引用格式：代燕, 黄晶晶, 王宁, 等. 无人集群安全技术综述 [J]. 电子科技大学学报, 2025, 54(4): 507-520.
DAI Y, HUANG J J, WANG N, et al. Secure communication technologies for UAV swarm: A survey[J]. Journal of University of Electronic Science and Technology of China, 2025, 54(4): 507-520.

无人集群安全技术综述

代 燕[1]，黄晶晶[2,3*]，王 宁[4]，王晓东[1]，伍冲翀[5]，沈正华[5]

（1. 中国电子科技集团公司第二十九研究所，成都 610036；2. 中国电子技术标准化研究院，北京 100007；
3. 北京赛西科技发展有限责任公司，北京 100176；4. 重庆大学 计算机学院，重庆 400044；5. 国网重庆市电力公司信息通信分公司，重庆 401120）

摘要：无人集群是无人系统重要的应用方式和关键的技术发展方向，相较于单架无人机系统，无人集群在覆盖范围、作战效率和执行复杂任务能力等方面表现出卓越的技术优势。尽管如此，无人机集群仍然面临着严峻的信息安全问题，由于无人集群需要运行在复杂、动态的开放电磁环境，其协作、通信、认证、识别等环节都存在许多安全方面的威胁和挑战。该文旨在深入调研无人集群安全问题，分析无人集群潜在的安全威胁，综述现有的安全技术手段，探讨新兴的安全解决方案，在集群单点安全、网络安全、身份安全、通信安全以及数据安全等无人集群的关键环节进行广泛调研与深入分析，以期为无人集群相关研究与应用提供有力支撑。

关键词：无人集群；集群安全；信息安全；安全威胁
中图分类号：TP18 **文献标志码：**A DOI: 10.12178/1001-0548.2024055

Secure communication technologies for UAV swarm: A survey

DAI Yan[1], HUANG Jingjing[2,3*], WANG Ning[4], WANG Xiaodong[1], WU Chongchong[5], and SHEN Zhenghua[5]

(1. The 29th Research Institute of China Electronics Technology Group Corporation, Chengdu 610036, China;
2. China Electronics Standardization Institute, Beijing 100007, China;
3. Beijing CESI Technology Co., Ltd., Beijing 100176, China;
4. College of Computer Science, Chongqing University, Chongqing 400044, China;
5. Information and Telecommunication Branch, State Grid Chongqing Electric Power Company, Chongqing 401120, China)

Abstract: Unmanned swarm is an important application and key technological development direction of unmanned systems. Compared to single unmanned aerial systems, unmanned swarms demonstrate significant technological advantages in terms of coverage range, operational efficiency, and ability to execute complex tasks. However, unmanned swarm still faces severe information security issues. Due to the need to operate in complex and dynamic open electromagnetic environments, there are numerous potential security threats and challenges in the collaboration, communication, authentication, and identification processes of unmanned swarms. This article aims to conduct an in-depth survey on the security issues of unmanned swarms, analyze potential security threats, review existing security measures, and explore emerging security solutions. It will extensively investigate and analyze key aspects of unmanned swarm security, including individual security, network security, identity security, communication security, and data security. The goal of this article is to provide a strong support for related research and applications of unmanned swarms.

Key words: unmanned swarm; cluster security; information security; security threat

近年来，无人机的研究与应用得到了飞速发展，其使用量迅速攀升，预计无人机市场的复合年增长率将在 2027 年达到 17.99%。无人机可以无须驾驶员的直接操控，实现自主飞行或通过地面站进

收稿日期：2024−03−12
基金项目：国家重点研发计划（2021YFB3101601）；四川省自然科学基金（2024NSFSC1455）；中国博士后科学基金第 75 批面上资助项目（2024M754233）；重庆市自然科学基金面上项目（cstc2021jcyj-msxm0465）；重庆市留学人员回国创业创新支持计划（cx2021012）
作者简介：代燕，博士，主要从事人工智能、无人机集群和电磁智能对抗方面的研究。
*通信作者 E-mail: hjj187264726@126.com

行操控，因其易于部署、覆盖范围广、成本低等优势而在农业、军事、搜救、环境监测、智能交通、目标检测等多个领域得到广泛应用[1]。然而，单架无人机的资源和覆盖范围有限，难以满足大型、复杂任务的需求，因此许多应用场景倾向于采用多架无人机组成无人集群，以协同执行任务。与单架无人机相比，无人集群具有协同效应、高效性、灵活性、可扩展性和安全性等优势。随着技术的进步和应用场景的不断拓展，无人集群在军事、救援、勘测、监测等领域中的应用前景广阔。无人集群的主要优势之一是能够实现高度协同工作，通过良好的通信和协调，完成复杂的任务，如搜索和救援、勘测和监测等，集群中的无人系统可以相互配合，共享信息和资源，以优化任务的执行效率和准确性。无人集群能够同时执行多个任务，从而提高整体工作效率，相比单个无人系统，集群可以更快地完成任务，减少任务执行时间，此外，无人集群中的个体可以根据需要进行自主决策，适应任务变化，进一步提高工作效率。无人集群通常由多个相互独立的无人系统组成，因此可以更灵活地适应各种任务需求，当某个系统故障或任务需要更多资源时，其他系统可以接替并继续完成任务，这种灵活性使得无人集群在复杂和危险的环境中更具适应性和可靠性[2]。无人集群还可以根据任务需要进行灵活扩展。通过增加或减少集群中的无人系统数量，适应不同规模的任务需求，这种可扩展性使得无人集群能够应对各种任务规模和复杂度的变化。

尽管无人集群拥有非常显著的优势和潜力，当前无人集群在协作、通信、认证、识别等方面仍然面临严峻的信息安全挑战[3]。首先，无人集群中无人机的数量众多，这导致了认证效率低下的问题，传统的身份认证方式无法满足大规模无人机的高效认证需求，需要研究和设计更加高效的认证机制，以确保无人机的合法性和可信度。其次，无人机通常受到能源、计算能力和存储空间等资源的限制，这意味着在保障信息安全的同时，需要尽量减少对资源的消耗，如何在有限的资源条件下实现高强度的无人集群安全机制，成为了一个亟待解决的挑战。此外，无人集群的结构和拓扑是动态变化的，如无人机在集群中的位置和角色的动态调整，以及需要跨越不同形态的地面网络，这给低时延隐私性识别与认证带来了挑战，最后，电磁环境的开放性使得无人机极易受到干扰和欺诈，攻击者可能通过干扰无人机的通信信号或者伪造信号来实施攻击，从而影响系统的稳定性和信息的安全性，需要研究和应用抗干扰和防欺诈的技术来保护无人集群的信息安全。

针对上述问题与挑战，本文旨在深入调研无人集群安全问题，分析无人集群潜在的安全威胁，综述现有的安全技术手段，探讨新兴的安全解决方案，在集群单点安全、网络安全、身份安全、通信安全以及数据安全等无人集群关键环节进行广泛的调研与分析。

1 无人集群基本结构与系统

1.1 无人机结构

当前无人机主要由控制单元、存储单元、机身、载荷以及传感器等部件构成，如图 1 所示。

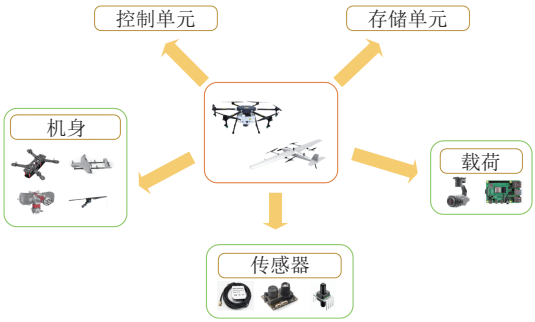


图 1 无人机部件

1）机身。无人机本身，包含机架、动力系统、电池等。

2）控制单元。负责发出控制命令并协调无人机内部各部件的正常运行。

3）存储单元。通常负责存储传输的数据和监测数据。

4）传感器。通常包括 GPS、光流传感器等，用于感知无人机自身状态或外部状态。

5）载荷。无人机配备的可用于各种任务的设备，如摄像头和用于监控、识别以及其他任务的机载计算机等。

只包含单架无人机的网络模型相对来说非常简单，在这种情况下无人机只需与地面站或其他地面设施进行通信。虽然这种配置具有成本低、灵活性高等优势，但它的任务执行能力有限。搭载多重负载的无人机通常需要持续监控能源消耗，因此难以实现大面积区域的同步覆盖。

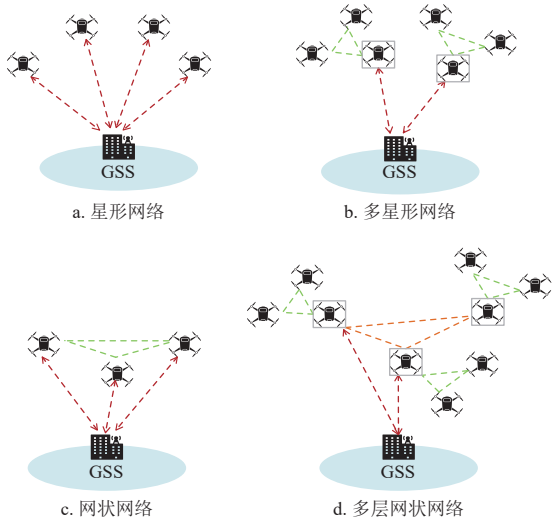
1.2 无人集群系统

在无人集群系统中，多架无人机可以携带不同种类的负载和设备以实现协同合作，弥补了单一无

人机系统的不足。此外，整个无人集群系统具备鲁棒性，即使有一小部分无人机出现问题，仍能够保持正常运行并提供服务。无人集群系统的结构可以以多种方式描述，文献 [4] 将无人机通信分为 4 个主要类别，包括集中通信、分散通信、多组无人机网络和多层无人机自组网，而文献 [5] 从不同的方面（基于基础设施、服务器/客户端、拓扑结构）描述了无人集群网络。本文根据拓扑结构、控制模式和通信结构对无人集群系统进行了分类。

1.2.1　拓扑结构

根据无人集群形成的网络拓扑结构，可分为星形拓扑、多星形拓扑、网状拓扑和分层网状拓扑。无人集群系统的不同拓扑结构如图 2 所示。



a. 星形网络　b. 多星形网络　c. 网状网络　d. 多层网状网络

图 2　拓扑结构

在星形拓扑结构中，所有无人机直接连接到一个中心地面站节点，它们之间必须通过这个中心节点进行通信，这种结构非常集中，容易出现单点故障，并且通信效率不高，形式如图 2a 所示。多星形拓扑结构将无人机分成不同的集群，每个集群都有一个领航无人机，负责与中心地面站通信。在同一集群内，无人机可以互相通信，但不同集群的无人机需要通过中心地面站来交流，形式如图 2b 所示。

网状拓扑结构允许无人机之间相互通信，同时它们也可以直接与地面站通信，而不需要依赖中心节点，形式如图 2c 所示。多层网状拓扑类似于多星形拓扑，但它引入了集群与领航无人机之间的直接通信，以便在不同层次上进行更复杂的通信，网状拓扑的主要优势在于其更灵活并且能够减少对中心设备的依赖，但这也导致网络结构更不稳定，需要考虑更多安全问题，其形式如图 2d 所示。星形拓扑结构和网状拓扑结构的比较如表 1 所示。

表 1　拓扑结构

参数	星形	网状
通信模块	点到点	多点到多点
通信基础设施	必须	非必须
作用范围	不能超过基础通信设施的范围	可以离开基础设施到偏远地区进行通信
通信跳数	单跳	多跳

1.2.2　控制模式

无人集群系统可分为控制模式和自主模式。在控制模式下，无人机由地面操作站遥控，这些操作可以通过系统控制台或人工操作进行，当无人集群由地面操作站控制时，其拓扑结构通常形成一个网状网络。信息的安全性可能取决于具体的基础设施，如公钥基础设施。在单层无人集群中，无人机可以直接相互通信，同时也可以与地面站进行通信。而在多层无人集群中，无人机不仅可以相互通信，还可以与特殊节点（通常称为领航无人机）进行通信。这些领航无人机既可以与地面站通信，也可以与其他无人集群中的领航无人机进行通信。在完全自主模式下，无人集群可以在没有地面控制站的情况下，独立决策、执行任务，无须外部干预。控制模式和自主模式之间的差异性可以从表 2 中体现。

表 2　无人集群控制模式的比较

参数	控制模式	自主模式
拓扑结构	星形/网状	网状
通信基础设施	必须	非必须
计算成本	低，许多计算可以依靠地面站或基础设施	高，需要机载计算机计算
通信成本	低，数据可以发送到基础设施	高，需要机载存储器
控制复杂度	低	高

1.2.3　通信结构

根据不同的通信结构，可以将无人集群的通信类型分为无人机对无人机（D2D）、无人机对地（D2G）、无人机对网络（D2N）、无人机对卫星（D2S）这 4 种类型，如图 3 所示。

1）D2D：无人集群中 D2D 的通信方式尚未被标准化。在集群内部，通信通常是在自组织网络环境下执行的，这种网络被称为飞行自组织网络（FANETs），无人机之间的通信通常被建模为点

对点通信。

2）D2G：无人集群需要与地面站（GS）进行通信，这种通信通常采用标准化的无线通信协议，如 Wi-Fi 802.11 或蓝牙等。

3）D2N：无人集群需要连接到公共网络设施，这时它们依赖于 3G、4G、LTE、5G 等技术。这种技术基于集中拓扑，其中每个区域都由一个基站提供服务。

4）D2S：当无人机需要在视距范围之外进行通信时，可以使用 D2S 通信，这种通信方式相对安全可靠，但与此同时，无人机的设备和通信成本也较高。

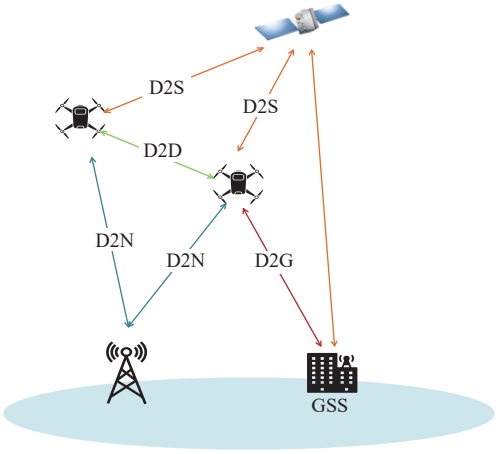


图 3 通信结构

1.3 特点

与传统节点组成的系统相比，无人集群系统主要包括以下特点。

1）网络拓扑结构：无人机具有较高的移动性，导致无人机形成的网络拓扑结构容易发生变化。

2）节点移动性：无人机比地面车辆或传感器网络更具移动性，并可以随时改变位置。

3）节点密度：在无人集群中，无人机在天空中彼此分离因此密度较低。

4）延迟：与传统网络相比，无人集群的网络结构不稳定导致延迟较高。

5）数据包丢失：由于无人集群在无线网络中且不断移动，其丢包率将高于传统的稳定网络。

6）覆盖范围：无人集群可以灵活的移动从而覆盖许多普通设备无法覆盖的区域，因此它们经常用于灾区。

7）网络寿命：与传统的网络结构相比，由无人机节点组成的网络具有更短的网络寿命。

8）资源问题：大型无人机可能对功耗不敏感，但小型无人机的电池容量和计算能力等资源均有限。

此外，考虑到无人集群具有自主模式，即该情况下无人集群具有较高的自控能力，可以在远离地面控制器的地方自主执行任务，这种特性衍生出新的技术特征。

1）自主权：无人集群具有更多的自主控制能力，但同时也需要更多关注无人集群内的鲁棒性和稳定性。

2）计算代价：无人机本身需要承担更大的计算成本，以更自主地执行任务。

传统结构（如传感器网络）、控制模式下的无人集群结构和自主模式下的无人集群结构的特点差异性如表 3 所示。

表 3 不同结构之间的比较

参数	传统结构	无人集群结构（控制模式）	无人集群结构（自主模式）
节点速度	低	高	高
延迟	低	高	高
节点密度	高	低	很低
丢包率	低	高	高
覆盖范围	低	高	很高
网络寿命	高	低	低
自主控制	低	低	高
传播模型	非视距（NLoS）	NLoS/LoS	NLoS/LoS
移动模型	通常为2D	通常为3D	通常为3D

1.4 无人集群系统信息安全挑战

基于上述无人集群的特点，在设计针对无人集群的信息安全方案时可能会面临以下挑战。

1）无线通信风险：无人机主要依赖无线链路在开放环境中传输数据，这让它们容易成为潜在攻击目标，攻击者可能试图干扰、截取或中断通信链路从而严重影响无人集群执行任务。

2）动态网络拓扑：由于无人机的高机动性，无人机组成的网络拓扑结构变化频繁，这对于设计有效的路由协议提出了挑战。

3）有限资源负载：尽管某些大型无人机拥有足够的计算和存储资源，能够执行复杂任务，但大多数小型无人机的计算和存储能力有限，这会严重限制可用于安全任务的计算和通信资源。

4）时延控制：许多无人机任务需要实时性，如位置共享。然而，在无人机网络中，丢包率较高，需要较高的通信重复和通信时延，这可能导致无法满足实时性需求。

5）可扩展性：无人机网络的规模可能非常庞大，因此系统的可扩展性对无人集群是非常重要的基本属性，但是这种可扩展性对设计信息安全机制形成了挑战。

6）异构性：不同制造商生产的无人机可能具有不同的硬件配置和通信协议，这增加了协调和整合多个无人机以执行任务的复杂性，给设计高效合理的信息安全协议带来了更大挑战。

2　无人集群安全威胁分析

面向无人集群的常见安全威胁和攻击方式，包括单节点安全威胁、集群网络安全威胁、集群身份安全威胁、集群通信安全威胁。

2.1　单节点安全威胁

在无人集群系统中，某些拓扑结构，如星形和多星形拓扑，依赖一个中心无人机或控制器来管理整个无人集群。在这种情况下，攻击者可能针对中心无人机或控制器发动攻击，造成系统的单点故障或获取对系统的控制权，从而影响系统的可用性。具体来说，攻击者可以采取以下方式对无人机系统造成危害。

1）故障注射攻击

攻击者可能在签名过程中发送不正确的签名，或干扰无人机内部的算法和工作流程，以破坏它们的正常运行。

2）软件攻击

攻击者可以通过在地面站或无人集群内部植入恶意软件来攻击无人机系统自身，从而绕过安全机制，如身份验证。

3）物理攻击

物理攻击包括实际的无人机捕获或摧毁，通常发生在低空地区。攻击者可以使用多种手段，如网、枪支等。

4）侧信道攻击

侧信道攻击是一种通过分析目标系统中泄露的信息来试图获取有用信息的攻击方式。这可能包括分析运行算法时泄露的操作代码或加密密钥信息。侧信道攻击可以采用多种方法，包括基于时间的功耗分析和电磁分析，以及组合不同的侧信道攻击方法。

5）传感器攻击

传感器攻击主要影响依赖外部环境传感器的无人机系统，如 GPS、雷达和红外传感器。最常见的攻击类型是 GPS 欺骗，文献 [6] 中攻击者发送虚假 GPS 信号，误导无人机的位置信息，还有一种方法通过使用多个天线发送虚假信号，使无人机沿着错误轨迹飞往攻击者指定的坐标。其他攻击方式包括激光攻击光流传感器[7] 等。此外，视觉传感器用于识别、导航和避障，一旦遭到破坏，可能导致无人机碰撞或任务失败。文献 [8] 提出了一种远程攻击方式，通过注入恶意激光来攻击传感器，导致系统故障。另外，微机电系统（MEMS）陀螺仪对高频噪音敏感，容易受到损害，从而影响无人机的空间位置测定。

6）联合攻击

通常情况下，攻击者会结合多种攻击技术，如故障注入攻击，以改变已加载或存在于目标系统中的程序代码的正常执行，从而获取额外的访问权限。

2.2　集群网络安全威胁

在无人集群系统中，无人集群网络通常是公开已知的，攻击者可以通过网络形式大范围大面积威胁多个无人集群节点单元，具体来说，攻击者可以采取以下方式对无人机系统造成危害。

1）拒绝服务攻击（DoS）

拒绝服务攻击在无人机网络中相当普遍，由于无人集群的网络通常是公开的，攻击者可以相对容易地发起这种攻击。在这种攻击中，攻击者会向合法的无人机发送大量请求，特别是针对领航无人机，导致系统超负荷，有时甚至造成合法无人机的请求被完全拒绝。此外，攻击者还可以针对控制节点发动攻击，破坏地面站和无人机之间的正常通信。

2）广播风暴

广播风暴在无人集群网络中也是一个常见问题，无人机网络由多个移动节点组成，广播风暴的攻击者可以发射针对性广播信息，导致频繁的网络中断或链路质量的波动，这种攻击方式会直接影响链路层，进而影响网络层，使 IP 路由失效。这会导致每个节点需要重复搜索路径，产生冗余的数据重播等问题[9]。

3）路由攻击

无人机系统容易受到路由攻击，这种攻击一般发生在 3 个阶段：路由发现、路由维护和数据转发[10]。由于无人集群的拓扑结构高度动态，基于路由的攻击在 FANETs 中非常普遍。如虫洞攻击是 FANETs 中最严重的攻击之一，虫洞攻击通常是由两个以上的恶意节点共同合作发动攻击，两个处于不同位置的恶意节点会互相把收到的绕路讯息，经由私有的通信管道传给另一个恶意节点，如此，虽

然这两个恶意节点相隔甚远，但两恶意节点间却犹如只有一步之隔。如此经过恶意节点的跳跃数，将有很大的机会比正常路径的跳跃数还要短，借此来增加取得路权的机会。

2.3 集群身份安全威胁

在无人集群系统中，无人节点的身份信息是非常关键的基础信息，无人系统的攻击者可以通过身份伪造、身份篡改等形式对无人集群系统造成威胁，具体来说，攻击者可以采取以下方式对无人机系统造成危害。

1）身份伪造

攻击者可能会窃取其他合法节点的身份信息，或尝试伪装成已被授权的节点，以加入无人集群的通信。成功进行身份伪装后，他们可以渗透到无人集群内部，损害无人机的正常操作或窃取更多的数据。如攻击者可能复制其他节点的证书以伪装成合法节点。

2）身份篡改

攻击者可能会恶意修改合法节点的身份信息，这会导致节点无法被系统识别和接受，从而破坏系统的可用性。此外，攻击者还可能劫持合法的无人机，并更改它们的身份信息，然后试图重新加入无人集群并获取不正当利益。

3）身份拒绝

在发生争议时，恶意节点可能会否认先前发送的数据，这种行为会导致难以验证或追踪恶意行为。

2.4 集群通信安全威胁

在通信方面，攻击者可能以多种方式干扰系统的正常运行或获取通信数据，从而威胁无人集群系统的可用性和安全性。

1）干扰攻击

这种攻击通常在通信协议结构的物理层面发生，攻击者可通过无线电频率干扰无人机与控制站的通信。具体而言，攻击者可能从地面或其他无人机发动干扰，通过将发射机调谐到目标通信频率，来混淆或阻止目标之间的正常通信。这种干扰攻击对各种拓扑结构都有效，尤其在开放环境中，蓝牙和 Wi-Fi 等信号容易受到影响，从而使无人机容易受到攻击。一旦通信被干扰，无人机可能因协议异常暴露更多安全漏洞，使攻击者能够利用其他攻击手段。

2）窃听攻击

攻击者通过监听通信信号可以获取控制信息或窃取传输的有用数据。攻击者还可以监视数据本身，或分析数据传输的频率和时间，以获取目标的敏感信息。这种攻击可以在系统的不同网络层次中发生，对用户的隐私和系统的保密性构成威胁。

3）篡改攻击

攻击者可能截取、拦截或篡改数据传输，以阻止通信或发送恶意数据给目标。这种攻击会危害系统的可用性和完整性。此外，中间人攻击是该攻击的变种，攻击者位于数据发送者和接收者之间，拦截和篡改数据，从中获得有用信息。

4）碰撞攻击

在链路级别上，攻击可能导致数据碰撞，这要求发射机重新传输信息，从而增加无人机的能源开销，甚至导致电池能量耗尽。

5）重放攻击

攻击者尝试通过重放先前截获的合法数据包，从而获取有用信息或实现非法认证。

3 无人集群安全方案

针对无人集群系统所面临的信息安全威胁，详细介绍不同级别的安全解决方案，包括网络安全架构、集群身份安全、集群通信安全。

3.1 集群网络安全

3.1.1 网络安全架构

无人机网络的特殊性使得传统的路由协议设计变得更加复杂。因此，引入新的网络架构来解决这些挑战是可以展望的方案。一种方法是采用软件定义网络（software defined network, SDN）这一新型网络范式来增强通信安全。SDN 架构将网络的控制层和数据转发层分离，使得网络更加可控。一种应用于无人机网络的 SDN 架构如图 4 所示。这种方法可以提高网络的韧性，抵抗如虫洞攻击、黑洞攻击和 DDoS 分布式拒绝服务攻击。文献 [11] 使用 SDN 技术来检测 DDoS 攻击，通过分析数据包传输速率向量的余弦相似性，实现对 DDoS 攻击的检测。文献 [12] 提出了一种以 SDN 为基础的无人机网络框架，其中无人机充当 SDN 交换机，以减轻本地故障和中断对网络的影响。仿真结果显示，这一方案降低了无人机网络的端到端中断率和延迟。文献 [13] 采用 SDN 技术确保 FANETs 的通信安全性，其中每架无人机都包含一个 SDN 交换机。与传统的基于 Iptables 规则（Linux 中的包过滤防火墙系统）的自适应需求距离矢量路由（Ad hoc on-demand distance vector, AODV）相比，这一方法具有更好的适用性。

文献 [14] 提出了一种名为 S-UAV 的安全无人机模型，它引入位置信息以在多架无人机之间建立无线网状网络（wireless sensor network, WSN）。作者还设计了一个算法，它能够有效地寻找最短通信路径，同时采用强加密技术以抵御潜在的安全威胁。仿真结果表明，这种方法具有高吞吐量、低功耗以及短加密解密时间的优点。文献 [15] 提出了一种基于区块链技术的无人集群自适应组网机制，它将全局唯一标识符（globally unique identifier, GUID）集成到区块链存储机制中实现了快速的身份认证，并成功解决了无人机集群中动态切换和身份漫游的相关问题。

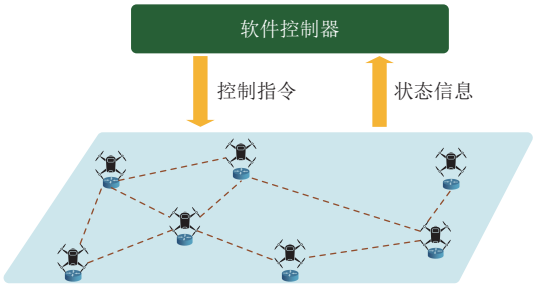


图 4　SDN 适用于无人机网络

3.1.2　入侵检测系统

在保障网络安全方面，入侵检测系统（IDS）发挥着重要作用，它被广泛应用于检测网络攻击和应用系统的恶意行为。然而，传统的入侵检测方法，特别是那些基于静态网络的方法，在动态无人机网络中的准确性较低，因此不能直接应用于无人集群网络。文献 [16] 提出了一种适用于 FANETs 的入侵检测系统，它结合了光谱流量分析和强健控制器，用于检测无人机网络中的异常行为并对抗 DDoS 攻击，并且验证了可行性。文献 [17] 提出了一种基于监督学习和数据算法的恶意无人机检测方法，用于发现 FANETs 网络中的恶意节点。这种方法依赖地面站从不同源节点和路由路径接收数据包，以此评估每架无人机的信用值，最后通过聚类算法提高准确性。

深度学习（DL）也已被引入入侵检测领域，并显示出明显的优势。文献 [18] 提出了一种利用人工智能来识别不同类型攻击的无人机入侵检测系统。由于在无人集群体中，当附近的无人机受到攻击时，通信模式会受到影响，借此检测附近无人机是否受到攻击。文献 [19] 提出了一种基于长短期记忆网络–循环神经网络（LSTM-RNN）的 FANETs 下入侵检测框架。每架无人机都配备分布式的 RNN 模块，将其流量发送到包含中央化 LSTM-RNN 模块的基站进而做出入侵检测决策。该方法在不同数据集上验证了准确性，但尚未在实际 FANETs 中应用。

此外，也有学者关注到了区块链技术在 IDS 中的应用潜力。文献 [20] 提出了一种基于区块链和径向基函数神经网络（radial basis function neural network, RBFNN）的去中心化入侵检测方案。每个无人机节点都可以使用共享的 RBFNN 预训练模型进行本地预测并在必要时与其他节点共享结果以提高整个网络的预测准确性。

3.1.3　广播风暴缓解算法

广播风暴问题通常源于病毒或回路连接，因此需要采取综合的防御和改进措施，如 IDS 和恰当的网络拓扑规划。此外，合理的算法可以减轻由无人机数量增加引发的网络拥塞问题。文献 [21] 针对 FANETs 场景中的命名数据网络，设计了一种基于流量统计、网络度量和链路层信息等多标准的转发策略 iFLAT，仿真实验显示，在广播风暴场景中，与现有的缓解方案 CONET 相比，该策略的流量负载减少了 25.75%。文献 [22] 在广播抑制算法中引入高级加密标准算法（AES）以确保广播消息的机密性，结果表明，强对称密钥加密对广播抑制算法的性能影响并不显著。文献 [23] 提出了一种名为动态域算法（DNA-DSP）的方法，利用动态邻居数量来智能决定何时重新传输消息，从而缓解 FANETs 中由无人机数量增加引发的网络竞争问题。

3.1.4　安全路由协议

安全路由协议是专注于提供安全性保障的网络协议，主要应用于 FANETs 中。目前，许多安全路由协议都是在已有协议的基础上进行扩展，这些扩展可以通过多种方式实现，包括采用定向天线技术、消息认证机制等，以应对潜在的路由攻击问题[24]。此外，考虑到 FANETs 场景下的硬件和能源限制，也有部分学者将研究重点转向了路由协议的性能优化。文献 [25] 针对 FANETs 场景下节点的高移动性和动态拓扑变化特性提出了一种基于强化学习 Q-Learning 的拓扑感知路由协议 QTAR，通过 Q-Learning 算法，QTAR 能够根据网络环境的变化动态调整学习率和奖励因子，自适应地调整路由决策，仿真结果表明，在不同的场景下，QTAR 在各种性能指标上都具有优秀的表现。

3.2　集群身份安全方案

无人集群系统经常涉及大量实时通信，为保障

系统的安全，只允许经过身份验证的用户或设备访问无人机的数据。尽管身份认证协议和访问控制协议都能解决这一问题，但由于无人机的计算能力和电池容量有限，一些传统的身份验证方法，如公钥基础设施（public key infrastructure, PKI），因其高昂的计算需求，难以适配资源约束型无人机系统的安全认证场景。因此，许多研究者正在开发专为无人机网络和无人机集群设计的身份认证和访问控制协议。这些协议旨在确保只有经授权的用户可以访问无人机数据，或在无人机集群中实现身份验证。

3.2.1 用户和无人机间的身份验证

生物特征识别通常用于用户对无人机进行身份认证，文献 [26] 提出了一种基于临时凭证的匿名用户身份认证机制，采用密码和生物识别技术，整体上具有轻量级特性，经过测试可以抵御各种攻击。文献 [27] 设计了一种基于椭圆曲线密码学（ECC）的身份认证方案，用于保护用户和无人机之间的通信。文献 [28] 采用用户生物特征认证，并使用模糊提取器、哈希和异或运算来实现用户身份认证。文献 [29] 将生物识别和物理不可克隆函数（PUF）结合，在用户端利用生物特征生成用户密钥，在无人机端通过 PUF 电路生成唯一响应作为无人机密钥，从而实现了在协商通信过程中的相互身份认证，并通过 BAN 逻辑（一种基于知识和信仰的推理结构性方法，用于分析和验证认证协议的安全性）、随机预言机模型（ROR）和 AVISPA 仿真（一种自动验证网络安全协议与应用程序的工具集）分析了该认证协商方案的安全性。

上述的解决方案基于密码学和生物特征，许多研究则侧重于更轻量级的解决方案。文献 [30] 提出的轻量级身份认证方案仅使用哈希函数和异或运算，并通过 ROR 验证。文献 [31] 将无人机应用于车载自组织网络（VANETs），提供了无人机、信任机构（TA）和原始动态路边单元（RSU）之间的轻量级认证。它能够抵御常见的攻击，并防止因物理捕获攻击而引起的对手冒充攻击。除了要考虑认证本身的轻量级，集群规模对身份认证效率也存在较大影响。尤其是当集群形成星形拓扑结构的情况下，随着规模的增加，中央地面控制站的身份认证压力也不断增加。文献 [32] 提出了一种可扩展的轻量级身份认证协议，使用 PUF 实现地面站对多架无人机的双向身份认证，所提出的方案的执行时间与无人机数量呈线性增加关系。此外，物理层安全可以依靠其轻量级的特性用于身份验证。文献 [33] 考虑了毫米波通信场景，其中单个基站为多个无人机提供服务。在窃听者存在的情况下，基站会向数据中添加人工噪音以抵御潜在的攻击，并使用用户的预共享密钥和数据符号进行身份验证。

3.2.2 无人机之间的身份验证

无人机之间的身份验证和访问控制方案在无人集群系统中同样重要。文献 [34] 结合轻量级的 AES、哈希函数和异或运算提出了一种基于改进 PKI 的身份认证协议，与现有工作相比，该协议被证明是高效的并可在无人机物联网（IoD）环境中实际部署。文献 [35] 考察了将无人机融入智能交通系统（ITS）的应用，并提出了一种结合了双曲线密码学（HECC）、数字签名和哈希函数的身份验证方案。文献 [36] 提出了一种适用于 5G 环境下无人集群安全通信的身份验证机制，该机制能在集群出现受损无人机时根据位置和能耗重新选举领导者。文献 [37] 提出了一种用于认证多个实体的群体认证方案，引入多个卫兵无人机以避免单点故障问题。文献 [38] 提出了一种基于 PUF 的无人机向地面站进行认证的方案，并将其扩展到了无人机之间的认证。然而，该方案存在一个限制，即无人机之间的认证需要通过地面站进行，这会给地面站带来较大负担。物联网技术同样可以引入机器学习技术以进行身份验证。在验证无人机身份时，数据收集可能涉及隐私问题。文献 [39] 提出了一种基于联邦学习的身份验证模型，它利用无人机的射频特性，不需要与服务器或其他无人机共享数据。在模型训练完成后，使用安全的平均方法传输权重参数和梯度到服务器。文献 [40] 从物理层安全角度出发，将无人机之间的通信信道物理特性作为信息交换的指纹，提出了一种基于物理层挑战-响应机制（challenge-response, CR）的身份验证方法，与其他的物理层验证方法相比，该方法在静态集群和动态集群的场景下都表现出了更高的准确率。

此外，一些研究者已经开始将区块链技术应用于身份验证方案。在基于区块链的方法中，身份信息被记录在区块链上，这有助于分析历史身份信息以确保无人机的状态得到更新。此外，区块链的共识机制也增加了攻击者冒充无人机的难度，因为在成功加入网络之前，他们的身份必须在网络中共享。文献 [41] 提出了一种在 IoD 环境中基于区块链的身份验证框架。无人机的身份和声誉信息被存

储在区块链上。该方案采用了权威证明（PoA）共识算法，以减少区块链计算的成本。文献 [42] 提出了一种基于区块链的轻量级分布式身份验证服务，适用于工业无人机场景。他们使用 Fabric 联合链，将与身份相关的操作记录在智能合约（SC）中，并将身份验证过程与椭圆曲线密码学相结合。然而，该方案在恶劣网络环境下存在部署局限性，同时面临基于算力垄断的 51% 共识攻击风险。

区块链技术是去中心化和分布式的，可适用于各种不同领域的场景，如图 5 所示。文献 [43] 引入了一个公共区块链解决方案，应用于智能城市环境。这一方案允许无人机在将身份信息注册到区块链后，能够快速、无缝地在城市内的不同区域移动，而无须反复进行身份验证。不过这种方案的性能与无人机的速度密切相关，可能会对无线连接的稳定性产生一定影响。文献 [44] 设计了一种面向跨领域场景的基于区块链的身份验证方案。该解决方案在分布式环境中采用本地私有区块链和联盟链，用于处理本地身份注册验证以及在跨领域情境下无人机的身份验证。这种方法有效地解决了不同领域之间的通信问题，尤其是在涉及第三方参与的情况下，解决了不信任领域之间的的通信难题。然而引入区块链技术可能会引发一些问题，如交易失败率和智能合约的读写延迟。

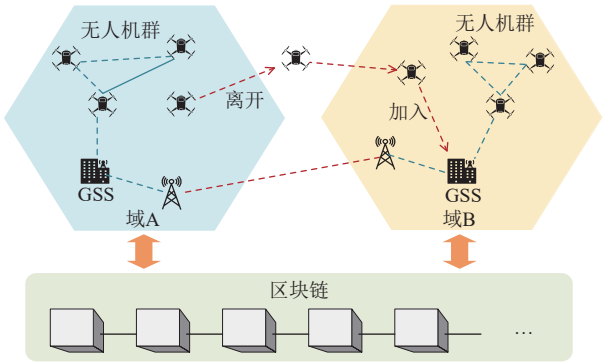


图 5　跨域场景中的区块链

3.3　集群通信安全方案

在无人集群体通信中，确保安全性需要考虑多个方面，包括通信加密和建立安全通道等。引入纠错编码和安全传递方案对于应对通信中的碰撞攻击非常关键，这些传统方法在无人机通信中同样适用。

3.3.1　密钥管理方案

为无人集群通信进行加密是有必要的。与传统的双方通信相比，无人集群密钥的协商和更新更为复杂，需要设计有效的密钥管理方案。文献 [45] 提出了一种基于证书的访问控制和加密协议方案，该方案应用了超椭圆密码（HECC）技术和单项目密码哈希函数，在 FANETs 场景中使用了 ROR 模型和 AVISPA 进行安全评估。文献 [46] 进一步改进了文献 [30] 的认证密钥协商协议，在同样仅使用哈希函数和异或运算的条件下解决了密码猜测、匿名性、用户/服务器冒充、内部攻击和中间人攻击等问题，改进后的协议在 ROR 模型中被证明是安全的。文献 [47] 提出利用物理层特性生成物理层密钥，并设计了一种基于聚类结构的椭圆曲线密码−群密钥协商（ECC-GKA）算法，与 ElGamal 等传统密钥协议相比，这种算法具有更高的数据传输精度和较小的计算负载。

相对于群组密钥协商协议，群组密钥分发协议依赖中心节点，但通常具有更好的可扩展性。常见的群组密钥分发机制通常基于预共享密钥或公共/私有密钥对的分发。如文献 [48] 提出了基于无人集群的群组广播协议（SBP），与基于公钥的协议相比，SBP 的带宽开销更低。文献 [49] 提供了一种密钥分发算法，该算法仅涉及逻辑异或运算和较少的数据传输，适用于集中式和分布式密钥分发。文献 [50] 采用经过身份验证的密钥管理（AKM）协议的方法，用于提供 IoD 环境中的安全性。该方案利用轻量级加密、椭圆曲线加密和哈希函数来执行 AKM 过程，并提供基于安全协议形式化分析工具（Scyther）的安全验证，以应对各种常见攻击。

一些解决方案正在将区块链技术引入密钥管理领域。区块链可以作为与密钥相关信息的载体，多个无人机可以协同维护一个区块链，确保密钥和群组成员信息的安全和一致性，尤其适用于多星拓扑结构，以便于无人机的迁移。如文献 [51] 提出了一种基于区块链相互修复的密钥分发方法，地面站负责维护整个区块链，而无人集群体维护区块链的最新部分。当密钥丢失时，相邻的无人机可以请求获取密钥信息，以恢复丢失的密钥。然而，这种方法中地面站作为中心节点容易成为攻击目标。文献 [52] 提出了一种面向无人机点对点通信的解决方案，该方案每次传输数据都要经过验证和记录。然而，该方法使用了双线性映射和非对称加密算法，增加了计算成本和时间成本。文献 [53] 考虑了这一问题，提出了一个基于区块链的异构 FANETs 分布式密钥管理方案。在这个方案中一个领航无人机负责更新区块链，而其他无人机保持区块链的最新状态，区块链用于存储密钥信息。这个方法可以

安全地分发和更新密钥信息，但会导致领航无人机负担较重。

3.3.2 信道安全方案

无人集群系统亟需强化其通信信道的安全性防御能力，以抵抗窃听攻击和恶意干扰。物理层安全（PLS）已经成为这类安全威胁的有效解决方案[54]。首先，在提出安全方案之前，有必要了解无人机相关参数对通信性能的影响。文献 [55] 对空中通信网络进行了建模，并分析了空中窃听通道的物理层安全性，最终的模拟结果显示，网络飞行平台（NFP）的高度、窃听密度和环境类型是影响物理层通信安全性的主要参数。文献 [56] 针对一组无人机窃听情况下，研究了空对空链路（A2A）的信噪比（SNR）的概率密度函数和累积分布函数，以及 A2A 通信系统的隐秘中断概率（SOP）和平均隐秘速率（ASC）。而文献 [57] 则讨论了智能反射表面（RIS）在增强无人机 PLS 方面的相关研究进展，并通过具体的案例分析展示了 RIS 能够在多窃听者场景下提高通信保密容量的能力。

文献 [58] 研究了无人机的通道安全性，使用多天线源向无人机传输人工噪声和信息信号，从而可以抵御窃听攻击和全双工主动干扰的恶意入侵。该研究还考察了无人机高度对安全性能的影响。文献 [59] 关注了无人机通信的物理层安全性，并应用基于块坐标下降和连续凸优化方法的迭代算法，以提高在 5G 无线网络下的无人机通信安全率。文献 [60] 注意到了无人机平台在振动和风扰动下的抖动，并利用这一特性来改善无人机与地面站传输链路的隐秘性能。

然而，上述研究未考虑无人机之间的相互依赖关系。文献 [61] 提出了一种联合友好干扰和带宽分配算法，用于解决多无人机通信系统的保密率问题，该方案考虑了在复杂网络拓扑下的通信资源分配。文献 [62] 开发了一个多目标优化问题（MOP）用于安全通信，旨在在无人机使用协同波束成形（CB）执行虚拟天线阵列（VAA）以与多个基站通信的情况下最大化无人机的安全率。

此外，无人机可以部署为移动基站充当通信中继，从而减轻蜂窝网络的负担。在这种情况下，由于环境不稳定性和有限的计算能力，信道状态信息（CSI）无法被完美估计[63]。文献 [64] 在这种情况下提出了一种基于协同速率分配（CRS）的安全设计，假设发射机只有不完整的信道状态信息（ICSI），并设计了一种资源分配算法，以在最坏情况下提高合法用户的安全性。

4 开放性问题与潜在研究方向

尽管现有文献中针对无人集群系统的信息安全方案已经能够解决一些无人集群系统面临的安全威胁，但仍然存在许多有待解决的开放性问题。

1）算法轻量化问题：在认证和密钥管理方案中，基于密码学的方案通常具有较高的计算和通信开销，而安全等级要求越高往往意味着所使用的密码算法和安全协议越复杂，这就造成了安全性和轻量化之间的权衡问题，也就是高安全性和高实用性很难在基于传统密码学的方案中并存。

2）区块链延迟问题：在利用区块链的方案中，区块链延迟几乎是不可避免的，而在许多无人集群应用场景中，较高的通信时延与计算时延是难以接受的，但是面对无人系统复杂的电磁环境和有限的计算资源，区块链需要的计算和交互过程往往造成较高的时延问题，这导致了区块链在无人集群系统中的应用受到限制。

3）跨域隐私保护问题：无人集群的一个显著特点是移动性，在无人集群执行任务的过程中，可能需要和地面网络保持连接沟通，但是地面网络节点不能保障是完全可信的，毫无安全措施的网络连接很容易暴露无人集群的路径及数据隐私。如何在保持地面网络连接获得网联服务的同时保障无人集群轨迹和数据的安全性和隐私性，成为了一个显著的隐私保护挑战。

4）极端环境通信问题：无人集群需要工作在一些极端环境，如军事对抗战场和地震救灾，在这些场景下电磁频谱空间环境可能遭遇非常严重的干扰，目前常见的无人集群协作与控制通信都有可能被严重阻塞，但保障无人集群在这些极端环境下顺利执行任务的研究尚不充分。

5）标准化问题：目前对于无人机及无人集群仍然缺乏统一的安全标准，尽管已经提出了许多适用于不同架构无人机的安全策略，但很难根据一个统一的标准来对它们进行评估，这就导致很难准确评价不同算法和方案的有效性。

针对上述问题与挑战，结合当前的技术发展趋势和新兴技术潜力，本文给出以下几种解决思路和研究方向。

1）新型群密钥机制：传统的群密钥机制都是利用密码算法设计通过多次节点之间的通信交互形成的群密钥方案，这种群密钥生成和管理会造成较

多的计算和通信负荷。针对这一问题，可以采用区域性物理层特征构建群密钥的生成与分发，将群密钥的生成和分发过程建立在集群节点对自身物理特征的感知上，而无须过多的通信交互与计算，这为无人集群群组密钥机制提供了一种高效的解决思路。如文献 [65] 基于信道的随机性（受到多径效应、散射和遮挡等因素的影响，信道的响应在时间和频率上都是变化的）和互易性实现了一种群密钥生成协议（SSGK），该协议能够利用 CSI 等区域性物理特性和物理不可克隆函数来高效、快速的生成成对的密钥并在集群中共享。同样的，文献 [66] 也关注到了 CSI 在群密钥机制中的应用潜力，将其与深度学习技术结合实现了名为 DroneKey 的群密钥生成方案，该方案通过训练深度神经网络来提取 CSI 流（捕捉了设备与无人机之间信道的动态变化）之间的隐藏相关性，并利用这些相关性在群组内的不同设备之间生成一致的群密钥，对比实验和安全分析证明，利用容易感知且难以被复制和预测的物理特性来生成群密钥的方法可以显著降低通信成本和计算成本并提供额外的安全保障。

2）本体特征学习：现有的无人集群认证和识别过程大都是基于数字签名算法或区块链技术，其认证识别过程需要较为繁琐的信息交互和计算过程，从而造成通信时延较长。为解决上述问题，可以利用本体特征学习，将无人集群自身的独特特征作为身份认证和识别的主要来源，从而简化认证和识别的复杂度，如无人集群通信过程中的射频指纹和提取电路不完美性的不可克隆函数；集群中每对无人机之间信道的物理特性和提取环境变换的挑战–响应机制[40]。这些新机制的高效性和安全性使得它们成为设计低延迟、高安全认证识别协议的有力技术手段。

3）协作式假名机制：在无人集群跨区跨域网络通信过程中，如果采用传统的自身身份信息注册，将会不可避免地造成身份信息泄露以及无人集群踪迹泄露，为解决这一问题，可以考虑协作式假名机制。目前，该机制已经在 VANETs 中广泛应用，并可迁移到 FANETs 中，如文献 [67] 实现了一种基于假名的无证书隐私保护认证方案（PCPPA）。在此方案中，车辆利用 TA 颁发的凭据在车辆到基础设施（V2I）认证阶段生成假名，路边单元（RSU）验证这些凭据和假名以确保只有合法车辆接入网络。在 V2I 认证成功后，RSU 帮助车辆生成车辆到车辆（V2V）通信所需的假名，从而保障通信的安全性和隐私性。此外，还可以考虑多域联合的假名生成和管理技术。将区块链智能合约技术和安全洗牌技术相结合，利用多域联合的形式共同生成针对特定无人集群的形式化假名，从而在保证无人集群节点的身份安全性的同时，实现数据的隐私保护和跨区跨域场景下的高效认证与识别。

4）基于姿态的安全通信：在面对电磁频谱空间受到严重干扰的情况时，仍然采用传统的无线电通信很难保障无人集群任务顺利执行。针对这一问题，一个潜在的解决思路是利用无人集群的自主化能力以及计算机视觉能力。目前，无人集群编队已在表演、广告等领域广泛应用，其本质即是通过编队的形状来传递文字、图像等特殊信息，类似的，在集群安全领域，可以将重要的消息内容通过无人集群的编队形状或节点之间不同的姿态传递给地面接收站，以及时调整通信策略或改变通信环境，从而避免无人集群因电磁空间的严重阻塞而无法完成既定任务。

5）标准化数据库和测试标准：针对目前无人集群信息安全机制评估过程缺乏统一标准的问题，可以通过开源数据库建立统一的测试环境和测试标准，在相同的数据集和相同的评价指标上完成对算法和模型的统一评测。

5　结束语

本文调研了无人集群的信息安全问题，从无人集群基础结构出发，首先介绍了无人集群系统的基本架构和特点，然后分析了现有无人集群信息安全面临的威胁和挑战，接着详细讨论了针对不同安全威胁的现有解决方案，从单一节点、集群网络、集群身份认证、集群通信安全等方面综述了现有解决方案，最后分别讨论了一些目前无人集群信息安全尚未解决的开放性问题和潜在的解决方法以及未来值得研究的方向。本文可以激发研究者对无人集群信息安全相关领域的兴趣，为无人集群广泛应用与产业发展提供有益引导。

参 考 文 献

[1] YANG W C, WANG S, YIN X F, et al. A review on security issues and solutions of the internet of drones[J]. IEEE Open Journal of the Computer Society, 2022, 3: 96-110.

[2] YAACOUB J P, NOURA H, SALMAN O, et al. Security analysis of drones systems: Attacks, limitations, and

recommendations[J]. Internet of Things, 2020, 11: 100218.
[3] ARAFAT M Y, MOH S. A survey on cluster-based routing protocols for unmanned aerial vehicle networks[J]. IEEE Access, 2018, 7: 498-516.
[4] LI J, ZHOU Y F, LOUISE L. Communication architectures and protocols for networking unmanned aerial vehicles//2013 IEEE Globecom Workshops (GC Wkshps). [S. l.]: IEEE, 2013: 1415-1420.
[5] GUPTA L, JAIN R, VASZKUN G. Survey of important issues in uav communication networks[J]. IEEE Communications Surveys & Tutorials, 2016, 18(2): 1123-1152.
[6] HE D J, QIAO Y R, CHEN S Q, et al. A friendly and low-cost technique for capturing non-cooperative civilian unmanned aerial vehicles[J]. IEEE Network, 2019, 33(2): 146-151.
[7] ZHI Y Y, FU Z J, SUN X M, et al. Security and privacy issues of UAV: A survey[J]. Mobile Networks and Applications, 2020, 25(1): 95-101.
[8] FU Z J, ZHI Y Y, JI S L, et al. Remote attacks on drones vision sensors: An empirical study[J]. IEEE Transactions on Dependable and Secure Computing, 2022, 19(5): 3125-3135.
[9] WISITPONGPHAN N, TONGUZ O, PARIKH J, et al. Broadcast storm mitigation techniques in vehicular ad hoc networks[J]. IEEE Wireless Communications, 2007, 14(6): 84-94.
[10] MAXA J A, MAHMOUD M S B, LARRIEU N. Survey on uaanet routing protocols and network security challenges[J]. Ad Hoc Sens Wirel Networks, 2017, 37: 231-320.
[11] YIN D, ZHANG L M, YANG K. A DDoS attack detection and mitigation with software-defined Internet of Things framework[J]. IEEE Access, 2018, 6: 24694-24705.
[12] SECINTI G, DARIAN P B, CANBERK B, et al. SDNs in the sky: Robust end-to-end connectivity for aerial vehicular networks[J]. IEEE Communications Magazine, 2018, 56(1): 16-21.
[13] GUERBER C, LARRIEU N, ROYER M. Software defined network based architecture to improve security in a swarm of drones[C]//Proceedings of the International Conference on Unmanned Aircraft Systems. New York: IEEE, 2019: 51-60.
[14] RAJA G, ANBALAGAN S, GANAPATHISUBRAMANIYAN A, et al. Efficient and secured swarm pattern multi-UAV communication[J]. IEEE Transactions on Vehicular Technology, 2021, 70(7): 7050-7058.
[15] ZHOU X, YANG L, MA L R, et al. Towards secure and resilient unmanned aerial vehicles swarm network based on blockchain[J]. IET Blockchain, 2024, 4(S1): 483-493.
[16] CONDOMINES J P, ZHANG R, LARRIEU N. Network intrusion detection or UAV ad-hoc communication: From methodology design to real test validation[J]. Ad Hoc Networks, 2019, 90: 101759.
[17] SUN S S, MA Z C, LIU L, et al. Detection of malicious nodes in drone ad-hoc network based on supervised learning and clustering algorithms[C]//Proceedings of the 16th International Conference on Mobility, Sensing and Networking. New York: IEEE, 2020: 145-152.
[18] BASAN E, LAPINA M, MUDRUK N, et al. Intelligent intrusion detection system for a group of UAVs[C]// Advances in Swarm Intelligence. [S.l.]: Springer International Publishing, 2021: 230-240.
[19] RAMADAN R A, EMARA A H, AL-SAREM M, et al. Internet of drones intrusion detection using deep learning[J]. Electronics, 2021, 10(21): 2633.
[20] HEIDARI A, NAVIMIPOUR N J, UNAL M. A secure intrusion detection platform using blockchain and radial basis function neural networks for Internet of Drones[J]. IEEE Internet of Things Journal, 2023(10): 8445-8454.
[21] ARAÚJO F R C, MADUREIRA A L R, SAMPAIO L N. A multicriteria-based forwarding strategy for interest flooding mitigation on named data wireless networking[J]. IEEE Transactions on Mobile Computing, 2023, 22(12): 7000-7013.
[22] ARNOSTI S Z, PIRES R M, BRANCO K R L J C. Evaluation of cryptography applied to broadcast storm mitigation algorithms in FANETs[C]//Proceedings of the International Conference on Unmanned Aircraft Systems. New York: IEEE, 2017: 1368-1377.
[23] PIRES R M, PINTO A S R, BRANCO K R L J C. The broadcast storm problem in fanets and the dynamic neighborhood-based algorithm as a countermeasure[J]. IEEE Access, 2019, 7: 59737-59757.
[24] PATEL A, PATEL N, PATEL R. Defending against wormhole attack in MANET[C]//Proceedings of the 5th International Conference on Communication Systems and Network Technologies. New York: IEEE, 2015: 674-678.
[25] ARAFAT M Y, MOH S. A Q-learning-based topology-aware routing protocol for flying ad hoc networks[J]. IEEE Internet of Things Journal, 2021, 9(3): 1985-2000.
[26] SRINIVAS J, DAS A K, KUMAR N, et al. TCALAS: Temporal credential-based anonymous lightweight authentication scheme for Internet of drones environment[J]. IEEE Transactions on Vehicular Technology, 2019, 68(7): 6903-6916.
[27] HUSSAIN S, CHAUDHRY S A, ALOMARI O A, et al. Amassing the security: An ECC-based authentication scheme for Internet of Drones[J]. IEEE Systems Journal, 2021, 15(3): 4431-4438.
[28] WAZID M, DAS A K, KUMAR N, et al. Design and analysis of secure lightweight remote user authentication and key agreement scheme in internet of drones deployment[J]. IEEE Internet of Things Journal, 2018, 6(2): 3572-3584.
[29] PARK Y, RYU D, KWON D, et al. Provably secure mutual authentication and key agreement scheme using PUF in internet of drones deployments[J]. Sensors, 2023, 23(4): 2034.
[30] ZHANG Y R, HE D B, LI L, et al. A lightweight authentication and key agreement scheme for Internet of Drones[J]. Computer Communications, 2020, 154: 455-464.
[31] CHENG Y Y, XU S Y, ZANG M, et al. LPPA: A

lightweight privacy-preserving authentication scheme for the Internet of drones[C]//Proceedings of the IEEE 21st International Conference on Communication Technology. New York: IEEE, 2021: 656-661.

[32] BANSAL G, SIKDAR B. Secure and trusted attestation protocol for UAV fleets[C]//Proceedings of the IEEE INFOCOM 2022 - IEEE Conference on Computer Communications Workshops. New York: IEEE, 2022: 1-6.

[33] MAENG S J, YAPICI Y, GÜVENÇ İ, et al. Power allocation for fingerprint-based PHY-layer authentication with mmWave UAV networks[C]//Proceedings of the ICC 2021-IEEE International Conference on Communications. New York: IEEE, 2021: 1-6.

[34] JAN S U, ABBASI I A, ALGARNI F. A mutual authentication and cross verification protocol for securing Internet-of-Drones (IoD)[J]. Computers, Materials & Continua, 2022, 72(3): 5845-5869.

[35] KHAN M A, ULLAH I, ALKHALIFAH A, et al. A provable and privacy-preserving authentication scheme for UAV-enabled intelligent transportation systems[J]. IEEE Transactions on Industrial Informatics, 2021, 18(5): 3416-3425.

[36] ABDEL-MALEK M A, AKKAYA K, BHUYAN A, et al. A proxy signature-based swarm drone authentication with leader selection in 5G networks[J]. IEEE Access, 2022, 10: 57485-57498.

[37] AYDIN Y, KURT G K, OZDEMIR E, et al. Group authentication for drone swarms[C]//Proceedings of the IEEE International Conference on Wireless for Space and Extreme Environments. New York: IEEE, 2021: 72-77.

[38] ALLADI T, NAREN, BANSAL G, et al. SecAuthUAV: A novel authentication scheme for UAV-ground station and UAV-UAV communication[J]. IEEE Transactions on Vehicular Technology, 2020, 69(12): 15068-15077.

[39] YAZDINEJAD A, PARIZI R M, DEHGHANTANHA A, et al. Federated learning for drone authentication[J]. Ad Hoc Networks, 2021, 120: 102574.

[40] MAZZO F, TOMASIN S, ZHANG H L, et al. Physical-layer challenge-response authentication for drone networks[C]//Proceedings of the GLOBECOM 2023 - 2023 IEEE Global Communications Conference. New York: IEEE, 2023: 3282-3287.

[41] AKRAM J, AKRAM A, JHAVERI R H, et al. BC-IoDT: Blockchain-based framework for authentication in Internet of drone things[C]//Proceedings of the 5th International ACM Mobicom Workshop on Drone Assisted Wireless Communications for 5G and Beyond. New York: ACM, 2022: 115-120.

[42] TAN Y W, WANG J D, LIU J J, et al. Blockchain-assisted distributed and lightweight authentication service for industrial unmanned aerial vehicles[J]. IEEE Internet of Things Journal, 2022, 9(18): 16928-16940.

[43] YAZDINEJAD A, PARIZI R M, DEHGHANTANHA A, et al. Enabling drones in the internet of things with decentralized blockchain-based security[J]. IEEE Internet of Things Journal, 2020, 8(8): 6406-6415.

[44] FENG C S, LIU B, GUO Z, et al. Blockchain-based cross-domain authentication for intelligent 5G-enabled internet of drones[J]. IEEE Internet of Things Journal, 2021, 9(8): 6224-6238.

[45] KHAN M A, ULLAH I, KUMAR N, et al. An efficient and secure certificate-based access control and key agreement scheme for flying ad-hoc networks[J]. IEEE Transactions on Vehicular Technology, 2021, 70(5): 4839-4851.

[46] CHAUDHARY D, SONI T, VASUDEV K L, et al. A modified lightweight authenticated key agreement protocol for Internet of Drones[J]. Internet of Things, 2023, 21: 100669.

[47] LV Z H, LI Y X, WU J Y, et al. Securing the Internet of drones against cyber-physical attacks[J]. IEEE Internet of Things Magazine, 2022(4): 74-78.

[48] GUO H P, LIU T Y, LUI K S, et al. Secure broadcast protocol for unmanned aerial vehicle swarms[C]// Proceedings of the 29th International Conference on Computer Communications and Networks. New York: IEEE, 2020: 1-9.

[49] HARN L, HSU C, XIA Z. Lightweight and flexible key distribution schemes for secure group communications[J]. Wireless Networks, 2021, 27(1): 129-136.

[50] TANVEER M, KUMAR N, HASSAN M M. RAMP-IoD: A robust authenticated key management protocol for the Internet of Drones[J]. IEEE Internet of Things Journal, 2021, 9(2): 1339-1353.

[51] LI X H, WANG Y W, VIJAYAKUMAR P, et al. Blockchain-based mutual-healing group key distribution scheme in unmanned aerial vehicles ad-hoc network[J]. IEEE Transactions on Vehicular Technology, 2019, 68(11): 11309-11322.

[52] GAI K K, WU Y L, ZHU L H, et al. Blockchain-enabled trustworthy group communications in UAV networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2021, 22(7): 4118-4130.

[53] TAN Y W, LIU J J, KATO N. Blockchain-based key management for heterogeneous flying ad hoc network[J]. IEEE Transactions on Industrial Informatics, 2020, 17(11): 7629-7638.

[54] HAMAMREH J M, FURQAN H M, ARSLAN H. Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey[J]. IEEE Communications Surveys & Tutorials, 2018, 21(2): 1773-1828.

[55] OMRI A, HASNA M O. Physical layer security analysis of UAV based communication networks[C]//Proceedings of the IEEE 88th Vehicular Technology Conference. New York: IEEE, 2018: 1-6.

[56] YE J, ZHANG C, LEI H J, et al. Secure UAV-to-UAV systems with spatially random UAVs[J]. IEEE Wireless Communications Letters, 2018, 8(2): 564-567.

[57] KHAN W U, LAGUNAS E, ALI Z, et al. Opportunities for physical layer security in UAV communication enhanced with intelligent reflective surfaces[J]. IEEE Wireless Communications, 2022, 29(6): 22-28.

[58] LIU C X, QUEK T Q S, LEE J. Secure UAV

communication in the presence of active eavesdropper (invited paper)[C]//Proceedings of the 9th International Conference on Wireless Communications and Signal Processing. New York: IEEE, 2017: 1-6.

[59] ZHANG G C, WU Q, CUI M, et al. Securing UAV communications via joint trajectory and power control[J]. IEEE Transactions on Wireless Communications, 2019, 18(2): 1376-1389.

[60] WU H C, LI H J, WEI Z Q, et al. Secrecy performance analysis of air-to-ground communication with UAV jitter and multiple random walking eavesdroppers[J]. IEEE Transactions on Vehicular Technology, 2021, 70(1): 572-584.

[61] ZHANG H L, HE X F, DAI H Y. Secure UAV communication networks via friendly jamming and bandwidth allocation[C]//Proceedings of the IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops. New York: IEEE, 2020: 894-899.

[62] LI J H, KANG H, SUN G, et al. Physical layer secure communications based on collaborative beamforming for UAV networks: A multi-objective optimization approach[C] //Proceedings of the IEEE INFOCOM 2021 - IEEE Conference on Computer Communications. New York: IEEE, 2021: 1-10.

[63] ZHANG H J, ZHANG J M, LONG K P. Energy efficiency optimization for NOMA UAV network with imperfect CSI[J]. IEEE Journal on Selected Areas in Communications, 2020, 38(12): 2798-2809.

[64] BASTAMI H, LETAFATI M, MORADIKIA M, et al. On the physical layer security of the cooperative rate-splitting-aided downlink in UAV networks[J]. IEEE Transactions on Information Forensics and Security, 2021, 16: 5018-5033.

[65] JANGSHER S, AL-DWEIK A, IRAQI Y, et al. Group Secret Key Generation Using Physical Layer Security for UAV Swarm Communications[J]. IEEE Transactions on Aerospace and Electronic Systems, 2023, 59(6): 8550-8564.

[66] HAN D Q, LI A, LI J W, et al. DroneKey: A drone-aided group-key generation scheme for large-scale IoT networks[C]//Proceedings of the Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2021: 1306-1319

[67] QI J Y, GAO T H, DENG X Y, et al. A pseudonym-based certificateless privacy-preserving authentication scheme for VANETs[J]. Vehicular Communications, 2022, 38: 100535.

编 辑 叶 芳