**DOI**:10.20189/j.cnki.CN/61-1527/E.202604002

# 基于网络攻击技术的分布式无人机蜂群反制方法综述

张艺驰,王　乐,高久安,刘枘池,席建祥*
(火箭军工程大学,西安 710025)

**摘　要**:随着现代控制技术向无人化与集群化方向延伸,分布式无人机蜂群凭借部署灵活与适应性强的优势在多个领域得到广泛应用。然而,蜂群技术的滥用对低空领域构成的威胁日益严峻,分布式无人机蜂群对现有低空防御体系提出了前所未有的挑战。基于此,本文对基于网络攻击技术的分布式无人机蜂群反制方法展开系统性综述。首先,对非合作分布式无人机蜂群进行概述,指出无人机蜂群对现有反制体系构成的严峻威胁。其次,从经典蜂群反制方法切入,分别从物理反制与电磁反制 2 个方面阐述现有蜂群反制技术,梳理各反制手段的优缺点及适用场景,并引出基于网络攻击的蜂群反制方法的实施方式。再次,通过概述当前网络攻击方法在分布式蜂群反制中的理论实践研究,重点阐述了基于拒绝服务攻击、欺骗攻击与诱导攻击的反制方法的作用途径、机制原理及研究进展,并对 3 种反制方法的优势与局限性进行分析。最后,结合分布式蜂群技术与网络攻击方法的研究现状,总结现有蜂群反制方法的局限性,探讨基于网络攻击的分布式无人机蜂群反制方法的未来发展趋势。通过对现有研究与技术方法的梳理,以期为非合作分布式无人机蜂群反制领域的研究提供参考,推动我国无人低空防御体系的建设。

**关键词**:分布式蜂群;集群反制;无人机;网络攻击方法;诱导反制
**中图分类号**:E91;V279　　**文献标志码**:A　　**开放科学标识码(OSID)**:
**文章编号**:2097-2741(2026)04-0022-16

听语音　聊科研　与作者互动

随着无人系统理论的快速发展,无人机控制技术取得了显著进步,群系统理论的发展进一步推动了无人机集群化的进程,无人机蜂群正在重塑低空经济生态与军事对抗形态[1-2]。分布式无人机蜂群是由大量具有一定自主能力的小型无人机构成,通过分布式网络架构实现协同作业的智能集群系统。其核心特征是分布式通信网络,每架无人机均可进行独立计算决策并通过分布式通信网络与其他无人机进行通信,进而涌现出类似蜂群的群体智能。分布式无人机蜂群以其可重构性、强抗毁性和鲁棒自愈性等特点成为当下群体智能领域的研究热点,具有广阔的应用前景。

然而,随着应用场景的拓展,分布式无人机蜂群在带来巨大效益的同时,其安全隐患也日益凸显。非合作无人机蜂群,即未经授权、目的不明或带有敌意的无人机蜂群,对低空领域的安全构成了现实且严峻的威胁。其不仅会扰乱空域管理,还可能进行渗透抵近,对关键设施设备和重要集会活动发起低成本、高隐蔽的攻击,潜在威胁巨大[3]。乌克兰策划实施的“蛛网行动”便是这一趋势的鲜明例证,充分暴露了非合作无人机蜂群作为非对称作战力量所带来的巨大威胁[4]。

分布式无人机蜂群的颠覆性威胁给现有防空体系带来了前所未有的严峻挑战,如何实现蜂群的有效反制已成为未来体系对抗研究的重要课题[5]。根据反制作用途径,当前的蜂群反制方法主要可分为物理反制技术与电磁反制技术两类。然而,这两类成熟的蜂群反制技术对分布式无人机蜂群的适

**收稿日期**:2026-01-13　　**修回日期**:2026-04-08　　**录用日期**:2026-04-17
**基金项目**:国家自然科学基金(U23B2064,62176263,62103434);陕西省自然科学基础研究计划青年项目(2025JC-YBQN-824)
**第一作者**:张艺驰(2002—),男,硕士研究生,主要从事无人机蜂群协同及反制技术研究。
*通信作者:席建祥(1981—),男,教授,主要从事群系统协同控制与智能集群反制研究。

**引用格式**:张艺驰,王乐,高久安,等. 基于网络攻击技术的分布式无人机蜂群反制方法综述[J]. 火箭军工程大学学报,2026,40(4):22-37. *ZHANG Yichi*,*WANG Le*,*GAO Jiuan*,*et al*. *Review on cyber-attack-based countermeasures for distributed unmanned aerial vehicle swarms* [J]. *Journal of Rocket Force University of Engineering*,*2026*,*40*(*4*):*22-37*.

用性有限。这是由于分布式蜂群具有分布式交互网络，呈现去中心化特征，即使蜂群内个别无人机遭到打击，整个蜂群的任务执行仍不受根本影响。因此，亟需探索适用于分布式无人机蜂群的新型反制方法。当前，已有研究将网络攻击方法应用于分布式无人机蜂群的反制实践中[6]。但需要说明的是，本文所讨论的网络攻击方法并非立足于攻击方视角，而是指反制系统采用网络攻击手段，对非合作分布式无人机蜂群实施反制的主动防御策略，其本质仍属于蜂群反制方法的范畴。

鉴于此，本文旨在对基于网络攻击的蜂群反制方法进行系统性综述。首先，介绍当前经典且成熟的两类蜂群反制技术，对比分析各种反制方式的优缺点及适用场景；其次，从理论层面阐述基于网络攻击的蜂群反制方法，剖析各种反制信号的设计原理与作用机制；最后，结合当前研究进展，探讨基于网络攻击的蜂群反制方法的发展趋势，以期为分布式无人机蜂群反制领域的研究与实践提供参考。

## 1　经典蜂群反制方法

经典的无人机蜂群反制方法大多针对蜂群系统中的无人机个体展开，通过对个体的逐个反制实现对蜂群的整体反制，这也是当前多数蜂群反制设备采用的方法。根据蜂群反制策略的不同，可将蜂群反制技术分为物理反制技术与电磁反制技术，下面分别对这两类反制技术进行介绍。

### 1.1　物理反制技术

物理反制技术是通过物理手段对蜂群进行拦截或摧毁，使其丧失任务能力，进而实现反制效果。根据作用效果和具体实施手段，物理反制技术可分为物理摧毁、捕获拦截与以群制群，3 种反制手段的对比如表 1 所示。

**表 1　物理反制技术对比**

**Table 1　Comparison of physical countermeasure technologies**

| 物理反制技术 | 反制机理 | 技术复杂度 | 反制效果 | 优点 | 缺点 | 适用场景 |
|---|---|---|---|---|---|---|
| 物理摧毁 | 通过动能或定向能毁伤硬件 | 动能打击技术成熟；定向能打击技术复杂度较高 | 毁伤彻底 | 反制效果直接 | 反制效费比较低；可能造成附带伤害 | 适用于对小规模、高价值无人机目标的精准打击 |
| 捕获拦截 | 通过拦捕网和飞爪等设备进行物理捕获 | 地面捕获技术简单；空中协同网捕技术复杂度较高 | 实现无人机完整回收 | 无附带伤害，可回收目标无人机 | 捕获效率有限；对机动性强的蜂群响应不足 | 适用于小规模蜂群或关键无人机的精准回收 |
| 以群制群 | 利用己方无人机群采用撞击、合围等方式进行打击 | 协同控制与博弈决策技术复杂度高 | 蜂群层面的系统对抗 | 可通过智能算法优化战术策略，战术选择丰富 | 对己方蜂群规模、协同能力及计算资源要求高；会造成己方无人机损耗 | 适用于大规模蜂群对抗 |

#### 1.1.1　物理摧毁

物理摧毁是通过动能打击或定向能打击对来袭无人机的硬件设施进行物理毁伤，使其丧失飞行动力或遂行任务能力。动能打击是依托防空导弹或高炮等防空武器，通过爆炸破片或直接命中实现对无人机的毁伤，技术成熟度高，但成本较高且对大规模蜂群的反制效费比不足[7]。定向能打击是利用高能激光或高功率微波破坏无人机的电路系统与电子元件，具有弹药无限且单次打击成本低等优势，但易受环境条件影响，便携性较为欠缺[8]。物理摧毁的一个难点是如何实现反制资源的高效分配，针对此问题，文献[9]提出了一种精确物理模型与多智能体强化学习相结合的方法，解决了面对大规模非合作无人机集群时的动态资源目标分配问题。物理摧毁反制手段的优势在于反制效果直接，能够彻底消除非合作无人机的威胁，但其效费比较低、难以应对大规模蜂群，且可能造成附带损害。总体而言，该手段更适用于小规模、高价值目标的精准打击，难以应对分布式蜂群的系统性威胁。

#### 1.1.2　捕获拦截

捕获拦截是通过拦捕网、飞爪或多无人机协同网捕对无人机蜂群进行捕获回收，进而实现蜂群反制。根据实施平台的差异，捕获拦截可分为地面捕获与空中拦截两类。地面捕获是依托固定或车载发射装置，通过弹射等方式将拦捕网或飞爪等设备投射至目标无人机的飞行路径[10]。空中拦截则是

通过无人机搭载网捕装置,利用视觉辅助与无人机的快速机动能力抵近目标无人机实施捕获拦截,可以有效弥补地面捕获在作用距离与机动性方面的短板[11]。为进一步提升对蜂群的反制效能,多无人机协同网捕成为重要研究方向,可以通过多无人机协同作业实现对多个目标无人机的连续或同时捕获[12]。捕获拦截的优势在于能够实现无人机的完整回收,便于后续分析与取证,同时避免了物理摧毁可能带来的附带损害。然而,该反制手段对技术要求较高,同时面对大规模蜂群时捕获效率有限。因此,捕获拦截更适用于对小规模蜂群或关键无人机的精准反制。

1.1.3 *以群制群*

以群制群是利用己方无人机群与来袭蜂群进行空中对抗博弈,采用撞击、合围等方式对非合作无人机蜂群进行打击。根据对抗策略的不同,可分为直接对抗与策略博弈两类。直接对抗依托己方低价值无人机的机动性与数量优势,通过撞击直接破坏非合作蜂群的结构完整性,即集群式动能打击[13]。策略博弈则是充分发挥无人机群的协同特性,借助智能算法将反制过程建模为动态对抗博弈,通过优化决策在局部实现以多胜少、以强制弱的效果,进而实现蜂群反制[14-15]。以群制群的优势在于能够实现蜂群层面的系统对抗,并可通过智能算法不断优化战术策略,反制过程中的战术选择较为丰富。然而,该反制手段对己方蜂群的规模、协同能力及计算资源均有较高要求,且会造成己方无人机损耗,反制成本高。

## 1.2 电磁反制技术

电磁反制技术是典型的电子对抗手段,通对电磁信号对无人机蜂群进行干扰、欺骗或控制,从而达到反制目的。电磁反制技术主要针对的是蜂群中无人机的无线网络、数据链路和卫星导航信号,根据作用手段可分为无线电压制、数据链入侵和导航干扰,其对比如表2所示,下面对3种反制手段分别进行分析。

**表2 电磁反制技术对比**

**Table 2 Comparison of electromagnetic countermeasure technologies**

| 电磁反制技术 | 作用途径 | 反制机理 | 技术复杂度 | 反制效果 | 优点 | 缺点 | 适用场景 |
|---|---|---|---|---|---|---|---|
| 无线电压制 | 无人机与地面站之间的通信链路 | 发射同频段大功率信号阻断通信链路 | 较低 | 迫使无人机自主降落或返航 | 原理简单、技术成熟 | 难以应对跳频通信;对自主飞行蜂群无效;电磁辐射较大 | 适用于依赖实时遥控的蜂群或需快速反制场景 |
| 数据链入侵 | 蜂群数据链路 | 破解控制指令,伪造反制指令并入侵数据链路 | 高 | 实现对蜂群的接管与引导 | 可精确控制蜂群飞行,附带损伤小 | 技术难度大;不适用于无指控链路的蜂群 | 适用于通信协议已被破解的特定蜂群 |
| 导航干扰 | 卫星导航系统 | 压制式:发射干扰信号抬高噪声基底<br>欺骗式:发送错误导航信号 | 压制式:较低<br>欺骗式:较高 | 压制式:蜂群导航系统失效<br>欺骗式:欺骗蜂群飞行轨迹 | 压制式:实现简单,反制效果好<br>欺骗式:隐蔽性强且反制效果可控 | 压制式:易被检测机制察觉<br>欺骗式:实现技术复杂,需获取蜂群导航参数 | 压制式:适用于依赖导航的蜂群<br>欺骗式:适用于高价值目标或需隐蔽反制的场景 |

1.2.1 *无线电压制*

无线电压制是利用遥控链路中信号的公开性,获取并破解其射频遥控信号,而后针对性产生并发射相同频段的大功率信号,压制原射频信号,使无人机无法接收指令信息。当遥控通信中断后,无人机将触发其保护机制而自主降落或返航,从而实现对无人机的反制[16]。针对无人机蜂群,文献[17]设计了一种全向蜂群反制模型,通过构建可覆盖三维空间的反蜂群无人机模型,依靠三维电磁屏蔽与集群协同打击模式,能够有效应对多方向来袭的蜂群威胁。当前蜂群多采用“跳频”通信,传统无线电压制技术难以实时响应跳变频率。因此,需增强压制覆盖能力并发展快速动态干扰技术。无线电压制原理相对简单、技术易于实现、设备可靠性较高,是当前应用最为广泛的蜂群反制手段,其局限性在于无法有效反制具备自主飞行能力的蜂群,且大功率电磁信号可能对环境及人体造成影响。

1.2.2 *数据链入侵*

数据链是蜂群重要的信息指令传输通道,无人机通过数据链路实现指令信息的接收与实时数据的回传。数据链入侵是采用技术手段破解无人机的数据链信息,依据这些信息仿照生成伪造的

反制指令，随后以更高功率入侵数据链，从而破坏蜂群的控制权。相较于无线电压制技术，数据链入侵对反制技术的要求更高，不仅需要破解射频信号的工作频段，还需掌握数据链的信息参数。数据链入侵能够有效避免反制过程中的二次伤害，且反制信号对周围设备正常运行的附带损伤较小。然而，随着蜂群数据链的安全防护越发完善，数据链入侵的技术难度显著增大。此外，该手段难以应对“跳频”等抗干扰通信方式，对于不存在指控数据链的分布式无人机蜂群，该手段很难取得理想的反制效果。

1.2.3　导航干扰

无人机当前主要采用的导航技术有卫星导航、惯性导航与视觉导航[18-19]，其中，卫星导航是其主要导航手段[20]，只需对卫星导航实施干扰就可使无人机导航系统出现异常。因此，本节讨论的导航干扰主要针对卫星导航展开。导航信号到地面时十分微弱，因此导航干扰易于实现[21]。根据干扰原理的不同，可以将导航干扰分为压制式导航干扰与欺骗式导航干扰两类[22]。

1）压制式导航干扰

压制式导航干扰的原理是通过定向天线或全向天线发射与导航信号频段相同的干扰信号，抬高接收机工作频段内的噪声基底，直接破坏无人机接收机的接收能力。由于压制式干扰技术简单且效果良好，美军方始终认为其是蜂群面临的主要威胁[23]。根据信号样式，可将压制式导航干扰分为噪声干扰、扫频干扰、脉冲干扰和匹配频谱干扰等，各种干扰信号的特点如表 3 所示。根据导航与干扰信号带宽之间的关系，可分为窄带干扰和宽带干扰[24]。窄带干扰即瞄准式干扰，指单个频段内干扰信号带宽小于导航信号带宽的 10%。由于窄带干扰信号带宽较小，因此易于实现且在单个频段内能产生较好的干扰效果，但其对分布式或多频点接收机的干扰能力有限，且在接收机端易被滤除。宽带干扰即阻塞式干扰，是指单个频段内干扰信号的带宽大于导航信号带宽的 10%。宽带干扰能够对多个频段内的导航信号同时实施干扰且不易被滤除，但宽带干扰对于干扰信号的功率有较高要求，其破坏性不如窄带干扰。

**表 3　压制式导航干扰信号特点**

**Table 3　Characteristics of suppression navigation interference signals**

| 信号样式 | 信号特点 | 技术复杂度 | 隐蔽性 |
|---|---|---|---|
| 噪声干扰 | 将较高功率的随机噪声调制到导航信号频率 | 简单 | 一般为宽带干扰，不易被滤除；部分频带噪声为窄带干扰，易被检测到 |
| 扫频干扰 | 逐渐变化干扰信号的中心频点，实现干扰信号的周期性扫描 | 简单 | 不易被检测机制检测滤除 |
| 脉冲干扰 | 在瞬时内产生较高功率的干扰信号 | 简单 | 信号特征较为明显，易被发现并滤除 |
| 匹配频谱干扰 | 干扰信号与蜂群接收机的功率谱密度相同 | 困难 | 与真实导航信号特征相似，不易被检测发现，隐蔽性较好 |

2）欺骗式导航干扰

欺骗式导航干扰是利用导航信号的公开性，向蜂群发送我方导航信号，使接收机的跟踪回路被我方信号欺骗。虽然该反制手段的技术复杂度更高且难以实现范围打击，但其优点是隐蔽性较强，对蜂群中高价值无人机的威胁较大。比如，伊朗通过该手段成功对美国的 RQ-170 无人机实现欺骗诱捕[25]。根据欺骗信号的作用效果，可将其分为时间欺骗型与位置欺骗型。时间欺骗型通过欺骗导航系统的时间影响蜂群的任务执行。文献[26]提出了基于修正卫星位置、修正伪距及二者联合的 3 类时间欺骗算法，能够实现时间欺骗的目的且欺骗时间可控。为进一步满足时间欺骗策略多样化的需求，Gao 等[27]提出了阶跃型与慢变型时间欺骗算法，阶跃型算法能够实现瞬时欺骗，但易被检测到；慢变型算法的平均误差较大，但提高了导航欺骗的隐蔽性。时间欺骗能够破坏协同效果，但反制效果相较位置欺骗型有所欠缺[28]。位置欺骗型通过生成并发送虚假的导航定位信号，使蜂群偏离预定任务轨迹[29]。为提高位置欺骗的隐蔽性，文献[30]提出了一种逐点偏移式位置欺骗方法，在不引发检测机制的前提下实现定向欺骗。这种欺骗位置的计算通常依赖于蜂群的参考轨迹，在实际情况中这些参数难以获取，因此，需要设计新型位置欺骗

策略[31]。

总之，针对非合作无人机蜂群的反制，现有的技术思路聚焦于对蜂群个体逐个实施反制，通过大量个体的失效实现对蜂群整体的反制。然而，这种方法不仅效率低，在面对大规模蜂群时难以达到理想的反制效果。对于分布式无人机蜂群而言，即便部分无人机被杀伤，其余个体仍可继续执行任务，对蜂群的协同效能削弱有限。因此，将反制重点转向蜂群的分布式通信网络成为新的研究方向，即基于网络攻击的蜂群反制方法。该方法通过将反制信号注入蜂群个体或机间通信链路，利用分布式交互网络的传播特性将反制信号扩散至整个蜂群，从而实现以点带面的整体反制效果。需要指出的是，该反制方法的关键在于如何设计有效的反制信号，其物理实现可依托电磁反制技术，前述几种电磁反制手段可作为基于该方法的具体实施方式。

## 2 基于网络攻击的蜂群反制理论

网络攻击是指攻击方利用通信网络对蜂群系统发起攻击行为，即通过窃取或干扰节点间的正常通信来破坏系统的整体协同效能。分布式无人机蜂群的关键在于分布式通信网络，而网络攻击方法恰好能够针对通信网络实施系统层面的破坏。因此，基于网络攻击方法进行分布式蜂群反制研究得到广泛关注[32-33]。

网络反制方法根据作用途径，可分为针对通信链路与针对蜂群节点两类。针对通信链路是指通过反制信号直接入侵通信网络以削弱蜂群的协同效能，而针对蜂群节点则是指通过干扰节点无人机的状态参数，利用分布式通信将反制信息在蜂群内扩散，进而实现蜂群系统的反制。如图 1 所示，文献[34]根据网络攻击实施原理，将其分为窃听攻击、拒绝服务(denial of service，DoS)攻击和虚假数据注入(false data injection，FDI)攻击等，分别通过破坏数据传输的保密性、可用性与完整性实现对系统功能的破坏。在实际蜂群反制场景中，非合作分布式蜂群作为威胁方，其通信信息通常难以被获知，即便能够窃听到蜂群通信数据，若不进行后续干预，也难以达到理想的反制效果，因此，针对通信数据保密性进行破坏的窃听攻击在蜂群反制中效果有限。基于上述分析，重点讨论基于 DoS 攻击与基于 FDI 攻击的反制机制，从理论层面深入剖析这些反制方法的内在机理，阐明反制方如何通过破坏蜂群系统通信数据的可用性与完整性，有效削弱蜂群的协同效能。

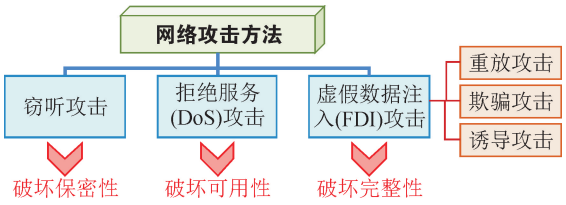


图 1 网络攻击方法研究

Fig. 1 Research on cyber-attack methods

### 2.1 基于 DoS 攻击的蜂群反制方法

DoS 攻击是网络攻击的常见形式，其原理是通过发送大量垃圾数据包来占用或消耗网络通道资源，达到阻止网络节点与邻居之间进行通信交互的目的，主要破坏的是系统通信数据的可用性[35]。针对无人机蜂群分布式交互网络，基于 DoS 攻击的反制方法能够有效阻断蜂群中各无人机之间通信信道传输的部分或全部信息，破坏协同信息的可用性，进而导致蜂群无法形成期望编队，实现无人机蜂群的反制[36]。

在时间$[t_0,t)$中，$t_0$ 为开始时刻，不失一般性，令 $t_0=0$，从反制信号发生时刻和反制持续时间的角度可将其描述为[37]

$$D_n \triangleq \{h_0\} \bigcup [h_n+\tau_n) \tag{1}$$

$$A_n = h_{n+1}-h_n, n \in \mathbb{N}_0 \tag{2}$$

式中：$h_n(n \in \mathbb{N}_0$ 且 $h \geqslant 0)$ 和 $\tau_n \geqslant 0$ 分别表示第 $n$ 次反制的发生时刻和持续时间；$\{h_n\}$ 表示反制开关切换序列；$\mathbb{N}_0$ 为自然数集合。$D_n$ 为第 $n$ 次反制的时间间隔，且反制时长为 $\tau_n$；$A_n$ 表示任意两次连续反制触发之间的时间间隔。如果 $\tau_n<A_n$，在 $A_n$ 和 $\tau_n$ 都为固定的常数时，该反制模型为周期性反制[38]，否则，模型为非周期性反制[39]。实际工程应用中，反制方通常在能量有界且时间受限的条件下实施基于 DoS 攻击的蜂群反制，因此需要满足如下假设[40]。

假设一（频率约束）：对于任意时间区间$[t_0,t_1]$，令 $n_1(t_0,t_1)$ 表示时间区间内 DoS 攻击发生的总次数，存在常数 $\eta_1 \geqslant 0$ 和 $f \geqslant 0$ 使得 $n_1(t_0,t_1)$ 满足下列不等式：

$$n_1(t_0,t_1) \leqslant \eta_1+(t_1-t_0)f \tag{3}$$

式中：$\eta_1$ 为 DoS 攻击容许的突发次数，$f$ 为 DoS 攻击在单位时间内平均发生频次的上界。

假设二（持续时间约束）：对于任意时间区间$[t_0,t_1]$，令 $n_2(t_0,t_1)$ 表示时间区间内 DoS 攻击占

据通信信道的总时长，存在常数 $\eta_2 \geqslant 0$ 和 $0 \leqslant T \leqslant 1$ 使得 $n_2(t_0,t_1)$ 满足下列不等式：

$$n_2(t_0,t_1) \leqslant \eta_2 + (t_1 - t_0)T \tag{4}$$

式中：$\eta_2$ 为 DoS 攻击容许的额外持续时间，$T$ 为攻击总时长在整个时间区间中所占比例的上界。

然而，上述研究均认为反制的目标是全部通信通道，即在持续时间内整个蜂群的通信网络是完全断开的[41-42]。实际上该反制方法也可以以独立的方式影响网络中的某个或部分通信通道。针对由 $N$ 个无人机组成的蜂群系统，根据反制目标不同，可建立如下反制信号模型：

$$\tilde{d}_j^i(t) = a_{ij}(t) d_j^i(t) \tag{5}$$

式中：$i,j = 1,2,\cdots,N$ 且 $i \neq j$；$d_j^i(t)$ 表示无人机 $j$ 向无人机 $i$ 在 $t$ 时刻发出的原始数据；$\tilde{d}_j^i(\mathrm{t})$ 为无人机 $i$ 在 $t$ 时刻接收到无人机 $j$ 的数据；$a_{ij}(t) = \{0,1\}$，其中，$a_{ij}(t) = 0$ 表示在 $t$ 时刻 $j$ 到 $i$ 的通信通道受到反制，$a_{ij}(t) = 1$ 则表示在 $t$ 时刻 $j$ 到 $i$ 的通信通道未受到反制。当 $\sum_{i,j \in N, i \neq j} a_{ij}(t) = 0$ 时，系统在 $t$ 时刻受到全通道反制；当 $\sum_{i,j \in N, i \neq j} a_{ij}(t) > 0$ 且 $\prod_{i,j \in N, i \neq j} a_{ij}(t) = 0$ 时，系统在 $t$ 时刻受到多通道反制；当 $\prod_{i,j \in N, i \neq j} a_{ij}(t) = 1$ 时，系统在 $t$ 时刻未受到反制[43]。因此，一些学者认为基于 DoS 攻击的反制可以随机发生，或者服从某种先验概率分布[44]。文献[45-46]将 $a_{ij}(t)$ 视作随机变量并且服从伯努利分布和马尔科夫过程。文献[47]从图拓扑的角度出发，将随机多通道的交互通信建模为随机拓扑切换，并使用马尔科夫过程 $S = \{1,2,\cdots,s\}$ 表示所有可能得到的拓扑有限状态空间。令 $\Upsilon = [\gamma_{pq}]_{1 \leqslant p,q \leqslant S}$ 为连续时间马尔可夫链的转移速率矩阵，给出随机多通道反制信号下一种拓扑切换到另一种拓扑的概率[48]，其可表示为

$$\begin{aligned} P_{pq}(t) &= \mathrm{Prob}\{r(t+h) = q \mid r(t) = p\} \\ &= \begin{cases} \gamma_{pq} h + o(h), & p \neq q \\ 1 + \gamma_{pq} h + o(h), & p = q \end{cases} \end{aligned} \tag{6}$$

式中：$r(t)$ 为切换信号，转移速率矩阵 $\Upsilon$ 行和为 0，即 $\sum_{q \in S} \gamma_{pq} = \gamma_{pq} + \sum_{q \in S, q \neq p} \gamma_{pq} = 0$；$\gamma_{pq}$ 是图拓扑 $p$ 到 $q$ 的转移速率，当 $p \neq q$ 时，$\gamma_{pq} \geqslant 0$，当 $p = q$ 时，$\gamma_{pq} = -\sum_{q \in S, q \neq p} \gamma_{pq} \leqslant 0$；$o(h)$ 表示 $h$ 的高阶无穷小。由此可知，基于 DoS 攻击的反制模型的建立主要与持续时间、反制频率与反制目标等参数指标相关，这些参数指标在不同方面影响着无人机蜂群的协同信息交互和编队形成[49]。

当反制方对非合作分布式无人机蜂群发起全通道 DoS 反制时，在反制持续时间内，被反制的蜂群个体不再接收邻居信息，图拉普拉斯矩阵 $\boldsymbol{L} = \boldsymbol{0}$，无人机均按照自身特性运动，此时失去交互能力的蜂群可能无法形成期望编队；在反制间歇时间内，假如无人机之间可以重新建立通信连接且增益矩阵 $\boldsymbol{K}$ 能够使蜂群编队收敛，此时在协同控制协议作用下，蜂群能够恢复编队并仍按既定轨迹运动，否则，蜂群依然无法形成期望编队[50]。当反制方对蜂群发起多通道 DoS 反制，部分蜂群个体之间通信链路被中断，此时在反制信号作用下蜂群通信拓扑结构在有限状态空间内随机切换，图拉普拉斯矩阵 $\boldsymbol{L}$ 相应发生变化，原有设计用来维持编队稳定的增益矩阵 $\boldsymbol{K}$ 可能无法适应 $\boldsymbol{L}$ 的变化，因此蜂群编队可能无法形成[51]，进而达到反制蜂群的目的。

综上，基于 DoS 攻击的蜂群反制方法通过向蜂群交互网络发送大量垃圾数据破坏分布式网络的可用性，阻塞正常分布式通信数据的传输，从而削弱蜂群协同效能，实现反制目的。其优点在于实现技术相对简单，垃圾数据无需精心设计，且无需解析蜂群的通信协议，普适性较好，能够迅速瓦解蜂群的编队保持与协同能力。然而，由于需要持续或间断向蜂群发送大量数据，在反制方资源有限时难以维持长期有效的反制效果。同时，大量数据的阻塞易被蜂群频谱监测或入侵检测系统发现，反制隐蔽性不足。此外，该方法的反制效果表现为蜂群中部分无人机因通信中断脱离原蜂群，但难以改变蜂群的整体运动轨迹，仍会有部分无人机沿预定飞行轨迹执行任务。因此，该反制方法适用于对依赖实时通信蜂群的快速反制场景，但难以应对自主性和鲁棒性较高的蜂群。

### 2.2　基于 FDI 攻击的蜂群反制方法

FDI 攻击是向分布式无人机蜂群的通信链路或蜂群内无人机的传感器－控制器、控制器－执行器通道注入虚假数据，并利用蜂群的分布式交互特性将虚假数据扩散至整个蜂群，进而实现对非合作蜂群的反制[52]。与破坏数据可用性的 DoS 攻击不同，FDI 攻击的核心目标是破坏蜂群通信数据的完整性，反制方通过访问无人机的物理组件或通信通道，篡改控制数据与测量数据。根据虚假数据类型的不同，FDI 攻击可分为重放攻击、欺骗反制与诱导反制。重放攻击通过截取蜂群传输的部分数据，并

持续向蜂群的通信网络重复注入，以达到干扰蜂群内无人机正常通信的目的[53]。然而，在现实反制场景中，由于蜂群的安全保护机制较为完善，完整截取通信数据较为困难，故重放攻击在蜂群反制的实际应用中难以奏效。因此，下面主要对欺骗反制与诱导反制进行详细介绍。

2.2.1 欺骗反制

基于欺骗攻击的反制方法是在蜂群原有通信数据的基础上，由反制方另行生成与蜂群通信数据格式相同的欺骗数据，并将欺骗数据注入蜂群中，从而干扰蜂群的任务执行[54]。被注入或接收到欺骗数据的无人机会脱离原蜂群编队，同时受分布式通信网络作用，蜂群的整体运动轨迹也会偏离原任务轨迹。反制信号的设计目标在于，对蜂群检测机制与保护机制保持隐蔽性的前提下，最大化蜂群实际运动轨迹与原任务轨迹之间的偏差，从而对蜂群系统的协同效能造成最大程度的破坏[55]。

相较于DoS，基于欺骗攻击的蜂群反制策略形式更加多样，根据欺骗信号的注入途径可分为两类。一是直接入侵蜂群的通信链路，篡改无人机之间的通信数据，从而实现欺骗信号在蜂群内的扩散。该方式的优点是反制效果作用迅速，能够快速完成欺骗信号的传播，但是由于蜂群的通信链路通常配备较为完善的保护机制，因此，反制信号的直接注入有一定挑战性[56]。二是入侵蜂群中一架或多架无人机的传感器－控制器或控制器－执行器通道，修改无人机的实时状态，进而利用分布式通信网络将篡改后的错误状态传递至整个蜂群，使其整体混乱并偏离任务目标。该方式的优点是反制信号的注入相对容易，可采用导航欺骗或电磁耦合等技术实现，但其反制效果受限于蜂群的拓扑结构，需准确识别关键节点才能实现较好的反制效果[57-58]。

1)针对通信链路的欺骗反制方法

分布式无人机蜂群通信链路的频段多为民用公开。利用这一特性，采用针对蜂群通信链路的欺骗反制方法，可直接将反制信号注入蜂群的分布式网络中而无需对节点无人机进行反制，这样可以实现欺骗数据在蜂群内的快速扩散，减少蜂群网络拓扑对反制效果的影响。根据注入通信链路的反制信号特性，可将其分为加性反制信号、乘性反制信号和替换反制信号。

加性反制信号的特点是仅在蜂群原通信信号的基础上叠加经过设计的欺骗反制信号，反制方无需掌握蜂群通信数据的具体信息，可操作性较强。加性反制信号可描述为[59]

$$\tilde{s}_{ij}(t)=s_{ij}(t)+s_{ij}^{a}(t) \tag{7}$$

式中：$s_{ij}(t)$表示蜂群通信链路中无人机$i$向无人机$j$传输的正常通信信号；$s_{ij}^{a}(t)$表示传输过程中注入的欺骗反制信号；$\tilde{s}_{ij}(t)$表示无人机$j$最终接受到由无人机$i$传输的信号。

乘性反制信号通过对蜂群通信链路中的正常信号进行放大或缩小，干扰蜂群内无人机的分布式交互，从而实现反制。由于乘性反制信号是在正常通信信号基础上进行调整，而非向蜂群中引入外部信号，因此不易被蜂群检测机制发现，反制隐蔽性较好。乘性反制信号通常可描述为[60]

$$\tilde{s}_{ij}(t)=c_{ij}(t)s_{ij}(t) \tag{8}$$

式中：$c_{ij}(t)$表示欺骗信号被放大或缩小的时变比例因子。由于加性反制信号与乘性反制信号均为线性反制信号，因此，可将其用统一的线性欺骗模型描述为

$$\tilde{s}_{ij}(t)=c_{ij}(t)s_{ij}(t)+s_{ij}^{a}(t) \tag{9}$$

替换反制信号则是完全用反制信号对蜂群通信链路中的正常通信信号进行覆盖，首先阻断正常通信信号的传输，随后用经过设计的反制信号进行替换。由于通信信号完全由反制方给定，因此该信号的反制效果显著，反制策略灵活多样，但对反制技术要求较高。替换反制信号模型可描述为

$$\tilde{s}_{ij}(t)=r_{ij}(t) \tag{10}$$

式中：$r_{ij}(t)$表示在无人机$i$向无人机$j$传输的通信链路上进行替换的预设反制信号。由于替换反制信号也可用线性模型进行描述，综上，可将上述3种反制信号转化为统一的线性反制模型，该模型可描述为

$$\tilde{s}_{ij}(t)=c_{ij}(t)s_{ij}(t)+\underbrace{s_{ij}^{a}(t)+\left[r_{ij}(t)-c_{ij}(t)-c_{ij}(t)s_{ij}(t)-s_{ij}^{a}(t)\right]}_{s_{ij}^{a}(t)} \tag{11}$$

2)针对蜂群节点的欺骗反制方法

无人机的控制回路是由传感器获取信息，送至控制器进行控制指令的生成并最终由执行器进行作用。因此，针对蜂群节点的欺骗反制主要是对无人机传感器－控制器通道的信息与控制器－执行器通道的控制指令进行欺骗。针对无人机的内部通道(传感器－控制器通道与控制器－执行器通道)，无论反制信号是状态信息还是控制指令，线性

反制信号均可表示为[61]

$$\tilde{f}_i(t)=f_i(t)+\sigma_i(t)f_i^{\mathrm{a}}(t) \tag{12}$$

式中：$f_i(t)$表示无人机 $i$ 的内部通道中正常的信息或指令；$f_i^{\mathrm{a}}(t)$表示注入无人机 $i$ 的反制信息或反制指令；$\sigma_i(t)$表示时变反制信号标志，$\sigma_i(t)=1$ 时表示无人机 $i$ 受到反制，$\sigma_i(t)=0$ 则表示无人机 $i$ 未遭受反制。当对无人机的传感器－控制器通道实施反制时，$\tilde{f}_i(t)$表示无人机 $i$ 控制器最终接受到的状态参数；当对无人机的控制器－执行器通道实施反制时，$\tilde{f}_i(t)$则表示为执行器最终的控制指令。

针对蜂群节点内部通道的反制策略，学者们开展了广泛研究。针对传感器－控制器通道，相较于理想反制对象，文献[62]研究了传感器数据欺骗情况下不确定切换非线性多智能体系统的一致性问题，使反制对象更具一般性，反制场景更为广泛。需要指出的是，传感器信号欺骗反制方法的实现方式相对简单，但无人机状态偏差的变化易被其状态估计器发现，反制隐蔽性不足。相较于传感器欺骗反制方法，针对执行器的欺骗反制方法直接对控制指令进行篡改，欺骗效果更显著，且不易被察觉，隐蔽性更好。针对控制器－执行器通道，文献[63]研究了执行器遭到欺骗信号时，非线性随机多智能体系统的领导跟随一致性问题，拓展了相应蜂群反制理论的实际应用场景。

基于上述研究，部分学者考虑将传感器欺骗反制方法与执行器欺骗反制方法相结合，既能弥补传感器反制隐蔽性不足的缺陷，又能提升蜂群反制的成功率，丰富反制策略选择[64]。文献[65]设计了双通道随机切换欺骗反制，欺骗信号可在传感器－控制器通道与控制器－执行器通道之间随机切换，大大提高了反制的成功率。进一步地，文献[66]考虑将欺骗信号同时注入 2 个通道，反制方可在数据到达控制器之前对传感器数据进行修改，也可在数据到执行器之前篡改控制指令。此外，将多种网络攻击方法耦合，同步或异步混合作用于分布式无人机蜂群以实施反制也是当前的研究热点[67-68]。

当反制方向蜂群中的多架无人机注入欺骗信息时，蜂群会分化为合作无人机（正常节点）与间谍无人机（反制节点），此类问题即为经典的拜占庭问题[69]。在反制信号作用下，间谍无人机会在蜂群中持续传播错误信息，进而欺骗整个蜂群偏离原任务轨迹。对于此种反制方法，可用系统中被转化为间谍无人机的数量表征实施反制的强度。当间谍无人机数量较少时，反制效果有限，但是当间谍无人机数量过多时，不仅对反制技术有较高要求，也易触发蜂群的检测机制。同时，分布式蜂群中存在对协同行为影响较大的关键无人机，因此，间谍无人机的数量与选取均会对反制效果产生重要影响[70]。文献[71]对多欧拉-拉格朗日系统中的拜占庭攻击进行了探讨，研究了有限个恶意节点情况下系统的弹性协同问题。此外，也可对反制方无人机的性能特征进行伪装，使其混入非合作无人机蜂群，通过转发反制信号对蜂群实施诱导，在不造成进一步伤害的情况下利用拜占庭攻击欺骗分布式无人机蜂群以改变其轨迹[72]。

综上，拜占庭攻击在分布式蜂群反制中的应用关键，在于将蜂群中的部分无人机转化为反制节点或将反制无人机混入非合作蜂群，而后利用蜂群的分布式交互特性实现反制信息在蜂群中的扩散。因此，该方法仅需对部分节点进行反制，即可实现对整个蜂群行为的欺骗。然而，该反制方法对蜂群的拓扑结构及鲁棒性能有一定要求，对于采用拜占庭容错协议的分布式蜂群，部分节点或关键无人机的异常状态易被检测到并被隔离，从而削弱反制效果。因此，如何在反制过程中提高反制信号的隐蔽性，是基于拜占庭攻击的蜂群反制方法需要进一步研究的关键问题。

3）智能欺骗反制方法

随着人工智能技术的发展，将欺骗攻击与智能方法相结合成为当前的研究热点，基于智能算法设计的欺骗反制方法能够更好地适应蜂群反制场景中动态复杂环境的变化[73]。文献[74]总结了近年来基于深度学习的欺骗攻击检测研究进展，涵盖卷积神经网络、循环神经网络和深度强化学习等典型深度学习模型。文献[75]聚焦网络安全问题，提出了一种基于条件生成对抗网络的欺骗方案，并利用此网络构建了欺骗信号与系统状态之间的耦合关系，推动发展更具隐蔽性和环境适应性的欺骗方法。

强化学习因其与环境交互方面的优势而得到广泛应用，在非合作分布式蜂群欺骗反制方法的研究中展现出显著潜力[76]。多智能体强化学习通过集中式训练、分散式执行等系统架构，能够有效协调多个蜂群反制节点，可实现对蜂群协同机制的渗透与干扰[77]。文献[78]针对无人系统提出了一种关键时间步动态投毒方法，通过对重要性较高的样本进行动态扰动，显著提高了欺骗的隐蔽性。文献

[79]提出了一种基于分层深度强化学习的欺骗方案,顶层通过双深度 Q 网络从可行组合中筛选可欺骗节点,底层基于演员-评论员网络生成欺骗数据,并利用策略分布优化提升欺骗隐蔽性。文献[80]将欺骗问题建模为部分可观测马尔可夫决策过程,采用近端优化算法学习欺骗策略,进一步增强了欺骗方法的适应性与鲁棒性。

然而,现有的智能欺骗方法仍存在一定局限性。比如:当前多数基于智能算法的反制方法设计仍依赖于仿真推演,但在实际复杂动态的对抗环境下,特别是蜂群动态拓扑与通信受限等复杂情况下,其有效性有待进一步验证。此外,当前研究多聚焦于反制信号的生成,而对蜂群反制可持续性与反制性能指标的研究较少,尚未形成系统的蜂群反制算法框架。因此,智能欺骗方法的未来发展可将实物与仿真结合,以半实物仿真验证欺骗反制算法在接近真实环境下的反制性能。同时,可发展具有在线学习能力与自适应调节机制的反制方案,设计蜂群反制性能指标,提升在资源受限或动态蜂群场景下欺骗算法的性能。

### 2.2.2 诱导反制

诱导反制可以被看作一种特殊的蜂群欺骗反制方法,其作用途径、信号样式与针对蜂群节点的欺骗反制一致。但是当前多数欺骗反制研究都是着眼于令非合作蜂群系统最终达到发散的状态,从而破坏蜂群的任务执行能力,而诱导反制则是结合蜂群实际动态,通过精心设计诱导反制信号实现对蜂群整体运动轨迹的诱导。也就是保证蜂群在维持原有编队的状态下按照反制方预定的轨迹运动,进而实现蜂群的可控反制,是一种更高明的欺骗反制,其示意图如图 2 所示。相较于欺骗反制,诱导反制能够实现蜂群被反制后轨迹的完全可控,能够显著减少对地面设施及人员的附带损伤,但是,诱导反制信号的设计及理论分析也更具挑战性。

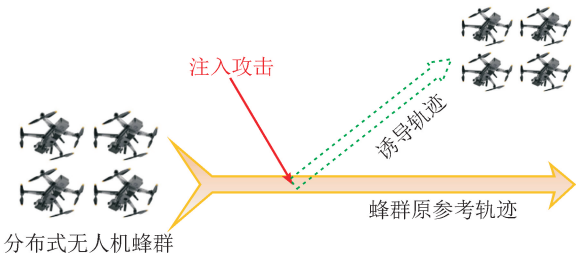


**图 2 诱导反制示意**

**Fig. 2 Schematic of induced attack**

文献[81]研究了孤立系统被诱导的反制策略,并应用于无人机。针对分布式集群系统,受文献[82]中基于内模原理的反制信号设计方法的启发,文献[83]首次提出了诱导反制的概念,初步探索了针对群系统的诱导反制策略。根据反制信号的注入方式及作用途径,同样可将诱导反制分为针对传感器—控制器通道的传感器信息诱导反制与针对控制器—执行器的执行器指令诱导反制。两种反制方法各有优劣,传感器信息诱导反制实现起来较为容易,诱导轨迹设计更简单,但反制隐蔽性略有不足;执行器指令诱导反制效果更显著,反制隐蔽性较强,但理论设计更复杂,诱导轨迹的确定相对困难。首先对执行器指令诱导反制方法进行介绍,其诱导反制协议可设计为

$$\tilde{u}_k(t)=u_k(t)+\varepsilon_k u_k^{\mathrm{a}}(t) \tag{13}$$

式中:$\tilde{u}_k(t)$为无人机 $k$ 的执行器实际接受到的控制指令;$u_k(t)$为基于一致性的分布式集群标称控制协议;$u_k^{\mathrm{a}}(t)$为反制方设计的诱导反制信号。$\varepsilon_k\in\{0,1\}$表示无人机 $k$ 的反制触发信号,若无人机 $k$ 受到反制,则 $\varepsilon_k=1$,否则 $\varepsilon_k=0$。反制方通过设定反制触发矩阵 $\tilde{\boldsymbol{v}}=\mathrm{diag}\{\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_N\}$,可对目标无人机蜂群施加更具策略性的诱导反制。诱导反制信号 $u_k^{\mathrm{a}}(t)$由生成外系统产生,具体可建模为:

$$\dot{u}_k^{\mathrm{a}}(t)=\boldsymbol{H}u_k^{\mathrm{a}}(t) \tag{14}$$

式中:$\boldsymbol{H}$ 为诱导反制信号生成矩阵,表征该生成外系统的动态特性,即规定了反制方设计的执行器诱导反制指令,反制方可通过外系统生成诱导反制信号和相应诱导驱离轨迹。从数学建模上看,诱导反制的数学模型与欺骗反制的数学模型形式相似,但是区别于欺骗反制信号被建模为噪声或扰动,诱导反制信号的设计需要结合非合作蜂群系统的部分参数,从而实现隐蔽注入、精准诱导。进一步地,文献[84]基于混合动态事件触发通信设计了一种完全分布式的诱导反制协议,事件触发能够显著减少反制信号所消耗的资源,同时对蜂群的诱导更加精准,更适合实际的蜂群反制环境,其诱导反制协议可设计为

$$u_k(t)=\sum_{j=1}^{N}c_{ij}w_{ij}[\bar{x}_j(t)-\bar{x}_k(t)]+u_k^{\mathrm{a}}(t) \tag{15}$$

式中:$c_{ij}$ 为耦合增益;$w_{ij}$ 为加权邻接矩阵的元素;$u_k^{\mathrm{a}}(t)$为反制方设计的诱导反制信号;$\bar{x}_k(t)$为反制后无人机 $k$ 状态 $x_k(t)$的估计值。

上述执行器指令诱导反制的实质是通过精心设计并篡改控制指令实现对蜂群轨迹的诱导，其实现技术比较复杂，反制信号设计与理论分析有一定难度。而传感器信息诱导反制则是通过改变无人机对环境及个体信息的感知实现轨迹的定向偏离，从而达到诱导反制的效果。传感器信息诱导反制信号可建模为

$$\tilde{x}_k(t)=x_k(t)+d_k x_k^{\mathrm{a}}(t) \tag{16}$$

式中：$\tilde{x}_k(t)$为无人机 $k$ 的传感器最终获取的经过诱导的状态信息；$x_k(t)$为无人机实际的真实状态；$x_k^{\mathrm{a}}(t)$为注入传感器的诱导反制状态信号；$d_k=1$ 表示该无人机受到传感器诱导，$d_k=0$ 则表示未受到诱导。在此基础上，文献[85]针对领导跟随双层非合作分布式无人机蜂群，设计了虚假偏差和给定状态两类传感器诱导反制信号，通过干扰领导层无人机的状态，蜂群能够在保持编队稳定的前提下被诱导至反制方所设定的飞行轨迹。进一步地，文献[86-87]分析了通信拓扑切换时蜂群系统的驱离条件，通过对领导者无人机的传感器施加诱导反制信号，使恶意信号扩散至整个编队控制系统，从而实现对蜂群的诱导反制。

值得注意的是，诱导反制信号的注入手段需要根据目标无人机的传感器或执行器类型进行调整，可结合实际采用电磁反制技术。针对依赖卫星导航的传感器，导航干扰是一种有效的信号注入手段，能够很好地实现对蜂群中无人机传感器的诱导反制信号注入。对于执行器指令诱导反制，文献[88]利用低频锯齿波产生的压降修改无人机无刷电机控制信号，实现了对执行器的指令篡改。文献[89]利用无人机携带高频电磁干扰设备抵近目标无人机，结果表明，被反制无人机的无刷电机按照预设反制信号转动。诱导反制可在不破坏蜂群编队的情况下，驱动系统整体沿反制方设计的特定轨迹运动，在蜂群反制应用中更具现实意义。同时，诱导反制信号考虑了系统原有控制协议设计，因而能够兼容现有大多数的安全协同控制策略，这些特性是基于 DoS 攻击或欺骗攻击的反制方法所不具备的。然而，当前对于诱导反制的研究相对较少，反制信号的设计及反制通道的选择还有很大的研究空间，值得进一步探索。随着工程技术的不断进步，诱导反制信号注入的物理手段也将会更加隐蔽多样。

上述 3 种基于网络攻击的蜂群反制方法的作用途径及反制效果如图 3 所示。基于 DoS 攻击的蜂群反制方法主要针对分布式蜂群的通信链路，通过破坏蜂群通信信息的可用性实现反制。该方法通过发送大量无效信息占用蜂群的通信资源，迫使部分无人机无法维持正常编队，进而破坏蜂群系统的一致性。其反制效果表现为不改变蜂群的整体飞行轨迹，但削弱蜂群的任务执行能力。欺骗反制主要针对分布式无人机蜂群的通信链路或节点，通过破坏蜂群通信信息的完整性实现反制。反制方生成虚假的状态信息或控制指令，并将其注入蜂群通信网络或节点无人机的传感器－控制器通道、控制器－执行器通道，影响无人机正常的状态感知或输出控制，从而破坏蜂群系统的一致性，最终使分布式蜂群的整体运动轨迹发生偏离。诱导反制则主要针对蜂群系统节点的内部通道，旨在实现蜂群整体飞行轨迹的可控诱导。反制方对虚假的状态信息或控制指令进行精心设计，并将其注入蜂群中节点的传感器与执行器通道，利用蜂群的分布式特性将虚假信息扩散至其他无人机，从而改变蜂群的整体运动轨迹。该方法可使蜂群在保持原有编队形态的前提下，按照反制方设定的轨迹运动，实现了分布式无人机蜂群反制的可控性。

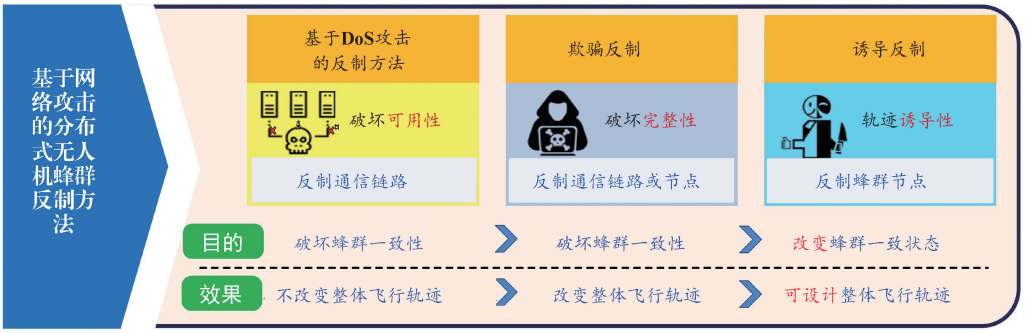


**图 3　基于网络攻击的蜂群反制方法总结**

**Fig. 3　Summary on cyber-attack-based countermeasures for UAV swarms**

## 3 基于网络攻击的蜂群反制方法发展趋势

当前,随着群系统控制理论的发展,分布式无人机蜂群的安全性与智能化水平也在迅速提升,对基于网络攻击的蜂群反制方法提出了更高要求。智能化蜂群的出现,推动网络反制方法向更精准、更多样和更智能的方向发展。下面结合当前研究现状,对基于网络攻击的蜂群反制方法的发展趋势进行探讨。

一是反制信号层面的精细化建模。基于网络攻击的蜂群反制方法关键在于反制信号的设计,而精细化建模是实现蜂群有效反制的基础。其建模主要分为蜂群网络建模与反制信号建模两个方面,蜂群网络建模是“知彼”,反制信号建模是“知己”。然而,当前研究面临非合作蜂群通信网络模型难以获取、反制信号模型未充分考虑蜂群及无人机特性等问题,限制了反制方法的实际效果。因此,后续研究可发展面向未知网络的蜂群系统辨识方法,提高蜂群网络模型的精准度;构建非线性时变的反制信号模型,充分适应环境及蜂群系统的动态变化;针对特定的蜂群通信协议精细化设计反制信号,增强反制的精准性与隐蔽性。

二是反制策略层面的多样化设计。在精细化建模的基础上,多样化的策略设计能够支撑更灵活高效的蜂群反制。然而,当前的反制策略以单一反制方式为主,难以应对日益复杂的蜂群协同机制与对抗态势。因此,未来研究可借鉴其他领域的成熟策略,并与网络反制实际有机结合。例如,间隔采样策略能够减少反制资源浪费;隐蔽诱导策略能够实现反制信号对蜂群系统完全隐蔽的无感注入;博弈策略将反制过程建模为反制方与蜂群之间的动态博弈,能够得到最优反制资源分配方案;混合网络反制策略能够更有效地对蜂群协同机制实施反制[90]。多种策略的有机融合能够显著提升反制体系的适应性与多样性,以应对分布式蜂群的多样化威胁。

三是反制方法层面的智能化升级。随着智能化蜂群技术的发展,传统反制方法的局限性日益凸显。目前,虽已有部分研究将智能技术引入蜂群反制领域,但相关技术仍处于理论阶段,距离应用还有差距[91-92]。因此,未来研究可考虑基于强化学习进行反制信号的动态优化,通过反制信号与蜂群环境的交互学习优化反制策略,进而实现复杂环境下对非合作蜂群的高效反制;可利用生成对抗网络设计反制信号,通过对抗训练与评价体系提升蜂群反制的隐蔽性;还可研究智能与人工混合决策的反制模型,依托智能算法自主完成反制决策,同时在关键节点保留人工决策权,兼顾网络反制方法的智能化与安全性。

## 4 结论

通过对基于网络攻击的分布式无人机蜂群反制方法进行全面综述,所得主要结论如下。

1)以经典蜂群反制方法为切入点,系统介绍了物理反制技术与电磁反制技术的相关反制手段,分析其优势与局限性,并对适用反制场景进行阐述。总体而言,经典蜂群反制方法技术较为成熟,能够应对一定程度的蜂群威胁,但在面对大规模蜂群特别是分布式蜂群时反制效果不理想。

2)结合分布式无人机蜂群的分布式交互特点,介绍了基于网络攻击的蜂群反制方法的作用机理。从破坏蜂群系统通信数据可用性与完整性两个维度,对基于DoS攻击与基于FDI攻击的反制方法的特点进行了说明,并结合非合作蜂群反制的实际,重点分析了欺骗反制与诱导反制的理论与研究进展,阐述了网络攻击方法在分布式蜂群反制中的具体实施方式。

3)结合当前分布式无人机蜂群技术与网络攻击方法的研究现状,从精细化建模、多样化策略与智能化升级3个维度,探讨了基于网络攻击的分布式蜂群反制方法的发展趋势,分析了当前存在的局限及未来需要关注的方向,对构建我国无人作战防御体系、推动我国低空安全建设提供参考。

## 参考文献

[1] Du Zhenpeng, Luo Chunbo, Min Geyong, et al. A survey on autonomous and intelligent swarms of uncrewed aerial vehicles (UAVs)[J]. IEEE Transactions on Intelligent Transportation Systems, 2025, 26(10): 14477-14500.

[2] Javed S, Hassan A, Ahmad R, et al. State-of-the-art and future research challenges in UAV swarms[J]. IEEE Internet of Things Journal, 2024, 11(11): 19023-19045.

[3] Sherman M, Shao Sihua, Sun Xiang, et al. Counter UAV swarms: challenges, considerations, and future

directions in UAV warfare[J]. IEEE Wireless Communications，2025，32(1)：190-196.

[4] 吴碧，江涛，陶宏，等. “蛛网行动”启示下低空新域攻防作战技术探讨[J]. 无人系统技术，2025，8(5)：11-19.
Wu Bi，Jiang Tao，Tao Hong，et al. Defending the low-altitude domain：lessons from spider-web[J]. Unmanned Systems Technology，2025，8(5)：11-19.

[5] Ceviz O，Sen S，Sadioglu P. A survey of security in UAVs and FANETs：issues，threats，analysis of attacks，and solutions[J]. IEEE Communications Surveys & Tutorials，2025，27(5)：3227-3265.

[6] Wei Xiaomin，Ma Jianfeng，Sun Cong. A survey on security of unmanned aerial vehicle systems：attacks and countermeasures[J]. IEEE Internet of Things Journal，2024，11(21)：34826-34847.

[7] Fan Tianfeng，Meng Xiaojing，Zhang Chi. Development status of anti UAV swarm and analysis of new defense system[J]. Journal of Physics：Conference Series，2023，2478(9)：092011.

[8] Wu Dejun，Yang Wei. Analysis of model based airborne laser weapon anti-UAV swarm[C]//Advances in Guidance，Navigation and Control. Singapore：Springer，2025：32-43.

[9] Liu Wei，Zhang Lin，Wang Wenfeng，et al. Dynamic resource target assignment problem for laser systems’ defense against malicious UAV swarms based on MADDPG-IA[J]. Aerospace，2025，12(8)：729-765.

[10] Xu Ran，Peng Qiang，Wu Husheng. Optimization design of flexible net capture system for low，slow，and small unmanned aerial vehicles based on improved multi-objective wolf pack algorithm[J]. Drones，2025，9(3)：190.

[11] Wang Jianan，Zhao Longze，Xia Kewei，et al. Discrete-time net capture against an intruder using multiple UAVs[J]. IEEE Transactions on Aerospace and Electronic Systems，2025，61(2)：2094-2105.

[12] Zhang Tao，Lu Ruitao，Yang Xiaogang，et al. UAV hunter：a net-capturing UAV system with improved detection and tracking methods for anti-UAV defense[J]. Drones，2024，8(10)：573.

[13] Xiang Lei，Xie Tao. Research on UAV swarm confrontation task based on MADDPG algorithm[C]//2020 5th International Conference on Mechanical，Control and Computer Engineering（ICMCCE）. Piscataway，NJ，USA：IEEE，2020：1513-1518.

[14] Wang Ershen，Liu Fan，Hong Chen，et al. MADRL-based UAV swarm non-cooperative game under incomplete information[J]. Chinese Journal of Aeronautics，2024，37(6)：293-306.

[15] Zong Jianan，Gao Xianzhong，Zhang Yue，et al. Research on target allocation for hard-kill swarm anti-unmanned aerial vehicle swarm systems[J]. Drones，2024，8(11)：666.

[16] 邱小剑，骆博雅，付珍，等. 国内外反无人机技术发展综述[J]. 战术导弹技术，2024(5)：63-73，98.
Qiu Xiaojian，Luo Boya，Fu Zhen，et al. An overview on development of domestic and foreign anti-UAV technology[J]. Tactical Missile Technology，2024(5)：63-73，98.

[17] Sun Zhenxin，Zhang Jin，Zhang Ning. A method of omni-directional anti swarm UAV[C]//2022 IEEE 6th Advanced Information Technology，Electronic and Automation Control Conference（IAEAC）. Piscataway，NJ，USA：IEEE，2022：694-697.

[18] Shi Hanzhang，Tang Chengkai，Zhang Lingling，et al. Distributed UAV cluster fusion positioning method with heterogeneous navigation information[J]. Measurement，2026，258：119420.

[19] Cao Zhengyang，Chen Gang. Enhanced deep reinforcement learning for integrated navigation in multi-UAV systems[J]. Chinese Journal of Aeronautics，2025，38(8)：103497.

[20] Qiu Ziyi，Lin Defu，Jin Ran，et al. A global ArUco-based lidar navigation system for UAV navigation in GNSS-denied environments[J]. Aerospace，2022，9(8)：456-480.

[21] Elamin A，Abdelaziz N，El-Rabbany A. A GNSS/INS/LiDAR integration scheme for UAV-based navigation in GNSS-challenging environments[J]. Sensors，2022，22(24)：9908.

[22] Li Xiangjun，Chen Lei，Lu Zukun，et al. Overview of jamming technology for satellite navigation[J]. Machines，2023，11(7)：768.

[23] 任思衡，姜晶莉，尚国强，等. GPS 区域性关闭信号的可能性分析与抗干扰对策[J]. 导航定位学报，2021，9(1)：5-9，24.
Ren Siheng，Jiang Jingli，Shang Guoqiang，et al. Possibility analysis and anti-jamming countermeasures on regional shutdown of GPS signals[J]. Journal of Navigation and Positioning，2021，9(1)：5-9，24.

[24] Qin Wenjian，Dovis F. Situational awareness of chirp jamming threats to GNSS based on supervised machine learning[J]. IEEE Transactions on Aerospace and Electronic Systems，2022，58(3)：1707-1720.

[25] 李威，张艳红，李冰，等. 分布式无人机蜂群导航欺骗反制方法研究[J]. 战术导弹技术，2023(3)：95-105.

Li Wei, Zhang Yanhong, Li Bing, et al. Research on navigation deception countermeasures for distributed UAV swarm[J]. Tactical Missile Technology, 2023(3): 95-105.

[26] Gao Yangjun, Li Guangyuan. Three time spoofing algorithms for GNSS timing receivers and performance evaluation[J]. GPS Solutions, 2022, 26(3): 87.

[27] Gao Yangjun, Li Guangyuan. Two time spoofing algorithms on GNSS receiver instrumentation of modifying satellite clock correction parameters in navigation message[J]. IEEE Transactions on Instrumentation and Measurement, 2023, 72: 8501511.

[28] 史鹏亮,王晓宇,薛瑞. 无人机位置欺骗诱导策略[J]. 国防科技大学学报,2021,43(2): 40-46.
Shi Pengliang, Wang Xiaoyu, Xue Rui. Induction strategy for unmanned aerial vehicle position spoofing[J]. Journal of National University of Defense Technology, 2021, 43(2): 40-46.

[29] Geng Xingshou, Guo Yan, Tang Kanghua, et al. A covert spoofing algorithm for SINS/GNSS tightly integrated navigation system[J]. IEEE Transactions on Automation Science and Engineering, 2025, 22: 6134-6142.

[30] 郭妍,唐康华,张鹭. 面向无人机的逐点偏移式卫星导航欺骗干扰方法[J]. 工程科学与技术,2023,55(2): 275-284.
Guo Yan, Tang Kanghua, Zhang Lu. GNSS navigation spoofing method of UAV based on point-by-point offset[J]. Advanced Engineering Sciences, 2023, 55(2): 275-284.

[31] Ma Xiaomeng, Gao Meiguo, Zhao Yangguang, et al. A novel navigation spoofing algorithm for UAV based on GPS/INS-integrated navigation[J]. IEEE Transactions on Vehicular Technology, 2024, 73(10): 15424-15439.

[32] Yu Haoyang, Wang Zidong, Zou Lei, et al. A survey on security control and estimation for cyber-physical systems under cyber-attacks: advances, challenges and future directions[J]. Artificial Intelligence Science and Engineering, 2025, 1(1): 1-16.

[33] He Wangli, Xu Wenying, Ge Xiaohua, et al. Secure control of multiagent systems against malicious attacks: a brief survey[J]. IEEE Transactions on Industrial Informatics, 2022, 18(6): 3595-3608.

[34] 卢剑权,邢梦平,张晶. 网络攻击下多智能体系统一致性安全与隐私保护研究综述[J]. 控制与决策,2025,40(11): 3201-3219.
Lu Jianquan, Xing Mengping, Zhang Jing. A survey on secure and privacy protection of multi-agent systems consensus under cyber attacks[J]. Control and Decision, 2025, 40(11): 3201-3219.

[35] Tan Cheng, Di Jianying, Guo Ge, et al. Exponential mean-square stabilization control for cyber-physical systems under random DoS attacks and transmission delay[J]. IEEE Transactions on Automatic Control, 2025, 70(1): 190-202.

[36] Ren Ziming, Liu Hao, Wen Guanghui, et al. Event-triggered data-driven security formation control for quadrotors under denial-of-service attacks and communication faults[J]. IEEE Transactions on Cybernetics, 2025, 55(11): 5226-5236.

[37] Zhang Xianming, Han Qinglong, Ge Xiaohua, et al. Resilient control design based on a sampled-data model for a class of networked control systems under denial-of-service attacks[J]. IEEE Transactions on Cybernetics, 2020, 50(8): 3616-3626.

[38] Xu Yong, Fang Mei, Shi Peng, et al. Event-based secure consensus of mutiagent systems against DoS attacks[J]. IEEE Transactions on Cybernetics, 2020, 50(8): 3468-3476.

[39] Zhang Dan, Feng Gang. A new switched system approach to leader-follower consensus of heterogeneous linear multiagent systems with DoS attack[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2021, 51(2): 1258-1266.

[40] Cao Hui, Han Liang, Li Dongyu, et al. Fully distributed dynamic event-triggering formation control for multiagent systems under DoS attacks: theory and experiment[J]. Neurocomputing, 2023, 552: 126546.

[41] Zhang Dan, Shen Yeping, Zhou Siquan, et al. Distributed secure platoon control of connected vehicles subject to DoS attack: theory and application[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2021, 51(11): 7269-7278.

[42] Han Zhen, Wang Wei, Huang Jiangshuai, et al. Distributed adaptive formation tracking control of mobile robots with event-triggered communication and denial-of-service attacks[J]. IEEE Transactions on Industrial Electronics, 2023, 70(4): 4077-4087.

[43] Li Yuanyuan, Li Yuanxin. Resilient distributed fixed-time tracking of heterogeneous UAVs-UGVs systems against DoS attacks[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2024, 54(9): 5780-5790.

[44] Amin S, Cárdenas A A, Sastry S S. Safe and secure networked control systems under denial-of-service attacks[C]//Proceedings of the 12th International Con-

ference on Hybrid Systems: Computation and Control. Berlin, Heidelberg: Springer, 2009: 31-45.

[45] Li Xiaomeng, Yao Deyin, Li Panshuo, et al. Secure finite-horizon consensus control of multiagent systems against cyber attacks[J]. IEEE Transactions on Cybernetics, 2022, 52(9): 9230-9239.

[46] Zhang Dan, Liu Lu, Feng Gang. Consensus of heterogeneous linear multiagent systems subject to aperiodic sampled-data and DoS attack[J]. IEEE Transactions on Cybernetics, 2019, 49(4): 1501-1511.

[47] Feng Zhi, Wen Guanghui, Hu Guoqiang. Distributed secure coordinated control for multiagent systems under strategic attacks[J]. IEEE Transactions on Cybernetics, 2017, 47(5): 1273-1284.

[48] Liu Jinliang, Dong Yanhui, Zha Lijuan, et al. Reinforcement learning-based tracking control for networked control systems with DoS attacks[J]. IEEE Transactions on Information Forensics and Security, 2024, 19: 4188-4197.

[49] Zhang Ruimei, Wang Hongxia, Park J H, et al. Secure distributed control for consensus of multiple EL systems subject to DoS attacks[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2024, 54(6): 3879-3890.

[50] Wu Jiancun, Tian Engang, Peng Chen, et al. Data-importance-aware attack strategy design and secure control countermeasure[J]. IEEE Transactions on Information Forensics and Security, 2025, 20: 944-954.

[51] Li Weihua, Zhang Huaguang, Zhang Juan, et al. Fully distributed event/self-triggered formation tracking for multiagent systems under denial-of-service attacks[J]. IEEE Systems Journal, 2023, 17(4): 5706-5713.

[52] Ma Lianlian, Wang Zhengxin, Hong Mei, et al. Bipartite synchronization for multiplex networks under false data injection attacks via pinning control[J]. Communications in Nonlinear Science and Numerical Simulation, 2026, 152: 109336.

[53] Fei Cheng, Shen Jun, Qiu Hongling, et al. Data-driven output synchronization of heterogeneous multi-agent systems under false data injection attacks[J]. IET Control Theory & Applications, 2025, 19(1): e70027.

[54] Hu Jueming, Ammar M, Zahid H B, et al. Reinforcement-learning-driven integrated detection and mitigation of UAV GPS spoofing attacks[J]. IEEE Internet of Things Journal, 2025, 12(18): 36926-36941.

[55] Geng Xingshou, Tang Kanghua, Guo Yan, et al. A distributed UAV swarm countermeasure method based on GNSS spoofing[J]. IEEE Internet of Things Journal, 2025, 12(16): 33455-33467.

[56] Jia Ruizhe, Wang Ting, Xue Wenchao, et al. Multitime scale consensus algorithm of multiagent systems with binary-valued data under tampering attacks[J]. IEEE Transactions on Industrial Informatics, 2025, 21(12): 9377-9388.

[57] Ning Chuanyi, Hao Fei, Yang Jiping. Optimal fusion deception attacks design and game analysis in multisensor systems[J]. IEEE Transactions on Network Science and Engineering, 2025, 12(5): 3837-3849.

[58] Yang Xinhe, Ren Zhu, Zhou Jingquan, et al. Optimal innovation-based deception attacks on multi-channel cyber-physical systems[J]. Electronics, 2025, 14(8): 1569.

[59] Yin Tingting, Gu Zhou, Park J H. Event-based intermittent formation control of multi-UAV systems under deception attacks[J]. IEEE Transactions on Neural Networks and Learning Systems, 2024, 35(6): 8336-8347.

[60] Yuan Hongbo, Yang Wen, Ding Wenjie, et al. Optimal deception attacks on remote state estimation under interval constraints[J]. IEEE Transactions on Automation Science and Engineering, 2025, 22: 16790-16800.

[61] He Jiangyan, Guo Xing, Chen Zili, et al. Secure impulsive synchronization control of multi-agent systems under switching deception attacks on dual channel[J]. Communications in Nonlinear Science and Numerical Simulation, 2025, 149: 108922.

[62] Ma Yajing, Li Zhanjie, Xie Xiangpeng, et al. Adaptive consensus of uncertain switched nonlinear multi-agent systems under sensor deception attacks[J]. Chaos, Solitons & Fractals, 2023, 175: 113936.

[63] Li Kuo, Hua Chuangchun, You Xiu, et al. Distributed consensus of feedforward nonlinear stochastic multiagent systems subject to actuator attacks[J]. IEEE Transactions on Cybernetics, 2025, 55(10): 4842-4851.

[64] Jin Kaijing, Ye Dan. Actuator and sensor attacks against multisensor state estimation with round-robin protocol[J]. IEEE Transactions on Industrial Informatics, 2025, 21(5): 3636-3644.

[65] He Jiangyan, Guo Xing, Chen Zili, et al. Adaptive distributed impulsive synchronization control for multi-agent systems under switching deception attacks on dual channels[J]. IEEE Transactions on Network Science and Engineering, 2025, 12(4): 2797-2809.

[66] Meira-Góes R, Marchand H, Lafortune S. Dealing with sensor and actuator deception attacks in supervisory control[J]. Automatica, 2023, 147: 110736.

[67] Zhang Ruiming, Yao Xiangyu, Wang Leimin, et al. Distributed fault-tolerant formation game for quadrotor UAVs with hybrid attacks[J]. IEEE Transactions on Aerospace and Electronic Systems, 2025, 61(5): 11338-11349.

[68] Ru Tingting, Cai Chenxiao, Park J H. Secured bipartite consensus control for nonlinear multi-agent systems against hybrid attacks: a component-based WTOD protocol[J]. IEEE Transactions on Automation Science and Engineering, 2025, 22: 11680-11692.

[69] Graham S L, Lamport L, Shostak R. The byzantine generals problem[J]. ACM Transactions on Programming Languages and Systems, 1982, 4(3): 382-401.

[70] Yang Yang, Sun Wei. Resilient bipartite consensus of high-order heterogeneous multi-agent systems under Byzantine attacks[J]. Automatica, 2024, 169: 111834.

[71] Li Yongming, Fang Yixian, Li Kewen. Resilient distributed cooperative backstepping control of Euler-Lagrangian systems under malicious link attacks[J]. IEEE Internet of Things Journal, 2025, 12(16): 34126-34136.

[72] Simonjan J, Probst S R, Schranz M. Inducing defenders to mislead an attacking UAV swarm[C]//2022 IEEE 42nd International Conference on Distributed Computing Systems Workshops (ICDCSW). Piscataway, NJ, USA: IEEE, 2022: 278-283.

[73] Fu Wei, Yan Yunqi, Chen Ying, et al. Temporal false data injection attack and detection on cyber-physical power system based on deep reinforcement learning [J]. IET Smart Grid, 2024, 7(1): 78-88.

[74] 李卓,谢耀滨,吴茜琼,等. 基于深度学习的电力系统虚假数据注入攻击检测综述[J]. 电力系统保护与控制, 2024, 52(19): 175-187.
Li Zhuo, Xie Yaobin, Wu Qianqiong, et al. Review of deep learning-based false data injection attack detection in power systems[J]. Power System Protection and Control, 2024, 52(19): 175-187.

[75] Nawaz R, Akhtar R, Khan S U, et al. Deep learning-driven false data injection attack in renewable integrated smart grids[J]. Engineering Applications of Artificial Intelligence, 2025, 156: 110953.

[76] Gong Zhenyu, Yang Feisheng. Secure tracking control via fixed-time convergent reinforcement learning for a UAV CPS[J]. IEEE/CAA Journal of Automatica Sinica, 2024, 11(7): 1699-1701.

[77] 罗彪,胡天萌,周育豪,等. 多智能体强化学习控制与决策研究综述[J]. 自动化学报, 2025, 51(3): 510-539.
Luo Biao, Hu Tianmeng, Zhou Yuhao, et al. Survey on multi-agent reinforcement learning for control and decision-making[J]. Acta Automatica Sinica, 2025, 51(3): 510-539.

[78] 周雪,尚大鹏,许晨,等. 无人系统中离线强化学习的隐蔽数据投毒攻击方法[J]. 通信学报, 2024, 45(12): 16-27.
Zhou Xue, Man Dapeng, Xu Chen, et al. Stealthy data poisoning attack method on offline reinforcement learning in unmanned systems[J]. Journal on Communications, 2024, 45(12): 16-27.

[79] Xiao Liang, Chen Haoyu, Xu Shiyu, et al. Reinforcement learning-based false data injection attacks in smart grids[J]. IEEE Transactions on Industrial Informatics, 2025, 21(4): 3475-3484.

[80] Shereen E, Kazari K, Dán G. A reinforcement learning approach to undetectable attacks against automatic generation control[J]. IEEE Transactions on Smart Grid, 2024, 15(1): 959-972.

[81] Yang Yue, Xiao Yang, Li Tieshan. Attacks on formation control for multiagent systems[J]. IEEE Transactions on Cybernetics, 2022, 52(12): 12805-12817.

[82] Mustafa A, Modares H. Attack analysis and resilient control design for discrete-time distributed multi-agent systems[J]. IEEE Robotics and Automation Letters, 2020, 5(2): 369-376.

[83] Li Junlong, Wang Le, Xi Jianxiang, et al. Induced attack with prescribed consensus trajectory against multiagent systems[J]. ISA Transactions, 2024, 146: 274-284.

[84] Pham T V, Nguyen Q T T. Induced attack on synchronization trajectory against a wide-area network with hybrid event-triggered communication[J]. Systems & Control Letters, 2025, 196: 106001.

[85] 李威,王乐,高久安,等. 面向领导跟随无人机蜂群的定向驱离攻击方法[J]. 航空学报, 2024, 45(12): 190-210.
Li Wei, Wang Le, Gao Jiuan, et al. Directional expelling attack on unmanned aerial vehicle swarm with leader-follower structure[J]. Acta Aeronauticaet Astronautica Sinica, 2024, 45(12): 190-210.

[86] 许兆胜,王乐,刘柟池,等. 基于传感器攻击的领导跟随多旋翼蜂群驱离方法[J]. 航空兵器, 2024, 31(6): 104-111.
Xu Zhaosheng, Wang Le, Liu Nanchi, et al. Leader-following multirotor UAV swarm expulsion method based on sensor attacks[J]. Aero Weaponry, 2024, 31(6): 104-111.

[87] 许兆胜,王乐,席建祥,等. 针对有向切换拓扑下无人机

蜂群的诱导攻击方法[J/OL]. 北京航空航天大学学报，(2024-09-10)[2025-12-19]. https://doi.org/10.13700/j.bh.1001-5965.2024.0488.
Xu Zhaosheng, Wang Le, Xi Jianxiang, et al. Induced attack on UAV swarms with switching directed topologies[J/OL]. Journal of Beijing University of Aeronautics and Astronautics, (2024-09-10)[2025-12-19]. https://doi.org/10.13700/j.bh.1001-5965.2024.0488.

[88] Selvaraj J, Dayanikli G Y, Gaunkar N P, et al. Electromagnetic induction attacks against embedded systems [C]//Proceedings of the 2018 on Asia Conference on Computer and Communications Security, NewYork, USA: ACM, 2018: 499-510.

[89] Dayanikli G Y, Sinha S, Muniraj D, et al. Physical-layer attacks against pulse width modulation-controlled actuators[C]//The 31st USENIX Security Symposium, Berkeley, USA: USENIX Association, 2022: 953-970.

[90] Guckert M, Le Cadre H, Le Hénaff J. A generalized potential game approach of UAV swarm coordination for hidden target localization[J]. IEEE Control Systems Letters, 2025, 9: 2681-2686.

[91] Ding Yahao, Yang Zhaohui, Pham Q V, et al. Distributed machine learning for UAV swarms: computing, sensing, and semantics[J]. IEEE Internet of Things Journal, 2024, 11(5): 7447-7473.

[92] Ahmed S, Yaakub A N, Junaini S N. Intelligent threat determination and PM in unmanned aerial vehicles: a review of deep learning perspective[J]. Unmanned Systems, 2025, 13(2): 1-18.

# Review on Cyber-Attack-Based Countermeasures for Distributed Unmanned Aerial Vehicle Swarms

ZHANG Yichi, WANG Le, GAO Jiuan, LIU Nanchi, XI Jianxiang*

(Rocket Force University of Engineering, Xi'an 710025, China)

**ABSTRACT**: With the extension of modern control technologies to unmanned and clustered systems, distributed unmanned aerial vehicle (UAV) swarms have gained widespread application across multiple domains because of their flexible deployment and strong adaptability. The abuse of UAV swarms poses an increasingly severe threat to low-altitude airspace, and distributed UAV swarms present unprecedented challenges to existing low-altitude defense systems. This paper provided a systematic review of countermeasures for distributed UAV swarms based on cyber attacks. First, an overview of non-cooperative distributed UAV swarms was provided, highlighting the severe threat they pose to existing countermeasure systems. Second, starting from the classic swarm countermeasure methods, this study elaborated on the existing swarm countermeasure technologies from the perspectives of physical and electromagnetic countermeasures. The advantages, disadvantages, and applicable scenarios of each countermeasure method were summarized, leading to the introduction of implementation methods for cyber-attack-based swarm countermeasures. Subsequently, focusing on cyber-attack methods, an overview of current theoretical and practical researches on cyber-attack methods in swarm countermeasure was conducted. Emphasis was placed on the operational pathways, mechanisms, and research progress of countermeasure methods based on denial-of-service, deception, and induced attacks, along with an analysis of the strengths and limitations of these three methods. Finally, based on the current research status of distributed UAV swarm technology and cyber-attack methods, the limitations of existing swarm countermeasures were summarized and the future development trends for distributed UAV swarm countermeasure methods based on cyber attacks were explored. Through the review of existing research and relevant technical methods, this study aims to provide a reference for research and practice in the field of non-cooperative distributed UAV swarm countermeasures, and promote the development of unmanned low-altitude defense systems in China.

**KEYWORDS**: distributed swarm; cluster countermeasure; unmanned aerial vehicle (UAV); cyber attack; induced countermeasure

(编辑：于福兴)