DOI:10.19651/j.cnki.emt.2417249

基于卡尔曼滤波的 ADS-B 虚假目标识别系统设计*

周苏宁 王 韬 班 恬
(南京理工大学电子工程与光电技术学院 南京 210094)

摘 要:为了应对虚假的广播式自动监视(ADS-B)信号对航迹信息带来的干扰,基于卡尔曼滤波对于飞行航迹的预测设计了一种对于 ADS-B 虚假目标的检测系统。报文解码基于软件无线电平台的 ADS-B 解调系统,在 Qt 端完成了解码校验部分并嵌入高德地图动态显示。制作了 ADS-B 虚假报文发射系统,并基于卡尔曼滤波完成了航迹预测部分。基于 ADS-B 预测数据的位置离散度,均方根误差设计了跳点率检测部分。根据实验测试,对于给出的虚假报文,成功检测到 90.4%的跳点。据此,该系统具有一定的 ADS-B 虚假目标检测能力。

关键词:ADS-B;航迹信息;卡尔曼滤波;假目标识别
中图分类号:TN713;TN973.3 **文献标识码**:A **国家标准学科分类代码**:510.1020

Design of an ADS-B false target identification system based on Kalman filtering

Zhou Suning Wang Tao Ban Tian
(School of Electronic and Optical Engineering, Nanjing University of Science and Technology, Nanjing 210094, China)

Abstract: In order to deal with the interference caused by false automatic dependent surveillance-broadcast (ADS-B) signals on flight trajectory information, a detection system for ADS-B false targets was designed based on Kalman filtering for the prediction of flight trajectories. The message decoding is based on an ADS-B demodulation system using a software-defined radio platform, with the decoding verification part completed on the Qt end and dynamically displayed using Gaode map. An ADS-B fake message transmission system was created, and the track prediction part was completed based on Kalman filtering. The jump rate detection part was designed based on the positional dispersion of the ADS-B predicted data and the root mean square error. According to experimental tests, for the given fake messages, 90.4% of the jumps were successfully detected. Therefore, this system has a certain capability to detect ADS-B false targets.

Keywords: ADS-B; trajectory information; Kalman filtering; false target identification

0 引 言

广播式自动相关监视技术[1](automatic dependent surveillance-broadcast,ADS-B)是一种自动从相关机载设备和全球导航卫星系统中获取参数,并向地面设备和其他航空器广播飞机的高度,速度,经纬度,航向,航班号等信息的监视技术[2]。因为其通信不受气候与地形的影响,可以达成全天候的实时通信。ADS-B 技术的发展使得空中交通管制更加容易,通过卫星导航系统能提高飞机的定位精度,并且可能在未来取代二级监视雷达[3]。然而,一方面,在 ADS-B 系统中,由于信号传输中存在各种干扰与丢包问题,导致数据本身完整性会受到一定的影响。另一方面,ADS-B 本身没有基本安全措施,如身份验证与加密,使得它们很容易被伪造或篡改,这会影响到传输飞机数据的可靠性与完整性,给航空管制带来了安全隐患。目前,已经有文献[4]介绍了 1 090 MHz 数据链存在的安全问题,详细讨论了 ADS-B 虚假目标的攻击种类与理论的应对措施,分析了检测方法优缺点和可行性,但缺乏具体的测试验证。也有文献[5]采用了导航源信息检测技术手段识别虚假目标,设计了基于地基增强系统(ground based augmentation systems,GBAS)完好性信息的 ADS-B 防欺骗算法,但该算法依赖消息报文中的导航不确定系数(navigation uncertainty coefficient,NUC)值,在虚假报文的 NUC 值和空中消息报文真实值相同的情况下,该方法将无法完成判

收稿日期:2024-10-31
*基金项目:南京理工大学研究生教育教学改革课题重点项目(KT2023A003)资助

别,因此具有一定的局限性。

为了解决以上问题,本文实现了一个基于卡尔曼滤波的虚假目标航迹识别系统。本文先对原本的 ADS-B 接收系统作了解码和航迹显示,然后用卡尔曼滤波对于实际的航迹数据进行了测试,并且用离散度距离标准差作为判定条件来甄别虚假目标,配合本身的接收与解码系统可以做到实时显示航迹与虚假目标甄别。该系统对于速度变化不大的客机,具有较高的预测精度。

第一部分,本文接收解调部分基于 Zynq-7000 系列的 ZedBoard 与软件无线电平台 AD9361,经过该系统可获得多条 112 位 ADS-B 报文,通过对报文进行解码和校验,可在 Qt 端嵌入网页地图完成动态显示,完成航迹显示系统。第二部分,本文通过卡尔曼滤波对 ADS-B 航迹进行位置预测,并通过对给定 ICAO 的飞机报文进行编码来完成假报文的制作。第三部分,本文通过对真实飞机航迹数据进行 500 个点的航迹预测实验,计算了离散度距离标准差和跳点率,设定了跳点判定方式,并在 Qt 中制作了跳点检测模块。最后,本文进行了跳点率检测的实验,通过在所有报文中加入 50 条制作的虚假报文并进行了 10 次测试,该系统识别了制作的 90.4%的伪目标点,验证了该系统具有一定的跳点检测能力。

1 ADS-B 接收与解码系统

1.1 硬件与软件平台

本系统接收解调部分的硬件实物如图 1 所示。

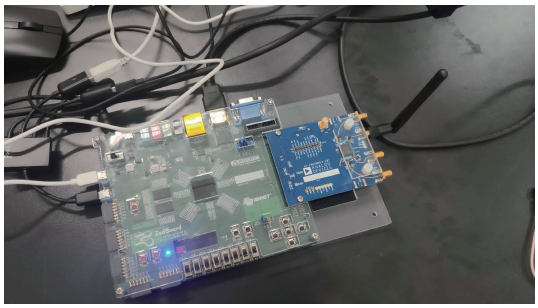

图 1 无线电接收系统

Fig. 1 Radio receiving system

由 ADI 公司的 AD9361 作为前端信号接收芯片,Xilinx 公司的 Zynq-7000 作为信号处理芯片,通过天线接收广播的无线电信号送到射频前端芯片 AD9361,经过混频、模拟滤波、模数转换器(analogue-to-digital conversion,ADC)、数字滤波等过程转换为基带信号[6],基带信号通过 FMC 接口送到 Zynq-7000 中,经过非相干解调算法将基带信号解调为相应的报文信息并且送到与芯片相连的外设中。

解码显示的软件平台选择 Qt5.9.9,Qt 具有跨平台强,库丰富,灵活性和扩展性强的特点,通过在 Qt 中与 web 网页进行交互,可以将高德地图,百度地图等网页嵌入在 Qt 界面中,并通过控件移动来方便对航迹进行直观绘制。最终将 Qt 端虚假目标仿真测试通过后,可将 Qt 程序移植到 Zynq-7000 中,与前端的接收解调系统相结合,实现一套完整的 ADS-B 航迹目标接收与虚假目标检测系统。

1.2 报文解码流程

如图 2 所示为 Qt 解码的软件流程,根据 1090ES ADS-B 报文标准,报文长度为 112 位,由 88 位数据位和 24 位校验位构成,首先要根据解调端拿到的报文数据,进行位数的检测,把合格的报文送到循环冗余校验(cyclic redundancy check,CRC)模块,通过 CRC 校验的则是有效的 ADS-B 报文。下一步,判断输入的数据报文类型,ADS-B 报文有 3 种报文类型,分别对应:身份、速度、位置,需要根据下行链路格式 DF(downlink format,DF)和数据字段 ME(message,ME)来进行解码。当 DF=17,ME 的前 5 位类型编码为 1~4 时,报文为飞行速度信息。56 位 ME 字段的 9~56 位为飞机的 8 位身份信息(identity,ID)。当 DF=17 时,ME 的前 5 位类型编码为 9~18,20~22 时,报文为飞行位置信息,其 22~56 位为经纬度信息,采用压缩位置报告(compact position reporting,CPR)编码方式,本系统采用本地解码的方式。当 DF=17,ME 前 5 位类型编码为 19 时,报文为飞行速度信息,其 14~35 位为水平速度位,包含了飞机的南北方向的速度以及角度,38~46 位为垂直速度。在对数据完成读取和校验后,本文将对应类型的数据根据对应解码步骤和公式解出飞机的相关数据,在 Qt 窗口右侧进行显示,与网页端飞机图标相互对应。同时将位置数据和速度数据通过 Qt 的 web 模块送到高德地图的接

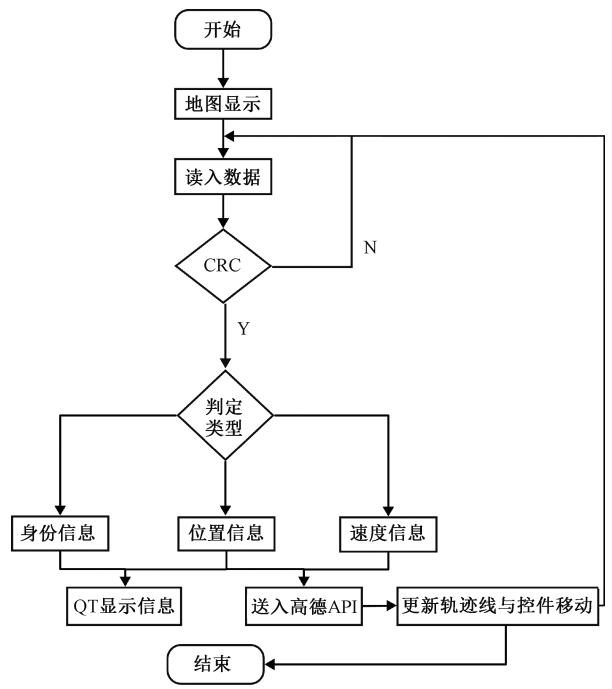

图 2 ADS-B 报文解码流程图

Fig. 2 ADS-B message decoding flowchart

口中，通过地图接口中的控件和画线功能，在高德地图网页上绘制动态轨迹线。

1.3　Qt 端飞机实时航迹显示

接收机所处的经纬度坐标为(118.855 6，32.028 9)，根据理论结果，接收到的 ADS-B 报文的经纬度应当在中心坐标附近。根据接收机测试结果，最远接收距离约为 100 km，因此解码飞机的定位不应超过接收机的接收范围，否则代表无效数据。通过解码获取的报文后可以在上位机 Qt 高德地图端观察到附近的飞机并以地图控件形式模拟飞机移动。在 Qt 信息显示端可以观察到目标飞机的相关信息，包括 ICAO 号，高度，经纬度，水平和垂直速度等，如图 3 所示，该组数据为本文的 ADS-B 接收系统获取的。通过获取每组报文的时间戳，并且根据解码出来的经纬度以及高度数据，对比了 Flightradar24 软件上的实时信息，如图 4 所示。同时查询了 MU9775 真实航班信息，如图 5 所示，验证了本文的接收系统的报文实时性。为了对飞机航迹进行航迹预测，本文重点关注飞机的经度、纬度，航向以及水平方向的速度信息。

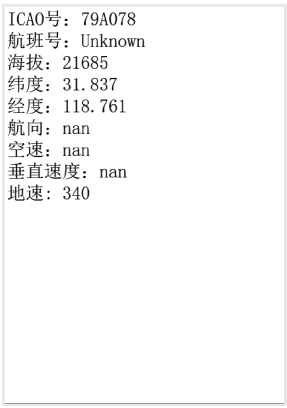

图 3　ADS-B 航迹信息端显示

Fig. 3　ADS-B track information display

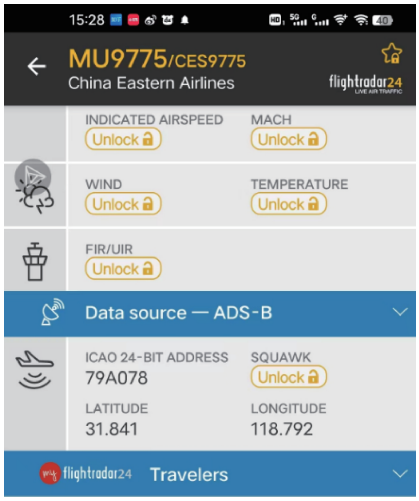

图 4　Flightradar24 实时航迹

Fig. 4　Flightradar24 real-time flight tracking

星期一 2024年11月18日	14:53 CST Wuxi - WUX	17:46 CST Chongqing Jiangbei Int'l - CKG	A321	2小时53分
星期日 2024年11月17日	14:55 CST Wuxi - WUX	17:30 CST Chongqing Jiangbei Int'l - CKG	A320	2小时35分
星期六 2024年11月16日	14:03 CST Wuxi - WUX	16:40 CST Chongqing Jiangbei Int'l - CKG	A320	2小时37分
星期五 2024年11月15日	14:11 CST Wuxi - WUX	16:54 CST Chongqing Jiangbei Int'l - CKG	A321	2小时43分
星期四 2024年11月14日	14:10 CST Wuxi - WUX	16:50 CST Chongqing Jiangbei Int'l - CKG	A321	2小时40分
星期三 2024年11月13日	14:46 CST Wuxi - WUX	17:21 CST Chongqing Jiangbei Int'l - CKG	A321	2小时35分

图 5　实际航班信息

Fig. 5　Actual flight information

2　ADS-B 虚假目标注入

2.1　针对 ADS-B 系统的攻击类别

ADS-B 技术采用了开放共享的广播式架构，广播监视的可靠性较差，安全性能有待提升[7]。目前研究定义的比较常见的 ADS-B 系统攻击类别有：1)欺骗信号攻击；2)淹没攻击；3)干扰攻击；4)针对航空电子设备攻击；5)针对 CRC 的攻击。其中欺骗信号攻击是针对单一飞机的攻击，通过发射单一欺骗目标信号，使得接收设备在显示系统显示单一的幽灵目标，从而产生错误判断。淹没攻击，是利用 ADS-B 未加密的特点，通过大量发送无意义的虚假 ADS-B 目标，从而淹没显示端的屏幕系统。CRC 攻击，是通过改变射频信道中噪声扭曲 ADS-B 信号的结果，使得 CRC 校验难以通过，而导致显示端无法正确解调出目标信号，导致丢失消息。本次设计针对的是干扰攻击，干扰攻击中主要有飞机消失与轨迹修改。飞机消失，攻击者通过生成与 ADS-B 信号同步反向的信号来抑制或抵消抵消真实信号，接收解调端正确截获并解调出信号的概率大大降低，然而，由于很难精确地实现定时同步，因此该攻击方式的执行效率较低。相对来说，轨迹修改攻击出现的频率要更大，攻击者通过发送高功率信号来抑制实际的低功率信号，攻击者可以将部分消息报文替换，在实际航迹中可能会呈现一些伪目标点，让显示端难以分辨，本次设计针对该部分来进行防御。

2.2　虚假目标信号的制作

为了最终在 Qt 端将报文甄别模块嵌入并完成验证，本文需要先完成虚假信号的制作，以便最后能完整的仿真。

第一步，要对目标报文进行编码，本文将会对一架真实的目标飞机航迹进行测试，因此首先要有一个基准的身份信息，然后需要对速度，位置，以及校验码做修改。对于 ADS-B 航迹位置的修改，根据 CPR 编码方式的相关要求，本文需要根据公式对输入的经纬度进行编码。对于 ADS-B 飞行速度信息的修改，本文需要将东西方向速度和南北方向速度反向代入公式，进行进制转换后替代报文的 14～35 位，此处速度单位为节。最后，修改数据报文需要对 CRC 位重新进行编码，此处生成多项式为 25 位[1111111111111010000001001]。首先对原始数据进行补 0 操作，在数据末尾添加生成多项式长度个 0，此处为 25 位。将拓展的数据前段与生成多项式对应位进行异或运算，计

算出的结果与后一段数据合并作为新的运算数据,重复该步骤,直到被除数的长度小于生成多项式的长度时,剩余的被除数即为校验码,25 位生成多项式最终可以获得 24 位的 CRC 校验码,每次将 88 位数据位修改后通过 CRC 模块可获取 112 位制作的新报文。将新报文重新通过解码系统解码,如果解出的信息数据与本文输入的数据相符合,则为有效报文。图 6 为报文制作界面。

图 6 ADS-B 假报文制作系统界面

Fig. 6 ADS-B false message fabrication system interface

第二步,为了生成真实的 ADS-B 模拟信号,本文选择 ADI 公司的软件定义无线电(software defined radio,SDR)平台 ADALM-PLUTO。该平台为 ADI 公司推出的 SDR 主动学习模块,该模块具有独立的接收和发射通道,可以在全双工模式下工作。Pluto 最高能以 61.44 MSPS 的速度,从 325 MHz~3.8 GHz 的频率范围获取和生成射频模拟信号。该平台通过 libiio 驱动程序启动,可支持 Windows 和 Linux 等多个系统。本次实验在 Linux 系统上进行启动,将上述编码过程移植到 Ubuntu 中,通过手动输入飞机的经度纬度高度等信息,控制 Pluto 发送模拟的虚假 ADS-B 信号,由本文的 ADS-B 接收解调设备进行测试,如图 7 所示。

图 7 为完整的无线收发设备,通过上位机制作的报文由 Pluto 发送出去,由天线接收,通过 AD9361 和 ZYNQ-7000 将报文解调出来,在 ZYNQ PS 端的 Linux 图形化界面显示报文结果。由本文在 Ubuntu 上指定飞机的 ICAO,经度,纬度,高度等,由 Pluto 的 TX 端进行发出,AD9361 的 RX 端进行接收。图 8 和图 9 为 ADS-B 信号生成,发送与接收。从上位机逐一发送指定的 500 个飞机点迹,设备同时能收到来自附近的其他飞机信号。经过测试,由 Pluto 发送的 ADS-B 信号均能被该系统捕获到。将该接收报文进行解码,与本文输入的目标参数相一致,证明该系统可以用来进行模拟的虚假目标测试。

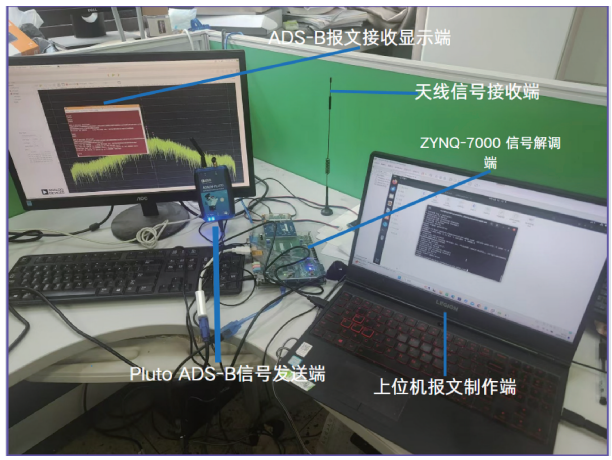

图 7 PlutoSDR 发送 ADS-B 信号测试

Fig. 7 PlutoSDR sending ADS-B signal test

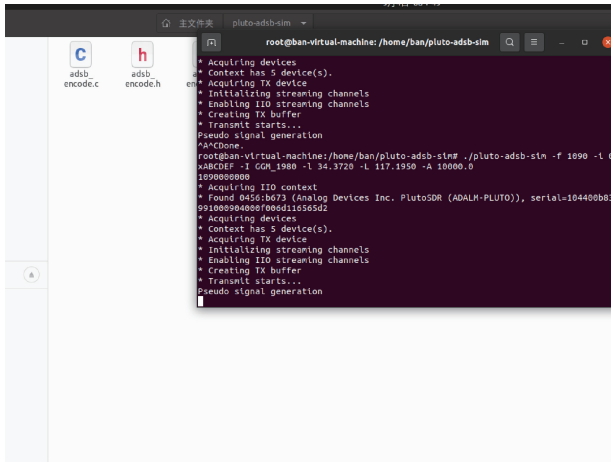

图 8 Ubuntu ADS-B 信号生成

Fig. 8 Ubuntu ADS-B signal generation

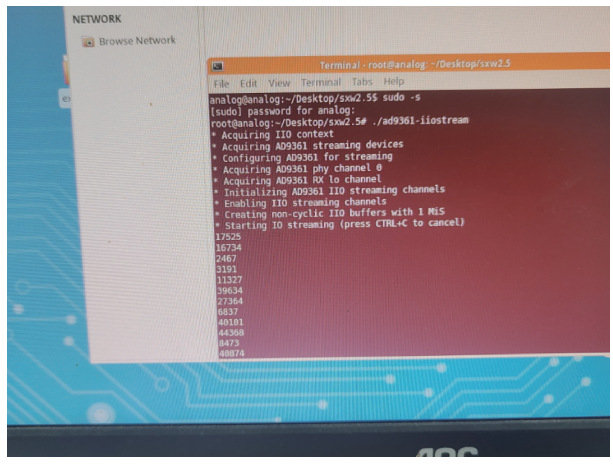

图 9 ZYNQ ADS-B 信号接收

Fig. 9 ZYNQ ADS-B signal reception

3　基于卡尔曼滤波的航迹预测

3.1　卡尔曼滤波

卡尔曼滤波是一种利用线性系统方程，通过系统输入输出观测数据[8]，用于估计线性动态系统状态的工具。该方法由 Rudoif E. Kalman 在 1960 年提出，广泛应用于控制系统、导航、信号处理等领域。主要思想是通过融合系统模型与实际观测数据来精准地估计系统状态，并根据系统动态进行状态预测。

卡尔曼滤波公式步骤如下：

已知 k 时刻的状态估计，计算 $k+1$ 时刻的状态估计：

$$\hat{\boldsymbol{S}}_{k+1/k} = \boldsymbol{C}_k \boldsymbol{S}_{k/k} + \boldsymbol{G}_k \bar{\boldsymbol{a}}_k \tag{1}$$

预测 $k+1$ 时刻状态协方差：

$$\boldsymbol{P}_{k+1/k} = \boldsymbol{C}_k \boldsymbol{P}_{k/k} \boldsymbol{C}_k^{\mathrm{T}} + \boldsymbol{Q}_k \tag{2}$$

预测 $k+1$ 时刻量测值：

$$\hat{\boldsymbol{Z}}_{k+1/k} = \boldsymbol{H}_{k+1} \hat{\boldsymbol{S}}_{k+1/k} \tag{3}$$

计算新息：

$$\boldsymbol{d}_{k+1} = \boldsymbol{Z}_k - \hat{\boldsymbol{Z}}_{k+1/k} \tag{4}$$

新息协方差：

$$\boldsymbol{F}_{k+1} = \boldsymbol{H}_{k+1} \boldsymbol{P}_{k+1/k} \boldsymbol{H}_{k+1}^{\mathrm{T}} + \boldsymbol{R}_{k+1} \tag{5}$$

卡尔曼增益：

$$\boldsymbol{K}_{k+1} = \boldsymbol{P}_{k+1/k} \boldsymbol{H}_{k+1}^{\mathrm{T}} \boldsymbol{F}_{k+1}^{-1} \tag{6}$$

状态估计更新：

$$\hat{\boldsymbol{S}}_{k+1/k+1} = \hat{\boldsymbol{S}}_{k+1/k} + \boldsymbol{K}_{k+1} \boldsymbol{d}_{k+1} \tag{7}$$

状态协方差估计更新：

$$\boldsymbol{P}_{k+1/k+1} = \boldsymbol{P}_{k+1/k} - \boldsymbol{K}_{k+1} \boldsymbol{F}_{k+1} \boldsymbol{K}_{k+1}^{\mathrm{T}} \tag{8}$$

由 ADS-B 得到的地面速度(ground speed，GS)单位为节(knots，kt)，预测用的时间单位为 s，在卡尔曼状态方程中，需要对速度进行转换，公式为：

$$1\ \mathrm{kt} = 1\ \mathrm{nmi/h} = 0.514\ 4\ \mathrm{m/s} \tag{9}$$

卡尔曼观测包括预测和更新两步[9]。预测过程的最终目的是为了获得系统的状态预测值和状态协方差预测值；更新过程的最终目的是为了获得滤波增益，同时对状态预测值和状态协方差预测值进行更新[10]。由于卡尔曼滤波本身具有丢包抑制，错误修正，高精度状态估计等优点，因此本文选择卡尔曼来进行航迹预测。

3.2　航迹预测

在航迹预测以及判定过程中，本文引入均方根误差(root mean squared error，RMSE)[11]，均方根误差公式为：

$$RMSE = \sqrt{\frac{1}{n} \times \sum (di^2)} \tag{10}$$

式中：di 为预测值和实际值的偏差。

经纬度换算距离的公式为：

$$alng = 360/(2\pi R \times \cos(lat)) \tag{11}$$

$$alat = 360/(2\pi R) \tag{12}$$

地球半径为 6 371 000 m，本地纬度坐标取为 31.83，由以上公式可得，经度(longitude，lng)每相差 1°，距离相差约 94 469 m，纬度(latitude，lat)相差 1°，距离相差约 111 234 m，在经纬度小数点后第 4 位的变动会带来水平距离约为 10 m 级的变化。

在 Qt 中制作二维的卡尔曼预测系统进行仿真测试，取一段飞机的实际飞机飞行数据，该段数据为飞机最后降落前 30 min 的数据，本文取该段数据前 17 min 的飞行数据，每 2 s 取一个坐标和速度，获得航迹中总计 500 个点，将设定值输入表中，部分预测如图 10 所示。

图 10　航迹预测系统界面

Fig. 10　Aircraft trajectory prediction system interface

由图 10 所示，通过卡尔曼预测获得的预测值与下一时刻的量测值求得偏差值，记录偏差值并分别计算 x 方向与 y 方向的均方根误差，并设定相关门限。由文献[12]指出，ADS-B 位置信息与标准位置信息的距离一般小于 300 m，超过此值可记为跳点。当预测和实际的距离小于参考值时系统会判定通过，因此此处设置误差为 0.003。在下一章本文会结合 *RMSE* 阈值给出综合的判定方式。

作出 500 点的航迹 x 方向与 y 方向速度比对图，如图 11 所示。

图 11 为完整 500 点的飞机速度变化，上方粗实线为 x 方向速度，下方虚线为 y 方向速度。可以看到飞机整体速度处于由高速往低速的趋势，x 方向与 y 方向速度变化节奏相似，飞机都是在前 300 点左右处于相对平稳飞行的状态，在 310 点和 430 点附近有较大的变速。

图 12 所示为部分预测经度值与实际经度值的对比，粗实线为卡尔曼预测值，虚线为原始值。可以看到预测大部分点的误差在 0.001 以内，在 314 点附近有较大的误差，与 x 轴在该点的速度突变相对应。

图 13 所示为部分预测纬度值与实际纬度值的对比，粗实线为预测结果，虚线为原始值，预测大部分点的误差也在 0.001 以内，在 430 点附近有较大的误差，与 y 轴在该点的

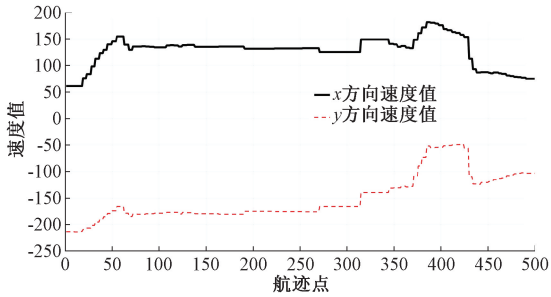

图 11 500 航迹点飞机 x 和 y 方向速度对比

Fig. 11 Comparison of the x and y directional velocities of an aircraft at 500 trajectory points

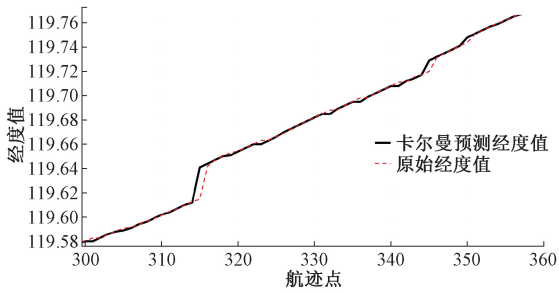

图 12 部分卡尔曼预测经度值对比

Fig. 12 Comparison of partial kalman filter predicted longitude values

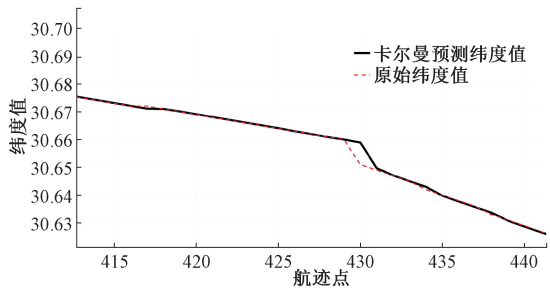

图 13 部分卡尔曼预测纬度值对比

Fig. 13 Comparison of partial kalman filter predicted latitude values

速度突变相对应。

综上可知,飞机的瞬时的机动加速度会影响卡尔曼滤波对于下一时刻的估计,速度变化越剧烈,卡尔曼滤波的估计偏差会越大,而实际中,经过多次测试,民航客机的整体速度变化不大,图 13 取样为飞机降落前的一段飞行数据,速度变化较为明显,卡尔曼滤波对于航迹整体的预测效果较好,大部分点的偏差都在百米之内,少部分点偏差会在两三百米附近,可见使用基于卡尔曼预测来进行后续的虚假目标识别具备可行性。而本文的系统本身具备一定的实时接收能力,考虑到二维卡尔曼滤波本身算法复杂度不高,Zedboard 的 Ps 端 CPU 为双核 Cortex-A9,主频为 667 MHz,具有较高的复杂计算处理能力,这为航迹显示中引入卡尔曼滤波提供了良好的平台保障,确保了流畅的实时显示效果。

4 ADS-B 航迹评估与伪目标识别

4.1 ADS-B 航迹位置的离散度

ADS-B 数据解码后通常会出现异常数据项,包括但不限于 ICAO 码或速度信息等[13],因此对于数据质量控制很重要。对于 ADS-B 数据质量评估,有一套完整的指标体系,如图 14 所示,是根据 RTCADO-260 和中国民航局对 ADS-B 监视系统验证评估内容的要求而制定[14]的。

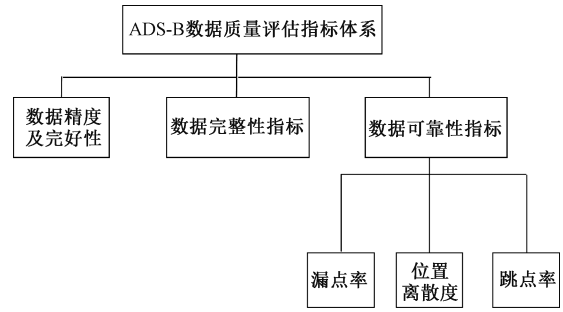

图 14 ADS-B 数据质量评估体系

Fig. 14 ADS-B data quality evaluation system

漏点率与接收机性能相关,本文引入位置离散度和跳点率。ADS-B 位置离散度是由各个航迹点离散距离所占的百分比构成,由实际点坐标 A($x0$, $y0$)与预测点坐标 B($x1$, $y1$),如式(13):

$$d = \sqrt{(x1-x0)^2+(y1-y0)^2} \tag{13}$$

计算不同航迹点的离散距离,作出相关的统计图,获取位置离散度指标。

4.2 ADS-B 航迹跳点率与门限判定

跳点率主要用于对报文数据的异常和畸变进行分析,ADS-B 航迹的跳点率为:

$$P = n/N \times 100\% \tag{14}$$

式中:跳点率为 P,伪目标数为 n,总点数为 N。

通过计算出真实飞机航迹各点的离散度距离的标准差,设标准差的阈值为 X,超过阈值的点为伪目标点,反之,认为是航迹上的实际点。

对航迹跳点判断进行的仿真验证步骤如下,首先计算该段航迹离散度距离的标准差 X,从而设定航迹滤波的相关阈值,然后在 Qt 制作跳点检测的模块,最后再通过加入假报文来对系统进行仿真测试。

选取真实飞机航迹上 500 个连续点,相邻点之间时间间隔为 2 s,进行卡尔曼滤波后,数据统计如表 1。

由实验得,离散度在 100 m 以内的点为 87.4%,然后计算离散距离度的标准差:

$$\delta = \sqrt{\frac{1}{N} \times \sum_i (di - d_{ref})^2} \tag{15}$$

实验中 N 为 500 个,计算得本组数据离散距离度的标准差 X 为 37.82,将此值设定为门限值,如果该组航迹数据点的离散距离度标准差超过该值,则判定为假航迹点。结

表 1　500 点离散度距离统计表

Table 1　Statistical table of 500-point dispersion distance

离散度/m	点个数	百分比/%
0～50	227	45.4
51～100	210	42.0
101～150	20	4.0
151～200	26	5.2
201～250	15	3.0
251～300	2	0.4

合上一章的均方根误差，航迹目标的均方根误差需要小于 300 m 且离散度距离需小于设定阈值，否则判定为跳点或伪目标点。

在此条件下，分别计算每个数据的均方根误差和离散度距离，并判断该段数据的跳点率，如表 2 所示。

表 2　500 点数据跳点率统计表

Table 2　Statistical table of data missing rate for 500 points

离散度标准差阈值/m	正确点个数	伪目标点个数	跳点率/%
37.82	457	43	8.6

由表 2 可知，在该阈值条件下，该段数据中有 43 个跳点。完成阈值设定后，开始制作跳点率检测部分，并将模块嵌入 Qt 中。跳点率检测模块，主要依据上述两个判定条件。而在卡尔曼滤波中，会根据当前观测值来进行下一步预测更新，如果出现一个偏离航线的跳点，卡尔曼滤波会在本次和下一次的预测中都出现偏差，结果上会因为出现一个伪目标点而导致有两个跳点被检测到，因此要对跳点后的一个点进行判断。在检测中再加入一个流程，取当前跳点处的预测值，对预测值进行状态预测，如果在该状态下，下一轮次的值与预测的值相差小于设定阈值 $E(200)$，会认为该点是被上一个跳点影响判断的点，会将该点从跳点中剔除，否则认为该点就是连续的跳点，维持跳点计数不变。

该部分流程如图 15 所示。

4.3　ADS-B 伪目标注入测试

加入跳点率检测后，先对该系统进行跳点仿真验证。

在 Qt 中加入轨迹预测与跳点率检测模块，飞机理论仿真的最终位置坐标为(120.124，30.51)。能在 Qt 地图端实时监控飞机控件移动，并且在 Qt 信息端显示飞机当前位置坐标以及该坐标是否为预测的真实值。Qt 的部分信息端显示如图 16 所示。

可以看到该段数据最终跳点个数为 43 个，与计算结果一致。

通过上位机控制 ADALM-PLUTO 发送模拟的 ADS-B 虚假信号，在测试中引入真实的 ADS-B 报文发送模块，可以进一步检验该系统的虚假目标识别能力。在 500 个真实航迹点中将 50 个非跳点数据改为虚假目标数据，设定虚假

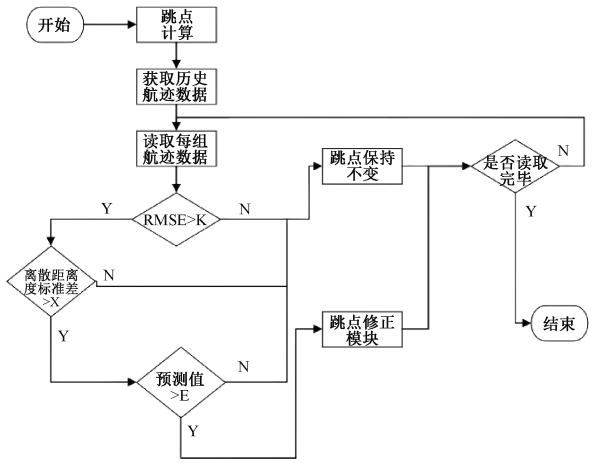

图 15　跳点检测模块流程图

Fig. 15　Jump point detection module flowchart

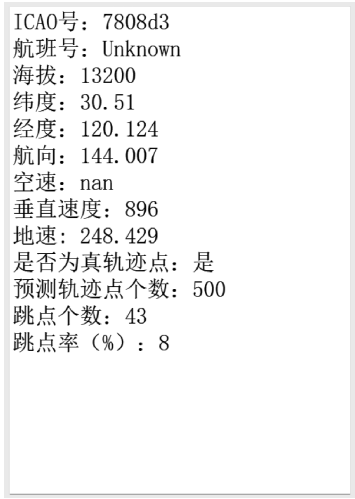

图 16　跳点仿真验证

Fig. 16　Skip point simulation verification

目标的值为与原始航迹数据平均偏差距离 200 m 的随机跳点数据，而原始航迹中已有 43 个跳点，该报文总共跳点数应为 93 个。通过 ADALM-PLUTO 逐一发送遭受修改的 ADS-B 模拟信号，在 ZYNQ 的 Linux 系统中成功收到报文总共 1 002 行，如图 17 所示。

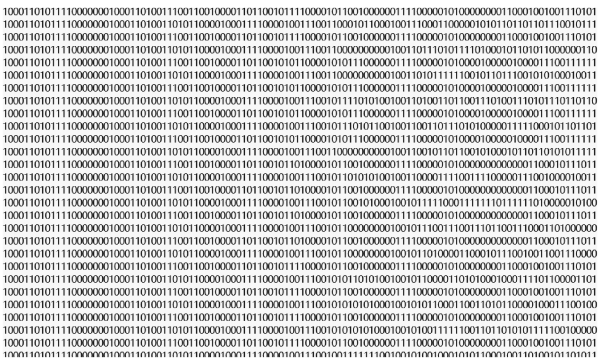

图 17　部分报文数据

Fig. 17　Partial message data

图 18 为 Qt 仿真信息端的部分数据信息,该组航迹数据可以检测到 88 个跳点,包含人为制作的 45 个虚假目标。

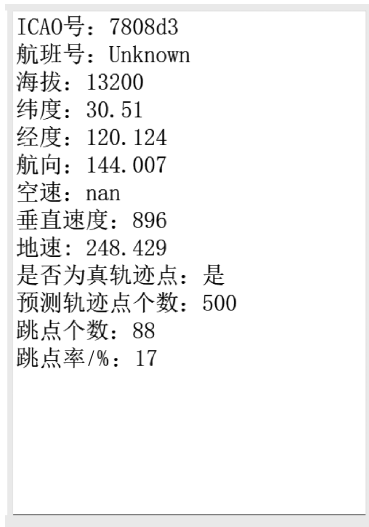

图 18 跳点率检测仿真

Fig. 18 Simulation of data missing rate detection

每次将制作的不同的 50 个虚假目标点混入目标报文中,总共进行 10 次实验,结果如表 3 所示。

表 3 虚假目标识别结果统计

Table 3 Statistical of false target identification results

组别	正确点个数	正确率/%
1	45	90
2	46	92
3	45	90
4	43	86
5	46	92
6	45	90
7	46	92
8	45	90
9	45	90
10	46	92

总计 500 个伪目标点中测到了 452 个点,预测正确率为 90.4%。在完成了针对单个目标飞机的跳点仿真验证后,后续在实际应用场景中,考虑到不同飞机目标的实际阈值差异,需要追加对于离散距离度的标准差阈值的实时更新。设定当飞机点数不足 10 时,仅针对航迹目标进行均方根误差判断,之后每累计 10 个点迹重新测算离散距离度的标准差阈值,并实时更新。

5 结 论

本文研究内容以及成果:针对 ADS-B 虚假目标的研究,本文相比于以往的 ADS-B 系统安全性的理论研究,在其基础之上,针对轨迹修改这一类别用 Pluto 和 Zedboard 做了报文收发和航迹显示。在伪目标识别上,将卡尔曼滤波应用在识别系统中,对于轨迹修改的攻击方式做了防御。由实验测试可得,该系统具备一定的 ADS-B 虚假目标甄别功能,可以与前端的 ADS-B 接收解调部分相结合,成为一个实时的 ADS-B 航迹显示与识别系统。

本系统的虚假目标识别方式仍有改进的空间,后续可以通过与前端的接收部分交互,通过读取 AD9361 中的 RSSI 寄存器的值,绘制 RSSI-d 的曲线图[15],通过三维的距离来识别信号真假,增强对于单一虚假目标的识别能力,与本文的卡尔曼滤波相结合,可以实现对于其他几种攻击方式的防御。综上,本系统具备一定的伪目标识别能力,易于搭建和扩展,具有良好的应用前景。

参考文献

[1] 邹伟,詹泉泉. ADS-B 航空监视系统设计及应用[J]. 通讯世界,2024,31(3):148-150.
ZOU W, ZHAN Q Q. Design and application of ADS-B air traffic surveillance system[J]. Communication World, 2024, 31(3): 148-150.

[2] ZOU H Q, BAN T, ZHUANG Z Y. An S mode ADS-B preamble detection algorithm[C]. 2019 IEEE 5th International Conference on Computer and Communications(ICCC), 2019: 178-182.

[3] 丁凯. 低空监视雷达信号处理方法研究[D]. 成都:电子科技大学,2017.
DING K. Research on signal processing methods for low altitude surveillance radar[D]. Chengdu: University of Electronic Science and Technology of China, 2017.

[4] 姚渊. 一种基于 ADS-B 数据处理中心系统进行假目标检测的方法[J]. 民航管理,2016(8):62-68.
YAO Y. A method for false target detection based on ADS-B data processing center system[J]. Civil Aviation Management, 2016(8): 62-68.

[5] 路璐. 基于 GBAS 完好性信息的 ADS-B 自主式防欺骗研究[D]. 天津:中国民航大学,2017.
LU L. Research on ADS-B autonomous Anti-Spoofing based on GBAS integrity information[D]. Tianjin: Civil Aviation University of China, 2017.

[6] 庄子源,班恬. 基于软件无线电的 ADS-B 信号接收机设计[J]. 电讯技术,2021,61(7):833-838.
ZHUANG Z Y, BAN T. Design of ADS-B signal receiver based on software defined radio[J]. Telecommunication Technology, 2021, 61(7): 833-838.

[7] 陈晓,毛烨炳. ADS-B 技术在低空空域安全中应用的现状与展望[J]. 电子测量技术,2022,45(20):61-67.
CHEN X, MAO Y B. Current status and prospects of ADS-B technology in low altitude airspace safety[J].

Electronic Measurement Technology, 2022, 45(20): 61-67.

[8] 刘宁庄,戴伟.基于卡尔曼滤波的质量流量计误差修正算法[J].电子测量技术,2022,45(15):172-177.
LIU N ZH, DAI W. Error correction algorithm for mass flow meters based on Kalman filtering [J]. Electronic Measurement Technology, 2022, 45(15): 172-177.

[9] 贾光耀,闫飞.基于卡尔曼滤波迭代学习的交通信号控制方法[J].电子测量技术,2023,46(8):126-133.
JIA G Y, YAN F. Traffic signal control method based on Kalman filtering iterative learning[J]. Electronic Measurement Technology, 2023, 46(8): 126-133.

[10] 卢献宇,张媛媛.基于卡尔曼滤波算法的 ADS-B 航迹预测[J].现代信息科技,2021,5(8):48-50,53.
LU X Y, ZHANG Y Y. ADS-B trajectory prediction based on Kalman filtering algorithm [J]. Modern Information Technology, 2021, 5(8): 48-50,53.

[11] 李韶华,李健玮,冯桂珍.基于 GA-LSTM 自适应卡尔曼滤波的路面不平度识别[J].振动与冲击,2024,43(9):121-130.
LI SH H, LI J W, FENG G ZH. Identification of pavement roughness based on GA-LSTM adaptive Kalman filtering[J]. Journal of Vibration and Shock, 2024, 43(9):121-130.

[12] 倪久顺. 星基 ADS-B 数据质量评估与数据挖掘研究[D].长沙:国防科技大学,2021.
NI J SH. Research on quality assessment and data mining of satellite-based ADS-B data[D]. Changsha: National University of Defense Technology, 2021.

[13] 陈敏,王浩楠,陈万通,等.基于 ADS-B 与 Mode-S EHS 联合观测的民航空域风场重建方法[J].国外电子测量技术,2024,43(6):102-109.
CHEN M, WANG H N, CHEN W T, et al. Reconstruction method of atmospheric wind field in civil aviation airspace based on joint observation of ADS-B and Mode-S EHS [J]. Foreign Electronic Measurement Technology, 2024, 43(6): 102-109.

[14] 张登茂.基于 ADS-B 的飞行器航迹处理及显示系统的研究[D]. 成都:电子科技大学,2017.
ZHANG D M. Research on aircraft trajectory processing and display system based on ADS-B[D]. Chengdu: University of Electronic Science and Technology of China, 2017.

[15] KHANDKER S, TURTIAINEN H, COSTIN A, et al. Cybersecurity attacks on software logic and error handling within ADS-B implementations: Systematic testing of resilience and countermeasures [J]. IEEE Transactions on Aerospace and Electronic Systems, 2022, 58(4): 2702-2719.

作者简介

周苏宁,硕士研究生,主要研究方向为 FPGA 信号处理。

王韬,硕士讲师,主要研究方向为算法设计与实现。

班恬(通信作者),博士教授,主要研究方向为信号处理算法的 FPGA 实现。

E-mail:tian. ban@njus. edu. cn