引用格式:吴浩,江莉,徐婧,等. 无人机导航诱骗技术研究现状及展望[J]. 信息对抗技术,2024, 3(6):1-9. [WU Hao, JIANG Li, XU Jing, et al. UAV navigation spoofing technology: its current status and prospects[J]. Information Countermeasure Technology, 2024, 3(6):1-9. (in Chinese)]

无人机导航诱骗技术研究现状及展望

吴 浩[1,2],江 莉[2],徐 婧[3,4*],张 劲[5],李 权[6]

(1. 清华大学电子工程系,北京 100084; 2. 成都空御科技有限公司,四川成都 610200;
3. 中国科学院成都文献情报中心,四川成都 610041; 4. 中国科学院大学经济与管理学院,北京 100190;
5. 四川大学生物医学工程学院,四川成都 610065; 6. 成都工业职业技术学院信息工程学院,四川成都 610213)

摘 要 随着无人机的广泛应用,导航诱骗技术已成为应对无人机恶意入侵、确保安全的重要手段之一。为此,全面分析了无人机导航诱骗技术的研究现状、技术原理和发展趋势。首先,深入分析了无人机导航诱骗技术的研究进展,根据信号生成方式、实现目的、实施显隐性的不同对该技术进行分类;其次,针对未来反诱骗技术的发展,预测无人机导航诱骗与反诱骗对抗、诱骗隐蔽性增强、多手段联合诱骗、模拟导航合作式应用和智能化诱骗等将成为主要发展趋势;最后,对未来违规飞行目标动态精准诱骗研究以及加强导航诱骗技术合规化使用进行了展望。

关键词 无人机;导航诱骗;联合诱骗;INS/GNSS 组合导航

中图分类号 TN 972+.3 **文章编号** 2097-163X(2024)06-0001-09

文献标志码 A **DOI** 10.12399/j.issn.2097-163x.2024.06.001

UAV navigation spoofing technology: its current status and prospects

WU Hao[1,2], JIANG Li[2], XU Jing[3,4*], ZHANG Jin[5], LI Quan[6]

(1. Department of Electronic Engineering, Tsinghua University, Beijing 100084, China;
2. Chengdu Sky Defence Technology Co. Ltd, Chengdu 610200, China;
3. National Science Library(Chengdu), Chinese Academy of Sciences, Chengdu 610041, China;
4. School of Economics and Management, University of Chinese Academy of Sciences, Beijing 100190, China;
5. College of Biomedical Engineering, Sichuan University, Chengdu 610065, China;
6. College of Information Department, Chengdu Vocational and Technical College of Industry, Chengdu 610213, China)

Abstract With the widespread application of unmanned aerial vehicles (UAVs), navigation spoofing technology has become one of the important means to deal with malicious invasion and ensure airspace security. To this end, a comprehensive analysis of the current research status, technical principles, and development trends of UAV navigation spoofing technology has been conducted. Firstly, the research progress of UAV navigation spoofing technology was deeply analyzed, classifying the technology based on different signal generation methods, purposes, and stealthiness of implementation. Secondly, in anticipation of the development of anti-spoofing technology, it was predicted that the confrontation between UAV navigation spoofing and anti-spoofing, enhancement of spoofing stealth, multi-method joint spoofing,

收稿日期:2024-07-23 **修回日期**:2024-10-10

通信作者:徐婧,E-mail:jingxu@clas.ac.cn

基金项目:国防基础科研计划项目(JCKYS2023DC05)

cooperative applications of simulated navigation, and intelligent spoofing will become the main development trends. Lastly, the paper proposed future prospects for precise spoofing research on unauthorized flight targets and strengthening the legal use of navigation spoofing technology.

Keywords UAV; navigation spoofing; combined spoofing; INS/GNSS integrated navigation

0 引言

随着无人机的不断普及,无人机已经从最初的军事应用逐渐扩展到民用、商业及科研等众多领域,其具有携带方便、操作简单、成本低廉等特点,在航拍、农业巡查、物流配送、救灾救援等多种场景中被广泛应用。然而,无人机的普及也引发了一系列新的安全问题和挑战,如隐私侵犯、非法侦察、无人机撞机事件以及恐怖主义袭击等。特别是在城市、机场、政府机构等一些敏感地区,黑飞、滥飞的无人机可能带来重大安全隐患,因此,对无人机实施有效管控成为低空安全的重要保障。为了应对各种空中威胁,目前世界各国军队广泛装备了防空导弹、高炮等传统防空武器,但由于无人机目标的特殊性,这类基于“硬杀伤”理念的武器在执行反无人机任务时的效果不佳且性价比低,还会对地面产生次生安全危害,不宜在民用无人机管控中使用。

导航诱骗技术作为一种“软处置”手段,在民用无人机管控中得到了广泛应用,它能够有效迷惑、控制或引导无人机飞往指定安全区域并降落,达到阻止非法入侵,保障空域安全的目的,同时,能够避免处置过程中由于无人机不可控而造成的二次安全事故,最大程度减少对周边环境和人员的潜在威胁。因此,无人机导航诱骗技术近年来成为研究热点[1]。然而,导航诱骗技术也面临诸多问题和挑战,包括:技术复杂性高、存在法律和道德问题、易被滥用造成安全隐患等。随着无人机技术的进步和反诱骗能力的增强,导航诱骗技术也需不断更新迭代。

本文对无人机导航诱骗技术从应用领域、发展过程、技术原理以及技术分类等方面进行全面分析与总结。在此基础上,对无人机导航诱骗技术的未来发展趋势进行预测,并提出了非合作式目标动态精准诱骗研究和加强导航诱骗技术及设备合规化使用的未来展望。

1 无人机导航诱骗技术研究现状

随着无人机技术的迅速发展与广泛应用,无人机在民用和军事领域的作用日益重要。在无人机反制打击技术中,导航诱骗以其隐蔽性强、效费比高、目标动态可控等优点[2]成为研发和应用的热点。

1.1 应用领域

在军事领域,导航诱骗技术主要用于防空系统,保护重要设施免受敌方无人机侦察或攻击。包括:1)军事基地设施防护。对进入军事基地周边的敌方无人机发送虚假导航信号,使无人机迷失方位、返航或迫降、偏离航线进行指定地点迫降,从而避免其进行侦察或攻击,这不仅可以保护军事设施的安全,还可以防止信息泄露。2)边境巡逻。在边境区域,部署导航诱骗装置可以有效干扰试图非法入境的无人机,从而加强边境安全,避免潜在威胁。3)干扰反制敌方战场侦察。在战场环境中,通过诱骗敌方无人机的导航系统,使其无法获取准确情报或进行有效打击,这不仅能扰乱敌方的战术部署,还可以保护己方士兵和设备的安全。4)伴随保障。在军队行军或战斗过程中,通过在部队周围部署导航诱骗设备,形成保护屏障,防止敌方无人机接近,从而保障部队行动的安全性和隐蔽性。

在民用领域,随着无人机在物流、农业、影视拍摄等领域的大量部署,防止无人机误入禁飞区、保障公共场所或设施安全、保护个人隐私和商业机密成为紧迫需求。导航诱骗技术在民用领域的应用[3]主要包括以下场景:1)国家基础设施;2)航空机场;3)文物景区防护;4)重要场所或重大赛事防护。

1.2 发展过程

1.2.1 诱骗技术发展

从最初的基础研究到目前的复杂应用系统,无人机导航诱骗技术发展经历了几个重要阶段,其关键技术的进步体现了无人机防御领域的不

断革新和深化，见表 1 所列。

表 1　无人机导航诱骗技术发展过程

Tab. 1　The development process of UAV navigation spoofing technology

阶段	时间	信号生成	导航模式
简单干扰	2001—2016 年	转发式	单模导航/惯性导航
精确诱骗	2016 年至今	转发式＋生成式	多模导航/惯性导航

2001 年，美国交通部介绍了全球定位系统(global positioning system，GPS)诱骗干扰与抗干扰技术[4]。2011 年伊朗防空部队使用诱骗干扰技术俘获了 1 架美国“RQ-170”哨兵无人机[5]，表明了诱骗技术的可行性。2012 年白沙导弹靶场进行了使用低成本设备的 GPS 无人直升机诱骗干扰试验[6]。2013—2016 年，研究者对转发诱骗进行了因素分析与改进方法的研究，提升了诱骗隐蔽性及成功率[7-11]。此后，研究者开始探索更为复杂的导航诱骗方法，即生成与真实卫星信号相似但含有误导性信息的信号。2017—2019 年，研究者主要研究了生成式诱骗技术和相关诱骗方案系统[12-14]。通过对诱骗轨迹优化、多轨迹信息融合等诱骗技术研究，实现对 GPS/INS(INS：inertial navigation system，惯性导航系统)组合导航系统的诱骗[15-16]。2021 年后随着人工智能和机器学习技术的发展，导航诱骗技术进入新的发展阶段。2021 年，DING 等[17]提出了一种基于 YOLO Nano 的多无人机协同 GPS 诱骗方案，能够对自主运动的目标无人机进行有效攻击。2022 年，GENG 等[18]根据卫星导航诱骗信号对组合导航位置输出的影响机理，提出了一种 INS/GNSS(GNSS：global navigation satellite system，全球卫星导航系统)组合导航隐蔽定向诱骗方法。2023 年，GAO 等[19]提出的 GNSS 隐蔽定向诱骗算法在整个诱骗过程中有效规避了无人机系统的最小二乘残差接收机自主完整性监测(least squares residual-receiver autonomous integrity monitoring，LSR-RAIM)，规避率达到 100%，实现了隐蔽诱骗，其诱骗偏航角误差低至 0.03°。通过算法优化和智能分析，这些技术现在能够更加精确地识别目标、生成诱骗信号，从而实时调整诱骗策略以应对目标无人机的防干扰措施，大大提高了导航诱骗技术的有效性和适用范围。

1.2.2　导航模式发展

随着技术水平的不断提升，导航系统从单模导航向多模导航逐渐演变[20]。早期的无人机主要依赖单一 GPS，在精度和覆盖范围上有显著优势，但容易被简单伪装的 GPS 信号诱导偏离其预定轨迹[21]。单模导航的局限性和易受干扰性促使了组合导航技术的发展。INS 凭借其自主性、高精度短期定位和抗干扰性，在无人机导航尤其是防诱骗领域中起到了重要作用。大量的研究围绕 GPS 导航和惯性导航下的无人机诱骗技术展开[20-22]。近年来除 GPS 之外，逐渐发展出包含俄罗斯的全球卫星导航系统 GLONASS(global navigation satellite system)、欧洲的伽利略卫星导航系统 Galileo(Galileo satellite navigation system)和中国的北斗卫星导航系统 BDS(BeiDou navigation satellite system)融合的多模导航技术，极大地提高了定位精度、冗余性和抗干扰能力，增强了无人机在复杂环境下的自主导航能力。多模导航系统条件下单一模式的诱骗干扰效率较低，因此，诱骗干扰技术也升级采用多模导航诱骗干扰设备和策略[23-26]。然而，随着惯性导航的辅助应用，其成本和实施难度显著增加[27]。研究人员通过研究 GNSS 诱骗信号对 INS/GNSS 集成导航位置输出的影响机制，推导出在 INS/GNSS 集成导航模式下使用具有 2 个可调参数的指数诱骗信号实现方向诱骗的可行性[18]；研究设计诱骗跟踪控制器[27]及定向诱骗算法[19]，使 INS/GNSS 组合导航的无人机在无意识的状态下偏离原定轨迹，达到隐蔽性诱骗效果。

2　无人机导航诱骗技术原理

2.1　技术原理

导航诱骗技术通过发射虚假的卫星导航信号对无人机导航终端实施诱骗，达到控制或欺骗无人机的目的。无人机的导航系统主要依赖于 GNSS，通过接收来自地球轨道上多个卫星的信号，计算出无人机的精确位置、速度和时间。这一过程涉及复杂的信号处理和时间同步技术，确保无人机能够在三维空间中准确定位。

诱骗过程开始于诱骗设备生成并发射虚假信号，这些信号在频率、相位和功率等方面精确模仿真实卫星信号，其目的是对无人机的导航接

收机实施诱骗。当无人机接收到这些伪造的信号后,其导航系统会解算出错误的位置和速度信息。随后,无人机的飞行控制链路会处理这些错误信息,并与预设的飞行计划进行比较。控制决策模块基于这一比较结果,生成指令以纠正检测到的“偏差”。由于这些“偏差”实际上是由于接收到的错误信号造成的,因此生成的纠正指令也是基于错误数据,导致执行机构执行了错误的飞行路径,最终使无人机偏离了原定航线。诱骗设备需要持续监测无人机的行为并调整虚假信号的参数。为了维持诱骗的有效性,诱骗系统利用附近的监测设备(如雷达和无线电侦测仪)来跟踪无人机的航线变化和飞行参数,从而间接获取无人机的反馈状态并持续调整虚假信号的参数。这一“持续调整”过程确保了虚假信号能够持续误导无人机的导航系统。如果无人机具备异常检测能力,它可能会识别出信号异常并尝试采取措施以避免被诱骗。图 1 展示了无人机导航诱骗过程的详细步骤,包括诱骗信号的生成、无人机行为的监测以及最终的诱骗位置等。整个过程从诱骗设备的初始信号生成开始,经过无人机接收终端的信号接收和处理,直至无人机行为的最终改变。

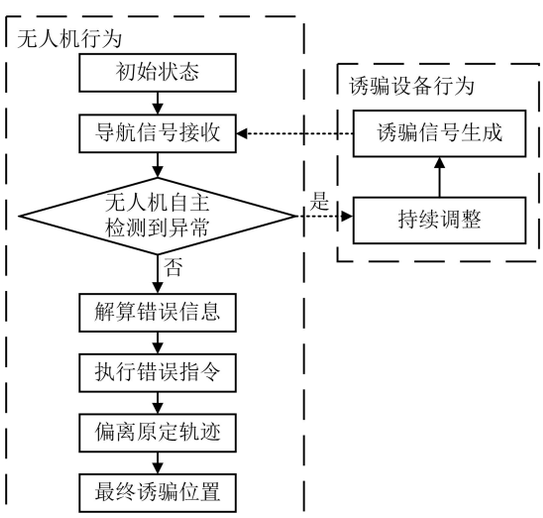

图 1 无人机导航诱骗过程

Fig. 1 Process of UAV navigation spoofing

2.2 导航诱骗技术分类

导航诱骗技术复杂多样,可以根据信号生成方式、实现目的及实施显隐性进行细致分类。

2.2.1 信号生成方式分类

信号生成方式可分为转发式和生成式 2 类,见表 2 所列。

表 2 无人机导航诱骗技术信号生成方式分类

Tab. 2 Classification of signal generation methods for UAV navigation spoofing technology

类别	技术类型	成本	精度	适用场景
转发式	直接转发式	低	中	低成本、简单的场景
	分离转发式	高	高	高精度要求的复杂场景
生成式	简易生成式	低	低	基础伪造信号的简单场景
	中等生成式	中	中	需要一定精度和复杂度的场景
	复杂生成式	高	高	高精度、复杂信号的高端场景

1) 转发式导航诱骗技术[28-30]。该技术通过捕获真实卫星信号并进行微小的时间延迟处理再适当放大转发,在转发过程中可增加特定的信号特性。接收机在接收到转发信号后计算虚假伪距,从而改变接收机位置。无人机的飞控系统根据错误定位进行相应的修正,从而引导无人机向诱骗方向飞行。时间延迟虽然不明显,但足以引起接收机计算出错误的位置信息。

转发式导航诱骗技术分为直接转发式和分离转发式。直接转发式捕获并转发原始卫星信号,通过加入微小的时间延迟,使无人机接收机计算出错误的位置信息。这种方式实施简单,但需要精确控制时间延迟的大小,以达到误导无人机导航系统的效果。分离转发式通过对捕获的原始信号进行处理后再转发,这种方法更为复杂,但能够更有效地干扰目标无人机的导航系统。

2) 生成式导航诱骗技术[31-32]。该技术完全独立于现有信号,模拟真实世界的物理环境和信号传播条件,利用复杂的算法生成具有欺骗性的导航信号。该技术要求深入理解卫星信号的结构和协议,并需要强大的硬件支持以实时生成信号。同时,该技术适用于实验室测试和军事训练,用于仿真复杂的电子战环境。

生成式导航诱骗技术分为简易生成式、中等生成式和复杂生成式。简易生成式主要使用基本的信号生成算法,产生与真实信号相似的伪造信号。该方法成本低,易于实施,但欺骗效果相对有限。中等生成式利用更为复杂的算法和信号处理技术,生成更为精确的伪造信号,包括动态调整信号特性以模拟真实环境。这种方法需要一定的技术基础和硬件支持。复杂生成式则

完全自主生成高精度伪造信号，能够模拟现实世界的物理环境和信号传播条件。这种技术要求深入理解导航信号的结构和协议，需要强大的计算和硬件支持，通常用于军事或高精度实验环境中。

2.2.2　实现目的分类

实现目的可分为方向驱离、禁飞区迫降、轨迹诱骗、控制权接管等，见表 3 所列。

表 3　无人机导航诱骗技术实现目的分类

Tab. 3　Classification of purposes for implementing UAV navigation spoofing technology

类别	成本	精度	适用场景
方向驱离[18]	低	低	保护敏感区域
禁飞区迫降[33]	中	中	重要设施、涉密关键基础设施
轨迹诱骗[34-35]	高	高	军事仿真、无人机性能测试和导航系统验证
控制权接管[38]	高	极高	军事和情报领域，实现对无人机的完全控制

1）方向驱离[18]。通过诱导无人机的导航信息，迫使其偏离预定航线，通常用于保护敏感区域或实施战术规避。例如，在某些敏感区域周围部署方向驱离设备，一旦检测到未经授权的无人机靠近，即启动设备将其引导至安全区域。

2）禁飞区迫降[33]。通过伪造禁飞区域位置信息，使接近的无人机认为其已经进入禁飞区，从而触发无人机飞控预设的应急程序，如返航或迫降。这种技术对于保护机场、政府机构等关键基础设施尤为有效，适用于商业无人机，但对自组装的无人机无效。

3）轨迹诱骗[34-35]。与其他技术相比，轨迹诱骗更加复杂和精细，它要求对目标无人机的导航系统有深入的理解和控制。基于获取无人机实际位置信息结合轨迹参数进行连续欺骗信号的生成，引导无人机沿预定轨迹飞行。轨迹诱骗包括匀速直线、加速直线、圆周运动、原地盘旋等，适用于无人机性能测试、导航系统验证及军事训练。

4）控制权接管[36]。控制权接管是导航诱骗技术中最高级、最危险的一种，不仅要求能够完全干扰和控制无人机的导航信号，还要求能够介入无人机的控制系统，实现对其完全的控制。这需要对无人机的操作系统、通信协议等有极深的了解，常见于军事和情报领域的应用。

2.2.3　实施显隐性分类

实施显隐性分为公然诱骗和隐蔽诱骗，见表 4 所列。

表 4　无人机导航诱骗技术实施显隐性分类

Tab. 4　Classification of overtness and covertness in UAV navigation spoofing technology

类别	成本	精度	适用场景
公然诱骗[16]	低	低	紧急且快速控制的场景
隐蔽诱骗[37-39]	高	高	长期监控、精确干扰的敏感环境

1）公然诱骗[16]。直接向目标发送强虚假信号，迫使目标无人机接收并信任虚假信号，从而控制其导航信息。这种方法的特点是功率大、技术相对简单、易于实施，可迅速且明显地影响目标导航系统。公然诱骗一般发射比真实卫星信号强得多的伪信号，以确保目标设备优先接收并处理这些信号，适用于紧急且不考虑发射源被察觉或暴露的情况。

2）隐蔽诱骗[37-39]。通过低强度、伪装的信号逐渐引导目标无人机偏离其原轨迹，同时不引起目标系统的警觉。隐蔽诱骗需要精密的技术设计和多步实施，信号引入缓慢且渐进，采用小幅度调整，结合多模、多频段信号，模拟真实卫星信号特性，增加欺骗信号的迷惑性和隐蔽性，降低设备的暴露概率，让目标设备逐步“误入歧途”。缺点是实施过程复杂、技术难度高，需要精确的控制和监测。适用于需要精准干扰的敏感环境。

3　发展趋势及未来展望

3.1　发展趋势

随着无人机在全球范围内的广泛使用，对导航安全的要求也随之提高。无人机导航诱骗技术的发展趋势体现在以下几个关键方面：

1）诱骗与反诱骗对抗式发展。不断发展的导航诱骗技术，也会成为不法分子手中的“武器”，因此反诱骗技术在无人机安全保障系统中同样扮演着重要的角色。诱骗信号的发展同步催生了更多、更先进的诱骗检测方法，其中包括公然与隐蔽欺骗攻击检测、协同定位检测以及信息冗余裁决检测等多种检测和反制导航欺骗攻击的方法[40]，提升接收机的抗干扰与欺骗检测技术[41-42]。这些研究表明，随着空间技术和无人机

应用的迅猛发展，诱骗和反诱骗技术激烈的动态对抗，推动着相关产业和研究不断发展与完善。

2）导航诱骗技术隐蔽化。隐蔽诱骗技术正朝着高精度与微扰动的方向快速发展。传统诱骗手段常会导致接收信号数据突变，接收机容易检测到此类突变信号，不响应此类突变异常信号或切换至其他导航技术，导致欺骗的失效。新一代隐蔽诱骗技术则研究逐步引导无人机偏离预定轨迹，以微小渐进式的扰动方式实现目标偏移诱骗，从而降低被检测的概率。这种方法不仅能绕过现有的大部分监测和防御系统，还能让操控者难以察觉到异常。随着无人机反诱骗技术水平的提高，隐蔽诱骗技术在克服惯性导航上显得尤为重要。

3）多手段联合诱骗。无人机大多采用 INS/GNSS 的组合导航方式，可实现在 GNSS 卫星遮挡场景下（如隧道、地下室、楼宇等）的自主导航。另外还有部分无人机采用基于视觉即时定位与地图构建（simultaneous localization and mapping，SLAM）的定位导航，可实现无人机在复杂环境下的自主飞行。当前通过基于 GNSS 的定向导航诱骗可使搭载 INS/GNSS 组合导航模式的无人机在无意识的状态下偏离原定轨迹，但难以有效实现 SLAM 导航系统的有效诱骗。单一诱骗手段难以实现 SLAM 导航型无人机反制，需要联合其他干扰手段实现有效管控。研究表明利用电磁干扰、强光干扰、声波干扰等多种反制手段[43]进行预先处置，无人机视觉系统在受到干扰后，将被迫切换至 GNSS 导航模式，然后诱骗手段即可发挥作用，实现有效的组合诱骗。因此，未来发展趋势为基于图像视觉的诱骗干扰手段研究，利用多手段联合反制方式，结合人工智能和机器学习算法进行动态调整诱骗策略[44]，使诱骗行为能自适应环境变化和目标无人机的反应，实现对组合导航系统的目标有效诱骗。无人机诱骗多手段包括：① 基于控制信息的动态诱骗航迹规划的多模诱骗手段；② 基于图像视觉的干扰诱骗（如地面隐藏烟雾弹、强光致盲、地面设置特殊图案迷惑等手段），比如，俄罗斯海军在“戈尔什科夫海军上将”号和“卡萨托诺夫海军上将”号护卫舰上安装的“菲林”视觉光学干扰系统会对武器装备的光电设备产生“致盲”效果；③ 基于 Wi-Fi（wireless fidelity）、蓝牙和射频识别（radio frequency identification，RFID）等短距离无线技术的干扰诱骗，旨在利用电磁干扰手段，使无线设备失灵。

4）模拟卫星导航合作式应用。模拟卫星导航手段与无缝导航技术相结合实现良性合作。在无人机、汽车、手机导航等设备进入物理屏蔽场景时，由于导航终端无法接收到卫星信号场景，进而无法执行基于 GNSS 的定位和导航功能。为解决上述问题，可将卫星信号模拟设备部署至物理屏蔽的场景中，通过根据真实场景提供的可信的卫星模拟信号，使得用户端在进入该场景后无须切换导航模式即可平稳运行，从而实现无缝导航，提高安全性。该项技术在 2022 年北京冬奥会期间得到了应用，研究人员构建了以北斗伪卫星为核心，结合 5G 通信网等多源信息的定位体系架构，为张家口赛区国家跳台滑雪中心及其周边区域提供了室内外亚米级可信定位服务。

3.2 未来展望

1）违规飞行目标动态精准诱骗研究。导航诱骗通常对区域范围内的所有目标的导航定位系统均产生影响，难以对特定目标实现精准控制。未来对违规飞行的无人机目标进行精确诱骗将成为一个重要的研究方向。比如，通过对合规飞行的目标提前提供诱骗指令预警，建议其关闭卫星导航系统并切换 INS 或 SLAM 等自主导航模式，避免其受到诱骗信号干扰，从而对非合作式目标实现单独诱骗。未来，该技术的实现将为无人机集群诱骗提供重要的技术支撑。

2）导航诱骗技术及设备的合规化使用。低空经济中飞行器的大量使用使得其对低效比的卫星导航依赖急剧增加，而导航诱骗对飞行器进行处理的同时不可避免地会对周围依赖卫星导航的合法设备造成影响。因此，未来导航诱骗技术和装备应加强管控，比如对使用方式及场景进行相应合规化管理，以保障低空经济安全运行。

未来，随着技术的进步和创新，导航诱骗及反诱骗检测技术将持续演化，促进该技术领域的健康发展，以应对日益复杂的安全挑战。

4 结束语

本文围绕无人机导航诱骗技术研究展开综述，全面梳理了该领域的应用领域及发展过程，深入分析了无人机导航诱骗的基本技术原理，并按照信号生成方式、实现目的和实施显隐性对无

人机导航诱骗技术进行分类阐述。进而预测了无人机导航诱骗技术的主要发展趋势，如隐蔽诱骗、多手段联合诱骗、模拟卫星导航合作式应用等。最后提出了非合作式目标的精准诱骗研究、加强导航诱骗技术的合规化使用的展望。

参 考 文 献

[1] 汪丹. 基于 PID 算法的无人机精确诱骗方法的设计与实现[D]. 西安：西安电子科技大学，2022.
WANG Dan. Design and implementation of precise spoof method for UAV based on PID algorithm[D]. Xi'an: Xidian University, 2022. (in Chinese)

[2] 徐锐泽. 自注意力机制下的 GPS 欺骗干扰检测[D]. 贵阳：贵州师范大学，2023.
XU Ruize. GPS spoofing and jamming detection under self-attention mechanism [D]. Guiyang: Guizhou Normal University, 2023. (in Chinese)

[3] NOH J, KWON Y, SON Y, et al. Tractor beam: safe-hijacking of consumer drones with adaptive GPS spoofing [J]. ACM Transactions on Privacy and Security, 2019, 22(2): 1-26.

[4] 张琳. 卫星导航系统接收机抗干扰关键技术研究[D]. 哈尔滨：哈尔滨工业大学，2007.
ZHANG Lin. Research on key techniques of anti-interference satellite navigation receiver[D]. Harbin: Harbin Institute of Technology, 2007. (in Chinese)

[5] COUTURIER A, AKHLOUFI M A. A review on deep learning for UAV absolute visual localization[J]. Drones, 2024, 8(11): 622.

[6] SHEPARD D P, BHATTI J A, HUMPHREYS T E. Drone hack: spoofing attack demonstration on a civilian unmanned aerial vehicle[J]. GPS World, 2012, 23(8): 30-33.

[7] 闫占杰，吴德伟，刘海波，等. GPS 转发欺骗式干扰时延分析[J]. 空军工程大学学报(自然科学版)，2013，14(4)：67-70.
YAN Zhanjie, WU Dewei, LIU Haibo, et al. Analysis of time delay in GPS repeater deception jamming[J]. Journal of Air Force Engineering University (Natural Science Edition), 2013, 14(4): 67-70. (in Chinese)

[8] 王海洋，姚志成，范志良，等. 一种针对转发式欺骗干扰信号的负延时补偿方法[J]. 电讯技术，2015，55(11)：1255-1259.
WANG Haiyang, YAO Zhicheng, FAN Zhiliang, et al. A negative time-delay correction method for repeater deception jamming signal [J]. Telecommunication Engineering, 2015, 55(11): 1255-1259. (in Chinese)

[9] BAZIAR A R, MOAZEDI M, MOSAVI M R. Analysis of single frequency GPS receiver under delay and combining spoofing algorithm[J]. Wireless Personal Communications, 2015, 83: 1955-1970.

[10] 万有达. 基于固定重要目标保护的多站转发 GNSS 欺骗干扰研究[D]. 长沙：国防科学技术大学，2016.
WAN Youda. Study of multi-station distributing methods based on GNSS spoofing-signal retransmission for immovable target protection[D]. Changsha: National University of Defense Technology, 2016. (in Chinese)

[11] 史密，牟京燕，陈树新. GPS 诱骗下 GPS/INS 组合导航偏差分析[J]. 电光与控制，2016，23(2)：16-20.
SHI Mi, MU Jingyan, CHEN Shuxin. Bias analysis of GPS/INS integrated navigation under GPS deception [J]. Electronics Optics & Control, 2016, 23(2): 16-20. (in Chinese)

[12] 施林，刘伟. 基于卫星导航欺骗干扰的无人机管制技术[J]. 指挥信息系统与技术，2017，8(1)：22-26.
SHI Lin, LIU Wei. UAV management and control technology based on satellite navigation spoofing jamming[J]. Command Information System and Technology, 2017, 8(1): 22-26. (in Chinese)

[13] 戴博文. GPS 欺骗干扰技术研究[D]. 杭州：杭州电子科技大学，2018.
DAI Bowen. Research of GPS spoofing technology[D]. Hangzhou: Hangzhou Dianzi University, 2018. (in Chinese)

[14] HE D J, QIAO Y R, CHEN S Q, et al. A friendly and low-cost technique for capturing non-cooperative civilian unmanned aerial vehicles[J]. IEEE Network, 2019, 33(2): 146-151.

[15] 何江，王晓君，康娇. 基于 GPS/INS 组合导航的无人机欺骗轨迹规划[J]. 网络安全技术与应用，2019 (7)：95-97.
HE Jiang, WANG Xiaojun, KANG Jiao. Deceptive trajectory planning for UAVs based on GPS/INS integrated navigation[J]. Network Security Technology & Application, 2019(7): 95-97. (in Chinese)

[16] 李畅，王旭东. 基于轨迹欺骗的无人机 GPS/INS 复合导航系统干扰技术[J]. 南京航空航天大学学报，2017，49(3)：420-427.
LI Chang, WANG Xudong. Jamming of unmanned aerial vehicle with GPS/INS integrated navigation system based on trajectory cheating [J]. Journal of Nanjing University of Aeronautics and Astronautics, 2017, 49(3): 420-427. (in Chinese)

[17] DING Y J, FU Z J. Multi-UAV cooperative GPS spoofing based on YOLO Nano[J]. Journal of Cyber Security, 2021, 3(2): 69-78.

[18] GENG X S, GUO Y, TANG K H, et al. Research on covert directional spoofing method for INS/GNSS loosely integrated navigation[J]. IEEE Transactions on Vehicular Technology, 2023,72(5):5654-5663.

[19] GAO Y J, LI G Y. A GNSS instrumentation covert directional spoofing algorithm for UAV equipped with tightly-coupled GNSS/IMU[J]. IEEE Transactions on Instrumentation and Measurement, 2023, 72:8501413.

[20] GUO Y, WU M P, TANG K H, et al. Covert spoofing algorithm of UAV based on GPS/INS-integrated navigation [J]. IEEE Transactions on Vehicular Technology, 2019, 68(7): 6557-6564.

[21] 李畅. 无人机导航系统中的 GPS 欺骗干扰技术研究[D]. 南京:南京航空航天大学,2018.
LI Chang. Research on GPS deception jamming in UAV navigation system[D]. Nanjing: Nanjing University of Aeronautics and Astronautics,2018. (in Chinese)

[22] 陈晨. NIS 约束下的无人机诱捕技术研究[D]. 天津:中国民航大学,2020.
CHEN Chen. Research on trapping UAV under NIS constraints[D]. Tianjin: Civil Aviation University of China,2020. (in Chinese)

[23] 郭妍,唐康华,张鹭. 面向无人机的逐点偏移式卫星导航欺骗干扰方法[J]. 工程科学与技术,2023,55(2):275-284.
GUO Yan, TANG Kanghua, ZHANG Lu. GNSS navigation spoofing method of UAV based on point-by-point offset[J]. Advanced Engineering Sciences, 2023,55(2):275-284. (in Chinese)

[24] CHAE M-H, PARK S-O, CHOI S-H, et al. Reinforcement learning-based counter fixed-wing drone system using GNSS deception[J]. IEEE Access, 2024, 12:16549-16558.

[25] CHAE M-H, PARK S-O, CHOI S-H, et al. Commercial fixed-wing drone redirection system using GNSS deception[J]. IEEE Transactions on Aerospace and Electronic Systems, 2023,59(5):5699-5713.

[26] 李豹,朱银兵,曹可劲,等. 北斗导航信号欺骗干扰建模与测试[J]. 海军工程大学学报,2019,31(3):23-27.
LI Bao,ZHU Yinbing,CAO Kejin,et al. Modeling and test on spoof jamming for BeiDou navigation signal [J]. Journal of Naval University of Engineering,2019, 31(3):23-27. (in Chinese)

[27] 郭妍. INS/GNSS 组合导航模式下无人机隐蔽性欺骗方法研究[D]. 长沙:国防科技大学,2022.
GUO Yan. Research on covert spoofing algorithm of UAV based on INS/GNSS integrated navigation[D]. Changsha: National University of Defense Technology, 2022. (in Chinese)

[28] 胡常一. 无人机导航欺骗系统关键技术研究[D]. 长沙:国防科技大学,2018.
HU Changyi. Research on key technology of UAV navigation spoofing system [D]. Changsha: National University of Defense Technology, 2018. (in Chinese)

[29] 尹中杰,侯博,王海洋,等. 无人机导航诱骗技术综述[J]. 电光与控制,2024,31(11):62-67.
YIN Zhongjie, HOU Bo, WANG Haiyang, et al. A review of UAV navigation spoofing technologies[J]. Electronics Optics & Control, 2024,31(11):62-67. (in Chinese)

[30] 颜靖华,侯毅,宋滔,等. 基于 GPS 诱骗的低空民用无人机干扰技术研究[J]. 中国电子科学研究院学报,2019, 14(6):618-624.
YAN Jinghua,HOU Yi,SONG Tao,et al. Research on interference technology of low altitude civil UAV based on GPS deception[J]. Journal of CAEIT,2019, 14(6):618-624. (in Chinese)

[31] 柳亚川,寇艳红. 同步式 GPS 欺骗干扰信号生成技术研究与设计[J]. 北京航空航天大学学报,2020, 46(4): 814-821.
LIU Yachuan,KOU Yanhong. Research and design of synchronous GPS spoofing signal generation technology[J]. Journal of Beijing University of Aeronautics and Astronautics,2020,46(4):814-821. (in Chinese)

[32] 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 Pengliang, WANG Xiaoyu, XUE Rui. Induction strategy for unmanned aerial vehicle position spoofing [J]. Journal of National University of Defense Technology, 2021,43(2):40-46. (in Chinese)

[33] HE D J,LIU H, CHAN S, et al. How to govern the non-cooperative amateur drones? [J]. IEEE Network, 2019, 33(3): 184-189.

[34] YI M J, WEN Z J, LI J H. Analysis of navigation deception method based on UAV flight control[C]// Proceedings of the 6th International Conference on Advanced Electronic Materials, Computers and Software Engineering. [S. l. : s. n.],2023: 599-604.

[35] 马超. 基于 GNSS 的无人机导航欺骗关键技术研究[D]. 长沙:国防科技大学,2021.
MA Chao. Research on the key technologies of UAV spoofing based on global navigation satellite system [D]. Changsha: National University of Defense Technology, 2021. (in Chinese)

[36] SATHAYE H, STROHMEIER M, LENDERS V, et al. An experimental study of GPS spoofing and takeover attacks on UAVs[C]//Proceedings of the 31st USENIX Security Symposium. [S. l. : s. n.],

2022：3503-3520.

[37] KERNS A J，SHEPARD D P，BHATTI J A，et al. Unmanned aircraft capture and control via GPS spoofing[J]. Journal of Field Robotics，2014，31(4)：617-636.

[38] GUO Y，WU M P，TANG K H，et al. Position deceptive tracking controller and parameters analysis via error characteristics for unmanned aerial vehicle [J]. International Journal of Advanced Robotic Systems，2019，16(1)：172988141882540.

[39] BETHI P，PATHIPATI S，APARNA P. Stealthy GPS spoofing：spoofer systems，spoofing techniques and strategies [C]//Proceedings of the 17th India Council International Conference. [S. l.]：IEEE，2020：1-7.

[40] 孟涟肖. 面向导航欺骗攻击的无人机威胁检测关键技术研究[D]. 哈尔滨：哈尔滨工程大学，2023.
MENG Lianxiao. Research on key technologies of threat detection for navigation spoofing attack to UAVs[D]. Harbin：Harbin Engineering University，2023.(in Chinese)

[41] 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.（in Chinese)

[42] 耿正霖. GNSS 欺骗干扰检测和抑制技术研究[D]. 长沙：国防科技大学，2019.
GENG Zhenglin. Study on GNSS spoofing detection and mitigation techniques [D]. Changsha：National University of Defense Technology，2019.(in Chinese)

[43] 吴长柯，侯强. 无人机 GNSS 诱骗与反诱骗技术论述[J]. 全球定位系统，2020，45(3)：37-40.
WU Changke，HOU Qiang. Spoofing and anti-spoofing technology of UAV in GNSS [J]. GNSS World of China，2020，45(3)：37-40.(in Chinese)

[44] ŠIMON O，GÖTTHANS T. A survey on the use of deep learning techniques for UAV jamming and deception[J]. Electronics，2022，11(19)：3025.

作 者 简 介

吴　浩

男，1985 年生，博士研究生，高级工程师，研究方向为无人机探测与反制、低空安全管控、多源信息融合

E-mail：wuhao@skydefence.cn

江　莉

女，1988 年生，高级工程师，研究方向为无人机探测与反制、低空安全管控、多源信息融合

E-mail：jiangli@skydefence.cn

徐　婧

女，1985 年生，博士，副研究员，研究方向为信息科技战略研究

E-mail：jingxu@clas.ac.cn

张　劲

男，1975 年生，博士，教授，博士生导师，研究方向为生物医学工程

E-mail：jing_zhang@scu.edu.cn

李　权

男，1976 年生，副教授，研究方向为网络与信息安全领域

E-mail：34372110@qq.com

责任编辑　殷文卓