ADS-B 系统面临的风险及应对措施

孙保明，陈娟，谷志鸣
（91977 部队，北京 100036）

摘　要：由于其公开的技术体制，广播式自动相关监视（ADS-B）系统易受人为主动欺骗和干扰，从而导致工作性能降低。针对该问题，分析了 ADS-B 技术特点，详细阐述了 ADS-B 系统可能面临的干扰和欺骗风险，并给出了抗干扰防欺骗技术途径。

关键词：广播式自动相关监视；抗干扰；防欺骗
中图分类号：F562
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2024222

Research on risks faced by ADS-B system and solutions

SUN Baoming, CHEN Juan, GU Zhiming
Unit 91977 of PLA, Beijing 100036, China

Abstract: Due to its open technical system, ADS-B system was vulnerable to active jamming and deception, resulting in reduced performance. Aiming at this problem, the technical characteristics of ADS-B were analyzed, the possible jamming and detection risks faced by ADS-B system were elaborated, and the solutions of anti-interference and anti-deception were given.

Keywords: automatic dependent surveillance-broadcast, anti-jamming, anti-deception

0　引言

随着世界航空业的快速发展，航班流量日益激增，航空安全受到越来越多的关注。空管监视作为空中交通管理的核心功能，对防止空中危险接近，保障用空安全至关重要。传统的陆基空管一/二次雷达因数据更新速率慢、监视误差大、存在监视盲区和建设成本高等缺陷难以适应航空运输业的迅速发展对空管监视能力的需求。相比于传统的监视系统，基于全球导航卫星系统（GNSS, global navigation satellite system）的广播式自动相关监视（ADS-B, automatic dependent surveillance-broadcast）系统具有数据更新快、监视精度高、无监视盲区以及建设成本低等突出优点[1]，因此得到国际民航组织（ICAO）的认可，被指定为未来新航行系统的主要监视手段。但是由于其开放共享式自动监视架构，以及其公开的技术标准与数据编码格式，ADS-B 系统易受人为干扰和欺骗，使管制人员无法获取真实的空中目标态势，给防相撞工作带来较大挑战。因此，如何科学合理地识别并应对干扰欺骗风险，成为制约航空运输业进一步发展的关键问题。文献[2]提出一种分布式 ADS-B 无源定位防欺骗方法，但该方法需要多个地面基站。文献[3]提出了一种基于到达时间差/到达时间的 ADS-B 系统防欺骗技术，但该技术对 ADS-B 系统的时间同步能力要求较高。文献[4]提出一种基于方位估计和空域滤波的抗干扰方法。本文基于 ADS-B 技术特点，分析 ADS-B 系统可能面临的干扰和欺骗风险，并研究相应的应对措施。

1　ADS-B 技术原理

ADS-B 系统由机载设备和地面设备组成，其架

收稿日期：2024–10–08
通信作者：陈娟，juan3156@163.com

构如图1所示。ADS-B机载发射设备利用1090ES数据链，将GNSS计算得到的飞机位置信息（包括经纬度、高度等）周期性地广播出去，ADS-B地面站接收这些ADS-B报文，通过有线方式传输至控制中心，实现地面对空中飞机的监视。同时，其他ADS-B机载设备也能接收这些ADS-B报文，获得其位置信息，为实现空中自主防相撞提供支撑。

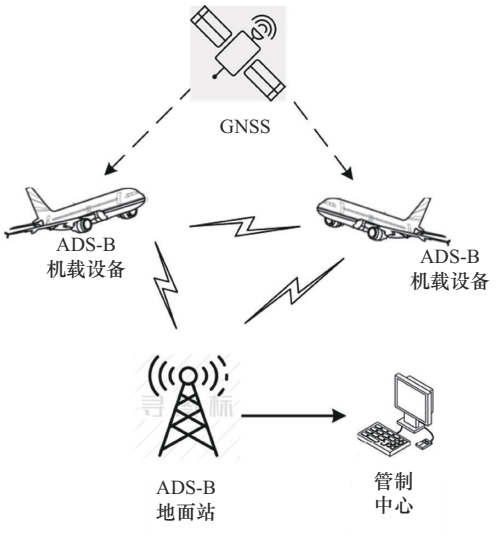

图1　ADS-B 系统架构

ADS-B机载发射设备通过各种总线接口获取GNSS系统、飞行管理系统、高度表等数据输入，按照标准规定的格式内容进行编码，并按照设定的时间要求形成基带时序，将基带信号调制到1090 MHz以后对外广播；地面设备和-ADS-B机载接收设备接收广播信号，完成射频解调和信息解码，解析出ADS-B报文，通过S模式地址进行关联，形成实时的飞行器航迹，并输出到机载设备和地面设备开展各类应用。

2　ADS-B 安全性分析

2.1　ADS-B 技术特点

基于1090ES数据链的ADS-B信号广播出去后，ADS-B地面站接收机载设备发出的ADS-B信号，实现ADS-B地空监视，管制人员根据监视信息进行空域管理。ADS-B广播信号或报文的完好性直接影响空域监视的准确性和安全性。基于1090ES数据链的ADS-B系统具有以下应用特点。

1) 采用脉冲位置调制（PPM, pulse position modulation），信息通过信号幅度表征。

2) 采用公开的1090 MHz点频收发。

3) 非独立监视，属于合作式监视。

4) 机载设备采用全向天线发射，地面站全向接收。

5) 明文广播，公开的校验机制。

6) 随机触发的报文发送时序。

7) 以S模式地址为基础的航迹关联方法。

2.2　ADS-B 系统缺陷

通过分析，ADS-B技术特点及其导致的应用缺陷如表1所示。

3　ADS-B 系统可能面临的风险

3.1　干扰攻击

ADS-B干扰攻击一方面如果在正常目标信号上叠加干扰信号，直接导致地面站无法正确解析出有效信号，称为交织干扰；另一方面通过产生海量的假目标的方式，超出地面站自身处理能力，无法输出正常可用的目标航迹，导致管制员无法获取空中态势信息，称为饱和干扰。

表1　　ADS-B 系统的安全性缺陷及常见的攻击手段

序号	技术特点	应用缺陷
1	采用PPM，信息通过载波的幅度表征	信号易受多径效应影响
2	采用公开的1090 MHz点频收发	1) 采用固定公开频率，容易受到同频干扰； 2) 采用单一频点，容易受到恶意欺骗干扰
3	非独立监视，属于合作式监视	1) 监视信息受到合作方的影响； 2) 易于受到合作方的主动欺骗干扰，被虚假信息混淆
4	常规设备中，机载设备采用全向天线发射，地面站全向接收	1) 容易受到来自各方位的信号干扰，系统容易饱和； 2) 无法区分信号来向，且无法验证ADS-B信息真伪
5	明文广播，公开的校验机制	1) 不具备保密机制，易于被恶意入侵和干扰欺骗； 2) 真实目标信息容易被检测和恶意篡改转播
6	随机触发的报文发送时序	1) 无法根据时域信息对真伪目标进行区分； 2) 真实目标信号容易被虚假信号交织，导致无法成功译码而丢失目标

3.1.1　交织干扰

传统的空管二次雷达通过在飞机上加装一个自动应答的装置（应答机），采用主动询问-被动应答的方式识别我方飞机。地面二次雷达称为询问器，其询问电波采用1030 MHz无线电波、飞机上的机载设备称为应答机，其应答电波采用1090 MHz无线电波。由此可见，ADS-B系统与机载雷达应答机采用相同的工作频率。如果在某一方向同时存在1090 MHz同频信号，由于工作信道的容量有限，空间中信号的密度会相应增大，且这些信号在空间传输过程中容易受到多径反射，这些信号发生碰撞的概率也会增大，导致地面站接收到的ADS-B信号严重失真以至于解调失败，这就是所谓的交织干扰。

3.1.2　饱和干扰

若某一区域存在ADS-B干扰源，通过模拟ADS-B信号生成海量的虚假目标。如果这些信号被ADS-B地面站接收后，未被识别并过滤，将会对地面站数据处理带来沉重负担，且真实目标会被淹没在海量的虚假目标之中，让管制员“无所适从”。

3.2　欺骗攻击

3.2.1　虚假目标欺骗

某一ADS-B干扰源通过产生标准格式的ADS-B报文以模拟虚假目标，若地面站将其视为真实ADS-B信号并加以解析，则在输出端会同时显示真实目标和虚假目标，给管制员造成严重干扰。虚假目标欺骗攻击原理如图2所示。

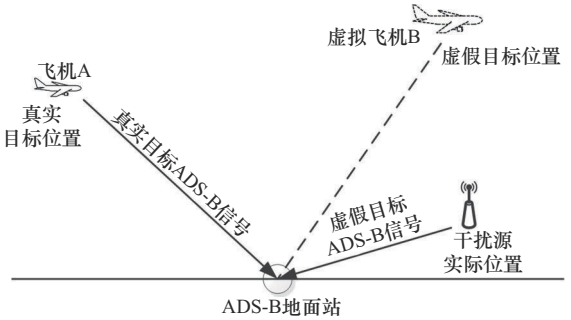

图2　虚假目标欺骗攻击原理

3.2.2　记录重放欺骗

若某一干扰源将接收到的真实目标ADS-B报文的时间信息进行延迟后广播出去，地面站接收并解析后，会产生2条真假难辨的航迹，管制员同样无法获取真实空中态势，导致发出错误指令，影响飞行安全。记录重放欺骗攻击原理如图3所示。

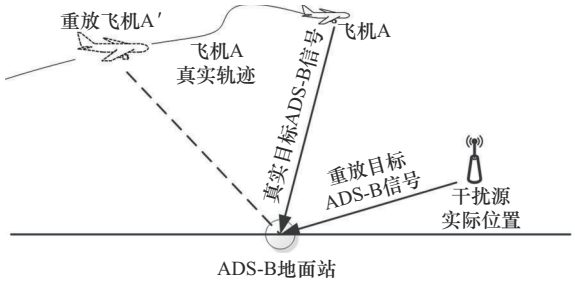

图3　记录重放欺骗攻击原理

3.2.3　报文篡改欺骗

一般情况下，ADS-B报文均以相对固定的周期进行广播；当应答机设置紧急代码时，也会触发ADS-B广播对应的紧急状态报文（如机械故障等）。干扰源通过接收空中真实飞机的ADS-B报文，对报文中的S模式地址、实时位置、速度、高度、航向等数据进行恶意篡改，然后转播出去，地面站会同时接收到这些符合格式的有效ADS-B报文以及真实飞机的ADS-B报文，从而受到严重欺骗干扰。报文篡改欺骗攻击原理如图4所示。

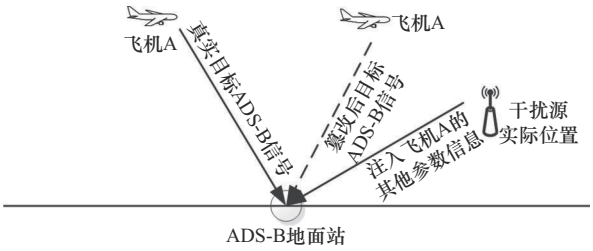

图4　报文篡改欺骗攻击原理

4　ADS-B抗干扰防欺骗技术途径

4.1　抗干扰技术途径

4.1.1　抗交织干扰手段

交织干扰是影响ADS-B监视能力、导致目标航迹不连续的一个重要原因。通过分析交织干扰的工作机制和影响因素可知，交织干扰的恶劣程度与飞行器数量（或空中报文数量）直接相关，因此可以利用天线方向性特征，通过空域覆盖分区管理，使空中信号只在所对应的空域方向上被接收，信号交织严重的空域方向不会影响其他空域方向的ADS-B信号接收，这种分区管理方法实现信号在方向上的隔离，最终降低了全空域方向上的ADS-B信号碰撞概率，交织干扰仅影响对应空域方向的目标；同时可对干扰ADS-B信号的空域方向进行隔离处理，降低干扰对全系统的影响，如图5所示。

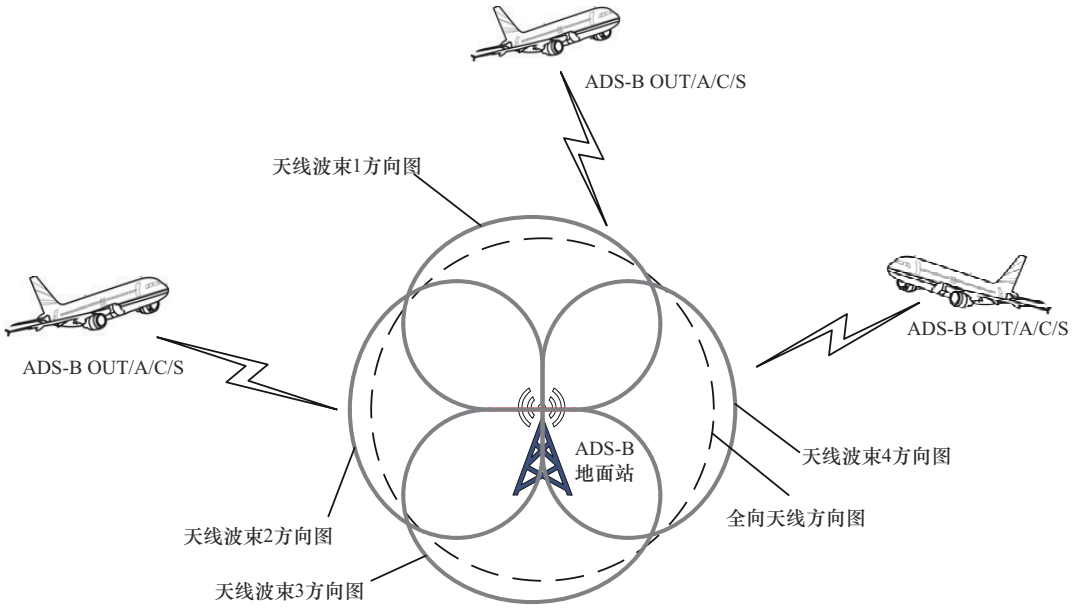

图5　交织干扰示意

4.1.2　抗饱和干扰手段

常规的ADS-B地面站采用全向天线接收，没有天线接收方向选择能力，大量虚假目标信号被接收而导致系统处理能力阻塞，系统很难处理饱和干扰。一旦出现这种干扰情况，地面站功能可能直接失效。一般地，干扰源的数量有限，很难实现全空域（水平360°范围）发射大量的干扰信号进行饱和干扰。因此，地面站可以对ADS-B信号发射源方位进行测量，在ADS-B航迹跟踪处理之前，建立ADS-B原始报文接收数量——信号方位的关系，当某个方位出现饱和干扰时，对应方位的ADS-B原始报文接收数量将明显增多，异于其他未受干扰方位。据此，可估计干扰源的方向，将该方向对应的天线波束置零，而其他方向对应的天线波束正常工作，从而对干扰方向的ADS-B报文进行剔除，有效消除饱和干扰带来的影响，如图6所示。

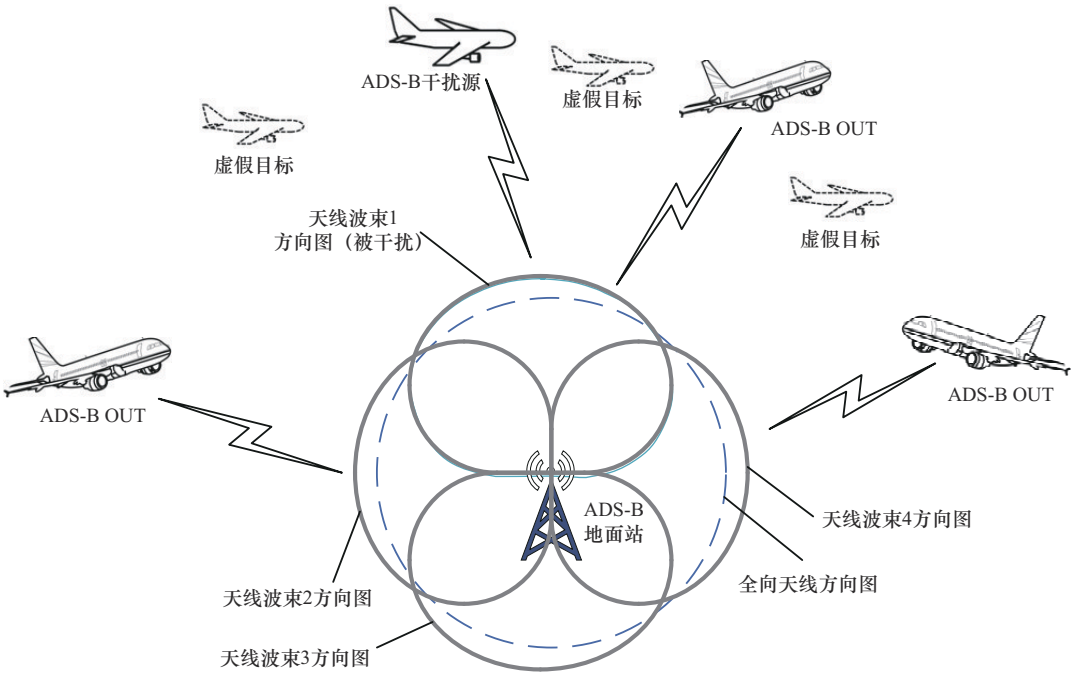

图6　抗饱和干扰原理示意

表2 抗干扰防欺骗ADS-B技术途径说明

威胁类型		技术手段	备注
干扰	交织干扰	空域覆盖分区管理	分区管理方法实现信号在方向上的隔离，最终降低了全空域方向上的ADS-B信号碰撞概率
		ADS-B增强译码技术	利用循环冗余校验（CRC）配合PPM信号的时域波形特征，实现对ADS-B数据的增强纠错能力
	饱和干扰	空域覆盖分区管理	攻击覆盖范围有限，通过天线设计隔离覆盖空域
		ADS-B增强译码技术	利用循环冗余校验配合PPM信号的时域波形特征，实现对ADS-B数据的增强纠错能力
		报文方位流量监视	建立报文数量随方位的关系，检测异常报文数量对应的方位，屏蔽该方位ADS-B数据，避免数据处理过载
欺骗	虚假目标欺骗 记录重放欺骗 报文篡改欺骗	目标方位一致性验证	虚假目标的信号发射源位置（距离、方位角以及俯仰角/高度）与报告位置不一致

4.2 防欺骗技术途径

通过虚假目标欺骗、记录重放欺骗和报文篡改欺骗攻击原理可知，3种欺骗攻击的一个共同特点是干扰源实际位置与虚假ADS-B信号报告的目标位置不一致。因此，可以利用到达时间差/到达时间计算目标真实位置，并进一步与ADS-B信号报告的目标位置进行比对。若两者一致，则认为该目标为真实目标，否则，判断为虚假目标。

综上所述，ADS-B面临的威胁类型及可用的抗干扰防欺骗手段如表2所示。

5 结束语

ADS-B技术是航空监视技术的一次飞跃，更是空管领域的一场技术革命。但由于其技术公开性，ADS-B系统同时面临着日益严峻的人为干扰和虚假欺骗问题，使管制员承受较大的安全压力。针对该问题，本文详细分析了传统ADS-B系统可能面临的干扰和欺骗风险，并从技术角度提出相应的抗干扰防欺骗手段，为建设具有抗干扰防欺骗功能的ADS-B系统和保障飞行安全提供技术支撑。

参考文献：

[1] 李自俊. ADS-B广播式自动相关监视原理及未来的发展和应用[J]. 中国民航飞行学院学报, 2008, 19(5): 11-14.
LI Z J. Principle, future development and application of ADS-B broadcast automatic correlation monitoring[J]. Journal of Civil Aviation Flight University of China, 2008, 19(5): 11-14.

[2] 马晓东, 袁伟娜, 凌小峰. 一种基于机会参考源的分布式ADS-B无源定位防欺骗方法[J]. 华东理工大学学报(自然科学版), 2020, 46(1): 121-127.
MA X D, YUAN W N, LING X F. Distributed ADS-B passive positioning anti-spoofing method based on opportunity reference source[J]. Journal of East China University of Science and Technology, 2020, 46(1): 121-127.

[3] 颜可壹, 吕泽均, 时宏伟, 等. 基于TDOA/TSOA的ADS-B系统防欺骗技术[J]. 计算机应用研究, 2015, 32(8): 2272-2275.
YAN K Y, LYU Z J, SHI H W, et al. ADS-B system anti cheat technology based on TDOA/TSOA[J]. Application Research of Computers, 2015, 32(8): 2272-2275.

[4] 李武旭, 李君惠, 李宏. 采用阵列信号技术的ADS-B系统抗干扰研究[J]. 舰船电子工程, 2022, 42(8): 74-80.
LI W X, LI J H, LI H. Research on improving the robustness of ADS-B system using array signal technology[J]. Ship Electronic Engineering, 2022, 42(8): 74-80.

[作者简介]

孙保明（1989– ），男，河南周口人，博士，91977部队工程师，主要研究方向为信号处理、空管通信。

陈娟（1981– ），女，江苏盱眙人，91977部队工程师，主要研究方向为空管通信、计算机技术。

谷志鸣（1988– ），男，河北石家庄人，91977部队工程师，主要研究方向为航空管制、航空监视。