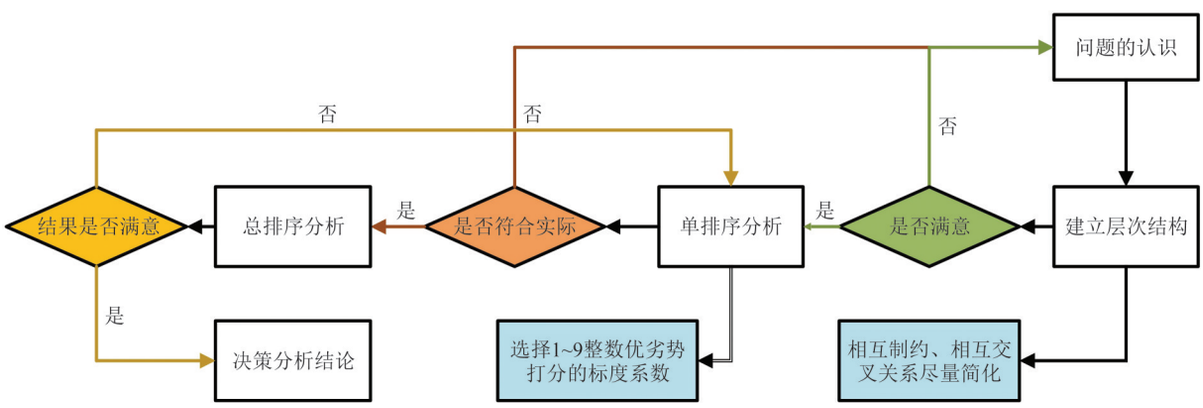


图5 AHP的技术路线

Fig. 5 Technical Route of AHP

专家系统(expert system, ES)作为人工智能的一个重要分支,其核心在于利用历史经验与专家知识构建知识库,并基于模型与网络结构实现推理机制。自1968年首个ES成功研制以来[37],该方法已成为降低定性指标不确定性的代表性途径之一。1995年,李德毅院士在概率论与模糊数学的基础上进一步提出了云模型,从定性评价的角度刻画主观认知对客观事物的反映以及理论概念本身的不确定性[38]。2000年之后,随着人工智能的快速发展,以云模型与ES为核心的多种融合智能方法不断涌现,推动相关技术在更广泛的领域中得到应用与推广。因此,根据上述评估方法的发展概述,总结了相关效能评估方法的属性对比,如图6所示。

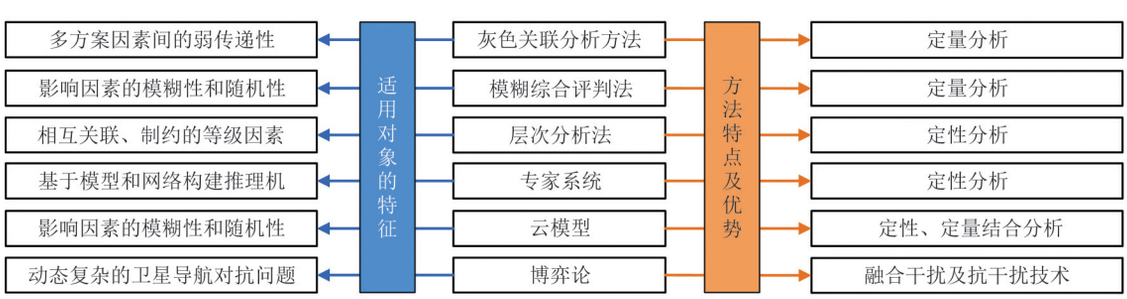


图6 相关效能评估方法的属性对比

Fig. 6 Attribute Comparison of Related Effectiveness Evaluation Methods

为应对对抗场景中动态演化与多维属性的复杂耦合,通信领域引入经典博弈论并将其应用于雷达对抗干扰效能评估,相关研究思路对卫星导航对抗具有重要参考价值。博弈论作为研究

竞争互动中策略优化问题的数学理论与方法,为该类问题的建模与求解提供了系统框架[39]。按照博弈模型的分类,通常将卫星导航对抗动态博弈看成是零和博弈,在此基础上,通过借鉴生物种群进化思想进行学习和模仿,结合历史经验与盈利结果,不断调整各自的策略选择,逐步发展成演化博弈[40]。如果将博弈理解成一个逐步优化的过程,有限理性的演化博弈就很好地解释了均衡的动态演进和收敛过程,已广泛应用于网络对抗、信息安全、基础科学等领域。

2　卫星导航对抗性能评估研究

考虑到性能评估是效能评估的重要基础和有效过渡,为开展相对完整的技术类评估,首先需要梳理针对卫星导航对抗的性能评估指标体系与性能评估方法的研究现状,具体如下。

2.1　性能评估指标体系

卫星导航对抗性能评估指标体系的构建需要依托科学的构建原则与评估标准。已有不少学者针对不同特性的评估对象开展了相关研究,其中,文献[41]提出将精度、完好性、连续性与可用性、兼容与互操作性等作为卫星导航系统性能评估体系的构建原则;文献[42]提出以自适应准则、功率准则、概率准则和衰减准则等作为评估组合导航系统性能评估体系的构建依据;文献[43]提出将完备性原则、针对性原则、独立性和层次性原则等作为装备性能评估体系的构建原则。已有构建原则存在启发意义,但评估对象不是面向卫星导航对抗的GNSS,致使其没有针对性,直接搬用已有原则容易陷入不适配的局限。

目前,针对完整的卫星导航对抗性能评估指标体系构建的研究较少,而针对其GNSS干扰与抗干扰性能分析的研究较多。文献[44]考虑了干扰对目标接收机信号处理的不同环节的影响,围绕欺骗信号功率提出了4个指标用于评估GNSS欺骗干扰的效果;文献[45]提出了5个指标用于评估GPS/捷联惯导系统组合型导航接收机抗欺骗干扰的效果;文献[46]提出了一个基于指标体系的硬毁伤效果评估系统,并给出了单项性能指标和综合能力指标的评估模型;文献[47]根据预警卫星系统的组成与工作流程,从预警任务、传感器使用、数据融合角度构建了侦察性能评估指标体系。上述指标不具有通用性,未能兼顾卫星导航对抗的动态复杂性,得到的性能评估结果能为设计者提供改进意见,但不能为决策者提供决策辅助。

此外,针对卫星导航对抗性能测试体系搭建,已有相关研究为评估GNSS干扰效果搭建了相关平台,文献[48-49]搭建了GNSS欺骗式干扰的效果评估实验平台,并利用已有指标的评估模型和检测步骤,基于Matlab等开展了干扰效果评估及性能量化分析。虽然已搭建的平台可用于GNSS干扰与抗干扰性能评估的测试,但现有研究的测试方法普适性不足,难以直接借鉴以推进本文研究。

2.2　性能评估方法

2.2.1　GNSS干扰能力

GNSS信号体制直接影响了压制干扰能力,目前针对压制干扰的评估研究集中在对不同导航终端的码跟踪精度和多径误差大小的性能分析上[50],而缺少针对不同信号体制导航信号的抗干扰能力的论证。为此,文献[51-52]先分析了单频干扰对部分民码导航信号载噪比和码跟踪误差的影响,但一方面研究仅针对单一干扰样式,另一方面其设置的仿真场景与实际不符,所得结果的可靠性有待商榷。为弥补不足,文献[53]针对不同压制干扰开展了跟踪性能分析,但仿真时设置的导航信号频谱是连续谱数这一仿真条件也不真实,且未能进一步总结压制干扰对不同信号调制方式的威胁程度。因此,文献[54-55]依据GNSS信号各自的频谱特点,依次推导了干扰等效载噪比和平均码跟踪误差,分析了压制干扰对GNSS信号体制设计的影响规律,给出了BDS现有信号调制方式的优化建议。

针对欺骗式干扰,文献[56]从欺骗对抗场景中的功率空间和欺骗对抗效果中的欺骗有效概率出发,设计了基于欺骗有效功率可行域的评估方法,但没有明确评估指标与数学模型;文献[57]建立了空间特征模型,给出了欺骗信号覆盖区域,分析了欺骗效果受欺骗信号与真实信号码相位差异的空间分布变化的影响,但仅就欺骗信号的空间覆盖特性模型开展了具体研究;文献[58]构建了BDS用户终端模拟环境和实装对抗实验环境,提出了欺骗干扰性能评估方法,但评估方法仅停留在定义阶段,不涉及数学模型与检测方法;文献[59]对GNSS欺骗干扰进行了性能评估,并提出相应的评估指标,但未兼顾GNSS欺骗的快速性、隐蔽性、时效性等关键特性及其功率分配的重要性,导致评估结果的可用性有待商榷;而文献[60]虽然针对GNSS欺骗信号的功率

分配问题提出了功率分配原则,但研究是面向欺骗设备的攻方视角,并非面向干扰与抗干扰间博弈的攻防视角开展综合评估。综上,已有研究存在评估视角单一、指标体系构建不全面、评估模型与检测方法不完善及实践性差和未考虑综合评估方法等问题。

此外,所有的评估对象均是单干扰源或基于单干扰源的抗干扰技术,而真实电磁环境下卫星导航对抗显然更加复杂:(1)单干扰源情形几乎不可能存在,压制式干扰与欺骗式干扰组成的多干扰源情形才是常态;(2)卫星导航对抗时各干扰源部署结构不同,对威胁性目标产生的干扰效果必然不同。因此,所得成果是理想的,仅可作为多GNSS干扰源干扰效果评估研究的参考值,辅助实现多干扰源全域协同的优化部署。然而,除了文献[61-63]分别针对压制式干扰源以及转发式欺骗干扰源开展单干扰源部署结构的研究外,针对多干扰源的协同部署及部署效果评估的研究却很少。

2.2.2 GNSS抗干扰能力

针对用户端抗干扰能力,为推进相关抗干扰技术的发展与成熟,开展合理的用户端抗干扰能力评估指标与评估方法研究是基础。现有文献中常能见到诸如干扰抑制能力达到x dB的结论[64],但没有给出干扰抑制能力的统一定义,不同文献的评估重点不同,给出的定义不一致,得到的结论缺乏统一比较的标准。在此基础上,已有研究提出了一些评估干扰检测与抑制算法效果的指标,如信噪比变化率、误码率变化率[65]、干扰门限和抗干扰改善因子[66]等。已有指标都是基于某一具体应用场景提出的,但考虑到不同场景对应的数学模型一般不同,因此,已有研究给出的评估模型往往不一致,最终,定义与模型上的不一致将导致性能评估结果不可靠。此外,现有研究开展体系构建与评估方法研究时多依据GNSS接收机的主动抗干扰能力、固有抗干扰能力和被动抗干扰能力[67],很少将用户端作为卫星导航对抗的博弈参与方并兼顾其在对抗时应对威胁的有效防护措施,故未以实施防护措施的主体装备作为评估对象开展分项性能评估与综合能力评估研究。

针对系统端抗干扰能力,以BDS为例,针对北斗二号系统(BDS-2)和三号系统(BDS-3)服务性能的评估研究较多。2012年,BDS-2建设之初,文献[68]针对该系统的服务性能初步提出了评估指标,并开展了性能评估;在此基础上,文献[69]以精密星历钟差为标准,利用2013-03—2016-09的观测数据详细分析了BDS-2空间信号精度这一指标的演进情况;文献[70]验证了BDS-3实验卫星的空间信号性能水平;文献[71]对BDS-3服务性能指标进行了分析论证;BDS-3建成后,文献[72]利用空间信号精度这一精度评估指标深入分析并验证了BDS-3的优异性能;2021—2023年,文献[73-75]对BDS-3的定位、导航、授时服务性能进行了全面评估,并设想了BDS下一代的发展目标与优化方向。以上研究主要探讨BDS在安全情形下的性能水平,但存在以下缺陷:(1)虽然安全情形是理想环境,除文献[76]外仍少有研究完成了对系统各类服务性能及其设施功能的全面评估;(2)BDS-3作为卫星导航对抗的参与者,所处电磁环境瞬息万变,空间部分与地面部分作为GNSS的核心组成,当其面对不同干扰强度的威胁时,鲜有研究对其抗干扰能力开展完善的分项性能评估与综合能力分析。

3 卫星导航对抗效能评估研究

效能评估研究已广泛应用于生物识别技术[77]、网络安全[78]、智能电网[79]和无人系统[80]等多个领域,以应对各类威胁源。根据效能评估的定义,卫星导航对抗本质上是一个在不完全信息条件下进行的复杂决策与博弈过程:它是一个多属性决策问题,需要基于已有信息对有限备选方案进行排序与择优;同时,按照博弈模型的分类,卫星导航对抗更是一个动态博弈过程,攻防双方在竞争环境中不断优化自身策略。卫星导航对抗效能评估研究的技术路线如图7所示。

针对卫星导航对抗的多属性决策研究,其核心在于通过运筹学方法,从系统工程角度对各项性能评估结果进行综合评估与决策分析。该过程主要包括指标定权与方案择优两个关键环节:先将性能评估结果输入至定权方法与多属性决策方法中,计算得到各层级指标的权重;然后通过计算各备选方案的相对贴近度等综合评估结果,择优选取评估值最优的方案。由此得到的定权结果与最优方案,构成了后续开展动态博弈效能评估的关键输入。在此基础上,决策者需要解决一系列问题,以完成从静态评估到动态博弈的跨越,例如,构建动态博弈模型并量化盈利矩阵,求解盈利方程并获得全局最优解,基于最优方案实现动态博弈与动态推演等。因此,针对动态博弈开展的

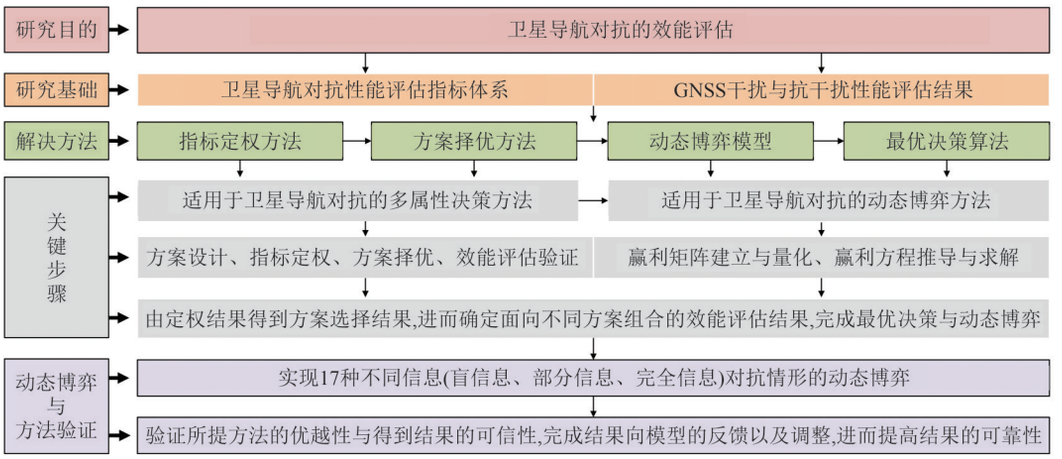


图 7　卫星导航对抗效能评估研究的技术路线

Fig. 7　Technical Route for Research on Effectiveness Evaluation of Satellite Navigation Countermeasures

研究主要包括博弈模型建立、模型要素量化、盈利方程求解、盈利结果确定等方面,本文将围绕这几个方面梳理卫星导航对抗效能评估的研究现状。

3.1　多属性决策方法

3.1.1　指标定权方法

指标权重能否有效确定直接关系到效能评估结果以及最优决策的有效性和准确性。运筹学中已有的定权方法包括主观赋权法和客观赋权法,典型的主观赋权法有 AHP[81],经典的客观赋权法有 EW[82]。两类算法的优缺点明确:AHP 不确定性高,缺少评估数据的度量;EW 客观性强,缺少不确定性的度量。而基于主客观赋权法的 CAM 则保留了两者各自算法的优势,得到的权值相对更合理[83]。例如,文献[84]采用主客观定权方法开展指标定权,对指标本身开展主观打分或者依据其测量值确定权重大小,但忽略了指标相对评估目标的重要性,即忽略了贡献度。因此,前人研究未提出兼顾指标定权的主客观性以及指标相对评估目标的重要性的定权方法[85]。

考虑到上述局限,还需要确定指标相对评估目标的重要性以改进指标定权方法。早期,武器装备系统效能评估指标的重要性是采用线性回归方法来确定的,结果越大表示指标越重要。近年来,随着机器学习及其算法的发展和应用,用于确定指标相对评估目标的重要性的效能评估方法越来越多,包括主成分分析(principal component analysis, PCA)、粒子群优化(particle swarm optimization, PSO)、粗糙集理论(rough sets, RS)、模糊理论(fuzzy logic, FL)、随机森林(random forest, RF)、云模型等。其中,PCA 将评估指标映射至新的空间,强调变量对总方差的贡献[86]。例如,文献[87]利用 PCA 精简掉了次要评估指标,确定了坡面特征是影响黄土沟谷发育的重要因子,但是得到指标的可解释性降低,而指标定权的一个重要目标就是确定各指标的对抗干扰能力及在效能评估中所起作用的大小,可解释性降低,不利于该目标的实现。文献[88]又提出了基于改进 PSO 算法的卫星星座优化设计方法,该方法适用于低轨遥感卫星星座设计,满足了高时间分辨率的要求,但当判别指标增多时,模型最优化问题尚未解决,所得结果易陷入局部最优。随后,文献[89]提出了一种基于 FL 的地磁图适配性分析方法,通过主观选择隶属函数来完成属性决策,提高了水下自主航行器的导航精度,但忽略了隶属函数本身的不确定性;而 RS 能从信息不确定性的角度刻画数据间的依赖关系,但只能处理离散属性集。因此,RS 与 FL 具有互补性,例如,文献[90]提出了一种基于模糊粗糙集(fuzzy rough sets, FRS)的作战效能评估方法,将数据集合从离散型变量推广至连续性变量,建立了卫星导航系统作战效能评估指标体系,给出了效能评估的决策规则,兼顾了影响因素的不确定性度量。

RF 性能优异,能解决回归和分类问题,对评估数据中的异常值和噪声具有很好的容忍度。例如,文献[91]提出了一种基于 RF 回归的闪烁指数预测模型,与传统电离层幅度闪烁指数计算方法相比,RF 回归模型预测得到的闪烁指数相关性更强、精度更高;文献[92]提出了基于 RF 的雷达智能抗欺骗干扰方法,该方法不必对信号参数进行估计、计算复杂度低,实验过程中干扰识别率均能达到 90% 以上。然而,上述研究运用 RF 时要求样本完整,而评估过程中常常因为暂时无法获取、人为因素缺失、设备故障、系统实时性要求较高等

造成指标量测值的缺失,从而降低RF度量评估指标贡献度的准确性,进而导致结果不可信。云模型常针对定性概念,能反映其自身具有的不确定性,并揭示客观事物的模糊性与随机性的关联,多用于机械工程[93]、网信领域[94]中复杂系统的综合评估与属性决策。例如,文献[95]提出了一种基于云模型的GNSS接收机抗干扰性能评估方法,通过计算云模型中综合评价云与各标准评价云之间的相似度大小获取最终评估结果,实现了对多个接收机抗干扰性能的准确有效评估。文献[94]结合权值,利用云模型将专家对指标的模糊语言评估进行定量转换得到评估值,提出了基于云模型的GNSS欺骗干扰效能评估方法,该方法能有效削弱评估存在的不确定问题。然而,上述研究多采用主观的单步式估计方法建立云模型的随机变量,包括数字特征,却忽略了云滴是通过两次随机过程产生,得到的结果既不能降低影响因素的不确定性,也未能建立稳定的双向认知。

综上,现有效能评估方法中,FRS与RF对解决导航领域相关问题具有更好的定权效果。

3.1.2 *方案择优方法*

卫星导航对抗效能评估面临多重不确定性挑战,这些不确定性主要源于电磁环境的动态复杂性、对抗策略的多维性、信息来源的多样性以及专家判断的主观认知差异性,具体表现为模糊性、随机性与动态性并存。受此影响,传统评估方法往往难以在不同对抗场景下得出合理且具有普适性的结果。为突破上述局限,实现复杂对抗环境下的有效寻优,必须立足实际,构建效能评估方法,并系统设置涵盖多种对抗方案及其组合的多样化测试场景。唯有通过这种多场景、多方案的对比与验证,才可能获得可信的效能评估结果。

卫星导航对抗是一种不完全信息的多属性决策问题,而已有多属性决策方法,例如理想近似法(technique for order preference by similarity to an ideal solution, TOPSIS),在导航安全风险评估、网络安全抗干扰能力、信息安全风险分析、预警飞行系统探测等领域的效能评估研究中得到了广泛应用,确定了复杂场景下的最优方案,完成了多属性决策研究。在此基础上,文献[96]进一步分析了TOPSIS在贫信息时存在的数据波动变化大、难以寻求其典型分布规律、不能直接反映指标序列变化趋势等缺陷,并引入区间分析的方法,提出了基于熵-TOPSIS方法的分发决策算法,结果表明,所提方法能很好地进行导航空间信息智能分发决策;文献[97-98]采用FL改进了TOPSIS,分别实现了传感器网络环境下车辆导航的模糊多属性决策,以及导航知识管理解决方案的择优排序。但上述研究在利用改进方法得到了方案排序结果后,没有进一步开展动静态效能评估分析,得到的结果既无法深入验证最优方案的更优性,也无法最大程度上掌握装备性能与实施效果,不利于生产方按需升级性能、决策者按需调控策略。

GRA是一种多属性决策方法,文献[84]基于欧氏距离提出了一种求解灰色关联度的新型评估方法,解决了机枪作战效能评估时所设方案与理想方案区分度不高的问题;文献[99]又利用GRA改进了模糊决策图,实现了机械设计方案的有效评价,解决了模糊数学在信息不足时未能反映指标序列变化趋势的问题。在此基础上,文献[100]采用GRA方法评估了BDS抗干扰性能的室内测试系统,提出了电磁干扰环境下北斗卫星定位抗干扰策略,但没有对指标间影响关系的传递性展开进一步研究;文献[101]提出了双向绝对灰色关系分析的模型,弥补了传统GRA在获得指标间影响关系的直接传递性方面的缺陷,更有效地处理了项目中由不确定数据所表征的不确定系统。

由此可知,GRA是一种从系统角度分析贫信息的决策方法,能确定典型的分布式规则,反映在信息不充分时指标序列的变化趋势和指标间影响关系的传递性,在一定程度上弥补了TOPSIS决策时存在的局限。因此,为削弱TOPSIS等多属性决策方法的局限性,已有研究采用GRA-TOPSIS方法在复杂条件下选择最优方案,以兼顾评估对象在多维空间中的实际距离和各指标间的关联度。例如,文献[102]提出了GRA-TOPSIS方法来选择最优方案,解决了导航安全风险评估中废弃信息回收利用的难题;文献[103]在多威胁源构成的复杂水下环境中,也引入了GRA来强化TOPSIS,精准且高效地确立消磁策略集合,提升了消磁策略决策的准确性与稳定性。但它们仍未能解决文献[97-98]分析时提及的多属性决策模型的实际运用及获得结果的落地问题。

3.2 动态博弈方法

3.2.1 *博弈模型与盈利矩阵*

卫星导航对抗被视为一种动态博弈,故需要建立适用于卫星导航对抗效能评估研究的博弈模型。博弈模型的基本要素是参与者、纯策略空间及相应的盈利矩阵。(1)博弈模型的参与者:威

胁系统包括软毁伤,即单GNSS干扰源与多GNSS干扰源协同干扰技术及其相关设备;防护系统包括GNSS及其各组成部分的相应抗干扰技术等。两类系统构成了博弈的参与者,即干扰策略At_p和防护措施Df_q。(2)博弈模型的纯策略空间:威胁系统所包含的干扰策略和防护系统所采用的防护措施分别构成了其对应的纯策略空间,分别为$S_{\mathrm{At}}=\{\mathrm{At}_1,\mathrm{At}_2,\cdots,\mathrm{At}_p\}$和$S_{\mathrm{Df}}=\{\mathrm{Df}_1,\mathrm{Df}_2,\cdots,\mathrm{Df}_q\}$。(3)盈利矩阵:虽然参与者的目标和评估标准是对立的,但它们共享相同的度量,即盈利矩阵。其表达式为:

$$\boldsymbol{E}=\begin{array}{c}\begin{matrix}\mathrm{At}_1 & \mathrm{At}_2 & \cdots & \mathrm{At}_p\end{matrix}\\ \begin{bmatrix}e_{11} & e_{12} & \cdots & e_{1p}\\ e_{21} & e_{22} & \cdots & e_{2p}\\ \vdots & \vdots & \vdots & \vdots\\ e_{q1} & e_{q2} & \cdots & e_{qp}\end{bmatrix}\end{array}\begin{matrix}\mathrm{Df}_1\\ \mathrm{Df}_2\\ \vdots\\ \mathrm{Df}_q\end{matrix}\tag{1}$$

式中,e_{qp}表示在干扰策略At_p下防护系统选择防护措施Df_q对抗威胁的防护盈利值。盈利矩阵是博弈模型的核心要素,主要通过重建并量化盈利矩阵来完成博弈模型的改进,以建立适用于卫星导航对抗的动态博弈模型。

近年来,已有博弈模型较多,已被广泛用于雷达对抗和网络对抗的干扰效能评估。例如,文献[104]运用博弈理论,提出了一种通过博弈模型将干扰和抗干扰有效联系起来的评估方法,完成了对抗策略选择,实现了合成孔径雷达最优化;文献[105]提出了评估遮盖性干扰动态效能的方法,掌握了雷达对抗博弈策略,建立了博弈模型及盈利矩阵;在此基础上,文献[30,106]分别对信号博弈和进化博弈进行了改进,构建用于雷达对抗的博弈模型,实现了最优决策;文献[107]又开展了压制干扰下组网雷达功率分配的深度博弈研究,用于组网雷达功率的分配以及干扰机资源的优化,提高了智能体的学习效率与交互性能。此外,文献[108-109]基于不完全信息条件下的网络安全对抗,分别提出了具有学习机制和自主性的攻防博弈模型,以提升网络安全对抗效能及其对无人机群的攻击效果,并做出最优策略选择;考虑到参与者的理性可能是有限理性,相比于仅考虑参与者是完全理性的纳什均衡,其演化稳定均衡且具有更强的预测性和抗干扰能力,文献[110-111]相继提出了基于系统动力学和人工智能的标准博弈、演化博弈、随机博弈、不完全信息博弈模型等,并论述了4种博弈的多智能体学习方法,优化了最优策略选取;基于此,文献[112]通过深度学习改进了已有的博弈模型[105],加快生成对抗网络中的先进性能提升。

因此,虽然已有用于其他对抗领域的博弈模型及盈利矩阵较成熟,例如雷达、通信等领域的电子对抗,但它们不适用于评估卫星导航对抗效能,具体体现在:(1)GNSS干扰模式与其他类型干扰手段的性能参数存在显著差异,相应地,GNSS抗干扰所涉及的应用前端与终端体制、信息处理流程、评估对象以及接收协议与接收要素等也与其他类型对抗有所区别。然而,在更宏观的方法论层面,适用于其他电子对抗领域的评估原则,如系统性、动态性等原则,对于构建和完善卫星导航对抗的评估原则仍具有重要的借鉴意义。(2)卫星导航对抗更多地关注设备在复杂电磁环境下的定位、测速、时效及导航信息的可信性。综上,上述用于不同类型对抗的博弈模型推导的方程解在理论上是最优的,但其盈利矩阵不具备通用性,需建立适用于卫星导航对抗的博弈模型,例如文献[59]建立的卫星导航对抗的盈利矩阵$\boldsymbol{E}$。

3.2.2　FCA与ES

盈利矩阵是博弈模型的核心要素,提供了一个定义(或称为性能框架),量化盈利矩阵是完成盈利方程求解以及盈利结果确定的必要步骤。据此,文献[113]通过测试和仿真量化了可量测的性能评估指标,以量化盈利矩阵;文献[114]通过经验赋值完成了不可量测性能评估指标的量化工作,进而实现了盈利矩阵的量化。然而,由于经验赋值得到的结果具有不确定性,获得的量化盈利矩阵必然具有不可忽视的不确定性;此外,虽然卫星导航对抗被视为是GNSS用户终端与系统设施同GNSS干扰设备之间的对抗,但实际上对抗更是一种围绕大脑主客观意识的评估与决策。综上,在量化盈利矩阵的过程中要更加重视不可量测指标的量化准确性,但它们通常被忽视。

为了实现盈利矩阵的量化,本文首先需要关注可量测指标的量化精度。可行的方法有模糊数学[40],其中的FCA在一定程度上能消除可量测评估指标量化的主观与片面性,减少运算过程中的模糊性和随机性,得到较客观的量化结果。近年来,不少学者利用FCA开展欺骗干扰效果的量化评估研究。例如,文献[115]利用FCA对目标接收机进行了多GNSS欺骗干扰效果的评估,得到待选部署方案的综合评估结果,确定了最优方案;文献[116-117]则选取激光制导设备作为评估对象,运用FCA并通过外场实验分析及信号仿真

模拟,量化评估了被测设备的干扰效果;此外,为增强GNSS的安全防护能力、提高评估效率,文献[118-119]运用FCA及其改进方法,实现了GNSS多参数欺骗检测以及欺骗效果评估体系的优化约简。

本文重点关注如何提高不可量测指标的量化精度。ES是降低不可量测指标不确定性最具代表性的方法之一[120],文献[121]对ES方法进行了改进,构建了可解释的置信规则库,降低了ES本身存在的不确定性;文献[122]利用ES在灵活性和可解释性方面的优势,提出了一种启发式模糊ES,实现了滤波器高效地自动调优。虽然这些研究利用ES为用户带来了积极效益,但该方法需要大量的先验信息且更新困难,导致其难以被推广。灰色系统理论包括绝对灰色关联和相对灰色关联,是建立在不完全信息基础上的不确定性系统,该方法对样本量没有严格要求,不遵循任何分布,可减少ES对大量先验信息的依赖[123]。考虑到卫星导航对抗的特征及其动态性与多维性,后续通过引入灰色系统理论来改进ES,也是一种可行思路。

3.2.3 数学规划与启发式算法

前人已对如何有效求解由盈利矩阵推导出的盈利方程并开展最优决策进行了相关研究。鉴于求解由盈利矩阵推导出来的盈利方程是一个数学规划问题,文献[40,124]利用可求解任意阶线性方程的线性规划方法建立了盈利方程,并分别评估了GNSS欺骗干扰效果和网络攻击效果。然而,该盈利方程得到的解既容易陷入局部最优,又容易无解,其有效性无法得到保障,选出的最优防护措施及求得的效能评估结果的可靠性也无法保证。因此,相关研究者在后续需关注如何求解盈利方程,以确保获得全局最优解。

随着信息智能技术的发展,已有研究多采用数值计算方法(包括蒙特卡洛等)和仿生智能算法(又称启发式算法,包括PSO等)求解盈利方程。其中,蒙特卡洛算法是利用随机数来解决计算问题,得到的解是近似解;而属于仿真智能算法的PSO、遗传算法(genetic algorithm, GA)、模拟退火算法虽然得到的解也是近似解,但它们均比蒙特卡洛算法的应用领域更广泛。对比3种算法可知:模拟退火算法更适用于解决非线性优化问题,其局部搜索能力强,但收敛速度慢,执行时间长,算法性能与初始值有关且参数敏感;GA适用于离散和连续问题的求解,能对复杂问题进行全局搜索和优化,并行性强且具有自适应性,但对空间最优解的逼近能力较弱,影响执行效率;PSO则对空间最优解的逼近能力很强,收敛速度更快,求解精度更高,却易陷入局部最优,局限于解决连续问题[125]。因此,GA和PSO更适用于求解盈利方程,且两者具有互补性。

此外,已有研究也常利用GA、PSO对线性规划方法进行优化,从而来解决数学规划问题。例如,文献[126]有效地利用GA求解了多目标数学规划问题;文献[127]开发了一种混合GA来优化线性规划模型,并揭示了GA收敛速度较慢的现象;文献[128]使用PSO解决了一个关于提取最准确几何信息的数学规划问题,并揭示了PSO易陷入局部最优的现象;文献[129]提出了一种将两种启发式算法组合的混合进化算法,即GA-PSO,解决了有关雷达干扰效果评估的数学规划问题,获得了全局最优策略。但GA-PSO每次收敛得到的最优解及其模型参数均有细微差异,如何稳定地获得全局最优解、缩短收敛时间并提高收敛效率,值得深入研究。

3.2.4 机器学习及其相关算法

误差反向传播神经网络(back propagation neural network, BP-NN)在弱化人为因素和不确定因素方面十分有益,能解决多指标综合的客观评估问题。考虑到卫星导航对抗的整体系统是一个复杂且多小系统的非线性大系统,利用BP-NN不仅能建立权重的学习机制,还能对变量进行贡献度分析并给出简化模型。因此,依靠BP-NN强大的自学习能力以及交互式的客观评估方式,可最终确定己方导航系统的最优措施与防护获益。

已有学者对BP-NN开展大量研究,文献[130]指出BP-NN方法在应用中遇到的最大问题是不能提供解析表达式,得到的结果不能解释为一种回归系数,也不能用来分析因果关系。同时,由于实际输出与期望输出之间存在误差,BP-NN事前要进行反复不断的训练来修正它们,直至将误差控制在给定标准的范围内。文献[131]指出BP-NN方法的初始权值和阈值是随机产生的,而在学习过程中各层的权值和阈值又会经过前向传播与误差反向传播来调整,随机误差会对模型的性能及可持续稳定造成较大影响,致使获得的模型参数趋于局部最优;而本文的最终目标是决策,全局最优和盈利最大是完成决策的评判条件。文献[132]指出该方法需大量的训练样本,应用范围有限;而本文探讨的研究方向本质

上属于大样本问题,但该方向已有的公开数据集(即评估指标的测量值)难获得,仅靠笔者几年的理论方法研究以及从相关部门采集的仿真数据分析。因此,本文探讨的研究方向实际上仅能归为小样本问题。

1)针对文献[130]所提的BP-NN存在的不足:数据包络分析(data envelopment analysis, DEA)能确定输入与输出间关系的解析表达式,其优点是无须任何权重假设,每一输入与输出的权重均是由决策单元的测量值求得的优化权重;但其缺点是指标规模受限,规模过大易使得结果失真。故BP-NN与DEA间存在优势互补,两种评估方法的优缺点如表1所示。文献[133]也引入DEA来改进BP-NN,并选取分项指标与综合指标分别作为BP-NN的输入与输出层,挖掘了两类指标间的交互关系并完成了模型训练。

表1　两种不同评估方法的优缺点

Table 1　Advantages and Disadvantages of Two Different Evaluation Methods

评估方法	原理	优点	缺点	应用于卫星导航对抗效能评估的优势
DEA	最优线性规划思想	无需提前设定参数,避免确定各指标权重带来的主观性	对指标规模存在限制,指标个数过多会使结果失真	DEA与BP-NN间存在优势互补,引入DEA可改进BP-NN存在的不能解析表达、所得结果无法分析因果关系等问题
BP-NN	非线性逐渐逼近目标值	强大的数据处理与自学习能力,可根据给定规则进行自学并纠正误差并逼近目标值	需要事前给定一个对应规则	

2)针对文献[131]所提的BP-NN存在的不足,比对现有非线性全局最优算法,包含基因GA、磷虾群算法(krill herd algorithm, KHA)、目标群搜索算法、模拟退火算法、模拟原子跃迁反演法、同伦反演法、PSO等。其中,KHA在位置更新处引入了较多的自适应参数,能够更有效地平衡全局搜索和局部搜索,不会轻易陷入局部最优,但多参数也在一定程度上增加了算法复杂度。为尽可能提高BP-NN的性能并降低其不稳定性,文献[134]采用了KHA优化BP-NN中的权值、阈值及迭代次数等模型参数,提高了评估与预测的可信度。

3)针对文献[132]所提的BP-NN存在的不足,处理小样本问题的方法大致分为两类:一类是贝叶斯估计方法,文献[135-136]指出该类方法得到广泛应用的原因主要是其能够利用先验信息,但其先验概率又通常取决于假设,假设模型又包括很多种,导致预测效果不佳;而先验结果又常用于决定后验概率,从而决定分类,因此,得到的分类结果也易存在错误率。另一类是Bootstrap方法,分为频率派自举法即经典自举法(frequency bootstrap, FB),以及贝叶斯自举法(bayesian bootstrap, BB),该类方法完全依赖实验样本本身的信息,无需主观假设和额外信息[137]。文献[138]指出FB更简单有效,更适用于小样本扩充问题,而BB更适用于参数估计问题;文献[139]进一步指出BB对原始样本信息的依赖性更强,当原始样本容量不足时易导致估计结果不准确,可信度降低。综上,考虑到现有GNSS干扰与抗干扰性能评估研究的小样本特性,文献[140]采用了更简明的FB对训练样本进行扩充,改进BP-NN以弥补其在小样本类型研究的不适用。

鉴于上述局限,相关研究者在后续可以聚焦于如何综合引入DEA、KHA和Bootstrap等方法来有效地改进BP-NN回归算法,以确定能够稳定全局最优,弱化不确定性的盈利结果。

4　思考与建议

4.1　现有研究局限

1)针对卫星导航对抗评估指标体系的构建,已有研究存在以下不足:(1)评估对象不是卫星导航对抗的完整系统,没有提出体系化的构建原则与完善的评估标准;(2)部分研究在追求全面的同时又存在概念化和理论性强的特征,所得成果无法辅助决策;(3)针对卫星导航对抗性能评估指标体系构建的公开研究很少,致使缺乏较完备的评估指标体系。

2)针对卫星导航对抗性能评估,已有研究存在以下不足:(1)内容分配不均衡,对GNSS干扰与用户端抗干扰等热点重复研究,缺少对多干扰源全域协同干扰、GNSS系统端抗干扰等方向的研究,影响性能评估结果的准确性与最优决策结论的可信度。(2)针对系统端抗干扰能力包含的部分服务性能与应用功能,已有研究完成了模型建立,但模型多适用于无干扰情形的性能分析,无法完成多变干扰场景的系统端抗干扰性能评估,也没有给出综合能力评估方法,无法总结分

项性能变化对综合能力的影响并辅助优化性能与设施维护。

3)实现卫星导航对抗性能评估向效能评估的高效过渡有以下局限:(1)评估与决策本身存在不可避免的不确定性;(2)已有指标定权方法的主观性强,且得到的权重没有兼顾指标相对评估目标的重要性和贡献度;(3)传统效能评估方法忽略备选方案择优与综合效能评估间的相关性,得到的结果仅反映方案优先级排序,无法综合验证择优结果,不利于后续动态博弈的推进。因此,需要有效的多属性决策方法来解决上述局限,而已有相关方法,如文献[90]等并没有全面兼顾并解决上述3个局限。

4)博弈理论在雷达对抗等其他对抗领域的效能评估中已有广泛应用,但在卫星导航对抗领域,其适用性面临以下主要局限:(1)现有博弈模型在卫星导航对抗效能评估中的应用尚不广泛,缺乏针对性研究;(2)现有模型缺乏普适性,亟待改进以构建适用于卫星导航对抗的核心模型要素,并实现这些要素的有效量化;(3)基于盈利矩阵推导的盈利方程易陷入局部最优,如何稳定收敛至全局最优解,并在对抗过程中动态调控最优措施,是亟待解决的关键问题;(4)面向不同信息对抗情形的动态博弈研究缺失,导致所提方法难以落地实践。因此,有必要专门开展卫星导航对抗动态博弈效能评估方法研究。

综上,考虑到相互作用和具有延续性的性能评估与效能评估相继开展即可完成卫星导航对抗性能与效能评估理论方法研究,但已有研究多集中在单一干扰源、单一场景的分项性能评估,评估视角单一,未针对多对抗场景与多干扰样式开展综合评估与最优决策,致使存在已有指标体系零散、性能评估模型不完善、权重可信度低、效能评估方法不适用、动态复杂性与模糊性及随机性未能统筹削弱、缺少验证反馈环节等问题,最终导致性能评估无法有效支撑效能评估,也无法保障己方导航系统的防护效益。卫星导航对抗性能与效能评估理论方法研究存在的不足如图8所示。



图8 卫星导航对抗性能与效能评估理论方法研究存在的不足

Fig. 8 Research Gaps of Theoretical Methods for Performance and Effectiveness Evaluation of Satellite Navigation Countermeasures

4.2 研究推进思考

1)针对卫星导航对抗性能评估指标体系构建的公开研究不多且零散片面的问题,如何设定评估标准以及基于标准来构建出相对合理完备的评估指标体系,为后续研究奠定基础。

2)针对卫星导航对抗性能评估视角单一、模型不完善和指标量化程度低的问题,如何改进并提出评估模型,完成性能检测、量化比对和综合评估,以实现GNSS干扰能力、用户端与系统端抗干扰能力的性能评估以及装备优化升级。

3)针对单一干扰源干扰范围小且易被探测和摧毁、多GNSS干扰源全域协同干扰研究少的问题,如何协同部署多干扰源、制定优化部署方案、评估其干扰效果并验证部署的合理性,以更好地干扰威胁性目标,从而进一步提升己方GNSS的安全防护能力。

4)针对效能评估方法研究中已有定权方法得到的权重主观性过强等问题,如何在考虑评估目标的前提下兼顾定权的主客观性以及指标对评估目标的贡献度量,提升定权结果的可信度,为后续开展包含多属性决策与动态博弈的效能评估研究奠定基础。

5)针对性能评估无法有效支撑效能评估的问题,性能评估模型得到的海量结果如何高效地应用于卫星导航对抗多属性决策,以实现性能评估向最优决策的高效过渡。

6)针对现有效能评估方法不完全适用的问题,如何重建并量化卫星导航对抗动态博弈模型,稳定地获得全局最优解,实现不同对抗情形的动态博弈,完成最优措施调控与验证,最大化己方GNSS对抗干扰威胁的防护获益。

结合以上6条,针对已有指标体系零散、评估视角单一、性能评估模型不完善、指标权重可信度低、已有效能评估方法不适用、性能评估无法有效支撑效能评估等难题,需要围绕卫星导航对抗性能评估指标体系构建、相关性能评估方法研究、关键效能评估方法研究,开展卫星导航对抗性能与效能评估理论与方法研究。研究内容可包含4个方面:(1)构建卫星导航对抗性能评估指标体系,为性能评估方法研究奠定体系基础;(2)基于性能指标体系,针对卫星导航对抗涉及的能力,包括单GNSS干扰源干扰能力与多GNSS干扰源协同干扰效果、用户端与系统端抗干扰能力,分别提出并完善分项性能与综合能力评估方法,为顺利开展效能评估研究奠定基础;(3)基于性能评估结果,完成效能评估,包括指标权重确定、备选方案择优及其效能评估验证的多属性决策,以及最优措施调控与防护盈利获得的动态博弈,保障以BDS为核心的GNSS安全应用,提升其安全防护能力;(4)建立验证反馈环节,围绕多种评判指标与验证规则实现模型可靠性、结果置信度及方法更优性的验证与反馈。

4.3　未来发展建议

除了上述研究推进思考之外,研究依然存在以下需要完善的内容以及修正的方向:

1)进一步梳理与深入研究卫星导航对抗性能评估指标体系和性能评估方法。针对卫星导航对抗性能评估体系的研究,涉及到的指标过广,期望面面俱到的后果就是无法深入研究并实施有效评估,致使性能评估模型梳理并改进起来相当复杂。因此,指标体系需要从多角度构建,例如构建围绕GNSS基本组成的评估指标体系以及基于博弈视角的评估指标体系等,性能评估方法则聚焦于GNSS各组成部分性能在面对干扰威胁和安全情形下的评估结果量化比对。前人完善了分项性能与综合能力评估方法,但体系分层、分级需更深入,所提理论方法的推广性与普适性都需要进一步探讨。故未来应站在宏观角度,在兼顾特定技术及热点发展的前提下给出评估标准,完成依托顶层逻辑的网络化评估体系建设,研究思路如图9所示。

2)当前仿真结果较多,实测实验有待补充。前人开展了欺骗定位精度、欺骗成功率以及最大干扰作用距离的外场实验,以及分布式压制干扰效果与压制辅助的生成式欺骗干扰效果的外场实验,但仍有大量的分项指标可以开展实测实验,例如动态测量精度、伪距修正能力等指标。未来可先补充真实场景需要考虑的因素或条件,对未兼顾的指标开展实测实验,解决仿真实验的结果可靠性不足的问题。随后,将获得的性能评估结果作为最优决策实现的输入量,用于盈利矩阵的量化、盈利方程的求解、盈利结果的获得,完成卫星导航对抗动态博弈的效能评估,根据干扰策略动态调控最优防护措施,最大化己方导航系统对抗干扰威胁的防护获益,实现从效能评估结果、动态博弈模型至性能评估方法的闭环反馈。

3)开发一套卫星导航对抗性能与效能评估软件,以实现实时评估与最优决策。前人围绕卫星导航对抗性能评估指标体系、相关性能评估方法、关键效能评估方法等做了较多工作,在仿真过程中依据指标的评估模型编写了指标的仿真程序。此外,在实验过程中,采集到了各种类型的原始数据,从数据预处理到指标定权、备选方案择优、最优决策实现等效能评估研究,结合合适的效能评估方法编写了部分小程序,用于求解盈利方程并获得全局最优解的混合进化算法。但这些小程序都是串联关系,故未来可基于所提模型与方法,围绕指标体系与评估原则,将代码串联起来,以开发出卫星导航对抗效能评估软

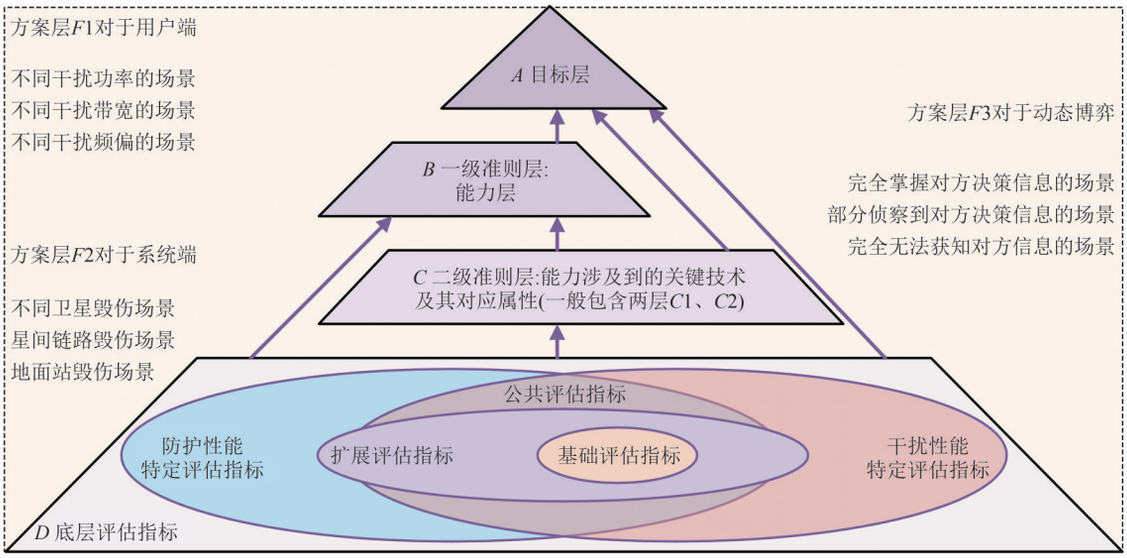


图9 依托顶层逻辑的网络化评估体系研究思路

Fig. 9 Research Ideas of Networked Evaluation System Based on Top-Level Logic

件,包含完整的性能评估与关键的效能评估软件,实现实时评估、最优决策的最终目标。

4)完成典型对抗场景的理论方法验证与优化、不同型号装备的评估结果对比与升级。为验证评估方法的有效性、普适性等优势,未来首先可选取不同型号、不同功能的GNSS装备、卫星、地面站,以及具备不同样式、不同强度干扰能力的GNSS干扰源。然后,依据不同装备的属性特征及其所处的工作环境设置多组卫星导航攻防对抗场景,开展实测实验,参与实际演习,获得原始数据。最后,将原始数据输入至自研的评估软件产品,再输出性能评估结果、最优防护措施、效能评估结果,通过不同型号装备或对抗场景间评估结果的量化对比,选取结果最优的场景,实现实时评估与最优决策,进一步提高结果可信度与评估效率,完成软件升级与模型迭代,扩大所提理论方法的验证及优化空间。

5 结 语

GNSS是保障现代社会大系统实时动态安全运行的战略基础资源,由于系统本身的脆弱性和易干扰性,卫星导航对抗逐渐成为导航领域争夺的焦点。为有效应对不断增长的安全威胁并推进卫星导航对抗相关技术的发展、相关设备的研发与测试,卫星导航对抗评估研究应运而生并逐渐成为热点,该研究的有效实现不仅有利于GNSS内部系统的更新与外部设施的维护、服务性能进一步优化,还能扩大系统防护获益,最终提升其安全防护能力。而导航工程、电子通信、网络安全、系统工程等学科在此领域的相关成果提供了许多可借鉴的发展经验。本文对这些经验进行了梳理和总结,通过对照分析和推进思考,对卫星导航对抗性能与效能评估研究发展提出了4个方面的改进建议。经过最近二三十年的发展,中国在该研究领域取得了进展,积累了研发经验,但面临的挑战也显而易见,需要不断推陈出新,所提发展建议也期望为相关部门下一步工作部署提供参考。

参考文献

[1] HUMPHREYS T E. Statement on the Vulnerability of Civil Unmanned Aerial Vehicles and Other Systems to Civil GPS Spoofing[R]. Austin: University of Texas at Austin, 2012.

[2] LIU Z, YUAN Y H, ZHAO B, et al. Trust Assessment Under the Integrated Air-Space-Ground Network Environment[J]. *Tsinghua Science and Technology*, 2023, 28(2): 405-420.

[3] 陆红亚, 王倩, 陈悦, 等. 美太空军事战略发展分析及对空间安全的影响研究[J]. 现代防御技术, 2023, 51(3): 31-38.
LU Hongya, WANG Qian, CHEN Yue, et al. Analysis of the Development of U. S. Space Military Strategy and Its Impact on Space Security[J]. *Modern Defence Technology*, 2023, 51(3): 31-38.

[4] DUAN T, DINAVAHI V. Starlink Space Network-Enhanced Cyber-Physical Power System[J]. *IEEE Transactions on Smart Grid*, 2021, 12(4): 3673-3675.

[5] 余南平, 严佳杰. 国际和国家安全视角下的美国

"星链"计划及其影响[J]. 国际安全研究, 2021, 39(5): 67-91.
YU Nanping, YAN Jiajie. The US Starlink Program and Its Implications: From the Perspective of International and National Security[J]. *Journal of International Security Studies*, 2021, 39(5): 67-91.

[6] SHEPARD D P, HUMPHREYS T E, FANSLER A A. Evaluation of the Vulnerability of Phasor Measurement Units to GPS Spoofing Attacks[J]. *International Journal of Critical Infrastructure Protection*, 2012, 5(3/4): 146-153.

[7] 边少锋, 胡彦逢, 纪兵. GNSS欺骗防护技术国内外研究现状及展望[J]. 中国科学: 信息科学, 2017, 47(3): 275-287.
BIAN Shaofeng, HU Yanfeng, JI Bing. Research Status and Prospect of GNSS Anti-Spoofing Technology[J]. *Scientia Sinica* (*Informationis*), 2017, 47(3): 275-287.

[8] 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.

[9] 王月. GNSS欺骗干扰效能评估指标与方法研究[D]. 郑州: 信息工程大学, 2020.
WANG Yue. Evaluation Indexes and Evaluation Methods of GNSS Spoofing Efficacy[D]. Zhengzhou: Information Engineering University, 2020.

[10] 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, 中国哈尔滨, 2018.
LIU Peng, WANG Dun, CHEN Yaohui, et al. Research Status and Development Trend of GNSS ElectronicWarfare [C]//The 9th China Satellite Navigation Academic Annual Conference, Harbin, China, 2018.

[11] 刘富, 舒展, 谢维华. 卫星导航对抗能力现状及发展趋势[J]. 导航定位学报, 2020, 8(6): 1-5.
LIU Fu, SHU Zhan, XIE Weihua. Status and Development Trends of Satellite Navigation Countermeasure Capability[J]. *Journal of Navigation and Positioning*, 2020, 8(6): 1-5.

[12] WANG H, CHANG Q, XU Y, et al. Adaptive Narrow-Band Interference Suppression and Performance Evaluation Based on Code-Aided in GNSS Inter-Satellite Links[J]. *IEEE Systems Journal*, 2020, 14(1): 538-547.

[13] RAJIVAN P, COOKE N. Impact of Team Collaboration on Cybersecurity Situational Awareness[M]// LIU P, JAJODIA S, WANG C. Theory and Models for Cyber Situation Awareness. Cham: Springer International Publishing, 2017: 203-226.

[14] 凌海风, 李瑞, 柏林元, 等. 俄罗斯反无人机装备发展现状及启示[J]. 国防科技, 2023, 44(3): 81-87.
LING Haifeng, LI Rui, BAI Linyuan, et al. Current Developments and Implications of Russian Anti-UAV Equipment[J]. *National Defense Technology*, 2023, 44(3): 81-87.

[15] 刘纪平, 王琢璐, 徐胜华, 等. 人工智能时代下的应急测绘[J]. 武汉大学学报(信息科学版), 2025, 50(6): 1029-1041.
LIU Jiping, WANG Zhuolu, XU Shenghua, et al. Emergency Surveying and Mapping in the Era of Artificial Intelligence[J]. *Geomatics and Information Science of Wuhan University*, 2025, 50(6): 1029-1041.

[16] CECCATO M, FORMAGGIO F, TOMASIN S. Spatial GNSS Spoofing Against Drone Swarms with Multiple Antennas and Wiener Filter[J]. *IEEE Transactions on Signal Processing*, 2020, 68: 5782-5794.

[17] PSIAKI M L, HUMPHREYS T E. GNSS Spoofing and Detection[J]. *Proceedings of the IEEE*, 2016, 104(6): 1258-1270.

[18] MOSAVI M R, BAZIAR A R, MOAZEDI M. De-Noising and Spoofing Extraction from Position Solution Using Wavelet Transform on Stationary Single-Frequency GPS Receiver in Immediate Detection Condition[J]. *Journal of Applied Research and Technology*, 2017, 15(4): 402-411.

[19] GAO Y J, LV Z W, ZHANG L D. Asynchronous Lift-off Spoofing on Satellite Navigation Receivers in the Signal Tracking Stage[J]. *IEEE Sensors Journal*, 2020, 20(15): 8604-8613.

[20] 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): 28.

[21] 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.

[22] CAPARRA G, CECCATO S, LAURENTI N, et al. Feasibility and Limitations of Self-Spoofing Attacks on GNSS Signals with Message Authentication [C]//The 30th International Technical Meeting of the Satellite Division of the Institute of Navigation, Portland, USA, 2017.

[23] GUO Y, WU M P, TANG K H, et al. Covert Spoofing Algorithm of UAV Based on GPS/INS-In-

tegrated Navigation[J]. *IEEE Transactions on Vehicular Technology*, 2019, 68(7): 6557-6564.

[24] 葛悦涛, 薛连莉, 李婕敏. 美国陆军PNT能力发展趋势分析[J]. 导航定位与授时, 2019, 6(2): 12-18.
GE Yuetao, XUE Lianli, LI Jiemin. Analysis of the Development Trends of US Army PNT Capability [J]. *Navigation Positioning and Timing*, 2019, 6(2): 12-18.

[25] 杨宁虎, 刘春保. 卫星导航系统赛博安全技术发展[J]. 卫星应用, 2018(9): 27-31.
YANG Ninghu, LIU Chunbao. Development of Cybersecurity Technology in Satellite Navigation System[J]. *Satellite Application*, 2018(9): 27-31.

[26] TUGNAIT J K. Pilot Spoofing Attack Detection and Countermeasure [J]. *IEEE Transactions on Communications*, 2018, 66(5): 2093-2106.

[27] SEO S H, LEE B H, IM S H, et al. Efficient Spoofing Identification Using Baseline Vector Information of Multiple Receivers[J]. *GPS Solutions*, 2018, 22(4): 115.

[28] 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.

[29] TANIL C, KHANAFSEH S, PERVAN B. Kalman Filter-Based INS Monitor to Detect GNSS Spoofers Capable of Tracking Aircraft Position[C]// IEEE/ION Position, Location and Navigation Symposium, Savannah, USA, 2016.

[30] ELDOSOUKY A, FERDOWSI A, SAAD W. Drones in Distress: A Game-Theoretic Countermeasure for Protecting UAVs Against GPS Spoofing [J]. *IEEE Internet of Things Journal*, 2020, 7(4): 2840-2854.

[31] 胡志刚. 北斗卫星导航系统性能评估理论与试验验证[D]. 武汉: 武汉大学, 2013.
HU Zhigang. BeiDou Navigation Satellite System Performance Assessment Theory and Experimental Verification[D]. Wuhan: Wuhan University, 2013.

[32] 李毅. 大数据战略背景下警务保障效能提升策略研究[D]. 北京: 中国人民公安大学, 2020.
LI Yi. Research on the Strategy of Improving the Efficiency of Police Support Under the Background of Big Data Strategy[D]. Beijing: Chinese People's Public Security University, 2020.

[33] 董铭涛, 程建华, 赵琳, 等. 惯性组合导航系统性能评估方法研究进展[J]. 自动化学报, 2022, 48(10): 2361-2373.
DONG Mingtao, CHENG Jianhua, ZHAO Lin, et al. Perspectives on Performance Evaluation Method for Inertial Integrated Navigation System[J]. *Acta Automatica Sinica*, 2022, 48(10): 2361-2373.

[34] 张军涛, 李尚生, 王旭坤. 基于灰色关联-模糊综合评判的雷达抗干扰性能评估方法[J]. 系统工程与电子技术, 2021, 43(6): 1557-1563.
ZHANG Juntao, LI Shangsheng, WANG Xukun. Method of Radar Anti-Jamming Performance Evaluation Based on Grey Correlation-Fuzzy Comprehensive Evaluation[J]. *Systems Engineering and Electronics*, 2021, 43(6): 1557-1563.

[35] ZHOU W L, LV Z W, DENG X, et al. A New Induced GNSS Spoofing Detection Method Based on Weighted Second-Order Central Moment[J]. *IEEE Sensors Journal*, 2022, 22(12): 12064-12078.

[36] SHANG X Y, SUN F P, WANG D M, et al. GNSS Spoofing Detection Based on Multicorrelator Distortion Monitoring[J]. *GPS Solutions*, 2023, 27(2): 94.

[37] LEE K, LEE J. Design and Evaluation of Symmetric Space-Time Adaptive Processing of an Array Antenna for Precise Global Navigation Satellite System Receivers[J]. *IET Signal Processing*, 2017, 11(6): 758-764.

[38] 王月, 郝金明, 刘伟平. 卫星导航欺骗干扰装备效能评估方法[J]. 兵工学报, 2020, 41(1): 108-118.
WANG Yue, HAO Jinming, LIU Weiping. Evaluation Method for Effectiveness of GNSS Spoofer[J]. *Acta Armamentarii*, 2020, 41(1): 108-118.

[39] 王月, 郝金明, 刘伟平. 基于灰色关联分析和模糊综合评判的GNSS欺骗干扰效能评估[J]. 电子学报, 2020, 48(12): 2352-2359.
WANG Yue, HAO Jinming, LIU Weiping. GNSS Spoofing Effectiveness Evaluation Based on Grey Relational Analysis and Fuzzy Comprehensive Assess Ment[J]. *Acta Electronica Sinica*, 2020, 48(12): 2352-2359.

[40] WANG Y, HAO J M, LIU W P, et al. Dynamic Evaluation of GNSS Spoofing and Jamming Efficacy Based on Game Theory[J]. *IEEE Access*, 2020, 8: 13845-13857.

[41] YANG Y X, DING Q, GAO W G, et al. Principle and Performance of BDSBAS and PPP-B2b of BDS-3[J]. *Satellite Navigation*, 2022, 3(1): 5.

[42] JIANG C, ZHANG S B, LI H, et al. Performance Evaluation of the Filters with Adaptive Factor and Fading Factor for GNSS/INS Integrated Systems [J]. *GPS Solutions*, 2021, 25(4): 130.

[43] 陈雷雨, 周志杰, 唐帅文, 等. 融合多元信息的武

器装备性能评估方法[J]. 系统工程与电子技术, 2020, 42(7): 1527-1533.
CHEN Leiyu, ZHOU Zhijie, TANG Shuaiwen, et al. Weapon Equipment Performance Evaluation Method with Multi-information Fusion[J]. *Systems Engineering and Electronics*, 2020, 42(7): 1527-1533.

[44] SHAFIEE E, MOSAVI M R, MOAZEDI M. Detection of Spoofing Attack Using Machine Learning Based on Multi-layer Neural Network in Single-Frequency GPS Receivers[J]. *Journal of Navigation*, 2018, 71(1): 169-188.

[45] 孙兆妍, 王新龙. SINS/GPS松组合与紧组合导航系统抗干扰性能比较与验证[J]. 航空兵器, 2014(4): 31-35.
SUN Zhaoyan, WANG Xinlong. Comparison and Demonstration of Interference Immunity of SINS/GPS Loosely Coupled and Tightly Coupled Integrated Navigation System[J]. *Aero Weaponry*, 2014(4): 31-35.

[46] 邓力源, 杨萍, 刘卫东, 等. 基于证据理论层次分析法的云贝叶斯网络在预警雷达毁伤效果评估中的应用[J]. 兵工学报, 2022, 43(4): 814-825.
DENG Liyuan, YANG Ping, LIU Weidong, et al. Application in Damage Effect Evaluation of Early Warning Radar of Cloudy Bayesian Network Based on Dempster-Shafer/Analytic Hierarchy Process Method[J]. *Acta Armamentarii*, 2022, 43(4): 814-825.

[47] 刘建业, 孙应统, 邢瑞阳, 等. 面向多任务的预警卫星系统效能评估[J]. 上海航天, 2019, 36(1): 10-15.
LIU Jianye, SUN Yingtong, XING Ruiyang, et al. Effectiveness Evaluation of Early Warning Satellite System for Multi-missions[J]. *Aerospace Shanghai*, 2019, 36(1): 10-15.

[48] 张伟, 何晶, 谢晓伟, 等. 联合战场导航对抗仿真评估系统设计与实现[J]. 系统工程与电子技术, 2022, 44(10): 3182-3189.
ZHANG Wei, HE Jing, XIE Xiaowei, et al. Design and Implementation of Simulation Evaluation System for Joint Battlefield Navigation Countermeasure[J]. *Systems Engineering and Electronics*, 2022, 44(10): 3182-3189.

[49] WANG Y, SUN F P, HAO J M, et al. Evaluation of Global Navigation Satellite System Spoofing Efficacy[J]. *Journal of Systems Engineering and Electronics*, 2022, 33(6): 1238-1257.

[50] 苏珂, 吴忠望, 焦国强, 等. GPS导航战综述:进展与启示[J]. 全球定位系统, 2024, 49(6): 127-134.
SU Ke, WU Zhongwang, JIAO Guoqiang, et al. Review of GPS Navigation Warfare: Progress and Revelation[J]. *GNSS World of China*, 2024, 49(6): 127-134.

[51] 毛虎, 吴德伟, 卢虎. GNSS信号体制抗干扰性能分析[J]. 电子科技大学学报, 2020, 49(4): 575-583.
MAO Hu, WU Dewei, LU Hu. Analysis of Anti-Jamming Performance to GNSS Navigation Signals Design[J]. *Journal of University of Electronic Science and Technology of China*, 2020, 49(4): 575-583.

[52] 毛虎, 吴德伟, 卢虎, 等. GPSM码信号压制干扰样式效能分析[J]. 电子科技大学学报, 2015, 44(3): 350-356.
MAO Hu, WU Dewei, LU Hu, et al. Effectiveness Analysis of the Blanket Jamming Mode to GPSM Code Signal[J]. *Journal of University of Electronic Science and Technology of China*, 2015, 44(3): 350-356.

[53] 杨琼. 卫星导航接收机抗干扰技术研究[D]. 西安: 西北工业大学, 2019.
YANG Qiong. Research on the Interference Mitigation Algorithm of Satellite Navigation Receiver[D]. Xi'an: Northwestern Polytechnical University, 2019.

[54] 严昆仑. 面向城市复杂环境GNSS高精度定位的标量深组合基带技术研究[D]. 武汉: 武汉大学, 2018.
YAN Kunlun. Research on GNSS Baseband Technology of Scalar Deep Integration for High Accuracy Positioning in Urban Harsh Environment[D]. Wuhan: Wuhan University, 2018.

[55] 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, LÜ Zhicheng, WANG Feixue. Spoofing Pattern Research on GNSS Receivers[J]. *Journal of Astronautics*, 2012, 33(7): 884-890.

[56] 唐小妹, 马鹏程, 马春江. 一种基于功率可行域的卫星导航欺骗干扰评估方法[J]. 武汉大学学报(信息科学版), 2023, 48(7): 1160-1169.
TANG Xiaomei, MA Pengcheng, MA Chunjiang. Evaluation Method of Satellite Navigation Spoofing Based on Power Feasible Region[J]. *Geomatics and Information Science of Wuhan University*, 2023, 48(7): 1160-1169.

[57] 刘宗敏, 王光明, 周超, 等. 天基卫导欺骗信号特征分析及作用效果评估[J]. 测控技术, 2022, 41(7): 69-74.
LIU Zongmin, WANG Guangming, ZHOU Chao,

et al. Characteristic Analysis and Effect Evaluation of Space-Based Satellite Navigation Spoofing Signal [J]. *Measurement & Control Technology*, 2022, 41(7): 69-74.

[58] 余辉, 张德欣, 方远, 等. "北斗"用户机欺骗干扰试验评估方法研究[J]. 航天电子对抗, 2019, 35(6): 10-13.
YU Hui, ZHANG Dexin, FANG Yuan, et al. Evaluation Method of BeiDou Receiver Spoof Jamming Test [J]. *Aerospace Electronic Warfare*, 2019, 35(6): 10-13.

[59] WANG Y, SUN F P, WANG X. Optimal Decision for the Satellite Navigation System Under Navigation Countermeasures Based on Spoofing Effect Evaluation Results[J]. *IET Control Theory & Applications*, 2023, 17(11): 1522-1542.

[60] 胡彦逢, 边少锋, 曹可劲, 等. GNSS接收机欺骗干扰功率控制策略[J]. 中国惯性技术学报, 2015, 23(2): 207-210.
HU Yanfeng, BIAN Shaofeng, CAO Kejin, et al. Spoofing Power Control Strategy for GNSS Receiver [J]. *Journal of Chinese Inertial Technology*, 2015, 23(2): 207-210.

[61] TANG X, WANG D W, ZHANG R N, et al. Jamming Mitigation via Aerial Reconfigurable Intelligent Surface: Passive Beamforming and Deployment Optimization [J]. *IEEE Transactions on Vehicular Technology*, 2021, 70(6): 6232-6237.

[62] HAN C, LIU A J, AN K, et al. Distributed UAV Deployment in Hostile Environment: A Game-Theoretic Approach[J]. *IEEE Wireless Communications Letters*, 2022, 11(1): 126-130.

[63] 刘志衡, 刘伟平, 焦博. 基于局部最优点的GNSS分布式压制干扰源部署算法[J]. 兵工学报, 2024, 45(9): 3240-3252.
LIU Zhiheng, LIU Weiping, JIAO Bo. GNSS Distributed Interference Source Deployment Algorithm Based on Locally Optimal Point[J]. *Acta Armamentarii*, 2024, 45(9): 3240-3252.

[64] DING M Y, CHEN W, DING W H. Performance Analysis of a Normal GNSS Receiver Model Under Different Types of Jamming Signals[J]. *Measurement*, 2023, 214: 112786.

[65] ZHU Z H, ZHANG L J, PEI K K, et al. A Robust and Lightweight Voice Activity Detection Algorithm for Speech Enhancement at Low Signal-to-Noise Ratio [J]. *Digital Signal Processing*, 2023, 141: 104151.

[66] WANG Y, SUN F P, WANG X, et al. Construction of the Performance Index System of Navigation Confrontation and Research on Its Related Evaluation Methods[J]. *IEEE Transactions on Instrumentation and Measurement*, 2022, 71: 3515316.

[67] WANG Y, SUN F, WANG X. Research on Relevant Protective Performance Evaluation Methods for a Global Navigation Satellite System in Satellite Navigation Countermeasures [J]. *IET Conference Proceedings*, 2023, 2023(21): 65-73.

[68] 高为广, 苏牡丹, 李军正, 等. 北斗卫星导航系统试运行服务性能评估[J]. 武汉大学学报(信息科学版), 2012, 37(11): 1352-1355.
GAO Weiguang, SU Mudan, LI Junzheng, et al. A Performance Evaluation of Beidou Navigation Satellite System[J]. *Geomatics and Information Science of Wuhan University*, 2012, 37(11): 1352-1355.

[69] WU Y, LIU X L, LIU W K, et al. Long-Term Behavior and Statistical Characterization of BeiDou Signal-in-Space Errors[J]. *GPS Solutions*, 2017, 21(4): 1907-1922.

[70] 何义磊. 北斗三号最简系统卫星信号质量分析[J]. 武汉大学学报(信息科学版), 2020, 45(3): 394-402.
HE Yilei. Quality Analysis of Satellite Signal for BDS-3 Simplest System[J]. *Geomatics and Information Science of Wuhan University*, 2020, 45(3): 394-402.

[71] 宋伟伟, 赵新科, 楼益栋, 等. 北斗三号PPP-B2b服务性能评估[J]. 武汉大学学报(信息科学版), 2023, 48(3): 408-415.
SONG Weiwei, ZHAO Xinke, LOU Yidong, et al. Performance Evaluation of BDS-3 PPP-B2b Service[J]. *Geomatics and Information Science of Wuhan University*, 2023, 48(3): 408-415.

[72] 张柔, 胡志刚, 陶钧, 等. 顾及不同天线相位中心改正模型的北斗空间信号精度评估方法[J]. 武汉大学学报(信息科学版), 2019, 44(6): 806-813.
ZHANG Rou, HU Zhigang, TAO Jun, et al. BDS Signal-in-Space User Range Error Evaluation Considering Different Antenna Phase Center Offset Models[J]. *Geomatics and Information Science of Wuhan University*, 2019, 44(6): 806-813.

[73] MI X L, SHENG C Z, EL-MOWAFY A, et al. Characteristics of Receiver-Related Biases Between BDS-3 and BDS-2 for Five Frequencies Including Inter-System Biases, Differential Code Biases, and Differential Phase Biases[J]. *GPS Solutions*, 2021, 25(3): 113.

[74] CAO X Y, KUANG K F, GE Y L, et al. An Efficient Method for Undifferenced BDS-2/BDS-3 High-Rate Clock Estimation [J]. *GPS Solutions*,

2022, 26(3): 66.

[75] YANG Y X, REN X, JIA X L, et al. Development Trends of the National Secure PNT System Based on BDS[J]. *Science China Earth Sciences*, 2023, 66(5): 929-938.

[76] 蔡洪亮, 孟轶男, 耿长江, 等. 北斗三号全球导航卫星系统服务性能评估: 定位导航授时、星基增强、精密单点定位、短报文通信与国际搜救[J]. 测绘学报, 2021, 50(4): 427-435.
CAI Hongliang, MENG Yinan, GENG Changjiang, et al. BDS-3 Performance Assessment: PNT, SBAS, PPP, SMC and SAR[J]. *Acta Geodaetica et Cartographica Sinica*, 2021, 50(4): 427-435.

[77] WANG Y, TIAN W, XU J Y, et al. Wearable Wireless Dual-Channel EEG System for Emotion Recognition Based on Machine Learning[J]. *IEEE Sensors Journal*, 2023, 23(18): 21767-21775.

[78] ZHAO D M, JI G Q, ZHANG Y L, et al. A Network Security Situation Prediction Method Based on SSA-GResNeSt[J]. *IEEE Transactions on Network and Service Management*, 2024, 21(3): 3498-3510.

[79] RISBUD P, GATSIS N, TAHA A. Vulnerability Analysis of Smart Grids to GPS Spoofing[J]. *IEEE Transactions on Smart Grid*, 2019, 10(4): 3535-3548.

[80] MA C, YANG J, CHEN J Y, et al. Effects of a Navigation Spoofing Signal on a Receiver Loop and a UAV Spoofing Approach[J]. *GPS Solutions*, 2020, 24(3): 76.

[81] SAATY T L. The Modern Science of Multicriteria Decision Making and Its Practical Applications: The AHP/ANP Approach[J]. *Operations Research*, 2013, 61(5): 1101-1118.

[82] QIAO C, WANG Y, LI C H, et al. Application of Extension Theory Based on Improved Entropy Weight Method to Rock Slope Analysis in Cold Regions[J]. *Geotechnical and Geological Engineering*, 2021, 39(6): 4315-4327.

[83] ZHU D R, WANG R, DUAN J D, et al. Comprehensive Weight Method Based on Game Theory for Identify Critical Transmission Lines in Power System[J]. *International Journal of Electrical Power & Energy Systems*, 2021, 124: 106362.

[84] 余俊, 明振军, 阎艳, 等. 考虑不确定性的机枪作战效能综合评估方法[J]. 兵工学报, 2018, 39(10): 2048-2055.
YU Jun, MING Zhenjun, YAN Yan, et al. Comprehensive Evaluation Method for Combat Effectiveness of Machine Gun Considering Interval Uncertainty[J]. *Acta Armamentarii*, 2018, 39(10): 2048-2055.

[85] SINGH S, SINGH S. Time-Cost Trade-off in a Multi-choice Assignment Problem[J]. *Engineering Optimization*, 2022, 54(4): 576-592.

[86] DE ASÍS LÓPEZ F, ORDÓÑEZ C, ROCA-PARDIÑAS J. A Generalized Additive Model (GAM) Approach to Principal Component Analysis of Geographic Data[J]. *Spatial Statistics*, 2024, 59: 100806.

[87] 苟娇娇, 罗明良, 王飞. 影响黄土高原集水面积阈值的地形因子主成分分析[J]. 武汉大学学报(信息科学版), 2017, 42(5): 704-710.
GOU Jiaojiao, LUO Mingliang, WANG Fei. Principal Component Analysis for the Terrain Factors of Flow Accumulation Threshold in Loess Plateau[J]. *Geomatics and Information Science of Wuhan University*, 2017, 42(5): 704-710.

[88] 沈欣, 刘钰霖, 李仕学, 等. 一种基于改进PSO算法的高时间分辨率遥感卫星星座优化设计方法[J]. 武汉大学学报(信息科学版), 2018, 43(12): 1986-1993.
SHEN Xin, LIU Yulin, LI Shixue, et al. An Optimization Design Method for High Temporal Resolution Remote Sensing Satellite Constellation Based on Improved PSO Algorithm[J]. *Geomatics and Information Science of Wuhan University*, 2018, 43(12): 1986-1993.

[89] 种洋, 柴洪洲, 刘帆, 等. 模糊决策理论的地磁图适配性分析[J]. 武汉大学学报(信息科学版), 2021, 46(1): 118-124.
CHONG Yang, CHAI Hongzhou, LIU Fan, et al. Suitability Analysis of Geomagnetic Map Based on Fuzzy Decision Theory[J]. *Geomatics and Information Science of Wuhan University*, 2021, 46(1): 118-124.

[90] 董成喜, 吴德伟, 何晶. 基于粗糙模糊集理论的卫星导航系统作战效能评估方法[J]. 山东大学学报(工学版), 2008, 38(4): 32-36.
DONG Chengxi, WU Dewei, HE Jing. Combat Effectiveness Evaluation Method of a Satellite Navigation System Based on Rough Fuzzy Sets[J]. *Journal of Shandong University (Engineering Science)*, 2008, 38(4): 32-36.

[91] 钟伦珑, 刘明远, 胡铁乔, 等. 基于随机森林回归的电离层幅度闪烁指数预测[J]. 计算机工程与设计, 2024, 45(8): 2350-2356.
ZHONG Lunlong, LIU Mingyuan, HU Tieqiao, et al. Prediction of Ionospheric Amplitude Scintillation Index Based on Random Forest Regression[J]. *Computer Engineering and Design*, 2024, 45(8):

2350-2356.

[92] 刘明骞,高晓腾,张俊林. 多类型的雷达有源干扰感知新方法[J]. 西安交通大学学报,2019,53(10):103-108.
LIU Mingqian, GAO Xiaoteng, ZHANG Junlin. A Novel Sensing Method for Multi-types of Radar Active Jamming[J]. *Journal of Xi'an Jiaotong University*, 2019, 53(10): 103-108.

[93] 王双川,贾希胜,胡起伟,等. 基于正态灰云模型的装备维修保障系统效能评估[J]. 系统工程与电子技术,2019,41(7):1576-1582.
WANG Shuangchuan, JIA Xisheng, HU Qiwei, et al. Effectiveness Evaluation for Equipment Maintenance Support System Based on Normal Grey Cloud Model[J]. *Systems Engineering and Electronics*, 2019, 41(7): 1576-1582.

[94] 王月,郝金明,刘伟平. 云模型对GNSS欺骗干扰效能的评估[J]. 测绘科学技术学报,2019,36(5):470-476.
WANG Yue, HAO Jinming, LIU Weiping. Evaluation of GNSS Spoofing Efficiency Using Cloud Model[J]. *Journal of Geomatics Science and Technology*, 2019, 36(5): 470-476.

[95] 姚志成,李昱婷,侯博,等. 云模型在GNSS接收机抗干扰性能评估中的应用[J]. 电光与控制,2021,28(7):1-5.
YAO Zhicheng, LI Yuting, HOU Bo, et al. Application of Cloud Model in Evaluation of Anti-Jamming Performance of GNSS Receivers[J]. *Electronics Optics & Control*, 2021, 28(7): 1-5.

[96] LIU H C, WANG L E, LI Z W, et al. Improving Risk Evaluation in FMEA with Cloud Model and Hierarchical TOPSIS Method[J]. *IEEE Transactions on Fuzzy Systems*, 2019, 27(1): 84-95.

[97] PHILIP CHEN C L. Fuzzy Multi-attribute Decision Making Algorithm for Vehicle Navigation in Sensor Network Environments[C]//The 4th IEEE International Symposium on Logistics and Industrial Informatics, Smolenice, Slovakia, 2012.

[98] PATIL S K, KANT R. A Fuzzy AHP-TOPSIS Framework for Ranking the Solutions of Knowledge Management Adoption in Supply Chain to Overcome Its Barriers[J]. *Expert Systems with Applications*, 2014, 41(2): 679-693.

[99] 阎艳,郝佳,陈中明,等. 基于模糊决策图与灰色关联分析的枪械设计方案评价[J]. 兵工学报,2016,37(10):1934-1940.
YAN Yan, HAO Jia, CHEN Zhongming, et al. Design Scheme Evaluation Based on Fuzzy Decision Maps and Grey Relational Analysis[J]. *Acta Armamentarii*, 2016, 37(10): 1934-1940.

[100] 张启福,徐世成,王章,等. 基于"导航战"的北斗卫星定位抗干扰策略[J]. 导航定位学报,2023,11(1):24-29.
ZHANG Qifu, XU Shicheng, WANG Zhang, et al. Anti-Jamming Strategy of BeiDou Satellite Positioning Based on Navigation Warfare[J]. *Journal of Navigation and Positioning*, 2023, 11(1): 24-29.

[101] JAVED S A, LIU S F. Bidirectional Absolute GRA/GIA Model for Uncertain Systems: Application in Project Management[J]. *IEEE Access*, 2019, 7: 60885-60896.

[102] LI X T. Personal Information Security Risk Assessment for E-Waste Recycling Based on Fuzzy-GRA-TOPSIS and FMEA[J]. *IEEE Transactions on Engineering Management*, 2024, 71: 8240-8250.

[103] ZHANG L, BAI W, XIAO H J, et al. Measuring and Improving Regional Energy Security: A Methodological Framework Based on Both Quantitative and Qualitative Analysis[J]. *Energy*, 2021, 227: 120534.

[104] 王刚. 基于博弈论的SAR有源干扰对抗技术[D]. 西安:西安电子科技大学,2016.
WANG Gang. Study on SAR Active Jamming Countermeasure Based on Game Theory[D]. Xi'an: Xidian University, 2016.

[105] 黄玉川,饶妮妮,刘永红,等. 博弈论应用于干扰效果动态评估的研究[J]. 电子科技大学学报,2007,36(5):876-879.
HUANG Yuchuan, RAO Nini, LIU Yonghong, et al. Dynamic Evaluation for Radar Jamming Effects Using the Game Theory[J]. *Journal of University of Electronic Science and Technology of China*, 2007, 36(5): 876-879.

[106] ABE O E, OTERO VILLAMIDE X, PAPARINI C, et al. Performance Evaluation of GNSS-TEC Estimation Techniques at the Grid Point in Middle and Low Latitudes During Different Geomagnetic Conditions[J]. *Journal of Geodesy*, 2017, 91(4): 409-417.

[107] 王跃东,顾以静,梁彦,等. 伴随压制干扰与组网雷达功率分配的深度博弈研究[J]. 雷达学报,2023,12(3):642-656.
WANG Yuedong, GU Yijing, LIANG Yan, et al. Deep Game of Escorting Suppressive Jamming and Networked Radar Power Allocation[J]. *Journal of Radars*, 2023, 12(3): 642-656.

[108] LIN X, LIU A J, HAN C, et al. LEO Satellite and UAVs Assisted Mobile Edge Computing for Tactical Ad-Hoc Network: A Game Theory Approach[J]. *IEEE Internet of Things Journal*, 2023, 10

(23): 20560-20573.

[109]KUSYK J, UYAR M U, MA K, et al. Artificial Intelligence and Game Theory Controlled Autonomous UAV Swarms[J]. *Evolutionary Intelligence*, 2021, 14(4): 1775-1792.

[110]ZHOU X, ZHAO R, CHENG L, et al. Impact of Policy Incentives on Electric Vehicles Development: A System Dynamics-Based Evolutionary Game Theoretical Analysis[J]. *Clean Technologies and Environmental Policy*, 2019, 21(5): 1039-1053.

[111]王龙, 黄锋. 多智能体博弈、学习与控制[J]. 自动化学报, 2023, 49(3): 580-613.
WANG Long, HUANG Feng. An Interdisciplinary Survey of Multi-agent Games, Learning, and Control[J]. *Acta Automatica Sinica*, 2023, 49(3): 580-613.

[112]TEMBINE H. Deep Learning Meets Game Theory: Bregman-Based Algorithms for Interactive Deep Generative Adversarial Networks[J]. *IEEE Transactions on Cybernetics*, 2020, 50(3): 1132-1145.

[113]HAN X Y, HUAN K W, SHENG S J. Performance Evaluation and Optimization Design of Photoelectric Pyrometer Detection Optical System[J]. *Defence Technology*, 2020, 16(2): 401-407.

[114]CAGLIERO L, GARZA P, PASINI A, et al. Additional Reviewer Assignment by Means of Weighted Association Rules[J]. *IEEE Transactions on Emerging Topics in Computing*, 2021, 9(1): 329-341.

[115]WANG Y, SUN F P, WANG X, et al. Full-Domain Collaborative Deployment Method of Multiple Interference Sources and Evaluation of Its Deployment Effect[J]. *Defence Technology*, 2024, 32: 572-595.

[116]王伟柱, 刘志国, 王仕成, 等. 激光角度欺骗干扰效果评估实验研究[J]. 红外与激光工程, 2018, 47(11): 67-72.
WANG Weizhu, LIU Zhiguo, WANG Shicheng, et al. Evaluation of Laser Angle Deception Interference Effect Based on Experiment[J]. *Infrared and Laser Engineering*, 2018, 47(11): 67-72.

[117]刘尊洋, 沈阳, 李修和, 等. 激光半主动制导武器角度欺骗干扰效果评估方法研究[J]. 弹箭与制导学报, 2018, 38(3): 67-70.
LIU Zunyang, SHEN Yang, LI Xiuhe, et al. Study on Estimating Method of Angle Deceptive Jamming to Semi-active Laser-Guided Weapon[J]. *Journal of Projectiles, Rockets, Missiles and Guidance*, 2018, 38(3): 67-70.

[118]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.

[119]WANG Y, SUN F P, HAO J M, et al. Reduction Research on Performance Index System of Satellite Navigation System Spoofing[J]. *GPS Solutions*, 2022, 26(2): 43.

[120]LIVIO J, HODHOD R. AI Cupper: A Fuzzy Expert System for Sensorial Evaluation of Coffee Bean Attributes to Derive Quality Scoring[J]. *IEEE Transactions on Fuzzy Systems*, 2018, 26(6): 3418-3427.

[121]CAO Y, ZHOU Z J, HU C H, et al. On the Interpretability of Belief Rule-Based Expert Systems[J]. *IEEE Transactions on Fuzzy Systems*, 2021, 29(11): 3489-3503.

[122]BI L Y, CAO W H, HU W K, et al. A Dynamic-Attention-Based Heuristic Fuzzy Expert System for the Tuning of Microwave Cavity Filters[J]. *IEEE Transactions on Fuzzy Systems*, 2022, 30(9): 3695-3707.

[123]GE J, ZHANG X L, DONG H B, et al. Gray System-Based Identification and Pre-culling of Outliers Applied to Magnetic Sensor in Aeromagnetic Compensation[J]. *IEEE Sensors Journal*, 2021, 21(3): 2783-2790.

[124]TAN Y, LI Y, CAO Y J, et al. Cyber-Attack on Overloading Multiple Lines: A Bilevel Mixed-Integer Linear Programming Model[J]. *IEEE Transactions on Smart Grid*, 2018, 9(2): 1534-1536.

[125]WAN J W, XU C, QIAO Y D, et al. Error Constraint Enhanced Particle Filter Using Quantum Particle Swarm Optimization[J]. *IEEE Sensors Journal*, 2021, 21(21): 24431-24439.

[126]FENG L Y, ZHANG L M. Enhanced Prediction Intervals of Tunnel-Induced Settlement Using the Genetic Algorithm and Neural Network[J]. *Reliability Engineering & System Safety*, 2022, 223: 108439.

[127]GOLI A, TIRKOLAEE E B, AYDIN N S. Fuzzy Integrated Cell Formation and Production Scheduling Considering Automated Guided Vehicles and Human Factors[J]. *IEEE Transactions on Fuzzy Systems*, 2021, 29(12): 3686-3695.

[128]ALIZADEH MOGHADDAM S H, MOKHTARZADE M, ALIZADEH MOGHADDAM S A. Optimization of RFM's Structure Based on PSO Algorithm and Figure Condition Analysis[J]. *IEEE Geoscience and Remote Sensing Letters*, 2018, 15(8): 1179-1183.

[129]MISTRY K, ZHANG L, NEOH S C, et al. A Mi-

cro-GA Embedded PSO Feature Selection Approach to Intelligent Facial Emotion Recognition [J]. *IEEE Transactions on Cybernetics*, 2017, 47(6): 1496-1509.

[130]LIU J G, HUANG J, SUN R, et al. Data Fusion for Multi-source Sensors Using GA-PSO-BP Neural Network[J]. *IEEE Transactions on Intelligent Transportation Systems*, 2021, 22(10): 6583-6598.

[131]ROSSEEL J, MANNONI V, FIJALKOW I, et al. Decoding Short LDPC Codes via BP-RNN Diversity and Reliability-Based Post-Processing [J]. *IEEE Transactions on Communications*, 2022, 70(12): 7830-7842.

[132]LV Z H, LOU R R, SINGH A K. AI Empowered Communication Systems for Intelligent Transportation Systems[J]. *IEEE Transactions on Intelligent Transportation Systems*, 2021, 22(7): 4579-4587.

[133]AZADI M, EMROUZNEJAD A, RAMEZANI F, et al. Efficiency Measurement of Cloud Service Providers Using Network Data Envelopment Analysis [J]. *IEEE Transactions on Cloud Computing*, 2022, 10(1): 348-355.

[134]刘东, 李帅, 付强, 等. 基于KHA优化BP神经网络的地下水水质综合评价方法[J]. 农业机械学报, 2018, 49(9): 275-284.
LIU Dong, LI Shuai, FU Qiang, et al. Comprehensive Evaluation Method of Groundwater Quality Based on BP Network Optimized by Krill Herd Algorithm [J]. *Transactions of the Chinese Society for Agricultural Machinery*, 2018, 49(9): 275-284.

[135]HE W J, LIU Y F, YAO H P, et al. Distributed Variational Bayes-Based in-Network Security for the Internet of Things[J]. *IEEE Internet of Things Journal*, 2021, 8(8): 6293-6304.

[136]KARIMNEZHAD A, BICKEL D R. Incorporating Prior Knowledge About Genetic Variants into the Analysis of Genetic Association Data: An Empirical Bayes Approach [J]. *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, 2020, 17(2): 635-646.

[137]AKHMETOV Y, NURMANOVA V, BAGHERI M, et al. A Bootstrapping Solution for Effective Interpretation of Transformer Winding Frequency Response [J]. *IEEE Transactions on Instrumentation and Measurement*, 2022, 71: 3508811.

[138]KIM S E, BA D, BROWN E N. A Multitaper Frequency-Domain Bootstrap Method [J]. *IEEE Signal Processing Letters*, 2018, 25(12): 1805-1809.

[139]ARFÈ A, MULIERE P. A General Bayesian Bootstrap for Censored Data Based on the Beta-Stacy Process[J]. *Journal of Statistical Planning and Inference*, 2023, 222: 241-251.

[140]HERNÁNDEZ PERDOMO W, CALDERÓN CÓRDOVA C, GONZALEZ V, et al. Bootstrap-Based Frequency Estimation Method [J]. *Measurement*, 2017, 95: 193-200.