空管监视系统中的无线通信技术及安全性分析

李 丹[1],张 晓[2]
(1.中国西南电子技术研究所,四川 成都 610036;2.空军装备部驻成都地区第三军事代表室,四川 成都 610036)

摘 要:空管监视领域不断更替的新概念与新技术对准确认识其运行机制提出了愈加多元的需求,其中安全性研究作为基本问题之一,由于贯穿空管监视系统的各个层面而成为认识系统涌现的重要线索。基于空管监视领域的安全研究尚未形成明晰体系的现状,重点介绍了当前空管监视系统中的无线通信技术以及面临的安全性问题,将空管监视系统分为两大类:空中交通管制和信息服务。空中交通管制用于管制员与机组人员之间的通信,信息服务主要为机组人员提供飞行所需信息,提高飞行员的情景意识。最后指出了空管监视领域尚待解决的安全性问题,及未来的关注热点及研究趋势。

关键词:空管监视;空中交通管制;信息服务;无线通信;安全性
中图分类号:TN95;V249 **文献标识码**:A **DOI**:10.16157/j.issn.0258-7998.200332

中文引用格式:李丹,张晓. 空管监视系统中的无线通信技术及安全性分析[J].电子技术应用,2020,46(9):29-33.
英文引用格式:Li Dan,Zhang Xiao. Wireless communication technologies and security in air traffic surveillance system[J]. Application of Electronic Technique,2020,46(9):29-33.

Wireless communication technologies and security in air traffic surveillance system

Li Dan[1],Zhang Xiao[2]
(1.Southwest Institute of Electronic Technology,Chengdu 610036,China;
2.The Third Military Representative Office of the Air Force Equipment Department in Chengdu,Chengdu 610036,China)

Abstract:The continual development of new concepts and techniques in the field of air traffic surveillance generates constantly more diversified demands for an accurate understanding of its operating mechanism. Security research, which deals with one of the fundamental issues of air traffic surveillance, emerges throughout the system at all levels, and provides important clues for exploring the emergence of air traffic surveillance system. However, there is as yet no widely accepted architecture for security research on air traffic surveillance up to now. Therefore, this article focuses on wireless communication technologies and security in air traffic surveillance system. In order to focus on the systems view, we divide all technologies used in air traffic communications into two categories according to their application: air traffic control and information services. Air traffic control are used to enable communication between controllers and pilots or their aircraft. Information services are technologies which provide information to pilots to improve their situational awareness. It also points out the future research and development trends in the field of air traffic surveillance and some key issues which remain to be solved.

Key words:air traffic surveillance;air traffic control;information service;wireless communication;security

0 引言

空管监视系统被誉为空中交通管制员的“眼睛”,主要是指检测、识别和跟踪目标以及报告影响飞行安全的天气现象。空管领域的监视手段种类繁多,尤其是近年来随着数据链及卫星技术的发展以及飞行密度的增加,出现了多种空管监视新技术,ADS-B、ADS-C、雷达、多点定位、视频监控等技术共存,每种监视手段基于自身的技术特点都具有各自的适用范围和监视性能,为了最优地利用各种空域监视技术,实现飞机状态的实时可信监视,基于多种手段的监视技术开始出现[1-6]。

信息安全一直是空管监视系统中非常敏感和关键的问题。由于空管报文大多是开放的数据格式,信息无加密或加密算法过于简单,通信链路公开、信息共享,地面监视设备与空域内飞机之间以网状和多点对多点的方式完成信息传递,不可避免面临着安全性威胁[7-9]。

1 空管监视系统中的无线通信技术

从系统应用层面讲,把空管监视系统中的无线通信技术分为两大类:空中交通管制和信息服务。空中交通管制用于地面管制员与机组人员之间的通信,在整个飞行阶段都要使用,包括甚高频/高频话音通信(VHF,Very High Frequency/HF:High Frequency)、一次监视雷达(PSR,Primary Surveillance Radar)、二次监视雷达(SSR,Secondary

Surveillance Radar)、广播式自动相关监视(ADS-B,Automatic Dependent Surveillance-Broadcast)、多点定位系统(MLAT,Multilateration)和管制员-飞行员数据链通信(CPDLC,Controller Pilot Data Link Communications)。信息服务主要为机组人员提供飞行所需信息,比如天气状况和交通信息等,提高飞行员的情景意识,包括飞机通信寻址与报告系统(ACARS,Aircraft Communications Addressing and Reporting System)、交通预警和防撞系统(TCAS,Traffic Alert and Collision Avoidance System),广播式飞行情报服务(FIS-B,Flight Information System-Broadcast)和广播式交通信息服务(TIS-B,Traffic Information System-Broadcast)。空管监视系统中的空-天-地无线通信技术如图1所示。

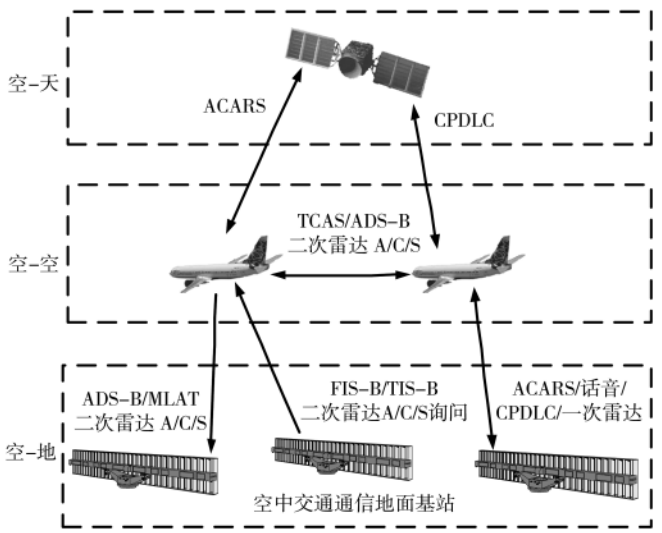

图1 空管监视系统中的空-天-地无线通信技术

1.1 空中交通管制

1.1.1 话音通信

话音通信(VHF/HF)是管制员和飞行员之间最主要的通信方式。飞行员通过地-空通话,在规定的报告点向管制员报告飞经的时间、飞行高度、飞行请求等,便于管制员及时确定和掌握航空器的交通态势。HF通常用于越洋航线和边远地区上空等超视距的远程通信联络。但话音通信本身仍然存在较多弊端,随着全球飞机数量的迅速增长,VHF通道十分拥挤,地-空、空-空、地-地之间传输的数据日益增多,基于无线电话音的通信方式无法满足当今的需求。

1.1.2 管制员-飞行员数据链通信(CPDLC)

管制员-飞行员数据链通信(CPDLC)是一种新型的地-空双向数据链,支持管制员和飞行员之间数据报文的直接交换,是管制员和飞行员之间利用数据替代话音的空中交通管制通信手段,可以作为空-地语音通话的有效补充。为弥补话音通信信号失真、延迟较大等不足,CPDLC作为一种适应新一代航行系统的新型通信技术在1993年应运而生,管制员和飞行员之间可进行文本信息交换和共享,包括申请、放行、请求、自由电文等。具有以下优点:

(1)通信消息为文本形式,为操作者提供实时显示,减少人为差错;

(2)通信消息可复制、粘贴、存储,便于随时查阅;

(3)可根据需求和空域能力,飞行员和管制员自主选择收发信息。

一些繁忙机场已经部署应用CPDLC数据链,辅助管制员进行地-空通信。管制员还可以通过CPDLC在以前VHF话音通信无法覆盖的区域内进行管制,包括沙漠地区以及越洋飞行的航线。

1.1.3 一次监视雷达(PSR)

一次监视雷达是最早应用在空管监视系统中的雷达,不需要被监视者配合,是一种由监视者独立完成对被监视者测量定位的监视方式。其利用无线电波来定位目标和确定目标距离。雷达发射的电磁波,碰到目标(如飞机)后反射,地面一次雷达根据接收到的反射信号与发射信号的时间差来测距,同时天线发射的窄波束是和天线旋转扫描同步的,通过测量天线在发现目标时的方位角来确定目标方位。这些位置信息在雷达屏幕上以光点的形式呈现给管制员。

目前,一次监视雷达是空中交通管制员保持对管制区域内所有飞机进行监视的唯一方法。一次监视雷达的产生,大大提高了空域监视技术水平。它摆脱了天气、地形变化以及人为等因素对飞行安全的影响,并且一次雷达监视的精度远高于基于话音通信的飞行员位置报告和管制员人工推算的精度,可缩小飞机之间的飞行间隔,空域利用率得到提高。但一次雷达本身仍然存在较多弊端,比如无法识别被监视目标的身份及高度信息、发射功率大、容易受到地面杂波的干扰、受制于被监视目标的雷达截面积、造价成本高等。

1.1.4 二次监视雷达(SSR)

二次监视雷达通过地面站对空中目标进行询问,机载应答机在接收到询问信号后进行应答。二次雷达不依赖于机载应答机来对目标进行定位,而是通过测量波束反射的方向和时间来确定目标位置。二次雷达向空中交通管制系统传输的信息以标牌的形式在屏幕上显示。

为了解决A/C模式航管二次雷达的同步串扰和异步干扰以及传输数据量有限等问题,引入了S模式二次雷达。它将二次雷达和S数据链相结合,可提供未来空中交通自动化管理所需的通信和监视能力,可用于终端区域及高飞行密度空域的空中交通监视。由于给每架飞机指定一个唯一的24 bit的地址码,地面询问机可进行“一对一”的选择呼叫,防止所有飞机同时应答时引起应答信号叠加、解码错误、系统饱和、显示混叠等问题。通过S模式数据链功能,能够互传更多的消息,同时也为VHF话音通信提供了备份,对S模式数据链进行扩展后为1090ES,可用于作为ADS-B的数据链,用于广播发

送飞机自身的 ADS 报文。相比于一次雷达，二次雷达具有发射功率小、干扰杂波少以及不存在目标闪烁的现象等优点，并且由于数据链的引入，地-空通信的信息更加丰富。

1.1.5 广播式自动相关监视(ADS-B)

广播式自动相关监视技术(ADS-B)是地-空通信数据链及空-空通信数据链中的一项关键技术，自动相关监视系统是国际民航组织推荐使用的空中交通管理监视系统。由于其定位精度高、抗干扰能力强、传递信息内容丰富、投入成本低等优点，ADS-B 技术近年来已经成为许多国家进行空管监视的主要技术手段。ADS-B OUT 依靠卫星导航接收设备来对本飞机进行精确定位，并以特定的间隔向空中广播自身的位置、速度等飞行信息，ADS-B IN 接收其他飞行器广播的消息，全面了解周边空域交通状况。其系统架构如图 2 所示。

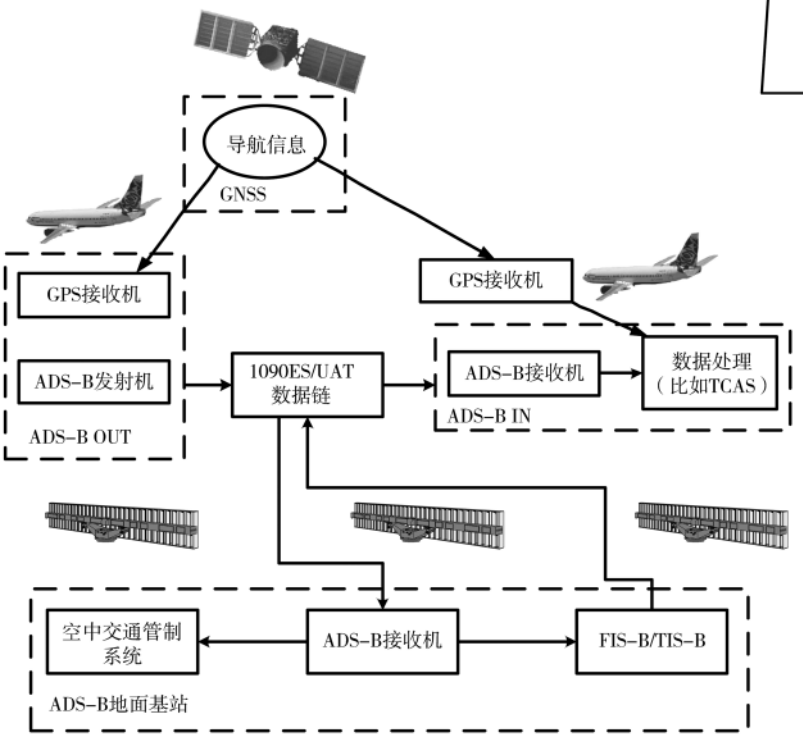

图 2 ADS-B 系统架构

1.1.6 多点定位系统(MLAT)

多点定位系统通过地面多点定位接收机接收飞机上现有机载应答机发射的 1 090 MHz 二次雷达 A/C/S 模式应答信号或者 ADS-B 信号，来实现对飞机的精准定位。多点定位系统工作原理图如图 3 所示。在同一时刻，目标至少被四个地面台站检测并解码，然后将数据传送至中央处理器。中央处理器比较来自多个地面台站的报告，根据每个地面台站的信号接收时间，从而计算得出目标位置，并通过高刷新率来跟踪定位目标，确定其运行航迹。

按照是否发射询问信号，多点定位系统可分为有源和无源两种，无源定位系统自身并不产生射频信号，仅由接收站点组成，系统本身不会对现有电磁环境产生额外干扰，但是其接收到的航管 A/C/S 应答信号并不规律且不可控。有源定位系统具有一个或多个发送设备，可以自主发射 1 030 MHz 的询问脉冲和 1 090 MHz 的应答脉冲，以便自主对装备有应答机的飞机进行询问。其中 1 030 MHz 的询问脉冲主要用于 A/C/S 模式的询问，A/C/S 询问模式交替进行，1 090 MHz 的应答脉冲一般仅用于发射下行链路格式为 DF=17 的 S 模式扩展报文。有源定位系统会对现有电磁环境产生干扰，因此有源多点定位系统尽可能地降低 A/C 模式的询问频率来减少对周边二次雷达和目标应答机的影响。

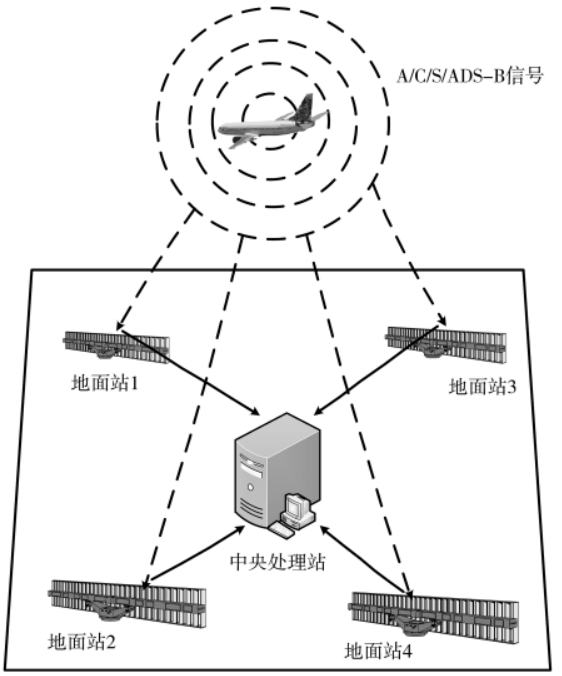

图 3 多点定位系统架构

多点定位系统由于其易安装、低成本、高精度等优点，在世界很多地方已经广泛应用，如我国的首都机场、美国以及欧洲的很多机场均已经应用，逐步取代一次雷达和二次雷达等传统监视设备。下一代空管监视系统将会广泛采用多点定位技术。但是其仍然存在弊端，理论上讲，多点定位技术只需要三或四个地面台站即可确定被监视目标的位置，但是在实际应用中考虑到遮挡、探测成功率以及冗余度等多方面的因素，地面台站的数量一般要更多，地面台站的选择是多点定位系统中非常重要的技术问题。比如英国希斯罗机场使用 15 个地面台站，德国法兰克福机场使用 19 个地面台站。接收应答信号的地面台站越多，进行定位求解所需的计算量也会越大，并且存在大量的信息冗余。

1.2 信息服务

1.2.1 飞机通信寻址与报告系统(ACARS)

ACARS 是一种通过无线电或卫星在地面站和飞机之间传输短消息(报文)的数字数据链系统。一般由机载设备、数据服务提供商、地面处理子系统三部分组成。其工作原理是:机载设备把飞机上各传感器提供的飞行状态数据收集上来,并处理成数据链报文发射给地面站,地面站通过信息中心把报文数据传送给航空公司运控中心、飞行管理、空中交通管理等相关部门。同样,上行数据链报文从地面发送,经 ACARS 机载设备接收处理后显示在机载输出设备上供机组使用。ACARS 报文的收发不需要飞行员手动操作。

机载 ACARS 可利用 VHF3(甚高频 3 号通信系统),HF(高频通信系统)或者卫星通信系统三种不同的方式与地面进行数据交互,一般使用国际民航专用的甚高频通信频段,标准的数据链频率有131.450 MHz、131.475 MHz、131.550 MHz 和 131.725 MHz。通过 ACARS 地空数据的实时交互,可在远距离时对飞机实时监控,在落地前飞机将健康管理系统所报飞机故障信息以及发动机参数信息传回地面,便于航空机务维修部门提前对飞机故障进行诊断,制定维修方案,提高故障排查效率。

1.2.2 交通预警和防撞系统(TCAS)

TCAS 可以监视本架飞机周围空域中其他飞机的存在、位置以及运动状况,能够帮助飞行员正确识别本机邻近空域的交通状况,主动地采取回避措施,防止与其他飞机危险接近。TCAS 由机载询问机、应答机、收发机和计算机组成。为了减少无线电干扰,TCAS 发射功率一般有所限制。

目前民航飞机以安装 TCAS II 的空中交通防撞系统为主,能够快速探测到本机监视范围内 A/C/S 模式应答机,在本机和入侵飞机之间运用防撞算法计算出威胁等级并进行跟踪和威胁评估,当两架飞机的进近最小接近点小于 48 s 时,进行交通咨询,若仍存在碰撞危险,则以音频和视频的方式指导飞行员进行冲突解脱。

把机载接收到的 ADS-B 信号应用到 TCAS 监视系统中,减少 TCAS 主动发射询问信号频率,减少电磁环境干扰,同时提高 TCAS 系统的监视范围和冲突检测精度,增强防撞告警功能,因此推广 ADS-B 技术在交通预警和防撞系统中的应用是未来发展方向之一。

1.2.3 广播式飞行情报服务(FIS-B)

地面管制中心将气象信息和飞行情报信息通过 FIS-B 数据链上传给安装有 ADS-B IN 设备的飞机。采用 UAT 数据链通信协议,工作在特定的 978 MHz 公共宽带信道上。FIS-B 是 ADS-B 功能的拓展应用,所传送的气象和航行情报等信息可以使机组实时了解空域限制条件及航路气象状况等运行相关信息。

1.2.4 广播式交通信息服务(TIS-B)

为实现对没有安装 ADS-B OUT 设备的飞机进行监视,地面管制中心将通过其他系统获得的飞机位置等相关监视信息通过上行数据链 TIS-B 传给装有 ADS-B IN 设备的飞机,显示在 CDTI 上,提高飞行员对飞机周围交通状况的感知能力,提高情景意识,TIS-B 提供了不同监视系统间(一次雷达、二次雷达、ADS-B、MLAT)的互通手段。

2 空管监视系统面临的安全问题

信息安全一直是空管监视系统中非常敏感和关键的问题。由于空管报文大多是开放的数据格式,信息无加密或加密算法过于简单,通信链路公开、信息共享,地面监视设备与空域内飞机之间以网状和多点对多点的方式完成信息传递,不可避免面临着安全性威胁[7-12]。安全威胁又可进一步分为被动攻击和主动攻击。被动攻击不对信息进行修改,只对其进行窃取。主动攻击却对信息进行故意篡改(如修改某飞机的航行信息等)。相对于被动攻击,主动攻击对于空管监视系统的安全威胁更大。针对空管监视系统中无线通信技术的弱点,信息安全问题主要有信息窃取、阻塞、消息注入、消息删除、消息篡改。

2.1 信息窃取

信息窃取是实施攻击的基础,通过蓄意监听飞机广播信息,能够很容易地得到飞机的识别代码及身份等信息,对于执行特殊任务的军用飞机或者搭载重要人物的政府飞机来说,飞机身份的暴露是非常危险的。各种空管监视系统,能够使地面管制人员监视飞机的位置,同时对于不法分子,只需要一个简易的接收设备及天线,也同样能获得飞机的相关飞行信息,增加了飞行安全风险,广播式传输模型中相关飞行信息的暴露成为学术界和工业界应用争论的焦点问题之一[10]。

2.2 阻塞

无线电信号的干扰是破坏空管监视系统正常运行非常容易且有效的手段。在特定工作频率上,比如 1 090 MHz(对于二次雷达和 ADS-B),一台高功率的无线电信号发射设备发射阻塞式干扰信号,就可以干扰空中交通管制信号的正常接收。阻塞干扰源可能是本机的一次雷达设备、周边无线通信发射台、商业广播电台发射塔,也可能是不法分子故意设置的。大多数国家已经制定了相关法律法规禁止恶意对空中交通管制系统工作频率的阻塞干扰,然而这对空管监视系统来说是不够的。

2.3 消息注入

由于空管监视系统中的大多数通信技术(ADS-B,TIS-B,FIS-B,SSR,TCAS)均是通过无线链路进行无加密方式传输,在数据链路层没有相关加密和身份验证措施。利用计算机模拟出特定格式的虚假信号,使用一套天线加简易的接收发射设备,播发伪造的虚假目标信号,导致幽灵飞机注入空管监视系统,屏幕上显示虚假混乱目标,影响空中交通管制的正常运行。如图 4 所示,在雷达显示屏上除了显示出由一次雷达和二次雷达探测到的合法目标外,还有被攻击者注入的虚假目标 ADSB5,ADSB6,管制员如果不能辨别此消息的真伪,会严重威

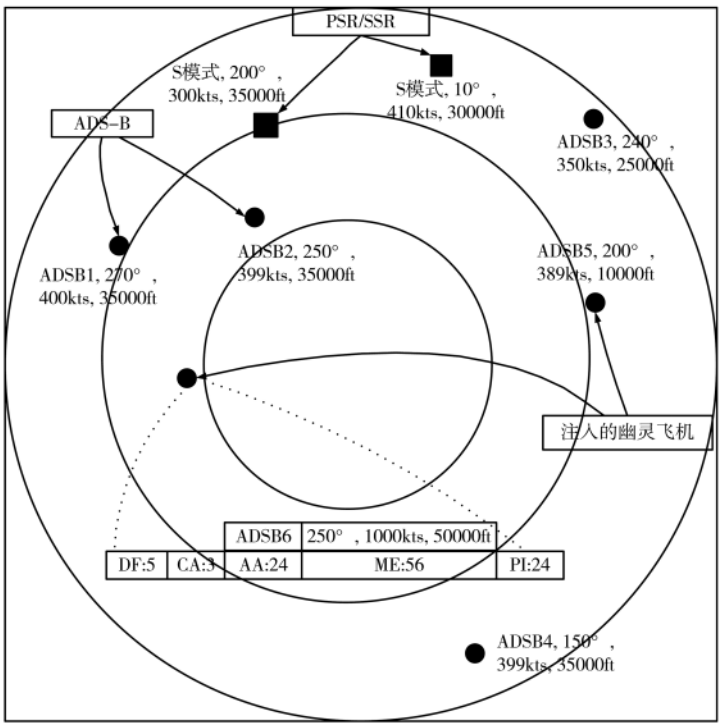

图 4 消息注入攻击效果图

胁到航空飞行安全。

2.4 消息删除

在地-空通信中，攻击者采取一定手段(破坏性干扰或建设性干扰)对链路中的特定合法消息进行物理删除，使其在地面管制显示界面上完全消失。破坏性干扰是攻击者发射出和合法发射方广播完全相反的信号，两者信号互相抵消，这种方式由于需要精准复杂的时序要求，实际运用有难度。建设性干扰则不需要时序同步要求，只要干扰合法消息中的一段，使比特位传输错误即可达到物理删除的目的。比如 S 模式扩展应答机中，CRC 校验纠正算法可以最多纠正出 5 个比特位的传输错误，如果一条消息中有超过 5 个比特位传输错误，接收设备会丢弃此包数据。建设性干扰效能取决于具体的干扰实施方法及周边环境。

2.5 消息篡改

攻击者将窃听到的合法消息进行修改(如修改部分航行信息)后向飞机或者管制员发送出去，如果接收端不能辨别此消息的真伪，会造成不可预知的后果。攻击方进一步还可以使用消息注入和消息删除的组合方式来实现虚假信息的传递。消息篡改可为非法侵入、恐怖活动等非法行为提供掩护。

3 结论

空管监视系统需要通信双方鉴别对方端系统的身份、鉴别应用消息的来源并确保应用信息的完整性。空管监视系统地面和空-地边缘中间系统需要鉴别对方的边缘中间系统的身份、鉴别路由信息的来源并确保路由信息的完整性。综上所述，空管监视系统中的安全性研究及相关解决方案是空管监视领域内关注的热点，针对保护空管监视系统数据链路安全，相应的防欺骗抗干扰技术策略研究会成为空管监视领域未来的研究趋势。

参考文献

[1] 张军.空域监视技术的新进展及应用[J].航空学报，2011，32(1)：1-14.

[2] 张召悦.空管监视技术[M].北京：国防工业出版社，2017.

[3] MATTHIAS S，MARTIN S，MATTHEW S，et al.Open-Sky report 2017：mode S and ADS-B usage of military and other state aircraft[C].IEEE/AIAA 36th Digital Avionics Systems Conference(DASC)，2017.

[4] 程擎，代言君.基于终端区的多基一次监视雷达布局研究[J].计算机仿真，2017，34(2)：25-29.

[5] 卢爽，李成功，刘卫香.空中交通管理系统云仿真技术应用构想[J].指挥信息系统与技术，2017，8(2)：71-76.

[6] 潘乐义，侯惠峰，张增军.空管通信系统与技术发展[J].指挥信息系统与技术，2016，7(4)：66-71.

[7] TIM S，ANDREAS H，THORSTEN M，et al.Towards a more secure ATC voice communications system[C].IEEE/AIAA 34th Digital Avionics Systems Conference(DASC)，2015.

[8] MATTHEW S，DANIEL M，MARTIN S，et al.Undermining privacy in the aircraft communications addressing and reporting system(ACARS)[C].Proceedings on Privacy Enhancing Technologies，2018(3)：105-122.

[9] MILAN R，MICHAEL F.Using speech analysis in voice communication：a new approach to improve air traffic management security[C].IEEE/7th International Conference on Cognitive Infocommunications(CogInfoCom 2016)，2016：181-186.

[10] DANIEL M，PATRICK L，VINCENT L，et al.Investigation of multi-device location spoofing attacks on air traffic control and possible countermeasures[C].Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking(MobiCom).ACM，2016：375-386.

[11] SATHYA S，LUKE J，ROBERT J.Safety benefit of automatic dependent surveillance-broadcast traffic and weather uplink Services[J].Journal of Aerospace Information Systems，2015，12(8)：579-586.

[12] 杨成，林琳.ADS-B 数据链应用风险与对策研究[J].现代电子技术，2014，37(21)：98-101.

(收稿日期：2020-04-23)

作者简介：

李丹(1986-)，女，硕士，工程师，主要研究方向：航空电子学。

张晓(1987-)，男，本科，工程师，主要研究方向：航空电子、装备项目及质量管理。

版权声明