http://bhxb.buaa.edu.cn jbuaa@buaa.edu.cn
DOI: 10.13700/j.bh.1001-5965.2025.0600

ADS-B 异常检测研究综述

杨宏宇[1,2,*]，赵子文[1]，朱友文[3]，胡慧玲[4]，胡俊成[5]

(1. 中国民航大学 安全科学与工程学院，天津 300300；2. 中国民航大学 计算机与人工智能学院，天津 300300；
3. 南京航空航天大学 计算机科学与技术学院，南京 211106；4. 中国民用航空中南地区空中交通管理局 空管部，广州 510440；
5. 吉林大学 计算机科学与技术学院，长春 130012)

摘 要：广播式自动相关监视 (ADS-B) 系统作为航空监视技术的重要组成部分，已得到广泛部署应用，显著提高了空中交通监视的覆盖范围和定位精度，但开放的广播通信机制使该系统易受数据篡改、恶意报文注入和干扰攻击等多种安全威胁，严重影响空中交通安全与管制决策，针对ADS-B系统的异常检测成为研究热点。基于此，系统总结并分析了当前国内外ADS-B系统异常检测的研究现状。对导致ADS-B系统出现异常数据的原因进行分析，总结该系统易遭受的攻击类型及其影响；从基于一致性检验的方法和基于深度学习的方法深入探讨ADS-B异常检测研究现状，分析各类方法在检测精度、泛化性与实际部署中的优缺点，并结合相应的应用场景对当前ADS-B异常检测产品进行分析总结；在总结已有研究成果的基础上，深入讨论当前面向ADS-B的异常检测方法所面临的主要挑战，并提出未来的研究方向与发展趋势。

关 键 词：广播式自动相关监视；异常检测；空中交通监视；一致性检验；深度学习
中图分类号：TP393
文献标志码：A **文章编号**：1001-5965(2026)11-3677-22

随着美国新一代航空运输系统项目及欧洲单一天空空中交通管理研究项目的启动[1]，航空电子基础设施开始更新，这些项目旨在设计高性能、低成本和更安全的航空电子系统。在过去的十几年中，航空电子系统已逐步实现了空中运行管理与监视的自动化，并与地面站、雷达等形成相互依存的结构，但随着系统日益复杂，系统自身产生了新的安全漏洞。因此，加强航空电子系统的安全性、可靠性和可持续性逐渐成为研究热点。

广播式自动相关监视 (automatic dependent surveillance broadcast, ADS-B) 系统作为新一代空中交通监视技术的重要组成部分，可由机载设备实时广播航空器的位置信息、速度和航向等数据，显著提升空中交通管理 (air traffic management, ATM) 的态势感知能力与运行安全性。2020年，美国联邦航空管理局表示，攻击者可以窃听ADS-B系统以对该系统进行中间人攻击[2]，利用ADS-B的安全漏洞，攻击者可以注入“幽灵飞机”信号或篡改实际航空器的定位信息，给空中交通管制 (air traffic control, ATC) 带来潜在风险。

为应对日益严重的ADS-B安全威胁，国内外研究者提出多种异常检测方法，主要分为基于一致性检验的ADS-B异常检测方法和基于深度学习的ADS-B异常检测方法。早期的一致性检验方法包括基于位置或信号时间到达差的检测[3]，该类方法通过将ADS-B报文广播的位置信息与雷达或多点定位系统所测量的独立位置信息进行交叉验证，并使用基于飞行动力学的模型分析轨迹的合理性，从

收稿日期：2025-08-26；**录用日期**：2025-11-07；**网络出版时间**：2025-11-20 12:16
网络出版地址：link.cnki.net/urlid/11.2625.V.20251119.1820.004
基金项目：国家自然科学基金民航联合基金重点项目 (U2433205)
*通信作者. E-mail：yhyxlx@hotmail.com

引用格式：杨宏宇，赵子文，朱友文，等. ADS-B 异常检测研究综述 [J]. 北京航空航天大学学报，2026，52（11）：3677-3698.
Yang H Y，Zhao Z W，Zhu Y W，et al. Review of ADS-B anomaly detection research [J]. Journal of Beijing University of Aeronautics and Astronautics，2026，52（11）：3677-3698（in Chinese）.

而判断报文数据的真实性和一致性。该类方法依赖额外的传感器信息和人为设定的阈值,难以全面覆盖复杂场景。2020年以后,基于密码学的一致性检验方法为ADS-B提供了更严格的完整性保证,通过在ADS-B通信中引入对称加密、数字签名、消息认证码和区块链等手段[4],对广播报文进行验证和防篡改保护。该类方法可确保只有授权方才能解读并验证报文来源,防止数据被伪造或中途篡改,从而确保ADS-B报文的完整性与来源的真实性。然而,该类方法在实际部署过程中仍存在密钥分发机制复杂、通信资源开销较大等问题,制约了其在广域航空监视场景中的大规模应用。

与此同时,基于深度学习的ADS-B异常检测方法[2]也逐渐得到了广泛应用,该类方法能够从海量正常飞行数据中自动学习正常航迹模式,当出现偏离正常模式的ADS-B报文时予以检测。但是,目前基于深度学习的异常检测方法高度依赖特征选择算法的设计及训练数据的质量,在应对未知环境和新型威胁时泛化能力不足。

综合上述问题,本文聚焦面向ADS-B的异常检测方法,通过梳理ADS-B异常检测方法的研究进展,深入分析各类方法在检测不同空域、机型、飞行模式和各类攻击方式时存在的优势与不足。同时,本文系统总结了ADS-B遭受的各类攻击方式,并深入分析了不同攻击方式造成的影响。在总结目前研究成果的基础上,针对实际应用中面临的挑战和技术瓶颈,提出包括对抗性抵御、大语言模型部署在内的具体研究方向,以期为推进异常检测技术在ADS-B系统中的进一步研究与实际应用提供参考依据。

在深入探讨具体的异常检测方法之前,有必要对本文的核心概念进行界定。“异常”是一个广义术语,指任何偏离预期正常模式的数据点或序列,其成因既包括设备故障、信号衰减等非恶意因素,也涵盖了由恶意实体发起的“攻击”。攻击是异常的一个关键子集,特指旨在破坏系统完整性、可用性或真实性的蓄意行为。本文的定位是ADS-B异常检测研究综述,该技术是保障航空安全的重要防线,其目标是识别所有异常模式,并重点关注对各类恶意攻击行为的检测能力与挑战。

1 ADS-B系统概述

ADS-B系统作为新一代空中交通监视技术[5],航空器通过无线电周期性广播自身的位置、速度、航向、识别号等信息,由地面站和其他航空器接收用于空管监视与碰撞预防。作为“下一代”空管系统的核心组成,ADS-B系统相较传统雷达具有诸多优势,包括态势感知能力提升、监视覆盖范围扩大、目标定位精度提高及运行成本降低等[5]。然而,ADS-B系统在设计上缺乏必要的安全机制,其广播报文为明文且无加密认证,这意味着任何人都可以在该系统所用频段发送格式规范的ADS-B信号而被接收端接收。本节将详细阐述ADS-B运行过程和ADS-B异常数据产生机理。

1.1 ADS-B运行过程

ADS-B系统的核心模块由ADS-B接收端和ADS-B输出端2个关键部分组成。ADS-B输出端设备安装在航空器或地面站,通过全球导航卫星系统(global navigation satellite system, GNSS)接收机获取航空器的实时位置信息、速度、航向等飞行数据,飞行管理系统(flight management system, FMS)处理这些数据后,由机载Mode S应答机将其转换为广播报文,并通过指定的数据链路定期广播出去,这些信息被地面站和其他运行航班ADS-B接收端设备所接收并进行解码,将提取到的飞行状态信息在地面站及飞行员的驾驶舱显示交通信息(cockpit display of traffic information, CDTI)界面进行展示,实现实时监控和空中交通管理,确保航班之间的安全距离并进行必要的避让,从而有效提升空中交通运行的安全性和空域资源利用的效率。ADS-B系统架构如图1所示。

1.2 ADS-B异常数据产生机理

ADS-B系统在实际运行过程中接收到的广播报文,除常规飞行数据外,往往还包含一定比例的异常数据。这些异常数据的产生,部分源于硬件精度、气象环境等非恶意因素[6-7],但更严峻的挑战来自其开放通信协议所固有的安全漏洞[8]。为了系统性地分析这些由恶意攻击导致的异常来源,本文引入业界权威的微软STRIDE威胁模型[9],该模型从欺骗、数据篡改、信息泄露、拒绝服务、权限提升和抵赖6个维度对安全威胁进行分类。ADS-B系统的异常数据产生机理可映射至该框架进行深入分析。

1.2.1 拒绝服务

拒绝服务攻击旨在破坏ADS-B通信的可用性,主要表现为信号干扰。攻击者可通过大功率噪声发射装置阻塞1 090 MHz信道,淹没合法信号,导致特定空域内的航空器信号“消失”或间歇性丢失,造成航班位置信息无法更新、轨迹不连续等异常[10-11]。这直接破坏了空管的态势感知能力。

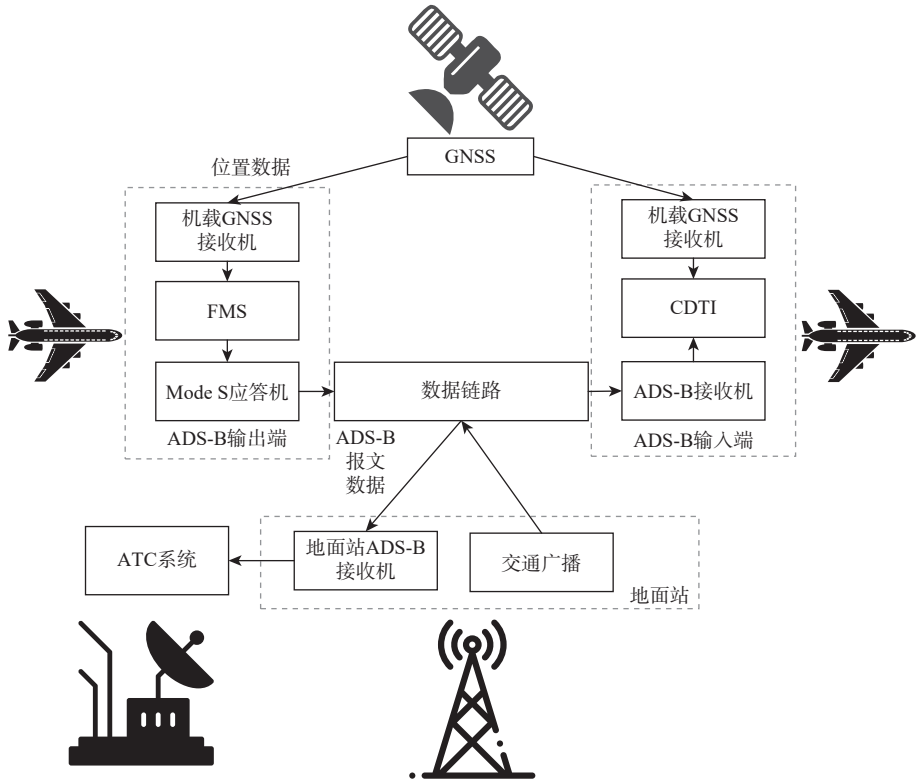

图 1　ADS-B 系统架构

Fig. 1　Architecture of ADS-B system

1.2.2　数据篡改

数据篡改攻击指合法 ADS-B 报文在传输过程中被恶意修改, 导致接收方获取不准确的状态信息。研究表明, 攻击者可通过信号叠加技术翻转报文中的比特位, 将真实信息篡改为虚假数据[12-13]。此类异常的特征是航班目标持续存在, 但其报告的轨迹、高度等信息与实际严重不符, 可能干扰空管决策, 引发安全隐患。

1.2.3　欺骗与信息泄露

由于 ADS-B 自身的特点, 使得所有相关数据流都会导致信息泄露。由于无法改变其本身的核心属性, 针对信息泄露, 只能通过后期对各类攻击进行精准检测与防御, 来维护该系统的正常运转。欺骗攻击是指非法航空器发出的虚假 ADS-B 广播信息出现在监视系统中, 通常由攻击者恶意生成。这类异常的数据源并非真实航空器, 而是攻击者利用无线发射设备伪造的“幽灵飞机”航班信号[14-16]。欺骗攻击的典型表现是监视显示出现额外的未知航迹: 空管雷达或接收站检测到一些并不存在于空域中的航空器目标。这些“幽灵飞机”航迹可能包含看似合理的识别号、位置和高度等数据, 但实际上没有对应的真实航空器。此类异常会对空管员和飞行员造成极大困扰, 需分辨哪些目标是真实的, 哪些是伪造的。如果攻击者生成的虚假目标与真实航空器航路接近, 甚至可能迫使空管采取不必要的分流措施, 影响正常航班调度。

1.2.4　权限提升与抵赖

在 ADS-B 场景下, 权限提升表现为攻击者通过广播虚假紧急代码, 使其伪造信息获得不成比例的关注和系统优先响应, 间接影响空管决策流程。而抵赖指的是 ADS-B 协议无法提供报文来源的不可否认性, 使得攻击者在实施了上述所有攻击后难以被追溯, 构成了系统性的安全短板。同时, 抵赖通常表现为攻击者伪装真实航班发送假位置或速度信息, 干扰 ATC 监控后删除或隐藏发送记录。由于 ADS-B 报文为明文广播且无签名机制, 任何软件无线电设备 (software defined radio, SDR) 都可发送报文, 系统无法追溯真实发射者。

综上, 基于 STRIDE 威胁模型, ADS-B 的异常数据来源可被系统性地归纳为: 由拒绝服务攻击导致的信号干扰与数据缺失; 由数据篡改攻击造成的报文内容失真; 由欺骗攻击引入的虚假“幽灵飞机”目标或身份冒用; 以及作为多种攻击前提的信息泄露。这一系统性的分类框架, 为后续深入分析 ADS-B 攻击技术和构建有效的防护方法奠定了坚实的理论基础。STRIDE 威胁模型在 ADS-B 领域的映射如表 1 所示。

表1 STRIDE威胁模型在ADS-B领域的映射

Table 1 Mapping of STRIDE threat model in ADS-B domain

元素	交互	在ADS-B系统中的具体表现形式和攻击示例	S (欺骗)	T (数据篡改)	R (抵赖)	I (信息泄露)	D (拒绝服务)	E (权限提升)
航空器	广播ADS-B报文给地面站或邻机	“幽灵飞机”注入,伪造航班或位置广播导致错误感知	★		★			
航空器	从进程接收ADS-B报文	伪装为地面服务下发错误情报;接收方日志被篡改后无法追溯	★	★				
进程	地面站监视系统获取航空器报文并处理	中间处理被篡改影响告警;处理日志被删除;接收缓存泄露	★	★		★	★	★
进程	地面站监视系统向航空器广播报文	下发被篡改的交通/天气信息	★	★			★	★
进程	ATC系统与数据库接口	中间报文或响应被篡改;审计记录被擦除		★	★			
进程	写入或读取飞行日志与数据库	写入端被回写假轨迹;数据库敏感字段被泄露		★	★	★		
数据流	航空器向地面站广播	广播被仿冒或重放;广播可被任何接收机窃听		★		★	★	
数据流	地面站向航空器回传	地面注入错误情报		★		★	★	
数据流	空对空广播	空对空“幽灵飞机”广播;广播被重放或延迟		★		★	★	

注:★表示对应交互中可能遭受的攻击类型。

2 ADS-B攻击技术

随着ADS-B系统大面积部署在各国民航系统中,其设计时所蕴含的问题逐渐暴露出来,通信链路未采用任何加密或认证手段,接收端对报文来源身份不做校验。这一架构上的弱点使得ADS-B易受到多种网络攻击的威胁,如被动窃听、虚假数据、干扰等。事实上,攻击者只需成本较低的软件无线电设备,便可在1 090 MHz信道上拦截或伪造ADS-B报文[17]。这些安全漏洞引发了对航空安全的严重担忧:攻击者可能利用ADS-B系统的弱点获取敏感航班信息、注入虚假目标、干扰正常通信,直接影响空管决策和飞行安全。因此,深入研究ADS-B的攻击模式与分类方法,对制定有效的防御策略至关重要。本节将详细阐述当前ADS-B系统所遭受的主要攻击方式,并对其进行分类总结。面向ADS-B主要攻击方式如图2所示。

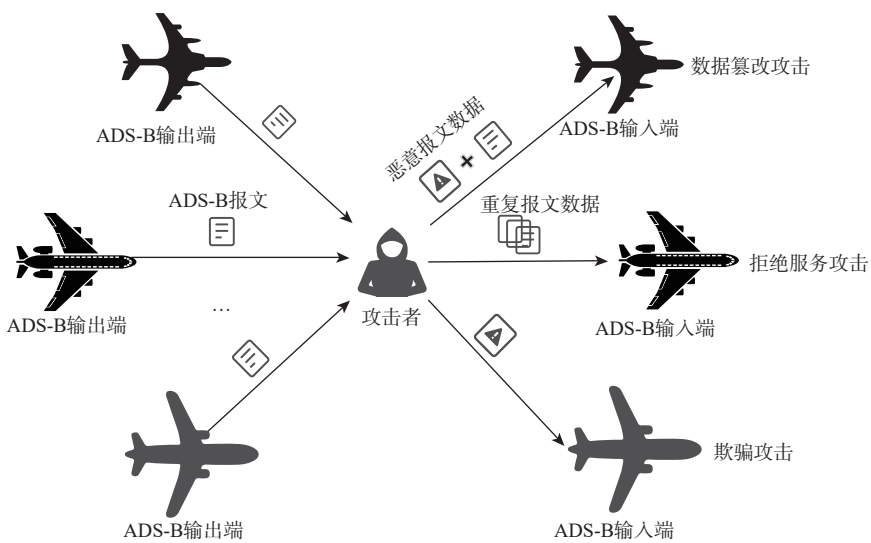

图2 ADS-B主要攻击方式

Fig. 2 Primary attack modes against ADS-B

2.1 被动窃听攻击

被动窃听是最基础的ADS-B攻击方式,属于被动信息获取。攻击者使用ADS-B接收机或软件无线电设备,调谐至1 090 MHz或其常用ADS-B频段,便可接收附近广播的ADS-B报文[18]。由于所有信息均为非加密,攻击者可以毫不费力地截获并解析这些广播内容。通过获取的ADS-B飞行数据,攻击者可以实现对航空器隐私侵犯、航迹跟踪,甚至对特定航班实施后续攻击。虽然该攻击方式对航空器运行造成的影响较小,但被动窃听攻击往往是其他主动攻击的前奏,攻击者在掌握目标航空器的飞机识别号、飞行高度、飞行速度等重要数据

后, 利用这些信息执行欺骗或干扰攻击。因此, 被动窃听攻击虽然不会直接干扰 ADS-B 运行, 但为后续其他高危攻击打开了大门[19]。由于 ADS-B 设计时便拥有的开放性质, 目前对被动窃听攻击本身缺乏有效的防御手段, 只有通过隐私保护机制在一定程度上缓解数据暴露。

2.2　虚假数据攻击

虚假数据攻击是目前 ADS-B 最具威胁的主动攻击方式, 主要包括欺骗攻击、注入攻击、数据篡改攻击。尽管 3 种攻击方式都涉及伪造或修改 ADS-B 数据, 干扰航空监视系统和空管决策, 但三者在攻击目标、技术实现及影响范围等方面存在显著区别。

2.2.1　欺骗攻击

欺骗攻击主要针对个别航班, 通过伪造已有航班的数据, 可能会导致空管人员误判航班位置, 从而影响航空安全。

GNSS 欺骗攻击向机载 GNSS 设备发送伪造全球定位系统 (global positioning system, GPS) 信号, 使航空器得到错误的位置数据并通过 ADS-B 广播, 影响空管的决策, 导致航班延误或误入管制空域[20-21]; 速度欺骗攻击针对获取后的 ADS-B 报文中速度字段的格式进行伪造, 生成新的速度数据, 来制造虚假的速度漂移趋势, 误导地面空管或机载防撞系统对航空器航迹的预测, 产生错误的判断[22-24]; ADS-B 身份欺骗攻击指的是攻击者通过伪造已有合法航空器的身份标识, 如 ICAO 地址, 并以此身份向 ADS-B 地面站或其他航空器广播虚假的位置、速度、高度等数据, 实现对 ADS-B 系统的误导或干扰[25-27], 此类攻击不仅会导致航空器身份混乱, 增加空中事故的发生, 还可能被用于掩盖其他非法行为, 如军用侦察机伪装民航客机对他国空域进行侵犯[28]; 重放攻击指的是攻击者截获合法 ADS-B 报文后, 在不同位置或时间重新广播这些报文, 使得空管人员或其他航空器误以为此类报文为实时数据, 由于 ADS-B 缺乏身份认证和时间同步机制, ADS-B 接收端无法区分原始报文与重放报文, 因此, 此类攻击极具隐蔽性[29-30]。

2.2.2　注入攻击

注入攻击主要用于系统攻击, 通过伪造大量新目标或错误警报来干扰空管系统的正常运行, 容易导致空管系统过载。

地面站目标注入攻击是攻击者专门针对地面站发送大量虚假的 ADS-B 地面目标报文, 造成大量虚假目标填满机场地面监视系统, 使空管人员对机场跑道或其他区域的使用情况出现误判, 影响航班起降安排[24]; “幽灵飞机”注入攻击[14-16] 是攻击者利用软件无线电设备, 向空管站点发送格式合法但虚假的 ADS-B 报文, 生成大量未运行航空器, 即“幽灵飞机”, 这些“幽灵飞机”可能具有虚假的 ICAO 代码、随机轨迹、非运行航班识别号等, 使得空管人员难以分辨真假, 最后需要花费大量时间排查“幽灵飞机”, 对航班管理造成重大影响; 错误警报注入攻击[31] 指的是攻击者广播伪造的 ADS-B 紧急代码, 如 7500(劫机代码)、7600(失联代码) 等, 导致空管系统对运行航空器产生误判, 最终导致航班被迫备降或空中紧急事件; 轨迹伪造攻击是攻击者通过主动注入伪造的 ADS-B 航迹数据或修改部分真实航迹数据[32-34], 使地面监视系统显示的轨迹与实际飞行轨迹严重不符, 造成空管决策失误或空中交通预警系统误报。

2.2.3　数据篡改攻击

数据篡改攻击较前 2 种攻击方式的不同点在于其攻击方式是对原始合法 ADS-B 报文进行获取并修改后进行重播, 所广播的内容中不包含未出现的航班信息, 只针对已有航班数据中的特定信息字段进行修改。

ADS-B 报文篡改是攻击者在截取合法 ADS-B 报文后, 通过对报文中特定数据(如位置、高度、速度等信息)进行实时修改或延迟广播当前航班的报文, 造成飞行员或空管人员对航空器实时状况的误判, 导致空中冲突警报、错误避让等情况发生[35-36]; 在此基础上, 攻击者对攻击方式进行改进, 通过物理层信号叠加实现数据比特位的反转, 精确篡改消息中某些特定字段, 使 ADS-B 接收端误以为消息未被篡改而接收虚假数据, 虽然此类攻击单次影响较小, 但累积后可能会造成空管决策混乱甚至发生事故[12-13]; 时序篡改攻击是攻击者在截获合法的 ADS-B 报文后篡改报文时间戳, 使 ADS-B 接收端设备在当前时刻接收到过去随机时刻报文[19]; 机载设备篡改攻击指的是攻击者未经授权或内部人员恶意接入 ADS-B 接收机和 GNSS 接收机, 直接修改设备数据, 广播虚假 ADS-B 报文, 此类攻击方式难以通过外部检测发现其虚假性[37]; 信号特征篡改攻击是攻击者利用 ADS-B 输出端所采用的射频指纹识别技术漏洞, 通过模拟合法航空器 ADS-B 输出端的射频特征, 篡改或伪造原始指纹, 使基于指纹识别的安全防护失效, 此类攻击不仅会导致 ADS-B 身份认证失效, 更会导致攻击者长期冒充合法航空器进行虚假数据广播, 严重扰乱空域监视和管理的可靠性[38-41]。

2.3　干扰攻击

干扰攻击指的是攻击者利用特定设备向 ADS-B 系统的通信信道发送大功率的干扰信号, 以阻断

ADS-B与地面站或其他航空器之间的正常通信。此类攻击通常利用连续高功率波形或特定频率的信号来实现干扰，从而使目标的ADS-B信号接收部分或完全失效。

无线电干扰攻击指的是攻击者在ADS-B标准通信频段，利用高功率射频干扰器增大攻击范围内ADS-B接收端的噪声水平，使得合法ADS-B报文被干扰或淹没，无法得到解析，造成监视服务短期甚至长期瘫痪的风险[27]；GNSS干扰攻击是攻击者针对GPS频段，通过高功率干扰信号，使航空器GNSS接收端无法正常接收正确位置信号，导致航空器无法获取精确定位，进而造成飞行员误入禁飞区或增加相邻航空器碰撞风险[42]；二次雷达(secondary surveillance radar, SSR)应答干扰攻击指的是攻击者发送大量格式相似或相同的ADS-B报文，使接收端无法分辨真实航空器信息与干扰信息，从而降低信息处理效率[43]；此外，ADS-B中最为常见的干扰攻击方式为分布式拒绝服务(distributed denial of service, DDoS)攻击，通过对其ADS-B所运行的频段持续发射强功率无线信号，如ADS-B报文前导码或随机噪声信号，使ADS-B输出端的完整正常报文严重干扰或完全被淹没，从而造成ADS-B通信服务的中断[4]。此外，攻击者采用数据泛洪攻击，利用ADS-B开放的通信特性，大量生成和发送虚假的ADS-B报文，使地面站或航空器接收端在短时间内处理大量的信息，导致设备处理能力过载甚至瘫痪，或者通过发送与ADS-B报文信号频率相同但相位相反的信号以完全抵消合法信号，阻止任何ADS-B报文的传输和解析，导致管制屏幕上目标完全丢失，形成区域性通信盲区，如在繁忙航线区域则可能引发严重飞行事故[44]。ADS-B攻击方式分类如表2所示。

表2 ADS-B攻击方式分类

Table 2 ADS-B attack modes classification

攻击方式	攻击层次	所属攻击类型	攻击手段	技术难度	影响范围	检测难度	攻击数据组成	典型危害	参考文献
无线电干扰	物理层	干扰攻击	频谱干扰	中等	区域性	中等	无报文数据	区域通信瘫痪	[27]
GNSS干扰	物理层	干扰攻击	GNSS频段干扰	中等	广泛	中等	无报文数据	导航失效	[42]
信号特征篡改	物理层	数据篡改攻击	无线电信号伪造	高	单一目标	高	虚假报文与真实报文	指纹识别失效	[38-41]
比特位反转篡改	物理层	数据篡改攻击	信号叠加造成数据位反转	高	单一目标	高	虚假报文与真实报文	误导性数据传播	[12-13]
机载设备篡改	物理层	数据篡改攻击	内部设备篡改	高	单一目标	高	虚假报文与真实报文	破坏设备	[37]
被动窃听	数据链路层	被动窃听攻击	ADS-B信号截获	低	单一目标	高	真实报文	信息泄露	[18-19]
ADS-B身份欺骗	数据链路层	欺骗攻击	伪造ICAO代码	中等	单一目标	中等	虚假报文与真实报文	身份识别混乱	[25-28]
SSR应答干扰	数据链路层	干扰攻击	大量类似报文干扰	中等	广泛	高	虚假报文与真实报文	真实目标识别困难	[43]
GNSS欺骗	数据链路层	欺骗攻击	伪造GNSS信号	高	单一目标	高	虚假报文与真实报文	位置错误	[20-21]
错误警报注入	数据链路层	注入攻击	伪造ADS-B广播	低	广泛	中等	虚假报文	管制决策混乱	[31]
“幽灵飞机”注入	数据链路层	注入攻击	大量虚假航迹注入	低	广泛	中等	虚假报文	空管超载	[14-16]
时序篡改	数据链路层	数据篡改攻击	延迟合法报文传播	中等	单一目标	高	真实报文	时序错误导致决策混乱	[19]
ADS-B报文篡改	数据链路层	数据篡改攻击	截获并篡改真实报文	高	单一目标	高	虚假报文与真实报文	数据误导	[35-36]
轨迹伪造	数据链路层	注入攻击	轨迹生成算法	高	单一目标	高	虚假报文与真实报文	位置误判	[32-34]
速度欺骗	数据链路层	欺骗攻击	伪造速度数据	中等	单一目标	中等	虚假报文与真实报文	错误避让决策	[22-24]
重放	数据链路层	欺骗攻击	报文重播	中等	单一目标	中等	虚假报文与真实报文	数据时间混乱	[29-31]
数据泛洪	网络层	干扰攻击	报文泛洪	较低	广泛	高	虚假报文	系统瘫痪	[44]
分布式拒绝服务	网络层	干扰攻击	多点伪造信息	中等	广泛	高	虚假报文	全面服务中断	[4]
地面站目标注入	网络层	注入攻击	伪造信息格式	低	区域性	中等	虚假报文	虚假目标干扰	[24]

2.4 异常检测问题形式化定义与评估指标

为了系统性地评述后续的异常检测方法，本节先对该问题进行形式化定义，并介绍通用的性能评估指标。

ADS-B数据本质上是多变量时空间序列。一条飞机的航迹可被表示为一个时间序列$T=\{\boldsymbol{x}_1,\boldsymbol{x}_2,\cdots,\boldsymbol{x}_n\}$。其中，$\boldsymbol{x}_n$为在时间戳$n$观测到的状态向量，该向量通常包含多个维度的信息，可以归纳为运动学状态(经度、纬度、高度、速度)、身份标识(ICAO地址、呼号)，即$\boldsymbol{x}_n=(J_n,W_n,G_n,V_n,\cdots,I)$，$J$为经度，$W$为纬度，$G$为高度，$V$为速度，$I$为身份标识。

基于此，ADS-B异常检测任务可以被形式化地描述为：构建一个判别模型$f(\cdot)$，该模型对时刻t下输入的单个数据点y_t(逐点检测)或一个包含上下文信息的航迹片段S_{sub}(序列检测)进行评估。模型的输出通常是一个连续的异常分数$s=f(y_t \text{ or } S_{\text{sub}})$，该

分数衡量了输入数据偏离正常模式的程度。最终，通过将该分数与一个预设或动态调整的阈值θ进行比较作出判断: 当$s>0$时，该数据点或航迹段被标记为异常。阈值θ的选择至关重要，其通常在验证集上根据可接受的误报率凭经验设定。

根据训练数据的不同，该任务可分为监督学习、半监督学习和无监督学习。由于真实攻击数据的稀缺性，无监督学习在 ADS-B 异常检测中尤为常见。

为定量评估检测模型$f(\cdot)$的性能，通常基于混淆矩阵计算一系列指标，混淆矩阵中的元素包括真正例 T_{P}、假正例 F_{P}、真反例 T_{N} 和假反例 F_{N}。常用评估指标包括精确率 P、召回率 R、F_1 分数及误报率 (false alarm rate, FAR)。评估指标的计算公式如下:

$$P=\frac{T_{\mathrm{P}}}{T_{\mathrm{P}}+F_{\mathrm{P}}} \tag{1}$$

$$R=\frac{T_{\mathrm{P}}}{T_{\mathrm{P}}+F_{\mathrm{N}}} \tag{2}$$

$$F_1=2\frac{PR}{P+R} \tag{3}$$

$$E=\frac{F_{\mathrm{P}}}{F_{\mathrm{P}}+T_{\mathrm{N}}} \tag{4}$$

式中: E为误报率。

2.5　ADS-B 数据特性与检测数据集构建

理解 ADS-B 数据的基本特性与评测数据集的构建方式，是评估和设计异常检测方法的前提。ADS-B 数据作为一种典型的多变量时空间序列，其关键特点给检测带来了挑战与机遇: 数据以秒级或亚秒级高频采样，形成了高密度序列; 其内容融合了时间戳、三维空间坐标与速度等多维属性，呈现出强烈的时空耦合性; 同时，飞机轨迹遵循物理规律，为模型提供了强运动学约束作为先验知识; 数据的统计特性会随飞行阶段变化而呈现非平稳性，对算法的泛化能力提出了更高要求。鉴于已标记的真实攻击数据在学术研究中极为稀缺，研究者通常采用模拟攻击注入的方式，在真实的正常数据集基础上构建评测基准。这些数据构造方法与本节讨论的攻击类型紧密呼应。具体而言，对于轨迹伪造攻击，当前的研究已经从简单的静态位置偏移，演变为动态和智能化的攻击模拟。例如, Panda 等[22]利用强化学习来训练一个攻击智能体，该智能体通过不断试探与学习，能够自主发现目标防御系统 (如空中交通冲突解脱算法) 的决策边界和弱点，从而生成一系列经过精心设计、以诱发安全冲突为最终目的的欺骗性飞行动作作为序列。这种方法生成的攻击数据不再是孤立的随机异常点，而是在整个时序上具有连贯性和高度对抗性的恶意轨迹，更能考验检测系统的极限性能。在“幽灵飞机”注入攻击方面，近期的研究焦点也从模拟单个虚假目标转向了大规模、协同化的攻击场景。例如, Melvyn 等[30]针对低空监控环境，深入研究了“幽灵飞机”泛洪攻击的数据生成与检测，攻击者并非注入一个孤立的假目标，而是同时生成大量看似合理但并不存在的飞行轨迹，旨在通过信息过载的方式，耗尽自动化系统的处理资源或造成人类操作员 (如管制员) 的认知饱和与决策困难。这种模拟生成协同飞行的虚假编队，比注入单个、无关联的“幽灵飞机”，对整个监视系统的韧性提出了严峻得多的挑战。此外，其他关键的数据构造方法也愈发精细。重放攻击的模拟通过截获一段真实的历史航迹数据，将其时间戳篡改为当前时刻后重新注入数据流，其目的在于制造一个位置完全错误但轨迹动态极为逼真的“时空错位”目标，这对缺乏消息新鲜性验证的系统是巨大威胁。而 ADS-B 身份欺骗攻击的模拟则通过全局替换航迹中的 ICAO 地址来实现，这不仅会造成空中态势图上的身份混淆，还可能被用于掩盖非法飞行活动或对特定合法航空器进行嫁祸式干扰。

3　ADS-B 异常检测方法

ADS-B 系统在设计之初未考虑系统级的安全防护机制，其开放式广播通信结构导致该系统在实际运行中面临严重的安全风险。上述攻击手段普遍技术门槛低、实施成本小，并具有较强的隐蔽性和破坏性，能够在短时间内对空管系统的稳定性与航班运行的安全性造成严重威胁。此外，不同攻击方式在影响范围、检测难度及所造成的危害呈现出显著差异，亟须系统地构建有效的安全防护体系。针对 ADS-B 系统脆弱的安全特性，异常检测作为重要的防御手段，在保障飞行信息完整性与系统运行可靠性方面发挥着关键作用。在深入探讨各类异常检测方法之前，理解 ADS-B 数据的基本特性与评测数据集的构建方式是研究的基础。ADS-B 数据是一种典型的多维时空序列，其关键特点包括: 由秒级广播形成的高频采样; 融合空间、时间与速度等多维属性的多维时空性; 遵循物理规律的强运动学约束; 随飞行阶段变化的非平稳性，这对模型的泛化构成了挑战。鉴于真实攻击数据的稀缺性，学术研究普遍采用模拟攻击注入的方式构建评测数据集，即在真实的正常数据基础上，通过恶意修改实现轨迹伪造、生成虚构航迹注入“幽灵飞机”、重播历史数据模拟重放攻击或篡改 ICAO 地址进行 ADS-B 身份欺骗。

3.1 基于一致性检验的ADS-B异常检测方法

基于一致性检验的ADS-B异常检测方法通过引入独立的观测数据源或其他可信信息，采用物理测量或数学计算方式，将ADS-B广播的报文与这些独立数据源进行交叉验证，以确定广播报文的真实性与一致性。当ADS-B广播报文与独立测量数据之间的差异超出预定阈值时，即可快速有效地识别出系统中存在的报文异常或遭受的恶意攻击，从而判断报文的完整性和真实性。

自2017年开始，基于独立定位技术的异常检测方法被用于ADS-B的异常检测，该类方法通过对ADS-B广播报文中的航空器位置信息与地面站独立测量的实际位置进行比对，检验ADS-B发送报文的真实性[43]。然而，此类方法对地面传感器布局的条件要求较高，且易受到同步误差及环境噪声的影响，导致单一数据源的定位精度下降，难以有效识别日益复杂的攻击方式。因此，国内外学者开始提出基于多源数据融合的方法，即综合ADS-B报文、一次雷达、SSR等多种独立监视数据源，通过交叉验证的方式提高异常检测的鲁棒性和精度[45]。同时，为了有效防范更为复杂的ADS-B报文篡改攻击，在之前2种方法的基础上提出了密码学的方法，通过添加数字签名或时间戳来验证当前ADS-B报文的真实性[4]。

本节将系统综述基于独立定位技术、多源数据融合、密码学方向在ADS-B异常检测中的应用，分析各类异常检测方法在检测精度、泛化能力方面的优势与不足。

3.1.1 基于独立定位的异常检测方法

基于独立定位的异常检测方法的检测过程为：首先，由多个地面站或接收机接收来自目标航空器的ADS-B广播报文；其次，利用接收到的报文，通过物理测量技术独立计算出航空器的实际位置，并与ADS-B广播的位置数据进行实时或准实时的对比分析；然后，计算这2种位置数据之间的偏差或误差，并与事先确定的阈值进行比较；最后，如果偏差超出正常容许范围，则将ADS-B报文判定为异常数据并触发警报。

针对ADS-B依赖航空器主动报告位置，容易受到攻击者发送虚假ADS-B报文的攻击，Naganawa等[43]提出了使用广域多点定位(wide area multilateration, WAM)系统的扇区天线阵列接收ADS-B信号，通过幅度单脉冲技术测量信号的入射角度和解码ADS-B信号获取到的航空器位置信息计算得到的期望到达角度做差，并将差值与预先设定好的阈值进行比对，判定该信号是否异常，但该方法的准确性严重依赖扇区天线的方向校准精度，使得检测效果受环境影响较大。在此基础上，Leonardi[19]提出了利用信号到达时间差(time difference of arrival, TDOA)结合K近邻(K-nearest neighbor, KNN)算法的方法，在离线状态下建立覆盖监视区域的二维网格，并计算网格中各点到多地面站的预期TDOA，将结果保存到数据库中，实时接收航空器的ADS-B广播报文以计算实际TDOA数据，并利用KNN算法在数据库中匹配与实时数据最近的k个点来估计航空器的实时位置进行比对，该方法不需要复杂的接收设备，也无需对传感器精度有较高的要求，但在复杂环境下会导致数据库数据频繁更新及在线实时处理时延增大。针对此问题，Leonardi等[14]将两步拓展卡尔曼滤波(two-step extended Kalman filter, TEKF)引入对ADS-B异常检测的方向中，将当前ADS-B报文与根据历史飞行状态预测得到的数据进行对比，执行第一次卡尔曼滤波更新，实现初步异常检测，利用众包传感器网络测量的TDOA数据进行二次卡尔曼滤波更新以检测精细轨迹欺骗攻击。同时，Zhao等[46]通过融合TDOA、AOA测量信息，并采用交互多模型(interacting multiple model, IMM)算法实现对ADS-B航路多点定位的监视方法，提高了ADS-B报文的检测精度。

为解决多源空中交通监视环境中无人机参与协作时难以识别ADS-B虚假报文的问题，Chai等[47]提出一种将到达时间总和(time sum of arrival, TSOA)与TDOA、AOA数据协同定位的异常检测方法，其架构如图3所示。首先，采用Chan算法对目标位置进行初步估计；然后，通过改进Taylor算法进行迭代修正，提升定位精度并消除传统方法中“二解”歧义问题；最后，将ADS-B广播位置与联合

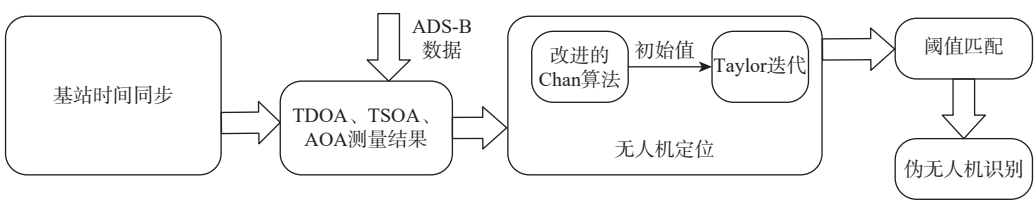

图3 数据协同定位方法架构[47]

Fig. 3 Architecture of data collaborative positioning method[47]

定位结果进行对比, 确定该报文真实性。近年来, 随着攻击手段不断增强, 攻击者开始针对地面站时间同步误差不敏感作为突破口, 使得之前的方法检测精度大幅下降。针对上述问题, 刘海涛等[21] 提出了一种到达时间间隔差 (interval difference of arrival, IDOA) 的方法, 与上述方法相比, IDOA 方法不需部署传感器或复杂的天线阵列, 仅需地面站接收到的相邻 2 条 ADS-B 报文位置消息的时间间隔差与理论位置计算得到的时间间隔差构造检验统计量, 以此判断 ADS-B 报文的真实性。

近年来, 基于独立定位的 ADS-B 异常检测方法的研究总体主要体现为“工程可解释、场景制约显著”。一方面, 依托外部空间测量与时间观测构建的独立位置估计, 为广播位置提供了可复核的物理证据, 因不依赖深度模型训练而具备较低的数据门槛、较强的可解释性与可迁移性, 且在身份伪装、轨迹伪造与报文篡改等高风险场景中显示出稳定的核验效能; 但另一方面, 现有成果普遍受制于传感器几何布设、站间时间同步与设备标定等工程条件, 易受地形遮挡、多径干扰与电磁环境波动影响, 导致在广域稀疏网络中定位精度下降, 阈值敏感性增加。综上, 研究前沿正由“单一独立核验”走向“多源协同与自适应阈值”的体系化方向, 同时亟须标准化评测数据、可复现实验流程与面向大规模运行环境的工程化验证。基于独立定位的异常检测方法总结如表 3 所示。

表 3　基于独立定位的异常检测方法总结

Table 3　Summary of anomaly detection methods based on independent positioning

检测方法	数据集	针对攻击/异常类型	应用场景	优点	缺点
AOA[43]	Beechcraft B300飞机航行实验数据集	欺骗攻击	扇区天线部署区域	在WAM系统空域背景下, 抗欺骗水平高	严重依赖扇区天线方向校准, 偏差过大时抗欺骗效果降低
KNN+TDOA[19]	OpenSky+自建仿真数据集	欺骗攻击	传感器分布稀疏区域	无需部署高精度接收设备, 非理想几何条件下定位精度高	网格划分较细的情况下, 计算复杂度变高, 实时处理时延增加
TEKF+TDOA[14]	OpenSky	GNSS干扰攻击	多个TDOA传感器部署区域	无需求解非线性多点问题, 检测范围更广	受网络布局影响较大, 容易导致TDOA精度下降
IMM+TDOA[46]	CCA1516航班数据集+自建仿真数据集	GNSS欺骗攻击、轨迹伪造攻击	GNSS信号易受攻击区域	在复杂航路下定位精度较高	受实时性影响较大, 大范围部署难度较大, 泛化性较差
TSOA+TDOA+AOA[47]	自建仿真数据集	欺骗攻击、轨迹伪造攻击	无人机参与的协作监视区域	定位精度高, 适用于复杂场景	对硬件要求较高, 更适用于军事或管制场景, 泛化性较差
IDOA[21]	自建仿真数据集	轨迹伪造攻击	时钟同步不理想区域	不再依赖地面站时间同步, 计算复杂度更低	对ADS-B报文中水平和垂直位置数据要求较高, 仍需多个地面站协调工作

3.1.2　基于多源数据融合的异常检测方法

基于多源数据融合的异常检测过程为: 首先, 系统同步地收集多个独立监视系统所观测到的同一目标航空器的数据信息, 包括 ADS-B 广播报文、雷达测量数据、SSR 数据及多边测量数据; 其次, 将来自不同数据源的飞行数据进行统一的时间轴匹配与对齐; 然后, 依据具体的融合策略对各数据源提供的位置、速度、高度等关键飞行参数进行一致性或相似性分析, 确定不同来源数据之间的残差; 再者, 针对这些残差建立通用或动态阈值, 并进行实时比对; 最后, 当来自不同数据源的同一飞行参数之间的差异持续超出阈值范围时, 判定 ADS-B 数据存在异常。

为解决传统多点定位方法要求 4 个及其以上地面接收机才能验证报文这一局限性, Darabseh 等[45] 提出了一种基于最少地面传感器 (minimal numbers of on-ground sensors, MNOS) 的 ADS-B 验证协议, 该方法在仅有 1～3 个地面接收机的情况下根据历史航线数据、飞机标识号、航班号分别构建概率矩阵, 并将最近可信 ADS-B 报文设为锚点, 与当前待检测 ADS-B 报文中的数据分别进行核验, 得到对应的比对结果并给出相应的分数, 将所有核验分数按预先固定好的权重进行加权计算, 判断该报文可信度, 但该方法对历史数据依赖较大, 同时对实时处理能力要求较高。针对此问题, 王布宏等[48] 提出了基于粒子群优化 (particle swarm optimization, PSO) 多核支持向量数据描述 (multi-kernel support vector data description, MKSVDD) 的 ADS-B 异常检测方法, 通过获取 ADS-B 报文数据与 SSR 数据并将其做差作为特征, 训练超球体分类器, 利用多核核函数提高分类精度, 采用 PSO 算法对惩罚因子、核参数进行自动优化, 提高检查性能, 实验结果表明, 遇到新航线时, 也可通过已有模型进行判断, 提高了对突发状况的检测精度。当前, ADS-B 报文常采用 1 090 MHz 扩展消息格式, 虽然其具有 24 bit 循环冗余校验机制, 但在数据传输或解析过程中仍存在错误, 导致接收到与正常轨迹偏离过远的位置, 影响可靠性。为解决此问题, Lukeš等[49] 提出了一种基于密度的

噪声应用空间聚类 (density based spatial clustering of applications with noise, DBSCAN) 异常检测方法，使用 ICAO 代码对待检测航班进行分组，将经纬度及飞行高度转换为地心固定 (Earth centered Earth fixed, ECEF) 坐标系，通过计算每个数据点的邻近点个数与预先规定好的阈值进行比对，判定是否为离群点，该方法适用于大规模数据处理，同时可以快速处理大偏差异常点。针对 ADS-B 身份欺骗攻击，Li 等[50]提出了一种基于轨迹数据 (track data, TD) 的异常检测方法，利用地面接收机解析 ADS-B 报文并提取其频率漂移特征，记录所接收到的 ADS-B 报文的中心频率与 1 090 MHz 频率的偏差，形成频率漂移曲线，同时通过多站点 ADS-B 数据比对，计算同一报文在不同接收站的信号相位差和幅度变化，结合 ADS-B 历史轨迹数据，与当前轨迹进行相似度匹配，输出轨迹评分，综合上述 3 种检测结果得出该航班是否存在异常数据或遭受恶意攻击。此类方法通过多种独立观测源的冗余信息来提升检测可靠性和鲁棒性，但对数据质量和同步性有一定的要求。

近年来，基于多源数据融合的 ADS-B 异常检测研究呈现出由“单一信号核验”向“跨模态协同感知”的体系化演进，同时涵盖数据层、特征层与决策层 3 类融合范式。总体上，多源融合显著提升了对身份伪装、轨迹篡改与环境诱发异常的可辨识性，并在复杂空域与极端工况下增强了鲁棒性，降低了误报或漏报。然而，现有工作仍受限于异构源的时间同步与空间匹配误差、传感器覆盖不均与缺失数据、跨域分布漂移及高维关联带来的计算开销。综上，当前研究方向亟须标准化数据集、统一评测协议与面向运行级别验证的工程实践。基于多源数据融合的异常检测方法总结如表 4 所示。

表 4　基于多源数据融合的异常检测方法总结

Table 4　Summary of anomaly detection methods based on multi-source data fusion

检测方法	数据集	针对攻击/异常类型	应用场景	优点	缺点
MNOS[45]	OpenSky	轨迹伪造攻击、ADS-B 身份欺骗攻击	地面站少，低资源环境	无需额外传感器，适用于低资源环境	对历史数据依赖较大，所用算法对实时性要求较高
MKSVDD[48]	OpenSky+SSR	拒绝服务攻击	高安全空域，具有SSR区域	适用于复杂空域，适应新航线能力较强	计算复杂度较大，异常数据解释性较弱
DBSCAN[49]	OpenSky	轨迹伪造攻击	航班密度大，海量轨迹数据	适用于大批量数据分析	需人工设定参数，对小幅异常位置检测能力有限
TD[50]		欺骗攻击	禁飞空域、机场周边	误报率低，对欺骗攻击检测精确度较高	依赖多地面站，对短时欺骗信号检测能力有限

3.1.3　基于密码学的完整性与真实性验证方法

与前述基于数据模式分析的异常检测方法不同，密码学技术本质上是一种主动的安全防御机制，其核心目标是通过加密、数字签名等手段从源头保证数据的完整性和来源的真实性。虽然其主要功能是预防和验证，而非传统意义上的“检测”，但它们构成了最确定的一种异常识别手段：任何未能通过密码学验证的报文都会被直接、确定性地判定为异常。因此，本节将其作为一种基于验证的确定性异常识别方法进行综述。

基于密码学的异常检测方法检测过程为：首先，消息发送端在广播 ADS-B 报文之前，使用事先约定或分配的密钥对报文内容进行认证处理，生成签名或哈希消息认证码；其次，将此认证码或签名附加在 ADS-B 广播报文中发送，接收端收到 ADS-B 报文后，依据共享的密钥或已知的公钥信息，对接收到的报文重新进行认证计算，验证报文的完整性和真实性；然后，比较接收端计算的认证码或签名与报文携带的认证码或签名是否一致；最后，若认证结果不一致，则认定该消息为伪造或篡改，判定为异常。

由于 ADS-B 报文仅提供明文广播，缺乏验证发送者身份及数据完整性的机制，针对此问题，Khan 等[51]提出了一种 ADS-B 安全认证框架，通过可信第三方基于椭圆曲线算法生成区域性的非对称公私钥对，并分发给相关区域地面站，航空器在飞行过程中随机生成对称密钥，同时利用分发好的公钥进行加密并对其进行拆分，形成若干片段，接收端重组片段后，利用接收报文中的校验字段生成初始向量，再将上述生成的密钥和初始向量在航空器端与地面端利用 AES-GCM 算法，对每条 ADS-B 报文生成安全认证标签，通过二者标签值比对对该报文进行判别，实验结果表明，该方法在不修改原始协议结构和硬件设备的前提下，带宽利用率与检测结果准确率较高，但并未考虑大规模密钥分发、证书管理等复杂场景。

在此基础上，Dabit 等[52]提出了一种面向全球的 ADS-B 安全区域认证框架，与之前方法相比，该方法通过椭圆曲线狄菲-赫尔曼 (elliptic curve Diffie-Hellman, ECDH) 协议计算共享密钥并进一步衍生出 AES-256 对称会话密钥，航空器端在发送 ADS-B 报文前，使用 AES-256 对报文内容进行加密，并

通过私钥对报文生成数字签名后一并广播, 地面端在收到报文后, 利用共享的 AES 会话密钥解密, 并以发送端的公钥验证数字签名, 实现对报文完整性与真实性的实时校验, 在实验仿真与分析中证明了对中等规模攻击具有明显的抵御效果且成本较低。

为解决大规模部署中证书管理负担过大的问题, Chen 等[53] 提出了一种基于分层身份签名 (based on hierarchical identity signature, BHIS) 的 ADS-B 安全框架, 其方法架构如图 4 所示, 由顶层密钥生成中心 (key generation center, KGC) 生成主密钥对, 并分发给下级航空公司服务器 (airline server, ALS), 为每架航空器进行身份密钥生成分配, 航空器利用自身私钥对广播报文进行签名, 地面端接收到报文后, 通过双线性配对运算重构签名, 并利用批量验证机制汇总多个航空器签名, 进行一致性校验, 该方法在消息处理效率与安全性方面有较大提升, 但并未对报文丢包问题进行研究。

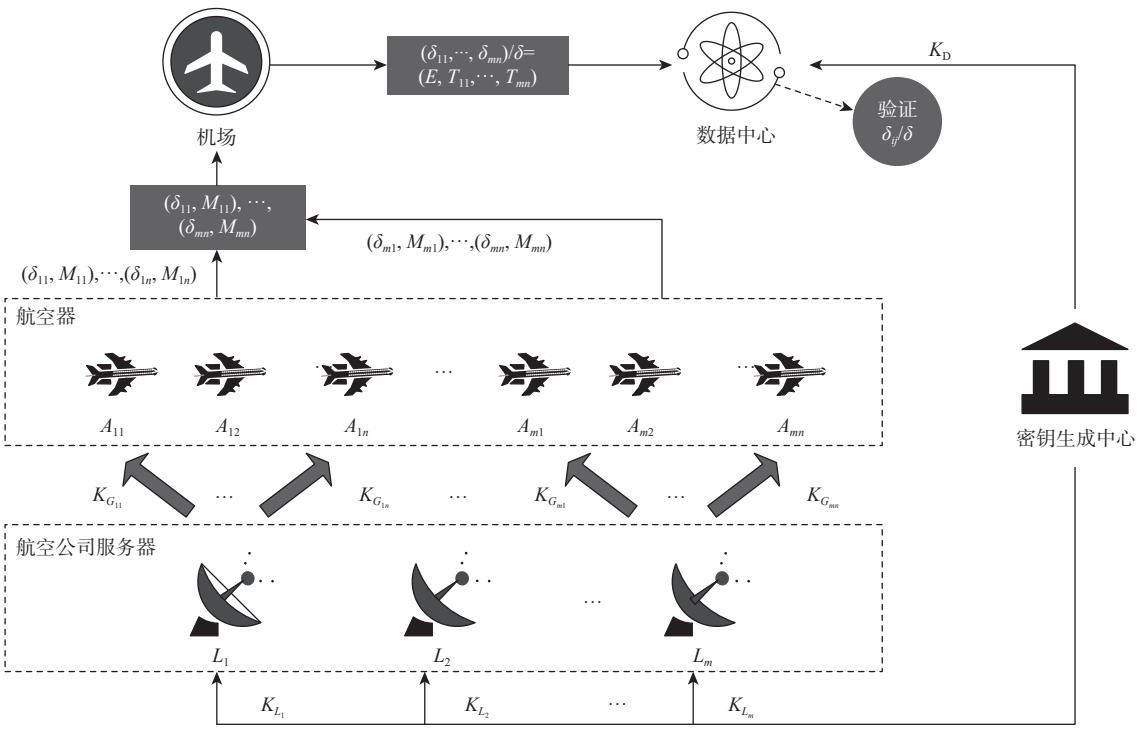

图 4　BHIS 系统架构[53]

Fig. 4　BHIS system architecture[53]

为解决上述问题, Yao 等[54] 提出了利用区块链与无证书签名结合的 ADS-B 认证方案, 通过 KGC 生成系统参数与部分私钥, 同时航空器端据此生成自身密钥对并将公钥上传至区块链, 航空器端用私钥签名 ADS-B 报文并添加时间戳, 并以纠删码分组传输, 地面端恢复签名后检查时间戳有效性, 并从区块链获取公钥进行批量签名验证。该类方法通过消息认证机制从源头识别异常, 避免伪造、篡改和重放等复杂攻击, 但密钥管理与通信开销是其普遍存在的挑战。

近年来, 基于密码学的完整性与真实性验证方法研究呈现出由通信链路被动监测到“源端认证-链路保护-接收端可追溯”的体系化演进。总体上, 此类方法以加密校验与身份绑定为核心, 通过在协议层提供报文完整性、消息新鲜性与发送方实体性证明, 显著降低了伪装、篡改与重放导致的误报或漏报, 具备强可解释性与形式化安全边界, 并在多站融合时能以密钥域为锚点实现跨网络一致性核验。然而, 现有工作同样受制于密钥生命周期管理与撤销机制、跨域信任根与证书基础设施的可扩展部署、航空适航与实时性约束下的时延或带宽开销, 并在复杂电磁和拥塞场景中, 时钟同步与丢包也会放大认证失败率并引入告警折中。面向此研究方向前沿, 亟须围绕标准化数据集、统一评测协议与运行级别试验场完成从安全性证明到工程化落地的闭环验证。基于密码学的异常检测方法总结如表 5 所示。

以上 3 种基于一致性检验的 ADS-B 异常检测方法优缺点如表 6 所示。此外, 一致性检验方法拓展了 ADS-B 异常检测的适用范围与适应能力, 为 ADS-B 提供了身份级、系统级的异常识别能力。

3.2　基于深度学习的 ADS-B 异常检测方法

随着 ADS-B 系统面临的攻击类型日趋复杂和多样化, 基于一致性检验的 ADS-B 异常检测方法

表5 基于密码学的异常检测方法总结

Table 5 Summary of anomaly detection methods based on cryptography

检测方法	数据集	针对攻击/异常类型	应用场景	优点	缺点
AES-GCM[51]	自采集数据集	ADS-B身份欺骗、ADS-B报文篡改、重放攻击	区域广播环境	不改变ADS-B原协议,实时性好,运算高效,低带宽占用	仍需密钥分发管理,丢包严重
ECDH[52]		数据篡改攻击、重放攻击	全球/洲际级广播环境	区域化分级密钥管理,实时性较好,性能开销适中	对跨区域管理场景关注不足,未处理丢包严重问题
BHIS[53]		数据篡改攻击	大规模/分层结构广播环境	有效解决跨区域管理场景下报文传输效率问题	计算开销相对较高,未有效处理消息丢包问题
ECB-CLS[54]	自采集数据集	欺骗攻击、数据篡改攻击、重放攻击、数据丢包	分布式/资源受限广播环境	无需证书管理,具备区块链透明性与抗丢包性,批量验证高效	系统复杂度高,区块链部署成本较高,增加通信开销

表6 基于一致性检验的ADS-B异常检测方法总结

Table 6 Summary of ADS-B anomaly detection methods based on conformance test

检测方法	主要针对的攻击类型	方法描述	优点	缺点
基于独立定位的异常检测方法	GNSS干扰攻击、欺骗攻击、轨迹伪造攻击	将独立物理测量量与广播信息对齐,构建检测统计量与误差度量,并与预设阈值比较进行检验	算法机制透明,可解释性强,且具有独立验证能力	依赖多站协同测量,部署与维护成本高,对测量误差及噪声较敏感
基于多源数据融合的异常检测方法	拒绝服务攻击、欺骗攻击	通过融合多源特征对正常轨迹进行建模,并计算当前轨迹与正常轨迹模型之间的偏差,实现异常检测	支持无监督学习,适应场景广泛,泛化性较好	计算复杂度较高,依赖大量训练数据,可解释性较差
基于密码学的完整性与真实性验证方法	重放攻击、数据篡改攻击、欺骗攻击	利用对称密钥或无证书签名算法对ADS-B报文进行加密,接收端获取公钥对报文进行验证	无需改变当前ADS-B协议格式,具有较好的向后部署性,并且具备批量验证与抗丢包能力	密钥分发管理需要消耗额外的资源,同时受限于ADS-B报文长度,嵌入认证信息具有一定负担

在实际应用中逐渐暴露自身存在的问题:外部独立测量资源的高度依赖、传感器部署成本高、密钥认证机制开销较大、实时响应能力弱及对复杂欺骗攻击识别能力不足等。这些问题在动态环境或资源受限区域中尤为突出,难以满足高密度空域下对安全性和实时性的双重需求。因此,研究重心逐步转向基于深度学习的ADS-B异常检测方法。

基于深度学习的ADS-B异常检测方法具有较强的数据学习能力和特征提取能力,能够适应海量高维度数据,从而在大规模数据场景下保持较好的性能与拓展性,同时能够捕捉复杂的时序关系,提高对缓慢偏移性异常数据或突发性异常数据的检测精度,有效提高了异常检测的泛化能力。

自2018年起,基于时序预测的思想开始被广泛应用于ADS-B异常检测领域中,其中,代表性模型包括长短期记忆网络(long short-term memory, LSTM)、卷积神经网络(convolutional neural network, CNN)、生成对抗网络(generative adversarial network, GAN)等,此类模型通常以正常样本训练,在推理时通过预测残差判别异常,适用于长期趋势与周期性变化的场景。但随着攻击方式愈发复杂,对时间序列数据检测的难度也随之增大,国内外研究者进一步引入了基于分类的思想,以射频指纹识别技术为代表,该技术借助深度网络从射频链路的硬件微差中学习设备身份表征,在有标签数据下直接输出正常、具体攻击类型、未知设备等类别,同时也发展出自监督或无监督学习以降低标签依赖,提升对未知设备的适应性。与此同时,基于数据重构的方法在缺乏标注时尤为有效:以自编码器(autoencoder, AE)等在正常数据上学习重构能力,检测阶段以重构误差为分数、无需先验异常知识即可发现潜在异常。

本节将系统综述基于时序预测思想、分类思想及数据重构思想在ADS-B异常检测中的应用,并分析各类基于深度学习的异常检测方法在特征提取、检测精度和泛化能力方面的优势与不足。

3.2.1 基于时序预测思想的异常检测方法

基于时序预测思想的异常检测过程为:首先,对连续的ADS-B报文进行滑动窗口切片与归一化预处理;然后,利用训练集学习窗口内的时间依赖,并对下一时刻或未来若干步的特征进行点预测;最后,依据正常数据的预测残差统计构建阈值,在检测阶段以预测残差与该阈值进行比较,实现对异常样本的判定。其中,LSTM模型多用于该思想的方法。

针对多航空器空间关联性不足的问题,Shabtai等[55]提出了一种基于空域状态序列(sequences of airspace states, SAS)的ADS-B异常检测方法,通过将提取到的区域特征与航空器特征组合成时序矩阵,利用编码器对时序矩阵进行特征编码,并将这些信息压缩为一个固定维度的隐状态向量,经过解码器将隐状态信息逐步生成预测序列并与真实序列对比,通过判别2个序列之间的相似度进行异常分类,该方法引入SHAP框架,增强了模型的可解释性,且实验结果表明,误报率低于0.15%,极大提

高了检测精度。

针对轨迹数据维度高、人工特征提取负担较大的问题, Ji 等[56] 提出了一种基于 LSTM 序列预测网络 (prediction network, PN) 的方法, 使用 Hausdorff 距离衡量待检测轨迹与正常轨迹模型的最大空间距离并设定评分, 构建轨迹语义兴趣序列, 计算待测轨迹与轨迹模型之间的语义相似度并输出评分, 通过阈值判别模块, 将 Hausdorff 距离评分、语义相似度评分分别与预设阈值进行比对, 判断该轨迹是否存在异常。

近年来, 商业航空受到严格的飞行规则限制, 在此情况下, 现有的异常检测方法对隐蔽性攻击检测精度不高。针对此类问题, Yue 等[57] 提出了一种基于 GAN-LSTM 的 ADS-B 异常检测方法, 其结构如图 5 所示, 通过关联飞行计划数据与 ADS-B 数据来构造空域飞行情景图像, 采用标准化相关函数对实时图像与预测图像进行对比, 并利用滑动窗口统计可疑图像数量进行分类。该方法解决了目前 ADS-B 异常检测方法未考虑 ATC 飞行规则而导致的检测精度低的问题, 能够有效捕捉飞行轨迹、速度等数据随时间演化的动态规律, 适用于识别缓慢漂移、突变或周期性异常等具有时序特征的攻击行为, 但对计算资源要求较高且在实时性要求较高的场景中应用受限。

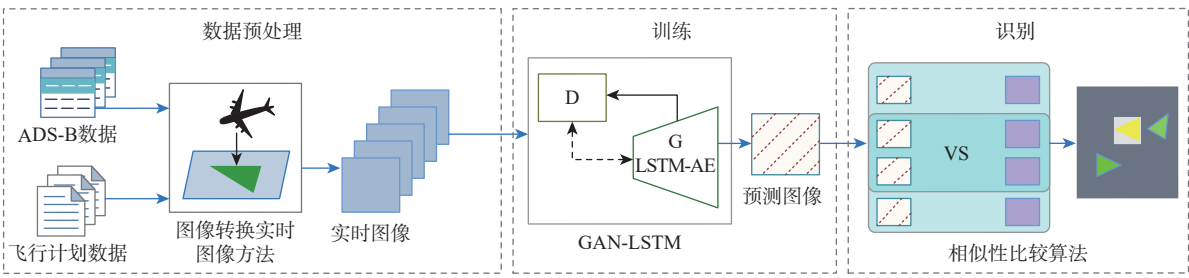

图 5　GAN-LSTM 结构[57]

Fig. 5　GAN-LSTM structure[57]

基于时序预测的 ADS-B 异常检测近年呈“单机轨迹点预测-区域多机场景预测”的演进。总体来看, 方法从单目标点预测走向多目标场景预测, 并与阈值学习深度耦合, 其优势在于对时序攻击的灵敏性和对业务规则的可融性。面向此研究方向前沿, 亟须围绕计算与时延约束、多机耦合与域漂移下阈值稳定及跨航线泛化与在线解释的权衡。基于时序预测思想的异常检测方法总结如表 7 所示。

表 7　基于时序预测思想的异常检测方法总结

Table 7　Summary of anomaly detection methods based on time series prediction thought

检测方法	数据集	针对攻击/异常类型	应用场景	优点	缺点
LSTM-SAS[55]	OpenSky	“幽灵飞机”注入	高流量机场周边空域	考虑并分析空域内多架飞机空间分布与相互关系, 内置异常原因可解释性	单机异常敏感度低, 计算复杂度较高
LSTM-PN[56]		轨迹伪造攻击	智慧交通系统	引入语义信息提高检测精度, 高效应对不同长度轨迹数据	严重依赖阈值设定, 对数据质量要求较高
GAN-LSTM[57]	CAAC	“幽灵飞机”注入、重放攻击、拒绝服务攻击	ATC环境下及具有商业航空背景	可视化异常情况, 预测精度增强	泛化能力受限, 计算资源需求较高

3.2.2　基于分类思想的异常检测方法

基于分类思想的异常检测过程为: 首先, 进行数据采集与标注, 完成清洗、对齐与分割; 然后, 依据任务定义构建类别体系, 并以监督学习训练判别器, 在开放场景下叠加开放集识别与持续学习机制; 最后, 在决策层输出离散类别及必要的定位或状态估计, 并辅以可解释性与运营级评估以支撑受监管的部署。其中, CNN 模型多用于该思想的方法。基于 CNN 的 ADS-B 异常检测框架如图 6 所示。

传统深度学习异常检测方法依赖轨迹特征, 并且缺乏端到端信号级伪造检测方案。为解决此问题, Joseph 等[25] 提出了一种基于生成对抗神经网络-卷积神经网络 (generative adversarial network-convolutional neural network, GAN-CNN) 的 ADS-B 异常检测方法, 通过将原始 ADS-B 报文输入到 GAN 模型中进行训练, 得到判别器, 利用一个二维 CNN 接收预处理后的 I/Q 数据矩阵, 并在时间维度上提取局部模式信息, 经过展平操作后输入至多个全连接层, 利用非线性映射实现高阶特征组合, 由 Softmax 输出各类航空器的识别概率, 但该方法依赖高质量原始数据, 同时识别航空器类型仅限于已

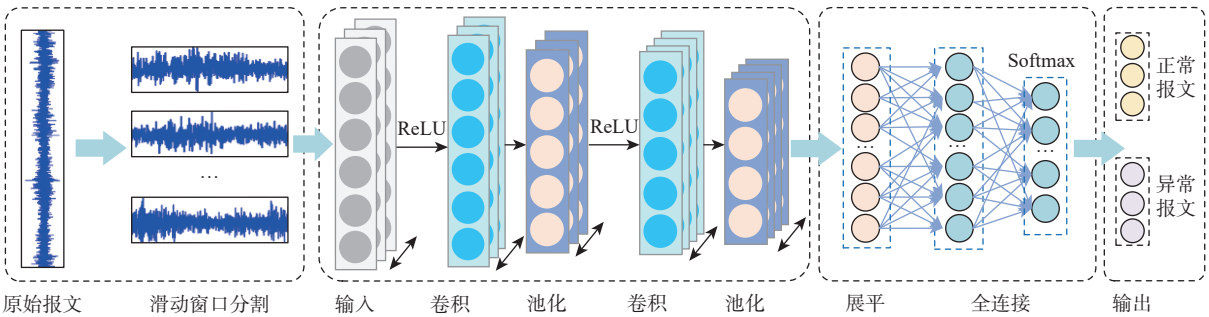

图 6 基于 CNN 的 ADS-B 异常检测框架

Fig. 6 ADS-B anomaly detection framework based on CNN

知类型，泛化能力有限。针对此问题，Cai 等[58]提出了一种基于注意力机制的卷积网络 (attention mechanism convolutional network, AMCN) 框架，通过构建逻辑回归分类器，对待检测范围内的 ADS-B 数据进行二分类，使用一维卷积网络提取单架航空器的时空特征，生成局部特征图并融合改进位置编码方法，将多个航空器的相对空间关系映射到注意力网络中，实现全局语义建模，将干扰源定位任务转化为干扰区相对位置的 16 类分类问题，并通过软标签的形式输出分类概率，最终确定干扰源所在网格区域。该方法通过先筛选再定位的分阶段策略有效减轻了模型负担，并使用相对位置分类策略提升了跨区域的鲁棒性和泛化能力，其结构灵活、可扩展性强，适用于高维 ADS-B 时序特征的分类或预测任务，特别是在数据具有明确标签和分布规律的情形下能够实现高精度识别，但对时间依赖性强的攻击模式敏感度较低，同时在异常样本稀缺或标签不完整的情况下性能可能下降。

为应对 ADS-B 系统故障或自然因素导致的未及时广播 ADS-B 报文情况下所带来的空域安全隐患，Heiselberg 等[59]提出了一种基于多光谱遥感图像与 CNN 的飞行器状态估计模型，利用 Sentinel-2 卫星图像中因通道成像延迟而产生的颜色错位特性，从中推断飞行器在成像时刻的空间位置与动态特征，利用 CNN 提取图像中飞机的空间形状与颜色错位特征，回归输出包含位置、尺寸、航向、速度、高度等 7 维状态向量，卷积层捕捉局部结构与位移信息，回归层联合输出物理状态，并采用 Smooth L1 与 focal loss 优化训练，该模型可在 ADS-B 缺失场景下对飞行器进行检测与状态估计，实现无源空域监控，但模型依赖训练集中已配准的 ADS-B 数据，难以应对无标签目标或训练样本分布外的新型飞行器。

同时，为解决 ADS-B 系统遭受注入攻击的问题，Vajrobol 等[31]提出了一种基于集成元学习 (ensemble meta-learning, EML) 与可解释 AI 的异常检测模型，采用 LSTM、随机森林及 XGBoost 这 3 种模型作为基础模型并输出各自的异常值，将 3 种模型的异常值作为元特征用于训练元模型并输出分类结果，可解释 AI 根据分类结果提供透明的决策解释。该方法相较于单一检测模型有较高的检测精度，同时具备更好的泛化能力。

为解决“闭时集训练、开时集部署”场景下由时间漂移与域偏移导致的识别率显著下降这一问题，Zheng 等[60]提出了一种以实收信号与基于统计建模的理想重建信号共同构造二维时频特征图 (time-frequency feature diagram, TFFD) 的方法，并在引入频偏建模层的 Swin Transformer 中完成判别，从系统层面打通“采集-解析-特征-识别”链路以提升跨时稳健性，该方案在闭时集与开时集均取得较优性能，优势在于充分利用物理先验与重建对齐以增强特征鲁棒性，但局限在于开时集精度仍有明显回落，对特征构造与较干净标注的依赖较强，跨更长期时漂与复杂电磁环境的泛化能力仍受限。

为缓解上述方法对充足标签依赖强，并难以在少样本条件下持续扩展等方面的局限，Li 等[61]提出了一种小样本开放集增量学习 (few-shot open-set incremental learning, FSOSIL)，联合原型正交化、开放集损失与自适应阈值机制实现识别已知、发现未知、低遗忘，该方法的优势在于仅依靠单样本训练且存在未知类别的情形下，仍能实现对已知目标的高精度识别，并对未知目标进行有效拒绝，但缺点在于训练流程复杂、对元任务采样与超参数敏感，且默认标签相对洁净，难以直接应对“严禁样本回放”的连续学习约束。

近年来，基于分类思想的异常检测研究总体呈现由封闭集判别向开放集-增量-噪声鲁棒的系统化演进。虽然此类方法实时性与可扩展性好，易与规则、物理先验及多源证据进行级联融合，但依赖标签，同时对时漂敏感，且流程复杂。综上，研究前沿亟须构建“开放集+类增量学习+少样本学习”统一原型框架并配合保形预测，并推进无回放的半监督持续学习与对抗合成数据扩增。基于分类思想的异常检测方法总结如表 8 所示。

表 8　基于分类思想的异常检测方法总结

Table 8　Summary of anomaly detection methods based on classification thought

检测方法	数据集	针对攻击/异常类型	应用场景	优点	缺点
FlightSense[25]	自采集数据集	ADS-B身份欺骗	未加密广播环境	无需手动特征提取, 自动学习信号特征	识别仅限已知飞机, 依赖高质量I/Q数据
AMCN[58]	中国民航数据主中心采集	GNSS干扰	地面无GNSS信号监测站的区域	支持大规模干扰源定位, 定位精度优于传统方法	依赖多个飞机数据协同分析, 对细粒度干扰事件灵敏度有限
EML[31]	Mendeley平台	“幽灵飞机”注入、速度欺骗攻击	对模型透明性有高要求的航空安全环境	高效的特征选择方法, 提升对特定攻击的敏感性, 内置决策解释机制	部署成本较大, 模型复杂度较高
Sentinel-CNN[59]	OpenSky	ADS-B设备故障	ADS-B缺失空域	实现无源目标检测, 有效提升空域态势感知能力	在姿态变化剧烈或强干扰条件下仍面临误差累积问题
TFFD[60]	自采集数据集	ADS-B身份欺骗	空管监视与航空通信安保的实时身份鉴别	成本可控, 便于维护	工程复杂度高
FSOSIL[61]	自采集数据集	伪造信息、身份欺骗	低样本、开集、增量场景下的设备身份鉴别与拒识	可持续拓展, 数据效率高	依赖元任务设计划分策略, 任务构造与调参成本较高

3.2.3　基于数据重构的异常检测方法

基于数据重构思想的 ADS-B 异常检测过程为: 首先, 在训练阶段仅观察正常轨迹, 学习正常数据在潜在空间的分布, 并尝试尽可能准确地重建输入信息; 然后, 在检测阶段, 待测报文经模型重构后与原始数据进行比较, 重构误差被用来衡量数据与正常模式的偏差; 当误差超过基于正常数据统计规律设定的阈值时, 即判断为异常。阈值可以通过支持向量数据描述或利用重构误差分布的高分位数自适应确定, 以保证对未知攻击的泛化能力。其中, AE 模型多用于该思想的方法。基于 AE 的 ADS-B 异常检测流程如图 7 所示。

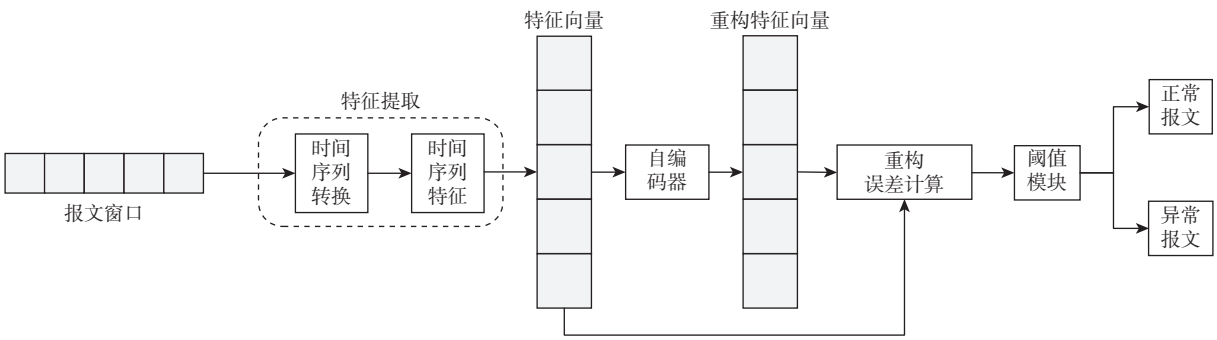

图 7　基于 AE 的 ADS-B 异常检测流程

Fig. 7　Flow chart of ADS-B anomaly detection based on AE

针对 ADS-B 协议本身缺乏安全机制导致的篡改、欺骗攻击等问题, Habler 等[62] 提出了一种基于 LSTM encoder-decoder 算法的 ADS-B 异常检测方法, 通过编码器将 ADS-B 广播报文序列编码为固定维度向量, 捕获时序依赖性, 利用解码器重新构造原始 ADS-B 报文序列, 对新的 ADS-B 序列采用余弦相似度, 计算重构误差, 并经由阈值模块判定是否存在异常。然而, 该模型需要一定的延迟积累窗口才能有效识别异常, 同时未能考虑空域中多个航空器之间的空间关联性。

ADS-B 协议因缺乏加密与认证机制, 极易遭受伪造、篡改、干扰等恶意攻击。然而, 现有方法还存在阈值设定机制缺乏自适应能力, 导致误判率高及模型存在过拟合或欠拟合风险的问题。为解决上述问题, Luo 等[63] 提出了一种变分自编码器-支持向量数据描述 (variational autoencoder-support vector data description, VAE-SVDD) 模型, 利用具备时序感知能力的编码器将序列映射至潜在空间, 捕捉其时间依赖性和分布特征, 通过解码器再从潜在变量中重构出原始序列, 由于每个数据点在多个滑动窗口中被重构多次, 为减少异常误判, 采用余弦相似度筛选其中位重构值作为最终输出, 计算重构值与真实值之间的差异, 并将误差序列输入 SVDD 模型中训练, 学习正常数据的边界分布, 通过测量新样本重构误差与 SVDD 球心的距离, 判断其是否越界, 从而实现异常识别。但该方法忽略了航空器飞行期间的上下文差异及重构值不稳定的问题。在此基础上, Chevrot 等[13] 提出了一种基于上下文自编码器 (contextual auto-encoder, CAE) 模型的 ADS-B 异常检测方法, 通过将 ADS-B 原始报文转换为标

准化后的多变量时间窗序列，并依据飞行阶段对数据进行标注分类，通过一个双向LSTM编码器进行特征编码，提取时间依赖性特征，并根据所处飞行阶段分别送入不同的上下文解码器重构数据，以重构误差为基础，分别为不同解码器计算对应的异常阈值，实现高精度的异常检测。该方法通过建模上下文差异，提高了对飞行阶段的异常检测精度，同时具有良好的可拓展性。

为了解决深度学习方法对新航线或历史数据缺失航班的检测精度和泛化性较差的问题，Fried等[28]提出了一种基于差分时序特征的自编码器(differencing time-series transformation autoencoder, DTTA)模型的ADS-B异常检测方法，通过将ADS-B报文中地理坐标转换为三维地心坐标系，并应用时间序列差分变换，以消除趋势性和季节性因素，提取反映飞行状态变化的动态特征，利用非递归结构的AE对正常航班数据进行训练，输入新数据后由模型进行重构，并计算其与原始输入之间的重构误差，将该误差与验证集上得到的误差分布进行比对，计算其在误差分布中的概率值，依据预设阈值进行异常判断。

为解决未知航班检测的泛化性不足及历史异常检测模型无法处理远距离依赖关系的问题，丁建立等[64]提出了一种基于Transformer-变分自编码器(Transformer-variational autoencoder, TVAE)的ADS-B异常检测模型，通过对原始ADS-B数据进行特征筛选与归一化处理，排除不随时间变化的冗余字段，针对时间点上的数据缺失，采用线性插值方法填补缺失值，以保持时序数据连续性，采用Transformer编码器进行长程依赖关系建模，通过自注意力机制，生成潜在的上下文特征表示，引入潜在随机变量来建模数据的随机性和整体性特征，估计该变量的后验分布，生成重构后的ADS-B数据，计算原始数据和重构数据之间的重构误差，并经过阈值模块来检测异常。该方法有效解决了现有方法无法处理长程时序数据的问题，提高了检测精度，但在实际应用中对训练数据的质量和分布覆盖范围高度敏感，若正常数据样本分布不完整或训练集存在异常混入，可能导致模型学习失效，重构能力泛化不足。在此基础上，Luo等[65]提出了一种基于时序卷积神经网络-Transformer-支持向量数据描述(temporal convolutional network-Transformer-support vector data description, TTSAD)的ADS-B异常检测模型，利用一维时序卷积网络(temporal convolutional network, TCN)模块对时间序列进行快速预测，将预测结果输入至Transformer重构模块，通过位置编码、自注意力和多头注意力机制对数据进行上下文建模与重建，以尽可能逼近原始序列，计算重构序列与真实序列之间的差值，并将该误差向量输入SVDD模块，其在高维空间中构造最小包围球，通过训练误差分布自动确定最优判定阈值，实现对异常数据的有效识别。该方法通过融合多模型，有效提升检测效率，同时实验结果表明在多种攻击场景下准确率可达94%，鲁棒性与泛化能力得到大幅提高。

近年来，基于数据重构思想的异常检测研究总体表现为不依赖异常标签，同时仅用正常数据即可建模，易与规则、多源证据级联，具备良好可迁移与实时部署潜力，但暴露出的问题在于对正常分布覆盖与数据洁净度敏感，且跨航线落地往往需要较多校准与流程治理。综上，研究前沿亟须以不确定性评估稳健化重构分数，同时利用无回放的半监督持续学习抵御污染与概念漂移，实现可解释、可运维、在线化的一体化框架。基于数据重构思想的异常检测方法总结如表9所示。

以上3种基于深度学习的异常检测方法优缺点如表10所示。深度学习方法通过训练可自动从

表9 基于数据重构思想的异常检测方法总结

Table 9 Summary of anomaly detection methods based on thought of data reconstruction

检测方法	数据集	针对攻击/异常类型	应用场景	优点	缺点
LSTM-编码器[62]	FlightRadar24	ADS-B身份欺骗、ADS-B报文篡改	单机或航空器内部	系统部署要求少，无需额外数据支持	高度依赖已知航线数据，实时性表现较差
VAE-SVDD[63]	OpenSky	拒绝服务攻击、数据篡改攻击	实时检测或历史数据回溯分析的高风险空域	较低的误报率和漏报率	对训练数据依赖较大，时序依赖捕捉能力有限
CAE[13]	OpenSky	错误警报注入	突发飞行事件识别	在不同飞行阶段的异常检测中表现优异	针对阶段过渡时的异常检测表现差
DTTA[28]	OpenSky	数据篡改攻击	不依赖历史数据检测航迹异常空域	对历史数据不足的航路或新航线泛化性较好	无法处理飞行中的动态变化
TVAE[64]	FlightRadar24	“幽灵飞机”注入、拒绝服务攻击	泛航线、无先验场景	有效捕捉时序数据的全局信息，处理大规模数据	训练过程资源消耗大，数据量小或包含噪声数据时，性能可能受到影响
TTSAD[65]	OpenSky	数据篡改攻击、重放攻击	轨迹安全监控	训练时间短，可拓展性好	结构相对复杂

表 10　基于深度学习的 ADS-B 异常检测方法总结

Table 10　Summary of ADS-B anomaly detection methods based on deep learning

检测方法	主要针对的攻击类型	方法描述	优点	缺点
基于时序预测思想	轨迹伪造、速度欺骗、重放攻击、“幽灵飞机”注入	通过建模时序数据, 能够捕捉序列中的长期依赖与动态行为变化	能有效建模序列数据中的长期依赖关系, 适用于飞行状态等具有时序性的行为模式识别	网络结构较为复杂, 训练过程计算资源消耗大, 且在长序列建模中存在梯度传播效率问题
基于分类思想	GNSS干扰、ADS-B身份欺骗	采用多层神经结构, 适合处理时序特征, 进行高维特征分类与学习	结构形式灵活, 适用于提取高维时序特征, 能够高效完成复杂模式的时序分类任务	对时间相关性建模能力有限, 难以捕捉数据随时间演化的动态特征
基于数据重构思想	数据篡改攻击、拒绝服务攻击	通过编码解码结构重构输入数据, 以重构误差判断样本是否异常	可在缺乏异常标签的情况下实现异常检测	模型对正常数据分布高度依赖, 若训练集覆盖不全, 容易对异常识别能力产生干扰

数据中学习关键特征, 挖掘潜在异常模式, 无需人工定义具体规则, 适应性更强, 且可根据不同应用需求灵活选择模型结构, 如监督、无监督或半监督模型, 也可融合多源信息, 适应多场景下的异常检测任务。

4　ADS-B 异常检测应用

在 ADS-B 的运行保障中, 现行空中管理体系仍然依赖飞行员与空管人员的人工报告、系统内置的运行告警、基于冗余导航手段等事后缓解措施, 并非实时对 ADS-B 报文进行可信性评估或 GNSS 干扰监测。文献 [66] 指出, 当前投入应用的射频干扰 (radio frequency interference, RFI) 报告并不能反映现场的真实情况, 报告数量只能提供小部分指示, 同时取决于人们是否愿意报告。因此, 需要将基于 ADS-B 异常检测技术的监测与评估模块嵌入既有监视体系, 以实现对报文可信性的在线评估与告警。

目前公布的 ADS-B 异常检测产品中, 主要采用几何一致性检验、多源数据一致性检验及时序预测方法, 在不改变现有监视链路的情况下, 面向航迹级与空域级 2 类目标提供自动检测、可信度评估与告警联动能力。相关应用场景如下:

1) 航迹溯源与可信度评分。对目标航迹进行几何重定位与运动学一致性比对, 给出报文来源可信度/验证得分, 溯源潜在的“幽灵飞机”航迹或冒名播发, 从源头降低伪造报文进入战术显示与自动化决策链的风险。

2) GNSS 干扰与欺骗态势监测。结合星基或地基 ADS-B 与多源监视, 在空域尺度统计导航完整性类别 (navigation integrity category, NIC) 或位置完整性类别 (position integrity category, PIC) 退化、定位漂移、丢报等指标, 形成近实时干扰热区与强度评估, 支持管制流量调配、航司运控改航及预案触发。

3) 已知异常模式识别与版本比对。利用时序模型 (如 EKF、IMM、深度学习预测残差) 对不同异常类型 (如位置偏移、速度/航向异常、轨迹伪造) 进行特征匹配与相似性检验, 判定是否命中既有异常样式库或出现新型异常类型。

随着复杂空域运行与数据规模的增长, 异常检测作为提升监视可靠性与安全韧性的核心手段, 已经成为学术界与工业界的研究热点。ADS-B 异常检测技术是新一代航空监视安全保障的重要基础。通过对航迹-报文-环境进行组成式分析, 提取多维度特征, 计算航迹可信度与空域健康度指标, 可在应用开发与运行维护全周期中检测异常航迹与不可靠数据源, 深度挖掘 GNSS 干扰、报文异常与数据质量风险, 实现从感知到决策的闭环管控。全面覆盖空域态势监测、运行审计取证、数据门控与第三方源管控及系统运维保障等应用场景。表 11 总结了当前已成功部署的 ADS-B 异常检测产品。

表 11　基于 ADS-B 异常检测技术的空域监测产品

Table 11　Airspace monitoring products based on ADS-B anomaly detection technology

产品名称	企业	检测对象与粒度	应用场景	优势	局限性
Aireon Safety Dashboard	Aireon	空域级指标化监测与趋势分析	面向航空导航服务机构与监管的空域风险监测	星基覆盖广、指标体系完善、支持区域与全球视角、运营成熟	商业化闭源、对接与采购成本较高、细节透明度有限
uAvionix truSky	uAvionix	航迹级报文真实性验证与可信度评分	面向无人机超视距任务	低时延服务、提供验证得分、生态集成成熟、易于接入现有管控链路	覆盖度受地面接收网络布局影响、空域级态势需与其他平台联动
Spire Global Aviation GNSS Interference	Spire Global	空域级干扰监测与区域告警	面向航空运营者和监管部门, 通过API提供ADS-B异常趋势与区域可靠性评估	全球覆盖, 支持实时API和自定义区域监测	算法细节和检测标准公开有限, 服务费用和对接成本较高
SkAI Data Services GPSwise	SkAI Data Services	空域级近实时干扰与疑似欺骗态势图与事件分析	航空公司运控评估、机队层级研判、研究与汇报	近实时可视化、开放生态灵活、易于快速验证与分析	数据完备性与一致性受众包网络密度影响、可靠性低于星基体系

5 面临的挑战与展望

近年来,尽管面向ADS-B的异常检测方法取得了显著进展,但在发展过程中仍面临诸多亟待解决的技术挑战,这些挑战不仅制约了现有检测模型在复杂环境下的检测性能和泛化能力,也影响了面向ADS-B系统异常检测技术在实际航空运行场景中的部署效果。随着攻击技术的不断演化,攻击者开始倾向采用更加隐蔽、复杂且具有对抗性的规避手段,使得传统检测机制难以有效识别与响应异常行为,暴露出当前检测模型在鲁棒性与可解释性方面的不足。本节将深入探讨当前研究中所面临的主要挑战,并展望未来可行的研究方向。

5.1 面临的挑战

1)对抗性攻击问题。随着技术的不断发展,异常检测方法进步的同时,也给恶意攻击者提供了新的技术手段。这些攻击是针对特定模型和数据集量身定制的,使其难以检测和防御,并导致异常检测中出现误报或漏报[67]。文献[68]明确指出,主流的深度学习异常检测模型在应对时间序列毒化攻击时极易被破坏。同时,文献[69]系统演示了针对基于深度学习的ADS-B欺骗检测器的物理层对抗攻击。因此,未来的研究应致力于系统引入对抗性稳健训练框架,将对抗样本融入模型训练流程,以增强模型对输入扰动的稳定性。同时,针对时间序列数据的特有结构,开发融合物理约束与时间连续性的攻击检测机制。

2)数据稀缺与不平衡。异常事件在真实航空运行中极为罕见,导致可用于模型训练的已标记异常数据十分稀少且样本分布不均。数据样本的不足和类别不平衡使得传统有监督模型难以有效学习异常模式,研究者往往不得不依赖无监督或半监督学习方法来检测异常,并通过模拟攻击数据来构建评估基准[70-71]。因此,未来的研究应关注合成攻击数据生成、多样化样本设计与多任务学习的融合机制。

3)可解释性缺乏。当前的深度学习检测模型大多属于“黑盒”,无法直观地向用户解释判定异常的依据[72-73],而传统统计模型基于高维特征空间超平面的判别同样难以被领域专家所理解。在航空安全这一关键领域,这种缺乏可解释性的现状不仅降低了用户对异常报警的信任度,也给后续人工分析带来困难。因此,后续研究应侧重于提高模型的可解释性,为深入理解数据与模型提供基础。

4)泛化能力不足。当前主流模型对新环境和未知模式的泛化能力欠缺仍是ADS-B异常检测的一大挑战。许多深度学习模型对训练数据的依赖性较强,当深度学习模型应用于训练分布以外的数据时(如新的航线、机型或全新手法的攻击),常出现检测性能显著下降的问题。部分方法甚至需要针对每条航线单独训练专门的模型,缺乏跨航线或跨区域的一般化能力[74]。同时,正常与异常的界限会随着时间推移和运行环境改变而发生漂移[75-76]。因此,未来的研究方向应在有限样本甚至零样本的条件下,让模型具备检测新型异常的能力。

5.2 未来研究展望

针对本文所指出的目前研究仍需面临的挑战,未来研究应集中于抵御对抗性攻击、增加可解释性及提高模型泛化性等方面,以进一步提高ADS-B异常检测方法的检测性能与实用性。未来可以重点研究的方向包括以下方面:

1)对抗性防御。为应对对抗性攻击威胁的加剧,未来研究应着重于设计更具鲁棒性的ADS-B异常检测模型,以抵御恶意攻击者的对抗性攻击、中毒注入攻击等其他攻击方式。可考虑通过“基础对抗训练+输入净化”的两段式策略构建安全退化通路。在训练阶段,针对物理可达扰动与小幅梯度扰动进行联合对抗训练以提升参数稳健性,推理阶段可叠加时序去噪与可行域投影以抑制异常微扰扩散,避免在未知分布下出现错误判决。

2)增强模型泛化能力。当前的ADS-B异常检测方法的研究大多依赖于版本落后或自采集数据集,但这些数据集存在时效性不足、可信度较差及严重的数据不平衡问题,难以满足当前异常检测模型提高泛化性的需求。因此,可考虑采用迁移学习等方法,实现预训练主干在目标空域少量标注上微调,并使用对抗式或统计匹配的域对齐削弱分布差异,同时跨站点以联邦方式聚合参数而非原始数据以满足合规与隐私约束,同时配合类别重加权与自适应阈值重标定维持稳定检出率与低误警率。

3)先验约束的重构学习。为增强ADS-B报文中的物理约束,可考虑以AE为核心,在解码端注入3类先验。物理先验通过对位移-速度-加速度的平滑约束,以及对协调转弯与升降率边界的惩罚,使运动过程连续且落在可行范围;当输出越界时,再用投影把点拉回可行域,对难以求导的硬规则生成可学习的惩罚。程序先验把进离场程序、扇区高度窗、禁飞区等编码为时空掩膜,对“违反规程”的片段在重构损失中加权放大,并用阶段感知门控在起飞、巡航、进近等阶段动态调节约束强度。运行先验把气象与调度作为条件输入,并用后验正则化协调多源先验的相对权重;同时将雷达或MLAT与

气象对齐做一致性重构, 用一致性偏差作为辅助告警信号。评测时除 F_1 分数外, 增加物理违约率、程序违规率与跨域稳健性等作为评估指标。

4) 大模型部署。在 ADS-B 异常检测中, 可将通用大模型当作“时空语义引擎”, 通过指令化微调与检索增强, 让模型同时理解轨迹与气象等上下文, 在推理阶段输出“异常分数+不确定度”。为兼顾实时性与算力, 采用“云端教师-边缘学生”的蒸馏方案, 并配合低秩适配与整模量化, 在不牺牲识别能力的前提下降低延迟与资源占用; 对高风险或高不确定样本, 采用“边缘筛查-云端复核”的两级架构, 并结合密码学验签与独立定位偏差形成多证据决策。上线运维遵循影子运行与分批发布, 持续监测时延、吞吐、能耗与检出率漂移, 确保系统稳定演进。整体上, 这一方案在“可解释、可复核、可落地”的同时, 保持对复杂场景的鲁棒性与可维护性。

6　结 束 语

由于 ADS-B 系统的报文明文传输方式及物联网、5G 等新技术的迅猛发展, 导致 ADS-B 数据获取难度大幅下降。同时对 ADS-B 的攻击手段也由早期的显性注入与篡改行为逐渐演变为隐蔽性更强、结构更复杂的攻击。因此, 如何在复杂时空背景下实现对异常行为的准确识别, 成为保障空中交通安全的关键任务之一。本文对 ADS-B 异常数据的基本概念和检测流程进行了系统梳理, 详细分析了基于一致性检验的 ADS-B 异常检测方法和基于深度学习的 ADS-B 异常检测方法的研究现状, 探讨了不同异常检测方法在异常检测精度、泛化能力和实时性方面的优势与不足。对已投入应用的 ADS-B 异常检测产品进行归纳总结。针对当前 ADS-B 异常检测领域所面临的主要挑战, 提出未来研究方向, 为后续研究提供参考。

参考文献 (References)

[1] CCOM, DCOM. Nextgen-SESAR state of harmonisation[R/OL]. Luxembourg: Publications Office of the European Union, 2018. https://www.faa.gov/nextgen/nextgen-sesar-state-harmonisation.

[2] Çevik N, Akleylek S. SoK of machine learning and deep learning based anomaly detection methods for automatic dependent surveillance-broadcast[J]. IEEE Access, 2024, 12: 35643-35662.

[3] Strohmeier M, Lenders V, Martinovic I. On the security of the automatic dependent surveillance-broadcast protocol[J]. IEEE Communications Surveys & Tutorials, 2015, 17(2): 1066-1087.

[4] Wu Z J, Shang T, Guo A X. Security issues in automatic dependent surveillance-broadcast (ADS-B): a survey[J]. IEEE Access, 2020, 8: 122147-122167.

[5] Hicok D S, Lee D. Application of ADS-B for airport surface surveillance[C]//Proceedings of the 17th Digital Avionics Systems Conference. Piscataway: IEEE Press, 1998, 2: 3401-3408.

[6] Corrado S J, Puranik T G, Fischer O P, et al. A clustering-based quantitative analysis of the interdependent relationship between spatial and energy anomalies in ADS-B trajectory data[J]. Transportation Research Part C: Emerging Technologies, 2021, 131: 103331.

[7] Zhang J, Liu W, Zhu Y B. Study of ADS-B data evaluation[J]. Chinese Journal of Aeronautics, 2011, 24(4): 461-466.

[8] McCallie D, Butts J, Mills R. Security analysis of the ADS-B implementation in the next generation air transportation system[J]. International Journal of Critical Infrastructure Protection, 2011, 4(2): 78-87.

[9] Da Silva M, Puys M, Thevenon P H, et al. Automated ICS template for STRIDE microsoft threat modeling tool[C]//Proceedings of the 18th International Conference on Availability, Reliability and Security. New York: ACM, 2023: 1-7.

[10] Khan H A, Khan H, Ghafoor S, et al. A survey on security of automatic dependent surveillance-broadcast (ADS-B) protocol: challenges, potential solutions, and future directions[J]. IEEE Communications Surveys & Tutorials, 2025, 27(5): 3199-3226.

[11] Chiocchio S, Persia A, Santucci F, et al. Modeling and evaluation of enhanced reception techniques for ADS-B signals in high interference environments[J]. Physical Communication, 2020, 42: 101171.

[12] Zhang X L, Li J S. SR-GNN: spectral residuals with graph neural networks for anomaly detection in ADS-B data[C]//Proceedings of the International Conference on Frontiers in Cyber Security. Berlin: Springer, 2024: 503-516.

[13] Chevrot A, Vernotte A, Legeard B. CAE: contextual auto-encoder for multivariate time-series anomaly detection in air transportation[J]. Computers & Security, 2022, 116: 102652.

[14] Leonardi M, Sirbu G. ADS-B crowd-sensor network and two-step Kalman filter for GNSS and ADS-B cyber-attack detection[J]. Sensors, 2021, 21(15): 4992.

[15] Dong C, Zhang Y F, Jia Z Y, et al. Three-dimension collision-free trajectory planning of UAVs based on ADS-B information in low-altitude urban airspace[J]. Chinese Journal of Aeronautics, 2025, 38(2): 103170.

[16] Cretin A, Vernotte A, Chevrot A, et al. Test data generation for false data injection attack testing in air traffic surveillance[C]//Proceedings of the IEEE International Conference on Software Testing, Verification and Validation Workshops. Piscataway: IEEE Press, 2020: 143-152.

[17] Jheng S L, Jan S S, Chen Y H, et al. 1 090 MHz ADS-B-based wide area multilateration system for alternative positioning navigation and timing[J]. IEEE Sensors Journal, 2020, 20(16): 9490-9501.

[18] Wang J, Zou Y K, Ding J L. ADS-B spoofing attack detection method based on LSTM[J]. EURASIP Journal on Wireless Communications and Networking, 2020, 2020: 160.

[19] Leonardi M. ADS-B anomalies and intrusions detection by sensor clocks tracking[J]. IEEE Transactions on Aerospace and Electronic Systems, 2019, 55(5): 2370-2381.

[20] Jansen K, Niu L, Xue N, et al. Trust the crowd: wireless witnessing to detect attacks on ADS-B-based air-traffic surveillance[C]//Proceedings of the Network and Distributed System Security Symposium. [S.l.]: NDSS, 2021.

[21] 刘海涛, 刘家祥, 李冬霞, 等. 基于到达时间间隔差的 ADS-B 位

置消息验证方法[J]. 北京航空航天大学学报, 2024(9): 2696-2703.
Liu H T, Liu J X, Li D X, et al. Verification scheme of position message for automatic dependent surveillance-broadcast system based on interval difference of arrival[J]. Journal of Beijing University of Aeronautics and Astronautics, 2024(9): 2696-2703(in Chinese).

[22] Panda D K, Guo W S. Action robust reinforcement learning for air mobility deconfliction against conflict induced spoofing[J]. IEEE Transactions on Intelligent Transportation Systems, 2024, 25(12): 21343-21355.

[23] Wang E S, Song Y S, Xu S, et al. ADS-B anomaly data detection model based on deep learning and difference of Gaussian approach[J]. Transactions of Nanjing University of Aeronautics and Astronautics, 2020, 37(4): 550-561.

[24] Çevik N, Akleylek S. Anomaly detection system for ADS-B data: attack vectors and machine learning models[J]. Internet of Things, 2025, 29: 101416.

[25] Joseph N S, Banerjee C, Pasiliao E, et al. FlightSense: a spoofer detection and aircraft identification system using raw ADS-B data[C]// Proceedings of the IEEE International Conference on Big Data. Piscataway: IEEE Press, 2020: 3885-3894.

[26] Ying X H, Mazer J, Bernieri G, et al. Detecting ADS-B spoofing attacks using deep neural networks[C]//Proceedings of the IEEE Conference on Communications and Network Security. Piscataway: IEEE Press, 2019: 187-195.

[27] Strohmeier M, Schäfer M, Lenders V, et al. Realities and challenges of nextgen air traffic management: the case of ADS-B[J]. IEEE Communications Magazine, 2014, 52(5): 111-118.

[28] Fried A, Last M. Facing airborne attacks on ADS-B data with autoencoders[J]. Computers & Security, 2021, 109: 102405.

[29] Li T Y, Wang B H. Sequential collaborative detection strategy on ADS-B data attack[J]. International Journal of Critical Infrastructure Protection, 2019, 24: 78-99.

[30] Melvyn P, Couturier R, Ambert F, et al. Detecting ghost aircraft flooding in the surveillance of low-flying civil and military aircraft[C]//Proceedings of the 4th International Conference on Computer, Control and Robotics. Piscataway: IEEE Press, 2024: 328-332.

[31] Vajrobol V, Saxena G J, Singh S, et al. Enhancing aviation control security through ADS-B injection detection using ensemble meta-learning models with Explainable AI[J]. Alexandria Engineering Journal, 2025, 112: 63-73.

[32] Li T Y, Wang B H, Shang F T, et al. Dynamic temporal ADS-B data attack detection based on sHDP-HMM[J]. Computers & Security, 2020, 93: 101789.

[33] Jasra S K, Valentino G, Muscat A, et al. Hybrid machine learning-statistical method for anomaly detection in flight data[J]. Applied Sciences, 2022, 12(20): 10261.

[34] Li T Y, Wang B H, Shang F T, et al. Online sequential attack detection for ADS-B data based on hierarchical temporal memory[J]. Computers & Security, 2019, 87: 101599.

[35] Li T Y, Wang B H, Shang F T, et al. ADS-B data attack detection based on generative adversarial networks[C]//Proceedings of the 11th International Symposium on Cyberspace Safety and Security. Berlin: Springer, 2019: 323-336.

[36] Karam R, Salomon M, Couturier R. A comparative study of deep learning architectures for detection of anomalous ADS-B messages [C]//Proceedings of the 7th International Conference on Control, Decision and Information Technologies. Piscataway: IEEE Press, 2020: 241-246.

[37] Cao Y P, Cao J W, Zhou Z G, et al. Aircraft track anomaly detection based on MOD-Bi-LSTM[J]. Electronics, 2021, 10(9): 1007.

[38] Zha H R, Tian Q, Lin Y. Real-world ADS-B signal recognition based on radio frequency fingerprinting[C]//Proceedings of the IEEE 28th International Conference on Network Protocols. Piscataway: IEEE Press, 2020: 1-6.

[39] Zhang Z C, Li G Y, Shi J T, et al. Real-world aircraft recognition based on RF fingerprinting with few labeled ADS-B signals[J]. IEEE Transactions on Vehicular Technology, 2024, 73(2): 2866-2871.

[40] Zhong L F, Yang H, Zhang L, et al. Spoofing attack detection in ADS-B data through frequency enhanced patch attention mechanism[C]//Proceedings of the 6th International Conference on Electronic Engineering and Informatics. Piscataway: IEEE Press, 2024: 999-1003.

[41] Nicolussi A, Tanner S, Wattenhofer R. Aircraft fingerprinting using deep learning[C]//Proceedings of the 28th European Signal Processing Conference. Piscataway: IEEE Press, 2021: 740-744.

[42] Kacem T, Wijesekera D, Costa P. ADS-Bsec: a holistic framework to secure ADS-B[J]. IEEE Transactions on Intelligent Vehicles, 2018, 3(4): 511-521.

[43] Naganawa J, Tajima H, Miyazaki H, et al. ADS-B anti-spoofing performance of monopulse technique with sector antennas[C]//Proceedings of the IEEE Conference on Antenna Measurements & Applications. Piscataway: IEEE Press, 2017: 87-90.

[44] Shang F T, Wang B H, Yan F H, et al. Multidevice false data injection attack models of ADS-B multilateration systems[J/OL]. Security and Communication Networks, 2019. https://doi.org/10.1155/2019/8936784.

[45] Darabseh A, AlKhzaimi H, Pöpper C. MAVPro: ADS-B message verification for aviation security with minimal numbers of on-ground sensors[C]//Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks. New York: ACM, 2020: 53-64.

[46] Zhao D X, Sun J L, Gui G. En-route multilateration system based on ADS-B and TDOA/AOA for flight surveillance systems[C]// Proceedings of the IEEE 91st Vehicular Technology Conference. Piscataway: IEEE Press, 2020: 1-6.

[47] Chai Y E, Liu M Q, Zheng W X, et al. False signal identification of ADS-B assisted by UAV cooperative localization[J]. Chinese Journal of Aeronautics, 2025, 38(10): 103439.

[48] 王布宏, 罗鹏, 李腾耀, 等. 基于粒子群优化多核支持向量数据描述的广播式自动相关监视异常数据检测模型[J]. 电子与信息学报, 2020, 42(11): 2727-2734.
Wang B H, Luo P, Li T Y, et al. ADS-B anomalous data detection model based on PSO-MKSVDD[J]. Journal of Electronics & Information Technology, 2020, 42(11): 2727-2734(in Chinese).

[49] Lukeš P, Matejovie M. Detecting outlier positions in publicly available ADS-B data sets[C]//Proceedings of the New Trends in Civil Aviation. Piscataway: IEEE Press, 2024: 19-25.

[50] Li J H, Zhou Y Z. Automatic dependent surveillance-broadcast deceptive jamming detection method based on track data[J]. Journal of

Circuits, Systems and Computers, 2024, 33(12): 2450203.

[51] Khan H, Khan H, Ghafoor S. Securing ADS-B communications through a novel authentication framework[PP/OL]. TechRxiv (2023-08-29)[2025-08-01]. https://doi.org/10.36227/techrxiv.24043494.v1.

[52] Dabit A, Al-Fayoumi M, Mahmoud K. A secure regional authentication layer for global ADS-B communications[C]//Proceedings of the International Jordanian Cybersecurity Conference. Piscataway: IEEE Press, 2024: 99-104.

[53] Chen X, He D B, Peng C, et al. A secure and effective hierarchical identity-based signature scheme for ADS-B systems[J]. IEEE Transactions on Aerospace and Electronic Systems, 2024, 60(4): 5157-5168.

[54] Yao C, Zhang X J, Liu Y Z, et al. Blockchain-based secure and efficient ADS-B authentication via certificateless signature with packet loss tolerance[J]. IEEE Internet of Things Journal, 2025, 12(8): 10574-10588.

[55] Habler E, Shabtai A. Analyzing sequences of airspace states to detect anomalous traffic conditions[J]. IEEE Transactions on Aerospace and Electronic Systems, 2022, 58(3): 1843-1857.

[56] Ji Y F, Wang L W, Wu W L, et al. A method for LSTM-based trajectory modeling and abnormal trajectory detection[J]. IEEE Access, 2020, 8: 104063-104073.

[57] Yue M, Zheng H, Cui H R, et al. GAN-LSTM-based ADS-B attack detection in the context of air traffic control[J]. IEEE Internet of Things Journal, 2023, 10(14): 12651-12665.

[58] Cai K Q, Di Z, Zhu Y B, et al. An attention-based convolutional network framework for detection and localization of GNSS interference sources[J]. IEEE Transactions on Aerospace and Electronic Systems, 2024, 60(3): 2995-3011.

[59] Heiselberg P, Sørensen K A, Heiselberg H. Aircraft detection and state estimation[C]//Proceedings of the IEEE International Geoscience and Remote Sensing Symposium. Piscataway: IEEE Press, 2024: 7693-7696.

[60] Zheng Y F, Zhang X J, Tan Y H, et al. Transformer-based identification for ADS-B transmitters in open-time sets[J]. Chinese Journal of Aeronautics, 2025, 38(8): 103418.

[61] Li T T, Wen Z Y, Jin C D, et al. Meta-RFF: meta-task adaptive-based few-shot open-set incremental learning for RF fingerprint recognition[J]. IEEE Transactions on Cognitive Communications and Networking, 2026, 12: 2115-2130.

[62] Habler E, Shabtai A. Using LSTM encoder-decoder algorithm for detecting anomalous ADS-B messages[J]. Computers & Security, 2018, 78: 155-173.

[63] Luo P, Wang B H, Li T Y, et al. ADS-B anomaly data detection model based on VAE-SVDD[J]. Computers & Security, 2021, 104: 102213.

[64] 丁建立, 张琪琪, 王静, 等. 基于 Transformer-VAE 的 ADS-B 异常检测方法[J]. 系统工程与电子技术, 2023, 45(11): 3680-3689.
Ding J L, Zhang Q Q, Wang J, et al. ADS-B anomaly detection method based on Transformer-VAE[J]. Systems Engineering and Electronics, 2023, 45(11): 3680-3689(in Chinese).

[65] Luo P, Wang B H, Tian J W. TTSAD: TCN-Transformer-SVDD model for anomaly detection in air traffic ADS-B data[J]. Computers & Security, 2024, 141: 103840.

[66] Nasser H. Use of ADS-B for GNSS RFI monitoring[R]. [S.l.]: IDM, 2022.

[67] Liu J, Liu Y, Lin J Y, et al. Networking systems for video anomaly detection: a tutorial and survey[J]. ACM Computing Surveys, 2025, 57(10): 1-37.

[68] Luo P, Wang B H, Tian J W, et al. ADS-Bpois: poisoning attacks against deep-learning-based air traffic ADS-B unsupervised anomaly detection models[J]. IEEE Internet of Things Journal, 2024, 11(23): 38301-38311.

[69] Shang F T, Wang B H, Li T Y, et al. Adversarial examples on deep-learning-based ADS-B spoofing detection[J]. IEEE Wireless Communications Letters, 2020, 9(10): 1734-1737.

[70] Wang C, Wang Z D, Dong H L, et al. Fusionformer: a novel adversarial Transformer utilizing fusion attention for multivariate anomaly detection[J]. IEEE Transactions on Neural Networks and Learning Systems, 2025, 36(8): 14479-14492.

[71] Entezami A, Sarmadi H, Behkamal B, et al. Early warning of structural damage via manifold learning-aided data clustering and non-parametric probabilistic anomaly detection[J]. Mechanical Systems and Signal Processing, 2025, 224: 111984.

[72] Zhang H, Wang Z, Zeng D, et al. DiffusionAD: norm-guided one-step denoising diffusion for anomaly detection[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2025, 47(8): 7140-7152.

[73] Lin Y X, Chang Y, Tong X, et al. A survey on RGB, 3D, and multimodal approaches for unsupervised industrial image anomaly detection[J]. Information Fusion, 2025, 121: 103139.

[74] 王布宏, 罗鹏, 阳勇, 等. 空中交通管理系统网络安全研究综述与展望[J]. 电子与信息学报, 2025, 47(5): 1230-1265.
Wang B H, Luo P, Yang Y, et al. A review and prospect of cybersecurity research on air traffic management systems[J]. Journal of Electronics & Information Technology, 2025, 47(5): 1230-1265(in Chinese).

[75] He H Y, Zhang J N, Chen H X, et al. A diffusion-based framework for multi-class anomaly detection[J]. Proceedings of the AAAI Conference on Artificial Intelligence, 2024, 38(8): 8472-8480.

[76] Liu Q H, Paparrizos J. The elephant in the room: towards a reliable time-series anomaly detection benchmark[C]//Proceedings of the 38th International Conference on Neural Information Processing Systems. New York: ACM, 2024: 108231-108261.

Review of ADS-B anomaly detection research

YANG Hongyu[1, 2, *], ZHAO Ziwen[1], ZHU Youwen[3], HU Huiling[4], HU Juncheng[5]

(1. School of Safety Science and Engineering, Civil Aviation University of China, Tianjin 300300, China;
2. School of Computer Science and Artificial Intelligence, Civil Aviation University of China, Tianjin 300300, China;
3. College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 211106, China;
4. Air Traffic Management Department, Central South Air Traffic Management Bureau CAAC, Guangzhou 510440, China;
5. College of Computer Science and Technology, Jilin University, Changchun 130012, China)

Abstract: The automatic dependent surveillance broadcast (ADS-B) system, as an important component of aviation surveillance technology, has been widely deployed and applied. The application of the ADS-B system significantly improves the coverage and positioning accuracy of air traffic surveillance. Nonetheless, owing to its open broadcast communication framework, this system is susceptible to numerous security risks including data manipulation, harmful message insertion, and interference assaults, which significantly compromise air traffic safety and control determinations. Anomaly detection for the ADS-B system has gradually become a research hotspot. This paper systematically summarizes and analyzes the current research status of anomaly detection in ADS-B systems at home and abroad. Firstly, it analyzes the causes of abnormal data in ADS-B systems and summarizes the types of attacks that this system is vulnerable to and their impacts. The present state of research on ADS-B anomaly detection is thoroughly examined from two perspectives: the consistency check-based approach and the deep learning-based approach. The merits and demerits of several techniques regarding detection precision, generalisation, and practical implementation are examined, with an analysis and summary of existing ADS-B anomaly detection products in relation to their respective application contexts. Ultimately, a comprehensive synthesis of the current research findings reveals the primary obstacles encountered by contemporary anomaly detection techniques for ADS-B, alongside potential future research avenues and developmental trajectories.

Keywords: automatic dependent surveillance broadcast; anomaly detection; air traffic surveillance; consistency check; deep learning

Received: 2025-08-26; **Accepted**: 2025-11-07; **Published Online**: 2025-11-20 12:16

URL: link.cnki.net/urlid/11.2625.V.20251119.1820.004

Foundation item: Key Project of the Civil Aviation Joint Research Fund of the National Natural Science Foundation of China (U2433205)

* **Corresponding author**. E-mail: yhyxlx@hotmail.com