

ADS-B 安全研究综述

谢丽霞¹, 宁亚洲², 杨宏宇^{1,2}, 朱友文³, 胡慧玲⁴, 成翔⁵

(1. 中国民航大学计算机科学与技术学院, 天津 300300;

2. 中国民航大学安全科学与工程学院, 天津 300300;

3. 南京航空航天大学计算机科学与技术学院, 江苏 南京 211106;

4. 民航中南地区空中交通管理局空管部, 广东 广州 510440;

5. 扬州大学信息工程学院, 江苏 扬州 225127)

摘要: 广播式自动相关监视 (automatic dependent surveillance-broadcast, ADS-B) 技术作为提升空中交通管理效率和安全性的关键技术, 已在全球广泛应用。民用航空器通过 ADS-B 自主广播其位置和动态信息, 为空中交通管制提供高效、实时的监视手段。然而, 由于 ADS-B 协议的公开性和采用的无线信道广播方式的明文消息发送模式, ADS-B 消息在传输过程中容易遭到诸如消息篡改和伪造等攻击。鉴于此, 调研和分析 ADS-B 所面临的安全挑战和安全问题, 总结、评估现有研究和解决方案, 并对其优势与不足进行分析。最后, 探讨了解决 ADS-B 安全问题的未来研究方向, 以期为 ADS-B 的安全性提升提供理论支持和技术参考, 促进航空通信安全的发展。

关键词: 广播式自动相关监视; 消息篡改; 异常检测; 位置验证; 区块链技术

中图分类号: TP309

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2025051

Review of ADS-B security research

XIE Lixia¹, NING Yazhou², YANG Hongyu^{1,2}, ZHU Youwen³, HU Huiling⁴, CHENG Xiang⁵

1. School of Computer Science and Technology, Civil Aviation University of China, Tianjin 300300, China

2. School of Safety Science and Engineering, 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 and Southern Regional Air Traffic Management

Bureau of CAAC, Guangzhou 510440, China

5. School of Information Engineering, Yangzhou University, Yangzhou 225127, China

Abstract: Automatic dependent surveillance-broadcast (ADS-B) technology, as a key technology for improving the efficiency and safety of air traffic management, has been widely adopted globally. ADS-B was utilized by civil aircraft to autonomously broadcast their position and dynamic information, providing an efficient and real-time surveillance method for air traffic control. Due to the openness of the ADS-B protocol and the use of plaintext mes-

收稿日期: 2025-02-06; 修回日期: 2025-05-11

通信作者: 杨宏宇, hyyang@cauc.edu.cn

基金项目: 国家自然科学基金民航联合研究基金重点项目 (U2433205)

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

引用格式: 谢丽霞, 宁亚洲, 杨宏宇, 等. ADS-B 安全研究综述[J]. 网络与信息安全学报, 2025, 11(5): 31-49.

Citation Format: XIE L X, NING Y Z, YANG H Y, et al. Review of ADS-B security research[J]. Chinese Journal of Network and Information Security, 2025, 11(5): 31-49.

sage transmission over wireless broadcast channels, ADS-B messages were recognized as vulnerable to attacks such as message tampering and spoofing during transmission. The security challenges and issues confronted by ADS-B were thoroughly investigated and analyzed. Existing research and solutions were systematically reviewed and assessed, with their respective advantages and disadvantages analyzed. Finally, future research directions for addressing the security issues of ADS-B were explored. These research directions are expected to provide theoretical support and technical references for enhancing the security of ADS-B, thereby promoting the development of aviation communication security.

Keywords: automatic dependent surveillance-broadcast, message tampering, anomaly detection, location verification, blockchain technology

0 引言

全球航空运输业的迅速发展导致空中交通量激增,为航空交通管制系统带来巨大挑战。作为国际民航组织(international civil aviation organization, ICAO)推荐的下一代空中交通管理方法,广播式自动相关监视(automatic dependent surveillance-broadcast, ADS-B)技术以其高效、高精度和低成本的特点备受青睐^[1]。ADS-B通过飞机自主广播其位置、速度和航向等信息,不仅提升了航空交通安全,还优化了空域利用,减少了飞行延误,从而显著提高了整体运营效率。这一技术的广泛应用标志着航空监控和管理进入了新时代。

ADS-B系统采用未加密的无线信道广播数据,这种开放性使其容易遭受窃听攻击。随着软件解码工具的普及和使用门槛的降低,许多地区对ADS-B信号使用监管不严,窃听风险增大,窃听成本进一步降低。欧美已发生多起ADS-B泄露飞机行踪事件^[2-6],凸显了这一问题的严重性。更值得警惕的是,自2020年以来,中国国家安全机关发现某些境外机构通过提供数据接收设备和共享信息等方式,诱导航空爱好者收集敏感数据并传输至境外^[7]。这些事件引发了公众对ADS-B安全问题的广泛关注,突出了加强ADS-B系统安全防护的紧迫性。

在ADS-B发展的进程中,已有多篇文献对该领域的研究进行了总结分析,文献[8-11]指出其存在安全设计缺陷和易受网络信息安全攻击的脆弱性。这些研究主要探讨了安全广播认证和位置验证等应对措施,并提出了安全改进方案和未来研究方向。然而,现有综述文献仅是探讨了已有的安全方案,对不同安全方案的适用场景等实际问题的探讨不够深入,并且缺乏对新兴技术

(如区块链和人工智能)在ADS-B安全中的应用探讨,对未来研究方向和发展趋势的总结不够全面,缺乏与相似领域如车联网等的类比。鉴于近年来出现的众多新研究成果和应用案例,有必要对ADS-B安全问题进行全面而深入的重新审视。

本文通过系统分析现有文献,深入剖析了ADS-B面临的安全挑战,聚焦于消息注入、篡改和干扰等典型攻击的危害。在此基础上,全面总结了ADS-B安全研究的主要方向,并客观评估了现有解决方案的局限性,如在应对高复杂度攻击场景时的完整性保障不足。本文的贡献在于:首先,提供了一个涵盖最新研究成果的全面综述;其次,从密码学、区块链、异常检测、位置验证和抗干扰技术等多个维度进行了深入分析;最后,结合人工智能和区块链等前沿技术,提出了具有前瞻性的研究方向。这些方向包括基于人工智能和机器学习的攻击检测机制、区块链驱动的数据安全优化方案、新型抗干扰通信策略以及车联网安全技术的潜在应用。

1 ADS-B概述

1.1 ADS-B工作原理

ADS-B是一种革新性的航空监视技术,利用全球导航卫星系统(global navigation satellite system, GNSS)和先进的机载设备,实现飞机位置、高度、速度和航向等关键信息的实时广播。与传统的雷达监视系统相比,ADS-B具有更高精度、更广覆盖范围和更低运营成本。ADS-B系统主要由3个核心组件构成:飞机端设备、地面接收站和空中交通管制中心。飞机通过机载设备获取GNSS信息并广播ADS-B数据,地面接收站接收

这些信息并传输至空管中心,用于实时动态监视和空中交通管理。ADS-B系统结构如图1所示。

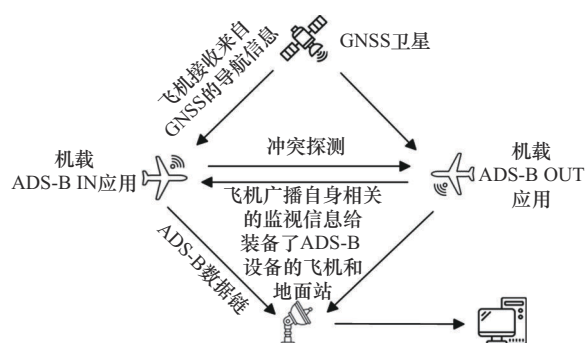


图1 ADS-B系统结构

Figure 1 Structure of ADS-B system

ADS-B主要采用3种数据链标准:1 090ES (1 090 MHz extended squitter)、UAT (universal access transceiver) 和 VDL (VHF data link) Mode 4。1 090 ES^[12]工作在1 090 MHz频段,是国际民航组织推荐的全球标准,能够广播包含飞机标识、位置、高度等详细信息的超长消息。UAT^[13]专为美国空域设计,工作在978 MHz频段,其以较低的数据速率和成本效益适用于高密度空域。VDL Mode 4^[14]基于VHF频段,支持双向通信,不仅能够广播飞机信息,还能接收空管指令和其他飞机数据。1 090ES因其技术成熟、信息更新率快、数据传输带宽高以及在监视和防撞技术方面的优势,应用最为广泛。本文主要针对1 090ES模式的ADS-B安全问题展开讨论。

标准的1 090ES模式的ADS-B消息采用112位的扩展暴露模式,包含8位下行格式标识符、24位ICAO航空器地址、56位消息数据字段和24位奇偶校验。1 090ES ADS-B信息格式如表1所示。

表1 1 090ES ADS-B的信息格式
Table 1 Information format of 1090ES ADS-B

名称	比特位置
控制位	1-8
ICAO地址	9-32
ADS-B信息域	33-88
奇偶校验位	89-112

1.2 ADS-B与传统监视系统的关系

传统雷达监视系统^[15]主要分为初级监视雷

达和二次监视雷达。初级监视雷达基于反射技术,不依赖飞机协作,主要用于军事区域和偏远地区,精度和覆盖范围有限。二次监视雷达依靠飞机应答机,对地面站询问进行回应,提供高度、识别码等信息。模式S在二次监视雷达基础上引入选择性询问,提高了数据传输效率,为ADS-B的应用奠定了基础。尽管二次监视雷达提升了信息传输效率,但在高密度空域和实时性方面仍有不足,促使更先进监视技术的出现。

相较于传统雷达,ADS-B具有显著优势。它结合GNSS和地面站,减少了对昂贵雷达基础设施的依赖,大幅降低了成本。ADS-B能实时广播飞机位置、速度等关键信息,确保数据时效性和准确性^[16]。借助GNSS高精度定位,ADS-B在复杂或高密度空域中表现更佳。这些优势使ADS-B逐渐成为空中交通监视和管理的主要手段之一。

1.3 ADS-B与其他监视方案的对比

除ADS-B和雷达监视方案,其他飞行监视方案如远程标识(remote identification, Remote ID)和多边定位(multilateration, MLAT)技术也在航空安全和空域管理中发挥着重要作用。

Remote ID技术^[17]专门针对无人机操作,其目标是为所有在空中飞行的无人机提供身份认定及实时位置信息。这一技术确保无人机在较高密度空域的可追溯性,大幅提高了低空飞行的安全性。Remote ID通过无线通信实现数据的传输,尽管它的传输范围通常较短,但其低功耗和实现便利性使得它特别适合无人飞行器的监管。相比ADS-B面向载人航空器的广泛应用,Remote ID更加关注于确保飞行无人机的安全与合规,其技术标准和执行方式均为无人机设计。

MLAT^[18]同样是在航空器监视领域的有效补充。MLAT能够通过多个地面接收站接收到的航空器发送的信号时间差来推算位置,适合机场及高流量区域的监视。与ADS-B相比,MLAT在使用过程中通常不依赖航空器主动广播,其无线电接收器的分布性使得该技术可以覆盖ADS-B信号的盲区,增强了航空器的监控能力。

值得注意的是,车联网^[19]作为无线通信技术,与ADS-B存在显著差异。尽管两者都属于交通领域的无线通信系统,但ADS-B通信距离

通常达数百千米,而车联网一般限于数百米;ADS-B 面向高速航空器(800~1 000 km/h),而车辆速度相对较低;ADS-B 还面临更严格的安全容错要求与三维空间的定位挑战。此外,ADS-B 系统的更新周期长达数十年,而车联网设备通常在 5~10 年。尽管车联网安全研究相对成熟并有较多标准化方案,但其技术解决方案难以直接迁移至 ADS-B 环境,需要针对航空特性进行重大调整。

通过比较这些技术可以看出,ADS-B 由于其覆盖广、精度高和实时性的优点,逐渐成为空中交通管理中的主要选择,Remote ID 进一步拓展了无人机监管领域,MLAT 则主要用于结合多种技术形成综合监视网络,以提升整个空域的安全性与运行效率。而车联网则专注于地面车辆通信的不同应用场景。随着各类监视与通信技术的进步与标准化,这些方案之间的优势互补与技术融合将在未来的交通安全管理中发挥更大作用。

ADS-B 的推行已在全球范围内逐步展开,成为新一代空中交通管理系统(如美国的 NextGen 项目和欧洲的同类项目)的一部分。ICAO 及地区性航空监管机构积极推动其在航班的配备和地面基础设施的部署。世界主要航空大国已逐步推行对新飞机安装 ADS-B 的强制性要求。在地面基础设施上,多个国家开发了广域多点定位系统^[20],以支持 ADS-B 数据的接收和处理,一些国家还引入了基于卫星的 ADS-B^[21],以提升全球覆盖和可靠性。

2 ADS-B 安全问题与挑战分析

ADS-B 系统在设计之初采用开放广播形式传播数据信息,缺乏加密认证措施,这使得其成为恶意攻击者的潜在目标。随着航空技术的快速发展和空中交通环境的日益复杂,ADS-B 系统面临着多方面的安全挑战。

窃听攻击^[22]是 ADS-B 系统面临的最基本且最容易实施的攻击形式。随着软件无线电技术的发展和普及,窃听攻击的技术门槛不断降低。攻击者无须物理接触,只需具备接收设备,就可以轻易获取范围内的 ADS-B 信号,并通过解调获得飞行器的位置信息、高度以及身份数据。尽管窃听攻击不会直接影响 ADS-B 系统的正常运行,

但其潜在危害不容忽视。首先,隐私泄露问题^[23],通过长期监听特定航班的 ADS-B 数据,可能会泄露个人或组织的行程信息。其次,敌对方可能利用 ADS-B 数据分析军事飞行活动模式,进行情报收集。更为严重的是,窃听获取的数据可能被用于设计更复杂的攻击方案,为其他类型的攻击提供信息支持。

窃听攻击的防御需要在保证系统兼容性和运行效率的同时实现数据加密。现代加密技术已经在多种无线通信场景(如 4G/5G 网络、车联网等)中成功应用,证明了高效加密在实时通信中的可行性。ADS-B 系统虽然与这些技术领域有相似之处,但其特殊性带来了独特的挑战。

ADS-B 系统要求每 0.5 s 广播一次位置信息,这种高频率的实时通信对加密处理的时间效率提出了严格要求。Jamal 等^[24]通过实际测试验证了格式保存加密在 ADS-B 环境中的应用可行性,也指出了参数选择和实现优化对维持系统性能的重要性。尽管现代加密算法在计算性能上已有显著提升,但在资源有限的航空设备上实现强安全性与高效率的平衡仍然是一个技术难点。

密钥管理的复杂性是 ADS-B 系统面临的另一个显著挑战。ADS-B 作为全球航空系统的核心组件,需要在不同国家、地区和航空公司之间保持一致的安全标准和互操作性。Back 等^[25]的研究表明,传统的密钥管理方案在全球范围内应用时存在效率和兼容性问题。尽管近年来基于身份的加密和区块链等技术为解决全球密钥管理提供了创新思路,但跨国界、跨组织的协调和标准化仍然是实际部署中的主要障碍。

欺骗攻击^[26]是对 ADS-B 系统构成重大威胁的攻击方式之一。在这种攻击中,攻击者通过伪造 ADS-B 信号,制造虚假的飞行器或错误的位置信息,从而误导空中交通管制系统。欺骗攻击技术难度高,要求攻击者精通 ADS-B 协议并具备复杂的信号处理能力。实施此类攻击通常需要使用软件定义无线电设备来生成和发射伪造的 ADS-B 信号。这些伪造信号在格式和内容上需要与真实的 ADS-B 消息完全一致,以避免被系统识别为异常。

欺骗攻击的危害是多方面的。它可能导致航班安全间隔减小,增加空中碰撞的风险。例如,攻击者可以伪造一个虚假的飞行器,使其与真实飞机的航线相交,这可能导致空中交通管制系统发出不必要的警报或指令,干扰正常的航空操作。此外,欺骗攻击可能造成空域管理的混乱。通过注入大量虚假的飞行器信息,攻击者可以使空中交通管制系统的监控画面变得杂乱,增加管制人员的工作负担,影响决策效率。

防御欺骗攻击的关键在于开发有效的数据完整性验证机制,以确保数据来源的真实性。这包括开发能够识别伪造信号特征的算法,如信号强度异常、到达时间不一致等;将 ADS-B 数据与其他独立的监视系统(如雷达)数据进行交叉验证,提高检测欺骗信号的准确性;在不显著增加系统时延的前提下,实现高效的认证方案;设计能够根据当前威胁态势动态调整的安全策略,提高系统的适应性。

信号干扰攻击^[27]是另一种严重威胁 ADS-B 系统正常运行的攻击方式。这种攻击通过发射与 ADS-B 系统相同频率的强干扰信号,破坏其通信能力。具体而言,攻击者利用高功率干扰设备在 ADS-B 使用的 1 090 MHz 频段发送干扰信号,覆盖或淹没合法的 ADS-B 信号。信号干扰攻击的技术实现相对简单,但其影响却非常广泛和严重。

信号干扰攻击可以采取多种形式,包括噪声干扰、智能干扰和选择性干扰^[28]。这类攻击会导致接收端无法正确解码 ADS-B 消息,造成飞机之间以及飞机与地面控制之间的通信中断。其后果包括位置信息丢失、安全间隔判断错误、决策时延,以及系统可靠性的整体降低。这些问题直接威胁到航空安全和空中交通管理的效率。

应对信号干扰攻击需要发展更强的抗干扰技术和信号监测机制,这涉及复杂的信号处理算法和硬件设计,是一个跨学科的技术挑战。主要研究方向包括开发自适应滤波技术、利用空间分集接收提高抗干扰能力、探索跳频技术的可能性、开发快速准确的干扰源定位技术,以及利用多个接收站的数据进行协作式干扰检测。这些技术的发展不仅需要在算法层面进行创新,还需要考虑

如何在现有 ADS-B 系统架构下实现,以确保与现有设备的兼容性。

消息注入攻击^[29]是 ADS-B 面临的另一个严重威胁,其特点是攻击者通过向系统注入伪造的消息来达到干扰或误导的目的。与欺骗攻击相比,消息注入攻击更加灵活和多样化,可以针对 ADS-B 系统的不同方面进行攻击。攻击者可能创建不存在的“幽灵飞机”,发送飞机处于紧急状态的虚假消息,伪装成合法的地面站发送错误指令,或者捕获并重新播放之前的有效 ADS-B 消息。

这些攻击可能导致空中交通管制系统过载、决策错误、资源浪费,以及对系统可靠性的信任度降低。防御消息注入攻击面临的主要挑战是确保对注入消息的判断在不同节点间保持一致。研究方向主要集中在利用机器学习算法建立正常通信模式的模型,通过历史数据分析快速验证新收到消息的合理性,结合物理层信号特征和数据链路层内容进行综合分析,设计能在分布式环境中快速达成一致的算法,以及建立对消息源的动态信任机制。

消息篡改攻击^[30]是一种更为隐蔽且技术要求更高的攻击形式。不同于完全伪造新的消息,消息篡改攻击是在拦截合法 ADS-B 消息的基础上,对其内容进行部分修改后再转发。这种攻击的特点是保留了大部分原始消息的特征,使得篡改后的消息更难被检测。实施这种攻击面临的技术难点包括满足极高的实时性要求、保持信号同步、正确更新误码校正码,以及精确控制重新发送的消息功率。

消息篡改攻击可能导致位置信息错误、高度信息误判、身份信息混淆,以及速度数据不准确等问题,这些问题都可能对空中交通管理造成严重影响。应对消息篡改攻击的技术挑战主要包括如何在显著增加消息长度和处理时延的情况下,为 ADS-B 消息添加有效的完整性保护机制,设计能够快速验证消息完整性的算法,开发适用于带宽受限的 ADS-B 系统的轻量级消息认证码或数字签名方案,以及建立基于历史数据和物理模型的异常检测机制。

ADS-B 的不同攻击类型具有各自的技术复杂

性和潜在影响,表2给出了ADS-B攻击类型及特点。为应对这些挑战,未来的研究方向包括利用人工智能和机器学习技术开发自适应异常检测算法、探索无密钥抗干扰机制和分布式节点协作通信策略、优化区块链技术在ADS-B中的应用以及借鉴车联网安全技术,针对ADS-B系统特性进行适应性调整。这些研究不仅需要在理论层面进行突破,还需要考虑如何在实际的ADS-B系统中进行部署和应用,以确保系统的安全性和可靠性。

表2 ADS-B攻击类型及特点
Table 2 Types and characteristics of ADS-B attacks

攻击	技术复杂性	实施成本	潜在影响
窃听攻击	低	低	数据泄露,隐私暴露
欺骗攻击	中	中	制造虚假信息,误导空中管理
信号干扰攻击	高	高	通信中断,增加安全风险
消息注入攻击	高	中	干扰空域秩序,导致航班调整
消息篡改攻击	极高	高	数据不一致,影响航空决策性

理解这些攻击的多样性及其可能产生的影响,是研究ADS-B安全防御措施的关键步骤^[31],ADS-B系统面临的安全挑战是多方面的^[32],涉及信息保密、数据完整性、通信可靠性等。应对这些挑战需要从系统架构、协议设计、信号处理、密码学等多个学科角度进行深入研究。

3 ADS-B安全应对方案分析

针对第2节中分析的ADS-B系统面临的5类主要攻击,研究者提出了多种安全应对方案。这

些方案可从技术实现角度分为5类:基于密码学的通信安全主要用于防范窃听和消息篡改;区块链技术重点解决数据完整性问题,有效应对消息篡改和伪造;异常检测技术可识别各类攻击行为,特别适用于欺骗和消息注入攻击的识别;位置验证技术专门针对位置欺骗问题设计;抗干扰技术则直接应对干扰攻击。本节将对这些研究成果进行系统分析。表3总结了各类安全应对方案与安全威胁的对应关系。

3.1 基于密码学的ADS-B的通信安全

随着民用航空交通量的不断增加,ADS-B系统作为新一代空中交通监视技术,其通信安全问题日益凸显。密码学技术通过算法和协议的实现,为ADS-B系统构建了多层次的安全防护体系。

根据应用目标的不同,基于密码学的ADS-B的通信安全可分为两类:一类是基于加密的ADS-B安全通信方案,主要关注数据保密性,防止未授权方截获敏感信息;另一类是基于身份验证的ADS-B安全通信方案,着重确保数据完整性和真实性,验证消息发送方的身份以及消息在传输过程中是否被篡改。基于密码学的ADS-B安全通信方案总结见表4。

3.1.1 基于加密的ADS-B安全通信方案

在ADS-B安全研究中,加密方案主要围绕两个核心技术挑战展开:如何在资源受限环境中实现高效加密,以及如何保持与现有系统的兼容性。

针对资源限制挑战,研究者提出了多种计算高效加密方案,从不同角度优化了ADS-B环境中的加密性能。Yang等^[33]采用了算法优化路径,结合时间有效流容错认证协议和格式保存加密技

表3 ADS-B安全应对方案与安全威胁的对应关系

Table 3 Correspondence between ADS-B security solutions and security threats

安全应对方案	窃听攻击	欺骗攻击	信号干扰攻击	消息注入攻击	消息篡改攻击
基于密码学的ADS-B的通信安全	★★★	★★	○	★★	★★★
基于区块链的ADS-B的数据保护	★	★★	○	★★	★★★
ADS-B的数据异常检测	○	★★★	★	★★★	★★
ADS-B的位置验证技术	○	★★★	○	★★	★
ADS-B信号抗干扰技术	○	○	★★★	★	○

注:★★★表示高效应对,★★表示有效应对,★表示部分应对,○表示几乎不应对。

表4 基于密码学的ADS-B安全通信方案总结

Table 4 Summary of cryptography-based secure communication schemes for ADS-B

方案	优点	不足	适用场景
计算高效加密 ^[25, 33-34]	低计算和带宽需求, 适合资源受限环境	加密强度受限制, 无法处理复杂攻击	通用的低资源ADS-B环境
格式保存加密 ^[24, 35]	保留数据格式, 兼容性好	加密和解密过程耗时较长	数据完整性要求高的场景
基于身份的签名 ^[36-38]	减少公钥管理复杂性, 提高签名效率	对高复杂度攻击场景的完整性保障不足	消息频繁的空通通信
批量验证技术 ^[39-42]	提升大规模数据验证效率, 适应实时空中交通管理需求	对低功耗设备的适应性较差, 难以部署	高密度交通环境

术, 在确保安全性的同时实现了与现有 ADS-B 基础设施的兼容性。An 等^[34]选择了加密原语优化路径, 通过隐式证书和椭圆曲线签密技术提出整体空中保护方案, 在相同安全强度下实现了更高效的认证过程。Back 等^[25]从密钥管理角度入手, 提出了分阶段基于身份的加密模型, 将密钥管理与加密过程分离, 有效应对了 ADS-B 环境中每 0.5 s 一次的高频数据传输挑战。这 3 种方案虽然技术路径不同, 但都致力于解决资源受限环境中的加密效率问题, 展示了计算高效加密的多元化发展方向。

在 ADS-B 环境中, 计算高效加密是指针对航空环境特定资源约束 (如有限计算能力、带宽和实时性要求) 进行优化的加密技术, 在文献^[33]中, 这种方案也被描述为轻量级, 即通过特定的算法优化和实现技术降低了计算复杂度。计算高效并非表示绝对的低计算复杂度, 而是在保证安全性的前提下, 针对 ADS-B 特定应用场景 (如每 0.5 s 的广播频率、多方通信、动态网络拓扑等) 所做的性能优化。这些方案通常在计算效率、通信开销和安全强度之间寻求平衡, 以适应航空电子设备的资源约束。

与计算效率导向的方案并行发展的是格式保存加密技术, 该技术注重保持数据格式不变以实现系统兼容性。Burfeind 等^[35]使用单向非对称加密的格式保存加密, 兼容现有系统, 避免影响不需要加密功能的用户。随着技术的成熟, Jamal 等^[24]在 2023 年的研究中将格式保存加密技术推向了新高度, 采用基于 Feistel 网络的加密方法, 不仅确保了与 ADS-B 协议的兼容性, 还结合区块链技术解决了密钥管理问题, 展示了从单一技术向混合方案发展的趋势。

加密方案在提升数据传输安全性方面表现优异, 但分布式环境中的密钥分发和撤销仍是重要挑战。为此研究者提出了身份验证方案, 通过减少对加密强度的依赖, 降低系统资源消耗, 并优化对消息真实性的保障。

3.1.2 基于身份验证的 ADS-B 安全通信方案

身份验证技术为 ADS-B 系统提供了防范伪造和欺骗攻击的能力, 其研究围绕两个主要目标展开: 简化密钥管理和提高验证效率。

在简化密钥管理方面, 基于身份的签名技术提供了有效解决方案。Back 等^[36]提出的在线/离线签名框架从计算负荷分配角度解决了实时性问题, 通过将复杂计算预先在离线阶段完成, 大幅降低了在线阶段的计算需求。Yang 等^[37]从通信效率角度入手, 设计了基于身份的消息恢复签名方法, 通过从签名中直接恢复消息内容减少了通信开销。Wu 等^[38]进一步综合了前两者的优势, 提出无证书短签名方法, 不仅避免了证书管理的复杂性, 还减少了签名长度, 同时保持了高验证效率。这 3 种方案展示了从单一优化目标向综合效率改进的技术演进过程。

在提高验证效率方面, 批量验证技术针对高密度通信场景提供了解决方案。Yang 等^[39]首先探索了 3 级分层签名结构支持批量验证的可能性, 为高密度空中交通环境提供了基础架构。Asari 等^[40]在此基础上引入了无证书认证概念, 解决了传统方案中的密钥托管问题, 增强了系统安全性。Yi 等^[41]和 Chen 等^[42]从性能优化角度进一步研究了分层验证技术, 使得验证 50 条消息的时间比单独验证减少了 84%, 实现了从基础安全保障到大规模高效验证的技术跨越。

这些身份验证方法虽然有效降低了资源开销,但在面对复杂攻击场景时的防御能力有限,推动了混合技术方案的发展。

3.1.3 基于混合技术的 ADS-B 安全通信方案

随着 ADS-B 安全需求的复杂化,研究者意识到单一技术难以同时满足保密性、完整性、效率和兼容性等要求,开始探索融合多种技术优势的混合方案。

Jamal 等^[24]的研究代表了加密与新兴技术融合的发展方向,通过结合格式保存加密与区块链技术,不仅解决了数据保密性问题,还通过区块链的分布式特性克服了集中式密钥管理的局限性。Wu 等^[38]展示了身份验证技术的综合优化路径,通过融合无证书技术与短签名方法,在避免证书管理复杂性的同时实现了高效签名生成和验证。

这些混合技术方案不再局限于解决单一安全问题,而是采用系统思维同时应对多重安全挑战,标志着 ADS-B 安全研究从单点突破走向系统整合的重要转变。混合技术方案虽然综合性能优异,但面临集成复杂度高和部署成本大的挑战,其实际应用仍需进一步探索和验证。这也反映出 ADS-B 安全研究仍处于发展阶段,特别是在资源受限、动态威胁环境下,仍需寻找更优的平衡点。

基于密码学的 ADS-B 安全方案在提升数据机密性、完整性和真实性方面取得了显著成效,但在实际应用中仍面临一些局限性。加密方案在资源利用与安全性之间存在权衡,公钥基础设施的复杂性仍是一大挑战;身份验证方法虽然简化

了密钥管理,但对高复杂度攻击场景的防御能力有限;混合技术方案性能优异但部署成本较高,普及性不足。这些局限性在特定场景中限制了方案的适用性,尤其是在资源受限、动态威胁环境下,需要进一步优化。

3.2 基于区块链的 ADS-B 的数据保护

密码学技术为 ADS-B 数据提供了机密性和完整性的保障,但其独立使用时难以适应复杂的分布式场景和动态攻击,区块链技术的引入为进一步提升安全性提供了可能。近年来,区块链技术因其去中心化和数据不可篡改的特性,受到了越来越多的关注,尤其是在航空安全领域,通过利用区块链技术,可以极大程度提高 ADS-B 数据的可信度和安全性,防止伪造和篡改,基于区块链的 ADS-B 的数据保护方案总结见表 5。

为了减轻消息欺骗和异常流量数据造成的 ADS-B 安全问题,Damis 等^[43]提出了一种微服务框架来用于 ADS-B 数据验证的区块链实现,使来自第三方接收器的数据源能够得到处理,并与空管地面站接收器的数据源相关联。该框架可以通过第三方支持来减少空中交通管制基础设施的成本。

仅关注与第三方数据源的整合,在处理更多数据源时可能存在局限性,为此 Wu 等^[44]提出将每一条 ADS-B 消息记录到区块链中,所有数据传输都可以进行透明且可验证的追踪,确保每一条消息的来源和内容都是可信的,即使在存在恶意攻击者的情况下,信息也无法被篡改。这一方法在已有基础上提升了对数据的保护层级。

表 5 基于区块链的 ADS-B 的数据保护方案总结

Table 5 Summary of blockchain-based ADS-B data protection schemes

方案	优点	不足	适用场景
微服务架构中的数据 来源验证 ^[43]	通过区块链集成来自第三方接收器的数据源,降低空中交通管制系统的运营成本和安全风险	面临实时性和扩展性挑战	适用于需要整合多数据源的航空系统
ADS-B 消息透明可验证 传输 ^[44]	每条信息均录入区块链,确保数据透明和无法篡改,提高信息传输安全性	时延和性能可能对实时应用造成影响	注重信息透明性和安全性的通信场景
使用防篡改公共分类 账的路径验证 ^[45]	提供基于区块链的防篡改分布式公共分类账,有效提升飞行数据真实性	实施成本较高,技术复杂性较大	要求高数据真实性和篡改防护的航空应用
空中交通管理的未来 安全架构 ^[46]	综合可信认证、数据共享和访问控制,提高空中交通管理安全	架构复杂,实施挑战大	适用于未来面向的综合航空管理系统

文献[43-44]在防范数据篡改方面取得了一定成效,但仍存在局限性。Swathi等^[45]通过防篡改的分布式公共分类账来解决此问题,介绍了使用防篡改的已认证飞行计划的分布式公共分类账来保护ADS-B数据,根据区块链分类账中存储的飞行路径/路线来验证相关飞机标识符的位置和其他参数。

Lu等^[46]从一个更为宏观的视角出发,设计了一种基于区块链技术的未来空中交通管理安全架构。其核心在于集成可信认证、数据共享和访问控制模块。该方案不仅关注数据自身的安全性,还试图通过系统性的设计促进空中交通管理的信息安全和技术创新,弥补了其他研究对空管流程整体保护的欠缺。

通过合并已有文献的不同方法,形成综合解决方案可以提升系统效能。例如,将Lu等^[46]的架构设计与Wu等^[44]的透明可验证方案结合,能够更好地解决现有方案无法有效应对的单点故障和高成本问题。Lu等^[46]的架构通过分布式节点配置提高了系统的容错能力,而Wu等^[44]的方案则通过引入透明的验证机制增强了数据的可信度。这两种方法的结合不仅提升了系统整体的可靠性,还降低了实施成本,为航空数据安全提供了一种更为经济且高效的保障机制。

基于区块链的方案在提升航空数据安全性方面展示了其潜力,但面临一定的挑战,区块链的性能和时延问题可能影响实时监控的需求,尤其是在处理大量数据时,要保证ADS-B系统的实时性还需要进一步的研究。

3.3 ADS-B的数据异常检测

异常检测系统是保障ADS-B数据安全的重

要组成部分,旨在检测恶意活动,主要针对ADS-B系统的欺骗、干扰或拒绝服务攻击,防止它们损害系统的完整性。根据方法和应用场景的不同,ADS-B的数据异常检测方案可分为基于深度学习、基于统计与自编码器、基于协作检测,以及基于高级时间动态检测4大类。ADS-B的数据异常检测方法总结如表6所示。

3.3.1 基于深度学习的模型检测

深度学习模型通过学习ADS-B数据的时序特性,建立飞行路径和行为的正常模式,能够有效地检测偏离正常轨迹的异常行为。Habler等^[47]提出了一种基于长短期记忆(long short-term memory, LSTM)网络编码器-解码器的模型,通过分析合法的ADS-B消息序列,检测由攻击者或妥协飞机发送的欺骗或操纵的ADS-B消息。Chevrot等^[48]进一步改进了LSTM模型,采用多个解码器来专门训练不同飞行阶段的数据(如爬升、巡航或下降),进一步提高了检测的精度。Yue等^[49]结合生成对抗网络与LSTM,提出了一种空域飞行图像预测和检测框架,通过生成未来图像并检测异常,识别潜在的攻击目标,特别适用于空中交通管控场景。

随着攻击手段的复杂化,深度学习方法在ADS-B欺骗攻击检测领域已提出更加精细的模型架构和检测策略。Ying等^[50]提出的SODA两阶段DNN检测系统代表了这一发展趋势。该系统通过结合消息级和飞机级的双重验证机制,分析物理层特征(如IQ样本和相位)进行初步筛选,再对特定飞机进行精确识别,达到了99.34%的地面欺骗攻击检测率和仅0.43%的误报率。与传统机器学习方法相比,这种深度学习架构能更好

表6 ADS-B的数据异常检测方法总结

Table 6 Summary of methods for anomaly detection in ADS-B data

方法	优点	不足	适用场景
基于深度学习的模型检测 ^[47-50]	捕捉复杂的时间序列模式,适用于多种攻击检测	依赖大量数据,实时性能可能受到限制	复杂攻击模式的检测(如欺骗和操纵攻击)
基于统计与自编码器的轻量化检测 ^[51-54]	异常检测精度高,误报率和漏报率较低	适应快速变化攻击的能力有限,模型复杂性高	资源有限环境中的高精度异常检测
面向分布式环境的协作检测 ^[55-56]	多节点协作提高系统鲁棒性,增强对复杂攻击的检测能力	需要额外的网络通信和资源支持,部署复杂性高	需要多节点协同检测的分布式环境
动态环境中的高级时间特征检测 ^[57-58]	动态适应不断变化的攻击模式,增强对复杂攻击的识别能力	模型复杂度较高,实时计算资源需求大	动态威胁环境下的攻击模式识别

得捕捉信号特征的微小变化,有效区分合法信号和高度仿真的欺骗信号。

深度学习方法的主要优势在于其强大的特征提取和模式识别能力,能够自动学习复杂的时空特征,无须人工特征。然而,这类方法也面临数据依赖性高、计算资源需求大、模型解释性差等挑战。特别是在航空电子设备资源受限的环境中,如何在保证检测性能的同时降低模型复杂度,成为深度学习方法实际应用的关键问题。

3.3.2 基于统计与自编码器的轻量化检测

相较于深度学习方法,统计与自编码器方法更注重轻量化设计,适合资源有限的场景。统计方法和自编码器通过对数据特征分布进行学习和重构来检测异常。Luo 等^[51]提出了一种结合变分自编码器 (variational autoencoder, VAE) 和支持向量数据描述 (support vector data description, SVDD) 的 ADS-B 异常检测方法。该模型通过 VAE 学习 ADS-B 数据的特征分布,对数据进行重构,并利用 SVDD 计算重构值与实际值的偏差确定异常阈值,提高了异常检测的精度。在此基础上,为解决现有 ADS-B 异常检测方法中长期依赖和分布特征、非轻量级模型和自适应阈值差的问题, Luo 等^[52]提出了 TTSAD (time-series transformer with support vector data description) 模型,该模型能够检测到由高度慢偏移和拒绝服务等攻击产生的 ADS-B 异常数据。特别针对消息注入攻击, Slimane 等^[53]提出了一种基于支持向量机的消息注入攻击检测模型,通过训练支持向量机分类器,分析每条 ADS-B 消息的特征,检测是否存在恶意注入行为,该模型在消息注入攻击的检测中具有较高的精度。

针对航空环境中常见的多种攻击类型,王布宏等^[54]提出了一种结合粒子群优化和多核支持向量数据描述的检测框架,该方法考虑了飞机机动性状态变化带来的数据波动,显著提高了在实际飞行环境中的适应性,这是传统检测方法常常忽视的因素。

统计与自编码器方法的核心优势在于其较低的计算复杂度和较强的轻量化特性,使其能够在资源受限的航空环境中实现实时检测。这类方法

通常比深度学习模型具有更好的可解释性,便于理解决策过程并进行调整。然而,这些方法在处理高度复杂或前所未见的攻击模式时可能效果有限,需要与其他检测方法结合使用以提高整体安全性。

3.3.3 面向分布式环境的协作检测

相比于基于统计与自编码器的检测方法,协作与分布式检测方法通过多节点协同可以在动态环境中提供更可靠的检测能力,协作检测方法通过结合多个节点的检测结果,增强对复杂攻击的检测能力。Li 等^[55]提出了顺序协同检测的概念,通过多个检测点 (如飞机或地面站) 对 ADS-B 数据进行协同检测,并将各检测点的结果组合为复合检测概率,从而提高对复杂攻击 (如欺骗和数据操纵) 的检测能力。该协作系统的设计有助于降低误报率,提供更可靠的检测结果。

随着 ADS-B 攻击形式的多样化发展,单一检测手段已难以应对所有威胁。Khan 等^[56]针对这一挑战,设计了能应对多种新型威胁的协作检测框架。该框架能够识别跳跃攻击 (攻击者突然改变身份)、虚假信息攻击、虚假航向攻击和虚假应答码攻击等复杂攻击模式,且各项指标均超过 99.80%。这一成果证明,通过合理选择和组合算法,协作式检测系统能够有效应对复杂多变的攻击场景。

协作检测方法能够利用多节点信息提高系统的鲁棒性,但其实现需要额外的网络通信和资源支持,增加部署复杂性,尤其是在航空环境中会面临资源和时延的挑战。

3.3.4 动态环境中的高级时间特征检测

相比协作检测方法,高级时间动态检测方法通过分析时间特征能够进一步增强对不断变化的攻击模式的适应能力。高级时间特征检测方法通过分析 ADS-B 数据的时间动态特征,识别复杂的攻击模式。Li 等^[57]提出了基于分层时态内存的模型,根据 ADS-B 数据的时间模式来检测攻击。通过分层时间记忆模型捕获 ADS-B 数据流中的短期和长期模式,为识别异常行为提供自适应机制。该系统在检测传统检测系统无法识别的新型攻击类型方面特别有效,通过不断在新数据中学习,时态内存系统可以实时检测攻击,并在

出现新的攻击模式时更新其检测功能,使系统能够高度适应ADS-B网络中不断变化的安全威胁。Li等^[58]在以往研究的基础上又提出使用隐马尔可夫模型和黏性分层狄利克雷过程来检测基于ADS-B数据的时间动态的攻击,动态适应不断变化的攻击模式,使其在检测可能试图避免传统异常方法检测的复杂攻击方面非常有效,增强了攻击检测系统的稳健性,并提供了对数据时间结构更细致的理解。

高级时间动态检测方法在不断变化的环境中表现出高度适应性,但其模型复杂性较高,实时计算的资源需求也较大,可能在航空电子设备上受到限制。

3.3.5 ADS-B数据异常检测的互补性

不同类型的ADS-B异常检测方法存在明显的互补关系。深度学习技术虽能有效捕捉复杂的攻击模式,但其计算复杂度往往制约了在资源受限环境中的应用;相比之下,统计方法计算负担较轻,适合快速筛选,但可能会漏检复杂攻击。结合这两种方法的互补优势,研究者已开发出多层次检测架构,实现了性能与效率的平衡。

实际应用研究中,这种互补组合已展示出显著的效果提升。王布宏等^[54]的PSO-MKSVDD (particle swarm optimization-multi-kernel support vector data description)模型通过结合多源数据(ADS-B与SSR数据的差值)作为检测基础,既增强了算法精度,又提高了系统对多种攻击类型的适应性。该方法在处理随机位置偏移、固定位置偏移、DoS攻击和重放攻击时均取得了优异表现,证明了多源数据与优化算法结合的有效性。

Ying等^[50]的SODA系统是技术互补的另一种典范,该系统通过两阶段设计实现了消息级和飞机级的双重验证。第一阶段利用物理层特征进行高速筛选,第二阶段则对可疑消息进行精细分类。这种分层架构既保证了系统处理效率,又确保了99.34%的检测率和0.43%的误报率。

尽管这些互补方法已取得显著进展,但在高误报率控制、动态攻击适应性及资源优化方面仍有提升空间,特别是在资源受限的航空环境中,更高效的异常检测技术仍需进一步探索。

3.4 ADS-B的位置验证技术

位置验证是确保ADS-B系统安全性的重要环节。ADS-B依赖飞机广播其位置信息,系统极易受到位置欺骗攻击,例如通过伪造位置报告,攻击可能导致航路偏离、空中碰撞或空中交通管制员态势感知失效,从而带来严重的安全隐患。ADS-B的位置验证技术通过分析信号的物理特性或位置信息的一致性,为位置伪造检测提供了重要手段。现有研究从不同维度对ADS-B位置验证技术进行了探索,主要分为基于时间差的验证方法、基于时间戳的验证方法,以及基于物理层特性的验证方法。这些方法针对不同的技术需求和应用场景提出了解决方案。ADS-B的位置验证技术总结如表7所示。

3.4.1 基于时间差的验证方法

到达时间差(time difference of arrival, TDOA)是一种通过测量信号在不同接收器之间的时间差进行位置验证的技术。Naganawa等^[59]介绍了使用TDOA验证飞机位置的理论框架,测量多个地面站或飞机接收到的信号之间的时间差,可以对飞机的位置进行三角测量,从而可以检测差异或

表7 ADS-B的位置验证技术总结

Table 7 Summary of ADS-B position verification techniques

方法	优点	不足	适用场景
基于TDOA的验证方法 ^[59-61]	高精度位置验证,适合长时间同步环境	对时间同步误差敏感,环境干扰可能降低精度	多接收器高同步精度的定位系统
基于IDOA的验证方法 ^[62]	减少对时间同步的依赖,鲁棒性更强	易受多路径传播和噪声干扰的影响	时间同步受限或多路径传播环境
基于时间戳的验证方法 ^[63-64]	快速筛选位置异常,适应动态环境	对时延误差和同步问题较为敏感	动态通信场景的快速位置筛选
基于物理层的验证方法 ^[65-66]	直接验证信号真实性,有效检测高级攻击	复杂信号处理需求高,易受环境干扰	检测位置伪造和复杂信号欺骗

操纵报告的位置。Elmarady 等^[60]进一步改进了 TDOA 方法,设计了一个增强系统,提高了位置验证的精度,并减少了计算时间。

传统 TDOA 方法虽然原理成熟,但在实际应用中受到传感器部署几何结构和计算复杂度的限制。随着研究的深入,基于 TDOA 原理的更先进方法不断涌现。Allmann 等^[61]利用同步传感器网络对 ADS-B 数据进行位置验证,不仅验证了实际 ADS-B 位置的准确性,还提出了自动阈值调整机制,显著提高了系统可靠性。

TDOA 方法在高精度时间同步环境中表现出色,但其对时间同步误差的敏感性限制了应用范围。为解决这一问题,到达时间间隔差 (interval difference of arrival, IDOA) 方法通过分析信号方向特性,减少了对时间同步的依赖,是对 TDOA 技术的有益补充。

刘海涛等^[62]建立基于 IDOA 的 ADS-B 位置消息验证系统模型,理论分析给出检验统计量的表达式及其统计特性,进一步给出检测门限的确定方法,通过仿真验证了所提方法的正确性和有效性。

IDOA 方法减少了对时间同步的需求,但在多路径传播和噪声较强的环境中可能会出现方向估计误差,从而影响验证效果。

3.4.2 基于时间戳的验证方法

时间戳方法通过对比信号的传播时间与预期时间来验证位置真实性。Kim 等^[63]介绍了一种称为 ADS-BT 的方法。该方法通过监控信号在发送方和接收方之间的传播时间,利用较小的时间戳值来测量实际飞行时间,并将其与基于位置数据的预期飞行时间进行比较。这种方法通过精确的时间分析,能有效检测并识别位置欺骗行为,为检测受损的 ADS-B 数据提供了一种可靠的方法。

苏志刚等^[64]针对时延转发电文的检测,提出了一种基于电文时间特性的方法。该方法根据 ADS-B 地面站接收电文的位置间隔分布特点,利用顺序电文间瞬时速度与关注期内平均速度的差异进行检测。这种方法使 ADS-B 地面站能够独立完成时延转发干扰检测和相应干扰台定位,特别适用于需要快速响应的动态通信环境。

时间戳方法对时延误差和同步问题较为敏感,能有效检测位置欺骗行为,但在动态通信环境中,由于数据传输时延的不确定性,其检测性能会受到一定限制。

3.4.3 基于物理层的验证方法

物理层验证方法通过分析信号的距离、方向等物理特性验证位置的真实性。Rudys 等^[65]提出了一种物理层验证解决方案,侧重于通过估计信号的距离和到达接收器的方向来验证 ADS-B 信号的真实性,通过分析物理层信号特性以检测潜在的欺骗或干扰攻击。Zhang 等^[66]针对拒绝服务攻击设计了一种误差适应机制,通过高效计算实现了对恶意攻击消息的生成和验证,有效应对多种类型的拒绝服务攻击。

物理层验证方法通过直接分析信号的物理特性,为高级攻击的检测提供了强有力的手段。然而,其复杂的信号处理需求和对环境干扰的敏感性限制了实际应用效果。在多方法协作中,物理层方法通常作为第一道防线,与其他方法结合能显著增强系统的整体性能。

3.4.4 ADS-B 位置验证技术的互补性

不同位置验证方法各有优势,适用于不同场景,组合使用可实现有效互补。实践证明,单一验证技术难以满足复杂航空环境的安全需求,需要多技术协同构建全面防御体系。

Allmann 等^[61]的研究是多技术互补应用的实例。该研究基于传感器网络构建了 ADS-B 位置验证系统,创新性地结合了 TDOA 测量和自动阈值调整机制。在仅使用两个传感器的情况下,该系统成功验证模拟的 ADS-B 位置信息,展示了 TDOA 技术在有限资源条件下的部署可行性。系统的自动阈值调整机制则解决了传统 TDOA 方法中阈值选择的难题,显著提高了验证的适应性和准确性。

更具突破性的是 Elmarady 等^[60]提出的 ATBAS (actual TDoA-based augmentation system),该系统将历史数据学习与 TDOA 验证相结合,构建了一种全新的指纹网格验证框架。通过利用 OpenSky 网络中的真实历史数据训练 TDOA 指纹网格,ATBAS 系统不仅显著提高了位置验证精度 (较传统 MLAT 系统提高 56.93%),还大幅减

少了计算时间（减少 77%）。这种方法特别适合需要处理海量数据的空中交通管控环境，展示了历史数据学习与位置验证技术结合的强大潜力。

苏志刚等^[64]的研究给出了时间特性分析与多点定位技术的互补优势。通过分析顺序电文间的瞬时速度与平均速度差异，该方法能有效检测时延转发电文；随后利用精确的接收时间戳和位置信息，通过多点定位技术实现对干扰台的精确定位。这种检测与定位相结合的方法，为 ADS-B 地面站提供了独立应对时延转发干扰的能力，展示了时间戳方法与定位技术互补的实际应用价值。

这些实例证明，跨技术、跨层次的方法组合是实现 ADS-B 位置验证效果最大化的关键途径。通常的互补路径包括：先使用高效的时间戳方法进行初步筛选，再对可疑数据应用更精确的 TDOA/IDOA 方法；或通过物理层特征分析与多点定位技术结合，既验证位置真实性，又实现对干扰源的精确定位。这种多层次防御不仅提高了系统的检测精度，还增强了面对复杂攻击时的鲁棒性。

未来位置验证技术的发展需要从系统架构层面设计更加灵活、自适应的验证框架，以适应动态多变的航空安全环境。

3.5 ADS-B 信号抗干扰技术

为了提升 ADS-B 信号的抗干扰能力，现有研究从硬件层、信号处理层和频谱管理层等多个维度提出了解决方案，主要包括基于多通道接收器的硬件抗干扰方案、基于随机差分扩频的信号处理方案以及基于频率分散的频谱管理方案。ADS-B 信号抗干扰技术总结如表 8 所示。

3.5.1 基于多通道接收器的抗干扰方案

基于多通道接收器的抗干扰技术通过多通道信号接收来提升 ADS-B 的抗干扰能力。Leonardi

等^[67]提出了一种通过多通道接收器中引入代数信号分离处理的抗干扰解决方案。该方案通过信号到达角度分析，分离干扰信号，并从多通道数据中恢复原始 ADS-B 信号。实验表明，在干扰环境下应用扩展投影算法可以将干扰信号的影响显著降低，使得原本无法解码的信号在 63.3% 的情况下恢复正常解码。

基于多通道接收器的抗干扰方案的优势在于无须对现有硬件进行大幅改造，只需进行软件层面的更新即可实现，从而降低了实施成本。然而，多通道接收的实现硬件资源要求较高，特别是在高密度的空中交通环境中，需要更多的天线和接收设备来支撑这一方案。

3.5.2 基于随机差分扩频的抗干扰方案

基于随机差分扩频的抗干扰技术能够在广播通信中提供更灵活的解决方案，并显著降低实施复杂度。Liu 等^[68]提出了一种随机差分直接序列扩频方案，通过不可预测的扩频码将信号扩展到更大的频谱范围，降低干扰的影响。实验表明，随机差分直接序列扩频方案在应对反应式干扰攻击时表现出色，显著提高了干扰信号的攻击难度。

在扩频技术领域，Hasjuks 等^[69]的研究比较了基于混沌的直序扩频（direct-sequence spread spectrum, DSSS）和跳频扩频（frequency-hopping spread spectrum, FHSS）多用户通信系统性能，展示了混沌扩频方案在提高安全性和降低多址干扰方面的优势。通过使用混沌序列而非传统的 m 序列进行扩频，该方法在特定场景下展现出抗干扰性能的提升。这种基于混沌的扩频技术特别适用于传播条件差、信噪比低、硬件能力有限的无线传感网络环境，为 ADS-B 抗干扰提供了新思路。

表 8 ADS-B 信号抗干扰技术总结

Table 8 Summary of ADS-B signal anti-jamming technologies

方案	优点	不足	适用场景
基于多通道接收器的抗干扰方案 ^[67]	有效分离干扰信号，降低实施成本	对硬件资源需求高，在高密度交通中限制较多	高干扰环境，多接收设备场景
基于随机差分扩频的抗干扰方案 ^[68-69]	提高抗干扰能力，无须共享密钥	对接收端计算能力和处理速度要求较高	广播通信场景，动态抗干扰环境
基于频率分散的抗干扰方案 ^[70]	分散干扰信号功率，显著提高成功解码率	需要硬件支持频谱管理，设计复杂性较高	干扰强度较高的动态通信场景

基于随机差分扩频的方案特别适用于广播通信的抗干扰场景,其无须发送方与接收方共享密钥,部署复杂性低。然而,对接收端计算能力和信号处理速度的高要求增加了实施成本。

3.5.3 基于频率分散的抗干扰方案

在高强度干扰场景中,频率分散技术凭借其灵活的频谱管理能力,能够进一步增强系统的抗干扰性能。Leonardi等^[70]探讨了动态频率跳跃策略和其他频率分散方法的应用。这些策略通过分散信号功率,使干扰器难以对特定信道施加高强度干扰,从而提高信号的成功解码率。

频率分散策略在应对复杂干扰方面表现优异,但其实现依赖于硬件支持动态频谱管理,增加了系统设计和部署的复杂性。此外,快速跳频和频谱分散算法可能带来额外的计算开销,需在高性能和低功耗间寻求平衡。

3.5.4 ADS-B 抗干扰技术的互补性

针对 ADS-B 信号易受干扰的特性,单一抗干扰技术难以应对复杂多变的干扰场景,互补技术的协同应用已成为构建综合性抗干扰策略的核心。实际研究证明,不同技术间的有效整合能大幅提升整体抗干扰能力。

Hasjuks等^[69]的研究展示了 DSSS 与 FHSS 技术互补的价值。通过对基于混沌的 DSSS 和 FHSS 系统进行全面比较,发现两种技术在不同场景下各有优势:DSSS 在多用户干扰环境中表现出更优的抗干扰能力,而 FHSS 则在应对选择性干扰和频率选择性衰落时效果更佳。这种针对不同干扰类型的互补特性,为构建分层抗干扰架构提供了理论基础。

在实际系统部署中,上述技术可基于干扰特性进行动态组合:针对高强度宽带干扰,可优先采用频率分散技术分散干扰功率;对于智能干扰,则可结合随机扩频技术增加干扰预测难度;而在资源充足的地面站点,多通道接收与代数分离处理能提供更全面的干扰隔离能力。

尽管互补技术的协同应用显著提升了 ADS-B 的抗干扰能力,但在资源受限、高动态的航空环境中,如何平衡抗干扰性能与实施成本、如何确保不同技术间的无缝协作仍是关键挑战,需要进一步的理论研究和实践验证。

4 ADS-B 安全未来研究方向

当前用于保障 ADS-B 安全的各种解决方案,在防范窃听、数据篡改、伪造和拒绝服务攻击等方面取得了积极成效。然而,随着航空业的持续发展和攻击手段的日益复杂,当前的安全方案仍面临诸多挑战。针对现有方案的不足,本文将探讨 ADS-B 安全的未来研究方向,提出多种可能的发展趋势,包括结合人工智能和机器学习的安全模型、提高 ADS-B 抗干扰能力、区块链方案的优化、车联网安全技术的潜在应用,以进一步提升 ADS-B 系统的防御能力和可靠性,为未来的航空管理系统提供安全保障。

4.1 ADS-B 数据异常检测的智能化方法

人工智能^[71]和机器学习^[72]技术的发展为 ADS-B 安全提供了新的可能性,现有的检测算法主要依赖固定模型和预定义规则,难以应对不断变化的威胁模式。为了提升检测能力,未来研究可以探索自适应算法的动态优化,开发能够根据实时威胁情境自适应调整的检测算法,如基于强化学习的模型。Reaney等^[73]在面向航空器 IT-OT 场景的网络入侵响应研究中证明了强化学习模型能够有效地学习安全防御策略,并随环境变化不断调整响应行为。

在强化学习应用场景中,ADS-B 检测系统可被建模为智能体,该智能体通过持续与航空通信环境交互,学习最优的异常检测策略。具体而言,在空管自动化系统中,强化学习模型可用于动态调整异常检测阈值,根据不同飞行阶段(起飞、巡航、着陆)自动优化检测参数。当检测到可疑的航迹突变时,强化学习模型可基于历史航班数据和当前空域密度,自适应判断是否为恶意欺骗攻击,从而减少误报率。强化学习模型还可学习区分正常的军事演习活动与恶意干扰,通过奖励机制不断优化对新型攻击模式的识别能力。

4.2 ADS-B 抗干扰通信的优化策略

文献[74]提出了一种无密钥的抗干扰机制,利用熵优化方法在常见的干扰攻击下提高通信的可用性和鲁棒性。该设计在现有航空系统法规框架内具备良好的集成潜力,尤其适用于应对虚假信息注入和拒绝服务攻击等典型威胁。未来的研究方向中,集成类似的抗干扰设计机制至关重

要,这不仅可以增强ADS-B系统的可靠性,还能提升其整体安全性。

分布式节点协作通信策略的引入可以在恶劣干扰环境下实现更强的鲁棒性。通过节点间动态调整发射功率和信道使用策略,可以有效避免特定信道的阻塞。在跨层优化设计方面,通过综合考虑物理层、链路层和网络层的抗干扰设计,构建统一的优化模型。在物理层采用干扰识别算法实时监测信道状态,在网络层动态调整路由策略,可减少干扰对整体通信系统的影响。

4.3 ADS-B系统中的区块链技术优化

区块链技术^[75]因其不可篡改性和分布式特性,在解决ADS-B数据的篡改和伪造问题上具有独特优势。然而,传统区块链方案面临低吞吐量和高能耗的问题,难以满足ADS-B系统对实时性和高效性的要求。未来的研究可以着重开发轻量级共识机制,以解决现有共识算法计算复杂度高的问题。通过基于拜占庭容错的简化协议,可以在保证数据可信性的同时显著降低计算资源需求。此外,引入分片技术^[76]对区块链网络进行分片处理,可进一步提高系统吞吐量。

在区块链与现有ADS-B系统的集成优化中,还需要解决协议兼容性和性能平衡问题。未来研究可开发模块化的区块链应用框架,以实现与现有航空管理系统的无缝对接,同时优化带宽和资源的使用。

4.4 车联网安全技术ADS-B中的潜在应用

随着车联网安全技术的迅速发展和成熟,探索其在ADS-B系统中的应用潜力具有重要价值。尽管第1.3节分析表明两种系统在通信特性和应用场景上存在差异,但作为交通领域的无线通信系统,它们在安全需求和威胁模型上呈现出一定共性,为跨领域技术迁移创造了可能性。

车联网研究领域中的轻量级认证机制具有显著迁移价值。Hathal等^[77]提出的无证书轻量级认证方案,通过使用认证令牌替代传统数字证书,在保持安全性的同时降低了通信和计算开销。这种特性与ADS-B带宽受限的环境高度契合,可为其提供高效的通信认证机制。同样,Luo等^[78]综述的物理层安全技术,通过利用无

线信号传播特性进行身份与位置验证,可为ADS-B位置验证提供辅助手段,尤其在传统加密机制难以实施时。此外,El-Sayed等^[79]提出的分层信任框架,有望简化全球范围内ADS-B系统的密钥管理问题,为跨区域的分布式信任提供解决方案。

技术迁移面临多重挑战,ADS-B系统的资源限制更为严格,每条消息仅有112 bit,要求安全机制必须进一步轻量化。同时,ADS-B需要全球范围内的互操作性,远高于区域性较强的车联网系统。此外,车联网主要在二维平面运行,而ADS-B需要在三维空间进行位置验证,增加了技术迁移的复杂性。

针对这些挑战,未来研究可从优化资源利用、构建跨区域信任框架和扩展空间验证模型3个方向推进。具体而言,可采用离线/在线计算分离策略,将复杂计算任务分配给地面基础设施;构建基于分层信任模型的全球密钥管理框架,支持区域间信任传递;并将物理层安全技术从二维扩展到三维,适应航空环境的定位需求。

这种跨领域的技术融合虽然面临挑战,但也蕴含创新机遇,有望为ADS-B系统安全提供更全面、更有效的保障措施。

未来的ADS-B安全研究将结合智能检测、抗干扰通信和区块链技术等多方面的先进技术,形成综合性的解决方案,以进一步增强系统的安全性和可靠性。从智能化算法的实时威胁识别,到分布式协同抗干扰机制的设计,再到区块链技术的优化应用,以及探索类似领域前沿技术的跨领域迁移,这些研究方向不仅能有效应对当前系统的局限性,也为未来航空管理系统的安全保障提供了基础。随着技术的不断进步,ADS-B系统的安全性将朝着更加智能化、高效化和协同化的方向发展,更好地满足未来航空业对安全性和可靠性的需求。

5 结束语

本文对ADS-B技术的安全研究进行了系统性综述,并从技术背景、安全挑战到解决方案的逻辑框架展开分析。本文首先介绍了ADS-B技术的工作原理、系统结构及其与传统监视系统的关系,为安全问题分析奠定了基础。接着剖析了

ADS-B 系统面临的安全挑战, 包括窃听攻击、欺骗攻击、信号干扰攻击、消息注入攻击以及消息篡改攻击, 并系统评估了各类攻击的技术复杂性、实施成本与潜在影响。

针对 ADS-B 系统面临的安全挑战, 本文探讨了已有的安全应对方案, 构建了一个多层次的分析框架, 系统性地评估了 5 大技术方向的研究进展。基于密码学的通信安全方案通过加密与身份验证技术保障数据机密性与完整性; 区块链技术利用去中心化与不可篡改特性提升数据可信度; 数据异常检测技术借助深度学习、统计方法和协作检测识别潜在威胁; 位置验证技术通过物理层特性分析验证位置信息真实性; 抗干扰技术则从信号处理角度增强系统稳定性。对每种技术都详细分析了其优势、局限性及适用场景, 并探讨了不同技术间的互补性与协同应用价值。

尽管现有的 ADS-B 安全方案在各自领域取得了显著进展, 但在性能与安全性平衡、全球范围内的密钥管理、面对复杂攻击的检测能力, 以及实际部署与资源约束等方面仍存在挑战。未来应聚焦于融合人工智能的智能化检测模型、无密钥抗干扰机制、区块链技术的轻量级优化, 以及车联网安全技术的跨领域应用等方面, 构建更全面、更高效的 ADS-B 安全防护体系。

本文的系统分析与综合评估为理解 ADS-B 安全研究现状提供了全面视角, 为未来航空通信安全技术发展提供了理论参考与实践指导, 对推动航空交通管理系统安全水平的提升具有重要的学术价值与应用意义。

参考文献:

- [1] CAPEZZUTO V, DUNSTONE G. Aireon space-based ADS-B implementation and operation[EB]. 2018.
- [2] CENCIOTTI D. US airborne communication plane could be tracked on the web for 9 hours during air strike that killed Taliban leaders in Afghanistan[EB]. 2021.
- [3] Musk threatens legal action against Twitter user who tracked his private jet[EB]. 2022.
- [4] MAGAZU D. Exploiting the automatic dependent surveillance-broadcast system via false target injection[D]. Wright-Patterson Air Force Base: Air Force Institute of Technology, 2012.
- [5] MCCALLIE D L. Exploring potential ADS-B vulnerabilities in the FAA's next gen air transportation system[D]. Wright-Patterson Air Force Base: Air Force Institute of Technology, 2011.
- [6] ESKILSSON S, GUSTAFSSON H, KHAN S, et al. Demonstrating ADS-B AND CPDLC attacks with software-defined radio[C]//Proceedings of the 2020 Integrated Communications Navigation and Surveillance Conference (ICNS). Piscataway: IEEE Press, 2020.
- [7] 中央电视台新闻频道. 警惕! 航空爱好者沦为“窃密志愿”[EB]. 2021.
CCTV News Channel. Beware! Aviation enthusiasts become "espionage volunteers" [EB]. 2021.
- [8] 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.
- [9] MANESH R M, KAABOUCH N. Analysis of vulnerabilities, attacks, countermeasures and overall risk of the automatic dependent surveillance-broadcast (ADS-B) system[J]. International Journal of Critical Infrastructure Protection, 2017, 19: 16-31.
- [10] STROHMEIER M, MOSER S M, LENDERS V, et al. Realities and challenges of next-gen air traffic management: the case of ADS-B [J]. IEEE Communications Magazine, 2014, 52(5): 111-118.
- [11] WU Z, SHANG T, GUO A. Security issues in automatic dependent surveillance-broadcast (ADS-B): a survey[J]. IEEE Access, 2020, 8: 122147-122167.
- [12] 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.
- [13] LO S, CHEN Y H. Automatic dependent surveillance-broadcast (ADS-B) universal access transceiver (UAT) transmissions for alternative positioning, navigation, and timing (APNT): concept & practice[J]. Journal of the Institute of Navigation, 2021, 68(2): 293-313.
- [14] SONG J H, OH K R, KIM I K, et al. Preliminary implementation of ground-to-ground surveillance test-bed based on ADS-B concepts [C]//Proceedings of the 2007 International Conference on Control, Automation and Systems. Piscataway: IEEE Press, 2007: 1434-1438.
- [15] WAGNER S, JOHANNES W, QOSJA D, et al. Small target detection in a radar surveillance system using contractive autoencoders[J]. IEEE Transactions on Aerospace and Electronic Systems, 2024, 60 (1): 51-67.
- [16] ZHANG J, LIU W, ZHU Y. Study of ADS-B data evaluation[J]. Chinese Journal of Aeronautics, 2011, 24(4): 461-466.
- [17] HUANG H, FANG Y, MAZOTTI B, et al. Privacy-aware design and analysis of drone remote identification systems[J]. IEEE Transactions on Intelligent Transportation Systems, 2024, 25(12): 21455-21468.
- [18] NGUYEN Q K, KIM S, HAN S H, et al. Improved self-calibration of a multilateration system based on absolute distance measurement[J]. Sensors, 2020, 20: 7288.
- [19] SUN N, WANG W, LIU K X, et al. Hybrid framework for security evaluation in Internet of Vehicles[J]. Computers & Security, 2025, 153: 104398.
- [20] REKKAS C. Status of WAM, ADS-B out and ATSAW deployment

- in Europe[C]//Proceedings of the 2014 Tyrrhenian International Workshop on Digital Communications - Enhanced Surveillance of Aircraft and Vehicles (TIWDC/ESAV). Piscataway: IEEE Press, 2014: 1-5.
- [21] STROHMEIER M, MOSER D, SCHAFFER M, et al. On the applicability of satellite-based air traffic control communication for security[J]. *IEEE Communications Magazine*, 2019, 57(9): 79-85.
- [22] COSTIN A. Ghost in the air (traffic): on insecurity of ADS-B protocol and practical attacks on ADS-B devices[C]//Black Hat USA. Las Vegas: Black Hat Briefings, 2012: 1-12.
- [23] SCIANCALEPORE S, ALHAZBI S, DI PIETRO R. Receivers location privacy in avionics crowd-sourced networks: issues and countermeasures[J]. *Journal of Network and Computer Applications*, 2021, 174: 102892.
- [24] JAMAL M H, ABDESSAMAD A, JEANMARC G, et al. Security establishment in ADS-B by format-preserving encryption and blockchain schemes[J]. *Applied Sciences*, 2023, 13(5): 3105.
- [25] BAEK J, HABLEEL E, BYON Y J, et al. How to protect ADS-B: confidentiality framework and efficient realization based on staged identity-based encryption[J]. *IEEE Transactions on Intelligent Transportation Systems*, 2017, 18(3): 690-700.
- [26] SCHÄFER M, LENDERS V, MARTINOVIC I. Experimental analysis of attacks on next generation air traffic communication[C]//Proceedings of the Applied Cryptography and Network Security. Berlin: Springer, 2013: 253-271.
- [27] WILHELM M, MARTINOVIC I. Reactive jamming in wireless networks: how realistic is the threat [C]//Proceedings of the 4th ACM Conference on Wireless Network Security. New York: ACM, 2011: 47-52.
- [28] 孙保明, 陈娟, 谷志鸣. ADS-B 系统面临的风险及应对措施[J]. *通信学报*, 2024, 45(S1): 114-118.
- SUN B M, CHEN J, GU Z M. Research on risks faced by ADS-B system and solutions[J]. *Journal on Communications*, 2024, 45(S1): 114-118.
- [29] 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.
- [30] 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.
- [31] GHOSE N, LAZOS L. Verifying ADS-B navigation information through Doppler shift measurements[C]//Proceedings of the 2015 IEEE/AIAA 34th Digital Avionics Systems Conference (DASC). Piscataway: IEEE Press, 2015.
- [32] FRIED A, LAST M. Facing airborne attacks on ADS-B data with autoencoders[J]. *Computers & Security*, 2021, 109: 102405.
- [33] YANG H M, ZHOU Q X, YAO M X, et al. A practical and compatible cryptographic solution to ADS-B security[J]. *IEEE Internet of Things Journal*, 2019, 6(2): 3322-3334.
- [34] AN B. Holistic air protection scheme of ADS-B communication[J]. *IEEE Access*, 2019, 7: 65251-65262.
- [35] BURFEIND B, HOOPER P, LACHOW A. Confidential ADS-B[C]//Proceedings of the 2019 IEEE Aerospace Conference. Piscataway: IEEE Press, 2019: 1-11.
- [36] BAEK J, BYON Y J, HABLEEL E, et al. An authentication framework for automatic dependent surveillance-broadcast based on on-line/offline identity-based signature[C]//Proceedings of the 2013 Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing. Piscataway: IEEE Press, 2013: 358-363.
- [37] YANG H M, HUANG R S, WANG X F, et al. EBAA: an efficient broadcast authentication scheme for ADS-B communication based on IBS-MR[J]. *Chinese Journal of Aeronautics*, 2014, 27(3): 688-696.
- [38] WU Z J, GUO A X, YUE M, et al. An ADS-B message authentication method based on certificateless short signature[J]. *IEEE Transactions on Aerospace and Electronic Systems*, 2020, 56(3): 1742-1753.
- [39] YANG A J, TAN X, BAEK J, et al. A new ADS-B authentication framework based on efficient hierarchical identity-based signature with batch verification[J]. *IEEE Transactions on Services Computing*, 2017, 10(2): 165-175.
- [40] ASARI A, ALAGHEBAND M R, BAYAT M, et al. A new provable hierarchical anonymous certificateless authentication protocol with aggregate verification in ADS-B systems[J]. *Computer Networks*, 2021, 185: 107599.
- [41] YI P, LI J G, ZHANG Y C, et al. Efficient hierarchical signature scheme with batch verification function suitable for ADS-B system[J]. *IEEE Transactions on Aerospace and Electronic Systems*, 2023, 59(2): 1292-1299.
- [42] 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.
- [43] DAMIS A H, SHEHADA D, FACHKHA C, et al. A microservices architecture for ADS-B data security using blockchain[C]//Proceedings of the 2020 3rd International Conference on Signal Processing and Information Security (ICSPIS). Piscataway: IEEE Press, 2020: 1-4.
- [44] WU Z J, SHANG T, YUE M, et al. ADS-B chain: a blockchain-based trusted service scheme for automatic dependent surveillance broadcast[J]. *IEEE Transactions on Aerospace and Electronic Systems*, 2023, 59(6): 8535-8549.
- [45] SWATHI P, NATARAJAN K. Securing ADS-B data transmissions using blockchain: a comprehensive survey and analysis[J]. *Aircraft Engineering and Aerospace Technology*, 2023, 95(3): 452-463.
- [46] LU X, WU Z J, CAO J B. ATM chain: blockchain-based security architecture for air traffic management in future[J]. *IEEE Transactions on Aerospace and Electronic Systems*, 2024, 60(4): 3872-3896.
- [47] HABLEER E, SHABTAI A. Using LSTM encoder-decoder algorithm for detecting anomalous ADS-B messages[J]. *Computers & Security*, 2018, 78: 155-173.
- [48] 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.
- [49] 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.
- [50] YING X H, MAZER J, BERNIERI G, et al. Detecting ADS-B spoofing attacks using deep neural networks[C]//*Proceedings of the 2019 IEEE Conference on Communications and Network Security (CNS)*. Piscataway: IEEE Press, 2019: 187-195.
- [51] 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.
- [52] 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.
- [53] SLIMANE H O, BENOUDAH S, AL SHAMAILEH K, et al. ADS-B message injection attack on UAVs: assessment of SVM-based detection techniques[C]//*Proceedings of the 2022 IEEE International Conference on Electro Information Technology (eIT)*. Piscataway: IEEE Press, 2022: 405-410.
- [54] 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-MKSVD[J]. *Journal of Electronics & Information Technology*, 2020, 42(11): 2727-2734.
- [55] 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.
- [56] KHAN S, THORN J, WAHLGREN A, et al. Intrusion detection in automatic dependent surveillance-broadcast (ADS-B) with machine learning[C]//*Proceedings of the 2021 IEEE/AIAA 40th Digital Avionics Systems Conference (DASC)*. Piscataway: IEEE Press, 2021: 1-10.
- [57] LI T, WANG B, SHANG F, et al. Online sequential attack detection for ADS-B data based on hierarchical temporal memory[J]. *Computers & Security*, 2019, 87: 101599.
- [58] 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.
- [59] NAGANAWA J, MIYAZAKI H. Theory of automatic dependent surveillance - broadcast position verification using time difference of arrival[J]. *IEEE Transactions on Aerospace and Electronic Systems*, 2021, 57(3): 1387-1404.
- [60] ELMARADY A A, RAHOUMA K. Actual TDOA-based augmentation system for enhancing cybersecurity in ADS-B[J]. *Chinese Journal of Aeronautics*, 2021, 34(2): 217-228.
- [61] ALLMANN C, STANZEL S, STEFFES C. TDOA-based position verification of ADS-B information using a sensor network[C]//*Proceedings of the 2022 Sensor Data Fusion: Trends, Solutions, Applications (SDF)*. Piscataway: IEEE Press, 2022: 1-6.
- [62] 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, 50(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, 50(9): 2696-2703.
- [63] KIM Y, JO J Y, LEE S. ADS-B vulnerabilities and a security solution with a timestamp[J]. *IEEE Aerospace and Electronic Systems Magazine*, 2017, 32(11): 52-61.
- [64] 苏志刚, 关静, 郝敬堂, 等. ADS-B 时延转发报文检测及干扰台定位方法[J]. *电子与信息学报*, 2021, 43(2): 329-334.
- SU Z G, GUAN J, HAO J T, et al. Method for detecting the delay-forwarding ADS-B messages and positioning of jammer[J]. *Journal of Electronics & Information Technology*, 2021, 43(2): 329-334.
- [65] RUDYS S, ALEKSANDRAVICIUS J, ALEKSIEJUNAS R, et al. Physical layer protection for ADS-B against spoofing and jamming[J]. *International Journal of Critical Infrastructure Protection*, 2022, 38: 100555.
- [66] ZHANG Q, WANG Z, WU B, et al. A robust and practical solution to ADS-B security against denial-of-service attacks[J]. *IEEE Internet of Things Journal*, 2024, 11(8): 13647-13659.
- [67] LEONARDI M, PIRACCI E, GALATI G. ADS-B jamming mitigation: a solution based on a multichannel receiver[J]. *IEEE Aerospace and Electronic Systems Magazine*, 2017, 32(11): 44-51.
- [68] LIU Y, NING P, DAI H Y, et al. Randomized differential DSSS: jamming-resistant wireless broadcast communication[C]//*2010 Proceedings IEEE INFOCOM*. Piscataway: IEEE Press, 2010: 1-9.
- [69] HASJUKS N, HELLBRUCK H, ABOLTINSA. Performance study of chaos-based DSSS and FHSS multi-user communication systems[C]//*Proceedings of the 2022 Workshop on Microwave Theory and Techniques in Wireless Communications (MTTW)*. Piscataway: IEEE Press, 2022: 23-28.
- [70] LEONARDI M, PIRACCI E, GALATI G. ADS-B vulnerability to low cost jammers: Risk assessment and possible solutions[C]//*Proceedings of the 2014 Tyrrhenian International Workshop on Digital Communications - Enhanced Surveillance of Aircraft and Vehicles (TIWDC/ESAV)*. Piscataway: IEEE Press, 2014: 41-46.
- [71] LI B, QI P, LIU B, et al. Trustworthy AI: from principles to practices[J]. *ACM Computing Surveys*, 2023, 55(9): 1-46.
- [72] PENG G C Y, ALBER M, BUGANZA TEPOLE A, et al. Multiscale modeling meets machine learning: what can we learn[J]. *Archives of Computational Methods in Engineering*, 2021, 28: 1017-1037.
- [73] REANEY M, MCLAUGHLIN K, GRANT J. Network intrusion response using deep reinforcement learning in an aircraft IT-OT scenario[C]//*Proceedings of the 19th International Conference on Availability, Reliability and Security*. New York: ACM, 2024: 1-7.
- [74] VÁZQUEZ-CASTRO Á. Asymptotically guaranteed anti-jamming spread spectrum random access without preshared secret[J]. *IEEE Transactions on Information Forensics and Security*, 2022, 17: 332-343.
- [75] ZHANG R, XUE R, LIU L. Security and privacy on blockchain[J]. *ACM Computing Surveys*, 2020, 52(3): 1-34.
- [76] DANG H, DINH T T A, LOGHIN D, et al. Towards scaling block-

chain systems via sharding[C]//Proceedings of the 2019 International Conference on Management of Data. New York: ACM, 2019: 123-140.

- [77] HATHAL W, CRUICKSHANK H, SUN Z L, et al. Certificateless and lightweight authentication scheme for vehicular communication networks[J]. IEEE Transactions on Vehicular Technology, 2020, 69(12): 16110-16125.

- [78] LUO X W, LIU Y L, CHEN H H, et al. Physical layer security in intelligently connected vehicle networks[J]. IEEE Network, 2020, 34(5): 232-239.

- [79] EL-SAYED H, ALEXANDER H, KULKARNI P, et al. A novel multifaceted trust management framework for vehicular networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(11): 20084-20097.

[作者简介]



谢丽霞（1974-），女，重庆人，硕士，中国民航大学教授，主要研究方向为网络信息安全。



宁亚洲（2000-），男，辽宁朝阳人，中国民航大学硕士生，主要研究方向为网络信息安全。



杨宏宇（1969-），男，吉林长春人，博士，中国民航大学教授、博士生导师，主要研究方向为网络信息安全。



朱友文（1986-），男，安徽阜南人，博士，南京航空航天大学教授、博士生导师，主要研究方向为信息安全、数据隐私。



胡慧玲（1971-），女，四川人，民航中南地区空中交通管理局高级工程师，主要研究方向为空中交通管制、低空运行管理。



成翔（1988-），男，新疆乌鲁木齐人，博士，扬州大学实验师，主要研究方向为网络与系统安全、网络安全态势感知、APT攻击检测。