

小型无人机安全研究综述

刘炜, 冯丙文, 翁健

(暨南大学网络空间安全学院, 广东 广州 510632)

摘要: 近年来, 随着制造成本的降低和技术的发展, 小型无人机正逐渐从军用和高端商用走向大众消费级市场, 并引起了学界较为广泛的关注。小型无人机在给人们生活带来便利的同时, 也面临日益严峻的安全问题。从小型无人机面临的安全威胁、利用小型无人机发起的攻击以及无人机的认证和溯源等方面总结和分析了国内外无人机安全领域的研究现状, 并对小型无人机安全的未来发展趋势进行了展望。

关键词: 小型无人机; 信息安全; 安全威胁; 隐私侵犯; 认证

中图分类号: TP391

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2016.00037

Survey on research of mini-drones security

LIU Wei, FENG Bing-wen, WENG Jian

(College of Information Science and Technology, Jinan University, Guangzhou 510632, China)

Abstract: With the decreasing of the manufacturing cost and the development of technology, mini-drones are spreading from military and high-end commercial areas to civilian and consumer areas, and they have attracted great interests in recent years. On the one hand, mini-drones bring convenient, and on the other hand, they face with serious security problems. The research status of mini-drones, including the security threats of mini drones, the security attacks from mini drones, the authentication and traceability of mini drones, etc were introduced and analyzed. Finally, the future development of security research in mini-drones was also prospected.

Key words: mini-drone, information security, security threat, privacy invasion, certification

1 引言

随着无人机行业爆炸式的发展, 无人机频繁地登上各大媒体的头条, 如大疆无人机被央视315晚会曝光存在安全漏洞^[1]。在2015年的国际消费类电子产品展览会(CES, consumer electronics show)上, 无人机被认为是最吸引人眼球的展品。美国《航空与太空技术周刊》刊登的分

析报告称, 自2014年起, 在未来10年, 世界无人机市场规模将达到673亿美元。无人机在民事领域上的应用也在近年来得到了迅速的发展, 研究机构EVTank发布的《2015年度民用无人机市场研究报告》显示, 2014年全球民用无人机销量为37.8万架, 到2020年全球无人机年销售量预计将达到433万架^[3]。我国目前已经有300~400家民用无人机企业^[4]。

收稿日期: 2016-02-17; 修回日期: 2016-03-01。通信作者: 翁健, cryptjweng@gmail.com

基金项目: 国家自然科学基金面上基金资助项目(No.61272413, No.61472165); 教育部高等学校博士学科点专项科研基金博导类基金资助项目(No.20134401110011)

Foundation Items: The National Natural Science Foundation of China (No.61272413, No.61472165), The Research Fund for the Doctoral Program of Higher Education of China (No.20134401110011)

如图1所示,无人机系统一般由飞行系统(机体、动力系统、导航系统、通信系统、飞机控制系统)、任务载荷系统(云台、相机、传感器、其他)和地面控制系统(无线电控制、数据处理系统、监控系统、辅助设备)3大部分组成。飞机系统和有任务载荷系统组成了整个飞行器,根据负载能力和实现任务的不同,一个平台可以搭载多套有效载荷系统,实现复杂功能。

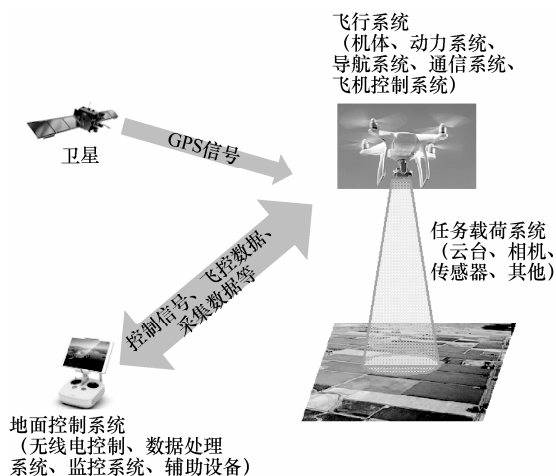


图1 无人机系统的组成

按照不同平台构型来分类,无人机主要分为固定翼无人机、无人直升机和多旋翼无人机3大平台,其他无人机平台还包括伞翼无人机、扑翼无人机和无人飞船等。按不同使用领域来划分,无人机可分为军用、民用和消费级3大类,对于无人机的性能要求各有偏重。本文主要关注小型无人机,小型无人机一般采用多旋翼技术,是消费级和部分民用用途的首选平台,可以原地垂直起飞和悬停,操纵简单、机动性灵活、成本较低^[5]。

小型无人机的应用场景越来越广泛,如航拍、监控、农业植保、空中无线网络、数据采集等领域均用到了小型无人机。小型无人机在给人们工作和生活带来便利的同时,也面临越来越多的安全隐私问题。本文将从小型无人机面临的安全威胁、利用小型无人机发起的攻击以及无人机的认证和溯源等方面介绍和探讨其现状和相关解决方法。

2 无人机面临的攻击

目前,对无人机的常见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。

2.1 无线信号劫持与干扰

由于无线信号是无人机和控制者之间的主要通信方式,对无线信号的攻击可以直接影响无人机的正常运作,乃至获得无人机的控制权。AR.Drone把无人机作为公开的Wi-Fi接入点并开发21、23等重要端口,Childers^[6]和Pleban等^[7]利用这些不安全的设置,成功入侵无人机并取得完全权限,不仅可以控制无人机的飞行功能,而且可以任意浏览、拷贝、篡改无人机上存储的数据。在2015年GeekPwn的开场表演项目中,一架正在空中飞行的大疆精灵3代无人机在几分钟内被“黑客”利用一系列漏洞成功劫持。“黑客”利用通信所用跳频序列太短并且在出厂时已经固化等弱点,夺得了无人机的控制权^[8]。对无线信号的干扰一般是对控制信号进行干扰,迫使控制信号中断。在丢失控制信号的情况下,无人机一般会原地降落、返回设定的航点或者继续航行,黑客可以根据相应情况进行攻击。

针对无线信号的劫持和干扰,Pleban等^[7]为了解决AR.Drone遭受入侵的问题,把地面控制站作为接入点,并使用WAP加密方式来保证信道的安全。在无人机与其他智能设备交互的应用场景中,Won等^[9]提出了基于无证书签密密钥封装机制的eCLSC-TKEM通信协议,它不仅能安全地在无人机和智能设备之间分享密钥,减少智能设备方面的开销,同时也使无人机机体被敌手捕获后信息尽可能少地泄露。Birnbaum等^[10]构造了一个UAV监控系统,利用回归最小二乘方法实时估计机身和控制参数,利用估计参数的异常来判断无人机是否被入侵者控制。Cabaniss等^[11]提出了2种可用于移动自组网(mobile ad hoc network)应用的安全覆盖网络,其拥有安全传送消息、防窃听和消息替换能力,可用于无人机自组网的私密通信。

2.2 GPS欺骗

攻击者通过伪造GPS信号,使无人机的导航系统得出错误的位置、高度、速度等信息。文献[12~14]成功地对多个GPS接收设备实施了GPS欺骗攻击。Kerns等^[15]从如下几个方面进行了详细的探究:1)无人机受伪造GPS信号欺骗的必

要条件; 2) GPS 欺骗进而控制无人机的可能性; 3) GPS 信号欺骗对无人机操作的影响。同时考虑了显性和隐性欺骗策略来躲避目标 GPS 接收器和导航系统状态估计器的检测。

针对 GPS 欺骗的解决方法也被广泛地研究。需要接收机自主导向天线技术的方法如文献[16~18], 不需要特殊天线硬件的接收机自主导向信号处理的技术如文献[19~21]。Chowdhary 等^[22]甚至使用视觉辅助导航系统来对抗 GPS 欺骗的问题, 但通过视觉辅助导航需要提前准备相应的地图, 并且受到环境限制, 比如在黑夜的环境下就无法使用。

2.3 针对传感器网络的攻击

无人机通常作为一个节点和其他无人机或传感器一起构成无线传感器网络。因此无线传感器网络中节点暴露、脆弱、无人监管等弱点也可被用于攻击无人机。在数据层面上, 无人机传输的数据如果缺乏有效的安全措施, 攻击者就能够通过捕获传感器传输的数据, 对数据进行分析或解密, 来获得无人机收集的大量信息^[9]。在网络层面上, 对传感器网络的攻击手段, 如拒绝服务攻击 (DoS, denial of service)、对传输消息的攻击 (attacks on information in transit)、女巫攻击 (sybil attack)、黑洞/污水池攻击 (blackhole/sinkhole attack)、Hello 泛洪攻击 (Hello flood attack)、虫洞攻击 (wormhole attack) 等^[23]都可以应用于破坏无人机与其他设备或无人机群之间的通信。由于无人机传输信息容易被监听, 且其用于通信的资源有限, 攻击者如果有足够的处理资源, 很容易中断、拦截、篡改通信数据分组, 发动对传输消息的攻击。而针对无人机群, 攻击者可以假冒为多出的节点发动女巫攻击^[24]。

针对这些攻击, 可以使用传感器网络加密算法、安全协议、安全路由等技术进行抵御。除对称加密外, 一些低开销的非对称加密算法, 如文献[25~27]等, 也可用于访问控制等特殊应用。而应用于传感器网络的安全协议 SPINS^[28]也可被用来提供数据机密性、双方数据鉴别、数据新鲜度等安全需求。安全路由一直是无线传感器网络安全研究最重要的内容, 安全路由协议可以通过多种手段实现, 如基于地理位置算法^[29,30]、基于多路径算法^[31,32]、

分簇安全路由协议算法^[33]、基于密码算法^[32,34]、基于智能算法^[35]等。在实际应用中需要根据无人机实际性能和安全级别的平衡选择合适的协议。除此之外, 密钥管理、身份认证、入侵检测、信任管理等安全技术也可应用于无人机上, 提供必要的安全性。

3 无人机发动的攻击、对隐私的侵犯

灵活的机动性使无人机犹如“盗贼”一般可以侵入违禁或者私人的领空, 配备的高清摄像头可能会窥探到别人的隐私^[36,37]。2015 年, 无人机闯入美国白宫成为各大媒体的头条^[38]。文献[39~41]描述了无人机可能被不法分子应用于恐怖主义、毒品走私、非常规武器 (如生化武器) 攻击等。越来越多的人向警察抱怨, 无人机带着摄像头堂而皇之地飞到家中庭院上方或窗户附近。无人机成为高科技领域的“偷窥狂”。来自加利福尼亚州和佛罗里达州的一些报道称, 无人机俯冲到海滩和度假村中, 拍摄人们穿比基尼或半裸晒太阳浴的画面, 随后这些视频被发布在网络上^[42]。无人机搭载热成像摄像头更是让这一问题雪上加霜。即便是把无人机用作特定场合的监控也存在侵犯隐私的问题, 比如停车场、道路、公园等的视频监控, 其中的隐私问题也被文献[43~47]提及。

无人机用作定位和跟踪的技术日趋成熟, 也会使无人机成为新一代的“跟踪狂”。Liu 等^[48]提出了基于等值地图线的定位方法, 并使用小型无人机实际测试对比了其他 5 种不同的定位技术。文献[49~51]通过摄像头数据计算无人机与目标的位移等信息, 并自动调整无人机的姿态和位置, 从而跟踪目标。

当无人机成为“盗贼”、“偷窥狂”和“跟踪狂”时, 不同层次的防范、解决方案也被相继提出。首先, 监管部门设定禁飞区。在发生无人机闯入白宫事件之后, 大疆无人机立刻强制升级固件, 禁止大疆无人机在华盛顿的禁飞区内飞行。大疆无人机的禁飞区可以在其官方网站上查询^[52], 图 2 为其在中国北京的禁飞区。实际上, 各国政府的相关监管部门都出台了相关监管政策并划定了禁飞区, 美国联邦航空局 (FAA, Federal Aviation Administration) 推出了无人机禁飞区标识, 如图 3 所示。各大无人机厂商不仅要根据 GPS 来判定是

否闯入禁飞区, 还需要加入图像识别禁飞标志的功能。一个自发的“**No Fly Zone**”组织也在尝试解决无人机侵犯个人隐私的问题。根据文献[53]的描述, 该组织让公众在自己家周围建立起禁飞区, 防止无人机窥探隐私。“**No Fly Zone**”网站^[54]的使用方法非常简单。用户只需输入自己的家庭住址, 并提供其他一些基本信息。“**No Fly Zone**”组织会对用户提供的信息进行验证和注册, 进而将GPS坐标录入该组织数据库。然后这个组织会与一些无人机生产商合作, 把相关坐标上传到无人机数据里, 自动阻止无人机飞越已注册房屋, 这项服务完全免费。目前, 已有多家硬件和软件公司承诺尊重这些无人机禁飞区, “**No Fly Zone**”组织的合作伙伴包括Ghost无人机、亿航、Horizon Hobby和PixiePath等。“**No Fly Zone**”组织表示, 并不能确保将家庭地址注册到该网站之后就一定能阻止无人机抵近, 因为这项禁令只适用于与该组织有合作协议的厂商生产的无人机。



图2 大疆无人机在北京的禁飞区



图3 无人机禁飞区标识

其次, 在无人机用作公共场合视频监控侵犯隐私的问题上, 隐私过滤方法也被广泛研究。Bonetto等^[55]从无人机在的停车场监控视频数据中得出基于典型的无人机监控序列, 并基于“众

包”的评估方法, 在监控可用和隐私保护的绩效之间取得平衡, 最终得到5个隐私保护过滤器。

最后, 当规则被打破, 攻击者绕过无人机自身对禁飞区的限定, 比如使用姿态模式、系统破解、GPS欺骗等, 那么就要使用强硬的方法来阻止无人机, 比如探测、入侵甚至捕获来犯的无人机。Mezei等^[56]通过无人机的声音特征来识别无人机的存在。Moses等^[57]设计出了一种轻巧的可以装配在任意小型无人机上的雷达系统, 在该系统中, 工作在10.5 GHz频段的雷达可以探测并鉴别其他无人机。在合法的情况下, 第2节中对无人机的攻击手段可以转化为防御无人机的手段, 如在干扰、获取无人机的控制权后, 迫使无人机降落到安全地点。全球各大安防公司也加紧对无人机的防御进行研发。文献[58]报道了在2016年春晚分会场亮相的天网“低慢小”目标拦截系统(简称“天网”), 该系统是中国航天科工二院206所为应对低空、慢速、小目标防控这一世界难题而研发的自主创新产品, 该产品能够对航空模型、动力三角翼、动力伞、风筝等低空慢速小型飞行器进行探测、预警、跟踪定位与高效拦截。

4 无人机认证及溯源

无人机的认证、溯源问题以及相关解决方案如下。1) 通信交互的身份认证。例如, 无人机用作传感器网络的数据收集, 在传感器上传采集数据给无人机前, 必须确认无人机的合法身份。文献[9]详细对比了包括该文献提出的安全通信协议的功能, 如表1所示。Senthil和Ilango^[59]提出了一种安全认证和完整性校验技术。该技术利用共享密钥提供身份认证, 并利用相互认证技术实现收发双方共享认证密钥。2) 无人机飞入特定区域的认证。例如, 个人设置自己的住处为禁飞区, 然而快递公司的无人机需要飞入该区域送货; 军事区域只允许自己的无人机进行巡航。目前并没有很好的安全架构对无人机飞入某个区域进行认证。3) 事故追责的溯源。据文献[60]报道, 在澳大利亚Geraldton Endure Batavia 3项全能比赛上, 一架用于记录赛况的无人机撞向运动员, 造成其头部轻微受伤, 需要进行缝针治疗。无人机的操作人员表示, 引发此次事故的原因是观众偷走了

控制器。2015年7月，大疆生产的“精灵3”无人机坠毁在巴控克什米尔地区，围绕此事印度和巴基斯坦两国互相指责。在这些事故中，无人机记录的数据能给责任的鉴定提供重要的帮助。

表1 不同通信协议的安全功能对比

协议	具有的安全功能			
	密钥协商	用户认证	不可抵赖性	用户撤销
Yang's CL-AKA ^[61]	是	是	否	否
Sun's CI-AKA ^[62]	是	是	否	否
CLSC-TKEM ^[63]	是	是	是	否
eCLSC-TKEM ^[9]	是	是	是	是

当无人机拍摄的隐私视频泄露到网上，为了追查拍摄的无人机也需要对无人机包括摄像头在内的物理配件特征进行鉴定。摄像头拍摄的照片、视频的噪声包含了该设备大量的指纹信息，这是因为摄像头处理信号时，有许多因素会导致噪声，如传感器有坏点形成的固定模式噪声（FPN），但更为普遍的来源是光电响应非均匀特性（PRNU）。如果把图片、视频的噪音看成摄像头的水印，那么可以从这些水印来辨别相应的摄像头。Lukas 等^[64]首次利用模式噪声提出了图像的摄像头来源鉴别方法。在这个基础上，研究人员对特征的提取^[65]、特征在大规模照片检测情况下的有效性^[66,67]、特征信息的高效使用^[68,69]等方面进行了改进。鉴定图像、视频来源的技术可以配合无人机飞行数据，从而得出更准确的判断。

5 结束语

随着制造成本的降低和技术发展和成熟，小型无人机正逐步走向大众消费级市场。小型无人机在给人们生活带来便利的同时，也面临日益严峻的安全问题。本文从小型无人机面临的安全威胁、利用小型无人机发起的攻击以及无人机的认证和溯源等方面总结和分析了国内外无人机安全领域的研究进展。基于对目前研究现状的总结和分析，认为小型无人机未来安全发展趋势主要有如下特点。

1) 基于无人机自身的特点存在的安全问题。例如，无人机的操控和巡航需要无线信号的操控以及GPS信号的导航，对无线信号的干扰、入侵、

GPS欺骗等攻防的研究将会不断深入。

2) 无人机与应用结合存在的安全问题。如使用高清摄像头、甚至热成像摄像头的无人机航拍侵犯隐私的问题；无人机作为传感器网络的数据采集点，需要安全协议在和传感器交互的过程中确保身份的认证、数据的安全传输等功能的问题；无人机自组网或者作为网络节点的安全问题。

3) 政策、法规监管盲区所存在的安全问题。如对非法无人机的探测、攻击、捕获的问题；无人机事故追责、泄露隐私数据，需要获取电子证据进行鉴定的问题。

参考文献：

- [1] 2016年3·15晚会[EB/OL]. <http://315.cntv.cn/special/2016/index.shtml>.
The 3·15 gala of China 2016[EB/OL]. <http://315.cntv.cn/special/2016/index.shtml>.
- [2] CES 2015: why the future of drones is up in the air[EB/OL]. <http://www.bbc.com/news/technology-30721339>.
- [3] EVTank. 2015年度民用无人机市场研究[EB/OL]. <http://www.199it.com/archives/345432.html>.
EVTank. 2015 market research on civilian drones[EB/OL]. <http://www.199it.com/archives/345432.html>.
- [4] 2015-2020年中国无人机行业市场分析与投资前景预测报告[EB/OL]. <http://wenku.baidu.com/view/51a21dd0f121dd36a32d82f3.html?from=search>.
Market research and prediction on China's drone industry of 2015-2020[EB/OL]. <http://wenku.baidu.com/view/51a21dd0f121dd36a32d82f3.html?from=search>.
- [5] 关于无人机，你需要知道的都在这里了[EB/OL]. <http://36kr.com/p/220702.html>.
All you need to know about drones[EB/OL]. <http://36kr.com/p/220702.html>.
- [6] CHILDERS B. Hacking the Parrot AR drone[J]. Linux Journal, 2014, 2014(241): 1.
- [7] PLEBAN J S, BAND R, CREUTZBURG R. Hacking and securing the AR. Drone 2.0 quadcopter: investigations for improving the security of a toy[C]//SPIE International Conference on Mobile Devices and Multimedia: Enabling Technologies, Algorithms, and Applications, San Francisco. c2014(9030):271-283.
- [8] 3·15晚会报道的无人机是怎么被劫持的？[EB/OL]. <https://security.tencent.com/index.php/blog/msg/103>.
The 3·15 gala of China report on how did drones got hijacked[EB/OL]. <https://security.tencent.com/index.php/blog/msg/103>.
- [9] WON J, SEO S H, BERTINO E. A secure communication protocol for drones and smart objects[C]//The 10th ACM Symposium on Information, Computer and Communications Security, New York. c2015: 249-260.
- [10] BIRNBAUM Z, DOLGIKH A, SKORMIN V, et al. Unmanned

- aerial vehicle security using recursive parameter estimation[C]//2014 IEEE International Conference on Unmanned Aircraft Systems (ICUAS), Orlando. c2014: 692-702.
- [11] CABANISS R, KUMAR V, MADRIA S. Multi-party encryption (MPE): secure communications in delay tolerant networks[J]. *Wireless Networks*, 2015, 21(4): 1243-1258.
- [12] HUMPHREYS T E, LEDVINA B M, PSIAKI M L, et al. Assessing the spoofing threat: development of a portable GPS civilian spoofer[C]//The ION GNSS International Technical Meeting of the Satellite Division, Savannah. c2008: 55-56.
- [13] SHEPARD D. Characterization of receiver response to spoofing attacks[D]. Austin: University of Texas at Austin, 2011.
- [14] SHEPARD D P, HUMPHREYS T E, FANSLER A A. Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks[J]. *International Journal of Critical Infrastructure Protection*, 2012, 5(3): 146-153.
- [15] 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.
- [16] BROUMANDAN A, JAFARNIA-JAHROMI A, DEHGHANIAN V, et al. GNSS spoofing detection in handheld receivers based on signal spatial correlation[C]//The IEEE/ION Position Location and Navigation Symposium (PLANS), Myrtle Beach. c2012: 479 - 487.
- [17] DE LORENZO D S, GAUTIER J, RIFE J, et al. Adaptive array processing for GPS interference rejection[C]//The 18th International Technical Meeting of the Satellite Division of the Institute of Navigation, Long Beach. c2005: 618-627.
- [18] MONTGOMERY P Y, HUMPHREYS T E, LEDVINA B M. A multi-antenna defense: receiver-autonomous GPS spoofing detection[J]. *Inside GNSS*, 2009, 4(2): 40-46.
- [19] DEHGHANIAN V, NIELSEN J, LACHAPELLE G. GNSS spoofing detection based on receiver C/No estimates[C]//The 25th International Technical Meeting of the Satellite Division of the Institute of Navigation, Nashville. c2012: 2878-2884.
- [20] WEISS S, SCARAMUZZA D, SIEGWART R. Monocular-SLAM-based navigation for autonomous micro helicopters in GPS-denied environments[J]. *Journal of Field Robotics*, 2011, 28(6): 854-874.
- [21] WESSON K D, EVANS B L, HUMPHREYS T E. A combined symmetric difference and power monitoring GNSS anti-spoofing technique[C]//2013 IEEE Global Conference on Signal and Information Processing, Austin. c2013: 217-220.
- [22] CHOWDHARY G, JOHNSON E N, MAGREE D, et al. GPS-denied indoor and outdoor monocular vision aided navigation and control of unmanned aircraft[J]. *Journal of Field Robotics*, 2013, 30(3): 415-438.
- [23] PATHANA K, LEE H W, HONG C S. Security in wireless sensor networks: issues and challenges[C]//The 8th IEEE International Conference on Advanced Communication Technology, Phoenix Park. c2007: 6-1048.
- [24] NEWSOME J, SHI E, SONG D, et al. The sybil attack in sensor networks: analysis & defenses[C]//The ACM 3rd International Symposium on Information Processing in Sensor Networks, New York. c2004: 259-268.
- [25] GURA N, PATEL A, WANDER A, et al. Comparing elliptic curve cryptography and RSA on 8 bit CPUs[C]//The 6th Springer International Workshop on Cryptographic Hardware and Embedded Systems, Springer Berlin. c2004: 119-132.
- [26] MALAN P T, WEISH M, SMITH M D. A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography[C]//The 1st IEEE International Conference on Sensor and Ad Hoc Communications and Networks, Santa Clara. c2004: 58-67.
- [27] WANG H, SHENG B, LI Q. Elliptic curve cryptography-based access control in sensor networks[J]. *International Journal of Security and Networks*, 2006, 1(3): 127-137.
- [28] PERRIG A, SIEWCZYK R, JYGAR J D. SPINS: security protocols for sensor networks[J]. *Wireless Networks Journal (WINE)*, 2002, 8(5): 521-534.
- [29] ZHOU Y, LI L. A trust-aware and location-based secure routing protocol for WSN[J]. *Applied Mechanics and Materials*, 2013, 373-375: 1931-1934.
- [30] KANG H S, KIM S R, KIM P. Traffic deflection method for dos attack defense using a location-based routing protocol in the sensor network[J]. *Computer Science and Information Systems*, 2013, 10(2): 685-701.
- [31] HAYAJNEH T, DOOMUN R, AL-MASHAQBEH G, et al. An energy-efficient and security aware route selection protocol for wireless sensor networks[J]. *Security & Communication Networks*, 2014, 7: 2015-2038.
- [32] SANGEETHA R, YUVARAJU M. Secure energy-aware multipath routing protocol with transmission range adjustment for wireless sensor networks[C]//The 2012 IEEE International Conference on Computational Intelligence & Computing Research (ICCIC), Coimbatore. c2012: 1-4.
- [33] LOTF J J, HOSSEINZADEH M, ALGULIEV R M. Hierarchical routing in wireless sensor networks: a survey[C]//The 2nd International Conference on Computer Engineering and Technology, Chengdu. c2010: 650-654.
- [34] CHEN X, MAKKI K, YEN K, et al. Sensor network security: a survey[J]. *IEEE Communications Surveys & Tutorials*, 2009, 11(2): 52-73.
- [35] HU T, FEI Y. QELAR: a machine-learning-based adaptive routing protocol for energy-efficient and lifetime-extended underwater sensor networks[J]. *IEEE Transactions on Mobile Computing*, 2010, 9(6): 796-809.
- [36] KORSHUNOV P, EBRAHIMI T. Using warping for privacy protection in video surveillance[C]//The 18th IEEE International Conference on Digital Signal Processing (DSP), Fira. c2013: 1-6.
- [37] KORSHUNOV P, EBRAHIMI T. Using face morphing to protect privacy[C]//The 10th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), Krakow. c2013: 208-213.
- [38] SCHMIDT M, SHEAR M. A drone, too small for radar to detect, rattles the White House[EB/OL]. <http://www.suasnews.com/2015/01/a-drone-too-small-for-radar-to-detect-rattles-the-white-house/>.
- [39] GORMLEY D M. UAVs and cruise missiles as possible terrorist weapons[EB/OL]. http://kms1.isn.ethz.ch/serviceengine/Files/ISN/14389/ichaptersection_singledocument/acad1aa7-4c58-4da5-a93a-f2558375a299/en/02_Gormley.pdf.
- [40] GORMLEY D M, SPEIER R. Controlling unmanned air vehicles:

- new challenges[J]. The Nonproliferation Review, 2003, 10(2): 66-79.
- [41] SIRAK M. Air force studies how to counter hostile UAVs[J]. Helicopter News, 2006, 1:1-2.
- [42] 无人机不乏黑暗面成天空监管一大隐患[EB/OL]. <http://tech.163.com/15/0529/08/AQP63QES000915BD.html>. The bad influences drone might brought to the sky surveillance[EB/OL]. <http://tech.163.com/15/0529/08/AQP63QES000915BD.html>.
- [43] PITT J, PERAKSLIS C, MICHAEL K. Drones humanus introduction to the special issue[J]. Technology and Society Magazine, 2014, 33(2): 38-39.
- [44] WILSON R L. Ethical issues with use of drone aircraft[C]//The 2014 IEEE International Symposium on Ethics in Science, Technology and Engineering, Chicago. c2014: 1-4.
- [45] VILLASENOR J. "Drones" and the future of domestic aviation[J]. Proceedings of the IEEE, 2014, 102(3): 235-238.
- [46] FINN R L, WRIGHT D. Unmanned aircraft systems: surveillance, ethics and privacy in civil applications[J]. Computer Law & Security Review, 2012, 28(2): 184-194.
- [47] VILLASENOR J. Observations from above: unmanned aircraft systems and privacy[J]. Harvard Journal of Law & Public Policy, 2013, 36: 457.
- [48] LIU Z, LI Z, LIU B, et al. Rise of mini-drones: applications and issues[C]//Workshop on Privacy-Aware Mobile Computing. c2015:7-12.
- [49] MAO H, YANG C, ABOUSLEMAN G P, et al. Automated multiple target detection and tracking in UAV videos[C]//SPIE-The International Society for Optical Engineering. c2010.
- [50] MEJIAS L, SARIPALLI S, CAMPOY P, et al. Visual servoing of an autonomous helicopter in urban areas using feature tracking[J]. Journal of Field Robotics, 2006, 23(3-4): 185-199.
- [51] HERISSÉ B, HAMEL T, MAHONY R, et al. Landing a VTOL unmanned aerial vehicle on a moving platform using optical flow[J]. IEEE Transactions on Robotics, 2012, 28(1): 77-89.
- [52] 安全飞行指引飞行区域限制[EB/OL]. <http://www.dji.com/cn/flysafe/no-fly>. Safety guide on aircraft movement area restrictions[EB/OL]. <http://www.dji.com/cn/flysafe/no-fly>.
- [53] 美国人这样阻止无人机窥探住宅隐私[EB/OL]. <http://tech.qq.com/a/20150210/072083.htm>. What Americans did to protect residents' privacy from drones[EB/OL]. <http://tech.qq.com/a/20150210/072083.htm>.
- [54] NoFlyZone[EB/OL]. <https://www.noflyzone.org/>.
- [55] BONETTO M, KORSHUNOV P, RAMPONI G, et al. Privacy in mini-drone based video surveillance[C]//The 2015 IEEE International Conference on Image Processing (ICIP), Quebec City. c2015: 2464-2469.
- [56] MEZEI J, FIASKA V, MOLNAR A. Drone sound detection[C]//The 16th IEEE International Symposium on Computational Intelligence and Informatics (CINTI), Budapest. c2015: 333-338.
- [57] MOSES A, RUTHERFORD M J, VALAVANIS K P. Radar-based detection and identification for miniature air vehicles[C]//The 2011 IEEE International Conference on Control Applications (CCA), Denver. c2011: 933-940.
- [58] 航天科工披露反无人机系统已执行多次任务[EB/OL]. <http://war.163.com/16/0220/08/BG8MJ36800014OVF.html?f=search>. China Aerospace Science & Industry Corporation has revealed assignments carried out by anti-drone system[EB/OL]. <http://war.163.com/16/0220/08/BG8MJ36800014OVF.html?f=search>.
- [59] ILANGO P. Secure authentication and integrity techniques for randomized secured routing in WSN[J]. Wireless Networks, 2015, 21(2): 443-451.
- [60] 盘点 12 起引发争议的无人机事故[EB/OL]. <http://digi.163.com/15/0324/11/ALFIAEN000162Q5T.html>. View points on 12 controversial drone accidents[EB/OL]. <http://digi.163.com/15/0324/11/ALFIAEN000162Q5T.html>.
- [61] YANG G, TAN C H. Strongly secure certificateless key exchange without pairing[C]//The 6th ACM Symposium on Information, Computer and Communications Security, New York, c2011: 71-79.
- [62] SUN H, WEN Q, ZHANG H, et al. A novel pairing-free certificateless authenticated key agreement protocol with provable security[J]. Frontiers of Computer Science, 2013, 7(4): 544-557.
- [63] SEO S, BERTINO E. Elliptic curve cryptography based certificateless hybrid signcryption scheme without pairing[R]. CERIAS, West Lafayette, IN, USA, 2013.
- [64] LUKAS J, FRIDRICH J, GOLJAN M. Digital camera identification from sensor pattern noise[J]. IEEE Transactions on Information Forensics and Security, 2006, 1(2): 205-214.
- [65] CHEN M, FRIDRICH J, GOLJAN M, et al. Determining image origin and integrity using sensor noise[J]. IEEE Transactions on Information Forensics and Security, 2008, 3(1): 74-90.
- [66] GOLJAN M, FRIDRICH J, FILLER T. Managing a large database of camera fingerprints[C]//IS&T/SPIE Electronic Imaging Symposium, San Jose. c2010.
- [67] GOLJAN M, FRIDRICH J, FILLER T. Large scale test of sensor fingerprint camera identification[C]//IS & T/SPIE Electronic Imaging Symposium, San Jose. c2009.
- [68] HU Y, YU B, JIAN C. Source camera identification technique using large components of imaging sensor pattern noise[J]. Journal of Computer Applications, 2010, 9: 31-35.
- [69] LIU B B, HU Y, LEE H K. Source camera identification from significant noise residual regions[C]//The 17th IEEE International Conference on Image Processing (ICIP), HongKong. c2010: 1749-1752.

作者简介:



刘炜(1985-), 男, 广西南宁人, 暨南大学博士生, 主要研究方向为无人机安全、密码学。

冯丙文(1985-), 男, 四川蓬溪人, 暨南大学博士生, 主要研究方向为信息隐藏、多媒体安全。

翁健(1976-), 男, 广东茂名, 暨南大学教授、博士生导师, 主要研究方向为密码学与信息安全。