



综述

无人机隐蔽通信网络研究综述

白恒志, 王海超, 李国鑫, 龚玉萍

(陆军工程大学通信工程学院, 江苏 南京 210007)

摘要: 无人机通信网络是未来空天地一体化网络的重要组成部分, 是实现通信网络全球全域三维立体泛在覆盖的有效支撑。无线信道的开放特性致使无人机通信网络易遭受非法用户恶意攻击。隐蔽通信技术为提升无人机通信网络安全防御和隐私保护能力提供了极具前景的创新性解决思路, 但无人机系统机动性特点与隐蔽通信场景需求相互交叠的特性带来严峻挑战。分别从场景需求、主要挑战、体系架构和关键技术等维度对无人机隐蔽通信网络进行分析讨论, 重点探讨了无人机隐蔽通信网络资源管理模型、效能表征和关键技术, 尝试勾勒出无人机隐蔽通信网络的整体框架和未来发展方向, 以期为后续展开无人机隐蔽通信研究提供方向性指引。

关键词: 无人机通信; 隐蔽通信; 资源分配; 博弈论

中图分类号: TN929.5

文献标志码: A

doi: 10.11959/j.issn.1000-0801.2023162

Review on unmanned aerial vehicle covert communication network

BAI Hengzhi, WANG Haichao, LI Guoxin, GONG Yuping

College of Communications Engineering, Army Engineering University, Nanjing 210007, China

Abstract: Unmanned aerial vehicle (UAV) communication network is an important part of the future integrated space-aerial-ground network, and an effective support to achieve the global three-dimensional coverage of the communication network. The open characteristics of wireless channels make UAV communication vulnerable to malicious attacks by illegal users. Covert communication provides a promising solution for improving the security defense and privacy protection capabilities of UAV communication. However, the overlapping characteristics of the mobility of UAV systems and the requirements of covert communication scenarios bring severe challenges to the collaborative optimization of network resources. The UAV covert communication network was investigated from requirements, challenges, framework and main technologies perspectives. The architecture and model, performance characteristic, as well as potential candidate technologies were analyzed and discussed, in an attempt to outline the overall framework of UAV covert communication, and provide guidance for the subsequent research on UAV covert communication.

Key words: UAV communication, covert communication, resource allocation, game theory

收稿日期: 2023-03-08; 修回日期: 2023-08-12

通信作者: 王海超, whcw10919@sina.com

基金项目: 国家自然科学基金资助项目 (No.62001514, No.62271501); 博士后创新人才支持计划 (No.BX2021371)

Foundation Items: The National Natural Science Foundation of China (No.62001514, No.62271501), The National Postdoctoral Program for Innovative Talents under Grant (No.BX2021371)



0 引言

无人机通信网络是未来空天地一体化网络的重要组成部分,是实现通信网络全球全域三维立体泛在覆盖的有效支撑,具有覆盖范围广、部署灵活和不受地面灾害影响的特点^[1]。伴随着无人机侦察、探测和反制等反无人机技术的快速发展,无人机与反无人机如同矛与盾,互为攻防、互为依托^[2]。

无线信道的开放特性致使无人机通信网络易遭受非法用户恶意攻击,窃听、干扰、欺骗等严重扰乱通信秩序的行为频发,对社会安全造成极大威胁。面对窃听、干扰、欺骗等恶意攻击,无人机通信网络的安全防御与隐私保护能力已成为社会发展的迫切需求,是下一代无线网络和无人系统研究的重要方向^[3]。

近年来,隐蔽通信作为一种保证无线安全的新模式而备受关注。不同于信息加密和物理层安全技术,隐蔽通信的目标是从信号检测的角度出发,通过多种手段实现对方(非法用户)低概率检测,从而达到隐藏通信行为或过程的目的^[3-4]。信息加密和物理层安全技术侧重于对传输内容的保护,其通信行为仍会被窃听方发现,从而造成隐私信息泄露。单单是通信行为的泄露也会造成重大损失,如无线传输本身可能会暴露源节点位置信息,传输模式和流量同样可被利用获取关键信息^[5]。隐蔽通信技术为无人机通信网络提供了第一道安全防线,为解决无人机通信网络面临的隐私保护问题提供了新的可能。

本文综述了无人机通信网络中的隐蔽传输技术。首先,从基础理论和传输方案设计两方面介绍了现有隐蔽无线通信技术;其次,对无人机隐蔽通信网络场景需求和主要技术挑战进行了分析,并与物理层安全技术进行对比;再次,重点阐述了无人机隐蔽通信网络中资源管理技术,包括资源协同优化模型、效能表征以及涉及的关键

技术;最后,总结了无人机隐蔽通信网络技术未来的发展方向以及面临的挑战,并对全文工作进行总结。

1 隐蔽无线通信技术

信息时代增加了人们对无线网络的依赖程度,大量隐私和敏感信息通过无线媒介传输。基于密钥的加密技术和利用无线信道差异特性的物理层安全技术在一定程度上为信息安全传输提供了保障,是应对窃听攻击的有效手段^[4]。除了通信内容,用户的通信行为也蕴含重要信息^[6],如非法用户可通过分析接收信号的流量获取通信方的位置和身份等隐私信息。隐蔽通信成为一种保证无线安全的新模式,其目标是提供极低的检测概率以隐藏通信行为,是无线通信的首道安全防线^[7-8]。文献[9]详细综述了隐蔽通信领域基础理论、关键技术与应用场景,并分析了未来发展方向。本文主要从基础理论和传输方案设计两个方面对现有无线隐蔽通信进行介绍。

1.1 隐蔽通信基础理论

在隐蔽通信基础理论研究方面,现有工作回答了隐蔽通信中的一些基本问题,特别是分析得到了不同信道条件下的隐蔽通信性能界。传统频谱扩展技术可被看作隐蔽通信的一种实现方式,但是从信息论的角度出发,很多理论性问题一直未给出解释。文献[10]建立了加性白高斯噪声(additive white Gaussian noise, AWGN)信道中隐蔽传输的平方根定律,给出了在非法用户监视下系统可以可靠且隐蔽传输的最大信息量。在此基础上,研究者将高斯白噪声信道拓展到二进制对称信道^[11]、离散无记忆信道^[12]、多址接入信道^[13]、多输入多输出(multiple-input multiple-output, MIMO) AWGN 信道^[14],并分析了在时延约束下的系统性能^[15]。

根据平方根定律,当信道利用数趋于无穷时,系统隐蔽容量趋近于零。这种过于悲观的结论促

使研究者思考如何利用噪声、信道、发送时间等因素的不确定性提升隐蔽通信的性能。研究证明,在非法检测方缺乏对噪声功率确定性了解的情况下,信道利用数趋于无穷时仍然可以获得正的隐蔽速率^[16-17],同时,增大噪声不确定程度能够提升系统隐蔽性能^[18]。由于实际环境中的温度变化、环境变化和量化误差等原因,噪声不确定性几乎无法避免,因此研究噪声不确定性对隐蔽通信的影响具有现实意义。当噪声不确定低于某一门限值时,信道不确定或者信道衰落有助于实现隐蔽通信^[19]。针对信道不确定场景,文献[20]给出了信道不确定条件下非法检测方的最优检测门限,分析了在给定中断概率约束下的可达速率。文献[21]研究了完美信道状态信息和只有信道分布信息条件下的非法检测方最优检测性能,分析了信息不确定性的影响。与噪声和信道不确定类似,在非法检测方对传输时间存在不确定性观测时,系统隐蔽容量也可以获得提升^[22]。与此同时,研究表明多天线能够给隐蔽通信带来新的增益^[7,23-24]。

在物理层的隐蔽通信技术方面,利用加权类分数傅里叶变换(weighted-type fractional Fourier transform, WFRFT)信号的特征可以有效实现隐蔽通信。文献[25]把跳频、直扩和交织的思想结合起来提出 WFRFT 系统变参数策略,并利用 WFRFT 信号类高斯统计特性设计波形承载信号的隐蔽通信方案,具有更强的隐蔽和抗干扰性能。而多参数的 WFRFT 信号星座具有复杂且特殊的分裂变化,这更有助于原始调制方式的隐蔽以及应对非目的接收机对变换参数的侦测^[26]。文献[27]首次将通用多分数傅里叶变换(general multi-fractional Fourier transform, GMFRFT)理论用于实现多输入单输出(multiple-input single-output, MISO)系统的物理层安全,当建立了从发射机到合法接收机的额外安全链路或在上层实现了可靠加密技术时,GMFRFT 将保护其变换阶免受窃听。文献[28]针对传统 WFRFT 方法应对

复杂环境加密手段较为单一的不足,分析利用极化特征强化信息传输安全性,提出一种基于多层加权类分数傅里叶变换(multi-parameter WFRFT, MP-WFRFT)的多维联合调制卫星隐蔽通信方案。

1.2 传输方案设计

在隐蔽通信传输方案设计方面,除被动利用噪声、信道等不确定因素外,还可以主动创造干扰或者人工噪声等信号作为通信掩体。引入协作干扰机、利用中继和全双工接收机,以固定功率或者随机功率发送电磁信号增加系统的不确定性,有助于提升隐蔽通信系统性能^[29-32]。无论利用友好干扰还是人工噪声,干扰信号都会对己方通信系统产生影响,因此在系统隐蔽性和传输有效性之间存在互耦折中约束关系^[33]。文献[34]推导得到了采用最高信噪比中继选择方案时系统错误检测概率和平均隐蔽速率,并分析了系统参数的影响。文献[35]研究了基于中继的多跳消息隐蔽传输方案,提出了面向吞吐量和端到端时延的路由算法。在中继选择的基础上,可以通过功率控制获得更好的期望性能;利用全双工中继也可以实现合法用户隐蔽通信,其本质是通过全双工中继制造干扰信号以迷惑非法检测方^[31];注意到无论是被动利用噪声、信道等不确定因素,还是主动引入干扰或者人工噪声等信号作为通信掩体,发射功率控制都是一个重要的考虑方面^[36]。

针对单用户和空间位置固定的场景,为同时满足通信隐蔽性和有效性的要求,需要优化配置网络资源,常用的方法包括中继选择、功率分配、干扰机选择、波束成形等。在实际通信系统中,除人为引入干扰和中继等通信掩体外,还可以利用现有的通信链路实现隐蔽传输,但其研究仍面临通信节点相互耦合、检测性能分析复杂等挑战。此外,在无人机通信中考虑隐蔽传输时,高性能检测节点(如具有空间移动性)会致使现有的很多隐蔽通信策略性能降低甚至失效,现有资源优化方法无法直接移植。为



此, 对抗高性能检测节点的隐蔽通信策略设计是一个重要研究方向。

2 无人机隐蔽通信网络概述与挑战

2.1 无人机隐蔽通信网络概述

无人机通信网络作为连接无人机系统和控制中心的纽带以及无人机群协作的桥梁, 发挥着至关重要的作用。美国在《2013—2038 年无人系统综合路线图》中明确通信是无人系统面临的 9 项瓶颈技术之一^[37]。新版无人机/无人系统综合路线图《2017—2042 年无人系统综合路线图》再次强调无人机相关技术应支撑跨域指控、跨域通信等^[38]。与传统地面通信网络相比, 由于无人机的空间移动性, 无人机通信呈现出不同的特点。首先, 无人机飞行高度高于传统地面基站, 两者在覆盖范围方面存在较大差异, 这也对无线链路产生了一定影响。其次, 无人机通信中节点具有很高的移动性。地面基站或者接入点通常部署位置固定, 而无人机可在空间中以受控的轨迹高速移动。此外, 在尺寸、质量与功率方面, 无人机与地面通信节点也存在很大差异。关于无人机通信的研究主要包括无人机辅助基站、中继、移动边缘计算

和数据缓存等^[39-40]。然而, 随着通信网络发展和信息安全需求的提升, 无人机通信安全性受到广泛关注^[41-42]。

无人机隐蔽通信网络示意图如图 1 所示, 无人机隐蔽通信网络为空地融合网络, 既包含无人机与地面用户之间的空地通信, 又包含无人机的空空通信链路。其中空中无人机机动能力强, 能够根据通信需要实时调整空间位置。检测节点分为地面检测节点和空中检测节点两类, 两类节点都存在移动能力。特别是空中检测节点移动速度快, 能够快速抵近目标节点进行侦察探测。从功能的角度看, 无人机可以作为基站直接为用户提供通信服务, 也可作为中继为分隔的用户提供数据转发服务, 同时还可以作为友好干扰机迷惑对方检测。此外, 由于网络中存在多对通信链路, 通信链路之间本质上也形成了隐蔽通信掩体, 能够相互掩护。无人机隐蔽通信网络也可与其他网络结合, 形成空天地一体化隐蔽通信网络。如文献[43]针对空天地一体化车联网, 提出了基于功率和非规则高斯信号(improper Gaussian signaling, IGS)联合优化的上行隐蔽传输策略。仿真结果表明, 所提 IGS 方法在中断概率上优于正则

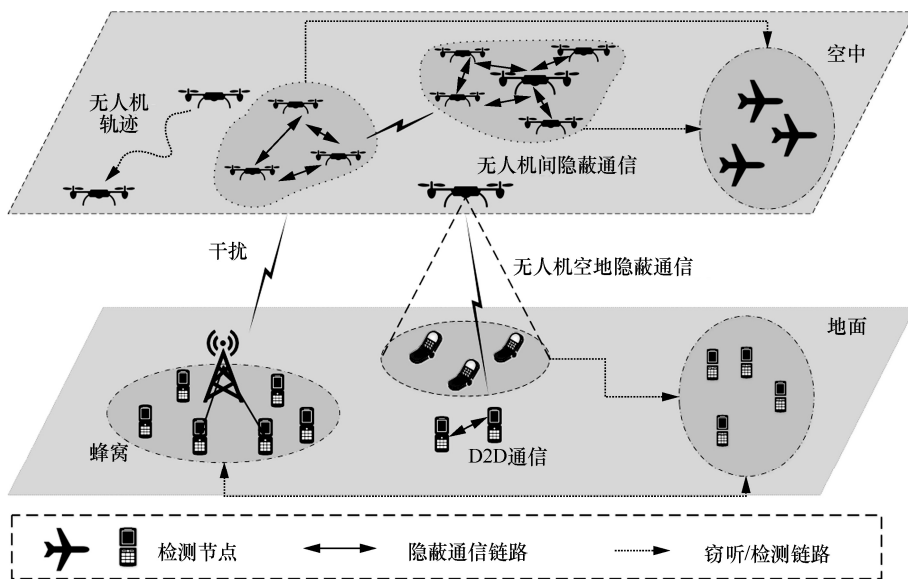


图 1 无人机隐蔽通信网络示意图

高斯信号 (proper Gaussian signaling, PGS) 方法。

2.2 主要技术挑战

从对抗的角度而言, 增大对方不确定性同时减少己方的不确定性可以提升系统的隐蔽性。为此, 在被动适应背景噪声、信道状态等不确定性因素的基础上, 还可以主动引入中继、友好干扰机、智能反射面等辅助节点, 并从发送功率、发送概率、传输时间、位置部署等多角度配置电磁资源, 进一步提升系统隐蔽性能。因此, 隐蔽通信系统性能提升的关键在于如何配置中继、友好干扰、发送功率、时间等网络资源。与传统地面通信网络相比, 由于无人机的空间移动性, 无人机通信网络在覆盖范围、移动速度、尺寸、质量与功率等方面呈现出不同的特点。无人机隐蔽通信面临无人机系统特点与隐蔽通信场景需求相互交叠带来的问题, 主要包括以下内容。

(1) 无人机隐蔽通信网络中的视距 (line of sight, LoS) 链路特性增大了通信行为被正确检测的概率。由于窃听方或者检测节点通常根据接收到的电磁信号判断是否存在通信行为, 因此隐蔽通信的基本实现手段是利用背景噪声、信道状态等不确定性因素提高检测节点误检概率, 以此掩盖真实通信行为。与传统地面通信网络中衰落信道相比, 视距信道大大降低了系统的不确定性。检测方能够更加准确地判断通信节点的位置、传输功率等, 如何主动制造更多的不确定性减轻视距链路的影响是无人机隐蔽通信网络面临的一大难题。

(2) 具备空间移动性的高性能检测方便无人机隐蔽通信系统设计更具挑战。从通信与检测对抗角度, 无人机隐蔽通信系统面临的检测方性能也在不断提升优化。可以动态调整检测位置的检测节点会使目前诸多隐蔽通信方案的效果大打折扣。隐蔽通信系统设计依赖于己方掌握的不对称信息, 从而利用或者主动创造不确定性以实现通信隐蔽性。而高移动场景会极大减少己方掌握的

信息, 双方主从关系不断变化、博弈对抗异常激烈。检测节点行为变化、无人机空间位置、决策复杂度和时效性要求都将增加隐蔽通信系统设计难度。

隐蔽通信技术为提升无人机通信安全防御和隐私保护能力提供了极具前景的创新性思路, 但无人机系统机动性特点与隐蔽通信场景需求相互交叠的特性给网络资源协同优化带来严峻挑战, 存在诸多理论和技术难点亟待解决。

3 无人机隐蔽通信网络资源管理技术

3.1 资源协同优化模型

无人机隐蔽通信系统中节点拓扑动态变化快, 资源协同优化依赖的全局信息难以完全掌握。当网络中节点数量较少或者节点之间相互影响较小时, 控制中心可以获得全局或者局部完美信息。此时, 集中式资源管理方式能够从系统角度优化配置网络资源, 发挥网络资源协同优势^[3]。然而, 随着无人机隐蔽通信系统中节点数量和类型增加, 网络拓扑快速变化, 全局信息难以掌握, 分布式资源优化模型更适合处理大规模用户相互耦合的情况。为发挥集中式和分布式资源优化的优势, 通常采用集中式与分布式相结合的混合式网络资源优化模型, 如图2所示。

当全局信息已知或者部分已知时, 控制中心利用收集的用户信息 (包括用户类型、通信需求、位置、移动性等信息)、无人机信息 (包括无人机通信能力、位置、速度、能量等信息)、检测节点信息、网络状态和频谱状态信息, 根据系统目标 (如频谱效率、能量效率、隐蔽性、覆盖率等指标), 优化配置网络资源, 将决策结果广播给通信用户和无人机, 而无人机和用户则反馈执行相应行动后的状态信息。集中式架构中所有的算法都在控制中心执行。网络状态信息指的是无线网络中地面基站、空中基站等各种接入点的状态, 频谱状态是指当前以及未来频谱的使用情况。

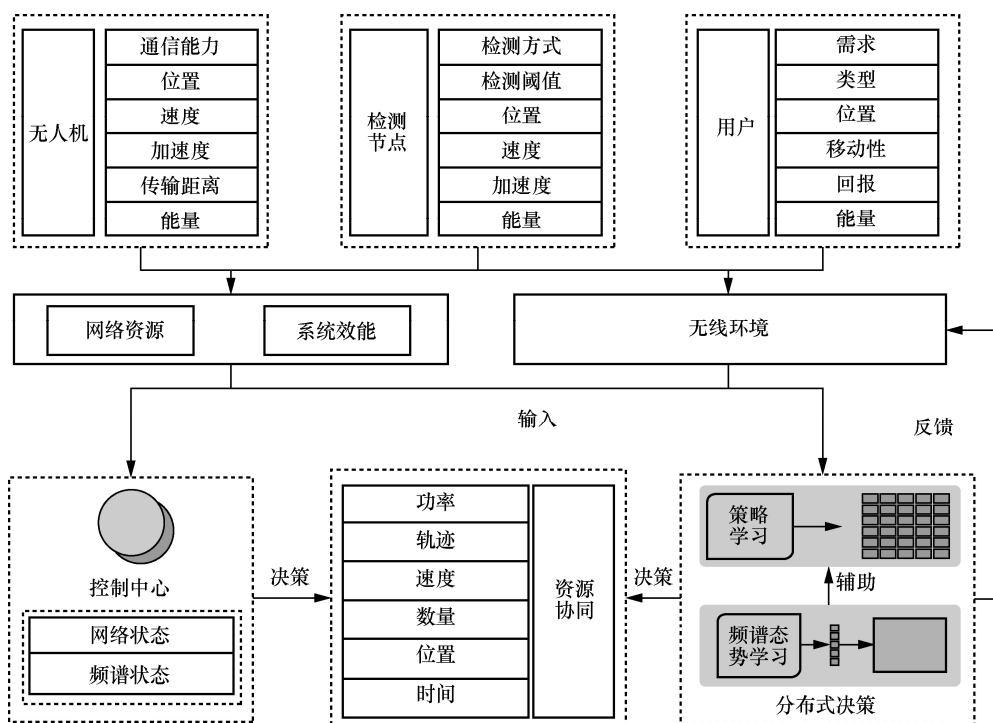


图2 混合式网络资源优化模型

在分布式资源优化模型中，一方面无人机和用户通过深度强化学习等方法直接学习隐蔽通信策略，得到最优策略后执行相应行动，并作用于外部环境^[2]；另一方面通过获得的环境信息建立频谱态势地图，并利用频谱态势地图推理预测未知空间、时间的频谱状态，从而为隐蔽通信系统设计提供信息辅助。考虑无人机与检测节点的对抗过程，可以利用机器学习的方法模拟其博弈过程，如生成对抗网络。

针对无人机的动态网络结构，需要结合具体场景采用不同形式的资源协同优化模型。在混合式资源协同优化模型中，集中式方法与分布式方法既可以并行使用，也可以串行使用。针对小规模用户或者局部信息已知，两种模型可以同时并行采用，并可以利用集中式方法得到的结果训练分布式算法，矫正并提升分布式算法的性能；对于大规模或者广域用户场景，可以综合利用两种方式。如基于分而治之的思想，可以先从宏观上对整体进行分簇，簇间资源协同采用分布式算法，

簇内各个用户的资源协同由簇头采用集中式方式决定，从而充分利用网络结构特性。

3.2 资源协同效能表征

在混合式网络资源优化模型中，网络资源与系统效能（system performance）分别决定了决策变量和优化目标。针对网络资源，可以从群体资源和无人机个体资源角度进行区分。群体资源主要从系统节点部署与调度的角度出发，而个体资源是指在节点部署与调度的基础上对节点资源的进一步配置，如功率资源、调制与编码方式等。

- 群体资源：无人机隐蔽通信系统涉及通信、中继、干扰等多种网络实体，因此从系统设计的角度，需要确定各个节点的角色。例如，在多个中继传输系统中，每条通信链路需要确定对应的中继节点以及各个节点的位置。在多个友好干扰辅助系统中，选择不同的干扰机会产生不同的效果，因此干扰机选择与配对也是隐蔽通信中的决策因素。

- 个体资源：当网络层级节点部署与调度优化完成后，需要优化配置节点资源，如各个节点的通信频率、通信时间、发射功率等。群体资源和个体资源的优化是相辅相成的，这两者有机衔接、互相增效，通过合理的组合和协调，可以在不同尺度和角度上使检测节点面临更大的不确定性，从而提高合法用户通信的效能。

无人机隐蔽通信系统效能以网络资源为基础，是多种网络资源共同作用的结果。隐蔽性是无人机隐蔽通信系统设计的必要指标，从信息传输的角度，还需要考虑通信有效性和可靠性等性能指标，这些指标直接体现出通信本身的意义。在资源协同优化模型中，综合考虑隐蔽通信场景需求和无人机位置可控特性，从用户体验质量、通信有效性和服务代价多个维度提出无人机隐蔽通信系统多维效能表征体系，并分析网络资源与系统效能之间的耦合约束关系，网络资源与系统效能关系如图3所示，具体如下。

- 用户体验质量：从通信服务需求方出发，衡量系统内各个通信用户的服务质量，具体指标主要有信干噪比、信道容量、传输速率、

传输时延、中断概率等。从通信满意度的角度而言，期望系统具备大容量、高速率、低时延等能力，从而满足用户需求。

- 通信隐蔽性：从通信系统第三方出发，刻画通信过程中对通信行为的保护程度。考虑与检测节点的对抗过程，通常采用检测节点的虚警概率和漏检概率表示。从通信安全角度讲，隐蔽通信是一种特殊的安全方式。为保障通信安全性，期望系统能够获得高隐蔽性。
- 服务成本：从通信服务供给方出发，表征系统为实现用户体验质量和通信隐蔽性而付出的代价。具体指标主要包括占用频谱资源、计算和存储资源、能耗等。特别是在无人机隐蔽通信系统中，无人机不仅存在通信、干扰方面能耗，维持飞行的机械能耗也是不可忽略的，并且机械能耗常远大于通信或者干扰能耗。

此外，系统稳健性和复杂度是实际应用中着重考虑的效能指标。由于复杂地理和电磁环境的影响，环境状态信息时变难以掌握。无论预先规划还是在线学习方式，都需要考虑系统稳健性以

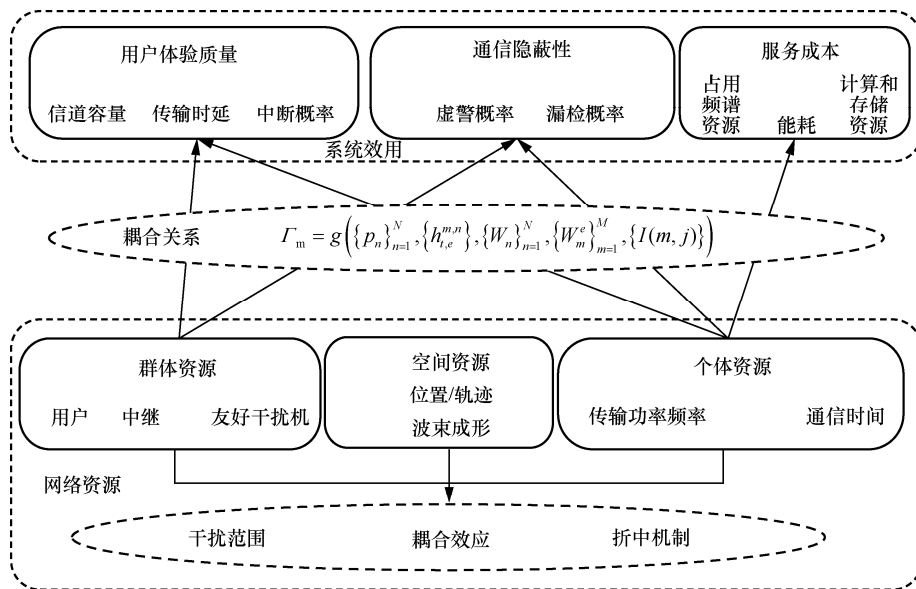


图3 网络资源与系统效能关系



应对不确定情况。从概率层面或者最坏情况的角度设计相应的资源协同方法。同时,为快速应对网络状态变化和恶意干扰攻击,对资源协同方法的响应时间也提出了很高的要求。

3.3 资源协同管理关键技术

从信号检测角度来看,检测节点主要利用接收到的信号判断是否存在通信行为。因此,噪声或者友好干扰机功率的不确定性能够致使检测节点误判。无人机空间移动性为隐蔽通信系统设计带来了新的挑战,也提供了新的优化维度。设计无人机的空间位置,可以增强隐蔽通信系统性能。关于无人机隐蔽通信的主要文献比较见表1,对无人机隐蔽通信代表性文献进行了比较说明。

3.3.1 无人机基站

当地面通信设施损坏或者无法满足通信用户

需求时,可以通过部署无人机基站辅助地面通信网络,无人机基站隐蔽通信场景示意图如图4所示,其中坐标轴表示节点三维空间位置。根据服务用户的数量,现有关于无人机基站隐蔽通信的研究可以分为单用户和多用户两类。

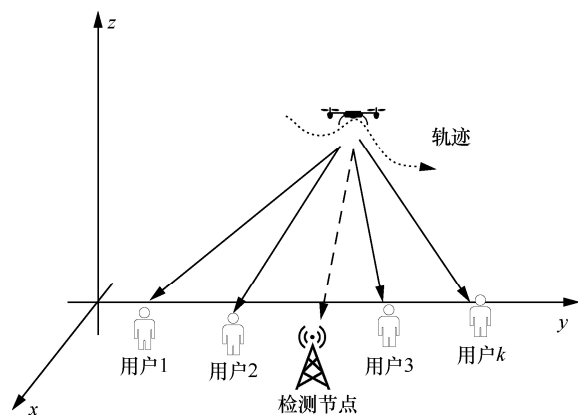


图4 无人机基站隐蔽通信场景示意图

表1 关于无人机隐蔽通信的主要文献比较

主要文献	研究场景	优化目标	主要约束	优化变量	主要方法
[44-45]	三节点场景	信噪比	隐蔽性 发射功率 高度	发射功率 无人机距离与角度	分类分析 启发式算法
[46]	三节点场景	隐蔽性	通信质量 高度	三维位置 发射功率	分类分析 闭式解
[47]	三节点场景	隐蔽速率	隐蔽约束 中断概率 飞行速度	无人机轨迹 发射功率	连续凸近似
[49]	三节点场景	传输速率	功率	波束数量 发射功率 无人机高度	最小化 最大化
[50]	多个地面接收机	平均速率	隐蔽性 飞行速度	无人机轨迹 时间分配 发射功率	块坐标下降
[51]	全双工无人机接收多个节点信息	平均速率	隐蔽性 用户调度	无人机轨迹 人工噪声功率 调度策略	连续凸近似
[53]	无人机中继	能效	隐蔽性 功率 速度	发射功率 相位 轨迹	连续凸近似
[59]	认知用户与主用户共存	隐蔽速率 误检概率	通信速率 飞行速度	无人机轨迹 发射功率	生成对抗网络
[60]	多个检测节点一个干扰机	传输速率	隐蔽性	无人机与干扰位置和功率	求导分析

针对单个无人机与一个地面节点通信的情况,文献[44]通过分析无人机高度和功率对隐蔽通信系统的影响,研究了通信质量、隐蔽约束和检测代价之间的折中问题。在此基础上,文献[45]给出了在隐蔽性约束条件下最大化通信质量的无人机部署(无人机与非法检测方之间的距离和角度)方法。与之相对应,在通信质量约束下,文献[46]分析得到了使通信隐蔽性最大的无人机最佳空间位置,并证明了相比于二维空间,三维空间位置部署能够带来更大的增益。考虑非法检测方和接收方的位置不确定,文献[47]提出了基于连续凸近似(successive convex approximation, SCA)的无人机轨迹和发送功率联合优化算法,实现了平均隐蔽速率最大化。从检测节点角度来看,文献[48]针对带波束扫描功能的多天线检测节点场景,推导了误检概率的闭式表达形式,并得到了使误检概率最小的波形设计方法。在实际场景中,无人机可能无法获取接收方和检测方的位置,文献[49]提出了一种基于时分波束扫描传输的机会通信方法,并通过优化波束数量、发射功率和无人机高度实现平均吞吐量最大化。

针对一个无人机服务多个地面用户的情况,文献[50]在考虑有限观测的情况下,研究了满足隐蔽约束条件的系统传输速率最大化问题,设计了基于块坐标下降的时间分配、发送功率和无人机轨迹联合优化方法。文献[51]考虑全双工无人机场景,无人机使用接收天线与地面用户通信,同时利用发射天线产生人工噪声干扰非法检测方。为提升系统性能,需要综合考虑无人机轨迹、人工噪声功率和用户的调度关系。由于无人机采用正交方式与多个用户通信,如时分多址,因此,多用户之间不存在相互干扰。

3.3.2 无人机辅助中继

由于中长距离的无线隐蔽通信中信号发射功率较大,容易被检测方检测到,无人机中继协助的隐蔽传输是一种解决方案,无人机中继辅助隐

蔽通信如图5所示。文献[52]在隐蔽通信约束下,联合优化发射机和中继的发射功率以及无人机的飞行高度,从而最大化隐蔽通信的吞吐量。仿真结果验证了系统的隐蔽性能。文献[53]设计了一种无人机携带可重构智能超表面(reconfigurable intelligent surface, RIS)辅助隐蔽通信的框架,通过联合设计功率、相位和无人机轨迹优化隐蔽通信能效。文献[54]分析了莱斯信道下无人机中继辅助的隐蔽通信系统性能,其中无人机既作为中继转发信号,又作为干扰机迷惑检测方。从对抗的角度看,无人机也可以作为非法检测方,例如,文献[55]提出了一种应对无人机检测的多跳中继方式。文献[56]考虑无人机检测方可以通过调整位置提升检测性能,提出了传输块长和功率联合优化方法。

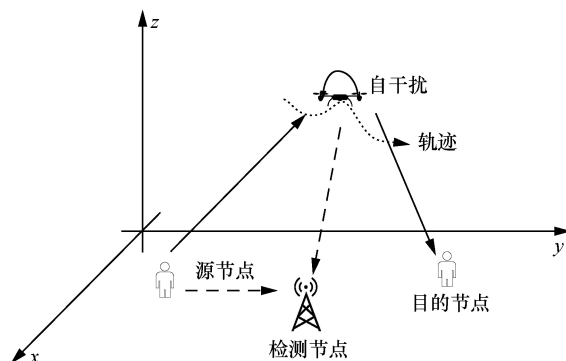


图5 无人机中继辅助隐蔽通信

3.3.3 无人机辅助干扰机

利用友好干扰机能够进一步提升隐蔽通信系统性能,友好干扰机辅助隐蔽通信如图6所示。文献[57]通过引入多天线干扰机辅助无人机与多个地面用户通信,仿真结果证明了引入干扰机可以提升系统效用。文献[58]得出了平均隐蔽概率和发射功率、无人机位置、无人机运动速度之间的关系,分析了移动无人机干扰场景下,发射功率、无人机位置以及无人机运动速度对平均隐蔽概率的影响。文献[59]采用无人机作为干扰辅助认知用户的隐蔽通信,设计了一种基于生成对抗网络(generative adversarial network, GAN)的无人机



轨迹和功率联合优化算法。文献[60]在无人机空地通信中引入友好干扰机，分析了检测节点的检测性能，并通过优化无人机和干扰机的位置以及地面节点的发送功率得到最大的传输速率。另外，发射机或者接收机本身也可以发送人工噪声 (artificial noise, AN) 以迷惑检测节点。文献[61]构建了无人机三维位置部署和 AN 功率以及发射机 (Alice) 的联合优化问题，推导了 Alice 发射功率和 AN 发射功率的最优解析表达式。文献[62]分析了 AWGN 和 Nakagami- m 信道条件下无人机作为友好干扰机实现的隐蔽速率，仿真验证了采用无人机作为干扰机可以提升系统性能。

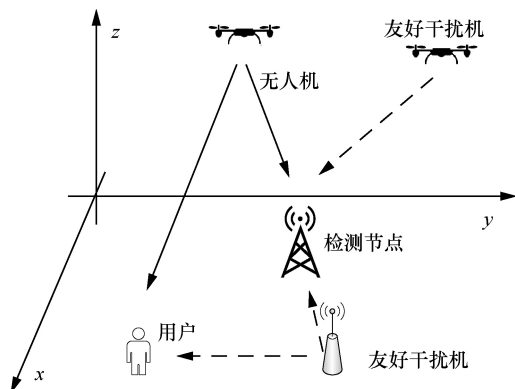


图6 友好干扰机辅助隐蔽通信

分析无人机隐蔽通信研究现状，可以发现在无人机轨迹规划、功率控制等资源优化方面已经有了一定技术积累，但是考虑对抗场景中检测节点位置捷变、无人机能量有限等特点挑战，仍存在一些亟待解决的问题。首先，无人机在尺寸、质量与功率等方面严格受限，需要综合考虑无人机特性和隐蔽通信需求；其次，在多用户无人机频谱共享网络中，检测节点的工作方式、任务分配以及检测性能未知，多用户协调困难；最后，无人机隐蔽通信网络节点众多、需求各异，网络资源协同优化面临大维决策空间和变量的挑战。因此，如何在检测节点动态移动和多用户频谱共享场景下进行网络资源协同，其研究仍有待进一步深入。

4 未来研究展望

4.1 基于博弈学习的隐蔽传输

博弈论 (game theory) 作为应用数学的一个重要分支，在功率控制、资源分配和流量控制等领域已经得到广泛应用，特别是针对多用户 (智能体) 相互影响的情况，基于博弈论的方法能够分析双方的动态对抗过程。在无人机隐蔽通信中，通信方与检测方相互对抗，两者之间的策略选择本身就是一个博弈过程；单从通信方 (或者检测方) 一方考虑，多个通信节点 (检测节点) 之间也呈现合作或者非合作现象。在此背景下，合作博弈和非合作博弈等博弈方法可以作为无人机隐蔽通信资源协同优化方法设计的有效工具，基于博弈学习的隐蔽传输如图7所示。

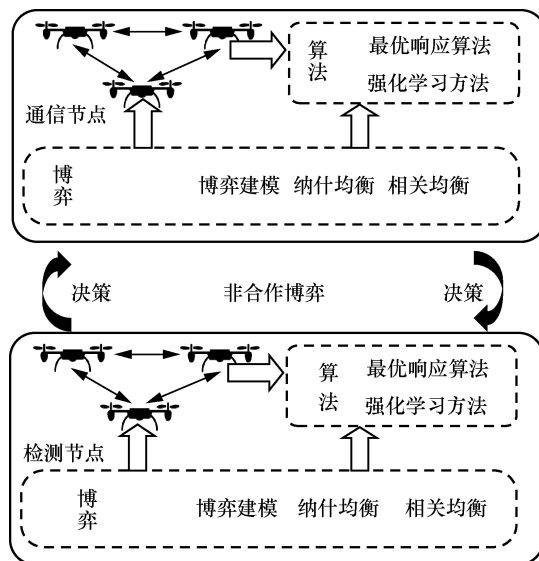


图7 基于博弈学习的隐蔽传输

由于通信用户之间存在合作关系，而通信方与检测节点是对抗关系，因此无人机与检测节点的决策优化其实是一个动态对抗过程。为此，可以利用斯坦伯格 (Stackelberg) 博弈模型刻画对抗双方非合作特性以及不同类型参与者 (即对抗环境中的通信节点和检测节点) 之间的相互影响关系。目前，两层斯坦伯格博弈模型已经被广泛应

用于分析和处理资源分配以及干扰决策问题。在两层斯坦伯格博弈模型中,具有强势地位的上层决策者率先制定策略,这个策略会作用于下层决策者;下层决策者据此做出使自身效益最佳的策略,这一过程又会反作用于上层决策的目标函数。在隐蔽通信系统中,需要首先考虑通信节点和检测节点的主从关系,从不同角度建立对抗博弈模型,分析博弈的均衡点的性质。考虑对抗环境下信息的非对称性,可进一步构建不完全信息条件下的斯坦伯格博弈模型。

为得到对抗场景下博弈双方策略,需要设计分布式资源分配算法。根据所需信息的程度,可以分为部分分布式和完全分布式学习算法两类。部分分布式学习算法中博弈参与者在接收到其他参与者的信号或者数据之后,结合自己的收益更新资源分配策略,如最优响应(best response)、虚拟行动(fictitious play)及其各类变形。完全分布式学习算法中博弈参与者仅根据自己的策略和收益更新策略选择,不需要其他参与者直接的反馈,典型方法如强化学习(reinforcement learning)。但考虑无人机高移动性,分布式算法的收敛速度成为实际应用面临的挑战之一。此外,多用户博弈中通常存在多个均衡点,所设计的算法能否收敛到最优均衡点也值得探究。

4.2 基于无人机空间位置优化的隐蔽传输

文献[9]提出在无人机隐蔽通信系统中引入不确定性的最典型技术之一是利用随机信道衰落,进一步将无人机的机动性与信道衰落相结合,可以大大改善检测方的不确定性,这有助于大大提高 Alice 的隐蔽性。无人机的特性在于其高移动速度,无人机移动性对增强物理层安全容量的作用已得到验证。但由于物理层安全通信和隐蔽通信的需求差异,无人机移动性究竟如何影响通信隐蔽性、通过空间域实时调整位置能否实现隐蔽通信系统性能提升等一系列问题亟须进一步研究。

特别是在对抗环境中,检测节点的动态性使通信隐蔽性下降,但通信用户亦可通过动态调整空间位置提升隐蔽性,此时无人机移动与资源分配策略设计成为关键所在。

动态调整检测位置的检测节点会破坏目前诸多隐蔽通信方案,无人机通信系统中节点移动性高,检测节点可以通过连续变化检测点位提升检测性能。同时,多个检测节点也可以通过联合检测的方式实现更为精准的通信检测。无论是对于无人机空地通信还是对于无人机间通信而言,传统隐蔽通信方法的性能将大打折扣。如传统方法可能利用特定情况下信道衰落特性实现隐蔽通信,但是检测节点的动态移动会降低衰落特性的影响,换言之,无法保证通信发射机和对方检测节点处于任意位置的通信链路衰落特性相同。为此,通信方无人机可以通过实时调整空间位置躲避移动检测节点的检测充分发挥受控移动的优势,但同时也面临决策空间巨大、多变量耦合、计算复杂度高等挑战。

现代通信已经不是简单的点对点通信,而是一个复杂的通信网络。控制网络的拓扑结构可以实现网络级的隐蔽通信。由于网络中存在多条通信链路,当某一链路易被检测发现或者无法实现隐蔽通信时,可以通过其他节点进行中继转发。基于联盟形成的网络拓扑控制如图 8 所示,多个无人机可以采用形成联盟的方式进行协同隐蔽传输,能够实现单个无人机无法达到的效果。因此,拓扑结构可以从物理空间和路由两个方面优化。一方面,无人机群可以通过调整空间位置换取功率资源,不同的空间位置也决定了不同的网络或者路由结构。另一方面,在空间拓扑固定的情况下,可以优化路由降低被对方检测的概率。网络级隐蔽通信可以充分利用网络结构,极大增强通信系统稳健性。

4.3 互为隐蔽通信掩护时群体资源协同

频谱资源有限性和空间异构性致使多用户共

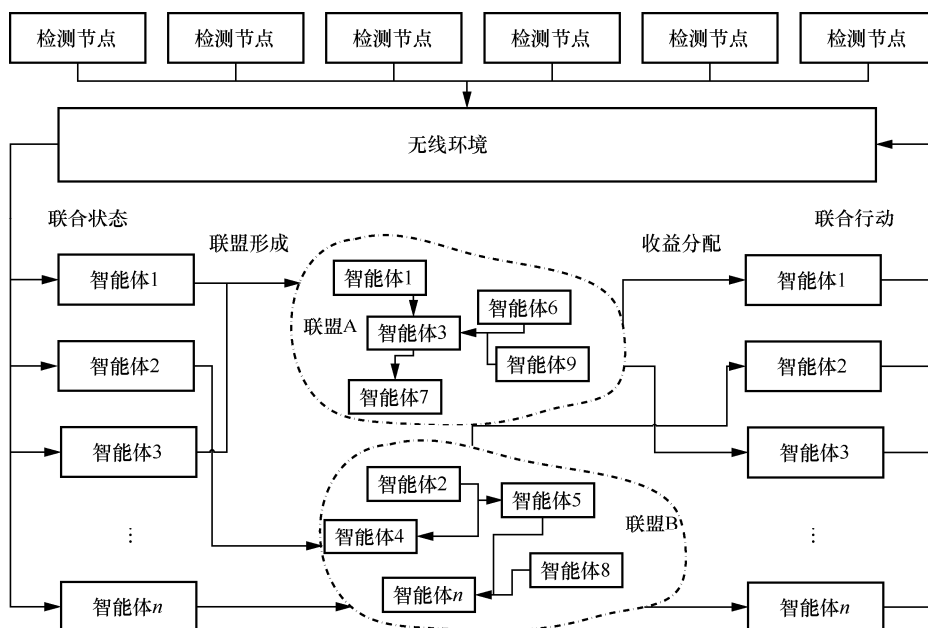


图8 基于联盟形成的网络拓扑控制

享同一频段成为必然选择。在此情况下，合作用户本身就可以作为其他用户的隐蔽通信掩体，为实现系统目标必须协调所有通信用户的通信行为，如位置和发射功率。合作用户各自的任务需求致使节点之间相互耦合且协同困难。此外，还需要精准筹划干扰、中继等辅助设备的调度策略，实现群体资源匹配协同，而此时又将面临大规模决策空间和优化变量的挑战。

为实现无人机通信网络的隐蔽传输，可以综合利用网络中我方通信节点和友好干扰机，内部节点与外部节点的智能协同能够极大提升网络隐蔽性能。针对多友好干扰机辅助多无人机通信场景，建立面向用户公平性的通信节点和友好干扰节点协同调度模型，分析多干扰机对隐蔽通信性能的影响；基于激励机制的网络节点智能协同如图9所示，由于通信节点和干扰节点的自私性，需要通过相应的激励补偿弥补通信或者友好干扰节点的能量等损失。为此，一个值得研究的方向是设计基于激励补偿机制的节点协同调度框架，探索激励设计和回报分配方式，构建面向目标函数的激励值优化模型。

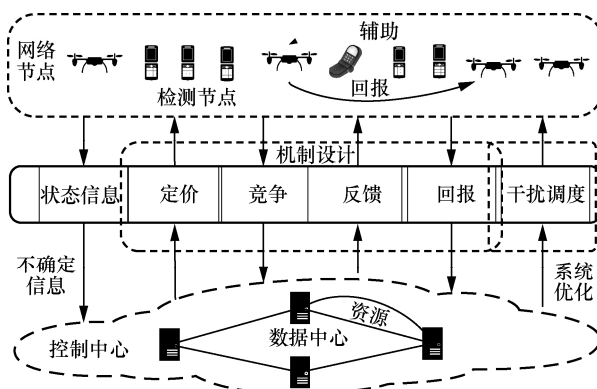


图9 基于激励机制的网络节点智能协同

多天线通信系统在发挥分集和复用增益的同时，也可以提高系统的安全性。特别是从物理层安全的角度而言，现有研究通过波束成形设计保证信息安全性。但是多天线在隐蔽通信领域的研究还处于起步阶段，还有大量问题亟待解决。特别是针对多个通信用户共存的情况，多天线波束的方向性给隐蔽通信实现带来机遇，但也给隐蔽通信系统设计提出了更大的挑战。通信节点与检测节点的对抗特性造成获得的信息必然不准确甚至无法获取信息，不完全信息条件下的系统设计有可能增大通信节点被检测的概率，为此，在考

虑系统隐蔽性的同时,还需要考虑算法的稳健性与复杂度。

4.4 未来发展趋势

从无人机通信网络的角度来看,可以采用空间位置优化、群体无人机协同的方式增加通信网络的隐蔽性。另外,新技术的发展也为无人机隐蔽通信网络的实现提供了更多的方式。首先,由大量低成本无源反射元件构成的智能反射面具备重新配置无线传播环境的能力,从而显著提高无线通信网络的性能^[63]。隐蔽通信的一个重要特点就是检测方通过观察频谱使用状态判断是否存在通信行为,引入智能反射面可以增加检测方的不确定性,混淆其对频谱使用状态的准确判断。同时,智能反射面的无源波束成形能力可以减少电磁辐射,增大检测方判断难度。其次,从合法方通信与非法方检测对抗的角度看,合法方也具备频谱感知与环境监测能力。为实现通信的有效性和隐蔽性,通信感知一体化是一种有效方法,在通信的同时实现感知功能,从而达到高精度定位、智能调度以及自组网等目的。考虑无人机计算、存储等能力有限,可以进一步将边缘计算和边缘智能技术引入,实现通信—感知—计算协同设计。此外,对抗环境下信息的不确定性显著增加,除信道信息不确定外,网络节点个数、组网方式、通信协议、运动模型等都呈现不确定性。如何刻画并分析这些不确定性是一个难题。

5 结束语

无人机群本身通信需求和无人机辅助地面通信促进了无人机通信网络的快速发展。一方面,无人机的控制离不开通信,其智能化水平更是对通信有较强的依赖;另一方面,无人机的受控移动性能够实现操纵信道的目的,从而极大增强传统地面通信网络。本文针对群体无人系统和空地一体化网络中的通信安全和隐私保护问题,将隐蔽通信理论与技术作为提升无人机通信防御能

力的解决思路。概述了无人机隐蔽通信网络的场景需求和主要技术挑战;从资源协同优化模型、效能表征和关键技术3个方面阐述了无人机隐蔽通信网络资源管理研究现状,从基于博弈学习的隐蔽传输、基于无人机移动的隐蔽传输、互为通信掩体时群体资源协同等方面分析了未来研究方向,有望为无人机通信安全防御与隐私保护开辟新思路,为未来无线网络有序频谱利用和群体无人系统通信对抗研究带来较高的价值。

参考文献:

- [1] SONG Q H, ZENG Y, XU J, et al. A survey of prototype and experiment for UAV communications[J]. Science China Information Sciences, 2021, 64(4): 140301.
- [2] 樊邦奎, 张瑞雨. 无人机系统与人工智能[J]. 武汉大学学报(信息科学版), 2017, 42(11): 1523-1529.
FAN B K, ZHANG R Y. Unmanned aircraft system and artificial intelligence[J]. Geomatics and Information Science of Wuhan University, 2017, 42(11): 1523-1529.
- [3] JIANG X, CHEN X Y, TANG J, et al. Covert communication in UAV-assisted air-ground networks[J]. IEEE Wireless Communications, 2021, 28(4): 190-197.
- [4] ZHENG T X, YANG Z T, WANG C, et al. Wireless covert communications aided by distributed cooperative jamming over slow fading channels[J]. IEEE Transactions on Wireless Communications, 2021, 20(11): 7026-7039.
- [5] ALEX. Russia creates a device capable of "hunting" Starlink antennas[EB]. 2022.
- [6] 赵华, 林钰达, 金梁, 等. 隐蔽无线通信综述[J]. 信息工程大学学报, 2020, 21(5): 520-525.
ZHAO H, LIN Y D, JIN L, et al. Covert wireless communication: a review[J]. Journal of Information Engineering University, 2020, 21(5): 520-525.
- [7] 林钰达, 金梁, 黄开枝, 等. 基于3D波束成形的隐蔽无线通信威胁区域构建[J]. 中国科学(信息科学), 2021, 51(8): 1360-1374.
LIN Y D, JIN L, HUANG K Z, et al. Threat region development of covert wireless communication based on 3D beamforming[J]. Scientia Sinica (Informationis), 2021, 51(8): 1360-1374.
- [8] YAN S H, ZHOU X Y, HU J S, et al. Low probability of detection communication: opportunities and challenges[J]. IEEE Wireless Communications, 2019, 26(5): 19-25.
- [9] CHEN X Y, AN J P, XIONG Z H, et al. Covert communications:



- a comprehensive survey[J]. *IEEE Communications Surveys & Tutorials*, 2023, 25(2): 1173-1198.
- [10] BASH B A, GOECKEL D, TOWSLEY D. Limits of reliable communication with low probability of detection on AWGN channels[J]. *IEEE Journal on Selected Areas in Communications*, 2013, 31(9): 1921-1930.
- [11] CHE P H, BAKSHI M, JAGGI S. Reliable deniable communication: hiding messages in noise[C]//*Proceedings of 2013 IEEE International Symposium on Information Theory*. Piscataway: IEEE Press, 2013: 2945-2949.
- [12] BLOCH M R. Covert communication over noisy channels: a resolvability perspective[J]. *IEEE Transactions on Information Theory*, 2016, 62(5): 2334-2354.
- [13] ARUMUGAM K S K, BLOCH M R. Keyless covert communication over multiple-access channels[C]//*Proceedings of 2016 IEEE International Symposium on Information Theory (ISIT)*. Piscataway: IEEE Press, 2016: 2229-2233.
- [14] ABDELAZIZ A, KOKSAL C E. Fundamental limits of covert communication over MIMO AWGN channel[C]//*Proceedings of 2017 IEEE Conference on Communications and Network Security (CNS)*. Piscataway: IEEE Press, 2017: 1-9.
- [15] YAN S H, HE B, ZHOU X Y, et al. Delay-intolerant covert communications with either fixed or random transmit power[J]. *IEEE Transactions on Information Forensics and Security*, 2019, 14(1): 129-140.
- [16] LEE S, BAXLEY R J, WEITNAUER M A, et al. Achieving undetectable communication[J]. *IEEE Journal of Selected Topics in Signal Processing*, 2015, 9(7): 1195-1205.
- [17] 戴跃伟, 刘光杰, 曹鹏程, 等. 无线隐蔽通信研究综述[J]. *南京信息工程大学学报*, 2020, 12(1): 45-56.
- DAI Y W, LIU G J, CAO P C, et al. A survey of wireless covert communications[J]. *Journal of Nanjing University of Information Science & Technology*, 2020, 12(1): 45-56.
- [18] HE B, YAN S H, ZHOU X Y, et al. On covert communication with noise uncertainty[J]. *IEEE Communications Letters*, 2017, 21(4): 941-944.
- [19] TA H Q, KIM S W. Covert communication under channel uncertainty and noise uncertainty[C]//*Proceedings of ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*. Piscataway: IEEE Press, 2019: 1-6.
- [20] SHAHZAD K, ZHOU X Y, YAN S H. Covert communication in fading channels under channel uncertainty[C]//*Proceedings of 2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*. Piscataway: IEEE Press, 2017: 1-5.
- [21] SHAHZAD K, ZHOU X Y. Covert wireless communications under quasi-static fading with channel uncertainty[J]. *IEEE Transactions on Information Forensics and Security*, 2021, (16): 1104-1116.
- [22] BASH B A, GOECKEL D, TOWSLEY D. Covert communication gains from adversary's ignorance of transmission time[J]. *IEEE Transactions on Wireless Communications*, 2016, 15(12): 8394-8405.
- [23] 林钰达, 金梁, 周游, 等. 噪声不确定时基于波束成形的隐蔽无线通信性能分析[J]. *通信学报*, 2020, 41(7): 49-58.
- LIN Y D, JIN L, ZHOU Y, et al. Performance analysis of covert wireless communication based on beam forming with noise uncertainty[J]. *Journal on Communications*, 2020, 41(7): 49-58.
- [24] 王旭, 金梁, 楼洋明, 等. 基于无线信道差异的隐蔽通信[J]. *信号处理*, 2021, 37(1): 86-94.
- WANG X, JIN L, LOU Y M, et al. Covert communication based on the difference of wireless channels[J]. *Journal of Signal Processing*, 2021, 37(1): 86-94.
- [25] 梅林. 加权类分数傅立叶变换及其在通信系统中的应用[D]. 哈尔滨: 哈尔滨工业大学, 2010.
- MEI L. Weighted fractional Fourier transform and its application in communication system[D]. Harbin: Harbin Institute of Technology, 2010.
- [26] 梅林, 沙学军, 张乃通. 加权分数傅立叶变换通信系统抗参数扫描及星座分裂性能分析[J]. *云南民族大学学报(自然科学版)*, 2011, 20(5): 361-366.
- MEI L, SHA X J, ZHANG N T. The secure communication system based on single/multi-parameter weighted-type fractional Fourier transform[J]. *Journal of Yunnan University Nationalities (Natural Sciences Edition)*, 2011, 20(5): 361-366.
- [27] DONG H, FANG X J, SHA X J, et al. Secure transmission for MISO wiretap channels using general multi-fractional Fourier transform: an approach in signal domain[J]. *IEEE Transactions on Vehicular Technology*, 2022, 71(8): 8702-8716.
- [28] 倪磊, 达新宇, 胡航, 等. 基于 MP-WFRFT 的多维联合调制卫星隐蔽通信研究[J]. *电子与信息学报*, 2023, 45(4): 1183-1191.
- NI L, DA X Y, HU H, et al. Research on multi-dimensional joint modulation for satellite covert communication based on MP-WFRFT[J]. *Journal of Electronics & Information Technology*, 2023, 45(4): 1183-1191.
- [29] SHU F, XU T Z, HU J S, et al. Delay-constrained covert communications with a full-duplex receiver[J]. *IEEE Wireless Communications Letters*, 2019, 8(3): 813-816.
- [30] SOBERS T V, BASH B A, GUHA S, et al. Covert communication in the presence of an uninformed jammer[J]. *IEEE Transactions on Wireless Communications*, 2017, 16(9): 6193-6206.
- [31] SUN R R, YANG B, MA S Q, et al. Covert rate maximization in

- wireless full-duplex relaying systems with power control[J]. *IEEE Transactions on Communications*, 2021, 69(9): 6198-6212.
- [32] 惠锴, 王滢, 张琰祥. 基于协作干扰对抗联合检测的隐蔽传输方法[J]. *计算机工程与应用*, 2022, 58(8): 109-116.
- HUI H, WANG Y, ZHANG Y X. Covert transmission against joint transmission detection based on cooperative jamming[J]. *Computer Engineering and Applications*, 2022, 58(8): 109-116.
- [33] SHAHZAD K, ZHOU X Y, YAN S H, et al. Achieving covert wireless communications using a full-duplex receiver[J]. *IEEE Transactions on Wireless Communications*, 2018, 17(12): 8517-8530.
- [34] SU Y J, SUN H J, ZHANG Z K, et al. Covert communication with relay selection[J]. *IEEE Wireless Communications Letters*, 2021, 10(2): 421-425.
- [35] SHEIKHOLESAMI A, GHADERI M, TOWSLEY D, et al. Multi-hop routing in covert wireless networks[J]. *IEEE Transactions on Wireless Communications*, 2018, 17(6): 3656-3669.
- [36] 李赞, 廖晓闽, 石嘉, 等. 面向认知物联网的隐蔽通信智能功率控制[J]. *物联网学报*, 2020, 4(1): 52-58.
- LI Z, LIAO X M, SHI J, et al. Intelligent power control for covert communication in cognitive Internet of things[J]. *Chinese Journal on Internet of Things*, 2020, 4(1): 52-58.
- [37] United States Department of Defense. Unmanned systems integrated roadmap: FY2013-2038[R]. U.S.: United States Department of Defense, 2013.
- [38] FACHEY K, MILLER M. Unmanned systems integrated roadmap 2017-2042[R]. Arlington County: Office of the Secretary of Defense, 2018.
- [39] ZENG Y, ZHANG R, LIM T J. Wireless communications with unmanned aerial vehicles: opportunities and challenges[J]. *IEEE Communications Magazine*, 2016, 54(5): 36-42.
- [40] NGUYEN K K, DUONG T Q, DO-DUY T, et al. 3D UAV trajectory and data collection optimisation via deep reinforcement learning[J]. *IEEE Transactions on Communications*, 2022, 70(4): 2358-2371.
- [41] WANG H C, WANG J L, DING G R, et al. Robust spectrum sharing in air-ground integrated networks: opportunities and challenges[J]. *IEEE Wireless Communications*, 2020, 27(3): 148-155.
- [42] 崔高峰, 徐媛媛, 张尚宏, 等. 基于最小能耗的多无人机无线网络数据安全数据卸载策略[J]. *通信学报*, 2021, 42(5): 51-62.
- CUI G F, XU Y Y, ZHANG S H, et al. Secure data offloading strategy for multi-UAV wireless networks based on minimum energy consumption[J]. *Journal on Communications*, 2021, 42(5): 51-62.
- [43] WANG D Y, QI P H, ZHAO Y, et al. Covert wireless communication with noise uncertainty in space-air-ground integrated vehicular networks[J]. *IEEE Transactions on Intelligent Transportation Systems*, 2022, 23(3): 2784-2797.
- [44] YAN S H, HANLY S V, COLLINGS I B, et al. Hiding unmanned aerial vehicles for wireless transmissions by covert communications[C]//*Proceedings of ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*. Piscataway: IEEE Press, 2019: 1-6.
- [45] YAN S H, HANLY S V, COLLINGS I B. Optimal transmit power and flying location for UAV covert wireless communications[J]. *IEEE Journal on Selected Areas in Communications*, 2021, 39(11): 3321-3333.
- [46] ZHOU X B, YAN S H, NG D W K, et al. Three-dimensional placement and transmit power design for UAV covert communications[J]. *IEEE Transactions on Vehicular Technology*, 2021, 70(12): 13424-13429.
- [47] ZHOU X B, YAN S H, HU J S, et al. Joint optimization of a UAV's trajectory and transmit power for covert communications[J]. *IEEE Transactions on Signal Processing*, 2019, 67(16): 4276-4290.
- [48] HU J S, WU Y P, CHEN R Q, et al. Optimal detection of UAV's transmission with beam sweeping in covert wireless networks[J]. *IEEE Transactions on Vehicular Technology*, 2020, 69(1): 1080-1085.
- [49] ZHANG J Y, CHEN X H, LI M, et al. Optimized throughput in covert millimeter-wave UAV communications with beam sweeping[J]. *IEEE Wireless Communications Letters*, 2021, 10(4): 720-724.
- [50] JIANG X, YANG Z T, ZHAO N, et al. Resource allocation and trajectory optimization for UAV-enabled multi-user covert communications[J]. *IEEE Transactions on Vehicular Technology*, 2021, 70(2): 1989-1994.
- [51] ZHOU X B, YAN S H, SHU F, et al. UAV-enabled covert wireless data collection[J]. *IEEE Journal on Selected Areas in Communications*, 2021, 39(11): 3348-3362.
- [52] 胡锦涛, 吴林梅, 束锋, 等. 无人机中继协助的有限码长隐蔽通信[J]. *电子与信息学报*, 2022, 44(3): 1006-1013.
- HU J S, WU L M, SHU F, et al. UAV-relay assisted covert communication with finite block-length[J]. *Journal of Electronics & Information Technology*, 2022, 44(3): 1006-1013.
- [53] LI M, TAO X F, LI N, et al. Energy-efficient covert communication with the aid of aerial reconfigurable intelligent surface[J]. *IEEE Communications Letters*, 2022, 26(9): 2101-2105.
- [54] ZHANG R, CHEN X Y, LIU M Q, et al. UAV relay assisted cooperative jamming for covert communications over rician



- fading[J]. IEEE Transactions on Vehicular Technology, 2022, 71(7): 7936-7941.
- [55] WANG H M, ZHANG Y, ZHANG X, et al. Secrecy and covert communications against UAV surveillance via multi-hop networks[J]. IEEE Transactions on Communications, 2020, 68(1): 389-401.
- [56] CHEN X Y, SHENG M, ZHAO N, et al. UAV-relayed covert communication towards a flying warden[J]. IEEE Transactions on Communications, 2021, 69(11): 7659-7672.
- [57] DU H Y, NIYATO D, XIE Y A, et al. Performance analysis and optimization for jammer-aided multiantenna UAV covert communication[J]. IEEE Journal on Selected Areas in Communications, 2022, 40(10): 2962-2979.
- [58] 胡静雯, 戴跃伟, 刘光杰, 等. 无人机辅助场景下基于波束成形的 LPD 通信性能分析[J]. 重庆理工大学学报(自然科学), 2022(3): 152-163.
- HU J W, DAI Y W, LIU G J, et al. Analysis of LPD communication performance based on beamforming in UAV assisted scenes[J]. Journal of Chongqing University of Technology (Natural Science), 2022(3): 152-163.
- [59] LI Z, LIAO X M, SHI J, et al. MD-GAN-based UAV trajectory and power optimization for cognitive covert communications[J]. IEEE Internet of Things Journal, 2022, 9(12): 10187-10199.
- [60] CHEN X Y, ZHANG N, TANG J, et al. UAV-aided covert communication with a multi-antenna jammer[J]. IEEE Transactions on Vehicular Technology, 2021, 70(11): 11619-11631.
- [61] 周小波, 彭旭, 于辉, 等. 无人机网络中人工噪声增强的短包隐蔽通信[J]. 信号处理, 2022, 38(8): 1601-1609.
- ZHOU X B, PENG X, YU H, et al. Artificial noise enhanced short-packet covert communications for UAV networks[J]. Journal of Signal Processing, 2022, 38(8): 1601-1609.
- [62] LIANG W, SHI J, TIE Z Z, et al. Performance analysis for UAV-jammer aided covert communication[J]. IEEE Access, 2020(8): 111394-111400.
- [63] WU Q Q, ZHANG R. Intelligent reflecting surface enhanced

wireless network via joint active and passive beamforming[J]. IEEE Transactions on Wireless Communications, 2019, 18(11): 5394-5409.

[作者简介]



白恒志 (1999-), 男, 陆军工程大学通信工程学院硕士生, 主要研究方向为 MIMO、隐蔽通信等。



王海超 (1991-), 男, 博士, 陆军工程大学通信工程学院副教授、硕士生导师, 主要研究方向为无人机通信、异构无线网络传输技术等。



李国鑫 (1990-), 男, 博士, 陆军工程大学通信工程学院副教授、硕士生导师, 主要研究方向为空天地一体化网络、隐蔽通信等。



龚玉萍 (1978-), 女, 陆军工程大学通信工程学院教授、硕士生导师, 主要研究方向为短波通信、隐蔽通信等。