无人机信息安全研究综述

何道敬[1] 杜 晓[1] 乔银荣[1] 朱耀康[1] 樊 强[2] 罗 旺[2]

[1](华东师范大学计算机科学与软件工程学院 上海 200062)

[2](南瑞集团公司(国网电力科学研究院) 南京 211106)

摘 要 随着科技的进步和制造成本的不断降低,无人机已经从军用领域开始走进工业生产和人们的日常生活.如今,无人机已经广泛应用于影视拍摄、农业监测、电力巡检、个人航拍、气象监测、森林火灾探测、交通控制、货物运输及应急救援等领域.然而,无人机在给我们的生产生活带来各种便利的同时,其所面临的安全问题也逐渐暴露出来.该文首先介绍了当前无人机的发展现状,然后介绍了无人机的组成结构和应用,之后分别从保密性、完整性和可用性方面系统地阐述了当前无人机所面临的信息安全威胁.接着,该文着重从传感器、通信、软件和网络四个方面对无人机所面临的安全威胁、现有安全防护措施以及国内外的研究现状进行了详细的阐述和分析.其中,结合当前国内外最新的研究成果和我们实验室的研究和实验,重点对针对无人机的卫星导航信号的欺骗攻击和针对无人机通讯安全的攻击及其应对措施进行了阐述和分析.最后,对无人机的安全和管理的未来研究方向进行了展望.

关键词 无人机安全;公共安全;无人机捕获;GPS 欺骗;无线电劫持

中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2019.01076

A Survey on Cyber Security of Unmanned Aerial Vehicles

HE Dao-Jing[1] DU Xiao[1] QIAO Yin-Rong[1] ZHU Yao-Kang[1] FAN Qiang[2] LUO Wang[2]

[1](*School of Computer Science and Software Engineering, East China Normal University, Shanghai* 200062)

[2](*NARI Group Corporation (State Grid Electric Power Research Institute), Nanjing* 211106)

Abstract With the rapid advancements of technology and the decreasing of the manufacturing cost, unmanned aerial vehicles (UAVs), also commonly known as drones, are spreading from military areas to industrial production and people's daily lives, during the past few decades. Nowadays, UAVs are now more easily accessible to the public and thus numerous new applications in civilian and commercial domains have emerged, with typical examples including film shooting, agricultural inspection, electrical inspection, personal photography, weather monitoring, forest fire detection, traffic control, cargo transport, emergency search and rescue. However, while a UAV gives people all kinds of conveniences, the cyber security problem of the UAV is gradually exposed. That is, cyber security is critically important for the success of the UAVs. In this article, we first give a state-of-the-art overview of UAV development, introduces the composition structure and various applications of the UAVs, and discuss the cyber security threats faced by the UAVs from the aspects of confidentiality, integrity and availability. In particular, this paper presents the cyber security threats, existing security protection measures, and the current research progress at home and abroad on the UAVs from the four aspects (i.e., sensor node, communication link, software and network) in details. Here we consider the sensor security of the UAVs as an example. Firstly, multiple sensor

收稿日期:2016-06-28;在线出版日期:2017-08-13.本课题得到国家重点研发计划课题(2017YFB0802805,2017YFB0801701,2017YFB0802302)、国家自然科学基金项目(U1636216,51477056,61601129)、国网公司科技项目、上海市青年科技启明星计划(15QA1401700)、上海市科委技术标准专项项目(16DZ0503000)资助.**何道敬**,博士,教授,中国计算机学会(CCF)高级会员,主要研究领域为系统及网络安全.E-mail:djhe@sei.ecnu.edu.cn.**杜 晓**,硕士研究生,主要研究方向为无人机安全.**乔银荣**,硕士研究生,主要研究方向为嵌入式系统安全.**朱耀康**,硕士研究生,主要研究方向为无人机安全.**樊 强**,学士,高工,主要研究方向为传输与路由交换.**罗 旺**,博士,高工,主要研究方向为信号与信息处理.

devices such as gyroscopes, accelerometers, magnetometers and barometers are often used in the design of the UAVs in order to achieve various functions. The erroneous data collected by a sensor node may make the UAV to make a wrong decision, which affects the flight safety of the UAV and even lead to its crash. The traditional sensor security research generally focuses on the security of data transmission in the sensor networks, but often ignores the security threat analysis and protection of the sensor node itself. In addition, due to technical or cost constraints, commercial sensors in a UAV are usually unable to distinguish normal and abnormal information. We have summarized and analyzed the current situation of the research on the sensors used in the UAVs. At present, there are two kinds of cyber security attacks for the UAVs, which are ultrasonic jamming on gyroscope and GPS deception. we have developed a low-cost record-and-replay system based on a software defined radio device. Also, this article reports the experimental results of some cyber security attacks and defense mechanisms on the UAVs. Especially, global positioning system (GPS) spoofing attack and defense on the UAVs are described in details. Moreover, our proposed UAV control system and its experimental results are described. This system does not need any physical contact or other electronic intrusion of the UAV system, and this method is applicable to most of the UAV models based on satellite navigation signal for navigation. The system can avoid the weaknesses of other UAV control methods such as resulting in UAV falling out of control and causing secondary disasters. Finally, the future research directions of the UAV security and management are discussed. Work in this direction is still in its early stages, and thus we hope this paper will stimulate further interest from researchers and engineers.

Keywords　unmanned aerial vehicle security; public safety; unmanned aerial vehicle capture; GPS spoofing; radio hijacking

1　引　言

随着科学技术的进步和发展，无人机在技术上越来越成熟，在生产生活中的应用也变得越来越广泛. 无人机具有成本低、体积小、重量轻、易操纵、高度灵活性、高度适应性、安全稳定性和便于隐蔽等优点，因此在处理影视拍摄、农业监测、自然灾害、事故灾难以及社会安全事件等方面发挥着重要作用.

在民用无人机领域，中国已经走在世界的前列. 据路透社报道，中国无人机制造公司大疆创新(DJI)在消费级无人机领域的市场占有率达 70%.

最近几年，无人机市场规模保持每年约 50%的高速增长态势. 在 2015 年，全球无人机销售量约为 58.7 万架，其中军用无人机约占 3%，民用无人机占 97%. 民用无人机销量中，专业级无人机销量约 17.1 万架，消费级无人机销量约 39.9 万架. 2016 年 6 月，著名专业机构艾瑞咨询发布《2016 年无人机行业研究报告》[①]，称民用无人机市场已进入快速成长期，市场规模增速达到 50%以上. 预计到 2020 年全球无人机年销售量将达到 433 万架.

本文第 2 节主要介绍无人机的组成结构以及无人机的应用；第 3 节介绍当前无人机所面临的安全威胁；第 4 节主要介绍无人机传感器所面临的安全威胁以及应对措施；第 5 节主要介绍无人机的通信所面临的安全威胁和应对措施；第 6 节主要介绍无人机以及地面站的软件安全所面临的威胁和防护措施；第 7 节主要介绍无人机网络以及其面临的安全威胁和防护措施；最后对无人机安全的未来研究方向进行了总结和展望.

2　无人机的组成和应用

无人驾驶飞机简称“无人机”(Unmanned Aerial Vehicle，UAV)，是利用无线电遥控设备操纵的不载人飞机. 从技术角度可以将无人机分为：无人固定

① http://www.iresearch.com.cn/report/2588.html

翼机、无人直升机、多旋翼无人机、无人伞翼机等[1].

2.1 无人机系统组成

如图 1 所示,典型的无人机系统主要由无人机、地面站以及传输信息的通信链路组成.

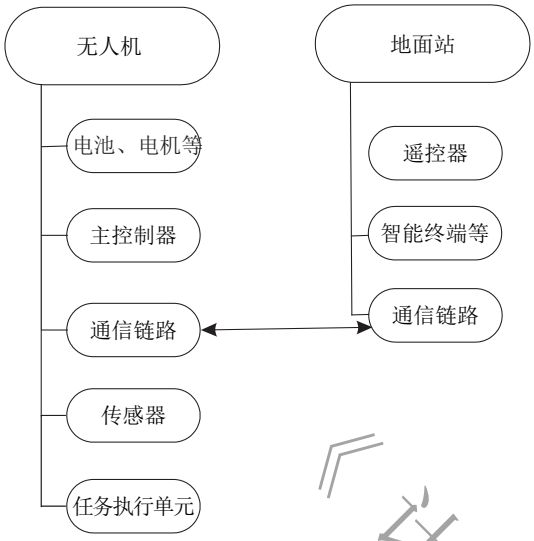

图 1 无人机的总体结构图

2.1.1 无人机部分

无人机主要由以下几部分构成:

(1)动力系统. 动力系统负责为无人机的飞行和稳定提供动力,无人机的动力来源一般有电动机和内燃机两种. 除了动力来源之外,无人机的动力系统还包含螺旋桨等设备;

(2)主控制器. 主控制器负责维持无人机的稳定和导航,并将接收到的控制命令转换成动力系统指令;

(3)通信链路模块. 无人机的通信模块主要包括遥控信号模块、无线数传模块和 Wi-Fi 通信模块;

(4)传感器. 传感器主要包括惯性测量单元(Inertial Measurement Unit,IMU)、磁力计(Magnetometer)、陀螺仪(Gyroscopic)、GPS(Global Positioning System,全球定位系统)模块、压力传感器、视觉传感器等;

(5)任务执行单元. 任务执行单元是无人机用来执行相应任务的部件,根据不同的任务选择相应的部件,比如,航拍一般采用云台相机,而农业检测则可能需要加载多光谱探测仪或热传感器等.

2.1.2 地面站部分

地面站是无人机操纵者操纵无人机的重要部分. 操纵者的控制命令都是通过地面站传输到无人机,从而使无人机根据命令做出相应的动作. 无人机采集的数据以及无人机自身的运行数据都将传输到地面站,并由地面站的显示器或者智能终端等设备进行显示. 地面控制部分具有无线电控制、数据处理及系统检测等功能.

地面站主要包括以下几个部分:

(1)遥控器. 由于遥控器具有操控方便、实时性和安全性较高等特点,当前民用无人机主要通过遥控器进行控制;

(2)智能终端. 智能终端可以更加直观地显示无人机自身以及所采集的数据,部分无人机则可以直接使用智能终端操控;

(3)通信链路模块. 地面站的通信模块一般与无人机的通信模块相对应.

2.1.3 通信链路部分

如图 2 所示,无人机的通信部分包括几个无人机组件和通信链路. 每个通信链路传输不同类型的信息数据. 一般来说,根据传输的信息类型的不同,无人机网络包括三种通信链路,分别为无人机与地面站之间的通信链路、卫星通信链路和无人机到无人机通信链路[2]. 无人机与地面站之间的通信链路传输遥测信息、视频和音频等数据;卫星通信链路传输 GPS 信号、气象信息等;无人机与无人机的通信链路是无人机网络的重要组成部分,用于无人机间的数据交换[3].

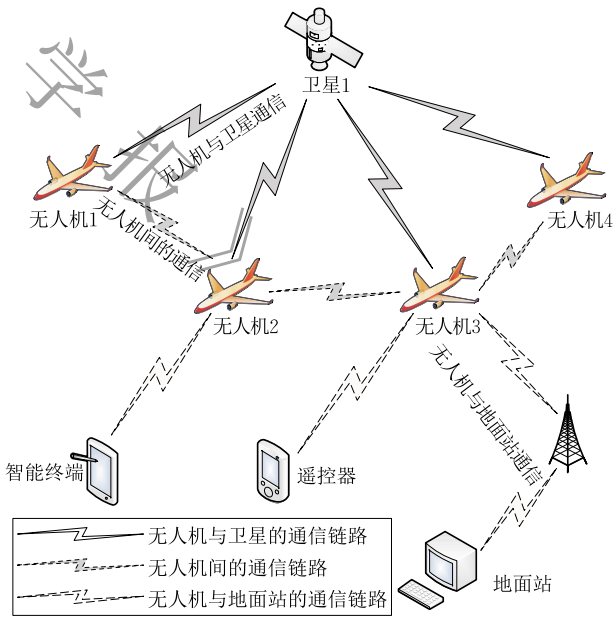

图 2 典型的无人机通信链路

2.2 无人机的应用

无人机作为飞行平台,搭载不同的工作设备,可以执行不同的任务. 如图 3 所示,无人机按照用途可以分为军用无人机和民用无人机. 军用无人机一般作为侦察机、靶机和攻击机,执行难度较低且危险性较高的任务. 民用无人机已经广泛应用于工农业生

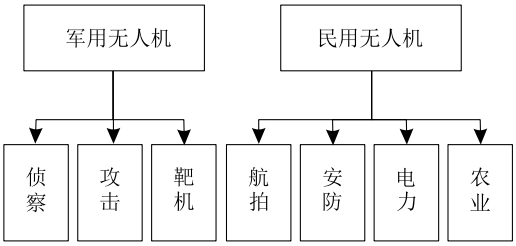

图 3　无人机的应用

产和人们的日常生活.

民用无人机按照用途可以分为工业级无人机和消费级无人机. 工业级无人机在工农业生产等方面发挥着巨大的作用：在农业方面可以用来喷洒农药、农业监测等[4-7]；在航拍方面，可以用来进行电影拍摄、新闻拍摄以及广告活动等；在安防领域，无人机则可以进行灾情检查、调度指挥、反恐维稳和协助巡逻等；在电力方面，无人机可以进行电力巡检和线路规划等[8]. 同时无人机在其他领域也发挥着很多的作用，比如城市规划、资源勘探、地图测绘、物流快递等[1,9].

3　无人机的安全威胁

随着无人机在生产生活的应用越来越广泛，无人机的安全问题也逐渐暴露出来. 在 2016 年的“3 · 15”晚会上，黑客利用大疆无人机的无线通信安全漏洞，通过无线劫持技术完全取得了大疆无人机的控制权. 另外，无人机安全领域最严重事件是 2011 年的伊朗捕获美国的 RQ-170 军用无人机事件. 除此之外，无人机还面临键盘记录病毒感染地面站等多种安全威胁.

上述的几个无人机攻击方式都是针对无人机的各个组件或者无人机网络进行攻击，虽然攻击对象和手段不同，但从信息安全的角度而言，其攻击主要破坏了无人机的保密性、完整性和可用性[10].

(1) 保密性，又称机密性，是保护数据不被非法访问. 针对保密性的攻击主要涉及未经授权的信息访问. 这种攻击最常见的方式是信息窃取. 在当前的无人机系统中，无人机、地面站和通信链路都可能会遭受保密性攻击. 对于地面站的威胁包括软件漏洞、病毒、恶意软件、木马、键盘记录程序等. 各种系统组件之间的通信链路的安全威胁包括口令破解、身份欺骗、跨层攻击[11]和多协议攻击[12].

(2) 完整性，包括数据完整性和系统的完整性. 数据完整性是指数据的正确性、一致性以及相容性；如果没有完整性的约束，攻击者可以通过插入、删除或修改等操作破坏关键数据的完整性. 当前，针对无人机完整性的攻击大部分为针对无人机数据完整性的攻击. 这些攻击有两种方式，分别为：修改现有信息和生成新的信息. 对无线数据链路或者传感器的干扰也可以影响数据完整性甚至窃取所传输的数据.

(3) 可用性，是指系统对合法的访问及时作出反应. 针对可用性的攻击是为了使无人机无法获取相应的数据或者无法根据指令做出相应的反应. 伪造攻击和拒绝服务(Denial-of-Service，DoS)[13-14]等主流的安全攻击方式可用来针对无人机网络的可用性进行攻击. DoS 或 DDoS(Distributed DoS，分布式拒绝服务)攻击是基于网络拥塞，使系统无法正常使用. 在这样的攻击中，系统或网络实际上是在为其他的“假”请求忙. 开展这样的攻击有三种方式，泛洪(Flooding)、Smurfing 和缓冲区溢出. 泛洪是通过发送大量的数据包，耗尽大量资源来瘫痪网络的攻击方式. 常用的泛洪攻击包括 SYN 泛洪攻击、DHCP 报文泛洪攻击、ARP 报文泛洪攻击和 Ping 泛洪. 缓冲区溢出是向缓冲区存放的数据位数超过缓冲区容量，往往会使程序崩溃导致拒绝服务. Smurfing 攻击利用 IP 的广播系统的伪装功能来增强 Flooding 攻击. 以上几种攻击方式除了会阻塞无人机的通信、破坏可用性，还会导致无人机的功耗增加，从而减少无人机滞空时间.

目前，对无人机的常见攻击主要包括针对无人机传感器的攻击、无人机网络的攻击、无线电干扰与劫持、GPS 欺骗. 接下来，本文从传感器、通信、软件和网络等四个方面对无人机所面临的安全威胁、现有安全防护措施以及国内外研究现状和我们实验室的研究和实验成果进行详细的阐述和分析.

4　无人机传感器安全

传感器是一种能感受到被测量的信息，并将检测到的信息转换为特定形式的电信号或者其他所需形式的信号进行输出的装置. 传感器是无人机系统检测自身和周围环境数据的重要组件. 随着微机电系统(Micro-Electro-Mechanical System，MEMS)和微机电去噪算法的逐渐成熟，越来越多的 MEMS 传感器被应用到无人机中，使得无人机自动控制技术更加成熟，从而导致了当下无人机热的情况.

新型无人机技术及其解决方案依赖于各种传感器的协作. 以当前流行的多旋翼无人机为例，无人机一般含有陀螺仪、加速度计、磁力计、GPS 和气压计等传感器. 陀螺仪用来检测无人机相对于坐标系的

角速度;加速度计用来检测无人机相对于坐标系的加速度;GPS 是用来获取无人机的位置信息;磁力计即电子罗盘用来检测方向信息.陀螺仪和加速度计是无人机系统惯性测量单元(Inertial Measurement Unit,IMU)的重要组成部分[15].

在无人机上,主控制器根据各种传感器采集到的数据,向动力系统下达相应的命令,以维持无人机的正常飞行.因此,传感器所采集到的错误的数据很可能使无人机做出错误的决策,影响无人机的飞行安全,甚至导致其坠毁.

传统的传感器安全一般侧重于传感器网络中数据传输的安全[16-17],而往往忽略了对传感器本身的安全威胁分析及防护[18].另外,由于技术或者成本的限制,一般商用传感器往往无法对正常和异常的信息进行检测和区分.

我们针对应用在无人机上的传感器的安全研究现状进行了汇总和分析.当前,针对无人机上传感器的攻击方式主要有超声波干扰陀螺仪和 GPS 欺骗两种.

4.1 超声波干扰陀螺仪

在无人机中,陀螺仪和加速度计等组成的惯性测量单元(IMU)可以用来测量无人机在三维空间中的角速度和加速度,并以此解算出无人机的姿态.一旦惯性测量单元采集的数据出现错误,无人机则无法正确解算出无人机当前的飞行状态,而这可能会导致无人机无法稳定飞行,甚至坠毁.所以,陀螺仪和加速度计对于无人机维护自己的姿态稳定具有重要意义[1,19].

由于微机电系统和微机电去噪算法的逐渐成熟以及无人机的成本和起飞重量的限制,无人机多采用 MEMS 陀螺仪和加速度计来维持无人机的飞行稳定.MEMS 传感器与传统的传感器不同,它采用振动物体传感角速度的概念,因而存在共振频率.当外界干扰的振动频率与 MEMS 陀螺仪的固有振动频率一致时,会产生共振效应,使其振动加强,从而影响陀螺仪输出数据的准确性甚至有可能会破坏传感器[20-23].

文献[24]介绍了一种使用超声波来对无人机的 MEMS 陀螺仪进行干扰,使无人机上的 MEMS 陀螺仪无法正常工作,从而致使无人机无法进行姿态控制,进而使无人机坠毁的方法.

图 4 是文献[24]检测 MEMS 陀螺仪的共振频段的流程图.如图 4 所示,运行在笔记本电脑上的脚本程序通过外置声卡生成特定频率的噪音,这些噪音经过声频放大装置的放大后,通过扬声器来干扰 MEMS 陀螺仪.连接陀螺仪的开源电子原型平台 arduino 将陀螺仪输出的数据采集并处理,然后将该数据发送到笔记本电脑,笔记本电脑通过对陀螺仪输出的数据的检测来判断当前频段是否为共振频段.

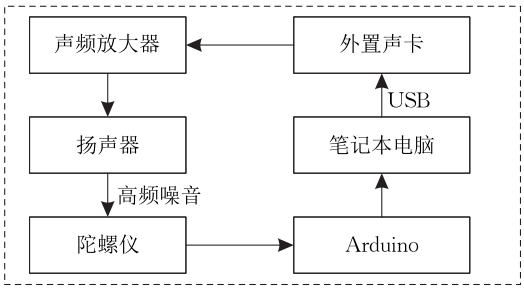

图 4 检测陀螺仪共振频段的流程图[24]

该文献对当前的商用 MEMS 陀螺仪进行了检测,发现大部分 MEMS 陀螺仪在共振频率噪声干扰下,其输出的数据出现较大误差 .研究人员据此对无人机进行了攻击实验.首先,研究人员找到一款采用了会产生共振效应传感器的无人机;然后,研究人员根据无人机上陀螺仪的型号找到相应的共振频段;之后,在无人机正常飞行的时候,研究人员使用相应频段的超声波对无人机进行攻击;最后,被超声波干扰的无人机由于陀螺仪无法正常工作而直接坠毁.

对于 MEMS 传感器的共振问题最简单的解决方法是对传感器进行物理隔离.该文献中提到,采用 L3G4200D 陀螺仪的无人机由于受到超声波干扰而坠毁,而 iPhone 5s 手机中的同一型号的陀螺仪却可以免受超声波噪声的干扰.这正是由于 iPhone 5s 手机的外壳减弱了超声波的功率.文献[25]提出了使用泡沫对 MEMS 传感器进行物理隔离的方案,一英尺的泡沫可以将超声波的噪声降低 120 分贝,从而可以很大程度上减轻超声波对 MEMS 传感器的干扰.文献[26]也介绍了一种物理隔离保护方案,即采用一种有镍纤维制作的保护罩来减弱超声波噪声对 MEMS 陀螺仪的干扰.虽然物理隔离可以缓解超声波对 MEMS 陀螺仪的影响,但是也带来一些其他方面的问题.比如,采用泡沫隔离板会带来散热不畅等问题.

针对物理隔离方法存在的一些缺陷,文献[26]提出了一种可以主动减弱超声波对 MEMS 陀螺仪影响的方案,即使用两个陀螺仪并配合一定的算法来缓解超声波对陀螺仪的影响.此外,还有一些文献提出在 MEMS 陀螺仪上加装其反馈调节装置来减少共振带来的影响.例如,文献[27-28]提出了通过

在 MEMS 陀螺仪上加装反馈电容来调节共振频率来减弱共振对陀螺仪的影响.

4.2　GPS 欺骗

全球定位系统(GPS)，又称全球卫星定位系统，其功能是为全球用户提供定位、测速和高精度的时间标准[29]. 对于无人机来说，GPS 是一个极其重要的传感器，它为无人机提供准确的位置信息[1]. 以大疆无人机为例，GPS 在航点模式、跟随模式、空中悬停、自动返航、失控返航和禁飞区中都有极其重要的作用.

GPS 提供的高精度的位置信息有助于减少甚至消除惯性测量单元(IMU)的累积误差. 在 GPS 和 IMU 组合导航的情况下，无人机的导航精度、可靠性和抗干扰能力都获得了提高[30-31].

随着 GPS 的广泛应用和软件无线电等技术的发展，GPS 受到的安全威胁越来越多. 当前 GPS 所面临的安全威胁主要包括 GPS 干扰和 GPS 欺骗. 顾名思义，GPS 干扰就是对 GPS 接收机施加干扰信号，使 GPS 接收机无法接收到真实的 GPS 信号从而无法获取位置信息和时间信息；而 GPS 欺骗则是通过伪造或者重放 GPS 信号的方式，使 GPS 接收机接收伪造或者重放的 GPS 信号，从而使 GPS 接收机解算出错误的位置和时间信息.

GPS 欺骗从信号的产生方式上可以分成转发式 GPS 欺骗和生成式 GPS 欺骗两类.

转发式 GPS 欺骗，首先将真实的 GPS 信号录制下来，然后再将其发射给的 GPS 接收机，从而使 GPS 接收机解算出错误的位置和时间信息.

生成式 GPS 欺骗是通过特定的程序生成特定位置和时间的 GPS 欺骗信号，发射给 GPS 接收机，然后 GPS 接收机接收并解析 GPS 欺骗信号，从而使 GPS 接收机解算出错误的位置和时间信息. 由于民用 GPS 信号的加密算法和检验矩阵的算法都已经公开，因此，对于按照这些算法生成的 GPS 信号是无法通过这些算法来检测欺骗的. 生成式 GPS 欺骗就是根据已经公开的 GPS 信号的信号结构、扩频码和调制方法以及加密和检验矩阵的算法伪造出特定的 GPS 信号，然后根据要发射的欺骗点的位置、GPS 卫星的位置，推算出每个 GPS 信号从 GPS 卫星发出到被 GPS 接收机接收所需要的延时，然后根据这些延时发射各个 GPS 信号. 当接收机接收到 GPS 欺骗信号的时候，GPS 接收机会根据三球定位原理来解算定位方程，由于延时都已经被设计好，所以，GPS 接收机就会被欺骗.

转发式 GPS 欺骗实现难度较低，但灵活性较差；生成式 GPS 欺骗则可以根据需要生成特定的 GPS 信号，但实现难度较大. 之前由于转发式 GPS 欺骗的局限性以及生成式 GPS 欺骗的实现成本较高，GPS 欺骗并没有引起人们的重视. 随着科学技术的发展，软件无线电技术的发展和成熟使得 GPS 的欺骗成本和技术难度大大降低[32].

GPS 欺骗对于自主导航设备的影响最为显著，特别是对于自主飞行的无人机和航行在大洋上缺少参照物的轮船. 美国德克萨斯大学的 Humphreys 教授领导的无线导航实验室，在 2013 年利用 GPS 欺骗技术使地中海上一个价值 8000 万美元的游艇偏离航向，在 2014 年欺骗了一架无人机，并使其改变飞行轨迹[33-34]. 很多安全研究人员注意到 GPS 欺骗对于无人机的影响[24,35]. 奇虎 360 的研究团队在低成本的 GPS 欺骗方面取得了重大进展，并对一架大疆精灵 3 无人机进行了禁飞区欺骗，即播放禁飞区内的 GPS 信号，使无人机无法正常起飞[32].

之前公开的 GPS 欺骗技术往往需要预先规划好要发射的 GPS 位置信息，在 GPS 欺骗的过程中无法动态地改变要发射的 GPS 欺骗点的位置. 我们实验室使用软件无线电技术，设计了一种可以基于生成式 GPS 欺骗攻击的可动态改变欺骗点的 GPS 欺骗系统，即可以在 GPS 欺骗过程中，根据需要动态地改变 GPS 欺骗点的位置. 图 5 所示的是我们实验室设计的 GPS 欺骗程序的流程图. 图 6 所示的是我们 GPS 欺骗系统的主要实验设备，包括主机、USRP(Universal Software Radio Peripheral，通用软件无线电外设)、放大器和天线以及连接线等. 该 GPS 欺骗系统分为 3 个部分：

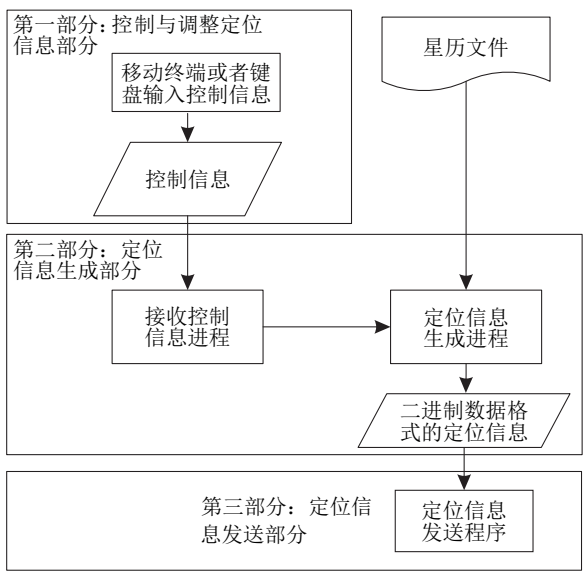

图 5　GPS 欺骗流程图

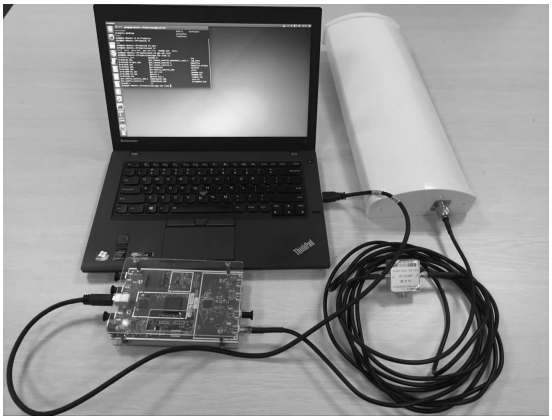

图 6 GPS 欺骗系统设备图
(包括主机、USRP 和天线)

第 1 部分,控制和调整位置信息部分,通过移动终端或者键盘来实时地调整要发射的经纬度坐标信息;

第 2 部分,定位信息生成部分,根据星历文件和需要发送的位置坐标信息,将相应的位置信息通过定位信息生成程序进行计算,然后生成二进制数据;

第 3 部分,定位信息的发送部分,通过 GNU-Radio(开源软件无线电平台)和 USRP 来发射二进制数据包.

图 7 是 GPS 欺骗手机的效果图,左侧两个图的测试手机为小米 5,测试软件为 GPS Test,右侧一个图的测试手机为 iPhone 6,测试软件为高德地图.图 7 中的两部手机(小米 5 和 iPhone 6)已经接收了 GPS 欺骗信号,并且定位到了大西洋上几内亚湾(0°S,0°W)附近(具体经纬度参见图 7 中间图上半部分所示的经纬度).图 8 是 GPS 欺骗无人机的效果图,在图 8 中大疆无人机已经接收 GPS 欺骗信号,并且定位到大西洋上几内亚湾(0°S,0°W)附近;图 9 是无人机在被 GPS 欺骗的时刻,无人机摄像头所拍摄的上海中山公园(31.221735°N,121.417832 9°E)

图 7 GPS 欺骗手机效果图
(测试手机为小米 5 和 iphone 6)

附近的建筑物;图 10 和图 11 是多款智能手机由于受到 GPS 欺骗而定位到中国在南极洲的科考站中山站(69°22′24.76″S, 76°22′14.28″E)附近(具体经纬度参见图 10 中间图上半部分所示的经纬度).

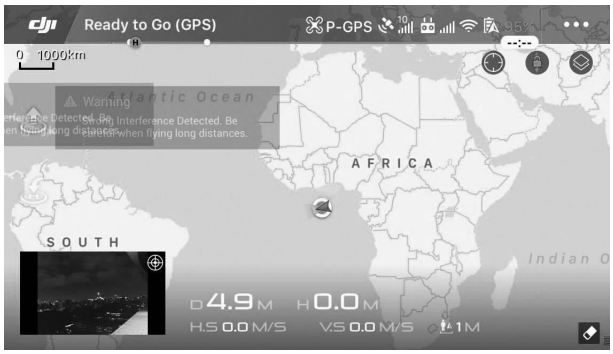

图 8 GPS 欺骗无人机效果图 1
(测试无人机为大疆精灵 3 标准版)

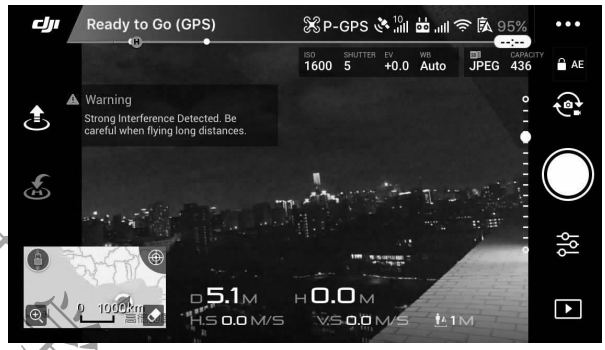

图 9 GPS 欺骗无人机效果图 2
(测试无人机为大疆精灵 3 标准版)

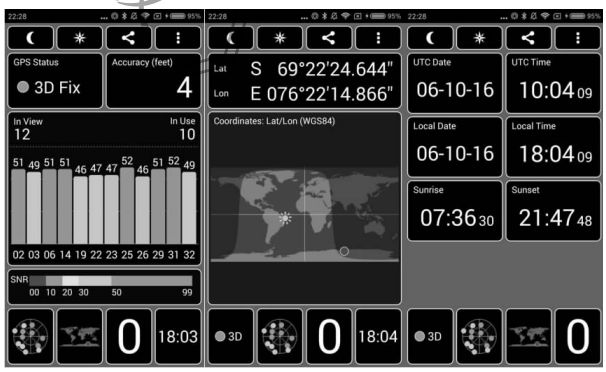

图 10 GPS 欺骗手机效果图
(测试手机为红米 1,测试软件为 GPS Test)

利用上述动态改变欺骗点的 GPS 欺骗系统和一套特定的策略,我们实验室已研发一套无人机管控系统,实现对一架大疆精灵 3 无人机进行了诱导,并使其按照我们的意图飞行.图 12 显示了一架大疆精灵 3 无人机在我们 GPS 诱导设备的控制下按照‘8’字轨迹飞行.

图 11　GPS 欺骗手机效果图
（左侧测试手机为 iPhone 6，测试软件为高德地图；
右侧测试手机为红米 note 4，测试软件为百度地图）

图 12　控制无人机按照'8'字轨迹飞行

对于 GPS 欺骗的危害，科学界和工业界早已有了较为全面的认识，并提出了很多的应对方法. 当前 GPS 反欺骗方法可分为以下几类：

（1）检测 GPS 信号的物理层特性. 真实的 GPS 信号来自于分布于天空中不同位置的 GPS 卫星，其与当前 GPS 接收机的距离和角度不同，所以其 GPS 信号到达 GPS 接收机时的信号的很多物理层特性也不同. 而 GPS 欺骗信号往往是通过一个天线发射出来的，其很多物理层特性往往相同或者相近. GPS 接收机可以对 GPS 信号的一些物理层特性进行检测来判断当前 GPS 信号是否为欺骗信号. GPS 接收机可以输出很多物理层特性的观测值（部分物理层特性的获取可能需要对 GPS 接收机进行设置），例如，自动增益控制（AGC）的值[36-37]，各颗卫星信号的接收信号强度（RSS）[38-39]，载波相位值、信号到达方向等[38]. 文献[36-38]提出了利用 GPS 信号的自动增益控制（AGC）来检测所接收到的信号是否为欺骗信号. 文献[39]介绍了根据接收信号强度和噪音等值来检测 GPS 欺骗. 文献[40]介绍了基于信号到达方向检测 GPS 欺骗的原理，并提出了根据 GPS 信号的到达方向的欺骗检测方案. 文献[41]提出了一种基于检测相关峰功率绝对值的欺骗检测方案.

（2）通过一些辅助设备来检测 GPS 信号. 比如通过使用高精度 IMU 或者全球卫星导航系统（Global Navigation Satellite System，GNSS）等作为辅助定位手段，当 GPS 定位的位置与辅助定位的位置的差距超过阈值后，则认为当前的 GPS 信号有可能是欺骗信号[42-44]. 文献[45]则提出了使用多个 GPS 天线组成的阵列来检测 GPS 欺骗并可以不受欺骗信号的影响，获得正确的定位.

（3）通过密码学的方式来验证 GPS 信号. 具体可以采用以下几种方案来检测 GPS 欺骗信号[41,46-47]：①采用类似于军码（P 码）的不可预测的 PRN Code；②验证广播者的数字签名来验证；③通过对比军码和民码的伪随机噪声的观测值.

我们实验室在对国内外 GPS 反欺骗技术进行研究和总结的基础上，实现了一种基于多普勒频移的 GPS 欺骗检测技术. 接收机与波源相对运动的时，会产生多普勒效应，即接收机接收到的信号的频率不再等于信号的发射频率. 而波源的发射频率与接收机的接收频率之间的差值即为多普勒频移.

当前基于多普勒频移的欺骗检测主要是根据以下几个方面：

（1）对于单天线的 GPS 欺骗攻击，其不同卫星信号的多普勒频移往往具有同样的变化规律，而 GPS 卫星在太空中分布的位置和运动速度往往并不相同，GPS 接收机所检测到的多普勒频移也往往不同；

（2）由于 GPS 欺骗发射器与被攻击的 GPS 接收器距离远远小于接收机与 GPS 卫星的距离，所以当接收机在做运动的时候，GPS 欺骗信号的多普勒频移值的变化率更高.

当前的多普勒频移检测往往采用检测不同 GPS 卫星信号的多普勒频移的变化规律是否相同的方法. 这是一种检测 GPS 欺骗的有效手段，能够检测大多数单一信号源的 GPS 欺骗.

然而，对一些更为高级的 GPS 欺骗，效果则较差. 比如，当攻击者采用多个 GPS 发射器来发射 GPS 欺骗信号，即每个 GPS 发射器发射一个特定卫星的 GPS 信号. 这样，不同卫星欺骗信号的多普勒频移

就可以不再具备相同的变化规律,从而使基于原理(1)的欺骗检测技术失效.甚至,攻击者可以在欺骗的过程中,动态地改变发射 GPS 信号的信号频率,以避免被基于原理(2)的多普勒频移的 GPS 欺骗检测方法检测出来.

我们所提出的基于多普勒频移的欺骗检测技术是在当前基于多普勒频移的欺骗检测技术的基础之上,设计的一种对比 GPS 信号多普勒频移值的欺骗检测算法.

步骤为:

步骤 1. 通过接收机的载波跟踪环路,获取当前卫星 s 信号的多普勒频移值 $f_{\mathrm{dr}}^{(s)}$,并且统计各个卫星的多普勒频移值,若有相同的变化规律则发出 GPS 欺骗警报并执行步骤 1,否则,则执行步骤 2;

步骤 2. 根据卫星 s 与接收机的单位观测向量 $\boldsymbol{I}$、卫星运行速度 $v^{(s)}$ 和接收机的移动速度 v,以及与发射频率 f 对应的信号波长 λ,按照如下公式得到 GPS 卫星的多普勒频移的理论值 $f_{\mathrm{d}}^{(s)}$:

$$f_{\mathrm{d}}^{(s)}=-\frac{(v^{(s)}-v)\cdot\boldsymbol{I}^{(s)}}{\lambda}.$$

步骤 3. 通过对比理论的多普勒频移值 $f_{\mathrm{d}}^{(s)}$ 和实际获取的多普勒频移值 $f_{\mathrm{dr}}^{(s)}$ 来进行欺骗检测.若两者的误差大于预设的发着则发出 GPS 欺骗警报,然后执行步骤 1.

表 1 对当前的 GPS 反欺骗技术进行了汇总和归纳.通过表 1 我们可以看出,以上检测 GPS 欺骗的方法各有利弊.检测 GPS 信号物理层特性中的几种方法,比如检测 GPS 信号的自动增益(AGC)和信号强度(RSS)这两种方法只能检测较为简单的 GPS 欺骗攻击;而根据 GPS 信号到达方向来检测 GPS 欺骗的方案虽然可以有效地检测 GPS 欺骗,但其处理大量的数据需要大量的计算能力和电力,显然不适合无人机系统.基于多普勒频移的 GPS 欺骗检测技术可以检测绝大多数的单天线发射的 GPS 欺骗,对于更高级的 GPS 欺骗也有很强的检测能力,但是并不是所有的 GPS 芯片都支持输出多普勒频移值.通过密码学方式中的验证签名的方法也无法短时间内实现.而通过一些辅助设备来检测 GPS 欺骗的几种方案则较为适合无人机.由于当前无人机普遍具有惯性导航装置,虽然精度可能不是很高,但是可以通过对比惯性导航的数据和 GPS 定位数据来检测多数的 GPS 欺骗.通过其他 GNSS 来检测 GPS 欺骗是最为可行的方案,该方案采用对比两个或多个星座的位置和时间信息的方法来检测当前 GPS 信号是否为欺骗信号.综上所述,当前无人机检测 GPS 欺骗可以采用多 GNSS 定位的方案、基于多普勒频移的欺骗检测方案和采用军码来验证 GPS 信号的方案.

表 1 GPS 反欺骗技术汇总

方法	简介	具体技术分类	缺点
检测 GPS 信号的物理层特性	通过观测 GPS 信号的自动增益控制(AGC)的值,各颗卫星信号的接收信号强度(RSS)、载波相位、信号到达方向和多普勒频移等来检测 GPS 欺骗	当 GPS 欺骗信号出现时,接收机接收到的振幅是真假信号的叠加值	仅能在 GPS 攻击开始等阶段检测 GPS 欺骗
		验证 GPS 信号的到达方向	至少需要 6 秒的时间来处理数据,才可判定 GPS 欺骗,功耗较大
		验证 GPS 接收器接收到的 GPS 信号强度	此种方式对高级的 GPS 欺骗无效
		根据多普勒频移规律来检测 GPS 欺骗	多数 GPS 芯片并不支持
通过其他导航技术检测 GPS 欺骗	通过对比 GPS 和其他导航技术的数据,检测 GPS 欺骗	GLONASS 或者北斗卫星导航系统	需要接收器支持或者添加额外的设备等
		惯性导航系统	需要加速度计等
		其他定位系统	需要相应的技术支持
通过密码学的方式来检测 GPS 欺骗	通过密码学的方式来验证接收机收到的 GPS 信号是否是欺骗信号	采用类似于军码的不可预测的 PRN Code;	接收机须携带加密过的密钥且密钥易被窃取
		验证广播者的数字签名来验证	需改变 GPS 信号格式和 GPS 接收机,同时存在延时
		通过对比军码和民码的伪随机噪声的观测值	需要一个在安全环境下的接收器

5 无人机通信安全

无人机是在地面站的指导和控制下完成飞行任务的,无人机和地面站之间依靠通信链路进行控制命令和数据的交互.卫星通信一般采用的是 Ku 波段战术通用数据链(Tactical Common Data Link,TCDL),无人机和地面站之间的通信采用的是 C 波段的无

线电信号[48]、2.4GHz 频段的无线信号或无线数传等方式. 文献[49]提到无人机和地面站之间的通信存在的威胁有网络监听、欺骗攻击、拒绝服务攻击和信号干扰[48].

5.1　无线电遥控安全

在 GeekPwn(极棒)2015 嘉年华上，来自腾讯的选手利用大疆无人机的漏洞和无线劫持技术，劫持了一架正在飞行的无人机，该无人机的型号是大疆精灵 3，选手攻破无人机防御机制并夺取了无人机的控制权. 精灵 3 所采用的射频芯片是 BK5811，腾讯的研究人员发现该芯片在某个频道进行数据发送时，会同时把数据发送到邻近的其他频道上. 研究人员以这个漏洞为突破点，找到了 16 个调频点和调频序列，接着研究人员只要在跳频后、遥控器发送信号之前的时间段，就可以控制无人机. 腾讯的研究人员利用信道的信息泄漏漏洞和信号覆盖漏洞取得了无人机的最高控制权①.

5.2　WIFI 通信安全

目前市场上常见的民用无人机如 Parrot、大疆等，都是可以通过 WIFI b/g 的方式实现无人机和手持智能设备的通信，Parrot AR. Drone 2.0 无人机只支持智能设备通过 WIFI 操控无人机，大疆的 Phantom 3 系列无人机可以用智能设备通过 WIFI 连接实现无人机定点巡航、一键返航设置和图像传输等功能. 智能设备对无人机有比较大的控制权，如果 Wi-Fi 通信链路出现了安全威胁，那么无人机的图像、视频等数据将会遭到泄漏，甚至无人机将会被俘获.

Aircrack-ng② 是一个评估 WIFI 网络安全的工具套件，它可实现对 WIFI 网络的监控、攻击、测试和破解，Aircrack-ng 可运行在 Linux、Windows、FreeBSD、OS X 等多种操作系统上，网卡在监控模式下，可以嗅探到附近的 WIFI 热点和连接到这个热点上的客户端，以及该 WIFI 热点的 MAC 地址、通道号、信号强度等信息. 对于无人机和智能设备的连接，无人机会建立一个 WIFI 热点，智能设备连接上这个热点后，就可与无人机进行通信，使用 airplay-ng 工具向连接无人机的智能设备发送解除认证(Deauthentication)信号，可实现断开无人机和智能设备之间建立的 WIFI 通信链路. 基于此工具可实现对无人机 WIFI 链路的攻击.

由于 Parrot AR. Drone 2.0 无人机采用公开的 WIFI 连接进行无人机的控制，Sammy Kamkar 利用该无人机的这个脆弱性，在 2013 年发布了一个可以用一架无人机去控制别的无人机的软件 SkyJack. 该软件就是基于 Aircrack-ng 实现的，可以运行在另一架无人机或其他的运行有 Linux 系统的平台上，在 WIFI 的通信范围内，该软件利用工作在监控模式下的网卡嗅探并断开目标无人机的通信链接，然后连接目标无人机，进而夺取无人机的控制权③.

大疆无人机的遥控器拥有对无人机的优先控制权，在一定程度上增加了安全性. 此外，大疆无人机引入了中继器来增加移动设备和无人机的通信距离，移动设备通过连接中继器建立的 WIFI 热点来接收无人机的视频、飞行状态等数据，此 WIFI 链接通过 WPA/WPA2 加密，增加了攻击者通过 WIFI 攻击无人机的难度，用户在使用的过程中一定要修改 WIFI 热点的密码，使之较为复杂，进一步提高安全性. 但是该 WIFI 链接仍然无法抵抗“解除认证(Deauthentication)”攻击，我们实验室对大疆 Phantom 3 系列无人机做了“解除认证”的攻击实验，利用 Edimax 无线网卡和 Aircrack-ng 工具可以轻易的断开无人机和移动设备之间的 WIFI 通信链路. 其攻击实验步骤如图 13 所示.

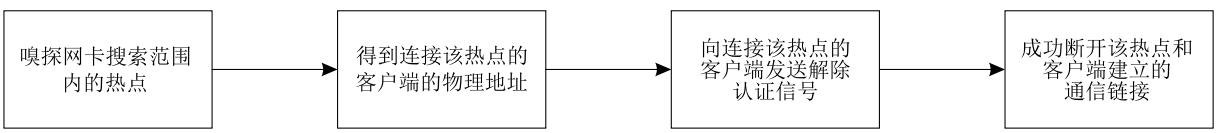

图 13　解除认证攻击实验步骤

5.3　eCLSC-TKEM 通信协议

在许多无人机相关的应用当中，无人机需要与传感器或嵌入式设备等智能实体进行通信. 因此需要高效的密钥管理协议确保通信安全. 协议的设计需要考虑智能实体受限的资源和无人机的移动性. 文献[50]提出了一种无人机与智能实体的安全通信协议. 作者设计了一种有效的无证书的签密标签密钥封装机制，简称为 eCLSC-TKEM，来支持所要求的安全功能，包括认证密钥建立、不可否认性和用户可撤销.

① https://security.tencent.com/index.php/blog/msg/103
② http://www.aircrack-ng.org/
③ Crook J. Infamous Hacker Creates SkyJack To Hunt, Hack, And Control Other Drones? Internet: http://techcrunch.com/2013/12/04/infamoushacker-creates-skyjack-to-hunt-hack-and-control-other-drones/

5.4 ADS-B 安全

文献[51]说明了 ADS-B 在无人机的应用中存在的安全威胁. ADS-B 的全称是广播式自动相关监视(Automatic Dependent Surveillance Broadcast),它的作用是无需人工操作,就可以从机载设备获取飞机的位置、速度、航向、高度、识别号等,并将这些信息广播出去,地面站和其他飞机可以接收到这些信息,从而管制人员可以对飞机的状态进行有效的监控. 全球大部分民航飞机都装配有 ADS-B 系统,而民用无人机很少有装配此系统的.

近年来,无人机产业蓬勃发展,无人机在航拍、农业、快递、电力等诸多行业开创崭新应用的同时,也存在大量的"黑飞"现象,无人机的不规范飞行延误民航客机的新闻也屡次见诸报端. 为给无人机操控者提供有效的民航客机的飞行路线,大疆公司在 2017 年 2 月首次在大疆经纬 M200 系列无人机上安装了 ADS-B 系统,到目前为止大疆 M200 系列、M600 系列等多款无人机装配了 ADS-B 系统,为了减少给民航系统造成干扰,这些无人机安装的仅仅是 ADS-B 的接收器,用来探测空中交通数据并反馈给飞手,该系统可搜索周围出现的民航信息,指导无人机飞手及时避开民航客机,以免造成不必要的损失.

无疑,ADS-B 系统将会是下一代航空管理系统的一部分,它会把民航客机,甚至无人机当前的位置、飞行方向、速度和目的地等信息广播出去,主要用于避免碰撞事故的发生. 由于 ADS-B 广播的信息针对附近所有飞机,所以它传输的数据是没有加密的,这就很容易造成虚假信息注入攻击. 对 ADS-B 的攻击有两种形式,一是干扰,使无人机无法正常接收到 ADS-B 数据,二是广播虚假的 ADS-B 数据. 前者可能使无人机无法避免碰撞,后者可能迫使无人机在任务执行中偏离航向. 对于简单的 ADS-B 攻击,可以采用多点定位(MLAT)的验证方法,去检测 ADS-B 数据是否存在伪造,但是此验证机制可以很容易地绕过[52].

5.5 无人机通讯安全小结

无人机通信链路是无人机的重要组成部分,也是最易受到攻击的部分. 通信链路层容易发生的攻击有网络监听、欺骗攻击、拒绝服务攻击和信号干扰等,本文列举了通信链路层常见的攻击方法,如无线电遥控信号欺骗、WIFI 控制信号欺骗和 ADS-B 信号攻击等.

这些已知的安全漏洞能给无人机的设计和研究者一定的参考价值,在设计无人机系统时要避免这些漏洞. 另外,比较重要的是在考虑的无人机系统严重受限的能源和计算等资源的基础上,设计出高效、安全的通信协议,这样即使无人机的通信链路遭到窃听或破坏,也不至于泄漏信息或失去控制权.

6 无人机软件安全

6.1 飞控软件概述

无人机飞控软件一般分为导航系统、飞行控制和任务管理三大模块[53]. 飞控软件配合传感器,管理设备,使得无人机能够自主飞行[54-55]. 我们把飞控软件分为四个层级,包括:组织层、分析决策层、执行层和支持层,这些层级相互协作通过读取导航指令,采集传感器的数据来实现对无人机的控制[56]. 同时,实时操作系统也被引入到无人机软件技术,我们从初始化、数据输入、软件控制、数据输出四个部分来叙述飞控的流程及功能.

(1)初始化模块. 在无人机起飞前,飞控软件会自行检查传感器模块以及飞机设备是否有异常;

(2)数据输入模块. 传感器采集无人机的经纬度、高度、时间等各种信息,并通过 RS-232 等通信协议输入飞控软件,统一进行解码处理;

(3)软件控制模块. 一方面计算传感器搜集来的多方面信息,另一方面协调各个飞行模块,实现无人机的自主飞行;

(4)输出数据模块:输出数据模块主要将无人机的经纬度信息,高度信息以及飞控各个参数信息传送给地面站控制系统.

6.2 Maldrone 无人机软件漏洞

图 14 所示的是,一般无人机的飞控软件管理系的结构图. 通过图 14 我们可以看到,飞控软件已经具备了强大的飞行控制能力,然而,飞控软件技术快速发展的同时,飞控软件受到的威胁也层出不穷[57-58]. 大部分的飞控系统在控制端都存在一定的软件安全漏洞,别有用心的黑客常常利用这些漏洞来干扰无人机的正常飞行. 2015 年 6 月发布的 Maldrone 无人机软件漏洞,是基于 Parrot AR 无人机嵌入式平台开发的一个针对无人机 ARM 芯片和 Linux 系统的攻击程序. 攻击者通过入侵无人机网络来接入无人机,在控制端安装后门程序. 安装成功后的程序开始在后台监听无人机传感器的数据采

集.同时攻击者通过操控端对无人机进行远程操控.攻击者通过该软件漏洞最终夺取了无人机的控制权限①.

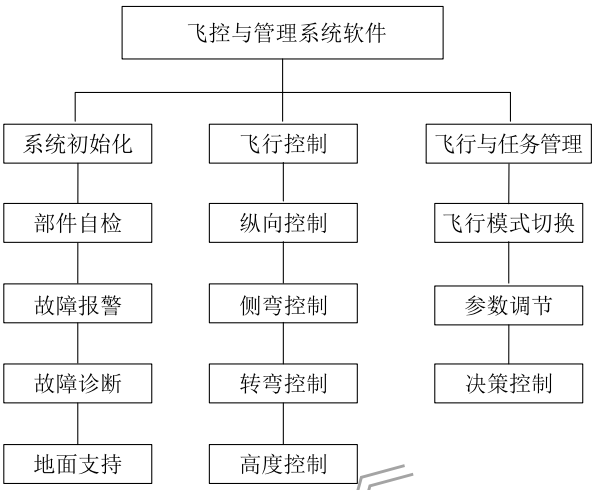

图 14　飞控软件管理系统

6.3　Zigbee 芯片威胁

无人机的信号传输模块存在许多安全问题.这里以 xbee 芯片为例,xbee 芯片是基于 Zigbee 技术的一个信号传输模块.2016 年一名德国无人机研究者发现大多数的无人机 xbee 芯片只是受到有线等效保密技术(WEP)的保护,而并没有采用严格的加密技术.攻击者可以在地面控制端植入命令代码,从而对 xbee 芯片进行中间人攻击,同时再通过破解 WiFi WEP 加密技术来断开无人机控制端的连接.攻击者还可以通过复制控制端的命令来完全控制无人机.为避免无人机受到类似的攻击,最有效的应对方式就是对信号传输模块固件进行升级以及对无人机与地面站传输的流量进行严格加密②.

6.4　键盘木马威胁

键盘木马病毒也称为 keylogger,是一种系统监控软件.Keylogger 当中采用了软件驱动的监控类程序,监控用户在计算机键盘上所作的每一次击键.2011 年,keylogger 病毒通过工作人员使用硬盘或可移动设备入侵到美国内华达州克里奇空军基地的控制站里.位于中东地区的无人机在执行任务的过程中会将数据与该地面站进行交互,而每一次的数据交互和指令都会被病毒记录下来③.

6.5　无人机移动端安全检测技术

目前,无人机存在多种操控方式,不仅可以通过遥控器来操控,同时也可以通过移动设备端来操控.而无人机移动设备对于潜在的软件威胁的检测主要有两种方式,它们包括:以特征码为基础的恶意软件识别方式[59-60]和以软件行为为基础的恶意代码检测方式[61].以特征码为基础的恶意软件识别方式依赖于恶意软件的逆向提取方法来对其进行判定,然后将其发布,当对移动设备端进行检测时,如果待测设备上检测到的恶意程序特征码与发布的特征码相同则该程序已受到恶意代码的入侵.而以行为检测技术为基础的恶意软件识别方式主要依赖于动静态检测来对程序的主要特征序列进行判断,直到确认该软件是否受到恶意代码的入侵[62].文献[63-64]使用机器学习的方式处理软件的特征码或者软件行为的数据,并据此来判断当前软件是否为恶意软件.

6.6　无人机地理围栏技术

无人机灵活度高、隐蔽性强的特性使得其能够在不被安防设备察觉的情况下入侵到私人区域,监视人们的正常生活,扰乱正常秩序.对无人机具有的危害,各国空管部门以及民间组织都制定了对无人机的管理规定,无人机必须在规定的空域中飞行.NoFlyZone 是一个能够录入 GPS 位置信息,将相关坐标上传到无人机生产商服务器里的民间组织,用户只需输入自己的家庭住址并提供一些基本信息便能在该组织服务器中进行备份存档,该组织使用其中的数据划定禁飞区域,当无人机飞跃已注册房屋时,无人机移动客户端便会弹出禁止命令对话框,提示无人机操作者不得擅自侵入他人领空④.

6.7　无人机软件安全总结

无人机飞控软件安全技术是近几年才兴起的新技术.传统的软件安全都是从执行机的角度来分析,而现如今的飞控技术主要通过将传感器与执行机进行相联来完善整个体系,同时从所连接的传感器的角度来分析不同的攻防情况,可以预见,未来飞控软件安全发展趋势是朝更高速、更完备的方向发展[65].

对无人机的加密安全技术将加强研究,例如之前提到的 zigbee 芯片就没有采用加密安全技术,对加密技术的研究将会不断深入.

对无人机飞控系统植入木马的安全问题也将继续加强研究.

同时对无人机飞控中涉及的政策、法规监管盲区存在的安全问题,需要加强鉴定.

---

① How to remotely hijack drones? Secret the first UAV back door http://www.freebuf.com/news/57690.html

② Watch Black Hat Asia black hat Asia Summit: UAV and fly away http://www.freebuf.com/news/100625.html

③ The security challenges facing the human computer-who moved my drones?http://www.360doc.cn/article/633076_168061138.html

④ NoFlyZone to help you set up a no fly zone over your house. http://techcrunch.cn/2015/02/23/noflyzone-lets-you-establish-a-no-fly-zone-over-your-property/

7 无人机网络安全

7.1 无人机网络

在特定场景下,无人机可能需要多机协同执行任务,这就需要搭建无人机之间的信息连接通道,形成一个无人机 Ad hoc 网络,无人机和地面站作为这种网络中的节点.处于网络中的无人机通过这一移动网络实现信息的实时共享,不再需要经过地面站的转发,从而有效地提高了无人机群的生存能力和作战能力.

7.1.1 无人机 Ad hoc 网络的特点

和传统的移动 Ad hoc 网络相比,无人机 Ad hoc 网络具有一些独有的特点:

(1)高速移动性.无人机自组网在实际应用中面临节点高速移动的问题,因此如何处理高速率节点移动与自组网稳定性之间的关系十分重要.

(2)面临强干扰环境.由于无人机执行任务时常处于敌对空间,电磁环境十分复杂且恶劣,因此无人机自组网对于强干扰应有一定的抵抗能力.

(3)高工作时间要求.无人机有一项重要的指标——空中停留时间.所以如何通过减小无人机自组网的功率以及减小通信终端的荷载来节省无人机能源,是设计无人机自组网需要考虑的重要因素.

(4)网络连用性.由于无人机的移动性,无人机之间的通信质量会降低,甚至导致通信的中断.另外,一个无人机的故障也会导致网络拓扑结构的变化.

(5)节点数量.无人机 Ad hoc 网络中无人机节点的数量平均为 3 到 4 架.

(6)实时性.通常,无人机 Ad hoc 网络都是基于实时性的任务应用,比如航空拍照、视频监控和环境监测等.

由此可见,设计出具有高度可适性、强抗干扰性并且高效节源的无人机网络具有重要的意义[66].

根据以上特点,文献[67]提到存在两种网络组织结构与无人机网络的需求相似:无线传感器网络(Wireless Sensor Networks,WSNs)和移动 Ad Hoc 网络(Mobile Ad-hoc Networks,MANETs).但由于 WSNs 覆盖范围远远小于无人机网络,并且无人机网络也不需要设立一个类似 WSNs 网络里的中心节点,相较而言,移动 Ad Hoc 网络是目前较为适合用于无人机网络的网络结构[67-70].

7.2 无人机网络面临的威胁

由于无人机 Ad hoc 网络是移动 Ad hoc 网络的一个子类,移动 Ad hoc 网络中常见的攻击同样会威胁到无人机 Ad hoc 网络,如虫洞攻击、Rushing 攻击、联合攻击、Sybil 攻击、拒绝服务攻击和窃听攻击等[71-72].

首先,MANETs 中所有的信号都通过不断变化的无线链路传播,正处于工作状态而没有足够保护的移动节点(即无人机本身)很容易被劫持和捕捉,因此无人机网络比固定的网络连接更容易受到攻击.攻击者可以监听所有无线通信信道甚至修改其中的信息,也可以伪装成为一个通信参与者直接使用信道.但由于 MANETs 网络没有任何中央支持基础设施,基于公钥密码体制的认证机制很难在其中实施.

第二,移动节点独立漫游,并且能够在任何方向上进行移动,因此,任何静态配置的安全解决方案对于动态变化的网络拓扑结构都是无法适用的.路由可以在源节点和目标节点之间建立,而网络拓扑结构中节点之间的信息交换大多数是由 MANETs 的路由协议完成的.所以,任何攻击者都可以恶意地使用格式正确的伪装路由来合法更新网络节点存储的路由表,比如可以很容易地启动拒绝服务.如果一个恶意节点向网络中发布虚假的路由信息,其他节点可能会在不知不觉中传播虚假消息.

第三,无人机网络的决策依赖于所有节点的参与和协作,恶意节点可以简单的阻止或者修改遍历它的流量,通过拒绝合作来打破合作算法.某些入侵检测机制对这种行为束手无策.

最后,作为 MANETs 节点的无人机是以电池或者其他手段作为能源的,这些能源很容易枯竭.攻击者可以创建一种新类型的拒绝服务(DoS),迫使节点重新传播数据包来耗尽它的能量.由于无人机节点网络的带宽容量、节点的电池容量等限制条件以及节点本身的高速移动导致了 MANETs 网络连接频繁中断,这种攻击方式也是很难检测出来的[73].

综上所述,无线自组的无人机网络是非常脆弱的.由于其节点基本处于开放环境及特有的动态拓扑结构,无人机网络并不具有很强的约束能力.现有的有线网络的安全解决方案也不能直接应用于无人机网络.

7.3 无人机网络的安全防护

基于无人机无线自组网多跳方法和节点分布方式这两个显著特点,总的来说有两种安全防护手段:

主动防护和被动防护. 主动防护是一种积极的防护方式，目的是消除安全威胁，通常是使用各种信息加密技术. 而被动防护旨在检测到安全威胁后做出恰当的反应. 这两种方法各有优劣，适用于整个领域中的不同类型问题，在实际使用中应针对不同环境进行选择. 例如，主动防护可以应用于路由协议，以确保移动节点之间的路由交换；而被动防护方法则广泛应用于保护数据包的转发操作.

完整的无人机无线自组网的安全解决方案应该结合主动和被动两种防护方式，包括三个组成部分：预防、检测和反应. 预防将显著提高攻击者入侵系统的难度，但是无数历史实践已经表明，无论设计预防机制时如何仔细，系统也不可能完全抵御入侵. 因此，有效的入侵检测和反应措施对避免持续的不利影响是必不可少的[74].

文献[75]提出了基于认知无线电(Cognitive Radio)系统的提高无人机网络可靠性和安全性的方法，提出了认知无线电在无人机网络防护和故障恢复方面的新见解. 文献[76]提出了一个安全的无人机 Ad Hoc 网络路由协议设计模型，它定义了身份验证、保密性和完整性服务，也尽可能减少了信令开销，保证了无人机的网络资源可以有效地进行数据交换. 文献[77]提出了运用贝叶斯博弈论(Bayesian Game-Theoretic Methodology)的方法检测无人机网络入侵，有效地平衡了无人机网络节点在入侵检测中的开销与检测正确率之间的关系，在提高无人机网络性能的同时实现了安全检测.

文献[71]提出多种针对无人机无线自组网的网络层的主动攻击类型，如表 2 所示：

(1) 黑洞(Black hole). 在这种攻击中，恶意节点利用路由协议，伪装自己是位于它期望截取数据包的目标节点的最短路径上的节点，欺骗目标节点从而截取数据.

(2) 拒绝服务(DoS). 当网络被恶意节点劫持时，拒绝服务的攻击有多种形式，其中经典的方式是集中攻击资源，使网络操作出错或者崩溃. 例如，恶意节点频繁产生不必要的路由信息，使网络资源不可用于其他节点.

(3) 路由表溢出(Routing table overflow). 攻击者试图创造路由通往不存在的节点，目的是使新路由的创建被阻止或者路由协议的实现被淹没.

(4) 模仿(Impersonation). 一个恶意节点可以在发送控制数据包时扮演另一个节点，在路由表中创建一个异常更新.

(5) 能量消耗(Energy consummation). 能源是无人机 Ad hoc 网络中的一个关键参数. 电池的省电措施是在确定必要的时候才会为传输通信进行供电. 攻击者可以通过请求路由或者转发不必要的数据包到下一个节点来消耗能量.

(6) 信息披露(Information disclosure). 恶意节点可能透露给没有得到授权的用户机密信息，从而使攻击者可以知道哪些节点位于目标路由上.

表 2　主动攻击类型对比

主动攻击类型	工作原理	是否攻击计算资源	是否攻击能源	是否截取信息
黑洞	欺骗并伪装成为最短路径上的节点	否	否	是
拒绝服务	产生不必要的路由信息，占用网络资源	是	否	否
路由表溢出	创建路由到不存在的节点，淹没路由协议	是	否	否
模仿	扮演另一个节点，创建一个异常更新	是	否	否
能量消耗	请求路由、转发不必要的数据包来消耗能源	是	是	否
信息披露	泄露机密信息给未授权的用户	否	否	否

文献[74]介绍了几种在协议防护中需要用到的消息认证方法并分析利弊：

(1) 哈希运算消息认证码(Hash-based Message Authentication Codes，HMAC). 使用哈希算法，输入为一个消息和一个密钥，然后生成消息摘要作为输出. 然而，HMAC 方法只能由接收者验证，故其不适用于广播消息认证.

(2) 数字签名(Digital signature). 信息发送者产生的无法伪造的一串数字，它可以证明信息发送者所发送信息的真实性. 但是，它为拒绝服务(DoS)攻击创造了条件，因为攻击者可能会向受害者节点提供大量虚假签名信息，用以耗尽受害者的计算资源[78-79].

(3) 单向 HMAC 密钥链(One-way HMAC key chain). 许多加密算法是单向函数，给出输出 $F(x)$，但是无法找出对应的 x. 这种输出函数可以用于产生相反的顺序对消息身份进行验证[80].

表 3 对这几种消息认证进行了对比. 无人机无线自组网的网络层安全所关注的是网络功能的保护，以确保移动节点之间交换的路由消息是一致的协议规范.

Maxa 等人[79]基于移动 Ad hoc 网络中性能最优的 AODV(Ad hoc On demand Distance Vector)协议，并整合了 MSAODV 和 AODV-SEC 协议的一

些特性，为了能有效抵御虫洞攻击，他们在新的协议中加入了 TIK(TESLA with Instant Key Disclosure)算法.进一步，为了保证认证性、完整性和保密性的安全需求，他们还在新的协议中运用了对称和非对称的加密方法.表 4 是新的安全路由协议用到的算法.

表 3 消息原语的加密认证方式对比

消息原语的加密认证方式	工作原理	存在的缺陷
哈希运算消息认证码	使用哈希算法，输入为一个消息和一个密钥，生成的消息摘要作为输出	只能由接收者验证，不适用与广播消息认证
数字签名	发送者产生的无法伪造的一串数字串以证明真实性	针对拒绝服务(DoS)攻击则不太灵活，易被耗尽计算资源
单向 HMAC 密钥链	利用单向函数产生相反的顺序对消息身份进行验证	

表 4 安全路由协议的组成

安全服务	加密机制	算法
认证性	数字签名，mCert	RSA
完整性	哈希函数	SHA-1
保密性	对称和非对称加密机制	AES DES
抵御虫洞攻击	数据包限制(Packet Leashes)	TIK

8 总结和展望

本文从无人机安全角度出发，从传感器、通信、软件和无人机网络等方面，对当前无人机所遇到的安全问题以及相应的解决方案进行了分析和总结，并根据当前无人机暴露出来的安全问题，对无人机安全的未来研究进行展望[81].

随着科技的进步和制造成本的进一步降低，无人机的数量将越来越多，性能也将大大提高，其应用也将越来越广泛.在未来的智慧城市中，电力和管道巡检无人机、快递无人机以及警用安保无人机将大量出现.综合来看，未来无人机的安全研究工作将从以下几个方面来展开：

(1)传感器安全.传感器是无人机获取外界数据的重要组件.当传感器受到干扰或者欺骗，无人机则无法获取自己当前的真实状态信息，很有可能会因此做出错误的反应，这很有可能会影响无人机的飞行安全.所以，我们不仅要继续发掘传感器存在的安全隐患，同时也要设计相应的算法来规避这些安全隐患所带来的不利影响.

(2)通信安全.无人机与地面站的通信方式包括无线电、无线数传、WiFi 和无线图传等，无人机在不同的通信链路上都存在不同程度的安全威胁.除了避免使用比较脆弱的通信方式外，设计出高效加密的通信协议将是未来的一项重要的研究工作.

(3)软件安全.软件安全主要是指无人机和地面站的控制软件安全.在软件设计和编码时，应将其放入到整个运行系统中进行分析，考虑软件、操作人员和系统之间的相互影响，尽量避免产生漏洞、采用更加安全的加密技术和协议.例如，本文 6.3 节中提到的 zigbee 芯片威胁就是因为没有采用加密安全技术.同时，对于无人机飞控系统植入木马的安全问题也将继续加强研究.

(4)无人机网络安全.无人机的无线自组网络是一种比传统有线、无线网络更加灵活的网络组织形式，最大的安全问题在于其动态的拓扑结构，没有中央基站提供约束，所以路由安全在整个网络安全中起着重要的作用.因此，有必要设计新的高效安全的路由协议，妥善解决这些高流动性的特点带来的安全隐患.

(5)无人机的自我保护.无人机在飞行过程中可以依赖的定位装置有卫星导航传感器(GPS、GLONASS 等)、运动传感器(加速度计、陀螺仪等)和视觉定位系统(摄像头等)，虽然运动传感器和视觉定位系统的定位精度不及卫星导航系统，但是在无人机遭到卫星导航欺骗攻击和通信攻击，无人机检测到受到攻击后，借助于运动传感器和视觉定位系统按照受到攻击前记录的飞行轨迹安全返回是一个有效的自我保护措施.

(6)隐私安全.消费机无人机市场蓬勃发展，由于缺乏有效的监管，有半数以上的无人机都在“黑飞”，配置有摄像头的无人机盘旋在高空，悬停在私人住宅的窗前，在一定程度上侵犯了公民的隐私，除了政府出台相应的法律法规规范无人机的飞行外，如何从技术手段上限制无人机拍摄的内容，从而保护公民的隐私安全，也是未来的一个重要的研究方向.

参 考 文 献

[1] Zhang Tian-Hang, Bai Jin-Ping. Development and trend of unmanned rotorcraft. Artificial Intelligence and Robotics Research, 2013, 2: 16-23(in Chinese)
(张天航，白金平. 旋翼式无人机的发展和趋势. 人工智能与机器人研究，2013，2：16-23)

[2] Goraj Z. UAV platform designed in WUT for border surveillance //Proceedings of the American Institute of Aeronautics and Astronautics (AIAA). Rohnert Park, USA, 2007: 1-18

[3] Kopeikin A, Ponda S, Johnson K, How J. Multi-UAV network control through dynamic task allocation: Ensuring data-rate and bit-error-rate support//Proceedings of the IEEE GLOBECOM Workshop on Wireless Networking for Unmanned Autonomous Vehicles. Anaheim, USA, 2012: 1579-1584

[4] Honkavaara E, Saari H, Kaivosoja J, et al. Processing and assessment of spectrometric, stereoscopic imagery collected using a lightweight UAV spectral camera for precision agriculture. Remote Sensing, 2013, 5(10): 5006-5039

[5] Grenzdörffer G, Engel A, Teichert B. The photogrammetric potential of low-cost UAVs in forestry and agriculture// Proceedings of the International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences. Beijing, China, 2008, 37(B1): 1207-1213

[6] Caris M, Stanko S, Sommer R, Wahlen A. SAPape—Synthetic aperture radar for all weather penetrating UAV application// Proceedings of the 14th International Radar Symposium (IRS). Dresden, Germany, 2013: 41-46

[7] Li Zong-Nan, Chen Zhong-Xin, Wang Li-Min, et al. Area extraction of maize lodging based on remote sensing by small unmanned aerial vehicle. Transactions of the Chinese Society of Agricultural Engineering, 2014, 30(19): 207-213(in Chinese)
(李宗南，陈仲新，王利民等. 基于小型无人机遥感的玉米倒伏面积提取. 农业工程学报，2014, 30(19): 207-213)

[8] Araar O, Aouf N, Dietz J L. Power pylon detection and monocular depth estimation from inspection UAVs. Industrial Robot: An International Journal, 2015, 42(3): 200-213

[9] Li Chao, Ke Zun-Jie, Chen Jiao. Application of quadrotor UAV in emergence surveying and mapping security in Yunnan. Surveying and Mapping of Geology and Mineral Resources, 2015, 31(3): 31-33(in Chinese)
(李超，柯尊杰，陈姣. 四旋翼无人机在云南应急测绘保障中的应用. 地矿测绘，2015, 31(3): 31-33)

[10] Javaid A Y, Sun W, Devabhaktuni V K, Alam M. Cyber security threat analysis and modeling of an unmanned aerial vehicle system//Proceedings of the IEEE Conference on Technologies for Homeland Security (HST). Waltham, USA, 2012: 585-590

[11] Wang W, Sun Y, Li H, Han Z. Cross-layer attack and defense in cognitive radio networks//Proceedings of the IEEE Globe Communication Conference (GLOBECOM) 2010. Miami, USA, 2010: 1-6

[12] Alves-Foss J. Multi-protocol attacks and the public key infrastructure//Proceedings of the 21st National Information Systems Security Conference. Arlington, USA, 1998: 566-576

[13] Carle G, Dressler F, Kemmerer R A, et al. Network attack detection and defense//Proceedings of the Manifesto of the Dagstuhl Dagstuhl Perspective Workshop. Dagstuhl, Germany, 2008: 15-25

[14] Barbeau M. WiMax802.16 threat analysis//Proceedings of the International Symposium on QoS and Security for Wireless and Mobile Networks (Q2SWinet). Montreal Quebec, Canada, 2005: 8-15

[15] Tao Feng, Timmermans H J P. Transportation mode recognition using GPS and accelerometer data. Transportation Research Part C, 2013, 37(3): 118-130

[16] He D J, Chen C, Chan S, et al. ReTrust: Attack-resistant and lightweight trust management for medical sensor networks. IEEE Transactions on Information Technology in Biomedicine, 2012, 16(4): 623-632

[17] Carman D W, Kruus P S, Matt B J. Constraints and approaches for distributed sensor network security. NAI Labs Technical Report No. 00-010, Network Associates Inc., New York, USA, 2002

[18] Shoukry Y, Martin P, Yona Y, et al. PyCRA: Physical challenge-response authentication for active sensors under spoofing attacks//Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. Denver, USA, 2015: 1004-1015

[19] Barbour N, Schmidt G. Inertial sensor technology trends. IEEE Sensors Journal, 2011, 1(4): 332-339

[20] Jose K A, Suh W D, Xavier P B, Varadan V K. Surface acoustic wave MEMS gyroscope. Wave Motion, 2002, 36(4): 367-381

[21] Castro S T, Dean R N, Roth G, et al. Influence of acoustic noise on the dynamic performance of MEMS gyroscopes// Proceedings of the International Mechanical Engineering Congress and Exposition. Washington, USA, 2007: 1825-1831

[22] Dean R N, Floers G T, Hodel A S, et al. On the degradation of MEMS gyroscope performance in the presence of high power acoustic noise//Proceedings of the IEEE International Symposium on Industrial Electronics. Vigo, Spain, 2007: 1435-1440

[23] Dean R N, Castro S T, Flowers G T. A characterization of the performance of a MEMS gyroscope in acoustically harsh environments. IEEE Transactions on Industrial Electronics, 2011, 58(7): 2591-2596

[24] Son Y, Shin H, Kim D, et al. Rocking drones with intentional sound noise on gyroscopic sensors//Proceedings of the 24th USENIX Security Symposium. Washington, USA, 2015: 881-896

[25] Roth G. Simulation of the Effects of Acoustic Noise on MEMS Gyroscopes [M. S. dissertation]. Auburn University, Alabama, USA, 2009

[26] Soobramaney P. Mitigation of the Effects of High Levels of High-Frequency Noise on MEMS Gyroscopes [Ph. D. dissertation]. Auburn University, Alabama, USA, 2013

[27] Adams S G, Bertsch F M, Shaw K. Capacitance based tunable micromechanical resonators//Proceedings of the 8th International Conference on Solid-State Sensors and Actuators, and Euro Sensors IX. Stockholm, Sweden, 1995: 25-29

[28] Jeong C, Seok S, Lee B, et al. A study on resonant frequency and Q factor tunings for MEMS vibratory gyroscopes. Journal of Micromechanics and Micro Engineering, 2004, 14(11): 1530-1536

[29] Kaplan E, Hegarty C. Understanding GPS: Principles and Applications. 2nd Edition. London: Artech House, 2006

[30] Wendel J, Meister O, Schlaile C, Trommer G F. An integrated GPS/MEMS-IMU navigation system for an autonomous helicopter. Aerospace Science and Technology, 2006, 10(6): 527-533

[31] Gong Zhen-Chun. Study and Application of GPS for Micro Unmanned Aerial Vehicle [Ph. D. dissertation]. Zhejiang University, Hangzhou, 2005(in Chinese)
(龚真春. GPS在微型无人机导航定位中的研究与应用[博士学位论文]. 浙江大学, 杭州, 2005)

[32] Huang L, Yang Q. GPS spoofing: Low-cost GPS simulator //Proceedings of the DEF CON Communications 23. Las Vegas, USA, 2015

[33] Jafarnia-Jahromi A, Broumandan A, Nielsen J, Lachapelle G. GPS vulnerability to spoofing threats and a review of antispoofing techniques. International Journal of Navigation and Observation, 2012, 2012(127072): 1-16

[34] Kerns A J, Shepard D P, Bhatti A J, Humphreys T. Unmanned aircraft capture and control via GPS spoofing. Journal of Field Robotics, 2014, 31(4): 617-636

[35] Faughnan M S, Hourican B J, MacDonald G C, et al. Risk analysis of unmanned aerial vehicle hijacking and methods of its detection//Proceedings of the IEEE Systems and Information Engineering Design Symposium (SIEDS). Charlottesville, USA, 2013: 145-150

[36] Akos D M. Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC). Navigation, 2012, 59(4): 281-290

[37] Bastide F, Akos D, Macabiau C, Roturier B. Automatic gain control (AGC) as an interference assessment tool//Proceedings of the 16th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GPS/GNSS 2003). Portland, USA, 2011: 2042-2053

[38] Warner J S, Johnston R G. GPS spoofing countermeasures. Homeland Security Journal, 2003, 25(2): 19-27

[39] Jahromi-Jafarnia A, Broumandan A, Nielsen J, et al. GPS spoofer countermeasure effectiveness based on signal strength, noise power, and C/N0 measurements. International Journal of Satellite Communications and Networking, 2012, 30(4): 181-191

[40] Psiaki M L, Humphreys T E, Stauffer B. Attackers can spoof navigation signals without our knowledge. Here's how to fight back GPS lies. IEEE Spectrum, 2016, 53(6): 26-53

[41] Cheng Xu-Wei, Tang Xia-Qing, Guo Li-Bin, Wu Meng. Research on GNSS receiver spoofing detection technology//Proceedings of the 6th China Satellite Navigation Conference. Xi'an, China, 2015(in Chinese)
(程旭维, 汤霞清, 郭理彬, 武萌. GNSS接收机抗干扰和欺骗检测技术研究//第6届中国卫星导航学术年会. 西安, 中国, 2015)

[42] Swaszek P, Pratz S, Arocho B, et al. GNSS spoof detection using shipboard IMU measurements//Proceedings of the 27th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+). Tampa, USA, 2014: 745-758

[43] Li Si-Hai, Liu Yang, Zhang Hui-Suo, Zhang Xiao-Dong. Inertial measurements aided GNSS spoofing detection technique. Journal of Chinese Inertial Technology, 2013, 21(3): 336-353(in Chinese)
(李四海, 刘洋, 张会锁, 张晓冬. 惯性信息辅助的卫星导航欺骗检测技术. 中国惯性技术学报组合导航技术, 2013, 21(3): 336-353)

[44] Lee J H, Kwon K C, An D S, Shim D S. GPS spoofing detection using accelerometers and performance analysis with probability of detection. International Journal of Control, Automation and Systems, 2015, 13(4): 951-959

[45] Daneshmand S, Jafarnia-Jahromi A, Broumandan A, Lachapelle G. A low-complexity GPS anti-spoofing method using a multi-antenna array//Proceedings of the 25th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2012). Nashville, USA, 2012: 1233-1243

[46] Wesson K, Rothlisberger M, Humphreys T. Practical cryptographic civil GPS signal authentication. NAVIGATION Journal of the Institute of Navigation, 2012, 59(3): 177

[47] Humphreys T E, Ledvina B M. Assessing the spoofing threat: Development of a portable GPS civilian spoofer//Proceedings of the 21st International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2008). Savannah, USA, 2008: 2314-2325

[48] Hartmann K, Steup C. The vulnerability of UAVs to cyber attacks—An approach to the risk assessment//Proceedings of the Cyber Conflict (CyCon) 2013 5th International Conference. Tallinn, Estonia, 2013: 1-23

[49] Mansfield K, Eveleigh T, Holzer T, Sarkani S. Unmanned aerial vehicle smart device ground control station cyber security threat model//Proceedings of the IEEE International Conference on the Technologies for Homeland Security (HST). Waltham, USA, 2013: 722-728

[50] Won J, Seo S H, Bertino E. A secure communication protocol for drones and smart objects//Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security. New York, USA, 2015: 249-260

[51] Kim A, Wampler B, Goppert J, et al. Cyber-attack vulnerabilities analysis for unmanned aerial vehicles//Proceedings of the American Institute of Aeronautics and Astronautics. Reston, USA, 2012: 1-30

[52] Krozel J, Andrisani D. Independent ADS-B verification and validation//Proceedings of the AIAA Aviation Technology Integration and Operations Conference Proceedings. Arlington,

Virginia，2005：1-11

[53] Yuan Suo-Zhong. Research and development of digital UAV flight control system. Computer Measurement and Control，2003，11(1)：64-65(in Chinese)
(袁锁中. 数字式无人机飞行控制系统研制. 计算机测量与控制，2003，11(1)：64-65)

[54] Miller J，Minear P，Niessner A，et al. Intelligent unmanned air vehicle flight systems. Journal of Aerospace Computing，Information，and Communication，2007，4(5)：816-835

[55] Hess R，Torrez J. The deep impact flight software architecture //Proceedings of the IEEE Aerospace Conference. Big Sky，USA，2006：1-9

[56] Zhou Zhi-Jiu，Yan Jian-Guo. DSP of the UAV flight control system software based on modular design. Computer Measurement & Control，2009，17(1)：221-223(in Chinese)
(周志久，闫建国. 基于 DSP 的无人机飞控系统软件模块化设计. 计算机测量与控制，2009，17(1)：221-223)

[57] Wang Quan，Zhang Xue-Hong，Zhou Min-Gang，Huang Hui. UAV flight control software testing method of computing technology aviation. Aeronautical Computer Technique，2008，38(2)：78-81(in Chinese)
(王泉，张学宏，周敏刚，黄晖. 无人机飞控软件测试方法研究. 航空计算技术，2008，38(2)：78-81)

[58] Yang Liu-Qing，Xiao Qian-Gui，Liu Jiu-Fu. UAV flight control software anti-jamming design. Micro Computer Application，2007，23(9)：1-2(in Chinese)
(杨柳庆，肖前贵，刘久富. 无人机飞控软件抗干扰设计. 微型电脑应用，2007，23(9)：1-2)

[59] Fang Xin-Xin. Malware Implementation and Detection on Android[M. S. dissertation]. Nanjing University of Posts and Telecommunications，Nanjing，2013(in Chinese)
(房鑫鑫. Android 恶意软件实现及检测研究[硕士学位论文]. 南京邮电大学，南京，2013)

[60] Zuo Ling. Design and implementation of malware detection system based on Android. University of Electronic Science and Technology of China，Chengdu，2012(in Chinese)
(左玲. 基于 Android 恶意软件检测系统的设计与实现[硕士学位论文]. 电子科技大学，成都，2012)

[61] Yan Yong. A detection method for Android malware based on dynamic monitor. Information Security and Communications Privacy，2014，(10)：104-108(in Chinese)
(严勇. 基于动态监控的 Android 恶意软件检测方法. 信息安全与通信保密，2014，(10)：104-108)

[62] Han Yang. Design and Implementation of the Android Application Security Evaluation Tool[M. S. dissertation]. Beijing Jiaotong University，Beijing，China，2012(in Chinese)
(韩扬. Android 应用软件安全评测工具的设计与实现[硕士学位论文]. 北京交通大学，北京，2012)

[63] Schmidt A D. Static analysis of executables for collaborative malware detection on Android//Proceedings of the 9th IEEE International Conference on Communications. Dresden，Germany，2009：1-5

[64] Shabtai A. Malware detection on mobile devices//Proceedings of the 11th International Conference on Mobile Data Management. Kansas City，USA，2010：289-290

[65] Liu Wei，Feng Bing-Wen，Weng Jian. A review of the research on safety of small UAV. Journal of Network and Information Security，2016，2(3)：39-45(in Chinese)
(刘炜，冯丙文，翁健. 小型无人机安全研究综述. 网络与信息安全学报，2016，2(3)：39-45)

[66] Wang Wei-Jiang，Zheng Feng，Guo Le-Jiang. Study of network architecture of UAV tactic networking. Journal of Air Force Radar Academy，2011，25(4)：287-295(in Chinese)
(王卫疆，郑锋，郭乐江. 无人机战术组网的网络体系结构研究. 空军雷达学院报. 2011，25(4)：287-295)

[67] Javaid A Y，Sun W，Devabhaktuni V K，Alam M. Cyber security threat analysis and modeling of an unmanned aerial vehicle system//Proceedings of the IEEE Conference on Technologies for Homeland Security (HST). Waltham，USA，2012：585-590

[68] Akyildiz I F，Kasimoglu I H. Wireless sensor and actor networks：Research challenges. Ad Hoc Networks，2004，2(4)：351-367

[69] Rappaport T S. Wireless communications：Past events and a future perspective. IEEE Communication Magazine，2002，40(5)：148-161

[70] Loong K M，Leng G. Sensors and communications range relations for UAV operations//Proceedings of the New Challenges in Aerospace and Technology Maintenance Conference. Singapore，2006：1-7

[71] Deng H M，Li W，Agrawal D P. Routing security in wireless ad hoc networks. IEEE Communications Magazine，2002，40(10)：70-75

[72] Agrawal D P，Zeng Q A. Introduction to Wireless and Mobile Systems. Boston，USA：Brooks/Cole Publishing，2002

[73] Zhou Li-Dong，Zygmunt J H. Securing ad hoc networks. IEEE Network，1999，13(6)：24-30

[74] Yang H. Security in mobile ad hoc networks：Challenges and solutions. IEEE Wireless Communications，2004，11(1)：38-47

[75] Reyes H，Gellerman N，Kaabouch N. A cognitive radio system for improving the reliability and security of UAS/UAV networks//Proceedings of the 2015 IEEE Aerospace Conference. Big Sky，USA，2015：1-9

[76] Maxa J A，Mahmoud M S B，Larrieu N. Secure routing protocol design for UAV ad hoc networks//Proceedings of the Digital Avionics Systems Conference(DASC) 2015 IEEE/AIAA 34th IEEE. Prague，Czech Republic，2015：4A5：1-4A5：15

[77] Sedjelmaci H，Senouci S M，Ansari N. Intrusion detection and ejection framework against lethal attacks in UAV-aided networks：A Bayesian game-theoretic methodology. IEEE Transactions on Intelligent Transportation Systems，2016，PP(99)：1-11

[78] Zapata M, Asokan N. Securing ad hoc routing protocols// Proceedings of the 1st ACM Workshop on Wireless Security (WiSE'02). New York, USA, 2002: 1-10

[79] Sanzgiri K, Dahill B, Levine B N, et al. A secure protocol for ad hoc networks//Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP'02). Paris, France, 2002, 2(1): 78-87

[80] Hu Y, Perrig A, Johnson D. Ariadne: A secure on-demand routing protocol for ad hoc networks. Wireless Networks, 2005, 11(1-2): 21-38

[81] Liu T, Sun Y, Liu Y, et al. Abnormal traffic-indexed state estimation: A cyber — physical fusion approach for Smart Grid attack detection. Future Generation Computer Systems, 2015, 49(48): 94-103

HE Dao-Jing, Ph. D., professor. His research interests include network and systems security.

DU Xiao, M. S. candidate. His research interest is unmanned aerial vehicle security.

QIAO Yin-Rong, M. S. candidate. His research interest is embedded system security.

ZHU Yao-Kang, M. S. candidate. His research interest is unmanned aerial vehicle security.

FAN Qiang, senior engineer. His research interests include transmission and routing.

LUO Wang, senior engineer. His research interests include signal and information processing.

Background

With the rapid advancements of technology and the decreasing of the manufacturing cost, unmanned aerial vehicles (UAVs) are spreading from military areas to industrial production and people's daily lives. Nowadays, UAVs have been widely employed in film shooting and personal photography, agricultural inspection, electrical inspection, and so on. However, while a UAV gives people all kinds of conveniences, the cyber security problem of the UAV is gradually exposed. This paper firstly introduces the composition structure and applications of UAVs, and then presents the cyber security threats on UAVs. In particular, this paper presents the cyber security threats, existing security measures, the current research progress and our experimental results on UAVs in four aspects (i. e., sensor, communication, software and network) in details. Finally, the future of the UAV security and management is discussed.

This research is supported by the National Key R&D Program of China (2017YFB0802805, 2017YFB0801701, and 2017YFB0802302), the National Science Foundation of China (Grants: U1636216, 51477056 and 61601129), the Shanghai Rising Star Program (No. 15QA140170), A special project of Shanghai Science and Technology Commission on Technical standards (No. 16DZ0503000), and the State Grid Corporation Science and Technology Project "The Pilot Application on Network Access Security for Patrol Data Captured by Unmanned Planes and Robots and Intelligent Recognition Based on Big Data Platform" (Grant No. SGSDDK000KJJS1600065).