

无人机系统安全靶场构建与攻防验证设计

李宇佳¹, 张辉¹, 多滨¹, 王梓斌², 周让¹, 李冬芬¹

(1. 成都理工大学计算机与网络安全学院, 四川 成都 610059; 2. 北京信息系统安全技术重点实验室 北京 100093)

摘要: 无人机技术当前被广泛应用于农业、物流、环境监测等领域, 其安全问题逐渐成为研究的焦点。但当前无人机安全研究中的仿真测试平台存在无法系统有效地开展威胁分析并识别攻击类型与风险点、难以生成高质量攻击数据集以支撑入侵检测模型训练、无法实现攻防迭代验证等问题。针对上述问题, 提出了一套无人机攻防闭环验证的实验框架, 设计了一个包含基础设施层、模拟层、通信层、应用层和智能调度层5层架构的新型人工智能辅助无人机系统安全靶场。借助靶场提供的仿真测试环境, 构建了从Wi-Fi发现、密码破解到指令欺骗的综合攻击场景。利用在该攻击场景下生成的实验数据, 设计了一种基于单类支持向量机的入侵检测系统, 经攻防迭代调整并不断优化实验参数, 该入侵检测系统在指令欺骗攻击检测任务中的检测精确率由85.6%提升至93.8%, 相比基于经典局部离群因子算法构建的模型, 优化后的单类支持向量机模型检测精确率在多种攻击场景下均更具优势, 证实了所提出的无人机系统安全靶场在威胁分析、数据集构建和攻防闭环验证方面的系统性、完备性和有效性。

关键词: 无人机系统; 安全; 威胁分析; 防护策略; 安全靶场

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2026010

Unmanned aerial vehicle system security cyber range construction and attack-defense validation design

Li Yujia¹, Zhang Hui¹, Duo Bin¹, Wang Zibin², Zhou Rang¹, Li Dongfen¹

1. College of Computer and Network Security, Chengdu University of Technology, Chengdu 610059, China

2. Beijing Key Laboratory of Information System Security Technology, Beijing 100093, China

Abstract: Unmanned aerial vehicle (UAV) technology is currently widely applied in fields such as agriculture, logistics and environmental monitoring, and its security issues have gradually become a research focus. However, in current UAV security research, existing simulation and testing platforms have problems: effective and systematic threat analysis cannot be carried out to identify attack types and risk points; high-quality attack datasets are difficult to be generated to support the training of intrusion detection models; “attack-defense iterative verification” cannot be realized, that is, the model is tested by attacks and then further optimized according to the results. To address the

收稿日期: 2025-08-13; 修回日期: 2025-12-13

通信作者: 多滨, duo_bin@163.com

基金项目: 国家自然科学基金 (No.62172060); 四川省高等学校创新性实验项目 “智能无人系统安全创新实验”; 2024-2026年成都理工大学高等教育人才培养质量和教学改革项目 (No.JG2420017, No.JG2430165)

Foundation Items: The National Natural Science Foundation of China (No. 62172060), Innovative Experiment Project of Colleges and Universities in Sichuan Province “Innovative Experiment on Security of Intelligent Unmanned Systems”, Higher Education Talent Training Quality and Teaching Reform Project of Chengdu University of Technology (No. JG2420017, No. JG2430165)

above problems, an experimental framework for UAV attack-defense closed-loop verification was proposed. A new artificial intelligence-assisted UAV system security testbed with a five-layer architecture (infrastructure layer, simulation layer, communication layer, application layer and intelligent scheduling layer) was designed and implemented. With the simulation test environment provided by the testbed, a comprehensive attack scenario covering Wi-Fi discovery, password cracking to command spoofing was constructed. Using the experimental data generated in this attack scenario, an intrusion detection system based on one-class support vector machine was designed. After iterative adjustment of attack and defense and continuous optimization of experimental parameters, the detection precision of the intrusion detection system for command spoofing attacks was improved from 85.6% to 93.8%. Compared with the model constructed based on the classic local outlier factor algorithm, the optimized one-class support vector machine model has more advantages in detection precision under various attack scenarios, which verifies that the proposed UAV system security testbed is systematic, complete and effective in threat analysis, dataset construction and attack-defense closed-loop verification.

Keywords: unmanned aerial vehicle system, security, threat analysis, protection strategy, security cyber range

0 引言

无人机 (unmanned aerial vehicle, UAV), 又称远程驾驶航空器, 是指由控制站进行管理 (包括远程操控或自主飞行) 的航空器^[1]。无人机系统主要由硬件、软件和通信系统三大部分构成。硬件部分包括机架、动力系统、飞行控制 (简称“飞控”) 系统和机载计算单元。机架通常采用碳纤维或铝合金等轻质材料制造, 从而确保无人机的稳定性和轻量化; 动力系统由电机、电子调速器和电池构成, 为无人机提供能量; 飞控系统通过多种传感器 (如惯性测量单元、气压计和全球导航卫星系统接收器) 实时感知并调节飞行姿态, 从而确保飞行的稳定性。软件部分, 飞控固件负责无人机的姿态控制, 地面站软件用于实现飞行任务的规划与实时监控, 智能驾驶模块借助人工智能技术提升任务执行能力 (如自主避障和目标识别)。通信系统用于实现无人机与地面站之间的实时数据传输, 通常采用 Wi-Fi、蓝牙或 4G/5G 等通信方式, 结合自组网技术来支持多无人机协同工作, 从而灵活应对复杂任务环境下的通信需求^[2]。中国民航局预测, 2035 年, 中国低空经济市场规模有望突破 3.5 万亿元人民币。该产业涵盖无人机、垂直起降航空器及其他通用航空装备^[3]。随着无人机技术的广泛应用, 其系统安全问题愈发受到关注。

近年来, 部分无人机遭遇了全球定位系统 (global positioning system, GPS) 干扰、控制信号劫持和网络攻击等安全威胁。2015 年, 在荷兰阿

姆斯特丹的一座机场, 部分无人机在遭遇信号干扰后被劫持, 导致其飞行路径被恶意改变^[4]。2020 年, 墨西哥警方通报了一起无人机遭非法控制事件, 犯罪分子利用干扰技术劫持无人机, 并将其用于走私毒品^[5]。2023 年, 有研究人员对大疆 Mini SE 无人机的增强 Wi-Fi 协议进行了逆向工程分析, 发现其控制命令存在安全漏洞。攻击者可以利用廉价的商用 Wi-Fi 路由器对无人机实施劫持攻击, 不仅能够改变其飞行路径, 甚至可以实现对无人机的完全控制^[6]。这类安全事件不仅会影响无人机的正常运营, 还可能带来严重的经济损失或公共安全隐患。因此, 如何提升无人机系统的安全性, 已成为当前研究领域亟待解决的一个关键问题。

当前针对无人机安全的研究主要可以分为安全威胁分析和防护策略两大方向, 如图 1 所示。在安全威胁分析方面, 研究聚焦于无人机系统面临的各类攻击 (如信号劫持、GPS 干扰、协议漏洞利用等)。部分研究关注针对无人机硬件的攻击, 但囿于篇幅, 本文主要探讨无人机系统在通信和软件层面所面临的安全威胁。在防护策略方面, 安全协议与入侵检测是研究热点。其中, 入侵检测技术尤为受关注, 其核心是通过对无人机运行行为的实时监控与分析, 及时识别潜在的攻击行为^[7]。

为有效验证上述安全威胁分析的准确性与防护策略的有效性, 需构建专门的实验环境来模拟真实的攻防场景。无人机安全测试平台通过模拟各种攻击场景, 能够对现有防护措施的有效性进

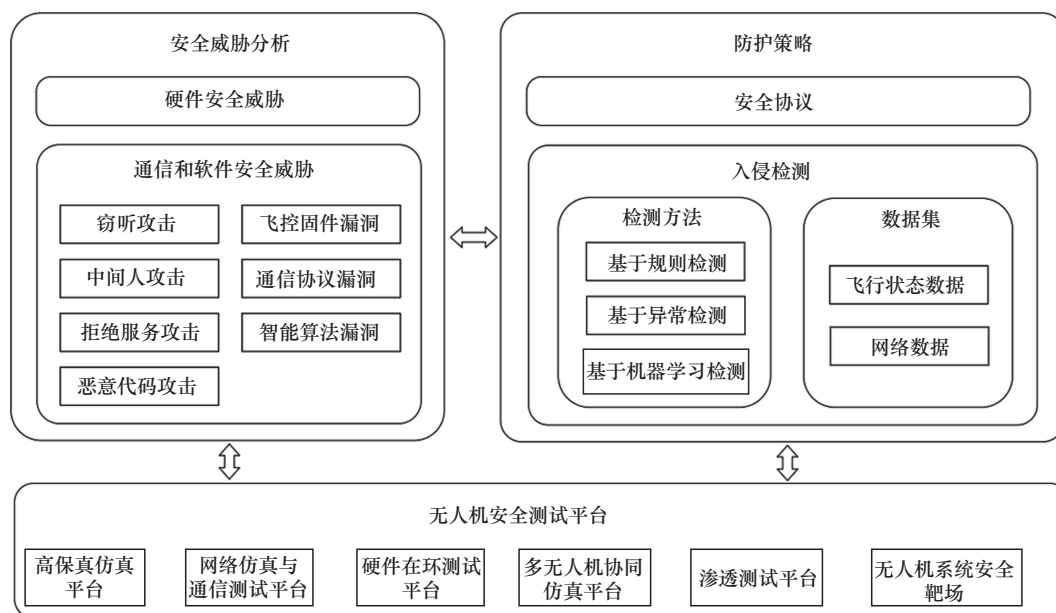


图1 无人机安全研究现状

行验证与评估,从而为无人机安全研究中的攻防场景模拟、防护技术验证及方案迭代优化提供关键的实验支撑。

(1) 无人机通信和软件威胁分析研究现状

无人机系统的核心安全风险集中在通信系统与软件两大层面,这也是当前安全威胁分析研究的重点方向。在通信系统层面,由于无人机受自身算力、功耗等资源约束,难以部署复杂的加密与认证机制,这为攻击者入侵通信链路,进而破坏数据的机密性、完整性与可用性提供了可乘之机^[8]。在软件层面,风险同样突出,飞控固件、地面站软件的设计缺陷或零日漏洞,以及智能算法相关漏洞,均易被攻击者利用;同时,恶意代码可以通过物理接触、网络渗透、社会工程学等途径入侵系统,直接威胁无人机的控制权与数据安全。

具体而言,当前研究揭示的主要威胁包括以下几类。

1) 窃听攻击。密码技术是保障无人机通信安全的关键手段,弱密码甚至无密码的协议极易遭受攻击。文献[9]指出,大疆无人机采用的 DroneID 跟踪协议因未加密,攻击者可以通过低成本的硬件设备拦截无人机,以及获取操作者的位置和身份等信息。此外,攻击者还可以窃取无人机与地面站之间的通信数据,威胁数据的机密性与

通信质量^[10]。

2) 中间人攻击。无线通信的开放性使得攻击者能够通过伪造控制信号接管无人机^[11]。通过中间人攻击,攻击者可以拦截并篡改无人机与地面站之间的射频通信数据^[12];还可以通过注入虚假的位置或轨迹信息,迫使无人机偏离预定航线^[13]。

3) 协议漏洞利用。利用软件定义无线电设备记录并重放无人机与控制器的射频信号,攻击者可以实施重放攻击,干扰起飞、着陆等关键操作^[14]。大疆精灵3无人机无人机的控制链路漏洞被破解后,攻击者可以通过伪造信号劫持无人机,进而剥夺合法操作者的控制权^[15]。

4) 拒绝服务(denial of service, DoS)攻击。无人机资源受限的特性使其易遭受DoS攻击。攻击者通过发送过量请求导致网络拥塞、系统资源耗尽,造成通信中断或服务失效^[16]。

5) 飞控固件漏洞。飞控固件易存在安全漏洞,攻击者可以通过逆向工程、模糊测试等手段加以利用。文献[17]指出,大疆御3无人机的固件被发现存在弱Wi-Fi密码、文件传输协议服务无认证等漏洞(CVE-2023-6951、CVE-2023-6949),攻击者可以借此窃取数据或完全控制无人机。此外,飞控固件通常采用加密签名保护且输入接口受限,导致动态分析难度大,漏洞难以及时发现^[18]。

6) 恶意代码攻击。恶意代码(如木马等)可以入侵机载系统或地面控制站,破坏系统运行、窃取数据或夺取控制权。文献[19]提到,美国 Predator 和 Reaper 无人机曾感染病毒,该病毒记录飞行员按键操作,存在敏感信息泄露的风险。

7) 智能算法漏洞。人工智能技术的引入带来了新的安全隐患。例如,多传感器融合系统可能被 3D 打印的“隐形”目标欺骗,导致感知失效^[20];强化学习路径规划算法易受梯度攻击和数据包丢失影响,导致路径规划性能下降^[9];Ad2Attack 是一种适应性对抗攻击方法,通过图像重采样扰动,可使无人机视觉跟踪系统丢失目标,且扰动难以被察觉^[21]。

当前无人机安全威胁分析研究面临若干挑战。首先,漏洞复现与威胁建模缺乏系统性,相关研究多局限于单一技术场景,实验设计大多基于“单攻击向量+静态环境”的理想模型,与真实场景存在较大差距。真实场景中的安全威胁往往呈现多维联合攻击特征,尤其是在通信安全领域,攻击手段的组合运用更加普遍。其次,无人机固件版本的高频迭代导致已发现漏洞的复现环境难以留存(如厂商实时修补 DroneID 协议加密缺陷、飞控固件漏洞等),研究者难以获得可以复现的标准化测试环境,制约了研究的延续性。最后,各种攻击相关研究因缺乏专用的安全沙箱,在实验过程中面临真实系统瘫痪的风险(如分析 Predator 无人机病毒样本时,必须在隔离环境中进行)。这些问题共同构成了当前无人机安全威胁分析研究的主要瓶颈,给现有研究带来了显著挑战。

(2) 无人机系统防护策略研究现状

针对无人机系统面临的安全威胁,近年来研究者提出了许多防护策略来增强无人机在复杂环境下的安全性。这些防护策略可以大致分为预防型和检测型两大类。其中,预防型策略聚焦于无人机通信协议的安全性研究,旨在通过改进加密技术、完善协议设计,提升系统的原生抗攻击能力^[22]。本文将重点围绕检测型策略展开论述,该方法通过监控和分析无人机系统的行为,实现对潜在攻击的及时识别。

当前,大多数研究倾向于根据检测方法对入侵检测系统进行分类(如基于规则的检测、基于

异常的检测、基于机器学习方法的检测等),本文从检测所依赖的数据集与特征入手,将现有的无人机入侵检测系统分为飞行状态数据驱动型和网络数据驱动型两类。前者通过分析无人机飞控系统日志文件记录的飞行器的位置、高度、速度、姿态和陀螺仪、加速度计、气压计等传感器数据,识别潜在的异常和入侵行为;后者聚焦于网络流量特征分析,通过监测流量大小、数据包的长度和到达时间间隔等信息,识别异常网络行为^[23]。

1) 使用飞行状态数据进行入侵检测。Whelan 等^[24]于 2020 年公开了一个无人机攻击数据集,该数据集由真实无人机和仿真的飞行日志组成,包含正常飞行的数据、遭受 GPS 干扰和欺骗攻击时的数据。Whelan 等^[25]使用该数据集对比了多种经典的机器学习检测方法的检测效率。但该数据集中存在部分未标注的数据,人工识别和标记异常数据比较困难,因此制约了检测模型的泛化能力。余丁辰等^[26]基于该数据集提出了一种收缩自编码器的协同检测方法,提升了模型的训练效率,其检测 GPS 欺骗攻击的准确率较原始自编码器提高了 1.63%。也有部分学者选择独立采集数据进行分析,这类数据选取的特征取决于研究侧重点。文霞^[27]使用一个带有 8 通道 GPS 接收机的复合翼无人机采集不同地点的真实 GPS 信号,并模拟了 3 种类型的 GPS 欺骗攻击,在该数据集上构建了堆叠支持向量机神经网络模型,用于检测 GPS 信号欺骗实例。文献[28]提出的基于长期记忆(long short-term memory, LSTM)的检测方法,能够高效检测 GPS 欺骗攻击,且无须升级硬件设备,结合特定飞行路径可以进一步提升检测准确性。但该数据集源于 MATLAB 仿真,缺乏无人机复杂特征及环境多样性,全面性不足。王路阳等^[29]使用真实无人机采集了 1 824 个样本数据,除了无人机飞行状态数据,还记录了环境风向等相关指标,经清洗后获得相关特征 36 项。该团队的核心工作是使用时间增强对抗网络进行数据增强,并使用 LSTM 神经网络训练模型进行检测,最终取得了比较理想的检测效果。

2) 使用网络数据进行入侵检测。Samriya 等^[30]提出了一种基于能量感知的深度神经网络

优化模型,用于无人机网络中的入侵检测。该研究使用 NSL-KDD 和 KDD Cup 99 数据集,结合蚁群优化算法进行特征选择和降维,再通过深度神经网络进行分类;为减少能量消耗,还采用了动态电压和频率缩放机制。实验结果表明,该模型在提高检测准确性、降低时间复杂度和误报率方面优于传统模型。Wu 等^[31]提出一种基于小型机器学习模型的无人机入侵检测系统。该系统使用 CSE-CIC-IDS2018 和 CIC-DDoS2019 数据集,通过改进的模糊粗糙集进行特征选择,结合随机森林和浅层深度学习模型,优化了特征提取和计算效率。该系统能够有效检测分布式拒绝服务(distributed denial of service, DDoS)等网络流量攻击,在减少冗余数据和减轻计算负担的同时保持较高的检测精度。Hassler 等^[32]于 2023 年公开了一个包含无人机正常操作与多种攻击场景下的网络物理数据集。该数据集包含模拟了 DoS、中间人攻击和 GPS 欺骗等的攻击数据,以及物理遥测数据。但该数据集未包含 GPS 坐标等关键物理参数,所模拟的攻击也仅限于网络攻击。赵长啸等^[33]基于该网络流量和物理数据集提出了一种基于双向时间卷积网络(BiTCN)的无人机指挥控制链路 DoS 攻击检测方法,解决了指挥和控制链路在遭受 DoS 攻击时的数据缺失问题。Hadi 等^[34]构建了 UAV-NIDD,该数据集专为无人机网络的网络安全和入侵检测研究而设计。数据通过一个实时测试平台采集,平台包含实际的无人机设备(如 DJI Mavic Air 和 PX4 Vision Dev Kit)、地面控制站和接入点。采集内容涵盖正常飞行状态及多种网络攻击(包括 DoS、DDoS、中间人、GPS 干扰、伪装着陆数据包等攻击)场景下的数据。该团队还采用孤立森林、多层感知机、前馈神经网络及模型无关元学习等机器学习模型在该数据集上开展了测试与对比实验。实验结果表明,在多种类型攻击的检测任务中,前馈神经网络模型在地面站端的检测精度表现最优。

尽管无人机入侵检测领域在检测方法方面开展了广泛研究并取得了丰富成果,但高质量攻击数据集的缺失仍是制约入侵检测模型训练的关键瓶颈。不少研究仍依赖 KDD99、CIC-IDS2017 等传统网络攻击数据集来分析无人机系统安全问

题,这类数据集存在协议适配性不足、无人机专属特征缺失等固有局限,难以匹配无人机系统的特殊应用场景。另有部分研究基于局部通信协议模拟仿真,构建小规模攻防数据集,但此类数据普遍存在维度较低,泛化能力不足的问题。综上,高质量的攻防数据集的匮乏,导致现有检测技术在复杂多变的真实攻击场景下缺乏充分的验证支撑,难以充分发挥其应有效能。

(3) 无人机系统安全测试平台研究现状

在无人机的渗透测试与安全防护技术研究中,构建高效可行的实验平台和测试环境,是推动无人机系统安全技术发展的核心基础之一。

在理想状态下,要全面、真实地评估无人机系统的抗攻击能力,研究人员本应使用真实的无人机开展测试。然而,受限于高昂的实验成本、复杂的资源调配、严格的时间约束和潜在的设备损坏风险,依赖实体无人机开展安全测试往往难以同时满足研究所需的全面性、可重复性和安全性要求。因此,越来越多的研究者转向更加经济、可控的仿真测试平台。

当前主流的无人机系统安全测试平台主要涵盖高保真仿真平台、网络仿真与通信测试平台、硬件在环测试平台、多无人机协同仿真平台、渗透测试平台和无人机系统安全靶场等类型,如表 1 所示。这些平台各有侧重,分别面向无人机的飞行控制、通信安全、渗透测试、硬件性能等的评估需求。例如, Gazebo + SITL^[9]和 Air-Sim^[35]等高保真仿真平台能够模拟无人机的飞行行为 and 控制系统,适用于飞行控制算法和任务规划的验证,但在渗透测试方面的支持较为有限。UavNetSim-v1^[38]和 FlyNetSim^[39]等网络仿真平台专注于无线网络和通信协议的安全性研究,能够模拟多种网络攻击场景。RFlySim^[40]等硬件在环测试平台通过集成真实的飞行控制系统硬件,能够有效评估硬件与软件之间的兼容性和系统对抗实际攻击的能力。然而,这些平台往往难以全面模拟各类攻击场景与攻击手段,且防护验证也主要集中于硬件层面,缺乏兼具系统性、综合性的安全测试能力。此外,渗透测试平台(如 INDRA: Sky Commander^[42])能够进行射频攻击和其他网络安全测试,特别适合小型无人

表 1 无人机安全测试平台

类别	平台示例	文献	描述	网络和通信模拟	实时监控	渗透测试支持	综合攻击场景构建	攻防闭环验证	AI 辅助
高保真仿真平台	Gazebo + SITL	[9]	适用于无人机控制算法和飞行任务规划的研究	是	是	否	否	否	否
	AirSim	[35]	适用于无人机仿真与深度学习算法测试, 在自动驾驶、图像处理和环境感知领域应用广泛	是	是	否	否	否	否
	MATLAB UAV Toolbox	[36]	专注于飞行控制器设计、任务规划和硬件测试	否	是	否	否	否	否
	OpenUAV	[37]	适用于教育、研究和无人机任务的调度与控制测试	是	是	是	否	否	否
网络仿真与通信测试平台	UavNetSim-v1	[38]	基于 Python 的仿真平台, 主要用于无人机网络层、通信协议的安全性研究	是	否	是	否	否	否
	FlyNetSim	[39]	集成了 NS-3 和 ArduPilot 的网络仿真平台, 适用于网络协议的安全性分析和验证	是	是	是	否	否	否
硬件在环测试平台	RFlySim	[40]	适用于控制系统的攻击测试与防护验证	是	是	否	否	否	否
多无人机协同仿真平台	XTDrone	[41]	适用于多无人机协同控制与任务规划的安全性研究	是	是	是	否	否	否
渗透测试平台	INDRA: Sky Commander	[42]	基于云的渗透测试平台, 专为小型无人机设计, 模拟射频攻击	是	是	是	否	否	否
无人机系统安全靶场	虚实结合的无人机安全靶场	[43]	集成了针对实体无人机和虚拟无人机的多种安全测试技术	是	是	是	否	否	否
	攻防闭环的 AI 辅助靶场	本文	实现攻防闭环验证的 AI 辅助无人机系统安全靶场	是	是	是	是	是	是

机的安全评估, 但缺乏对复杂攻击场景的全面支持。

现有无人机安全测试平台的上述局限, 以及其在设计之初未重视融合防护方法, 导致当前研究难以实现攻防迭代验证 (即无法在统一平台内先通过攻击测试验证防护模型的有效性, 再依据测试结果对模型进行针对性优化)。这使得防护技术验证相关实验多停留在理论阶段, 且多数实验的测试环境仅包含无人机的部分特征, 未能提供完整的、可复现的标准化测试场景。此外, 许多防护策略的实验仅针对单一的预设攻击手段, 这极易造成验证结果的鲁棒性虚高 (即模型在特定条件下表现优异, 但面对真实世界中复杂、未知的复合攻击时, 防护效果显著下降)。

(4) 网络靶场研究现状

鉴于无人机系统安全靶场领域现存文献资料相对匮乏, 本文采用横向借鉴的研究思路, 通过系统梳理网络靶场技术在其他应用领域的最新研究进展, 为无人机安全靶场的理论构建和技术实现提供参考依据。

在国内, 邹星等^[44]系统梳理了网络靶场的定义、功能与发展阶段, 并分析了美国国家网络靶场等典型案例, 指出仿真技术和数据采集评估是靶场构建的核心挑战。王佰玲等^[45]聚焦工业控制领域, 总结了工业控制靶场的关键技术 (如虚拟化和协议仿真), 并指出了高保真工业控制环境模拟的难点。

在国外, Davis 等^[46]的早期研究将靶场划分为模拟、仿真和叠加 3 类, 指出训练是其主要应用场景, 并预测混合技术将因成本效益而成为主流发展方向。Ukwandu 等^[47]综述对比了学术与

工业界靶场,发现模拟类技术应用最为广泛、开源工具被普遍采用。

网络靶场研究相对比较成熟,许多技术与设计(如虚拟化技术、网络仿真技术、靶场管理与监控等)为无人机安全靶场的构建提供了重要的技术参照。然而,传统网络靶场缺乏对无人机飞控系统运行逻辑及 MAVLink 等专用通信协议的高保真模拟能力,无法复现对无人机通信系统和软件层面的安全测试。而在无人机安全测试领域,虽有研究开始探索集成靶场(如文献[43]),但其设计重心仍偏向攻击端的能力验证,缺乏对防护端测试的支持,无法实现攻防闭环验证,同时也缺乏对靶场底层的虚拟化等技术的探讨。

本文的主要工作及贡献体现在以下 4 个方面。首先,本文提出了一套无人机攻防闭环验证的实验框架,设计了一个新型无人机系统安全靶场。该靶场以基于 Docker 的容器化技术和网络仿真为基础,利用 Gazebo 仿真平台和软件在环 (software in the loop, SITL) 仿真技术^[48]模拟无人机系统各组件,并在各组件之间搭建了 MAVLink 通信链路,为复杂的安全测试提供了可靠的基础平台。其次,本文基于所构建的无人机安全靶场提出了一套无人机系统安全攻防验证与优化方法。具体而言,靶场通过模块化设计准确模拟了窃听、欺骗、DoS 攻击等典型威胁场景;通过捕获和记录各种攻击场景下的数据(如网络数据包、飞行日志等),靶场可以获取丰富的攻击数据样本,进而构建多维度的攻击实验数据集。本文利用靶场生成的标准化数据集训练防护模块中的入侵检测系统,结合靶场监控数据对攻击效果与防护性能进行分析,不断迭代以互相验证实验效果,实现“攻击测试—入侵检测—效果验证”的闭环验证机制。再次,本文引入了人工智能技术来提高靶场在渗透测试等方面的易用性和效率。最后,通过仿真实验验证了靶场的有效性与优越性。实验结果表明,优化后的单类支持向量机模型在指令欺骗攻击检测任务中的精确率由 85.2% 提升至 93.8%,相比基于经典局部离群因子算法构建的模型,优化后的单类支持向量机模型在检测精确率上表现出显著优势。该结果充分验证了本文构建的靶场在以下 3 个方面的关键价

值:①多维攻击仿真与威胁评估能力;②实时采集攻防对抗数据与高质量训练样本集构建能力;③防护技术验证与闭环优化能力。

1 无人机系统安全靶场设计

1.1 无人机系统安全靶场的架构设计

针对测试平台功能单一、难以实现攻防闭环验证,以及网络靶场在无人机领域适配性不足等问题,本文提出了一种轻量化、模块化、可扩展的无人机系统安全靶场架构。该架构以无人机仿真与攻防模块为核心,通过软件模拟替代物理硬件,降低了平台的部署门槛与使用成本。如图 2 所示,靶场的整体架构自下而上划分为基础设施层、模拟层、通信层、应用层和智能调度层 5 个层次。各层之间采用标准化接口进行衔接,遵循“模块化可扩展”的设计理念(即每一层均可独立开发并添加攻防模块)。下文将对各层的核心技术与功能进行详细阐述,展现该架构在低成本、易扩展前提下实现多样化安全测试的综合能力。

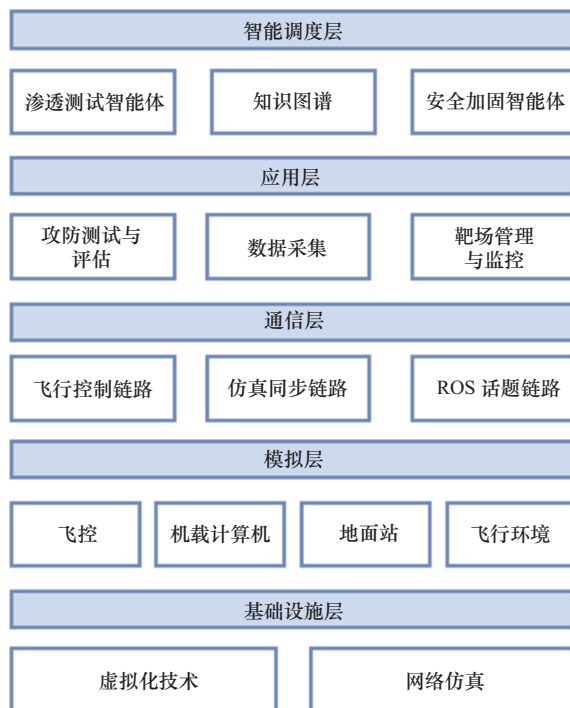


图2 无人机系统安全靶场的整体架构

(1) 基础设施层

基础设施层的核心是虚拟化技术和网络仿

真。本文采用基于 Docker 的容器虚拟化技术，将无人机系统的核心组件封装在独立的容器中运行。每个组件都拥有稳定且隔离的运行环境，既避免了组件之间的相互干扰，又增强了系统的独立性和可扩展性。这种隔离机制能够有效限制恶意代码的影响范围，为研究人员提供一个安全可控的实验空间，极大地便利了对恶意代码行为的研究与分析。

靶场的网络仿真模块配置了模拟的无线网络（Wi-Fi 802.11 接口），利用 mac80211_hwsim 内核模块创建虚拟无线接口，模拟真实的无线环境。这一设计为用户提供了实践攻击无人机无线网络的操作平台。例如，用户可以通过该虚拟接口捕获 Beacon 帧来识别目标网络。

（2）模拟层

模拟层以机器人操作系统（robot operating system, ROS）作为开发框架。ROS 集成了中间件、工具库和生态系统，旨在通过节点之间的通信实现机器人或无人机功能的模块化开发^[49]。本文借助 ArduPilot SITL 与 Gazebo 的深度集成，实现了对无人机、地面站、飞控逻辑和通信链路的高精度仿真。这一技术栈不仅为安全研究人员提供了可交互的攻击面，还通过模块化设计实现了对真实无人机系统的虚拟化部署与漏洞暴露。其在靶场中的核心功能体现在以下 3 个关键维度。

1) 攻击面虚拟化：模拟层将无人机系统的关键组件（如飞控、机载计算机、地面站）抽象为可独立操控的数字实体，通过注入已知漏洞和脆弱配置，构建了一个安全可控的攻击实验环境。这一设计使研究人员能够在不接触实际飞行器的情况下深入研究无人机系统的安全边界。

2) 行为一致性保证：通过 SITL 技术，模拟层实现了与真实 ArduPilot 固件的行为一致性（包括传感器数据处理逻辑、控制算法响应模式和通信协议实现细节）。这种一致性确保了在模拟环境中发现的漏洞和攻击方法具有实际应用价值，能够有效映射到物理无人机系统中。

3) 场景可扩展性：基于 Docker 的容器化架构赋予了模拟层极高的灵活性和可扩展性。研究人员可以根据需求快速部署不同型号的无人机系统、配置多样化的网络环境，甚至构建复杂的多

机协同场景，为高级攻击技术的研究与验证提供了理想的实验平台。

（3）通信层

通信层为各组件之间的有效协作提供了保障。通过飞行控制链路、仿真同步链路和 ROS 话题链路，飞控、机载计算机、地面站和仿真模块之间能够实时地传输控制指令与状态反馈信息，实现信息的共享和同步。

地面站通过飞行控制链路将起飞、降落、转向等指令经由机载计算机发送给飞控，飞控则实时反馈无人机的姿态、速度等信息。仿真同步链路为仿真模块与飞控、机载计算机之间的数据一致性提供了保障，让虚拟环境中的无人机状态与实际控制逻辑紧密同步。ROS 话题链路为各组件提供了一种灵活的发布和订阅机制，使得不同组件可以根据自身需求发布或订阅特定的数据主题，实现高效的数据共享。

在本文所述的无人机安全靶场中，通信层的核心价值是对无人机特有的通信协议进行模拟。该层不仅为安全测试提供了必要的交互环境，还支持通过配置通信协议模拟各种安全攻击场景。这有助于安全研究人员挖掘各种协议的安全漏洞，测试其安全性能。

（4）应用层

应用层具有攻防测试与评估、数据采集及靶场管理与监控方面的核心技术及功能，是本文构建一个全面、高效且安全的无人机模拟测试环境的落脚点。

攻防测试与评估模块采用模块化设计，支持不同的攻防测试工具的灵活开发与轻松集成，便于在靶场环境中开展实验。该模块具有良好的开放性和可扩展性，研究人员可根据需求定制并引入各种类型的攻击（涵盖从基础的 DoS 攻击到复杂的协议篡改等攻击）测试工具。每个攻击测试工具既可独立运行，又能与其他模块（如防护测试模块、仿真模块等）无缝对接，确保测试过程中数据的准确记录与模块间的高效联动。这种灵活的设计使靶场能够快速满足不同的测试需求，提升实验的多样性和覆盖面，有效支持无人机安全研究中的攻防验证。

在数据采集方面，靶场可以捕获并记录多种

攻击场景下的关键数据，形成丰富的攻击样本库。利用这些数据深入分析攻击的原理、过程和影响，有助于挖掘无人机系统中潜藏的安全漏洞。采集的无人机系统运行数据和攻击数据可以用于验证安全防护机制的有效性。通过在模拟攻击场景下观察系统的响应和数据变化，评估攻击和安全防护效果。

靶场管理与监控模块为用户提供了一个简单易用的网页控制台，支持便捷地触发攻击场景和控制无人机的飞行状态，显著提升测试效率。该模块具备实时监控能力，能够动态跟踪无人机的飞行状态及网络通信情况，一旦发现异常，能够配合内置的入侵检测系统及时发出预警，并支持快速部署安全加固方案。此外，靶场还集成了多版本软件与协议漏洞库，预存主流无人机的历史固件、软件版本及通信协议（包含存在已知漏洞的未修补版本），支持直接加载具有安全缺陷的旧版软件与协议，有效解决了厂商版本更新导致的漏洞验证失效问题，同时为研究不同协议版本的安全特性提供了标准化的环境支撑，方便研究人员全面复现历史攻击场景并开展对比分析。

(5) 智能调度层

智能调度层作为靶场的智能化中枢，依托人工智能技术实现测试流程的自动化与交互方式的便捷化，旨在降低安全测试的技术门槛，提升攻防场景验证的效率。该层以大语言模型的应用程序接口（application program interface, API）和智能体（Agent）为核心技术支撑，通过与应用层的标准化接口对接，形成“人机交互—方案生成—任务执行”的智能闭环，其 workflow 设计如图 3 所示。智能调度层的核心功能如下。

1) 自然语言交互接口：支持用户以自然语言下达操作指令。通过大语言模型对自然语言进行语义解析与任务映射，将任务自动转化为靶场可执行的操作序列（如调用应用层的攻防测试模块、配置模拟层的无人机参数），大幅降低非专业用户的使用门槛。

2) 智能方案生成：基于靶场实时采集的系统状态（如无人机型号、飞控固件版本、通信协议类型）信息，结合内置的无人机安全知识库（涵盖典型攻击手段、漏洞特征和防护策略），自动生成针对性的渗透测试路径和安全加固建议。

3) Agent 辅助执行：智能体模块将生成的测试方案拆解为原子任务，通过调用应用层的靶场管理接口，驱动各底层模块协同执行，并实时监控任务进度与执行结果，提升攻防测试的自动化水平。

该层通过模块化设计与标准化接口，既保留了对现有架构的兼容性，又通过智能化手段解决了传统靶场操作复杂、依赖人工经验的问题，尤其适用于教学场景和小型研究团队的安全测试场景。

1.2 无人机系统安全靶场关键技术模块设计

本文设计的无人机安全靶场通过有机整合飞控模块、机载计算机、地面站（QGC）、仿真模块（Gazebo）、攻击测试模块、防护测试模块和安全攻防智能体，构建了一个完整的测试系统，如图 4 所示。

靶场架构采用“模块化可扩展”设计理念，每个模块都有独立的核心功能，并通过标准化接口与其他模块实现高效协同工作。具体而言，飞控模块与机载计算机通过串行通信进行数据交换，既保障了飞行控制逻辑的实时反馈，又支持机载计算机完成辅助任务处理。仿真模块提供高保真

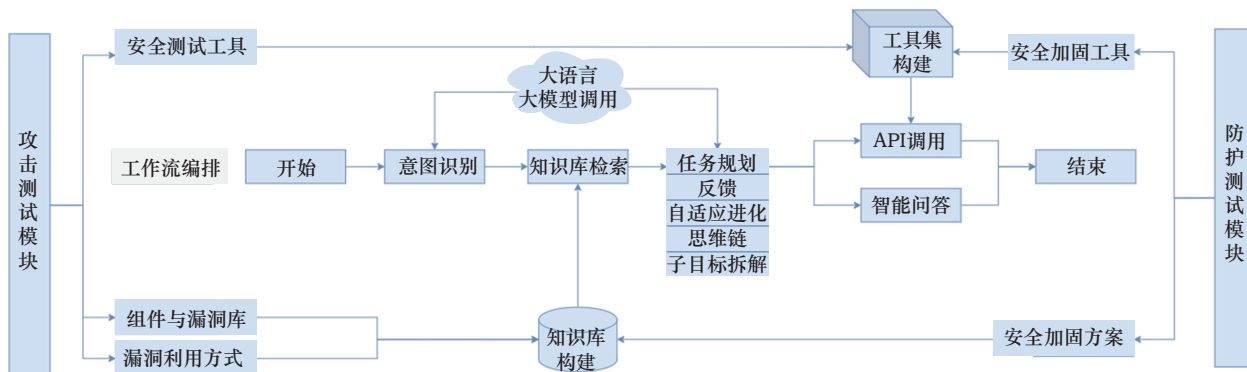


图3 智能调度层 workflow 设计

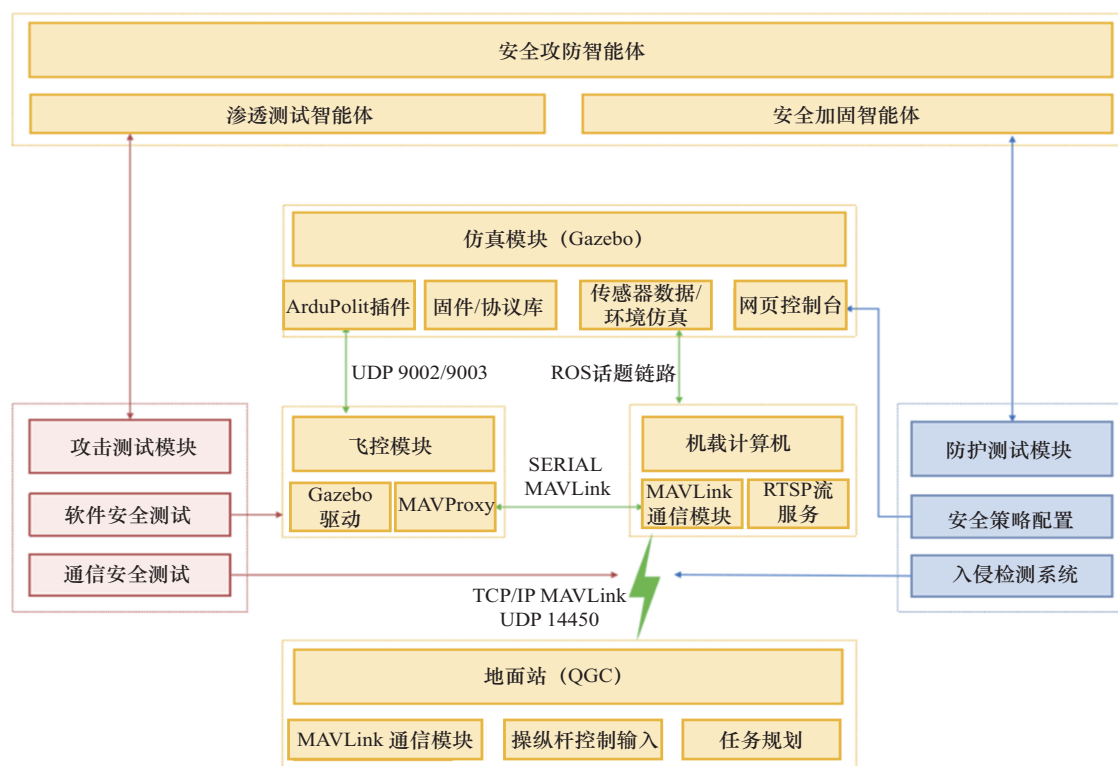


图4 无人机系统安全靶场模块架构与协同机制示意

虚拟环境，通过SITL技术与飞控系统、机载计算机保持实时数据同步，确保仿真环境中的无人机行为与物理系统保持一致。仿真模块不仅模拟飞行物理特性，还提供实时状态监控功能，便于研究者对攻击场景进行实时调整和验证。通信层通过飞行控制链路、仿真同步链路和ROS话题链路，保障无人机与地面站之间的数据传输与状态同步，使所有组件能够在统一协调的框架内高效运行。

在此基础上，本文设计了攻击测试模块、防护测试模块和安全攻防智能体三大模块。它们不仅是靶场的核心组成部分，也是提升系统整体测试深度和效能的关键所在。

（1）攻击测试模块

攻击测试模块是基于安全靶场开发的一个相对独立且具备复用性的组件。该模块将已完成的安全实验代码进行整合与封装，以便对无人机系统开展多样化的攻击测试。其模块化设计提高了代码的可维护性与可扩展性，为无人机系统安全研究与实验提供了有力的支撑。

1) 模拟攻击场景：在仿真环境中，模块通过复现真实协议格式、校验逻辑及飞控响应机制，

确保攻击过程（如伪造飞行终止指令）的真实性。靶场提供了多种攻击场景，包括侦察、协议篡改、DoS、注入、数据提取和固件等攻击场景。研究人员通过调用封装好的代码接口，即可快速启动各类攻击测试，避免了重复编写复杂攻击代码，有效提高了测试效率。丰富的攻击场景为研究人员提供了多维度的研究视角，有助于系统性地分析与挖掘无人机系统的安全漏洞。

2) 集成实验逻辑：攻击测试模块将安全实验步骤与操作逻辑进行集成，研究人员只需按照模块提供的接口进行操作，即可完成整个攻击测试流程。以MAVLink命令注入攻击为例，模块会在智能调度层的辅助下自动执行相关的命令，并记录攻击过程和结果，为后续分析提供数据支持。

3) 攻击评估框架：在无人机安全靶场的攻击评估框架中，针对多样化的攻击场景设计了一套量化评估体系。每次攻击执行后，系统通过实时监控无人机的响应状态，收集飞行日志、控制命令、传感器数据等关键数据。这些数据会被传输至智能体，智能体依据预设的规则和算法对数据进行处理，从中提取攻击特征，并生成如表2所

示的攻击评估量化指标。通过这一机制，靶场能够实现对各类攻击的系统化、定量化评估，为优化安全防护策略提供科学依据。

(2) 防护测试模块

安全加固方案同样可以划分为预防型和检测型两大类。预防型方案的研究主要聚焦于加密与认证技术。加密技术通过保护通信内容的机密性，防止数据在传输过程中被窃取或篡改^[50]；认证通常需要考虑无人机的计算资源限制，研究重点在于如何实现高效、低开销的身份验证机制^[51]；检测型方案以入侵检测系统为代表，通过实时监控和分析无人机系统的行为，及时发现潜在的攻击行为。由于针对硬件和软件的攻击通常具有其特殊性，通常需要部署专门的入侵检测系统以应对相应的安全威胁^[28]。这些防护策略的综合应用为无人机系统提供了多层次的安全保障，有效提升了无人机在恶劣环境中的生存能力和任务执行的可靠性。

本文设计的防护测试模块融合了安全协议的集成与动态调整、入侵检测系统，并采用了一些经典指标来构建安全防护评估框架。

1) 安全协议的集成与动态调整：本模块将安全协议融入靶场的通信机制中，用户可以通过网页控制台灵活配置安全策略。在无人机系统的仿真过程中，若暴露潜在的安全漏洞或出现异常状况，可以依据实际情况调整仿真参数（如更换安全协议、开启或关闭端口等），从而修补系统中潜藏的漏洞，增强系统的抗攻击能力。

2) 入侵检测系统：该模块集成了一个基于单类分类器的入侵检测系统，利用无人机正常飞行时的传感器数据（如GPS经纬度、加速度计数值

等）训练模型学习“正常行为模式”。具体流程如下：首先采集无人机无攻击状态下的飞行日志，通过数据清洗去除无效值，并按传感器类型进行聚类（如将GPS数据单独分组），随后运用主成分分析（principal component analysis, PCA）对每组数据进行降维，保留关键特征以降低计算复杂度；接着使用单类支持向量机、自编码器神经网络或局部离群因子（local outlier factor, LOF）等单类分类器进行训练。系统可以实时监测无人机传感器数据流，通过对比当前数据与训练得到的正常模型分布，识别出偏离正常模式的潜在攻击（如GPS欺骗导致的位置异常漂移），并触发警报。

3) 安全防护评估框架：安全防护评估框架通过模拟多种攻击场景来测试防护系统的有效性。评估核心包括系统的检测能力、误报率、漏报率和响应时间。为精准量化防护系统的性能，本文引入了混淆矩阵（入侵检测系统中常用的评估工具），用来评估防护系统在不同攻击场景下的表现。通过混淆矩阵可以计算出真正例（True Positive, TP）、假正例（False Positive, FP）、真负例（True Negative, TN）和假负例（False Negative, FN）等指标值，然后通过这些值推算出表3所示的指标值。所有防护评估数据会被实时收集并交给智能体处理，智能体分析防护策略的响应情况，量化评估防护系统在各类攻击下的表现，为防护策略的优化提供数据支持。

(3) 安全攻防智能体

安全攻防智能体是靶场智能化能力的核心载体，整合了强化学习、知识图谱与自动化决策技术。安全攻防智能体可以分为渗透测试智能体和安全加固智能体。

表2 攻击评估量化指标

指标	描述	计算方法
攻击成功率	攻击能够突破防护机制，成功控制或影响无人机系统的比例	攻击成功次数/总攻击次数
攻击影响程度	攻击对系统功能的影响，具体包括飞行中断、控制失效或数据丢失等	通过飞行任务完成度、系统功能恢复时间、飞行控制稳定性等评估影响程度
响应时间	系统从攻击发生到开始采取防护措施的时间	从攻击开始到防护系统启动的时间
攻击复杂度	执行攻击所需的步骤与攻击手段的复杂度，考虑是否涉及多种攻击手段的联合	攻击步骤数量、攻击方式（单一攻击与联合攻击）的对比
系统稳定性下降幅度	攻击发生后，系统稳定性下降的幅度，反映系统在攻击过程中是否丧失控制权	通过飞控系统的稳定性（如位置偏差、断连）测量变化程度

表3 攻击评估量化指标

指标	描述	计算方法
精确率	防护系统正确检测到攻击的能力	$TP / (TP + FP)$
误报率	防护系统错误地将正常行为判定为攻击的比例	$FP / (FP + TN)$
漏报率	防护系统未能检测到实际攻击的比例	$FN / (FN + TP)$
F1 分数	综合考虑精确率与召回率的指标, 衡量防护系统的综合性能	$2 \times (\text{精确率} \times \text{召回率}) / (\text{精确率} + \text{召回率})$
召回率	防护系统识别出攻击的能力	$TP / (TP + FN)$
特异性	防护系统正确识别正常行为的能力	$TN / (TN + FP)$
响应时间	防护系统从攻击检测到响应的的时间	从攻击开始到防护系统启动的时间 (单位为s)

渗透测试智能体以发现深层漏洞为目标, 设计为能够自主完成信息采集、智能规划、自动化执行与迭代优化的闭环系统。其工作流程如下: 首先, 通过应用层接口获取无人机型号、固件版本等系统信息; 然后, 依托通用大模型API的语义理解与推理能力, 结合内置漏洞特征库与强化学习算法生成最优渗透路径(例如, 针对通信协议, 可以通过大模型分析协议逻辑, 自动定位指令注入风险点并规划测试步骤); 随后, 将攻击步骤拆解为原子任务, 驱动攻击测试模块执行操作并采集响应数据; 最后, 根据执行反馈动态调整策略, 高效复现复杂攻击链, 显著降低对人工经验的依赖。

本研究构建的安全加固智能体, 是与防护测试模块深度联动的动态防御决策单元, 其核心依托通用大模型API实现策略生成与优化。该类智能体实时接收入侵检测告警, 结合攻击日志识别威胁类型并评估影响范围, 并基于防护知识库生成针对性加固方案。同时, 通过仿真环境模拟验证加固效果, 利用反馈结果迭代优化策略参数(如调整检测阈值), 将静态防护规则转化为动态防御能力, 提升系统应对未知攻击的韧性。

渗透测试智能体和安全加固智能体两者协同形成“以攻促防”的智能循环。渗透测试智能体主动暴露系统脆弱性, 安全加固智能体据此生成防御方案, 大幅提升靶场在漏洞挖掘与防护验证中的自动化水平和测试深度。

靶场的模块化设计与协同机制为无人机仿真构建了高真实度的环境和行为响应体系, 为在虚拟空间中开展多样化的安全测试与研究提供了坚实支撑。在此基础上, 开发攻防测试模块模拟各种复杂的攻击情景, 助力研究者便捷地获取无人

机遭受攻击时的各项数据。通过对这些数据的深度分析, 研究者得以探索并验证有效的防护方法, 持续迭代优化安全策略。

2 无人机系统安全靶场攻防实验验证

基于前文提出的靶场架构, 本文设计了涵盖Wi-Fi发现、地址解析协议(address resolution protocol, ARP)攻击辅助密码破解、典型MAV-Link指令欺骗的综合攻击实验, 从而系统性地分析无人机面临的安全威胁。攻防流程时序图如图5所示, 靶场环境通过精确控制实验变量(如通信加密状态、协议版本、硬件配置等), 构建了标准化的测试场景, 并通过靶场监控获取无人机飞行数据, 进而完成对攻击行为的检测。

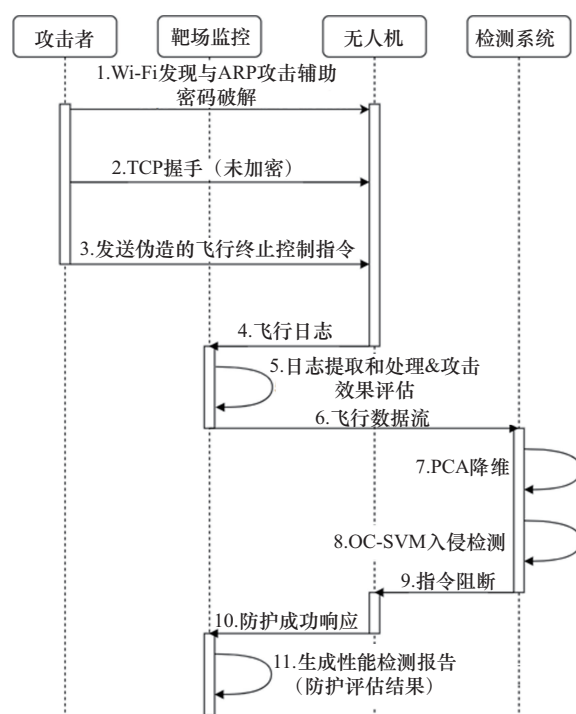


图5 攻防流程时序图

2.1 综合攻击场景构建和效果评估

(1) Wi-Fi发现与ARP攻击辅助密码破解

攻击者首先需在网络环境中发现目标无人机。通过使用 airodump-ng 工具扫描周边的 Wi-Fi 网络, 可以获取无人机所使用的 Wi-Fi 网络的相关信息。针对采用 Wi-Fi 保护接入 (Wi-Fi protected access, WPA) 和 WPA2 加密的网络, 攻击者可以结合 ARP 攻击和 aireplay-ng、aircrack-ng 工具实施密码破解。ARP 攻击通过发送大量的 ARP 请求和响应数据包, 迫使接入点重新发送握手包, 从而增加有效握手包的捕获概率, 加速密码破解进程。

(2) 主机端口发现

成功接入目标无人机的 Wi-Fi 网络后, 攻击者需要了解目标无人机的开放端口和运行的服务。使用端口扫描工具 Nmap 对无人机的 IP 地址进行扫描, 可以发现其开放的端口和对应的服务。需要特别关注 MAVLink 协议所使用的端口 (如 5760、14550 等), 确认端口后, 攻击者便可与无人机建立非法通信连接。

(3) 指令欺骗攻击

无人机飞控系统的关键指令欺骗漏洞构成了严重的安全威胁。本文针对 MAVLink 协议中的飞行终止指令设计了一个典型的欺骗攻击场景。攻击者通过未加密的传输控制协议 (transmission control protocol, TCP) 通信链路, 向运行 PX4 或 ArduPilot 固件的无人机注入恶意指令, 成功诱使无人机执行非预期的紧急终止动作。

(4) 攻击效果评估

该攻击的核心在于对协议语义的恶意利用, 其使用的指令格式完全符合协议规范, 虽然其触发条件与无人机实际飞行状态明显不符, 但飞控系统在接收到该指令后, 仍然会立即中断当前飞行任务, 执行紧急降落或悬停操作。通过实时监控系统的响应消息, 可以确认攻击是否成功执行。实验数据显示, 在未采取防护措施的情况下, 此类欺骗攻击的成功率超过 90%。攻击覆盖范围广、影响程度大, 可导致无人机直接失控。然而, 该攻击的隐蔽性较差, 在多种检测模型下的检出率均超过 80%。同时, 由于攻击并未完全

夺取无人机的控制权, 攻击的平均恢复时间在 1 min 以内。

2.2 AI辅助渗透测试

为验证靶场智能调度层的实际效能, 实验过程中同步融入了 AI 辅助攻击路径规划与自动化执行功能。用户通过自然语言向靶场下达“对当前靶场进行渗透测试”任务, 智能调度层的大语言模型 API 首先对该需求进行语义解析, 结合靶场实时采集的环境信息 (包括但不限于当前可以识别的 Wi-Fi 网络列表、已知无人机型号对应的固件特征), 自动生成结构化的渗透测试路径, 具体如图 6 所示: ①调用 Wi-Fi 扫描模块定位目标无人机; ②启动 ARP 攻击辅助密码破解模块获取网络访问权限; ③调用端口扫描工具确认 MAVLink 通信端口; ④调用指令构造模块生成符合协议规范的恶意飞行终止指令; ⑤通过 TCP 链路注入恶意指令并监控执行结果。

系统将该路径转化为靶场可以直接执行的操作序列, 如图 7 所示, 将“Wi-Fi 扫描”步骤映射为 airodump-ng 工具的参数配置, 将“端口扫描”步骤转化为 Nmap 的指令集, 再由智能体调用攻击测试模块的标准化接口依次执行。在执行过程中, 智能体实时回传各环节的状态信息 (包括握手包捕获进度、指令注入结果等关键信息) 至网页控制台, 实现全流程可视化监控。整个过程无须人工编写攻击脚本, 仅通过自然语言交互即可完成复杂攻击场景的自动化复现, 既验证了智能调度层“自然语言交互—方案生成—任务执行”闭环的有效性, 又凸显了靶场在降低安全测试技术门槛、提升攻击场景复现效率方面的实际价值。

2.3 基于单类支持向量机(OC-SVM)的欺骗攻击检测

(1) 数据处理与特征提取

无人机系统产生的 MAVLink 消息数据构成了检测模型的基础输入。本文采用 InfluxDB 时序数据库存储和检索飞行数据, 通过定义特定的消息类型及其关键特征字段 (pos_horiz_ratio、flags 等), 实现了高效的数据采集。为确保数据质量, 研究人员设计了完整的数据预处理流程。首先对原始数据进行标准化处理, 消除不同传感器的量

Agent Interaction

请结合当前靶场的无人机配置信息，给出渗透测试建议

Task Completed

- Duration: 57.99 seconds
- Total Input Tokens: 24515
- Final Result: 以下是针对靶场无人机配置的渗透测试建议 (中文):
 - Wi-Fi扫描:** 使用工具如 airodump-ng 识别目标无人机的Wi-Fi网络及连接设备。
 - ARP欺骗:** 部署 Ettercap 或 arpspoof 等工具, 通过ARP攻击获取网络访问权限。
 - 端口扫描:** 利用 Nmap 扫描无人机开放端口, 重点关注MAVLink协议端口 (如TCP 5760)。
 - 指令注入:** 通过 MAVProxy 或自定义脚本构造恶意MAVLink指令 (如飞行终止指令)。
 - 实时监控:** 通过网页控制台实时监控攻击进度, 验证指令注入效果。

此建议基于AI驱动自动化框架, 确保全面测试无人机的安全漏洞。

Status: Success

图6 智能体交互图



图7 智能体思考和任务执行图

纲差异; 随后应用PCA进行降维, 保留85%的方差信息, 在降低计算复杂度的同时有效捕捉数据的主要特征模式。值得注意的是, 借助时间戳标注技术, 系统能够精确区分正常飞行时段和受攻击时段的数据, 为监督学习提供了可靠的标签基础。

(2) 模型构建与优化

本文采用OC-SVM作为核心检测算法。OC-SVM通过构建一个超球体来界定正常数据的分布范围。它以高斯核函数为基础, 借助超参数 ν

和 γ 来优化该超球体的边界。在训练阶段, OC-SVM利用正常飞行日志数据确定正常数据在特征空间中的聚集区域, 让尽可能多的正常数据落在这个超球体内。在实时监控时, 对于接收到的传感器数据, 计算其在特征空间中的位置。若该数据点落在超球体之外, 表明其偏离了正常数据的分布范围, 则判定该数据为异常攻击信号。这种判定方式基于OC-SVM对正常数据分布的学习和界定, 能够有效地识别出与正常模式不符的

潜在攻击。其优势在于仅需正常飞行数据即可建立检测模型，符合实际应用中异常样本稀缺的特点。模型通过径向基函数（RBF）将数据映射到高维空间，构建最优分离超平面。

在参数优化阶段， ν 控制着支持向量的数量及误报率， γ 为RBF的参数（影响决策边界的复杂度），二者均为无量纲的超参数。在实际应用中，合适的 ν 和 γ 组合能显著提升模型的异常检测性能。该函数通过网格搜索的方式，在指定的取值范围内系统地尝试不同的 ν 和 γ 组合。具体而言， ν 在 1×10^{-5} 到 1×10^{-1} 之间均匀取 n 个值， γ 在 1×10^{-6} 到 1×10^{-3} 之间均匀取 n 个值。对于每一种 ν 和 γ 的组合，函数会创建一个OC-SVM分类器实例，使用训练数据 X 对其进行训练，然后对训练数据进行预测，计算预测为异常样本的比例 p ，并求出 p 与当前 ν 值之间的绝对差异。通过不断比较这个差异值，找到差异最小的组合，即为最优超参数组合。与传统的离散点测试方法不同，网格搜索系统地覆盖了超参数空间，能够更全面地找到最优组合，显著提高了模型的检测性能和搜索效率。图8中的红色标记（X）即为最优的超参数组合，经过网格搜索，当 $\nu=0.021\ 1$ 、 $\gamma=0.000\ 3$ ，即 $\log_{10}\nu=-1.675\ 7$ 、 $\log_{10}\gamma=-3.522\ 9$ 时，模型在检测准确率上表现最佳。

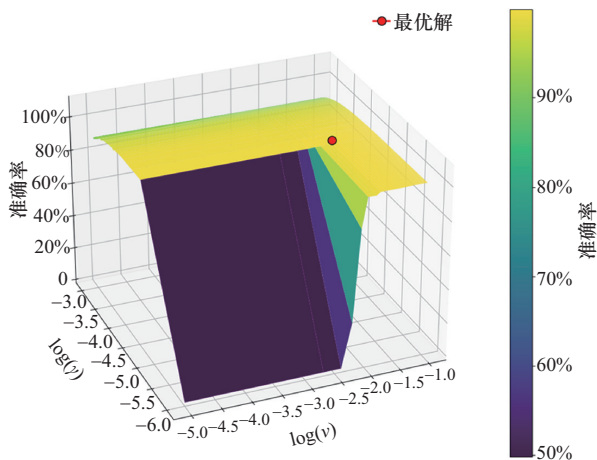


图8 单类支持向量机超参数搜索结果可视化

（3）检测流程与性能对比分析

本文选取LOF方法^[52]与OC-SVM进行对比研究。LOF是一种基于密度的异常检测方法，通过计算数据点相对于其邻域的局部密度偏差来识

别异常。其核心优势在于能够发现非线性分布的局部异常点，但对训练数据中正常样本的分布密度和质量有较高的要求。

本文使用两种方法分别对数据注入、GPS欺骗两种单一攻击场景，以及第2.1节所述的综合攻击场景进行检测，检测流程采用标准的两阶段处理。在离线训练阶段，OC-SVM方法仅需正常飞行数据即可建模，利用核技巧将数据映射到高维空间后建立封闭的决策边界。该过程通过5折交叉验证优化惩罚系数 C 和核参数 γ ，确保模型的泛化能力。而LOF方法则需要同时在训练集中加入5%~10%的异常样本，通过调整邻域参数 k 和污染系数来优化密度估计。在线检测阶段，实时飞行数据经标准化处理后输入模型。

实验结果见表4，从中可以看出，OC-SVM的关键性能指标在多种攻击场景下均显著优于LOF。在飞行终止欺骗攻击检测场景中，OC-SVM达到93.8%的检测精确率和89%的正常模式召回率，平均响应时间为 (0.15 ± 0.02) s，展现出优异的稳定性和可靠性。而LOF虽然在异常检出率上达到100%，但正常样本的误报率达29.8%，且性能表现对训练参数设置更加敏感。

分析上述差异可能源于算法本质特性：OC-SVM的全局优化策略使其决策边界更加明确，而LOF基于局部密度比较的机制虽然能识别复杂异常，但容易受到数据分布波动的影响。此外，单一攻击场景的检测精确率高于综合攻击场景的检测精确率，这是因为复杂攻击会影响更多的数据维度，导致检测精度下降。这一结果也从侧面印证了靶场对于综合攻击场景模拟的有效性。

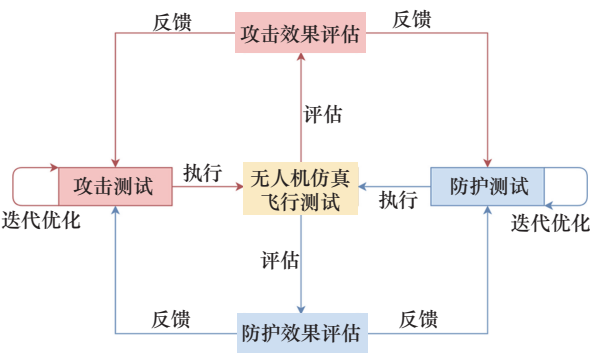
（4）攻防闭环验证

本文构建的无人机安全靶场为指令欺骗综合攻击场景的异常检测提供了完整的验证闭环，其作用体现在3个方面。首先，靶场环境通过精确复现真实飞行场景（包括GPS信号、控制指令等关键要素），确保攻击实验既具有高度真实性又避免对实际系统造成危害。在飞行终止欺骗攻击案例中，靶场成功模拟了从攻击注入、异常检测到系统恢复的全过程，验证了OC-SVM算法在实际场景中的有效性。其次，靶场的数据采集系统实现了高精度的多源数据（包括MAVLink通信日

表 4 检测结果分类报告

攻击场景	模型	评估指标	异常类（-1）	正常类（1）	宏平均	加权平均
综合攻击场景	OC-SVM	精确率	72.2%	100%	86.1%	93.8%
		召回率	100%	89.0%	94.5%	91.4%
		F1 分数	83.9%	94.2%	89.0%	91.9%
	LOF	精确率	49.0%	100%	74.5%	88.7%
		召回率	100%	70.2%	85.1%	76.8%
		F1 分数	65.8%	82.5%	74.1%	78.8%
数据注入攻击	OC-SVM	精确率	78.0%	100%	89.0%	95.0%
		召回率	100%	88.0%	94.0%	92.0%
		F1 分数	87.5%	93.9%	90.7%	93.5%
	LOF	精确率	53.0%	100%	76.5%	88.0%
		召回率	100%	71.0%	85.5%	77.0%
		F1 分数	69.3%	83.1%	76.2%	82.5%
GPS 欺骗	OC-SVM	精确率	84.4%	98.8%	91.6%	95.0%
		召回率	95.0%	85.0%	90.0%	90.0%
		F1 分数	89.5%	91.7%	90.6%	92.5%
	LOF	精确率	71.2%	98.0%	84.6%	92.0%
		召回率	92.0%	75.0%	83.5%	86.0%
		F1 分数	80.8%	86.0%	83.4%	89.0%

志、传感器原始数据及检测模型的中间计算结果)的同步记录,为算法优化提供了详实的分析依据。实验数据显示,通过靶场收集的超过 200 次攻击测试样本,使 OC-SVM 模型的检测精确率从 85.6% 提高至 93.8%。最后,靶场支持快速迭代的攻防对抗验证,如图 9 所示,可以根据检测结果动态调整攻击参数(如指令注入间隔、信号强度等),同时优化模型的决策阈值和特征选择策略,形成“攻击—检测—改进”的良性循环。这种闭环验证机制不仅加速了安全技术的成熟,也为制定无人机系统防护标准提供了科学依据。



3 未来展望

本文提出的 AI 辅助无人机系统安全靶场已实现单机多场景攻防模拟、闭环验证及智能化测试核心功能。然而,随着无人机技术向集群化、智能化演进,且与新兴技术深度融合,其安全测试需求持续升级。未来研究可以将靶场作为核心载体,围绕靶场功能拓展、复杂场景模拟、AI 辅助能力强化三大主线,系统性突破现有研究瓶颈,推动无人机安全测试技术向智能化、体系化、高保真方向演进。

3.1 靶场安全测试功能的多维拓展

现有靶场聚焦网络通信与软件层安全测试,未来可以面向无人机系统的感知、决策、隐私保护及新兴技术等层面的安全问题拓展测试维度与深度。在感知安全方面,可以针对无人机传感器数据的时序性、多模态特性,构建数据投毒与对抗样本攻击测试模块^[53]。在隐私保护测试方面,可以强化场景特异性,构建侧信道攻击、脱敏数据重建等隐私泄露验证环境,研发并验证基于同态加密、差分隐私的轻量化隐私保护方案,平衡

隐私安全与系统性能。此外,随着无人机系统逐步融入新兴技术,模拟区块链节点劫持^[54]、数字孪生镜像篡改、大模型提示词攻击等新型威胁,验证无人机系统与新兴技术融合后的安全适配性也将成为非常有价值的研究方向。

3.2 复杂无人机系统的高保真模拟

当前靶场测试多局限于单机理想环境,未来可以拓展无人机集群与复杂场景的模拟能力。在集群模拟方面,可以增强靶场的多节点协同仿真能力,构建支持多协议融合的集群通信环境,模拟路由欺骗、协同指令伪造等集群特异性攻击,以及DDoS攻击的集群效应,验证集群通信协议的抗攻击性能与自愈机制。在复杂场景模拟方面,可以集成高保真物理环境仿真模块,融合气流扰动、电磁干扰、城市建筑群遮挡等异构环境因素,模拟环境与安全威胁的耦合攻击效果,测试无人机在多目标冲突、动态拓扑变化场景下的安全决策能力。此外,还可以探索类似“无人机—地面机器人—卫星”的跨域协同系统模拟,以验证跨域通信时延、异构节点权限管理等潜在的安全风险,实现从单机测试向集群化、跨域化测试的跃升。

3.3 AI辅助能力强化

AI辅助能力是提升无人机安全靶场测试效率、拓展测试深度的核心支撑,随着社会对人工智能决策过程的透明度和可理解性需求的提升,未来的靶场将在可解释性基础上强化自动化迭代与自适应威胁识别能力。在检测结果解释层面,通过可解释性相关算法量化传感器特征对检测结果的贡献度^[55],将复杂模型的决策边界转化为人类可理解的规则集,追溯异常行为的演化路径及其对系统的影响链路,从而提升安全测试的可信度。

依托强化学习与智能体技术的发展,未来靶场将实现攻防策略的动态迭代与自主优化。在攻击侧,智能体通过分析靶场监控数据,自动调整攻击参数,生成针对性的攻击路径;在防护侧,基于攻击反馈数据动态调整安全策略。通过这种方式,可以在无须人工干预的前提下提升靶场对复杂攻击场景的覆盖度与防护验证精度。

4 结束语

本文聚焦无人机系统安全领域,为突破当前无人机安全研究中使用仿真测试平台面临的威胁分析碎片化、生成的实验数据集质量不高、攻防闭环验证深度欠缺三重瓶颈,提出了一套无人机攻防闭环验证实验框架,设计了一个新型AI辅助无人机系统安全靶场。该靶场的核心架构基于Docker容器化技术,通过整合SITL仿真、Gazebo物理引擎、MAVLink通信协议,能够支持从侦察到固件攻击的多元攻击场景模拟。靶场通过标准化数据采集接口记录飞行日志与通信数据,结合PCA降维与单类分类器实现异常检测;同时,还集成了通用大模型API调用能力,可以借助AI辅助完成渗透测试、提供安全加固方案建议等任务。在攻防实验中,验证了靶场对综合攻击场景的全流程复现能力及AI辅助渗透测试的效果,所采集的数据为防护策略优化提供了量化依据。在飞行终止欺骗综合攻击实验中,检测精确率从初始的85.6%提升至93.8%,有效降低了漏检与误报风险。经对比,优化后的模型在多种攻击场景下的检测精确率均优于经典LOF方法构建的模型,该结果也从侧面印证了靶场在综合攻击场景模拟上的有效性。相较于传统测试环境,该靶场不仅在攻防数据采集的效率与质量上展现出显著优势,还通过量化验证为防护策略优化提供了可靠支撑,为无人机系统漏洞挖掘、数据采集和防护技术迭代提供了高效的实验平台。未来,随着无人机向集群化、智能化演进,并与新兴技术深度融合,安全测试需求将持续升级。本文提出的AI辅助无人机系统安全靶场,需重点拓展集群与复杂场景模拟能力,拓展数据投毒、对抗样本等新兴安全测试功能,同时融入可解释性AI强化辅助能力,推动安全测试向体系化、高保真方向演进,为无人机在关键领域的规模化应用提供更加坚实的安全保障。

参考文献:

- [1] 陈广承,柏艺琴.民航局《轻小无人机运行规定》解读[J].中国应急管理,2016(1):40-41.
Chen G C, Bai Y Q. Interpretation of civil aviation administration's

- regulations on the operation of light and small unmanned aerial vehicles[J]. China Emergency Management, 2016(1): 40-41.
- [2] 张军, 陈磊, 高智杰, 等. 低空无人机技术研究现状与展望[J]. 中国工程科学, 2025, 27(2): 73-85.
- Zhang J, Chen L, Gao Z J, et al. Low-altitude unmanned aerial vehicle technology: current status and prospects[J]. Strategic Study of Chinese Academy of Engineering, 2025, 27(2): 73-85.
- [3] Huang X. The small-drone revolution is coming: scientists need to ensure it will be safe[J]. Nature, 2025, 637(8044): 29-30.
- [4] Florido-Benítez L. The types of hackers and cyberattacks in the aviation industry[J]. Journal of Transportation Security, 2024, 17(1): 13.
- [5] Gomez-Thomas R. From corruption to combat: the militarization of organized crime in Mexico[D]. Waltham: Brandeis University, 2025.
- [6] Pratama D, Moon J, Ari Laksmo A M, et al. Behind the wings: the case of reverse engineering and drone hijacking in DJI enhanced Wi-Fi protocol[C]//Proceedings of the 2024 International Conference on Platform Technology and Service (PlatCon). Piscataway: IEEE Press, 2025: 127-132.
- [7] 蒋玉长, 蒋利兵, 黄凯. FL-IoV: 基于联邦学习的综合车联网入侵检测方法[J]. 网络与信息安全学报, 2025, 11(4): 127-140.
- Jiang Y C, Jiang L B, Huang K. FL-IoV: comprehensive intrusion detection method for Internet of vehicles based on federated learning[J]. Chinese Journal of Network and Information Security, 2025, 11(4): 127-140.
- [8] 章阳, 顾宏宇, 冯博豪, 等. 语义通信下基于强化学习的无人机通信容错协同控制[J]. 网络与信息安全学报, 2024, 10(2): 69-80.
- Zhang Y, Gu H Y, Feng B H, et al. Semantic communication aware reinforcement learning for communication fault-tolerant UAV collaborative control[J]. Chinese Journal of Network and Information Security, 2024, 10(2): 69-80.
- [9] Panda D K, Guo W S. Fragility impact of RL based advanced air mobility under gradient attacks and packet drop constraints[C]//Proceedings of the 2023 IEEE 98th Vehicular Technology Conference (VTC2023-Fall). Piscataway: IEEE Press, 2023: 1-7.
- [10] Duo B, Luo J S, Li Y L, et al. Joint trajectory and power optimization for securing UAV communications against active eavesdropping[J]. China Communications, 2021, 18(1): 88-99.
- [11] Huang K W, Wang H M. Combating the control signal spoofing attack in UAV systems[J]. IEEE Transactions on Vehicular Technology, 2018, 67(8): 7769-7773.
- [12] Rodday N M. Exploring security vulnerabilities of unmanned aerial vehicles[D]. Enschede: University of Twente, 2015.
- [13] Pandey G K, Gurjar D S, Nguyen H H, et al. Security threats and mitigation techniques in UAV communications: a comprehensive survey[J]. IEEE Access, 2022, 10: 112858-112897.
- [14] Omar T, Duran T, Al-Tarazi M, et al. SDR based replay attack for drone intervention[C]//Proceedings of the 2024 Wireless Telecommunications Symposium (WTS). Piscataway: IEEE Press, 2024: 1-5.
- [15] Lyu C Y, Zhan R J. Global analysis of active defense technologies for unmanned aerial vehicle[J]. IEEE Aerospace and Electronic Systems Magazine, 2022, 37(1): 6-31.
- [16] Wei X M, Ma J F, Sun C. A survey on security of unmanned aerial vehicle systems: attacks and countermeasures[J]. IEEE Internet of Things Journal, 2024, 11(21): 34826-34847.
- [17] Abdulrazak C. Cybersecurity threat analysis and attack simulations for unmanned aerial vehicle networks[J]. arXiv:2404.16842, 2024.
- [18] Kim Y, Cho K, Kim S. Challenges in dynamic analysis of drone firmware and its solutions[J]. IEEE Access, 2024, 12: 106593-106604.
- [19] Florido-Benítez L. Identifying and classifying cyberattacks on airports[J]. Cyber Security: A Peer-Reviewed Journal, 2024, 8(1): 63-79.
- [20] Cao Y L, Wang N F, Xiao C W, et al. Invisible for both camera and LiDAR: security of multi-sensor fusion based perception in autonomous driving under physical-world attacks[C]//Proceedings of the 2021 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE Press, 2021: 176-194.
- [21] Fu C H, Li S H, Yuan X N, et al. Ad2Attack: adaptive adversarial attack on real-time UAV tracking[C]//Proceedings of the 2022 International Conference on Robotics and Automation (ICRA). Piscataway: IEEE Press, 2022: 5893-5899.
- [22] 陈世康, 周冰, 曹宝, 等. 无人机安全通信协议研究综述[J]. 通信技术, 2024, 57(3): 213-221.
- Chen S K, Zhou B, Cao B, et al. Literature review of secure communication protocols for UAV[J]. Communications Technology, 2024, 57(3): 213-221.
- [23] 黄明义, 邹福泰, 周纸墨, 等. 基于知识图谱和污点传播的网络攻击检测方法[J]. 网络与信息安全学报, 2025, 11(1): 151-164.
- Huang M Y, Zou F T, Zhou Z M, et al. Network attack detection method based on knowledge graph and taint propagation[J]. Chinese Journal of Network and Information Security, 2025, 11(1): 151-164.
- [24] Whelan J, Sangarapillai T, Minawi O, et al. UAV attack dataset[J]. IEEE Dataport, 2020, 167(1): 1561-1573.
- [25] Whelan J, Sangarapillai T, Minawi O, et al. Novelty-based intrusion detection of sensor attacks on unmanned aerial vehicles[C]//Proceedings of the 16th ACM Symposium on QoS and Security for Wireless and Mobile Networks. New York: ACM, 2020: 23-28.
- [26] 余丁辰, 王威, 王加琪, 等. 基于收缩自编码器的无人机GPS欺骗攻击协同检测方法[J]. 信号处理, 2024, 40(4): 706-718.
- She D C, Wang W, Wang J Q, et al. Collaborative detection method of UAV GPS spoofing attack based on shrink autoencoder[J]. Journal of Signal Processing, 2024, 40(4): 706-718.
- [27] 文霞. 小型无人机抵抗GPS欺骗攻击的SVM-CNN模型研究[J]. 计算机技术与发展, 2025, 35(8): 166-172.
- Wen X. Research on SVM-CNN models for small UAVs to resist GPS spoofing attacks[J]. Computer Technology and Development, 2025, 35(8): 166-172.
- [28] Wang S Q, Wang J, Su C H, et al. Intelligent detection algorithm against UAVs' GPS spoofing attack[C]//Proceedings of the 2020 IEEE 26th International Conference on Parallel and Distributed Systems (ICPADS). Piscataway: IEEE Press, 2021: 382-389.
- [29] 王路阳, 孙一宸, 于明鑫, 等. 基于TimeGAN-LSTM的无人机GPS欺骗干扰检测模型[J]. 电子测量与仪器学报, 2023, 37(6): 122-135.

- Wang L Y, Sun Y C, Yu M X, et al. UAV GPS spoofing detection model based on TimeGAN-LSTM[J]. *Journal of Electronic Measurement and Instrumentation*, 2023, 37(6): 122-135.
- [30] Samriya J K, Kumar M, Tiwari R. Energy-aware ACO-DNN optimization model for intrusion detection of unmanned aerial vehicle (UAVs)[J]. *Journal of Ambient Intelligence and Humanized Computing*, 2023, 14(8): 10947-10962.
- [31] Wu Y X, Yang L, Zhang L, et al. Intrusion detection for unmanned aerial vehicles security: a tiny machine learning model[J]. *IEEE Internet of Things Journal*, 2024, 11(12): 20970-20982.
- [32] Hassler S, Mughal U, Ismail M. Cyber-physical dataset for UAVs under normal operations and cyber-attacks[J]. *IEEE Dataport*, 2023, 10.
- [33] 赵长啸, 方玉麟, 汪克念. 基于 BiTCN 的无人机指挥控制链路 DoS 攻击检测方法[J]. *航空学报*, 2025, 47(1): 332048.
- Zhao C X, Fang Y L, Wang K N. BiTCN-based DoS attack detection method for UAV command and control link[J]. *Acta Aeronautica et Astronautica Sinica*, 2025, 47(1): 332048.
- [34] Hadi H J, Cao Y, Khan M K, et al. UAV-NIDD: a dynamic dataset for cybersecurity and intrusion detection in UAV networks[J]. *IEEE Transactions on Network Science and Engineering*, 2025, 12(4): 2739-2757.
- [35] Madaan R, Gyde N, Vemprala S, et al. AirSim drone racing lab[C]// *Proceedings of the Neurips 2019 competition and demonstration track*. PMLR, 2020: 177-191.
- [36] Quan Q, Dai X H, Wang S. Multicopter design and control practice: a series experiments based on MATLAB and Pixhawk[M]. Singapore: Springer Singapore, 2020: 18-19.
- [37] Schmitt M, Lukina A, Vacek L, et al. OpenUAV: a UAV testbed for the CPS and robotics community[C]// *Proceedings of the 2018 ACM/IEEE 9th International Conference on Cyber-Physical Systems (ICCPS)*. Piscataway: IEEE Press, 2018: 130-139.
- [38] Zhou Z H, Dai Z P, Huang L Y, et al. UavNetSim-v1: a Python-based simulation platform for UAV communication networks[C]// *Proceedings of the 2025 IEEE/CIC International Conference on Communications in China (ICCC)*. Piscataway: IEEE Press, 2025: 1-6.
- [39] Baidya S, Shaikh Z, Levorato M. FlyNetSim: an open source synchronized UAV network simulator based on NS-3 and ardupilot[C]// *Proceedings of the 21st ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems*. New York: ACM, 2018: 37-45.
- [40] Dai X H, Ke C X, Quan Q, et al. RFlySim: Automatic test platform for UAV autopilot systems with FPGA-based hardware-in-the-loop simulations[J]. *Aerospace Science and Technology*, 2021, 114: 106727.
- [41] Xiao K, Tan S C, Wang G H, et al. XTDrone: a customizable multi-rotor UAVs simulation platform[C]// *Proceedings of the 2020 4th International Conference on Robotics and Automation Sciences (ICRAS)*. Piscataway: IEEE Press, 2020: 55-61.
- [42] Devine T R, Cunningham D J, Hasselman T J K, et al. INDRA: a drone penetration testing platform for cybersecurity education[C]// *Foundations of Computer Science and Frontiers in Education: Computer Science and Computer Engineering*. Cham: Springer, 2025: 235-251.
- [43] 高健. 虚实结合的无人机靶场设计与实现[D]. 西安: 西安电子科技大学, 2022.
- Gao J. Design and implementation of UAV cyberRange co-mbining virtual and real[D]. Xi'an: Xidian University, 2022.
- [44] 邹星, 胡宁, 顾钊铨, 等. 网络靶场研究现状与展望[J]. *网络与信息安全学报*, 2024, 10(5): 1-22.
- Zou X, Hu N, Gu Z Q, et al. Cyber ranges: survey and perspective[J]. *Chinese Journal of Network and Information Security*, 2024, 10(5): 1-22.
- [45] 王佰玲, 刘红日, 张耀方, 等. 工业控制系统安全仿真关键技术研究综述[J]. *系统仿真学报*, 2021, 33(6): 1466-1488.
- Wang B L, Liu H R, Zhang Y F, et al. Review on key technologies of industrial control system security simulation[J]. *Journal of System Simulation*, 2021, 33(6): 1466-1488.
- [46] Davis J, Magrath S. A survey of cyber ranges and testbeds[J]. 2013: 1-38.
- [47] Ukwandu E, Ben-Farah M A, Hindy H, et al. A review of cyber-ranges and test-beds: current and future trends[J]. *Sensors*, 2020, 20(24): 7148.
- [48] Nikolaiev M, Novotarskyi M. Comparative review of drone simulators[J]. *Information, Computing and Intelligent Systems*, 2024(4): 79-98.
- [49] 白天翔, 王帅, 沈震, 等. 平行机器人与平行无人系统: 框架、结构、过程、平台及其应用[J]. *自动化学报*, 2017, 43(2): 161-175.
- Bai T X, Wang S, Shen Z, et al. Parallel robotics and parallel unmanned systems: framework, structure, process, platform and applications[J]. *Acta Automatica Sinica*, 2017, 43(2): 161-175.
- [50] Bagchi P, Maheshwari R, Bera B, et al. Public blockchain-envisioned security scheme using post quantum lattice-based aggregate signature for Internet of drones applications[J]. *IEEE Transactions on Vehicular Technology*, 2023, 72(8): 10393-10408.
- [51] Son S, Kwon D, Lee S, et al. Design of secure and lightweight authentication scheme for UAV-enabled intelligent transportation systems using blockchain and PUF[J]. *IEEE Access*, 2023, 11: 60240-60253.
- [52] Jalil-Hadi H, Cao Y, Li S F, et al. Real-time collaborative intrusion detection system in UAV networks using deep learning[J]. *IEEE Internet of Things Journal*, 2024, 11(20): 33371-33391.
- [53] 武阳, 刘靖. 面向图像分析领域的黑盒对抗攻击技术综述[J]. *计算机学报*, 2024, 47(5): 1138-1178.
- Wu Y, Liu J. A survey on black-box adversarial attack in image analysis[J]. *Chinese Journal of Computers*, 2024, 47(5): 1138-1178.
- [54] 王群, 李馥娟, 倪雪莉, 等. 域间路由安全增强及区块链技术的应用研究[J]. *计算机科学与探索*, 2024, 18(12): 3144-3174.
- Wang Q, Li F J, Ni X L, et al. Research on blockchain-based inter-domain routing security enhancement[J]. *Journal of Frontiers of Computer Science & Technology*, 2024, 18(12): 3144-3174.
- [55] 邢颖. 基于可解释性人工智能的软件工程技术方法综述[J]. *计算机科学*, 2023, 50(5): 3-11.
- Xing Y. Review of software engineering techniques and methods based on explainable artificial intelligence[J]. *Computer Science*, 2023, 50(5): 3-11.

[作者简介]



李宇佳（2001- ），男，湖南衡阳人，成都理工大学计算机与网络安全学院硕士生，主要研究方向为无人机系统安全。



王梓斌（1982- ），男，山东莱阳人，北京信息系统安全技术重点实验室高级工程师，主要研究方向为无线网络安全、无人机系统安全。



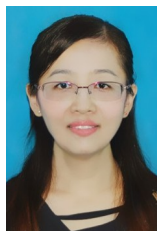
张辉（1983- ），男，山东蓬莱人，成都理工大学计算机与网络安全学院讲师，主要研究方向为网络安全、密码学。



周让（1987- ），男，重庆人，成都理工大学研究员，主要研究方向为密码学、访问控制安全及数据安全。



多滨（1982- ），男，河北衡水人，成都理工大学计算机与网络安全学院教授，主要研究方向为无人集群系统安全、无人集群智能组网与协同通信关键技术。



李冬芬（1979- ），女，青海海东人，成都理工大学教授，主要研究方向为信息安全、移动互联安全、量子密码通信等。