计算机科学
COMPUTER SCIENCE

无人机系统安全性综述

王震, 周超, 樊永文, 石鹏飞

引用本文

王震, 周超, 樊永文, 石鹏飞. 无人机系统安全性综述[J]. 计算机科学, 2024, 51(6A): 230800086-6.

WANG Zhen, ZHOU Chao, FAN Yongwen, Shi Pengfei. Overview of Unmanned Aerial Vehicle Systems Security [J]. Computer Science, 2024, 51(6A): 230800086-6.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.230800086

无人机系统安全性综述

王 震 周 超 樊永文 石鹏飞
中国人民解放军 63891 部队 河南 洛阳 471000

摘 要 近年来,无人机越来越受欢迎,无人机在军事、农业、交通运输、电影、供应链和监控等各个行业都有着巨大的潜力。尽管无人机给人们提供了种种便利,但如今与无人机相关的安全事件却层出不穷。恶意方可能对无人机进行攻击,并利用无人机进行危及生命的活动。因此,世界各国政府已经开始规范无人机的使用。无人机需要一种智能和自动化的防御机制,以确保人类、财产和无人机本身的安全。而无人机操作系统防护是防止入侵攻击的一个重要部分。首先,对无人机结构进行了简要介绍;然后,研究了用于消费和商用无人机的现有操作系统的安全性。最后,调查了无人机操作系统的各种安全问题和可能的解决方案。

关键词:无人机;无人机安全;操作系统安全;解决方案
中图分类号 TP393

Overview of Unmanned Aerial Vehicle Systems Security

WANG Zhen, ZHOU Chao, FAN Yongwen and Shi Pengfei
Unit. No. 63891, Luoyang, Henan 471000, China

Abstract In recent years, with the increasing popularity of unmanned aerial vehicle(UAV), UAVs have enormous potential in various industries such as military, agriculture, transportation, film, supply chain, and surveillance. Despite the various conveniences provided by UAVs, security incidents related to UAVs are constantly emerging today. Malicious parties may attack UAVs and use them for life-threatening activities. Therefore, governments around the world have begun to regulate the use of UAVs. UAVs require an intelligent and automated defense mechanism to ensure the safety of humans, property, and the UAV itself. The protection of UAV operating systems is an important part of preventing intrusion attacks. Firstly, a brief introduction to the structure of UAVs is given, and then the security of existing operating systems for consumer and commercial UAVs is studied. Finally, various security issues and possible solutions for the UAV operating system are investigated.

Keywords Unmanned aerial vehicle, Unmanned aerial vehicle security, Operating system security, Solution

1 引言

无人机被定义为利用无线电遥控设备和自备的程序控制装置操纵的不载人飞机[1]。近年来,无人机已经成为人们重点关注的领域,因为其可以用于许多军事和民用应用,包括军事攻击、国家情报和监视、边境安全、通信中继、农业和遥感等。此外,无人机爱好者和各行各业的研究人员正在不断寻找有效使用无人机[2-3]的方法,无人机的应用彻底改变了许多企业并为其发展创造了新的机会。

和所有的新技术一样,无人机也可以被恶意使用,也可以成为恶意行为者的攻击目标。无人机遥控主要采用一个飞行控制器,该控制器由传感器和执行器组成网络,通过通信链路与地面控制系统进行通信。因此,无人机系统很容易受到针对网络、控制器、无线链路或多个组件[4]组合的攻击。目前有许多无人机相关事件的报道[5-7],一些国家已经采取了天空管制的政策[8]。无人机也可能对隐私和人类安全造成威胁[9]。比如一架装有摄像头和麦克风的无人机在我们的私人空域内飞行,我们几乎不可能识别出操控无人机的人。事实上,即使有严格的规定,恶意用户也会将无人机用于非法目的。因此,反无人机技术也在不断发展,利用跟踪、干扰等技术摧毁恶意无人机。

除了检测和禁用恶意无人机,我们还需要技术来保护无人机免受外部恶意行动者的攻击。每个系统都存在漏洞,无人机也不例外。针对无人机的网络攻击可以对大型飞机、机场和人类财产等物理实体构成重大的安全风险。如果无人机受到攻击,则可能会比普通 IT 设备造成更长的影响。因此,和像汽车行业一样,无人机需要高度可靠的软件和严格的监管合规。

负责确保无人机安全的主要组件之一是操作系统。然而,大多数无人机仍然使用为无人机飞行控制器专门定制的基本实时调度器或操作系统/固件。因此,未来的无人机需要复杂的操作系统,以使无人机更高效、更轻量、更自主。本文首先研究了现有的用于开源和商用无人机的操作系统;然后,分析了无人机操作系统有关安全的问题,并确定了需要重点关注的未来无人机操作系统面临的安全性挑战。

2 无人机介绍

Austin[10]将无人机定义为包含许多子系统的系统,包括

通信作者:王震(45778695@qq.com)

其有效载荷(无人机可以携带的重量),地面控制站(或其他远程站)和通信子系统。本章简要说明不同类型的无人机及其硬件、软件和通信架构。

2.1 无人机的种类

无人机的主要类型有3种:单旋翼、多旋翼和固定翼。单旋翼无人机有一个大旋翼,外形与传统直升机相似。虽然这种类型的无人机不是很常见,但其结构坚固,飞行时间更长,载荷能力大。多旋翼无人机更便宜,而且可以根据旋翼的数量进行分类。最常见的形式是四旋翼无人机(4个旋翼)。多旋翼无人机虽然易于控制,但飞行时间和载荷能力有限。固定翼无人机看起来像传统飞机,使用固定的、静态的机翼,有时与旋翼结合使用。其需要更长的飞行和降落空间,而且难以机动。固定翼无人机的飞行高度更高,飞行时间更长,但不能在空中盘旋。图1展示了这3种无人机。

(a)单旋翼 (b)多旋翼 (c)固定翼

图1 不同类型的无人机

Fig. 1 Different types of UAV

无人机的建造尺寸不同,在载荷能力、操作高度和航程方面也具有不同的能力。表1列出了无人机的尺寸及其特征。

表1 无人机的尺寸及其特性

Table 1 Dimensions of UAV and its characteristics

种类	机身重量/kg	操作高度/m	航程/km	载荷能力/kg
极小型	小于0.2	小于90	0.090	小于0.2
微小型	0.25～2	小于90	5	0.2～0.5
小型	2～20	小于900	25	0.5～10
中型	小于150	小于1500	50～100	5～50
大型	大于150	小于3000	大于200	25～200

2.2 无人机系统架构

一架无人机由机体、合适的推进系统、飞行控制器、精确导航系统和感知与避免系统组成。通常情况下,无人机还携带有效载荷和配套计算机,用于高级分析和自主飞行功能。无人机系统主要由地面控制站(Ground Control Station, GCS)、通信链路、飞行控制器、有效载荷等组成。无人机系统架构如图2所示。

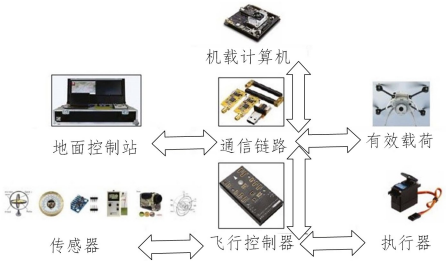

图2 无人机系统架构图

Fig. 2 Architecture diagram of UAV system

1)地面控制站:地面控制站是一套硬件和软件,方便操作人员对无人机及其有效载荷进行通信、控制或监控。与无人机一样,GCS的大小和能力也各不相同,并取决于其控制的无人机的类型和任务。对于休闲无人机来说,GCS可以是一个移动应用程序,也可以是一个小型的手持发射器。对于任务关键的政府无人机,GCS可以是一个拥有多台计算机和软件的大型设施。

2)通信链路:无人机与GCS之间的通信主要有两种类型。一种是指挥与控制通信,也称为控制与无载荷通信,用于GCS与无人机之间的可靠通信(命令报文、非有效载荷遥测数据、空中交通管制语音中继、非有效载荷视频下行数据等),以保证无人机的飞行安全运行。这种链路可以是视距或超视距,视无人机类型而定。另一种通信类型是有效载荷通信,用于将非关键数据(如图像和视频)从无人机传输到控制站。无人机可以通过多种方式与GCS进行通信,包括WiFi、蓝牙、LTE/4G、5G、LoRa、RMILEC和卫星。

3)飞行控制器:飞行控制器是无人机连接传感器和执行器的中央处理单元,负责高度稳定、飞行航路点生成、任务规划等[11]。它读取传感器提供的数据,并将处理后的信息传递给GCS或供给执行器。飞行控制器具有核心传感器集,如加速度计、陀螺仪、GPS和红外摄像机。如果有有效载荷,它还可以连接外部传感器。目前比较流行的飞行控制器有Pixhawk, DJI Naza, Raceflight等。

虽然机载飞行控制器足以满足基本的无人机飞行,但对于"跟随另一个物体"和"障碍物检测和规避"这样的高级自主飞行,需要一个功能强大的机载计算机。此外,对于无人机来说,最好是由一台单独的计算机来执行云同步和有效载荷数据管理等任务。一些伴生计算机的例子有NVIDIA Jetson TX2, Intel Aero, ODROID XU4等。

4)有效载荷:无人机有效载荷通常为外部传感器和附着在其上的设备。我们可以附加任何我们想要的东西,除非尺寸和重量超过无人机的能力,例如披萨、信件和包裹、药品和用品。

3 常见的无人机机载操作系统及其安全措施

一架无人机需要一系列软件才能正常工作。我们需要一个飞行控制器的固件/操作系统来管理所有集成的传感器和执行器。它还托管负责基本飞行操作、路径规划和安全的软件。因此无人机机载操作系统是无人机的控制核心,其自身威胁所带来的安全风险,也是无人机的最大安全风险。由于无人机的操作具有时效性,因此该固件/操作系统需要是实时的。飞行控制器通常需要一个功能齐全的操作系统,如Linux或Windows,因为许多自主功能依赖于复杂的软件库(如深度学习)。目前有很多针对无人机的开源和商业软件项目。本章主要介绍主流无人机所使用的机载操作系统及其安全措施。

3.1 ArduPilot

ArduPilot[12]是开源无人机系统平台的先驱之一。项目从Arduino硬件(ARM 8位MCU)开始,后来系统已经进化到针对基于ARM的32位MCU。ArduPilot可以在许多不同类型的无人机上工作,包括多旋翼、固定翼、直升机,甚至潜艇。Ardupilot努力使这些设备完全自主。ArduPilot使用GPL许可,这意味着对代码库的任何更改都需要添加回父项目。ArduPilot为基于stm32的板卡运行的实时操作系统,也

可以在基于 Linux 的板卡上运行（例如树莓派）。

ArduPilot 没有任何特殊的安全措施来保护设备免受外部攻击。它使用 MAVLink 协议[13]与外部设备通信。根据文献[14]的说法，MAVLink 协议容易受到几种常见攻击，并且不提供 CIA（机密性、完整性和可用性）安全服务。该协议容易受到窃听和其他与机密性和隐私相关的攻击。此外，MAVLink 协议不能抵御中间人攻击（如重放和注入攻击）。攻击者还可以阻止消息到达无人机，从而使控制站失去作用。最近，MAVLink 发布了用于消息认证的支持报文签名的版本，但是消息还没有加密。为了缓解 MAVLink 的安全问题，学术界提出了几种解决方案[14-15]。

3.2 PX4

PX4 系统包含飞行控制软件、地面控制站和仿真软件[16]。PX4 主要与 pixhawk 兼容的飞行控制器工作，支持固定翼、多旋翼、单旋翼等。PX4 使用 BSD 许可证，因此很受商业公司欢迎。PX4 使用 QGroundControl 作为地面控制站，使用 MAVlink 协议进行通信。和 ArduPilot 一样，PX4 可以自己运行，也可以运行在 Linux 之上。由于 PX4 使用了 MAVLink，因此它具有与 ArduPilot 一样的问题。

3.3 Paparazzi

Paparazzi 是一个开源项目，是一个完整的无人机系统，包括硬件、飞控软件、自动驾驶仪、地面控制站（GCS）和模拟器[17]。Paparazzi 飞行控制器可配置控制多旋翼、固定翼、扑翼、直升机和不同配置的混合飞机，以及多架无人机系统。从 Paparazzi 地面控制站可以设置参数和读取传感器数据。我们还可以设置包括自定义制导、导航和控制算法在内的飞行计划。Paparazzi 使用 GPL 许可证，可以安装在专用的飞行控制器或基于 linux 的无人机上。

Paparazzi 项目使用 PPRZLINK 作为通信工具包（消息定义、代码生成器、库等）。它定义了 3 种类型的消息：上行链路（数据链）、下行链路（遥测）和地面到地面（地面代理之间交换的消息）。2018 年，Paparazzi 项目使用了安全 PPRZLINK，这是一种用于无人机的加密通信协议。它使用了带有 Poly1305 认证器的 Chacha20 和一个正式验证的密码库 HACL，是唯一一个提供加密无人机通信的开源协议。

3.4 大疆无人机系统

大疆是顶级的消费级无人机制造商之一。大疆的所有产品都使用了专有的硬件和软件。它还销售面向爱好者的飞行控制器。大疆的产品主要使用 WiFi，OcuSync 和 Lightbridge 无线链接。其中，Lightbridge 和 OcuSync 是专有协议，性能比 WiFi 要好得多，它们更可靠，带宽和范围也更大。

由于大疆无人机的源代码尚未开源，因此很难对大疆固件的安全性进行评论。不过，部分研究人员成功破解了部分大疆无人机系统程序，并发现了几个安全问题[18-20]。近年来，大疆已经提高了无人机的安全性[21]，现在其专有的通信链路（Lightbridge 和 OcuSync）已经可以实现加密功能。OcuSync 2.0 支持 AES 256，用于适用于政府和执法机构的无人机。

无人机技术还处于起步阶段，我们注意到，大多数可供爱好者使用的飞行控制器还不支持成熟的操作系统。事实上，飞行控制器大多只有一个没有任何实时内核的调度器（例如 Betaflight，Cleanflight，Raceflight 和 INAV）。是否需要为无人机飞行控制器配备一个成熟的操作系统，目前还不清楚。但是，如果无人机携带了用于高级自主功能的配套计算机，那么它将需要一个成熟的操作系统。此外，未来的无人机可能拥有多个硬件系统，这些系统将需要适合其功能的独立操作系统。

4 常见无人机安全问题综述及可能的解决方案

本章将讨论无人机操作系统的各种安全问题和可能的解决方案。

4.1 信息与软件安全

无人机内容（采集数据、飞行运行数据、任务相关数据、配置文件等）的安全性非常重要，然而，截至目前，它们大多被忽视。当无人机是军事/政府行动的一部分，在敌对环境中运行时，这些问题最为重要。如果被敌方特工捕获，操作系统需要确保数据不会被泄露，并且以后可以检测到对硬件/软件的任何修改。即使是消费级无人机，也存在无人机官方固件被越狱，用户能够绕过禁飞区的情况[22]。

为了保证数据在静止状态下的安全，我们可以使用一些加密技术。例如，软件全盘加，指加密硬盘上的所有数据，包括操作系统。只有在认证成功后，才允许启动序列和后续访问数据。相比之下，硬件全盘加密是存储控制器的一个功能。此外，还有文件加密和平台加密。对于军事行动，可以分层使用多种技术，以提供更高的安全级别。然而，随着安全功能的增多，在无人机这样资源受限的设备上，效率永远是一个挑战。

为了保护软件（操作系统、配置文件和应用程序）的完整性，可以使用一个硬件信任根。基于可信处理模块的安全启动过程将检测对软件的修改。可信处理模块还可用于生成和保护加密密钥，因为它们被设计为抵抗包括物理攻击在内的一系列攻击[23]。

最后，公钥加密可以用来为无人机提供一个可信的身份。例如，为了验证无人机的身份，地面站可以使用无人机的公钥加密其公钥。然后，无人机将使用自己的私钥解密消息，恢复地面站的公钥。现在，无人机可以通过挑战发送其序列号。如果地面站的响应成功，它们的身份就可以互相验证了。在无人机被敌人捕获的情况下，无人机的私钥可以通过可信处理模块进行保护。

除了讨论的功能之外，还应遵循标准的操作系统加固程序，以最大限度地减少安全威胁。系统加固是通过正确配置系统的各种设置来保护系统的过程。加固可以减少系统的攻击面，从而消除攻击者利用常见攻击向量的可能性。

4.2 传感器安全

无人机包含许多传感器（如加速度计、陀螺仪、磁力计、气压计、GPS 和相机），这些传感器对其实时机动至关重要。因此，操作系统需要有保护措施来挫败不同类型的基于传感器的攻击，因为没有人来验证输入。

一种常见的攻击是针对 GPS 的，因为 GPS 广播是免费访问的，而且信号是未加密或未认证的。欺骗和干扰攻击都是可能的。GPS 干扰是有意或无意干扰信号，使其无法被接

收。另一方面,GPS 欺骗指攻击者向无人机发送比真实 GPS 信号功率稍高的假 GPS 信号,欺骗无人机相信它在另一个位置。Kerns 等[24]证明,通过欺骗 GPS 信号,就有可能控制无人机。也有其他研究提出利用 GPS 欺骗[25-27]来劫持和/或使无人机瘫痪的技术。

在民用 GPS 广播系统中实施一种形式的认证可以为 GPS 欺骗提供解决方案,然而,这项任务并非微不足道,需要对卫星系统的基础设施进行更改。为了检测 GPS 欺骗攻击,研究者[28-29]提出了各种基于软件和硬件的解决方案。另一种方案建议检查 GPS 观测值,并使用中间信号来检测欺骗攻击[30]的存在。此外,检测到不同信号参数的突然变化可以作为欺骗攻击开始的一个指标。Eldosouky 等[31]提出了一种保护无人机免受欺骗攻击的博弈论方法。解决 GPS 信号受干扰可以采用替代导航方法,如安全着陆、返航或自主导航到预定目的地。

无人机传感器使用红外、无线电和光电技术,这些技术会受到外部影响。攻击者可以利用容易获得的设备操纵这些传感器。例如,MEMS 加速度计和陀螺仪在其共振频率下容易受到超声波的攻击。Son 等[32]利用这个漏洞,伪造了他们的无人机的陀螺仪输出,迫使其着陆。后来,Choi 等[33]提出了一种控制不变方法,可以用来挫败这类攻击。他们的方法从无人机的物理属性监视不同的控制不变量,并可以检测出控制不变量与推导值的偏差。

很快,所有消费级和商用无人机都将配备自动依赖监视-广播(ADS-B)系统,该系统每秒广播飞机的位置和速度,以避免与其他有人驾驶或无人驾驶飞机[34]发生碰撞。但与 GPS 一样,ADS-B 信号也是未经加密和认证的,可能会被欺骗或干扰。McCallie 等[35]描述了许多基于 ADS-B 信号的攻击,例如飞机侦察、飞机洪水拒止和飞机幽灵注入。

为了挫败 ADS-B 欺骗攻击,Kim 等[36]提出了对 ADS-B 帧的一种修改。他们添加了一个时间戳,测量飞机之间的消息帧的飞行时间,并将其与根据飞机之间的距离得出的飞行时间进行比较。Kacem 等[37]设计了一个入侵检测系统来检测可疑的 ADS-B 消息。

另一项研究[38]演示了一种劫持无人机的方法,该方法通过欺骗来稳定无人机的光流摄像机。对于攻击者来说,这是一个很好的目标,因为他们可以简单地通过模糊相机拍摄的图像来与传感器互动。Davidson 等[38]使用激光和投影仪成功地发动了攻击。他们还提出了以不同方式合成传感器输出的算法,用以抵御此类攻击。

可见传感器安全涉及方方面面,没有统一的标准研究方向,只能根据传感器的实际情况来分析,确保设备的安全使用。

4.3 通信安全

无人机主要与地面控制站通信。无人机与 GCS 之间交换的信息包括控制无人机的命令、遥测反馈和非关键载荷数据。由于这些通信使用不同的无线通信技术(如 WiFi、蓝牙、LTE 和 Zigbee)进行,干扰和欺骗攻击可能与上述传感器攻击类似。

干扰是最流行的拒绝服务(DoS)攻击,可以针对无线链路执行。有研究者设计了一种反无人机系统[39-40],并使用定向天线产生大功率干扰信号,以断开无人机与控制器的连接。Curpen 等[41]评估了商用 LTE 信号干扰机对抗基于 LTE 的无人机的效率。他们得出的结论是,干扰距离约 60m(适用于家庭住宅)。然而,测量结果会受到城市干扰、无人机和干扰机高度等变量的影响。

Pärlin 等[42]提出了一种协议感知的干扰系统,并表明他们的方法可以比扫描干扰器更有效地快速干扰 ACCST 远程控制系统。软件定义无线电(SDR)协议感知干扰考虑了目标通信系统的特性(信道频率、调制类型和扩频技术),可以有效解决通信系统中的抗干扰和兼容性问题。

文献[43-45]提出了几种减轻干扰攻击的技术。文献[44]使用概率算法来躲避干扰频率。文献[45]提出了一种新颖的技术,利用干扰机本身来减轻威胁,使无人机完成其任务。另一种选择是使用扩频方法,如直接序列扩频(DSSS)和跳频扩频(FHSS)[46]。一旦设置正确,任何不了解扩频码或跳频模式的人都很难窃听通信。

Rodday 等[47]通过入侵用于无人机和地面控制站之间遥测的 Digi XBee 868LP 射频模块,进行了一次中间人(Man-in-the-middle,MITM)攻击。该模块提供了一项功能,允许另一个芯片修改其地址。他们利用这一特性,在系统中引入一种新的芯片。他们能够修改地址,使所有数据包都通过攻击者的芯片发送。另外还提出了一些补救措施,如硬件加密、应用层加密和 XBee 模块板载加密。

针对基于 wifi 的无人机的一种流行攻击是身份认证攻击,即向无人机和地面控制站重复发送认证数据包,这会导致无人机与控制器断开连接[48]。也有研究者讨论了针对此类攻击的几种对策[49]。例如,建议启用 WPA2 加密是保护无线网络安全的一种好方法。然而,应谨慎选择加密密钥的长度,以抵抗蛮力攻击。

对无人机进行认证,实施加密通信,安装某种形式的入侵和攻击检测,都是确保无人机通信环境安全所必需的。

结束语 无人机是现代科技的奇迹之一,将很快给不同的行业带来革命。无人机将被用于运送食品和商品、执行停车规则、执行监视等。在不久的将来,无人机也有可能提供一种替代的交通方式。然而,无人机在安全和隐私方面带来了重大挑战,而无人机的操作系统将在这方面发挥至关重要的作用。本文回顾了现有无人机可用操作系统的安全性,并且发现大多数开源无人机目前还不支持成熟的操作系统,其中一些允许附加一个单板计算机,我们可以在其中安装一个传统的操作系统。然而,大多数现有的无人机固件或操作系统甚至缺乏基本的安全功能。我们调查了常见的无人机安全问题,发现无人机操作系统需要保护传感器和所有内外部通信链路,便于取证调查。此外,无人机和地面控制站使用的任何软件和数据都需要受到保护,免受恶意攻击。在资源受限的设备中,整合安全功能始终是一项具有挑战性的任务,为此需要进行大量研究。

参 考 文 献

[1] YANUSHEVSKY R. Guidance of unmanned aerial vehicles

[M]. CRC Press，2011.

[2] ILLMAN M. 9 cool ways drones are being used to deliver goods to you[EB/OL]. https://www. pocket-lint. com/drones/news/146105-things-drones-can-deliver-to-you.

[3] MOON M. Faa makes it easy for drone hobbyists to fly in controlled airspace[EB/OL]. https://www. engadget. com/2019/07/24/faa- opens-laanc-to-drone-hobbyists/.

[4] CONSTANTINIDES C，PARKINSON P. Security challenges in uav devel-opment[C]// 27th Digital Avionics Systems Conference. IEEE，2008：1-8.

[5] EVANS A. Not in my backyard! Woman throws stones before using a gun to get rid of nosy neighbour's drone[EB/OL]. https://www. dailymail. co. uk/news/article-4283486/Woman-grabs-gun-shoots-nosy-neighbour-s-drone. html.

[6] GETTINGER D. The soleimani killing and 5 things to know about drones in iraq[EB/OL]. https://thebulletin. org/2020/01/soleimani-and-beyond-5-ways-that-drones-have-destabilized-iraq/.

[7] MARGARITOFF M. Tobacco-smuggling drone fo und by ukraine border patrol reveals region's black market[EB/OL]. https://www. thedrive. com/tech/23447/tobacco-smuggling-drone-found-by-ukraine-border-patrol-reveals-regions-black-market.

[8] NASSI B，SHABTAI A，MASUOKA R，et al. SoK-security and privacy in the age of drones：threats，challenges，solution mechanisms，and scientific gaps[J]. arXiv：1903. 05155，2019.

[9] CLARKE R. Understanding the drone epidemic[J]. Computer Law & Security Review，2014，30(3)：230-246.

[10] AUSTIN R. Unmanned aircraft systems：UAVS design，development and deployment[M]. John Wiley & Sons，2011.

[11] WANG H，ZHAO H，ZHANG J，et al. Survey on unmanned aerial vehicle networks：A cyber physical system perspective[J]. IEEE Communications Surveys & Tutorials，2019，22(2)：1027-1070.

[12] Ardupilot[EB/OL]. https://ardupilot. org/.

[13] Mavlink[EB/OL]. https://mavlink. io/en/.

[14] ALLOUCH A，CHEIKHROUHOU O，KOUBÂA A，et al. MAVSec：Securing the MAVLink protocol for ardupilot/PX4 unmanned aerial systems[C]// 2019 15th International Wireless Communications & Mobile Computing Conference(IWCMC). IEEE，2019：621-628.

[15] BUTCHER N，STEWART A，BIAZ S. Securing the mavlink communication protocol for unmanned aircraft systems[J/OL]. https://eng. auburn. edu/files/acad_depts/csse/csse_technical_reports/csse14-02. pdf.

[16] Px4[EB/OL]. https://px4. io/.

[17] Paparazziuav[EB/OL]. https://wiki. paparazziuav. org/wiki/Main Page.

[18] DEY V，PUDI V，CHATTOPADHYAY A，et al. Security vulnerabilities of unmanned aerial vehicles and countermeasures：An experimental study[C]// 2018 31st International Conference on VLSI Design and 2018 17th International Conference on Embedded Systems(VLSID). IEEE，2018：398-403.

[19] LIAO S. Dji drones can get past no-fly zones thanks to this russian software company[EB/OL]. https://www. theverge. com/2017/6/21/15848344/drones-russian-software-hack-dji-jailbreak.

[20] TRUJANO F，CHAN B，BEAMS G，et al. Security analysis of dji phantom 3 standard[J/OL]. https://courses. csail. mit. edu/6. 857/2016/files/9. pdf.

[21] Dji lightbridge[EB/OL]. https://www. dji. com/ca/dji-lightbridge.

[22] Chibios[EB/OL]. http://chibios. org/dokuwiki/doku. php.

[23] Apache nuttx[EB/OL]. https://nuttx. apache. org/.

[24] KERNS A J，SHEPARD D P，BHATTI J A，et al. Unmanned aircraft capture and control via GPS spoofing[J]. Journal of Field Robotics，2014，31(4)：617-636.

[25] LUO A. Drones hijacking[J/OL]. https://media. defcon. org/DEF%20CON%2024/DEF%20CON%2024%20presentations/DEF% 20CON% 2024% 20-% 20Aaron-Luo-Drones-Hijacking-Multi-Dimensional-Attack-Vectors-And-Countermeasures-UPDATED. pdf.

[26] VERVISCH-PICOIS A，SAMAMA N，TAILLANDIER-LOIZE T. Influence of GNSS spoofing on drone in automatic flight mode[C]// ITSNT 2017：4th International Symposium of Navigation and Timing. Ecole nationale de l'aviation civile，2017：1-9.

[27] HE D，QIAO Y，CHEN S，et al. A friendly and low-cost technique for capturing non-cooperative civilian unmanned aerial vehicles[J]. IEEE Network，2018，33(2)：146-151.

[28] FENG Z，GUAN N，LV M，et al. Efficient drone hijacking detection using onboard motion sensors[C]// Design，Automation & Test in Europe Conference & Exhibition(DATE)，2017. IEEE，2017：1414-1419.

[29] FENG Z，GUAN N，LV M，et al. An efficient UAV hijacking detection method using onboard inertial measurement unit[J]. ACM Transactions on Embedded Computing Systems(TECS)，2018，17(6)：1-19.

[30] WEN H，HUANG P Y R，DYER J，et al. Countermeasures for GPS signal spoofing[C]// Proceedings of the 18th International Technical Meeting of the Satellite Division of the Institute of Navigation(ION GNSS 2005). 2005：1285-1290.

[31] ELDOSOUKY A R，FERDOWSI A，SAAD W. Drones in distress：A game-theoretic countermeasure for protecting UAVs against GPS spoofing[J]. IEEE Internet of Things Journal，2019，7(4)：2840-2854.

[32] SON Y，SHIN H，KIM D，et al. Rocking drones with intentional sound noise on gyroscopic sensors[C]// 24th USENIX Security Symposium(USENIX Security 15). 2015：881-896.

[33] CHOI H，LEE W C，AAFER Y，et al. Detecting attacks against robotic vehicles：A control invariant approach[C]// Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. 2018：801-816.

[34] Dji adds airplane and helicopter detectors to new consumer drones[EB/OL]. https://www. dji. com/ca/newsroom/news/dji-adds-airplane-and-helicopter-detectors-to-new-consumer-drones.

[35] 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.

[36] KIM Y，JO J Y，LEE S. A secure location verification method for ADS-B[C]// 2016 IEEE/AIAA 35th Digital Avionics Systems

Conference(DASC). IEEE, 2016: 1-10.
[37] KACEM T, WIJESEKERA D, COSTA P, et al. An ADS-B intrusion detection system [C] // 2016 IEEE Trustcom/BigDataSE/ISPA. IEEE, 2016: 544-551.
[38] DAVIDSON D, WU H, JELLINEK R, et al. Controlling {UAVs} with sensor input spoofing attacks [C] // 10th USENIX workshop on offensive technologies(WOOT 16). 2016.
[39] ABUNADA A H, OSMAN A Y, KHANDAKAR A, et al. Design and implementation of a RF based anti-drone system[C] // 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies(ICIoT). IEEE, 2020: 35-42.
[40] MULTERER T, GANIS A, PRECHTEL U, et al. Low-cost jamming system against small drones using a 3D MIMO radar based tracking [C] // 2017 European Radar Conference (EURAD). IEEE, 2017: 299-302.
[41] CURPEN R, BĂLAN T, MICLOȘ I A, et al. Assessment of signal jamming efficiency against LTE UAVs[C] // 2018 International Conference on Communications (COMM). IEEE, 2018: 367-370.
[42] PÄRLIN K, ALAM M M, LE MOULLEC Y. Jamming of UAV remote control systems using software defined radio[C] // 2018 International Conference on Military Communications and Information Systems(ICMCIS). IEEE, 2018: 1-6.
[43] WANG Q, NGUYEN T, PHAM K, et al. Mitigating jamming attack: A game-theoretic perspective[J]. IEEE Transactions on Vehicular Technology, 2018, 67(7): 6063-6074.
[44] DI PIETRO R, OLIGERI G. Freedom of speech: Thwarting jammers via a probabilistic approach[C] // Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks. 2015: 1-6.
[45] DI PIETRO R, OLIGERI G, TEDESCHI P. JAM-ME: exploiting jamming to accomplish drone mission[C] // 2019 IEEE Conference on Communications and Network Security(CNS). IEEE, 2019: 1-9.
[46] SODERI S, MUCCHI L, HÄMÄLÄINEN M, et al. Physical layer security based on spread-spectrum watermarking and jamming receiver [J]. Transactions on Emerging Telecommunications Technologies, 2017, 28(7): e3142.
[47] RODDAY N M, SCHMIDT R O, PRAS A. Exploring security vulnerabilities of unmanned aerial vehicles[C] // 2016 IEEE/IFIP Network Operations and Management Symposium (NOMS 2016). IEEE, 2016: 993-994.
[48] KRISHNA C G L, MURPHY R R. A review on cybersecurity vulnerabilities for unmanned aerial vehicles[C] // 2017 IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR). IEEE, 2017: 194-199.
[49] HE D, CHAN S, GUIZANI M. Communication security of unmanned aerial vehicles [J]. IEEE Wireless Communications, 2016, 24(4): 134-139.

WANG Zhen, born in 1986, master. His main research interest is information security.