面向城市低空安全的反无人机技术：从探测、识别到中和

王景璟[1]，王智伟[1]，高畅[1]，陈健瑞[1,2]，杜皓华[1]，姜春晓[3]
（1.北京航空航天大学网络空间安全学院，北京 100191；2.鹏城实验室，广东 深圳 518100；
3.清华大学信息国家研究中心，北京 100084）

摘要：低空经济的快速发展推动了无人机的大规模应用，但未经授权的飞行活动日益威胁城市安全，引发碰撞、侵权及违规袭扰等严重隐患。针对这一新兴空域环境，对反无人机技术的相关研究进行了系统性综述。首先，概述了城市低空安全所面临的独特挑战，如复杂的感知环境、困难的目标识别，以及有限的反制手段等。随后，围绕感知、识别和反制3个阶段，详细梳理了当前的主流技术手段：在感知层面，涵盖了雷达、射频、光学与红外、声学及多模态融合等探测技术；在识别层面，剖析了基于身份与基于行为的识别技术；在反制层面，归纳了干扰压制、欺骗劫持、物理捕获、打击毁伤等中和技术。同时，总结了各阶段的核心评估指标与实验环境设定，对比了学术界与工业界之间的差异。最后，展望了反无人机技术的未来趋势，即感知网络化、识别智能化与反制协同化。

关键词：低空安全；反无人机技术；多源感知；分类识别；目标中和
中图分类号：V279
文献标志码：A
doi：10.11959/j.issn.1000–436x.TXXB260380

Anti-UAV technologies for urban low-altitude security: from detection and identification to neutralization

Wang Jingjing[1], Wang Zhiwei[1], Gao Chang[1], Chen Jianrui[1,2], Du Haohua[1], Jiang Chunxiao[3]
1. School of Cyber Science and Technology, Beihang University, Beijing 100191, China
2. Peng Cheng Laboratory, Shenzhen 518100, China
3. School of Information Science and Technology, Tsinghua University, Beijing 100084, China

Abstract: While the booming low-altitude economy accelerates UAV adoption, unauthorized flights increasingly threaten urban safety, giving rise to collision, privacy-related, and security risks. Addressing this emerging airspace environment, anti-UAV technologies were reviewed systematically. Firstly, key urban low-altitude challenges were outlined: complex sensing environments, difficult target identification, and limited countermeasure options. Subsequently, mainstream technologies were reviewed across three stages: sensing (radar, RF, optical/infrared, acoustics, and multimodal fusion), identification (identity- and behavior-based methods), and countermeasures (jamming, spoofing/hijacking, physical capture, and kinetic damage). Meanwhile, core evaluation metrics and experimental setups were summarized, highlighting the gap between academia and industry. Finally, future trends were discussed toward networked sensing, intelligent identification, and collaborative countermeasures.

Key words: low-altitude security, anti-UAV technology, multi-source sensing, classification and identification, target neutralization

收稿日期：2026–06–29；**修回日期：**2026–08–23
通信作者：王景璟，drwangjj@buaa.edu.cn
基金项目：国家自然科学基金资助项目（No.U24A20213, No.62571011, No.72542016）；北京市自然科学基金资助项目（No.QY24126）
Foundation Items： The National Natural Science Foundation of China (No.U24A20213, No.62571011, No.72542016), The Natural Science Foundation of Beijing (No.QY24126)

0　引言

近年来，低空经济这种新型经济形态发展迅速。由相关数据可知，2023 年我国低空经济规模已达 5 059.5 亿元，同比增长约 33.8%，预计到 2035 年将会突破 3.5 万亿元[1]。低空经济是国家战略性新兴产业与未来产业的培育重点，它的发展不仅需要无人机等新型航空器技术的进步，还需要完善的空域分类管理、适航审定、运行监管以及安全保障等制度体系[2]。在未来，随着制度的不断完善，低空经济将在智慧交通、物流配送等多领域有越来越多的应用。

然而，低空空域高密度飞行也会带来严峻的安全挑战，特别是城市场景下大量无人机的无序涌入已经对公共安全造成了直接威胁。虽然无人机的常规飞行高度与民航巡航的高度并不重叠，但在机场周边及起降航线附近，违规无人机的侵入已经多次威胁到了民航的安全运行，例如，成都双流机场曾因无人机扰航导致超万名旅客滞留。另一方面，部分无人机被用于非法航拍或违禁品运输，这严重威胁到了城市安全和隐私保护。此外，低空环境复杂，且现有监管体系不完善，很难实现对高隐蔽、不易预测的非法无人机的可靠管控，整体安全风险增大。这些现实中存在的痛点，更加凸显了研发和部署反无人机技术的重要性和紧迫性[3]。

这一重要性和紧迫性也直接反映在学术研究的发文趋势中。自 2018 年以来，全球反无人机技术研究热度持续攀升，发文量稳步增长，2018—2024 年反无人机技术发文趋势如图 1 所示。具体而言，该领域的研究热点正从单一的探测、识别与中和技术，逐步转向多传感器融合、协同防御及空天地一体化等系统防控方向，以满足城市低空场景的安全需求。

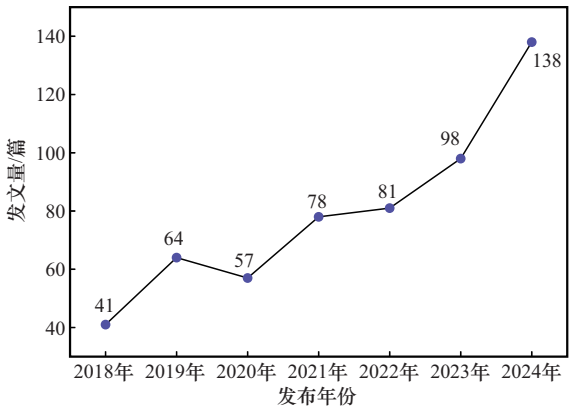

图 1　2018—2024 年反无人机技术发文趋势

在此背景下，反无人机技术实际应用场景不断拓展，其典型应用场景如图 2 所示。

为了更好地应对城市低空场景下的安全风险，

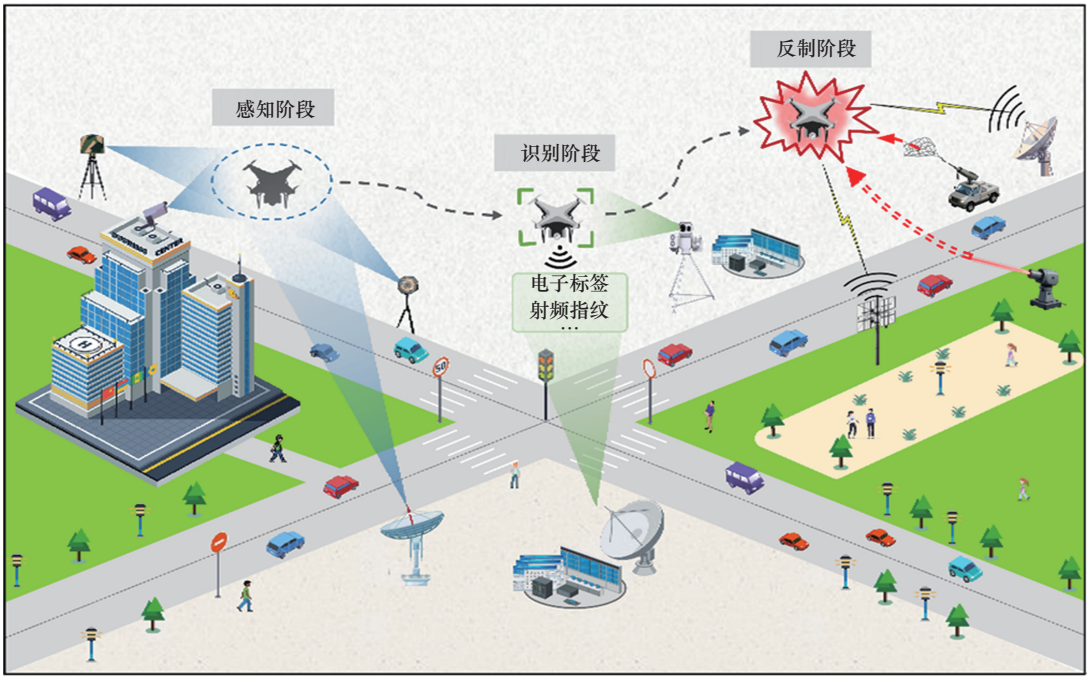

图 2　反无人机技术的典型应用场景

需要对现有的反无人机技术进行全面梳理与评估。本文旨在全面综述该领域的研究进展，分析各类技术在低空环境下的优缺点，方便后续的理论研究与工程实践。

1　研究背景与安全挑战

为系统论述城市低空场景下反无人机系统的设计前提，首先，本节深度剖析复杂低空环境中反无人机系统面临的挑战，阐明感知、识别与反制层面的核心技术难点；其次，系统梳理无人机目标的“人–机”双维特征及威胁分级特性，指出反无人机系统必须具备差异化的动态处置能力；再次，归纳现行的政策法规与监管框架，厘清其对无人机目标与反无人机系统的双向约束边界；在此基础上，探讨地理围栏这一预防性空域管理与合规控制技术的防范原理及其局限性；最后，提炼反无人机系统的工作流程并将其概括为五大阶段，从而为后续探测、识别与中和技术的详细论述提供整体框架。

1.1　反无人机系统面临的挑战

相较于 1 000 m 以上的传统中高空空域，复杂的低空环境使反无人机系统的实际运行面临独特挑战，具体表现为以下 3 个方面：感知难、识别难和反制难。

感知难：环境复杂化制约传感效能。城市密集建筑引发的遮挡与多径效应，直接降低了雷达与射频定位的有效性[4]。同时，城市高强度背景噪声严重干扰声学探测，大幅增加系统误报率。此外，无人机 20~120 m 的低空飞行特征使其极易与鸟类、城市反光等背景杂波混淆，致使视觉与红外传感器的检出率显著下降[5]。因此，反无人机系统必须具备多模态感知体系与复杂环境适应能力。

识别难：目标同质化阻碍精准识别。在城市低空空域，合法与非法目标交织，二者在气动外形、工作频段及通信协议上高度同质化，导致基于物理外观或射频特征的传统识别方法极易失效。为此，现有系统多采用静态的“黑白名单”机制，即通过比对目标电子标识与已知数据库进行身份识别。然而，该机制对缺乏电子标识的自制与改装无人机目标的识别效果欠佳[6]。此外，合法目标误入管制区域、非法目标伪造合法协议的现象也时有发生，这同样加剧了现有系统的误判与漏判风险。因此，反无人机系统必须具备更精细的身份识别与行为意图分析能力[7]。

反制难：影响敏感化掣肘反制手段。传统反制手段多具破坏性，在人口与设施密集的城市场景下存在显著局限性。具体而言，电磁干扰手段易对周边合法通信导航设施造成附带影响，动能拦截手段（如网枪、枪械或激光）则极易引发针对人员与财产的二次伤害，两者均难以在民用空域常态化部署。此外，城市无人机目标的高密度与强机动性，进一步压缩了系统的有效响应窗口。因此，面对严苛的安全约束与极短的决策时间，反无人机系统必须具备多源信息处理与人工智能辅助决策能力[8]。

综上，为了应对感知难、识别难和反制难这三大挑战，新一代反无人机系统必须针对性地攻克探测、识别与中和的技术难题。

1.2　“人–机”双维特征及威胁分级特性

商用、民用无人机集成了多类传感与通信模块，支撑其自主飞行和任务执行。其中，光电/红外传感器负责图像采集、目标识别和环境感知；惯性测量单元依托加速度计与陀螺仪实现姿态估计与短时导航；全球导航卫星系统构成了轨迹规划的核心，负责提供高精度位置和速度数据；无线通信模块则维系与地面站的遥控链路、图传链路及数据链路。部分平台为满足环境建模、避障和定高的需求，还选配了激光雷达、超声波传感器或气压高度计。上述硬件载荷和通信链路是飞行安全的基础，但也成为反无人机系统实施电磁压制或协议接管的突破口[9]。

除无人机特征外，操作者群体的复杂性特征同样深刻影响着目标的威胁等级与反无人机系统的设计需求。合规操作者风险最低，其核心诉求在于避免被系统误判为非法目标。无经验操作者易因技能欠缺或航线规划不当误入管制空域，虽主观危害有限，但极易诱发次生安全事故。非法操作者多为未经注册或蓄意规避监管的人员，其飞行行为隐蔽且轨迹无序，构成城市空域管理中的灰色隐患。恶意攻击操作者多具备较强的技术能力和规避手段，常通过采用改装平台、关闭电子信标或伪造合法协议等方式，对公共安全构成实质性威胁[10]。因此，城市低空场景下的威胁分级特性，客观上要求反无人机系统必须具备差异化的动态处置能力：对合规

目标须避免误判干扰；对误入目标宜采取非破坏性的驱离或诱导；对非法与恶意目标，则须部署严苛的强制中和策略。

1.3 政策法规与监管框架

政策法规与监管框架确立了反无人机系统部署的合法性基础与设计边界。国内层面，《无人驾驶航空器飞行管理暂行条例》作为民用无人机运营的基础性法规，确立了实名登记、飞行备案以及统筹公共与国家安全的运行原则[11]。《民用无人驾驶航空器运行安全管理规则》等配套规章则明确了空域管理、适航标准与追责处罚机制，并严格规范了无人机的飞行高度、活动区域及运营许可[12]。国际层面，各国也相继出台监管规章。例如美国联邦航空管理局实施的《Remote Identification》，强制要求所有已注册或预注册的无人机在飞行期间实时广播遥控器和飞行器的身份和位置[13]。

现行的管控措施包含了对无人机目标的禁飞空域、禁飞时段以及高度限制。我国法规严禁无人机驶入民用机场净空区和法定禁飞区域，并强制实行实名登记准入制[12]。类似地，美国的《Remote Identification》法规实现了对非法飞行活动和越界闯入禁飞区设备的甄别[13]，也成为一种核心管控手段。

同时，法规对反无人机系统的使用方式和手段也施加了限制。例如，无线电干扰技术会波及周边合法的通信与导航设施，因此这类反制手段在多数民用城市场景中被严格管控，在机场周边与管制空域受限更大[12]。此外，人口密集区、重点安保区与关键基础设施区等区域的受限等级和法律追责标准不同，直接影响反无人机系统可以采用的探测、识别与中和手段。

1.4 地理围栏技术

在当前政策法规和监管框架下，地理围栏成为无人机端侧落实合规要求的关键技术手段。其核心机制是将禁飞区与限高区等空域规则映射为虚拟边界，在目标逼近或企图越界时自主触发悬停、返航或迫降等限制指令。该技术依托全球导航卫星系统定位与云端数据库，兼具低成本与易部署优势，现已广泛普及于商用与消费级无人机，有效约束了常规用户的活动空域[8]。政策层面，中华人民共和国国务院、中华人民共和国中央军事委员会发布的《无人驾驶航空器飞行管理暂行条例》和美国联邦航空管理局的B4UFLY计划，均鼓励制造商将地理围栏功能集成到飞行控制系统中，以辅助合规运营[11,13]。然而，地理围栏作为一种内嵌式模块，其约束效力高度依赖于终端系统的完整性与用户的合规意愿，因此在面对蓄意规避限制或被恶意篡改的无人机时，往往形同虚设。由此可见，地理围栏本质上被界定为一种预防性的空域管理与合规控制技术，并不属于反无人机系统的范畴。

1.5 反无人机系统工作流程

综合城市空间特征、无人机威胁分类及现行监管约束，并结合已有研究[4,6]，城市低空场景下反无人机系统的工作流程可概括为五大阶段：一是预防阶段，即利用地理围栏等前置手段实施空域约束，防止合法用户误入敏感区域；二是感知阶段，即依托多源手段持续监测低空空域，实现对可疑目标的早期发现；三是识别阶段，即结合目标身份、轨迹特征与空域规则，综合判定目标的合法性及威胁等级并形成处置建议；四是反制阶段，即依据识别结果，执行从干扰引导到物理摧毁的分层应对措施；五是反馈阶段，即记录处置信息与事件数据，并回传至监管平台以支持问责与系统优化。综上所述，反无人机系统的工作流程如图3所示。本文第2～4节将以此流程为脉络，分别对感知阶段的探测技术、识别阶段的识别技术，以及反制阶段的中和技术展开详尽论述。

2 反无人机系统中的探测技术

感知阶段是反无人机系统的首要环节，系统通过传感器捕获空域内的潜在目标，并输出其初步的空间位置与运动参数。该阶段的重点是无差别地发现所有飞行器，但暂时不判定其身份与合法性。系统依托具体的物理探测技术实现这一感知任务，这也构成了系统早期预警的核心基础。当前主流的探测技术主要包括雷达探测、射频信号探测、光学与红外探测以及声学探测4类。各类探测技术的整体特点如表1所示。

2.1 雷达探测

雷达探测可以实现大范围内全天候的空域监测，是反无人机系统中最成熟、应用最广的技术。按照是否依赖自身辐射源划分，雷达主要包括主动雷达与被动雷达两类。

主动雷达通过发射高频电磁波并接收目标反射信号获取无人机的距离、速度及方位等信息[6]，常

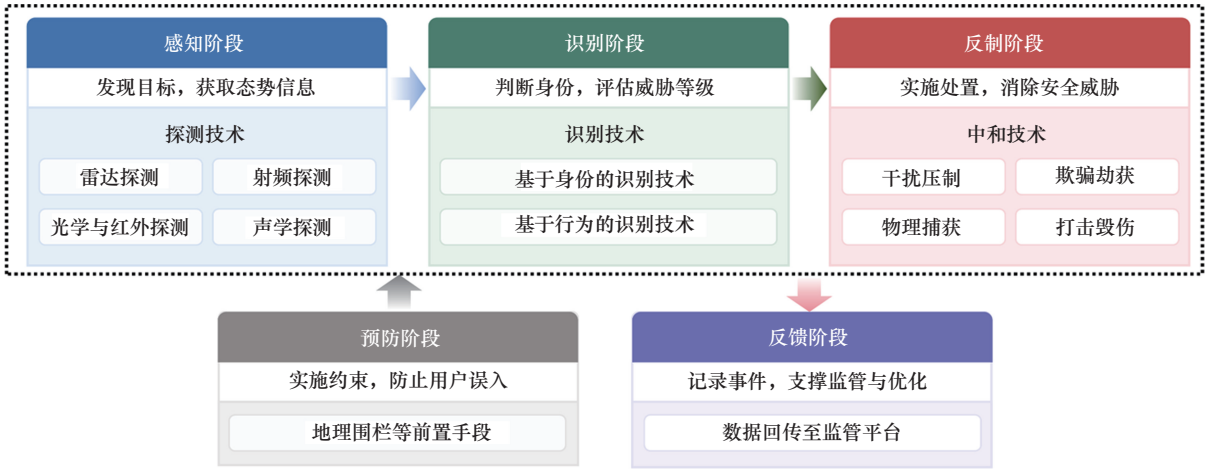

图3　反无人机系统的工作流程

表1　　**各类探测技术的整体特点**

探测技术	天气敏感性	抗干扰能力	隐蔽性	静默可探测	设备成本	探测范围/ km	文献
雷达探测	弱	强	弱	能	高	3	文献[14-21]
射频探测	中	弱	强	不能	中	1	文献[22-28]
光学与红外探测	强	中	强	能	低	3	文献[29-34]
声学探测	中	中	强	能	低	0.2	文献[35-36]

应用在机场、边境及城市空域的安全管理中。现有系统多工作在X波段和Ku波段，部分系统采用多波段融合体制增强对中大型无人机的探测[4]。然而，主动雷达在对低空微小型无人机目标的探测上仍存在很大的挑战。无人机多采用塑料或复合材料机体，雷达散射截面较小，在实际环境中极易与鸟类、风筝等杂波目标混淆，引发误报[6]；同时，复杂地形或城市密集建筑造成的多径效应及遮挡易造成探测盲区，降低了覆盖的连续性[37]。由此，微型无人机的有效探测距离一般为1～5 km，高性能三维雷达可将探测距离扩展到15～20 km，但在城市环境中，该距离往往还是会被压缩到3 km以内[5]。为此，近期研究主要关注微多普勒特征挖掘与新型体制的应用。Babu等[14]将微多普勒特征与多基站雷达结合，在复杂环境中对微型无人机识别准确率可达98%以上。Nucum等[15]利用无人机与鸟类的微多普勒精细化建模，减少了系统的误报。此外，基于V波段的多输入多输出（multiple-input multiple-output，MIMO）雷达结合数字波束成形技术，在高分辨率探测方面发展潜力较大[16]。相关研究结果显示，不同类型的无人机旋翼结构和多普勒调制特性存在固有差异，在约10 km的范围内可以进行一定程度的类型识别[17]。尽管前沿研究解决了一些缺陷和问题，但主动雷达在城市低空环境中的性能仍受目标尺度与环境复杂性的双重制约。因此，主动雷达更适合作为反无人机系统的基础监测手段，为系统提供大范围、全天候的空域感知能力。

被动雷达则利用环境中已有的第三方无线电辐射源进行目标探测，成本低、能耗小、隐蔽性强。其适合应用在电磁受限或对辐射敏感的场景，并且在电子对抗的条件下有较强的生存能力[18]。然而，该系统的探测性能高度依赖外部信号源分布，三维定位精度有限，且其在复杂城市电磁环境中易出现误报和漏检，系统部署难度与信号处理复杂度较高[7]。为了弥补上述缺陷，近期研究改进信号处理算法并引入新型辐射源，尝试提升被动雷达的性能。Sun等[19]基于长期演进（long term evolution，LTE）基站信号和数字阵列构建了双基地被动雷达系统，在无人机轨迹跟踪中实现了米级精度。Raja等[20]利用卫星数字视频广播信号的前向散射拓扑结构，并结合微多普勒效应，验证了被动雷达对弱散射目标的探测能力。相关实证研究同样为基于LTE的雷达系统配置和信号处理提供了核心支

撑[21]。这些研究有效降低了被动雷达对外部信号源分布的依赖，增强了其在城市环境中的识别与跟踪能力。在有源辐射受限或外源信号丰富的场景下，被动雷达可以作为主动雷达的补充，具有独特优势。

总体而言，主动雷达在覆盖范围和连续监测方面优势明显，而被动雷达在隐蔽性和电磁生存能力方面表现突出。在城市低空场景下，将主/被动雷达进行融合应用有助于弥补单一体制的性能局限，是提升反无人机系统在复杂城市环境中整体探测能力的有效途径。

2.2 射频探测

射频探测通过持续监测无人机与地面控制站之间的无线电通信链路，实现对低空目标的态势感知。其核心原理是捕获无人机通信系统在常用频段（如2.4 GHz和5.8 GHz）内发射的射频信号，并对其进行时频特征分析与参数提取。该技术由于不依赖视觉视距，因而具备较强的抗遮挡与跨非视距传播能力，且能通过对上行链路的逆向跟踪实现对地面操作者的溯源定位，适用于大多数采用常规遥控体制的无人机场景[22]。然而，射频探测的局限性也十分明显。一方面，对于采用全自主飞行或预编程航线控制的无人机，由于其在运行过程中不依赖地面站的通信且不产生射频辐射，该方法无法对其进行有效识别[23]；另一方面，在电磁干扰密集的城市环境中，该方法极易受到背景噪声与同频干扰的叠加影响，导致出现误检或漏检，其有效探测距离在典型城区场景下通常不足1 km[24]。

针对上述不足，近期研究主要聚焦于先进信号处理算法与鲁棒性定位方法的开发，以提升射频探测在复杂电磁环境中的实用化水平。在低信噪比与强干扰场景下，基于时频图像特征并采用深度学习构建的检测器，展现出显著优于传统分类器的鲁棒性[25]。循环平稳特征分析方法则使系统可以更好地识别与协议无关或跳频的链路[26]。为打破测向与定位瓶颈，新型入射角估计方法结合了单通道接收与波束切换阵列，在有限的硬件复杂度下对宽带突发信号的测向效果良好[27]。同时，利用接收信号强度指示比值与几何约束的轻量级算法，无须部署高昂的同步设备即可对无人机控制器进行米级高精度定位[28]。这些研究缓解了外界干扰和信号方向图时变对传统射频探测的影响，使系统可以更好地适应环境。

总体而言，射频探测是获取无人机电磁身份、追踪地面操作者的核心手段。然而，该技术高度依赖无线电辐射信号，无法探测实施射频静默或全自主飞行的无人机目标。因此，在城市低空场景中，需要引入其他探测技术以实现多维能力的互补。

2.3 光学与红外探测

光学与红外探测是反无人机系统中最为直观、应用也最为广泛的感知手段，主要依托图像和辐射信息实现对低空无人机目标的探测与识别。其中，光学探测利用摄像机与图像处理算法提取目标的纹理和几何特征，成本低、部署灵活并且可以直接提供图像级证据，多应用于机场、城市核心区及重要基础设施的监控取证[29]。然而，该技术的探测性能受光照与气象条件影响显著，在夜间、雾霾等低能见度环境下，系统的目标探测率会急剧下降，其中典型光学摄像机的有效探测距离通常会被压缩到0.5～3 km[6]。红外探测则利用目标与背景之间的热辐射温差进行成像。由于不依赖可见光，其在夜间、弱光或部分遮挡的条件下仍能保持工作[6]。该技术能够精准捕捉无人机电机、螺旋桨及电池等关键部件的热辐射特征，由此确认目标存在并进行后续的取证工作[32]。尽管如此，红外探测在实际应用中仍有特定局限。微小型无人机的自身热信号较弱，当目标与背景温差减小或出现“热交叉”现象时，系统极易发生漏检与误检[38]；另外，复杂城市环境中的多热源干扰也会使系统误报增加[39]，同时还会导致有效探测距离缩小到3 km以内[33]。

为解决上述缺陷，近年来该领域更加关注智能化算法与多模态融合方向。研究人员开始引入深度学习技术，使系统的目标探测和识别更加鲁棒。部分研究还利用了多尺度特征提取与数据增强策略，提升了复杂背景下系统对微小目标的探测能力[29]。在红外成像方面，研究人员引入可变形卷积结构，大幅增强了系统的弱信号识别和杂波抑制性能[40]。同时，光学与红外的融合探测正成为提升系统连续性与可靠性的重要方向。光学传感器能够提供高分辨率的纹理与结构信息，而红外传感器则弥补了光学传感器在低能见度环境下的成像短板，二者协同互补，使系统可以在全天候和多场景下可靠识别[6]。目前，这种融合机制逐渐转变为深度学习驱动的多模态架构，采用卷积神经网络与多分支特征

提取模型，可以实现跨模态特征的高效对齐和目标信息的深度融合。相关实验结果显示，在夜间及恶劣天气条件下该多模态融合系统的探测性能要优于单一传感器系统[41-42]。

总体而言，光学与红外的融合探测弥补了单一传感器的不足，成为新一代反无人机系统的重要技术手段。在机场、能源枢纽和大型公共活动等城市低空场景中，该融合体制能够昼夜连续监测并进行图像级取证，保障重点低空区域的安全。

2.4　声学探测

声学探测主要用麦克风阵列采集无人机螺旋桨或发动机在运行过程中产生的特征声纹信号，并利用时频分析与特征匹配算法探测低空目标。不同类型的无人机在旋翼数量、转速及结构设计上存在固有差异，在频谱分布与调制特性上形成了易于区分的声学特征，可支撑目标识别。该技术无源隐蔽、结构简单、易于小型化与低成本部署，适合在视距受限或声波环境复杂的城市密集场景中应用。然而，由于声波空间传播特性的限制，该技术对环境噪声、风速、降雨等背景条件高度敏感，在交通噪声密集或背景声复杂的区域容易出现误报和漏检[6,8]。因此，声学探测的有效作用距离通常小于300 m。

针对上述瓶颈，近年来该领域的研究主要聚焦于声学特征提取与分类算法，目的是提升系统在复杂环境下的鲁棒性。无人机声纹识别任务通过引入基于卷积神经网络和循环神经网络的深度学习方法，挖掘了微弱声纹在时频域的深层表征，提高了复杂背景噪声条件下系统的识别准确率。同时，引入多模态融合机制成为突破单一声学传感器性能极限的重要途径。声学特征与光学或射频特征的异构数据融合，可在不破坏系统无源隐蔽性的基础上抑制杂波并降低误报率，增强系统对低空微小目标的稳定探测能力[35-36]。

总体而言，受限于物理传播机制，声学探测技术难以独立承担大范围的空域监测任务。然而，其无源性、便携性和低成本的特点使其成为反无人机系统重要的补充手段，在实际部署中常应用于近距离预警、盲区覆盖以及多传感器融合体系中的辅助感知层。

2.5　多传感器联合探测

多传感器联合探测集成了雷达、射频、光学、红外及声学等多维探测手段，对低空无人机目标进行协同探测、识别与跟踪，可以实现不同传感器之间的互补融合，突破了单一传感器的性能上限。例如，系统可以用主动雷达捕捉实施射频静默的低空自主飞行无人机；而对因视觉遮挡或热差减小导致光学和红外传感器漏检的目标，系统可利用射频或声学手段补充探测[6]。这种多源协同体制能够扩展系统的空域覆盖范围，使整体探测的鲁棒性、准确度提升，还可以增强系统适应复杂电磁与气象环境的能力。然而该体制也存在系统结构复杂、硬件成本高昂等局限，且其对数据融合和智能算法有更高的要求[7]。近期研究显示，深度学习驱动的多模态融合方法在目标探测方面存在较大优势[43-44]。

总体而言，在工程实现层面，多传感器融合技术已经较为成熟，相关方案主要由工业界推动，且普遍应用于实际系统。而学术界多将其作为系统的集成手段，较少对融合机制本身进行深入研究。在城市低空场景下，该技术已经成为反无人机系统的主流发展方向，可以更稳定地防护城市重点区域。

3　反无人机系统中的识别技术

在反无人机系统中，探测与识别技术既环环相扣又各有侧重。探测的核心任务是实时感知并确认空域内是否存在无人机目标；而识别则进一步确定目标的具体属性、身份特征及潜在威胁等级，是确保后续中和过程精准、合规的关键前提。在实际复杂场景下，受鸟类、风筝等杂波的干扰，单纯依托探测技术一般只能捕获目标的物理存在，无法判别其具体类别，极易导致系统高频虚警[6]。因此识别技术是整个反无人机系统中非常重要的一环。

目前，主流的无人机识别技术体系分为两类：一是基于身份的识别，其典型代表包括射频识别（radio frequency identification，RFID）、广播式自动相关监视（automatic dependent surveillance-broadcast，ADS-B）和射频指纹识别（radio frequency fingerprinting，RFF）等体制；二是基于行为的识别，其主要依托飞行轨迹预测等方法实现。值得注意的是，虽然地理围栏作为前置管控手段已在多国推行使用，但其在国际上并非强制性标准。由于各国政策环境及不同厂商准入规范的差异，部分消费级或自制无人机仍游离于统一监管之外[7]。此外，在城市低空经济高密度运行场景下，常有合法注册的无人机因执行物流、巡检等常规任务进入

防区或特定敏感空域。面对这类复杂态势，系统亟须通过识别技术深度验证目标的真实性与合法性，避免产生防御误操作，并为后续的威胁评估与分级响应提供支撑。各类识别技术的整体特点如表 2 所示。

3.1 基于身份的识别

身份识别是反无人机系统中的关键环节，通过设备或信号特征确认无人机的合法性和身份属性，实现差异化管控与精准处置。现有的基于身份的识别技术主要包括射频识别、广播式自动相关监视及射频指纹识别等方法。

射频识别技术主要通过在无人机上加装电子标签并利用地面设备读取完成身份信息的采集与识别。该技术成本低、增重轻，且易于部署，适合在短距离监控场景中应用[6]。然而，该方法依赖额外硬件部署，且识别距离有限，在大范围空域或复杂环境中受限。为弥补不足，部分研究尝试将射频识别技术与计算机视觉技术融合，利用空间图像信息弥补射频覆盖盲区，进而提升系统的稳定性[45]。

广播式自动相关监视技术要求无人机按照固定周期主动广播自身的位置、高度及识别码等信息，由地面站或其他无人机进行接收。与射频识别相比，ADS-B 的覆盖范围更广、信息标准化程度更高，适用于大规模空域管理。然而，该技术的系统成本与能耗相对较高，且现行广播信号易受到电磁干扰或恶意篡改。针对上述问题，相关研究提出了轻量化的 ADS-B 模块设计，在大幅降低运行能耗的同时，显著提升了其在民用无人机平台中的适用性[7]。

射频指纹识别技术是近年来兴起的新方向，其直接利用无人机通信链路中硬件不完善引入的固有差异作为身份“指纹”。与传统 RFID 和 ADS-B 不同，RFF 属于非协作式识别，仅需被动采集目标发射的无线信号，具有无须改变无人机结构、隐蔽性较强、难以伪造等独特优势。然而，该技术易受信道衰落效应、电磁背景噪声及接收端硬件畸变的影响，因而环境敏感度较高，并且该技术仍处于起步阶段，现有研究多局限于原型验证与方法探索，缺乏多场景、多条件下的系统性评估。最近一项研究基于无人机遥测无线电的瞬态 I/Q 信道数据，通过联合卷积神经网络与自组织映射网络构建射频指纹识别算法，在 30 dB 室内测试中实现了 92.3% 的平均识别率，并完成了室外可行性验证[49]。

总体而言，在城市低空场景下，基于身份的识别技术通过区分无人机的身份属性，为反无人机系统的精准管控提供核心支撑，从而在减少误拦截的同时，有效提升系统的处置效率与空域资源利用率。

3.2 基于行为的识别

与基于身份的识别技术不同，基于行为的识别技术更关注无人机的实际行动与潜在意图。该技术主要依赖飞行轨迹预测，即通过连续分析无人机的实时空间位置、三维飞行轨迹、速度和加速度等多维动力学特征，推断目标的未来位置与运动模式，识别目标是否存在航线偏离、异常悬停或急速逼近等异常行为。该技术无须目标身份信息便可自主识别潜在威胁，并评估威胁等级[6]。

然而，在实际工程应用中，该技术主要基于视频信息，极易受到强光照射、雨雪大雾等复杂气象条件，以及空域中多目标交叉遮挡与背景杂波的干扰，导致轨迹跟踪与预测精度受到不同程度的降低。为了解决上述问题，现有的研究引入了深度学习与概率建模方法来增强特征提取能力并提高鲁棒性。部分研究基于长短期记忆网络进行飞行轨迹预测，利用其在处理长序列时间数据上的优势，在无人机集群场景下取得了较高的预测精度[50]。同时，针对传统长短期记忆网络未充分挖掘多维数据间的关联且缺乏对关键特征的权重增强机制等问题，研究人员进一步引入了注意力机制，通过强化重要数据并削弱次要因素的影响，实现了对飞行器四维轨

表 2 各类识别技术的整体特点

识别技术	典型方法	协作模式	伪造风险	隐蔽性	环境敏感度	成本	文献
基于身份	RFID	协作式	中	弱	中	低	文献[45]
	ADS-B	协作式	高	弱	高	高	文献[46-47]
	RFF	非协作式	低	强	高	中	文献[48-49]
基于行为	飞行轨迹预测	非协作式	低	强	高	中	文献[50-52]

迹更为精准的时空特征捕获与动态预测[51]。此外，还有研究利用生成对抗网络进行异常轨迹识别，通过对抗训练提升模型的泛化能力，能够有效区分合规飞行和异常飞行[52]。

总体而言，在城市低空场景下，基于行为的识别技术承担着评估目标威胁等级的任务，是反无人机系统决定采取何种中和措施的直接依据。

4　反无人机系统中的中和技术

中和技术是反无人机系统实施反制的核心手段，目的是削弱或消除潜在的低空安全威胁。按照破坏机理与毁伤形式划分，中和技术通常归为软杀伤与硬杀伤两类：软杀伤主要通过干扰压制、欺骗劫持等方式使无人机通信瘫痪、触发返航或迫使其就地降落；硬杀伤则依托物理捕获、打击毁伤等方式对无人机实施直接捕获与摧毁。当前，主流的中和手段可以分为干扰压制、欺骗劫持、物理捕获、打击毁伤四大类。各类中和技术的整体特点如表 3 所示。

4.1　干扰压制

干扰压制技术是指通过向无人机的工作频段施加高功率电磁能量，以干扰或淹没目标信号的软杀伤中和技术。该技术能够直接破坏无人机与控制器、卫星定位系统间的正常数据交互，使其脱离操纵者的控制，进而触发返回起点或紧急降落等应急响应。根据作用对象的不同，此技术通常可分为两类：射频干扰和全球导航卫星系统（global navigation satellite system，GNSS）干扰。

射频干扰技术通过在无人机与控制器的通信频段发射高功率电磁信号，使接收机无法正常解调，进而导致链路中断，触发无人机返航、悬停或迫降等应急响应。该技术的作用距离通常在 10 km 以内，具备响应速度快、覆盖范围广且对通信协议不敏感等核心优势，非常适用于紧急情况下的快速处置[6]。然而，传统的干扰压制技术不具备选择性，极易对周边合法通信设施造成附带干扰[8]。针对这一问题，研究人员提出了多种改进思路，如利用阵列天线进行波束成形实现能量的定向集中，同时结合频谱感知与自适应算法对目标频段进行针对性抑制，或采用多节点协同干扰，在扩大干扰范围的同时降低单点发射功率，减少对无关用户的干扰[53]。

GNSS 干扰技术是通过在导航频段发射高功率电磁信号以覆盖卫星信号，使无人机因无法可靠解算自身位置而产生航迹漂移或位置丢失，进而触发返航、迫降等应急响应。与射频干扰技术相比，该技术直接作用于导航信号，而非地空通信链路，并同样对复杂的通信协议细节不敏感。该技术的作用距离通常在 15 km 以内，其优势在于能够快速削弱无人机的自主导航与路径规划能力，迫使其偏离预设航线[56]。然而，针对采用多模卫星导航或惯性导航的无人机，该技术的干扰效果显著下降，且大范围使用时极易对周边的民用导航服务造成附带干扰[57]。针对上述问题，有研究基于地形传播模型进行分布式干扰效能评估与部署优化，通过协调多点定向辐射以及功率、指向管理，在目标空域内形成局部抑制场[58]。

总体而言，在城市低空场景下，干扰压制技术被定位为局部、短期的软杀伤中和技术。其中，射频干扰技术属于相对低风险的管控措施，主要服务于突发态势下的局部快速处置。而 GNSS 干扰技术则属于高风险的管控措施，主要服务于紧急空域封锁或重大活动安保，不宜作为常态化反制手段。在实际部署中，干扰压制技术应与探测、识别等前置技术协同配合，在准确掌握目标态势的前提下实施有限度的定向干扰，从而在保障反制效能的同时，最大程度降低对低空合法运营活动的附带影响。

4.2　欺骗劫持

欺骗劫持技术是反无人机系统中一类典型的软杀伤中和技术，其核心原理是通过人为构造的虚假信号、传感器信息或控制指令等误导无人机的导航

表 3　各类中和技术的整体特点

中和技术	破坏性	对周边环境干扰	附带损伤风险	无人机型号依赖性	范围	文献
干扰压制	低	高	高	中	远	文献[53-58]
欺骗劫持	低	中	低	中	中	文献[59-62]
物理捕获	中	低	中	低	近	文献[63-67]
打击毁伤	高	高	高	低	中远	文献[68-69]

或控制系统，使其偏离预定航线、改变任务行为，甚至实现安全接管[6]。根据作用对象的不同，该技术主要可分为GNSS欺骗、机载传感器欺骗以及劫持控制三类。

GNSS欺骗技术是目前研究最成熟、应用最广泛的欺骗手段，其基本原理是通过在导航频段发射与真实卫星同步的虚假信号，以高功率逐渐覆盖原始信号，使无人机因跟踪锁定虚假导航数据而产生错误的定位结果。与GNSS干扰技术不同，该技术不会中断信号链路，而是通过注入虚假信号误导无人机，从而在保持其正常通信的同时实现轨迹控制[70]。该技术的作用距离通常在2 km以内，具备非接触、远距离、低风险等核心优势，非常适用于反制严重依赖卫星导航的无人机。然而，GNSS欺骗技术对时频同步和相位控制的精度要求极高，且针对采用多模导航或惯性导航的无人机，其欺骗效果显著下降。针对上述问题，有研究尝试利用多频同步生成、波束定向发射与动态欺骗路径规划等方法，以提高其制导精度与隐蔽性，使其能够在复杂的城市环境中有效作战[59]。

机载传感器欺骗技术则是通过构建虚假的环境输入或传感器数据，诱导无人机对自身姿态或外部距离产生错误感知，进而丧失稳定控制。与GNSS欺骗技术不同，该技术直接作用于无人机的自主感知系统，因此特别适用于反制依赖视觉、惯性或激光测距等多元感知手段的无人机。然而，目前大多数无人机仍以GNSS导航为主，其他机载传感器多作为辅助，机载传感器欺骗技术的相关研究成果明显较少。此外，该技术通常需要在较近距离内实施，且易受到地形遮挡和环境噪声的影响，在复杂场景下的应用范围受限。Davidson等[71]提出了一种通过视觉输入欺骗来实现飞行路径偏转的方法，证明了机载传感器欺骗技术在精确干预方面的潜力，但也表明其在实际对抗中难以形成广域应用。

劫持控制技术通过信号模拟、指令重放或协议漏洞侵入无人机的数据链路或控制协议，绕过原控制终端实现飞行干预或完全接管[6]。该技术不造成物理损毁，且具有可取证性，对高价值或危险目标的处置更精确、灵活。然而，该技术需要深度破解目标的通信协议与软件结构，易受加密和抗干扰机制的限制，且其成功率高度依赖于无人机的型号、反制距离和电磁环境，有效作用距离通常小于500 m。近期研究表明，劫持控制技术正从简单的信号注入向基于协议逆向和智能控制的精确接管方向发展。例如，Donatti等[62]利用射频模拟系统完成了对非法无人机的链路接管实验，表明了劫持控制技术在无人机精细化管控中有一定应用潜力。

总体而言，在城市低空场景下，欺骗劫持技术灵活可控、附带损害低。其中，GNSS欺骗技术适合大范围空域内的远程驱离或降落引导，机载传感器欺骗技术主要用于狭窄空间或特定复杂态势下的精确干预，劫持控制技术则常用于近距离高价值或危险目标的应急接管与取证。

4.3 物理捕获

物理捕获技术是指通过机械手段或无人机编队对目标无人机进行实体拦截的硬杀伤中和技术。与干扰压制、欺骗劫持等软杀伤技术不同，该类技术对目标实施实体介入，但通常不会造成结构性破坏，在法律和公众接受度方面更具优势，适合在城市低空环境中使用。按照实施方式划分，物理捕获技术主要包括网捕技术与围捕技术两类。

网捕技术通过发射或展开网状装置对目标无人机实施机械约束，利用网体缠绕旋翼或限制机体运动使其丧失飞行能力[63]。该技术的典型实现方式包括手持或肩扛式网枪、车载网枪以及投掷式网袋等，有效作用距离通常在100 m以内，基本不破坏目标、易于保全证据，在民用场景中非常适用[72]。然而，受射程和拦截精度的限制，网捕技术对高速机动目标的处置能力相对有限，且被捕获目标在坠落过程中仍存在引发二次伤害的风险。对此，现有研究从多个方向入手：研究人员尝试改进目标跟踪与制导算法，提高命中率；结合降落伞或缓降装置降低目标坠落风险；采用地面发射与空中部署协同模式，扩大系统覆盖范围[64]。同时，也有研究尝试用机器学习方法优化发射时机与搜索策略，提升系统拦截复杂机动目标的能力[65]。

围捕技术利用拦截无人机或多无人机编队在空中跟踪、包围或捕获目标，实现对目标的非破坏性控制。该技术的典型实现方式包括拦截无人机携带捕捉网抵近释放、多机编队气流干扰以及拖绳限制等，以此迫使目标降落或离开受保护空域。目前，单机拦截的有效范围通常为300～800 m，多机编队或地空协同系统可将有效范围扩展至2 km[5]。与网捕技术相比，围捕技术具备机动性更强、覆盖范

围更广等核心优势，能够有效应对高速机动目标。然而，该技术对飞行控制精度与目标定位能力依赖性强，且存在能耗较大、成本较高以及拦截过程中可能发生空中碰撞等缺点。针对上述问题，现有研究一方面尝试将强化学习与协同控制算法相结合，来优化任务分配和路径规划，使编队能够在复杂空域中实现自适应协调追击[66]。同时，也有研究采用三维时空协同制导模型，实现多架无人机之间的同步交会与攻角约束，从而显著提高空中捕获的命中率和时效性[67]。

总体而言，在城市低空场景下，物理捕获技术被定位为非毁灭性且次生风险可控的硬杀伤中和技术。该技术能够以非破坏性的方式主动拦截非法或失控无人机，反制效果直接可靠，是反无人机系统中重要的末端处置手段。其中，网捕技术适用于重要设施周边的近距离拦截与执法取证，围捕技术适用于开阔空域高机动目标的主动追击与驱离，两者均能有效保障目标的完整性。

4.4　打击毁伤

打击毁伤技术是反无人机系统中最直接的硬杀伤中和技术，直接作用于无人机本体，通过使其结构损坏或功能失效来剥夺其飞行能力。该技术反制效果直接、处置速度快，一般用于高威胁目标或其他反制手段失效的极限场景，主要包括定向能毁伤与动能拦截两类[5]。

定向能毁伤技术主要利用高能激光或高功率微波等能量束聚焦目标，通过热效应烧蚀关键部件、破坏电子设备或干扰内部电路实现对无人机的物理毁伤。该技术响应速度快、打击精度高、单次拦截成本低，可以很好地应对无人机集群或高速机动目标。例如，Lockheed Martin等防务企业已开展多型高能激光反无人机系统的研发与测试，并验证了其对小型无人机和无人机集群目标的毁伤能力[68]。然而，定向能武器的作战效能易受雨雾、烟尘等环境因素影响，且对持续照射时间与跟踪精度要求较高。

动能拦截技术是通过发射防空弹药、拦截飞行器或借助生物体直接命中目标，利用碰撞产生的巨大动能实现物理摧毁。该技术反制效果明显且成熟度较高，目前已经在军事拦截与要地守卫领域广泛应用。例如，RTX公司研发的Coyote Block 2反无人机拦截器采用小型化飞行器，以精确撞击方式直接物理摧毁目标，且已在多项实战测试中验证了对小型无人机的拦截能力[69]。此外，生物动能拦截技术可以作为常规动能拦截技术的补充，如法国军方曾训练猛禽拦截小型无人机，并在机场等特定场景投入实际部署。然而，动能拦截技术的单次使用成本较高，其命中率易受目标高机动性能的影响，且其产生的高空坠落碎片在人员密集区域存在较大的安全隐患。

总体而言，在城市低空场景下，打击毁伤技术被定位为效果显著但适用性受限的极端硬杀伤中和技术。其实际应用必须满足严格的安全隔离要求，视具体技术不同，可能对周边电子设备与通信系统产生附带干扰，或面临坠落碎片、热辐射等潜在次生风险，因而难以作为常态化中和手段进行部署。

5　反无人机系统核心评估指标与实验环境设定

目前，学术界与工业界尚无适用于所有反无人机系统的统一评估指标体系，不同研究的指标命名与测试方法亦存在客观差异。然而，通过大量实验推演与工程实践，行业内已对一些核心评估指标达成基本共识。需要指出的是，“感知、识别、反制”三大阶段的核心指标各有侧重，其对应的实验设计、测试条件及环境设置亦表现出明显差异。各阶段的核心评估指标与实验环境设定如表4所示。

感知阶段的评估主要包括探测距离、探测精度、虚警率及环境适应性4项指标。探测距离反映了系统的感知覆盖范围，是评估各类探测技术感知

表4　各阶段的核心评估指标与实验环境设定

阶段	核心评估指标	实验环境设定	文献
感知	探测距离、探测精度、虚警率、环境适应性	不同光照、天气、风速、有无遮挡、不同噪声背景、有无电磁干扰	文献[73-76]
识别	轨迹预测误差、识别精度、标签识别成功率	有无视线遮挡、多目标干扰、复杂电磁环境、不同场景密度	文献[77-81]
反制	有效距离、反制成功率、系统响应时间	飞行速度、飞行高度、信号干扰强度、不同能见度条件	文献[82-86]

能力的基础指标[73-75]。探测精度用于评估系统对无人机目标状态参数估计的精确度，虚警率则可以表示在复杂背景下系统的误报概率，这两者已成为多模态感知算法中的核心判据[73,75]。环境适应性可以衡量气象波动和光照突变时系统的稳健性，研究人员常引入风速、能见度等控制变量来评估外界干扰对感知结果的影响[74-76]。在实验环境设定方面，雷达与射频探测技术依赖特定的电磁干扰场及多地形环境检验效果[86]，光学与红外探测技术需在不同光照条件下进行对比验证[76]，声学探测技术则多用不同密度的背景噪声验证探测算法的鲁棒性[74]。

识别阶段的评估指标主要聚焦于识别精度、轨迹预测误差及标签识别成功率。轨迹预测误差展示了系统在动态跟踪过程中对无人机运动状态的预测精度，常通过比对估计路径与真实航迹的偏差进行量化[78-79]。识别精度是此类研究中最常用的性能指标，直接体现系统区分无人机类别与具体型号的能力[6,77]。标签识别成功率则可以评估系统捕获无线识别信号的可靠性，常在基于RFID或ADS-B的身份合法性认证机制中使用[80-81]。实验环境设定方面，研究人员多测试识别算法在视线遮挡、多目标干扰以及复杂电磁环境下的稳定性，并验证系统在低空高密度场景下的普适性[6,78]。

反制阶段的评估指标主要关注有效距离、反制成功率及系统响应时间。有效距离界定了系统在不同场景下维持干扰或拦截效果的空间范围[80,82]。反制成功率显示了系统对目标无人机实施有效干预的成功概率[8,83]。系统响应时间则反映了系统从发现目标到实施反制的时效性，可以评估整体防御体系的协同效率[80,84]。在实验环境设定方面，研究人员常用无人机飞行速度、飞行高度、信号干扰强度及环境能见度等控制变量来评估不同中和技术在各种场景下的表现[78,85]。

总体而言，虽然目前没有适用于所有反无人机系统的统一评估指标体系，但感知、识别和反制这3个阶段的核心评估指标已在众多研究中反复验证。虽然不同研究的实验设计有差异，但都强调要严密控制变量和定量评估系统性能，确保测试结果可比。当前低空经济的发展和无人机的应用场景越来越多样，未来的指标体系还需纳入环境复杂性、系统能耗等新指标，既能深入评估某个具体场景，又能跨场景对比，支撑反无人机系统的工程部署与标准化测试。

6 学术界与工业界的差异

通过上述对探测、识别与中和技术的整体梳理，可以发现算法突破是学术界在反无人机领域的核心研究路径。这些算法成果虽能不断突破系统性能的理论上限，但其验证过程多依赖于标准化数据集、数字仿真平台或部分特定场景，而在复杂电磁环境、政策法规约束以及规模部署的限制下难以推行。因此，在低空经济的产业化落地中学术成果与工业实用仍有一定距离。

工业界更加关注真实场景下的实际需求，研发的侧重点与学术界不同。在国外市场中，Dedrone公司的DedroneTracker平台集成了射频监听、微型雷达、光学摄像机和声学阵列，可实现全天候、多场景下的无人机监测，并在美国匹兹堡国际机场、德国法兰克福机场以及英国内政部安保体系中投入实际使用。DroneShield公司的DroneSentry系统同样重点关注多源融合和城市环境部署能力，其射频探测模块、AI识别算法与云端指挥系统已在伦敦警察厅、欧洲能源基础设施及多项大型公共活动中使用。同时，国内市场工程化也开始加速，多家本土企业捕捉到了低空经济下城市治理与园区安全的诉求。例如，大疆AeroScope系统通过深度解析遥控链路信号，将生态体系内的无人机注册编号，并对其实时定位，现在已经在多地机场和重要活动区域广泛应用；海康威视等企业推出的反无人机解决方案面向园区、车站、赛事场馆等商业化场景，通过工程化集成雷达、射频及光学技术，实现了与现有安防平台、城市智能网联系统的兼容部署。综观国内外市场，商用反无人机系统存在共同特征，即系统必须通过电磁兼容、安全合规等多项行业法规认证，且需在城市多径效应、密集通信干扰与复杂气象条件下进行长期外场运行测试。更关键的是，与学术界的单点算法演进不同，工业界产品整合了硬件防护、边缘计算、通信调度、人机交互界面及空域管理互操作等全链条工程要素，强调全生命周期成本、维护便利性与法规合规性。

总体而言，学术界与工业界的差异主要源自研发导向与考量约束的不同。学术界侧重在可控环境下提升算法性能，而工业界则必须在真实低空经济场景中确保系统的可靠部署、稳定运行与合法运

营。两条技术路径并非方向相左，而是受制于截然不同的场景需求与工程成熟度。因此，未来的关键路径在于建立贯通实验研究与工程实践的验证链路与标准体系，加速学术成果在真实低空经济场景下的转化与应用。

7　反无人机技术的未来趋势

在低空经济快速发展的背景下，反无人机系统正从单点式防护向“感知网络化、识别智能化、反制协同化”转变。其中，5G/6G 通感网络赋能、AI 原生反无人机体系和多节点协同网络将是后续研究的关键所在。

首先，5G/6G 通感网络赋能是未来反无人机系统的技术驱动。5G 网络高带宽、低时延，可以密集部署，这使基站可兼具通信和感知功能[5]。基于同步信号块与定位参考信号的有源/无源探测方法[87-88]以及结合压缩感知的回波分析模型[89]，都表明 5G 网络可以在不额外增加硬件的同时实现三维定位与弱信号检测。5G 网络物理层信号的高采样率特性也被用于射频指纹识别和威胁判断[90-91]，结合多接入边缘计算的 5G 控制链路则能有效支撑低时延协同反制[92-93]。此外，向前演进的 6G 通信技术将利用太赫兹频段、智能超表面与通感一体化技术提升无人机探测的距离分辨率、角分辨率及弱特征识别能力[94-95]。依托 6G 的原生 AI 架构，未来网络将可以实现对无人机行为的实时理解与异常预测，同时能自适应生成反制策略，构建自动化、泛在化的低空监测体系[96]。

其次，AI 原生反无人机体系是未来反无人机系统的核心架构。当前，AI 在此类系统中的角色已不再只是感知链路的附加增强，还逐渐成为支撑全系统运行的底层逻辑。这一底层逻辑通过集成弱信号深度表征学习、跨模态数据融合、序列轨迹与意图预测，以及自适应威胁等级评估等核心技术，共同构建起“从感知到反制”的智能流水线[97]。尤其在密集城市场景下，AI 动态调度各节点的任务负载，实现高效识别与分层处置，不仅降低了误报率和漏报率，还进一步提升了系统的时效性[75]。

最后，多节点协同网络是未来反无人机系统的部署形态。随着地面站、6G 基站、车载平台与低空拦截无人机等多维节点的融合，反无人机系统正由单点设备升级为“可重构、可扩展、可自治”的任务网络[98]。各节点可依据时空态势动态构建“探测—识别—中和”的链式或网状结构，通过边缘协同与分布式决策实现区域级乃至城市级的实时防护[99]。该网络能够有效应对多目标、强干扰及集群飞行等复杂情况，可显著提升系统整体的鲁棒性与响应速度。

总体而言，未来反无人机技术将呈现感知网络化、识别智能化、反制协同化的发展趋势。5G/6G 技术为系统提供基础的通感一体化能力，AI 原生架构深化系统的理解与判断水平，而多节点协同网络则保障系统空间维度的可靠覆盖与实时响应。未来研究将聚焦于复杂环境下的系统鲁棒性、资源受限条件下的分布式学习机制，以及跨平台协同的标准化建设，为低空经济时代构建可持续、可扩展的空域安全体系。

8　结束语

本文系统梳理了近年来反无人机探测技术、识别技术以及中和技术等方面的进展，全面阐明了现有技术体系的发展历程。

然而，面对低空经济的新型应用需求，现有研究仍存在以下局限：一是缺乏面向低空经济典型真实场景的实验数据支撑，模型与算法验证多局限于可控理想环境；二是应用研究体系尚不完善，尚未建立跨领域协同机制与标准化测试体系。

未来技术的发展方向将集中在感知网络化、识别智能化和反制协同化 3 个维度。特别指出的是，低空经济的规模化发展导致社会对合法性与安全性的要求不断提高，低损伤、可控制的新型中和技术将是未来的研究重点。

最后，为更好融入低空经济的整体布局，反无人机技术应与低空网络基础设施、低空空域管理体系协同发展。未来需要建设统一的低空安全监管与反无人机响应体系，推动科研机构、骨干企业与监管部门的标准对接和数据共享，实现低空经济与国家安全良性共生。

参考文献：

[1] Liu S, Liu M M. Research on the security risk governance roadmap in low-altitude economic field based on the economic externality theory[J]. Engineering Proceedings, 2025, 80(1): 14.

[2] 中华人民共和国中央人民政府网 .《中共中央关于制定国民经济和社会发展第十五个五年规划的建议》[EB]. (2025-10-28)[2026-07-01].

The Central People's Government of the People's Republic of China. Recommendations of the central committee of the Communist party of China for formulating the 15th five-year plan for national economic and social development[EB]. (2025-10-28)[2026-07-01].

[3] Jin Y Y. The evolution and challenges of low-altitude economy: Insights from experience in China[C]//Proceedings of the 1st International Conference on Modern Logistics and Supply Chain Management (MLSCM 2024). Setúbal: SciTe Press, 2024: 32-36.

[4] Zmyslowski D, Skokowski P, Kelner J. Anti-drone sensors, effectors, and systems-a concise overview[J]. TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation, 2023, 17(2): 455-461.

[5] Gonzalez-Jorge H, Aldao E, Fontenla-Carrera G, et al. Counter drone technology: a review[PP]. V1. (2024-02-09) [2026-07-01]. arXiv: arXiv.202402.0551.

[6] Park S, Kim H T, Lee S, et al. Survey on anti-drone systems: components, designs, and challenges[J]. IEEE Access, 2021, 9: 42635-42659.

[7] Chauhan D, Kagathara H, Mewada H, et al. Nation's defense: a comprehensive review of anti-drone systems and strategies[J]. IEEE Access, 2025, 13: 53476-53505.

[8] Kanu N J, Gupta E, Pendkar S M, et al. A few suggestions to improve anti-drone measures for combating against the drone menace[J]. Journal of the Institution of Engineers (India): Series C, 2024, 105(3): 761-787.

[9] 胡杨林, 张天魁, 李博, 等. 无人机使能的通信感知一体化组网与技术研究综述[J]. 电子与信息学报, 2025, 47(4): 859-875.
Hu Y L, Zhang T K, Li B, et al. A survey on UAV-enabled integrated sensing and communication networking and technologies[J]. Journal of Electronics & Information Technology, 2025, 47(4): 859-875.

[10] 何道敬, 杜晓, 乔银荣, 等. 无人机信息安全研究综述[J]. 计算机学报, 2019, 42(5): 1076-1094.
He D J, Du X, Qiao Y R, et al. A survey on cyber security of unmanned aerial vehicles[J]. Chinese Journal of Computers, 2019, 42(5): 1076-1094.

[11] 中华人民共和国国务院, 中华人民共和国中央军事委员会. 无人驾驶航空器飞行管理暂行条例[EB]. (2023-05-31)[2026-07-01].
State Council of the People's Republic of China, Central Military Commission of the People's Republic of China. Interim regulation on the administration of the flight of unmanned aircraft[EB]. (2023-05-31) [2026-07-01].

[12] 中华人民共和国交通运输部. 民用无人驾驶航空器运行安全管理规则[EB]. (2023-12-15)[2026-07-01].
Ministry of Transport of the People's Republic of China. Rules on the safety management of civil unmanned aircraft[EB]. (2023-12-15) [2026-07-01].

[13] Federal Aviation Administration. Remote identification of unmanned aircraft[EB]. (2021-01-15)[2026-07-01].

[14] Babu J, Adidev K S, Halarnkar V N, et al. Micro-Doppler signature analysis for UAV detection: a review on advanced techniques and challenges[PP]. V2. (2025-07-22)[2026-07-01]. arXiv: arXiv.5246346.

[15] Nucum K, Biswas S, Ball J E. Micro-Doppler models of drones, birds, and bird-like drones[C]//Radar Sensor Technology XXIX. Bellingham: SPIE, 2025: 107-123.

[16] Rizzi Varela V G, Brown M C, Li C Z. Drone movement detection using V-band FMCW MIMO radar with digital beamforming[C]//Proceedings of the 2023 16th International Conference on Advanced Technologies, Systems and Services in Telecommunications (TELSIKS). Piscataway: IEEE Press, 2023: 122-125.

[17] Yan J, Hu H P, Gong J K, et al. Exploring radar micro-Doppler signatures for recognition of drone types[J]. Drones, 2023, 7(4): 280.

[18] Tang Z B, Ma H, Qu Y M, et al. UAV detection with passive radar: algorithms, applications, and challenges[J]. Drones, 2025, 9(1): 76.

[19] Sun Y F, Yu C, Luo Y, et al. An experimental study of passive UAV tracking with digital arrays and cellular downlink signals[J]. IEEE Open Journal of the Communications Society, 2025, 6: 3779-3794.

[20] Raja Abdullah R S A, Alhaji Musa S, Abdul Rashid N E, et al. Passive forward-scattering radar using digital video broadcasting satellite signal for drone detection[J]. Remote Sensing, 2020, 12(18): 3075.

[21] Dan Y P, Yi J X, Wan X R, et al. LTE-based passive radar for drone detection and its experimental results[J]. The Journal of Engineering, 2019, 2019(20): 6910-6913.

[22] Kabiri M, Cimarelli C, Bavle H, et al. A review of radio frequency based localisation for aerial and ground robots with 5G future perspectives[J]. Sensors, 2022, 23(1): 188.

[23] Yousaf J, Zia H M, Alhalabi M, et al. Drone and controller detection and localization: trends and challenges[J]. Applied Sciences, 2022, 12 (24): 12612.

[24] Hindle P. Drone detection and location systems[J]. Microwave Journal, 2017, 60(2): 3.

[25] Elyousseph H, Altamimi M. Robustness of deep-learning-based RF UAV detectors[J]. Sensors, 2024, 24(22): 7339.

[26] Bisio I, Garibotto C, Haleem H, et al. RF/WiFi-based UAV surveillance systems: a systematic literature review[J]. Internet of Things, 2024, 26: 101201.

[27] Han S M, Jang B J. Drone's angle-of-arrival estimation using a switched-beam antenna and single-channel receiver[J]. Sensors, 2025, 25(8): 2376.

[28] Wang Y H, Zeng Y H, Sun S M, et al. Drone controller localization based on RSSI ratio[J]. Sensors, 2023, 23(11): 5163.

[29] Liu Z Y, An P, Yang Y, et al. Vision-based drone detection in complex environments: a survey[J]. Drones, 2024, 8(11): 643.

[30] Al Dawasari H J, Bilal M, Moinuddin M, et al. DeepVision: enhanced drone detection and recognition in visible imagery through deep learning networks[J]. Sensors, 2023, 23(21): 8711.

[31] Wang Y H, Feng X F, Li F, et al. Lightweight visual localization algorithm for UAVs[J]. Scientific Reports, 2025, 15(1): 6069.

[32] Yang S Q, Cheng Q, Tang C S, et al. Applications and advancements of infrared thermal imaging technology in geotechnical engineering: a review[J]. Journal of Rock Mechanics and Geotechnical Engineering, 2026, 18(3): 2437-2451.

[33] Park K W, Kim S H, Kim C Y, et al. Analysis and evaluation of the target detection range of infrared electro-optical tracking systems[J]. Current Optics and Photonics, 2025, 9(1): 19-28.

[34] Wang H X, Wang H L, Han F. Detection of low-altitude infrared small targets for UAVs using a density-based artificial bee colony algorithm[J]. Scientific Reports, 2025, 15: 23344.

[35] Mohtadifar M, Cheffena M, Pourafzal A. Acoustic-and radio-

frequency-based human activity recognition[J]. Sensors, 2022, 22(9): 3125.

[36] Frid A, Ben-Shimol Y, Manor E, et al. Drones detection using a fusion of RF and acoustic features and deep neural networks[J]. Sensors, 2024, 24(8): 2427.

[37] Griffiths D, Jahangir M, White D, et al. Urban clutter analysis for drone detection using L-band staring radar[C]//Proceedings of the 2023 IEEE International Radar Conference (RADAR). Piscataway: IEEE Press, 2023: 1-6.

[38] Chen Y Z, Sun H Y, Tian L, et al. Detecting infrared UAVs on edge devices through lightweight instance segmentation[J]. PLoS One, 2025, 20(8): e0330074.

[39] 周建, 周易, 倪歆玥, 等. 偏振集成红外光电探测器研究进展与应用[J]. 光电工程, 2023(5): 230010.
Zhou J, Zhou Y, Ni X Y, et al. Research progress and applications of polarization integrated infrared photodetector[J]. Opto-Electronic Engineering, 2023(5): 230010.

[40] 乔庆元, 程换新. 基于改进YOLOv8的红外无人机目标检测算法[J]. 激光与红外, 2024, 54(12): 1941-1947.
Qiao Q Y, Cheng H X. Infrared UAV target detection algorithm based on improved YOLOv8[J]. Laser & Infrared, 2024, 54(12): 1941-1947.

[41] Pereira A, Warwick S, Moutinho A, et al. Infrared and visible camera integration for detection and tracking of small UAVs: systematic evaluation[J]. Drones, 2024, 8(11): 650.

[42] 丁斋生, 周冬明, 聂仁灿, 等. 基于视觉显著性与残差网络的红外-可见光图像融合方法[J]. 云南大学学报(自然科学版), 2019, 41(6): 1108-1117.
Ding Z S, Zhou D M, Nie R C, et al. Infrared and visible image fusion using residual network and visual saliency detection[J]. Journal of Yunnan University (Natural Sciences Edition), 2019, 41(6): 1108-1117.

[43] 董莺艳. 基于深度学习的声纹识别方法研究[D]. 重庆: 重庆理工大学, 2019.
Dong Y Y. Research on voiceprint recognition method based on deep learning[D]. Chongqing: Chongqing University of Technology, 2019.

[44] Vakil A, Liu J, Zulch P, et al. A survey of multimodal sensor fusion for passive RF and EO information integration[J]. IEEE Aerospace and Electronic Systems Magazine, 2021, 36(7): 44-61.

[45] Ma Y T, Su D F, Li Y T, et al. Spatial perception of tagged cargo using fused RFID and CV data in intelligent storage[J]. IEEE Internet of Things Journal, 2022, 10(2): 1574-1587.

[46] Semenov S, Krupska-Klimczak M, Mazurek P, et al. Improving unmanned aerial vehicle security as a factor in sustainable development of smart city infrastructure: automatic dependent surveillance – broadcast (ADS-B) data protection[J]. Sustainability, 2025, 17(4): 1553.

[47] Duffield M O. Automatic dependent surveillance-broadcast for detect and avoid on small unmanned aircraft[D]. Provo: Brigham Young University, 2016.

[48] Nair M, Cappello T A, Dang S P, et al. Rigorous analysis of data orthogonalization for self-organizing maps in machine learning cyber intrusion detection for LoRa sensors[J]. IEEE Transactions on Microwave Theory and Techniques, 2022, 71(1): 389-408.

[49] Tian Y, Wen H, Zhou J X, et al. Optimized radio frequency footprint identification based on UAV telemetry radios[J]. Sensors, 2024, 24 (16): 5099.

[50] Shu P, Chen C B, Chen B H, et al. Trajectory prediction of UAV based on LSTM[C]//Proceedings of the 2021 2nd International Conference on Big Data & Artificial Intelligence & Software Engineering (ICBASE). Piscataway: IEEE Press, 2021: 448-451.

[51] Jia P Y, Chen H P, Zhang L, et al. Attention-LSTM based prediction model for aircraft 4-D trajectory[J]. Scientific Reports, 2022, 12(1): 15533.

[52] Aksoy M, Ozdemir O, Guner G, et al. Flight trajectory pattern generalization and abnormal flight detection with generative adversarial network[C]//AIAA Scitech 2021 Forum. Reston: AIAA, 2021: 0775.

[53] 许彤, 陈亚洲, 王玉明, 等. 无人机数据链带内连续波电磁干扰效应研究[J]. 北京理工大学学报, 2021, 41(10): 1084-1094.
Xu T, Chen Y Z, Wang Y M, et al. Research on in-band continuous wave electromagnetic interference effect of unmanned aerial vehicle data link[J]. Transactions of Beijing Institute of Technology, 2021, 41 (10): 1084-1094.

[54] Cheng L B, Xu Z X, Zhou J S, et al. Adaptive spectrum anti-jamming in UAV-enabled air-to-ground networks: a bimatrix Stackelberg game approach[J]. Electronics, 2023,12(20): 4344.

[55] Jiang P F, Geng X S, Pan G W, et al. GNSS anti-interference technologies for unmanned systems: a brief review[J]. Drones, 2025, 9(5): 349.

[56] Radoš K, Brkić M, Begušić D. Recent advances on jamming and spoofing detection in GNSS[J]. Sensors, 2024, 24(13): 4210.

[57] 王晓燕, 杨晶晶, 黄铭, 等. GNSS干扰和欺骗检测研究现状与展望[J]. 信号处理, 2023, 39(12): 2131-2152.
Wang X Y, Yang J J, Huang M, et al. Research status and prospect of GNSS jamming and spoofing detection[J]. Journal of Signal Processing, 2023, 39(12): 2131-2152.

[58] Liu Y, Xu K, Xia X C, et al. Joint power control and passive beamforming optimization in RIS-assisted anti-jamming communication[J]. Frontiers of Information Technology & Electronic Engineering, 2023, 24(12): 1791-1802.

[59] 张鑫. 卫星导航欺骗干扰信号检测技术综述[J]. 全球定位系统, 2018, 43(6): 1-7.
Zhang X. Overview of satellite navigation spoofing signal detection technology[J]. GNSS World of China, 2018, 43(6): 1-7.

[60] Fotiadis F, Sadler B M, Topcu U. Coordinated UAV beamforming and control for directional jamming and nulling[PP]. V2. (2025-09-16) [2026-07-01]. arXiv: arXiv.2508.17433.

[61] Yang H W, Liu Y, Li X R, et al. Physical layer security and covert communication in UAV-ISAC networks: a comprehensive survey[J]. Journal of King Saud University Computer and Information Sciences, 2025, 37(10): 312.

[62] Donatti M, Frazatto F, Manera L, et al. Radio frequency spoofing system to take over law-breaking drones[C]//Proceedings of the 2016 IEEE MTT-S Latin America Microwave Conference (LAMC). Piscataway: IEEE Press, 2016: 1-3.

[63] Sherman M, Shao S H, Sun X, et al. Counter UAV swarms: challenges, considerations, and future directions in UAV warfare[J]. IEEE Wireless Communications, 2025, 32(1): 190-196.

[64] Yin Y, Chen S, Wang J L. Architecture and challenges for low-altitude security system[C]//Proceedings of the 2020 Chinese Control and Deci-

sion Conference (CCDC). Piscataway: IEEE Press, 2020: 1991-1996.

[65] Zhang W Y, Luo S, Wang J, et al. Development and prospect of intelligent air-to-ground precision strike munition[C]//International Symposium on Advanced Launch Technologies (ISALT 2022). Bristol: IOP Publishing, 2023: 012169.

[66] Xia B Z, Mantegh I, Xie W F. UAV multi-dynamic target interception: a hybrid intelligent method using deep reinforcement learning and fuzzy logic[J]. Drones, 2024, 8(6): 226.

[67] Tao H, Lin D F, Song T, et al. Optimal spatial-temporal cooperative guidance against a maneuvering target[J]. Journal of the Franklin Institute, 2023, 360(13): 9886-9903.

[68] Kang H G, Joung J, Kim J, et al. Protect your sky: a survey of counter unmanned aerial vehicle systems[J]. IEEE Access, 2020, 8: 168671-168710.

[69] Congressional Research Service. Department of defense counter unmanned aircraft systems: background and issues for congress[EB]. (2025-03-31)[2026-07-01].

[70] 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 C K, Hou Q. Spoofing and anti-spoofing technology of UAV in GNSS[J]. GNSS World of China, 2020, 45(3): 37-40.

[71] Davidson D, Wu H, Jellinek R, et al. Controlling UAVs with sensor input spoofing attacks[C]//10th USENIX workshop on offensive technologies (WOOT 16). Berkeley: USENIX Association, 2016: 221-231.

[72] Chiper F L, Martian A, Vladeanu C, et al. Drone detection and defense systems: survey and a software-defined radio-based solution[J]. Sensors, 2022, 22(4): 1453.

[73] Ezuma M, Erden F, Anjinappa C K, et al. Detection and classification of UAVs using RF fingerprints in the presence of interference[PP]. V1. (2019-09-12)[2026-07-01]. arXiv: arXiv: 1909.05429.

[74] Tejera-Berengue D, Zhu-Zhou F F, Utrilla-Manso M, et al. Analysis of distance and environmental impact on UAV acoustic detection[J]. Electronics, 2024, 13(3): 643.

[75] Seidaliyeva U, Ilipbayeva L, Taissariyeva K, et al. Advances and challenges in drone detection and classification techniques: a state-of-the-art review[J]. Sensors, 2023, 24(1): 125.

[76] He T L, Hou J Y, Chen D. Multimodal UAV target detection method based on acousto-optical hybridization[J]. Drones, 2025, 9(9): 627.

[77] Dong Y F, Wu F Y, Zhang S J, et al. Securing the skies: a comprehensive survey on anti-uav methods, benchmarking, and future directions[C]// Proceedings of the 2025 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW). Piscataway: IEEE Press, 2025: 6661-6675.

[78] Brewczyński K D, Życzkowski M, Cichulski K, et al. Methods for assessing the effectiveness of modern counter unmanned aircraft systems[J]. Remote Sensing, 2024, 16(19): 3714.

[79] Chen S F, Chen B H, Shu P, et al. Real-time unmanned aerial vehicle flight path prediction using a bi-directional long short-term memory network with error compensation[J]. Journal of Computational Design and Engineering, 2023, 10(1): 16-35.

[80] De Cubber G, Doroftei D, Petsioti P, et al. Standardized evaluation of counter-drone systems: methods, technologies, and performance metrics[J]. Drones, 2025, 9(5): 354.

[81] Chen S C, Zheng S L, Yang L F, et al. Deep learning for large-scale real-world ACARS and ADS-B radio signal classification[J]. IEEE Access, 2019, 7: 89256-89264.

[82] Wu J M, Huang S J, Wang X Q, et al. Study on the performance of laser device for attacking miniature UAVs[J]. Optics, 2024, 5(4): 378-391.

[83] Rozenbeek D J. Evaluation of drone neutralization methods using radio jamming and spoofing techniques[D]. Stockholm: KTH Royal Institute of Technology, 2020.

[84] Pliska M, Vrba M, Báča T, et al. Towards safe mid-air drone interception: strategies for tracking & capture[J]. IEEE Robotics and Automation Letters, 2024, 9(10): 8810-8817.

[85] Zhang Z, Zhou Y, Zhang Y, et al. Strong electromagnetic interference and protection in UAVs[J]. Electronics, 2024, 13(2): 393.

[86] de Macedo S O, Caetano M, da Costa R M. Drone detection in airport environments: a literature review[J]. Array, 2025, 28: 100511.

[87] Jopanya P, Osorio D P M. Utilizing 5G NR SSB blocks for passive detection and localization of low-altitude drones[C]//Proceedings of the 2025 IEEE 26th International Workshop on Signal Processing and Artificial Intelligence for Wireless Communications (SPAWC). Piscataway: IEEE Press, 2025: 1-5.

[88] Blandino S, Golmie N, Sahoo A, et al. Detecting airborne objects with 5G NR radars[C]//Proceedings of the MILCOM 2025 - 2025 IEEE Military Communications Conference (MILCOM). Piscataway: IEEE Press, 2025: 1260-1265.

[89] Özbay E, Bishoyi P K, Petrova M. Empowering 5G PRS-based ISAC with compressed sensing[C]//Proceedings of the 2024 IEEE 25th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC). Piscataway: IEEE Press, 2024: 341-345.

[90] Gao N, Zeng T R, Chen B W, et al. Multi-domain supervised contrastive learning for UAV radio-frequency open-set recognition[J]. IEEE Journal on Selected Areas in Communications, 2026, 44: 4083-4098.

[91] Viana J, Farkhari H, Sebastião P, et al. Deep attention recognition for attack identification in 5G UAV scenarios: novel architecture and end-to-end evaluation[J]. IEEE Transactions on Vehicular Technology, 2024, 73(1): 131-146.

[92] Solanki S, Mahmood A, Singh V, et al. MEC-assisted low latency communication for autonomous flight control of 5G-connected UAV[C]// Proceedings of the 2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring). Piscataway: IEEE Press, 2023: 1-5.

[93] Viana J, Farkhari H, Gil Jiménez V P. Securing 5G and beyond-enabled UAV links: resilience through multiagent learning and transformers detection[J]. IEEE Access, 2025, 13: 153993-154007.

[94] Joy A T, Tishchenko A, Taghvaee H, et al. RIS-enabled ISAC in 6G: exploring the role of wave domain computing[J]. IEEE Communications Standards Magazine, 2026, 10(1): 137-144.

[95] Wang Z W, Wang J J, Wu G Y, et al. Joint design of transmit beamforming and receive filters for MIMO ISAC systems under low-altitude dynamic scenarios[J]. IEEE Journal of Selected Topics in Signal Processing, 2026: 3681471.

[96] Yan H, Chen Y F. Terahertz integrated sensing communications and powering for 6G wireless networks[PP]. V1. (2025-01-22) [2026-07-01]. arXiv: arXiv.2501.13006.

[97] Othman W M, Ateya A A, Nasr M E, et al. Key enabling technologies for 6G: the role of UAVs, terahertz communication, and intelligent reconfigurable surfaces in shaping the future of wireless networks[J]. Journal of Sensor and Actuator Networks, 2025, 14(2): 30.

[98] Castrillo V U, Manco A, Pascarella D, et al. A review of counter-UAS technologies for cooperative defensive teams of drones[J]. Drones, 2022, 6(3): 65.

[99] Baktayan A A, Zahary A T, Sikora A, et al. Computational offloading into UAV swarm networks: a systematic literature review[J]. EURASIP Journal on Wireless Communications and Networking, 2024, 2024(1): 69.

[作者简介]



王景璟（1990– ），男，博士，北京航空航天大学教授，主要研究方向为无线通信与安全、低空智能网。



王智伟（2003– ），男，北京航空航天大学硕士生，主要研究方向为通感一体化技术、信号处理。



高畅（2003– ），女，北京航空航天大学硕士生，主要研究方向为低空安全、网络安全和机器学习。



陈健瑞（1997– ），男，北京航空航天大学博士生，主要研究方向为无人机通信网络。



杜皓华（1991– ），女，博士，北京航空航天大学助理教授，主要研究方向为人工智能安全、物联网系统安全。



姜春晓（1987– ），男，博士，清华大学副教授，主要研究方向为博弈论、优化理论及统计方法在通信网络与资源分配领域的应用。