文章编号:1000－1638(2019)02-0205-07 DOI:10.13484/j.nmgdxxbzk.20190214

几种小型UAV安全漏洞攻击研究*

郑 瑛[1],白青海[2,3]

(1.内蒙古民族大学 学术期刊社,内蒙古 通辽 028043;
2.内蒙古民族大学 计算机科学与技术学院,内蒙古 通辽 028043;
3.内蒙古民族大学 计算机应用技术研究所,内蒙古 通辽 028043)

摘要:近年来小型无人机在各个领域迅速普及并广泛应用,与此同时也暴露出一些安全问题.小型无人机安全方面的研究包括攻击技术和防御技术,针对无人机的几种攻击方式进行了研究,对漏洞成因及利用方法做了总结并提出相应的防御措施.

关键词:小型无人机;通信安全;GPS欺骗;无线安全;WIFI安全

中图分类号:TP309 **文献标志码**:A

无人驾驶飞行器(Unmanned Aerial Vehicles,UAV),通常称为无人机,是指利用无线电遥控或内置程序运行的不载人的飞行器.它起源于军事应用,但其使用范围正在迅速扩展到商业、科学、娱乐、农业和其他应用,目前用于商用及民用的无人机的数量已经大大超过用于军事领域的数量[1].

近年来,无人机已经迅速普及.它已经被用于各种场景,如影视航拍、快递运输、灾害救援、公共安全等,并对许多行业产生了颠覆性的改变.无人机的主要优势在于提高工作效率,减少工作量和生产成本以及提高工作精确度.随着越来越多的企业认识到无人机技术在各个行业的潜力,其应用已经迅速从时尚转化为一种趋势.而小型无人机由于其更加便携、对飞行条件要求更低等优势,也逐渐在会务、置景、测距、航拍等领域兴起.

然而,无人机在带来各种便利的同时,也渐渐暴露出一些安全问题.无人机作为一种智能设备,其遭受的网络安全威胁非常严重.近年来频频爆出因无人机网络安全问题导致的无人机失控、坠毁、被劫持等新闻.例如2016年的央视"315晚会"上,安全技术研究人员利用"大疆"无人机的通信安全漏洞劫持了无人机,并获得了无人机的控制权.

目前,对无人机的攻击包括无线信号劫持与干扰、GPS欺骗和针对传感器网络的攻击等方面[2],一方面我们需要充分了解这些威胁,同时,也需要发展相应的安全防护措施.由于无人机的安全隐患会对无人机的发展造成恶劣的影响,我们需要针对小型无人机存在的安全漏洞及隐患进行修复,从多方面对无人机安全问题进行研究.

无人机作为新一代科技产品,其安全漏洞不仅会影响用户生命与财产安全,也会影响行业进一步健康发展.因此,通过调查研究小型无人机安全漏洞,以促进无人机厂商加以技术改进,做出更加完善的产品.基于此,对小型无人机安全漏洞进行研究具有十分重要的意义.

1 IEEE802.11无线攻击

针对CX-10wd小型无人机进行IEEE802.11无线攻击,尝试一系列针对无人机的攻击手段,发

* **收稿日期**:2018-11-09
基金项目:内蒙古高等学校科学研究项目(NJZC16191)
作者简介:郑 瑛(1969－),女,内蒙古通辽人,副编审,硕士.主要从事网络安全方面的研究.E-mail:13947595286@163.com

现此无人机的漏洞并加以利用.最后设想了一种可能的攻击流程,并加以实现.

硬件设备:CX-10wd(无人机),kali linux(攻击机); 软件:Aircrack-ng,nmap,wireshark.

1.1 解除认证攻击

目标无人机启动后,会自动生成一个WIFI热点,用于手机端app连接来控制无人机的飞行,以及实现视频信号的传输.这样一来就可以通过扫描附近的热点来找到无人机的MAC地址,发动解除认证(deauth)攻击.

首先使用kali linux下的Aircrack-ng工具实现这一攻击过程.先将无线网卡设置为监听模式,这样攻击机的网卡就可以查看所有经过的流量.之后进行扫描,获得附近所有ap的mac地址(BSSID)及名称,这样就获取到无人机的mac地址以及所处频道.该案例中,无人机mac地址为E0:B9:4D:5D:18:9C,名称为CX-10,手机mac地址为54:33:CB:59:88:B0,通道为1.

之后把网卡设置到无人机热点的频道,可以发现所有连接到该热点的设备的mac地址,也就是无人机控制端的mac地址.之后就可以选择该地址执行解除认证攻击,通过将攻击机的mac地址伪造成无人机ap,向控制端发送解除认证信息,控制端与无人机很快断开连接.此时,被控制的界面的实时视频信号定格在受到攻击之前的画面,并且无法再对无人机发送控制命令,而无人机失去控制信号,原地降落.

从上述过程可以看出,Aircrack-ng工具套件可以实现解除认证攻击,但需要分步进行操作,并且需要一些人工分辨,过程比较繁琐.所以针对本款无人机,编写了一款自动化实现扫描无人机热点并自动进行解除认证攻击的脚本工具.该工具只需要将网卡开启监听模式后即可运行.该工具使用了python中的scapy库,这是一个用于网络分析的交互式数据包处理库.它能够捕获请求、伪造数据及解码大量协议的数据包.

通常无人机等电子设备拥有固定前缀的WIFI热点名称(如CX-10XXXX)或固定前缀的mac地址(通常前三位为公司特点mac地址).基于这一特点,该程序通过拆分捕获的数据流量,识别无人机热点特定的名称或mac地址,以确认附近是否存在无人机设备.发现目标后程序打印无人机设备信息并自动在802.11层发送解除认证数据包,断开控制端该设备的所有连接,实现自动化扫描与攻击的功能.

1.2 命令伪造攻击

除了拒绝服务类型的攻击,还可以通过连接无人机的热点,发送伪造的控制命令达到劫持无人机的目的.这种攻击方式需要捕获无人机与控制端之间的通信内容并进行分析通信过程与控制命令的格式,之后构造合法命令实现攻击.

首先需要连接到无人机热点,许多无人机的热点都使用弱口令或默认口令,可以使用Aircrack-ng工具进行破解.尝试后发现该无人机使用空密码,可以直接连接.

之后寻找无人机热点的IP地址并尝试扫描端口,寻找类似ftp或telnet等常见的服务,尝试是否可以执行系统命令或获取文件.这里可以使用nmap工具进行扫描,首先扫描存活IP,发现无人机热点即为网关,位于172.16.10.1.接着继续用nmap扫描端口,发现设备只开放了8888端口,并没有开启可利用的服务.

获取了无人机的IP地址后,可以通过抓包分析流量来还原无人机的通信过程[3].抓包可以使用中间人攻击(MITM)的方式,在攻击机上截获无人机与手机之间的通信数据,也可以在手机上拦截数据进行分析.因为主要目的是分析流量而不是拦截,故本实验采用第二种方法,如图1所示.

通过wireshark抓取手机与无人机通信的流量包并进行分析,由数据包可以得出如下结论:(1)控制命令使用udp协议在无人机的8895端口进行通信,视频传输以及通信链路控制使用tcp协议,并且都使用8888端口,一共开启四个连接,与手机四个高位端口对应.(2)其中一个tcp通信是发送心跳包,确认设备在线,从通信启动开始每2秒发送一次.(3)每次通信启动时手机端会发送5个确认

数据包，无人机确认后连接成果建立.(4)视频内容是 ffmpeg 编码数据流，不能直接获取，但可以通过 ffmpeg 软件进行解码观看拦截的视频内容.(5)控制信号是 8 字节长的数据，每个字节有特定含义.通过查询相关资料与进行实验测试，得到结果如表 1 所示.

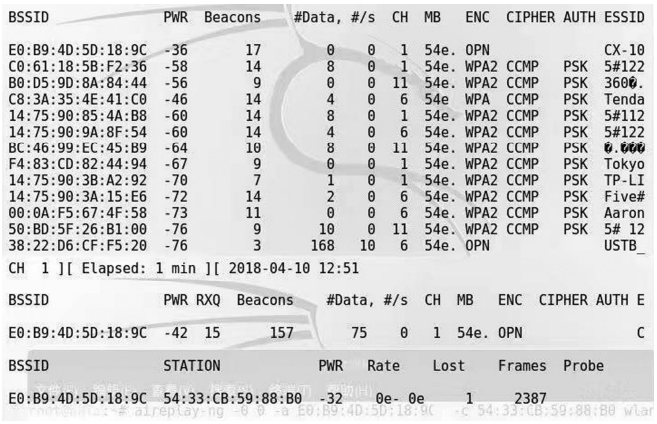

图 1　Wireshark 抓包结果

Fig. 1　Wireshark capture results

表 1　控制命令分析结果

Table 1　Analysis results of control command

CC	roll	pitch	throttle	yaw	Takeoff	Sum	33
0	1	2	3	4	5	6	7

其中，第一位与最后一位是固定值，分别为 0xCC 和 0x33.第 2、3、5 位为方向控制信息，称为 roll、pitch、yaw，航空界的叫法分别代表翻滚角、俯仰角和偏航角.roll 是绕着机身所在的那个轴，pitch 是以翅膀所在的直线为轴发生旋转，而 yaw 是绕着重力方向为轴.这三个参数是控制无人机姿态的重要参数.第 4 位参数叫 throttle，代表油门，也就是用于进行飞机的速度控制.第 6 位是起飞参数，用来标记飞机是起飞状态还是落地状态.第 7 位是校验和字段，由前六位进行校验计算获得，用来确保数据传输的正确性.

分析完通信过程与控制字段的组成之后，就可以编写程序实现命令伪造，从攻击机控制无人机的起飞.程序有两个主要文件，分别为 drone.py 和 command.py.其中后者是一个控制命令的类文件，用于构造合法的控制命令.前者引用命令类后建立正常通信流程，构造并发送命令.

程序在无人机与攻击机之间建立 2 个 socket 连接，分别在 8888 和 8895 端口，使用多线程模拟遥控端的数据发送过程.当无人机开机闲置时，攻击机连接无人机热点，运行该程序即可控制无人机起飞降落等行为，实现劫持.

由上述两个实验可以看到，对于 WIFI 控制的无人机，一方面可以选择 DOS 类型攻击使其与控制端失去联系，一方面可以使用伪造的命令对其进行操作.这样，一种攻击流程就是连接到无人机所在热点，先执行解除认证攻击的脚本，此时控制者会无法操作无人机，而无人机会降落.之后运行伪造命令的程序，无人机在攻击者的命令下被劫持.

由此可见，基于 IEEE802.11(WIFI)协议的无人机在安全性上有很强的安全隐患.这是因为解除认证攻击的门槛很低，用计算机和网卡就可以实现.而中间人攻击、抓包分析流量等技术手段也涉及 WIFI 相关安全内容，因而这种漏洞破坏性强，危害很大.

2　GPS 欺骗攻击

许多无人机都具有 GPS 定位功能，可以根据定位点进行巡航、定点降落等功能.GPS 模块接受卫

星所发送给它的信号,从而进行定位,这种传播是由卫星单向传输给 GPS 接收器的.如果一个 GPS 模拟器把自己伪装成卫星,从而发送一个虚假的信号给 GPS 接收器,由于模拟器所发送的信号比卫星发送的信号强,那么这个时候接收器会接受到 GPS 模拟器所发送出的信号而不是卫星的信号,达到欺骗的目的[4].

GPS 欺骗分为转发式和生成式 GPS 欺骗两类,其目的是控制目标 GPS 接收器的位置-速度-时间(PVT).转发式 GPS 欺骗是将真实的信号录制下来再转发,使目标计算出错误的位置和时间信息.而生成式 GPS 欺骗可以自行伪造位置和时间信息,更具有灵活性[5].当欺骗者有关于目标接收者看到的 GPS 信号的信息时,欺骗可以最有效地完成.这时欺骗者可以产生符合规则的伪造的信号.这种类型的欺骗攻击军事信号基本是不可能的,因为军事信号是加密的,对于一个欺骗者来说是不可预知的.另一方面,民用 GPS 信号是公开的并且容易预测,所以容易进行欺骗.近年来,民用 GPS 欺骗已被认为是许多使用 GPS 信号的关键基础设施应用的严重威胁[6],而具有 GPS 定位功能的无人机也是其中一种潜在的受攻击者.针对 GPS 欺骗有一些相应的硬件设备,最流行的是软件自定义无线电——SDR(Software Defined Radio),常见设备包括 HackRF、bladerf 等.利用这种发射设备,测试人员可以自行编程设置合乎格式 GPS 信号并且发送给接收器,实现伪造 GPS 信号的目的.

德克萨斯大学奥斯汀分校的一项研究分析和论证了无人机通过全球定位系统(GPS)信号欺骗采集和控制的理论和实践[7].这项工作的目的是探索无人机 GPS 信号欺骗漏洞.具体而言,通过 GPS 欺骗为无人机捕获建立了必要条件,并且探索了无人机可能捕获后的控制范围.当欺骗者能够获得最终指定无人机的位置和速度估计值时,即可认为无人机被捕获.在捕获后的控制过程中,欺骗者可以操纵无人机的真实状态,这有可能导致无人机远离其飞行计划飞行而不会引起警报.因为欺骗者企图逃避目标 GPS 接收器和目标导航系统状态估计器,其被假定可以访问非 GPS 导航传感器数据.文献[8]介绍了几种自主式 GPS 干扰技术的模型以及干扰机的设计,并进行了仿真与验证.

同样有很多关于 GPS 欺骗的防御技术[9],常见三种主要方式:加密、信号失真检测、波达方向(DOA)检测.完全防御的防御是不可能实现的,多种方法同时使用才能最大程度的防御.信号失真检测和波达方向感应的综合防御效果最好.另外还有基于阵列天线 GPS 接收机的抗欺骗式干扰方法[10].

本文实验将针对“大疆”matrice 100 无人机进行 GPS 欺骗攻击,观察无人机控制端 app(DJI GO)定位状态以及无人机的相关表现,并分析该漏洞危害.

硬件设备:matrice 100(无人机),ubuntu(攻击机),HackRF(SDR 设备).

2.1 实验环境配置

首先需要配置环境,由于 GNURadio 安装依赖比较多,过程比较复杂,本实验选择直接下载 GNURadio 官网提供的镜像文件,之后可以选择直接用虚拟机加载镜像,或做成系统启动 U 盘.本实验选择第二种方法,因为这样可以即插即用,也可以直接安装操作系统.由于 SDR 设备在运行时需要比较大的信号传输速率,虚拟机可能无法满足需要,所以本实验采用 U 盘安装 Ubuntu 双系统进行实验.之后再安装 HackRF 所需的驱动程序即可.

GPS 欺骗攻击流程分为两部分,首先根据 GPS 信号格式,通过相关程序计算生成用于欺骗的二进制 GPS 基带信号文件,之后使用 SDR 设备将其发送到民用 GPS 所在频率,以干扰无人机的导航定位模块.

2.2 生成 GPS 基带信号

本实验使用 gps-sdr-sim 生成可用的 GPS 信号,这是一款用于生成 GPS 基带信号的软件,可以产生能够被 SDR 设备直接使用的 GPS 基带信号数据流.下载编译完成后,首先需要读取一个 GPS 星历文件,可以从 NASA 官网下载,下载时需要注意选择最新的文件,星历时间与当前时间差别过大可能会导致欺骗失败.之后设定生成的经纬度坐标以及海拔等信息,即可在同文件夹下生成名称为

gpssim. bin 的用于欺骗的基带文件.

2.3　发送 GPS 欺骗信号

生成基带信息文件后,下一步是使用 HackRF 配合相关软件发送信号到民用 GPS 通信频道. 本实验使用 GNURadio 构造 grc 流程图,实现发送功能. 程序读取基带信号文件 gpssim. bin,选择设备为标记号为 78080f 的 HackRF,采样率为 2. 6M,发射频率为民用 GPS 信号频率 1. 57542GHz.

运行该流程图之后几秒到几分钟,附近有 GPS 定位功能的设备都被欺骗,定位信息变为 gps-sdr-sim 设定的经纬度(本实验大致模拟地区在北欧). 实验所用无人机也被欺骗,如图 2; 从手机控制端 app 可以看到定位信息已经由北京海淀区切换到了瑞典斯德哥尔摩附近,如图 3 所示.

图 2　手机定位被欺骗

Fig. 2　Mobile phone positioning was deceived

图 3　无人机定位被欺骗

Fig. 3　Unmanned serial vehicle location was deceived

由于搭载 GPS 模块的无人机通常都设置有禁飞区,GPS 欺骗可用于欺骗无人机当前处于禁飞区使其降落或返航,达到干扰的效果. 但室外环境下攻击者通常与无人机距离较远,可能发送功率不足以实现干扰效果. 但攻击者也可以将树莓派等小型系统搭载在攻击者的无人机上,接近目标无人机并发动攻击,这样就可以大辐增加欺骗信号强度.

综上可以看出,GPS 欺骗攻击有一定的设备及技术要求,并且攻击条件也比较受限,但依然是一种常见并且比较难防御的针对无人机的攻击方式.

3　射频无线电攻击

本实验将针对 cx-10wd 小型无人机进行 RF 射频无线攻击,通过分析无人机通信过程,实现无线电攻击如干扰攻击、重放攻击等,并对通信过程所使用的无线电通信协议进行分析.

设备:CX-10wd(无人机),Ubuntu(攻击机)软件:GNURadio,gqrx,inspectrum.

3.1　无线电干扰攻击

对通信过程进行分析首先需要找到通信信号所在的频率,gqrx 是一款可以直观的观察各个无线电频道上信号活动情况的软件. 安装好后使用 HackRF 作为 SDR 设备,就可以选择频段进行侦听. 通过查询该无人机的设备信息,发现该无人机使用工作在 2. 4Ghz 的 XN297L 芯片.

Gqrx 可监听的频率宽度大概有 20Mhz,选择监听中心频率为 2. 4Ghz,开启无人机遥控器,发现在 2. 402Ghz 有强烈信号出现,推测为遥控器与无人机的配对信号.

此时通过 GNURadio 捕捉该频率,可以观察到信道内容如图 4.

而通过生成随机高斯噪声并发送,可以在指定频率的通信信道实现干扰,GNURadio 自带噪声模块,可以搭建流程图指定频率与带宽,功率大时便形成了干扰. 通过执行 grc 程序后无人机便无法与遥控器配对.

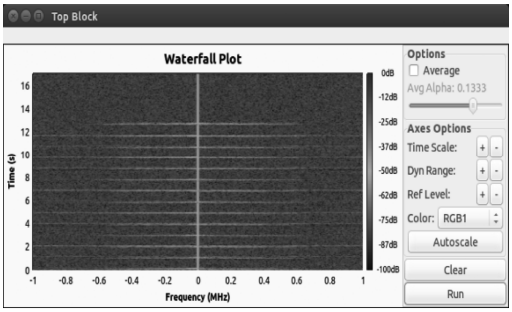

图 4 正常的配对信号

Fig. 4 Normal pairing signal

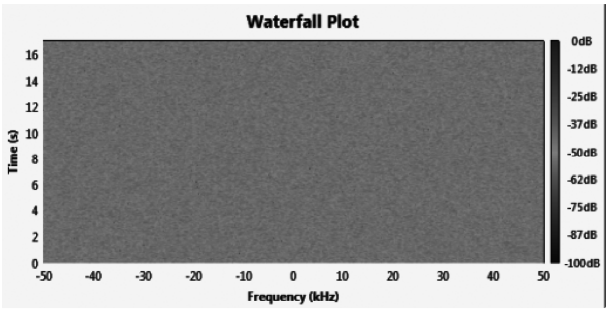

图 5 运行效果

Fig. 5 Running result

该程序在 2.402Ghz 左右 20Mhz 带宽上发送高斯噪音,使该频率通信信道完全被噪声充满,达到拒绝服务的效果,干扰程序运行效果如图 5 所示. 可见,无线干扰是针对无线电的一种攻击方法,因为它会使该频率的所有设备全都无法正常工作.

3.2 无线电重放攻击

重放攻击是针对无线电设备的攻击方式,具体方式为录制无线电控制信息并且重新播放,并不需要知道命令的具体内容. 本实验计划录制无人机起飞信号,当无人机闲置时重放该信号即可使无人机在攻击者控制下起飞.

首先需要寻找无人机控制信号的通信频率,同样使用 gqrx 在 2.4Ghz 寻找. 根据 XN297L 芯片的信息发现该芯片工作频率在 2.400-2.483Ghz,在该区间范围内寻找,发现在 2.473Ghz、2.475Ghz、2.477Ghz、2.479Ghz 频率上存在信息. 推测这是无人机在 4 个频道上跳频传输控制信息,可以选择其中一个频道进行录制,运行 grc 程序并发送起飞命令,就可以得到用于重放攻击的录制信息.

录制好起飞信息后,只需要选择对应的频率进行播放即可,并不需要理解捕获的数据信号的内容. 按编制的脚本实现发送功能,运行后处于闲置状态的无人机在没有遥控器控制的情况下自行起飞.

重放攻击并不需要复杂的无线电知识,只需要找到合适的频率录制并进行播放即可,危害较大,需要注意防范.

3.3 无线电协议分析

重放攻击虽然简单易行,但因为录制时不可避免的会混杂控制命令之外的噪声信号,有时不能实现理想的效果. 这就需要对录制的信号进行分析,根据协议自行设计控制命令,发送无噪声的伪造命令.

分析波形可以使用 inspectrum 工具,这款工具可以自动解码波形数据并转化成二进制的信息. 导入录制好的无人机起飞命令的信息. 根据波形高低可以分辨出二进制 01 信息,通过将波形切分可以得到振幅数据,将振幅信息数字化转化为二进制数据进行分析.

通过分析获取的波形数据,得到无人机无线电通信协议格式如下:

第一个字节是状态字,判断当前是设备绑定状态或控制状态,之后四个字节是跳频信息字段,控制无人机的跳频信道. 之后四个字节是无人机 ID,然后是 roll(翻滚角)、pitch(俯仰角)、throttle(油门)、yaw(偏航角),各占 2 个字节,最后一个字节是 CRC 校验字节,用以确保信息传输正确. 每个数据包以十六进制的 0x710f55 同步字开头.

分析出通信过程后一样可以尝试构造二进制数据流用于伪造控制命令,如起飞、降落等,对于没有加密通信过程的无人机设备,这种攻击方式具有很强的针对性,但是分析过程比较繁琐.

4　总结

调研了国内外相关资料，针对几种小型 UAV 安全漏洞，选择设备进行实验，分析其危害，对于已经验证的安全漏洞，提出相应的防御措施，为改进产品提出建议. 文章对无人机的 IEEE802. 11 无线攻击、GPS 欺骗攻击和射频无线电攻击进行了细致的研究实验，记录了攻击所需要的设备及技术手段，并验证了攻击发生的流程. 分析了攻击的危害程度，以及漏洞潜在的利用方式. 对攻击方式的深入了解有助于进行防御，提高无人机设备的安全性能，为更好的应用无人机设备做技术上的完善.

参考文献：

[1] 何道敬，杜晓，乔银荣，等. 无人机信息安全研究综述[J/OL]. 计算机学报，2017：1-21.

[2] 刘炜，冯丙文，翁健. 小型无人机安全研究综述[J]. 网络与信息安全学报，2016，**2**(3)：39-45.

[3] 乔世成，张智丰，廉洁. IP 首部校验和算法研究[J]. 内蒙古民族大学学报：自然科学版，2016，**31**(5)：400-402.

[4] Tippenhauer N O，Pöpper C，Rasmussen K B，et al. *On the requirements for successful GPS spoofing attacks* [C]//Proceedings of the 2012 ACM conference on Computer and communications security. New York：ACM，2011：75-86.

[5] Viet H N，Kwon K R，Kwon S K，et al. *Implementation of GPS signal simulation for drone security using Matlab/Simulink*[C]//Electronics，Electrical Engineering and Computing (INTERCON)，2017 IEEE XXIV International Conference on. IEEE，2017：1-4.

[6] 严子军. 四旋翼无人机反欺骗及通信加密技术研究[D]. 成都：电子科技大学，2017.

[7] 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.

[8] 熊振伟，陈路. 民用 GPS 自主式欺骗技术与应用[J]. 电子测试，2017(23)：40-41，31.

[9] 李馥娟，王群. GPS 欺骗攻击检测与防御方法研究[J]. 警察技术，2018(1)：45-48.

[10] 郝鹏飞. 阵列天线 GPS 接收机抗欺骗式干扰方法研究[D]. 西安：西安建筑科技大学，2016.

（**责任编委**　侯宏旭）

Research on Security Vulnerability Attacks for Several Small UAVs

ZHENG Ying[1]，BAI Qing-hai[2,3]

(1. *Academic Periodicals Agency，Inner Mongolia University for Nationalities，Tongliao* 028043，*China*；
2. *College of Computer Science and Technology，Inner Mongolia University for Nationalities，Tongliao* 028043，*China*；
3. *Institute of Computer Application Technology，Inner Mongolia University for Nationalities，Tongliao* 028043，*China*)

Abstract：UAV is widely used in various fields，while some security issues are exposed. The research on the security of small UAVs includes attack technology and defense technology. Several kinds of attack methods of drones were studied，the causes of vulnerabilities and corresponding defense measures were put forward.

Key words：UAV；communication security；GPS spoofing；wireless security；WIFI security