

卫星隐蔽通信综述：现状、关键技术和未来挑战

邓浩^① 孙维远^② 朱政宇^{*③} 潘高峰^④ 孙钢灿^③

^①(河南大学物理与电子学院 开封 475004)

^②(河南大学未来技术学院 郑州 450046)

^③(郑州大学电气与信息工程学院 郑州 450001)

^④(北京理工大学网络空间安全学院 北京 100081)

摘要：卫星隐蔽通信具有保护信息内容和隐藏通信行为的双重能力，已成为信息对抗和保障战略通信连续性的关键技术。本文全面综述卫星隐蔽通信的理论基础、关键技术现状及未来发展挑战。首先，基于Alice-Bob-Willie模型，深入分析卫星信道特性对隐蔽容量的影响机制，阐明多普勒频移等因素对隐蔽通信速率的制约关系，并探讨修正型平方根定律下的理论边界。其次，围绕天基、空基、地基三层协同架构，系统梳理信号伪装编码、波束成形、频谱分集、量子加密与人工智能辅助等核心技术，并总结抗监听与抗干扰的多层级防护机制。最后，结合当前典型安全威胁，探讨卫星隐蔽通信面临的主要挑战，展望低轨动态组网、非理想信道鲁棒传输、人工智能与量子技术深度融合等未来发展方向，为构建高安全性、强隐蔽性的空间通信网络提供理论依据和技术支撑。

关键词：卫星隐蔽通信；隐蔽编码；波束成形；频谱捷变

中图分类号：TN927.2

文献标识码：A

文章编号：1009-5896(2026)00-0001-16

DOI: 10.11999/JEIT260177

CSTR: 32379.14.JEIT260177

1 引言

卫星通信是空间信息网络的重要组成部分，已广泛应用于媒体广播、网络回程传输、新闻采集直播等多元化场景^[1]。随着卫星通信技术快速发展及其承载的无线服务规模持续扩大，超大规模网络架构下的空间信息传输面临严峻的安全挑战，尤其在恶意攻击风险显著加剧的背景下，卫星通信的安全问题日益重要。

典型的卫星通信系统由空间段、地面段和用户段构成。空间段包含卫星星座及星载处理单元^[2]，地面段涵盖信关站、测控系统设施及网络运营中心，用户段涵盖部署于固定或移动平台的各类用户终端^[3]。相比地面无线通信系统，卫星通信系统具有传输距离远、覆盖范围广的特点。然而，这也使得恶意节点可在空天地实施全域攻击。由于被动监

听行为具有极高的隐蔽性，不仅难以被检测与处置，更导致卫星链路面临严峻的监听、干扰及非法接入的风险。低地球轨道卫星星座的快速部署带来了巨大机遇^[4]，同时引发了前所未有的安全风险，恶劣太空环境与资源约束进一步降低了系统可靠性，亟须构建适配卫星通信的安全防护机制。

隐蔽通信作为信息对抗领域的关键技术，其通过信号波形设计、时频域资源调度等物理层方法隐藏通信行为，使得非合作方难以从背景噪声中检测到通信信号。与传统的加密技术不同，隐蔽通信不仅保护数据内容，更重要的是隐藏通信行为本身，在物理层面上为卫星通信增加了新的安全屏障。隐蔽通信还可以与加密技术相结合，形成隐藏通信行为与保护信息内容的多层次安全防护体系，从根本上改变卫星通信“被动防御”的安全范式。由此，卫星隐蔽通信受到了学术界和工业界的广泛关注。

现有部分综述文献对卫星隐蔽通信相关研究进行了总结与梳理，涵盖了物理层安全机制、信号伪装与传输优化等典型技术^[2,4-6]，并对不同类型卫星网络中的隐蔽通信策略和应用场景进行了较为系统的归纳。但总体而言，现有综述多聚焦于单一技术路径或特定应用场景，缺乏对空天地三层协同架构下网络模型、信道特性、关键核心技术与多层次安全防护体系的系统性梳理，对人工智能(Artificial Intelligence, AI)、量子通信等新兴技术赋能下的卫星隐蔽通信趋势关注不足，尚未形成从理论基础到工程实现的全景式分析。

收稿日期：2026-02-09；改回日期：2026-07-06；网络出版：2026-07-19

*通信作者：朱政宇 iezyzhu@zzu.edu.cn

基金项目：国家自然科学基金项目(62571495, 62571182)，北京邮电大学网络与交换技术全国重点实验室(SKLNST-2025-1-07)，河南省自然科学基金优秀项目(232300421097)，河南省高校科技创新人才支持计划资助(23HASTIT019)

Foundation Items: National Natural Science Foundation of China under Grant 62571495, 62571182, State Key Laboratory of Networking and Switching Technology (Beijing University of Posts and Telecommunications) under Grant SKLNST-2025-1-07, Natural Science Foundation of Henan Province under Grant 232300421097, Program for Science & Technology Innovation Talents in Universities of Henan Province under Grant 23HASTIT019

本文将全面系统地综述卫星隐蔽通信领域的最新研究进展和未来挑战。首先,分析卫星隐蔽通信的基础理论和网络模型,深入探讨信道特性对隐蔽容量的影响。其次,梳理隐蔽编码、波形设计、波束成形及抗干扰等关键技术及其优化手段。然后,系统总结隐蔽通信面临的主要威胁及多层次安全防护策略。最后,展望卫星隐蔽通信未来的发展方向,重点关注低轨动态组网、AI与量子通信深度融合、第六代移动通信(6th Generation, 6G)非地面网络(Non-Terrestrial Networks, NTN)等前沿领域,为后续研究和工程应用提供理论参考与技术支持。

2 卫星隐蔽通信基础理论

2.1 隐蔽检测机理与信道特性分析

基于经典的Alice-Bob-Willie模型,隐蔽通信通常被建模为针对背景噪声、干扰与信号叠加的二元假设检验问题。在该模型中,发送方Alice将数据信息发送给接收方Bob,而监听方Willie则试图判断通信行为是否存在。这一过程可以建模为以下公式所示的假设检验问题:

$$\mathcal{H}_0: y_w[i] = \sum_{k \in \Phi} \sqrt{\mu_k h_{kw}} x_k[i] + n_w[i] \quad (1)$$

$$\mathcal{H}_1: y_w[i] = \sqrt{\mu_a h_{aw}} x_a[i] + \sum_{k \in \Phi} \sqrt{\mu_k h_{kw}} x_k[i] + n_w[i] \quad (2)$$

其中 $i = 1, 2, \dots, L$ 为信道使用或采样索引。 $y_w[i]$ 和 $x_a[i]$ 分别为Willie的接收信号和Alice的发射信号, $x_k[i]$ 为干扰源的发射信号。 $n_w[i]$ 为接收端的加性高斯白噪声, μ_a 和 μ_k 分别为Alice和干扰源的发射功率, h_{aw} 和 h_{kw} 分别表示Alice到Willie和干扰源到Willie之间的信道增益。 $\mathcal{H}_0$ 和 $\mathcal{H}_1$ 分别对应于Alice保持静默状态的零假设和Alice正在发送信号的备选假设。 Φ 代表干扰源的索引集合,即所有参与向Willie发送干扰信号的干扰源所对应的编号(或标识)构成的集合。 $k \in \Phi$ 表示集合中第 k 个干扰源的索引。

由于缺乏对信号波形的先验信息,且卫星信道环境复杂,Willie通常采用能量检测法,即统计观测窗口内接收信号采样点的平均功率,并将其作为检测统计量。Willie的平均接收信号功率 $\bar{P}_w$ 定义为:

$$\bar{P}_w = \frac{1}{L} \sum_{i=1}^L |y_w[i]|^2 \quad (3)$$

其中 L 为信道使用次数,反映了观测窗口的长度。获得 $\bar{P}_w$ 后,Willie将其与预设的功率检测门限 P_{th} 进行比较以执行二元假设判决:当 $\bar{P}_w > P_{th}$ 时,

Willie判定Alice处于发送状态 $\mathcal{H}_1$;当 $\bar{P}_w \leq P_{th}$ 时,Willie判定Alice处于静默状态 $\mathcal{H}_0$ 。基于该判决准则,Willie的判决可能出现虚警(概率为 P_{FA})或漏警(概率为 P_{MD})。Willie的目标是通过优化检测阈值 P_{th} ,最小化总检测错误概率 $\xi = P_{FA} + P_{MD}$,而Alice的目标则是通过波形设计与资源分配,尽可能增大 ξ 使其趋近于1,使Willie达到随机猜测水平^[7]。

然而,上述标准的能量检测模型隐含了一个严苛的物理前提,在整个观测窗口 L 内,背景噪声功率 σ_w^2 需保持严格的平稳性。在实际的卫星隐蔽通信场景中,节点的超高速运动、多普勒频移的剧烈时变以及多轨干扰源的叠加,会导致Willie接收到的环境噪声呈现出显著的非平稳特性。这种非平稳性对Willie的采样窗口 L 选择构成了致命的博弈挑战。若Willie将观测窗口设置过长,试图累积更多的信号能量,动态漂移的噪声方差就会在窗口内被平均化或引发剧烈抖动,导致静态检测门限 P_{th} 彻底失效,进而引发极高的虚警概率 P_{FA} 。反之,若Willie采用极短的采样窗口以捕捉瞬态噪声分布,检测统计量又会因缺乏足够的独立样本支撑而丧失统计显著性,导致漏警概率 P_{MD} 剧增。因此,在非平稳噪声背景下,Willie难以依赖单一的全局时窗,而被迫转向基于动态短时窗的能量检测或时频联合特征提取,但这将大幅增加其星上计算开销与误判风险。

从Alice的防御视角来看,这种由卫星高动态信道内生的非平稳检测机理,恰好提供了额外的时间维度隐蔽自由度。Alice可以结合短时突发传输模式,预测并利用环境噪声起伏的峰谷规律,将隐蔽信号精准对齐于Willie处的噪声高波动区间或多普勒畸变剧烈的时间切片内,从而通过恶化Willie的窗口对齐精度来最大化隐蔽裕度^[8]。然而,这种利用短时突发传输来最大化隐蔽裕度的策略,是以牺牲通信速率为代价的。平方根定律(Square Root Law, SRL)^[9]指出,在加性高斯白噪声(Additive White Gaussian Noise, AWGN)信道下,在保证Willie的检测错误概率 $\xi \geq 1 - \varepsilon$ 的前提下,Alice在 L 次信道使用中能可靠传输的最大信息比特数 $M(L)$ 存在理论上限:

$$M(L) \leq \sqrt{\frac{2L\sigma_w^2}{e\mu_a^2|h_{aw}|^4}} \left(\mu_a = o\left(\frac{1}{\sqrt{L}}\right) \right) \quad (4)$$

其中 μ_a 为Alice的发射功率, h_{aw} 为信道增益, σ_w^2 为噪声功率。该定律表明,在保证任意低被检测概率的前提下,Alice可传输的比特数最多仅与信道使用次数的平方根 $\sqrt{L}$ 成正比。这一定律从信息论层面深刻揭示了隐蔽通信的根本权衡:为实现高隐蔽

性，必须将发射功率压制到噪声水平，这从根本上制约了在满足隐蔽性前提下可实现的有效通信速率。

从检测理论角度看，虽然基于似然比检验(Likelihood Ratio Test, LRT)的检测器在理论上具有最优性能，但其依赖于接收端对发射波形及实时信道状态信息(Channel State Information, CSI)的精确掌握。在卫星通信场景中，长距离传播损耗、多普勒频移及节点高速运动导致的信道非平稳特性，使Willie难以获取精确的实时CSI。尽管能量检测在噪声不确定性环境下的性能弱于理论最优的LRT，但凭借其低复杂度且无需先验信息的鲁棒性，仍是卫星隐蔽通信中最典型的工程检测模型，属于实际场景下的次优解。

从信道特性分析的角度来看，上述平方根定律的推导通常基于理想的AWGN信道。相比之下，卫星通信链路具有显著的非平稳时变特征。一方面，卫星信道通常采用Rician或阴影Rician模型描述，强视距(Line of Sight, LOS)分量使得Willie能结合轨道可预测性更精确地估计背景噪声功率，从而压缩Alice的隐蔽功率裕度。另一方面，低轨卫星与地面或空中节点之间的高速相对运动会产生显著的多普勒频移，导致载波频率发生偏移与扩展。这种大尺度频移会导致信道相干时间缩短，引发的信号畸变与CSI不确定性等效于降低了接收端的有效信噪比，迫使Alice必须进一步降低编码速率或增加导频开销以维持隐蔽性^[10]。

从信息对抗的博弈视角来看，卫星信道的高动态与非平稳特性并非完全是隐蔽通信的劣势。传统平方根定律所揭示的隐蔽容量极限严格依赖于监听

方对背景噪声功率和理想信道状态的精准掌握。在实际的空天地协同网络中，低轨卫星的高速运动与大气扰动不可避免地引入了噪声不确定性与信道衰落起伏。一方面，大尺度的多普勒频移引发了频谱展宽，叠加星地链路特有的阴影瑞利衰落，使得监听方处的瞬时接收信噪比发生剧烈波动。在这种非平稳观测环境下，监听方无法设定一个恒定且极紧凑的能量检测门限，否则将面临极高的虚警概率。另一方面，发送方可以主动利用这种监听端的信道与噪声不确定性，将隐蔽信号的发射功率隐藏在噪声方差的合理波动区间内。理论研究表明，当监听方处的噪声不确定性超过一定阈值或窃听信道经历连续的动态衰落时，传统的平方根定律将被打破，此时发送方能够以恒定的正功率发射信号，实现渐进隐蔽速率趋于非零常数，而不再受限于传统极限下趋于零的速率限制^[11]。因此，在卫星高动态环境下，隐蔽通信的系统设计核心从单纯的极低功率压制转变为动态不确定性利用。这要求合法通信双方具备高精度的多普勒补偿与信道状态预测能力，在保障自身鲁棒传输的同时最大化监听方的检测盲区。

2.2 卫星隐蔽通信网络架构

卫星通信系统采用三层立体架构，天基、空基、地基各层协同配合，实现了全域覆盖与隐蔽传输，如图1所示。图中以天基Willie为例标注了信道增益 h_{aw} 与噪声功率 σ_w^2 ，该模型同样适用于空基与地基监测场景。

天基、空基与地基节点共同构成卫星隐蔽通信立体化的物理网络底座。天基网络从多维轨道分层组织空天地资源，地球静止轨道卫星(Geostation-

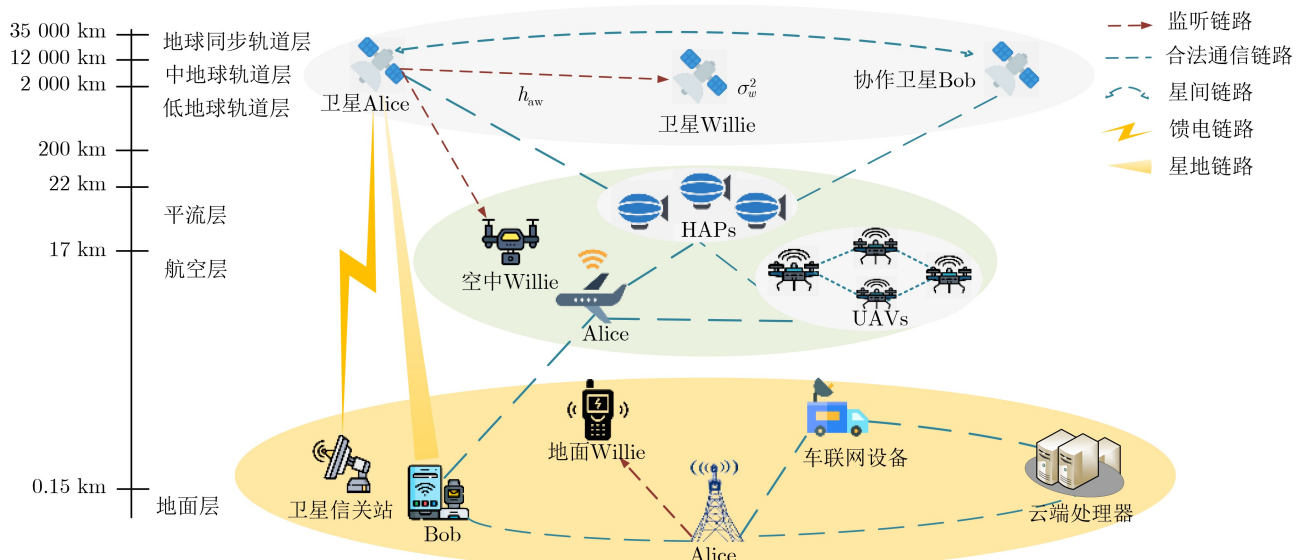


图 1 空天地协同隐蔽通信系统架构图

ary Earth Orbit, GEO)负责量子加密密钥分发,中地球轨道卫星(Medium Earth Orbit, MEO)实施拓扑感知与人工噪声辅助的隐蔽调度机制,低地球轨道卫星(Low Earth Orbit, LEO)通过星间链路(Inter-Satellite Link, ISL)实现低截获概率通信^[12]。空基网络通过高空平台(High Altitude Platform Station, HAPS)与无人机(Unmanned Aerial Vehicle, UAV)构建动态中继。现有研究广泛讨论UAV的隐蔽增强策略,文献^[13]利用深度强化学习解决了动态环境下的隐蔽传输决策问题,文献^[14]则进一步提出基于轨迹规划与发射功率联合优化的隐蔽增强策略,而文献^[15]针对无人机接入低轨卫星的场景,设计了自适应冗余的隐蔽随机接入协议。地面网络作为卫星隐蔽通信的接入层,可通过软件定义网络(Software-Defined Networking, SDN)和量子密钥分发(Quantum Key Distribution, QKD)等手段实现路径自适应与加密保障,提升抗毁性与安全性^[4]。

然而在实际空天地协同交互中,不同物理链路的电磁环境平台约束与潜在窃听威胁存在显著差异。这要求系统不能采用一刀切的隐蔽策略,而必须针对上行链路、下行链路及中继转发链路的独有特征进行差异化设计:

(1)卫星上行链路主要承担地面或海面终端向卫星的数据上传任务。其核心挑战在于地面终端通常受限于发射功率与天线尺寸,且极易面临周边地面或低空Willie的近距离监测。因此上行链路的隐蔽设计侧重于利用地面复杂的建筑物遮挡与多径效应作为天然掩护,结合终端的动态功率压制与极化伪装防止终端物理位置及通信行为的暴露。

(2)卫星下行链路负责卫星向广域地面节点的

数据广播或分发。由于卫星波束覆盖范围极广,下行信号不可避免地会暴露在众多潜在监听节点之下,地面Willie则可通过分布式节点协同或高增益窄带扫描设备对卫星下行链路实施定点监听。同时星载平台在功耗与算力上的严苛限制使得下行链路难以采用高能耗的复杂隐蔽算法。其隐蔽需求侧重于在广域覆盖下进行精准的三维空间波束成形与人工噪声定向投射以压缩地面的可截获区域。

(3)中继转发与星间链路主要用于跨轨道或星机节点间的数据接力。星间链路通常处于视距传播环境且背景噪声极低,导致传统的基于噪声不确定性的伪装手段难以奏效。然而星间链路凭借极窄波束与高方向性将信号能量高度集中,大幅降低了空间截获概率并为隐蔽通信提供了天然优势。面对拥有轨道预判能力的太空Willie,中继链路的隐蔽要求聚焦于高频段极窄波束对准以及基于拓扑快速重构的路由隐蔽。

由于卫星网络的多层架构,位于地面、空中和轨道不同高度的Willie处在显著差异的电磁环境中,其检测能力和策略各不相同。为了建立多层物理架构与隐蔽对抗场景的映射关系,表1系统归纳不同空间层次下Willie的特征与威胁、隐蔽通信面临的挑战及其对应的核心信道特性。

2.3 卫星隐蔽通信的特征与挑战

卫星隐蔽通信的独特性源于其三维立体架构与全域覆盖能力,与传统地面隐蔽通信在拓扑形态、信道机理和对抗环境等方面形成本质差异(见表2)。

在物理层信道层面,卫星链路受到轨道运动、多普勒频移、电离层扰动等因素的共同影响,呈现强时变、非平稳特征,难以沿用地面场景中基于平稳假设的隐蔽容量与检测模型。隐蔽信号设计必须

表 1 Willie在卫星隐蔽通信中的场景分类

场景类型	Willie位置描述	特征与威胁	隐蔽通信挑战	信道特性
地面Willie	地面监听	检测能力强	隐蔽性与可靠性难以兼顾	受限于地面传播的遮挡和多径效应
空中Willie	空中监听	检测范围广	难以应对其移动性	非遮挡时视距传播为主
卫星Willie	轨道监听	全域监听	轨道变化、空间干扰	通常为自由空间传播信道

表 2 卫星与地面隐蔽通信核心特征差异及卫星通信挑战

对比维度	卫星隐蔽通信	地面隐蔽通信	关键差异	卫星隐蔽通信难点
覆盖范围与拓扑 ^[1,3]	空天地三层动态拓扑	地面平面静态拓扑	覆盖尺度	轨道驱动拓扑变化
信道特性 ^[10]	强时变非平稳信道	准平稳多径信道	时变程度	非平稳信道建模
安全威胁 ^[5,32]	多域窃听与干扰节点	局部窃听与干扰	对手能力	多域对抗不确定性
侦测难度 ^[20,33]	多位置协同侦测	单平面侦测	侦测维度	侦测维度不完备
成本与资源 ^[34]	功耗频谱受限	资源相对充足	平台约束	星载资源受限
应用价值 ^[6]	全球高生存通信	区域灵活通信	战略层级	长时稳定隐蔽

面向动态信道构建时变鲁棒的容量分析与波形优化方法。

在安全威胁与侦测环境方面，卫星通信暴露于空、天、地多域协同侦测之下，窃听者可利用高增益天线、空基平台及地面阵列构建分布式截获网络。隐蔽机制因而需要从适配单一侦测模型，转向面向多域、异构甚至部分未知对手的鲁棒设计。

星载平台在功耗、算力和频谱等方面的严苛约束，则进一步限制了高复杂度隐蔽算法的工程可行性。在轨设备难以频繁升级，这要求隐蔽通信技术在保障低可检测性与抗干扰能力的同时，实现模型与算法的轻量化设计，并通过星地协同计算等方式在性能与资源开销之间取得平衡。

2.4 性能指标

在卫星隐蔽通信系统设计中，隐蔽性、可靠性与有效性三者存在严苛的物理折中关系。隐蔽性通常以检测者的检测错误概率来衡量，可靠性可由合法接收端的中断概率或误码率界定，有效性体现为系统的最大隐蔽传输速率或吞吐量。在单一星地直连场景，由于极大的自由空间损耗，提升系统有效性与保障通信可靠性均依赖于较高的接收信干噪比，但是发射功率的提升会使监听端接收信号的KL散度(Kullback–Leibler divergence)激增，极易突破隐蔽性安全红线。这导致有效性与隐蔽性呈现零和博弈态势，其极限性能严格受制于隐蔽通信的平方根法则。在多波束卫星或存在协作干扰节点的场景下，人工噪声(Artificial Noise, AN)的引入改变了量化约束模型。此时通过分配给AN的功率比例来压制非法探测、提升隐蔽性，同时不致严重恶化合法信道的信干噪比保障可靠性与有效性。

为寻求多重约束下的最优折中边界，现有文献针对此类高度非凸的多目标优化问题演化出了三类典型求解算法。一是基于连续凸近似与半正定松弛等传统凸优化理论，在信道先验信息已知时联合优化功率分配与波束成形，将多目标转化为单目标极值问题^[16]；二是引入Stackelberg等博弈论模型，在合法节点与协作干扰者之间建立对抗与激励机制以求解纳什均衡^[17]；三是针对卫星高动态信道导致的

环境未知或状态空间爆炸问题，广泛采用深度强化学习等智能算法，通过环境持续交互动态逼近三者的最优折中前沿^[13]。现有研究也开始引入生成式AI，通过无监督学习与迭代去噪机制动态生成自适应的隐蔽传输策略^[18]。

3 卫星隐蔽通信关键技术

为系统性梳理空天地一体化卫星隐蔽通信的关键技术脉络，本文在综合现有研究工作的基础上，对不同技术路径进行横向对比，如表3所示。

3.1 隐蔽编码方法

隐蔽编码是卫星隐蔽通信的核心物理层技术，旨在通过修改合法传输数据或利用协议冗余字段，将秘密信息嵌入看似正常的空天地协同传输流中。该技术需同时适配多层架构和卫星信道时变特性，以规避多维监听的检测。典型的信道编码隐蔽传输通用框架如图2所示，发送端在信道编码阶段引入秘密信息，使得生成的编码符号在经过无线信道传输后，对于合法接收端可正常解调，而对于被动监听终端则难以从背景噪声或正常业务流中区分出隐蔽信息的存在。

3.1.1 信号伪装类隐蔽编码方法

信号伪装类隐蔽编码方法通过在编码阶段塑造发射信号的统计分布，使其在功率、频谱及高阶统计特性上与信道背景噪声高度一致，从而在物理层规避Willie的存在性检测。该类方法的核心思想源于SRL框架下对统计不可区分性的研究，并已被证明在高斯及近高斯信道中尤为有效。典型代表是Yu等人^[19]提出的高斯随机化编码方案，该方法通过随机编码使发射信号在分布上逼近高斯噪声，从而显著降低Willie基于能量或统计特征的检测能力。上述基于统计伪装的隐蔽编码思想及其典型实现形式，已在Chen等人^[20]的隐蔽通信综述工作中得到系统梳理和总结，为卫星场景下物理层隐蔽编码设计提供了统一的理论视角和方法框架。

3.1.2 AI辅助的自适应隐蔽编码方法

AI辅助的自适应隐蔽编码方法以深度学习、强化学习等智能算法为赋能工具，通过编码规则的动

表 3 卫星隐蔽通信关键技术横向对比

关键技术	实现复杂度	卫星载荷资源需求	隐蔽增益	主要优势	局限性
隐蔽编码 ^[19,20]	传统易部署，AI交互状态复杂	AI模型算力与能耗开销极大	受限于平方根定律理论界限	射频硬件免改，协议平滑兼容	非平稳信道下易漏警失配
扩频技术 ^[22]	需攻克严苛的收发时序同步	需极大射频带宽及前端处理	降低功率谱密度，抗窄带侦测	抗截获与抗干扰能力强	频带占用极大，频谱效率极低
波束成形 ^[21,24]	需动态拓扑下的高速波束对准	大规模阵列受限体积与功耗	物理压缩三维可截获空间区域	隐蔽与高速率传输可兼得	极度依赖实时CSI，受老化影响
人工噪声 ^[17,27]	需协同节点与干扰矩阵分发	严重挤占星上有效发射功率	主动打破敌方检测门限收敛性	主动防御，对抗强位置先验窃听	耗能高，且需敌方先验

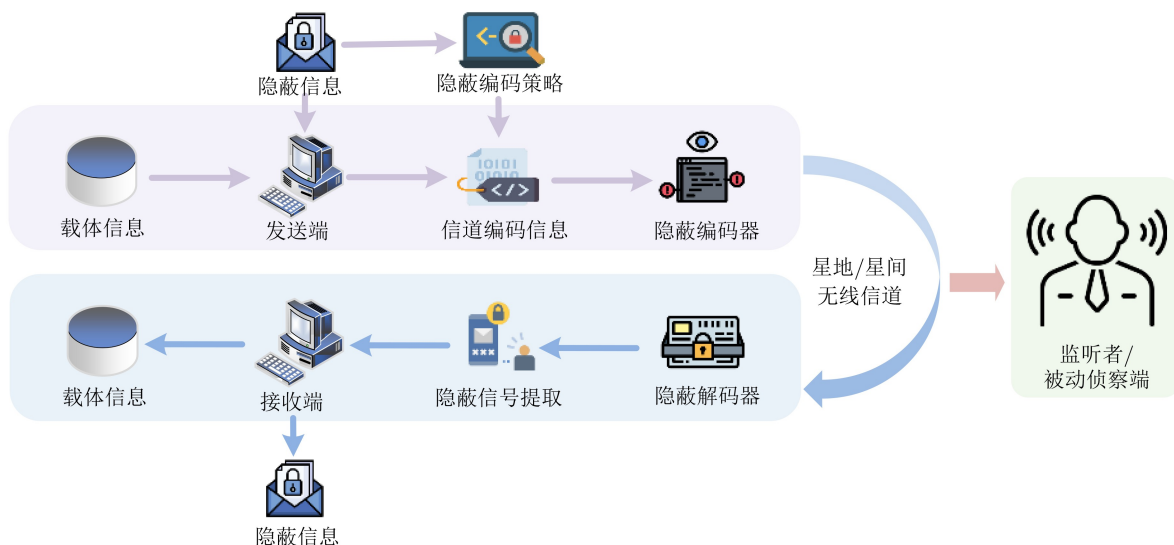


图 2 信道编码隐蔽传输框架图

态优化，适配卫星信道的复杂多变特性，核心是编码方法的自适应调整能力，而非算法本身成为编码方法。

自适应编码优化基于深度学习模型实时分析卫星信道状态，动态调整编码参数与调制规则。通过强化学习算法平衡隐蔽性、抗干扰性和传输效率的多目标需求，相较于传统固定编码方式，可根据卫星信道的动态变化实现最优传输策略，降低被敌方检测的风险。在复杂卫星信道条件下，还可通过编码冗余度的动态提升或调制方式的切换，保障通信可靠性。

在工程实现上，AI辅助隐蔽编码常与模型驱动设计结合，形成较为常见的两阶段实现流程：首先由学习模型对噪声不确定性、干扰态势或可用通信窗口等关键状态进行估计与预测；随后在在线环节联合优化码率、冗余度、发射功率与占空比等参数，从而在满足隐蔽约束的同时兼顾可靠性与实时性。考虑星载算力与能耗受限以及在轨环境分布漂移，相关方案通常采用轻量化网络结构，并配合低开销的在线更新或自适应校准机制，以降低计算与通信开销并提升工程可部署性。

3.2 隐蔽波形设计

在隐蔽编码实现信息嵌入的基础上，物理层波形设计通过对信号时频特性、空间传播形态及能量分布的精细控制，进一步降低信号被Willie检测的概率。与隐蔽编码侧重信息映射不同，隐蔽波形设计以信号可检测性最小化为核心目标，通过削弱异常能量聚集、限制可观测信号特征维度，使卫星发射信号在统计特性上更接近背景通信或噪声环境，从而规避频谱侦测与能量检测等常见监测手段。

3.2.1 时频域波形优化技术

时频域波形优化通过对信号表示域结构进行重构，在不显著改变平均功率与频谱占用的前提下，降低非授权接收方对信号的检测与恢复能力。与空间域通过能量定向辐射抑制监听不同，时频域方法侧重引入额外的参数不确定性和结构混淆，使信号在错误变换域下呈现出类噪声统计特性，从而削弱基于能量检测、匹配滤波及特征提取的监听性能。

分数域变换及其扩展形式为时频域隐蔽波形设计提供了新的实现途径。通过在二维调制框架中引入连续可调的分数域参数，信号能量可在时域、频域以及延迟多普勒域之间实现灵活映射。文献[10]通过分数域双索引调制对二维波形结构进行重构，在合法接收方已知参数的条件下实现可靠通信，同时利用域匹配失配显著降低Willie的信号可恢复性。

总体而言，时频域波形优化并非直接以最小化检测概率为目标，而是通过破坏非授权接收方的信号可恢复性，间接提升系统的隐蔽性能。该类方法可作为空间域隐蔽波形设计的有益补充，尤其适用于与多天线、波束可控的卫星通信系统相结合的场景。

3.2.2 空间域波形优化技术

空间域波形优化通过控制信号的空间传播方向和能量分布，实现对合法用户的定向增强与对窃听者的能量抑制，是卫星隐蔽通信中区别于地面系统的重要技术方向。依托多天线和卫星波束控制能力，空间域优化可显著降低信号在非目标区域的可观测性。波束成形优化是空间域隐蔽波形设计的核心技术之一。通过合理设计发射波束成形向量，在

最大化合法用户接收信号功率的同时，有效抑制窃听者方向上的有用信号能量，从而显著降低信号被截获的概率。文献[21]在噪声不确定和瑞利衰落信道条件下分析了波束成形对隐蔽概率、连接中断概率和隐蔽吞吐量的影响，结果表明，非理想噪声条件会显著削弱隐蔽性能，因此需要在空间域波形设计中加以针对性优化。

进一步地，文献[22]提出的时频空多维域能量弥散隐蔽通信模型，通过联合控制空间域能量分布、天线方向性函数及空间衰减特性，为多波束卫星系统及多轨道卫星协同组网场景下的隐蔽波形设计提供了有效思路，可在更大空间尺度上抑制信号的可检测性。除常规阵列波束优化外，近期也有研究引入可移动天线(Movable Antenna, MA)这一结构自由度，通过联合优化阵列位置与发射波束，在满足隐蔽约束的条件下提升多用户隐蔽和速率，并在角度估计误差等条件下表现出更强鲁棒性[23]。此外，针对高动态场景，Hua等人[24]提出了基于视觉感知的波束控制框架，利用视觉传感器动态锁定合法接收端位置，在高频段实现波束的即时重构与精准指向，从而在规避监听的同时有效降低信号的截获概率。

值得注意的是，尽管MA与可重构智能表面(Reconfigurable Intelligent Surface, RIS)已被证明能够有效重构星地受阻链路并为系统提供丰富的空间自由度[25]，但在星地高动态网络中部署上述架构面临着严峻的CSI获取难题。首先，RIS通常由大量无源反射阵子组成，而MA则引入了连续的空间位置变量，这使得整个系统的级联信道模型变得极其复杂。若采用传统的正交导频估计方法，将面临变量高度耦合与导频开销呈指数级增长的维度灾难。其次，低轨卫星的高速移动导致空间几何拓扑剧烈时变，信道相干时间大幅缩短。在极其有限的通信窗口内，传统的基于实时大容量导频的信道估计机制不仅挤占有效数据吞吐量，且极易因估计时延导致瞬时信道状态信息(Instantaneous Channel State Information, I-CSI)严重老化失效。

为克服空间动态几何拓扑带来的挑战，现有研究主要演化出两类降维与解耦策略。首先是基于先验信息与AI赋能的信道预测技术[24]。该类技术结合视觉感知等物理位置先验或卫星轨道星历的可预测性，提前预测并补偿多普勒频移，以指导MA和RIS进行宏观的视距对准。其次是基于多变量解耦的双时间尺度信道估计机制[23,25]。该方案不再试图一次性获取全维度的I-CSI，而是利用星地信道的空间稀疏性，将复杂的级联信道估计过程进行多维

度的解耦提取。具体而言，针对MA的连续空间位置变量、RIS的海量阵子相位变量以及多径信道衰落变量高度耦合的难题，系统在时间尺度与参数维度上进行剥离。在慢时间尺度上，系统首先利用开销极低的统计信道状态信息(Statistical Channel State Information, S-CSI)或位置先验，完成大尺度的角度估计，以此驱动对MA与RIS的宏观参数重配；而在快时间尺度上，由于宏观层面的对准已经大幅降低了有效信道的维度，系统此时仅需极少量的导频交互，即可完成对低维I-CSI的精准估计与追踪。这种解耦估计策略直接绕开了全维导频获取的难题，化解了高动态环境下的导频开销与估计时延矛盾。

3.3 隐蔽传输模式

隐蔽传输模式是在既定隐蔽编码与波形设计基础上，侧重于网络层面的传输组织与节点协作机制。该模式通过在时间、空间及网络维度上的资源调度，降低通信行为在宏观尺度上的被发现概率，主要包含非协同自主传输与多节点协同传输两类典型范式。

3.3.1 非协同隐蔽传输

非协同隐蔽传输聚焦于单卫星节点的自主优化，核心在于通过自适应调整传输参数实现抗检测。该模式无需外部节点协作，尤其适用于单星独立执行任务的场景。从信息论角度看，非协同隐蔽通信在被动Willie存在的条件下面临严格的传输速率约束。文献[9]研究表明，在加性高斯噪声信道中，若要求Willie的最优检测错误概率之和保持接近1，则在 L 次信道使用内可实现的隐蔽可靠传输信息量仅随 $\mathcal{O}(\sqrt{L})$ 增长，即隐蔽通信容量趋于零。

为应对这一挑战，现有研究主要聚焦于多维资源的精细化管控，利用高增益窄波束在空间域规避监听，并采用短时突发传输策略压缩暴露时间窗口[26]。此外，基于信道状态信息的自适应功率控制也是关键，通过动态调整发射功率使其紧贴噪声掩蔽门限，旨在满足隐蔽约束的同时最大化单链路的有效吞吐量。

3.3.2 协同隐蔽传输

协同隐蔽传输依托多节点之间的联合协作，通过分布式干扰伪装、协同波束成形与虚假目标构造等手段，在更大空间尺度上削弱信号的可检测性。相比非协同模式，该方式能够在更复杂侦测环境下显著提升隐蔽性能，但同时节点间的同步精度、能量供给与协作控制能力提出了更高要求。

在具体实现中，多波束卫星系统可通过多个波束并行发射伪随机人工噪声或伪装信号，对外部侦

测设备形成分布式干扰,从而降低目标通信链路在空间域和频谱域内的可分辨性。此外,可引入无人机作为协作节点,在卫星通信过程中向特定空间区域注入可控干扰或虚假目标信号,实现对潜在Willie的定向伪装与误导。图3(a)示意了双无人机协同参与的隐蔽通信与动态频谱协同抗干扰场景,直观展示了协作节点在空间域内对卫星通信链路的掩护机制。通过多节点间的信道协作与协同干扰设计,可在不显著增加总发射功率的前提下,有效提升通信链路的隐蔽性与鲁棒性。

协同隐蔽传输在工程实现中主要面对两类关键问题,协作节点的资源约束问题与多节点协同的同步与信道失配问题。一方面,无人机作为移动协作节点受限于能量与算力资源,可通过联合资源调度与能量管理机制维持长期协作。已有研究从能量补给与协同调度角度探讨了无人机长期协作受限问题,提出可结合同步无线信息与能量传输技术,由卫星向无人机定向传输能量,并采用隐蔽能量传输波形以降低能量链路的暴露风险^[27]。另一方面,为应对低轨卫星与高机动无人机等跨层协同中的双重高动态特性,CSI交互与获取机制的设计成为研究重点。星间及星机链路的长距离传播与高速相对运动会引入显著的时延不确定性与多普勒频移,传统的全量瞬时CSI反馈会导致严重的信令暴露风险与高昂开销。对此,近期文献提出了一种基于感知信息辅助的CSI降维与反馈策略,在宏观尺度上利用全球导航卫星系统提取的无人机位置和速度等先验感知信息进行辅助压缩,在微观尺度上结合这种低维感知信息在延迟多普勒域内对信道估计误差进行自适应动态抑制与补偿^[28]。这种机制不仅大幅降低

了高动态场景下的反馈开销,还能有效保障协同波形的精确性。

在此基础上,跨层联合资源调度正成为提升广域隐蔽能力的关键。现有研究不再局限于单一节点参数优化,而是实现了星载发射功率与无人机三维轨迹及协作干扰强度的多维联合调度。通过构建星地与星机联合的拓扑重构模型,在满足无人机运动学约束和能量效率的前提下,动态调整波束指向与干扰功率,从而实现全域隐蔽性能的系统级跃升^[29]。这种跨层协同不仅有效克服了单层网络的物理覆盖盲区,更通过多维资源的深度耦合增强了系统对抗分布式侦测网的鲁棒性。

3.4 干扰辅助与频谱捷变技术

区别于波形设计等内生性隐蔽手段,主动防御技术侧重于通过频谱博弈与能量对抗,在复杂的电磁环境中保障链路的生存能力并主动恶化监听方的检测环境。

3.4.1 认知频谱捷变技术

针对卫星通信面临的全域监听与恶意干扰威胁,具备认知能力的频谱捷变与精细化功率控制是保障隐蔽链路生存的关键物理层手段。

一方面,动态功率隐蔽是抗监听的核心。传统的固定功率策略难以适应卫星的高动态信道变化,容易导致信号溢出噪声掩蔽门限。而基于CSI的自适应功率控制技术,能够根据链路损耗和背景噪声的实时波动,将发射功率严格动态压制在噪声水平附近,从而在保证最低解调门限的同时最大化隐蔽裕度。另一方面,认知抗干扰技术承担着维持隐蔽链路可靠性的关键角色。如图3(b)所示,卫星系统可结合频谱动态规划、自适应调制编码以及多节点

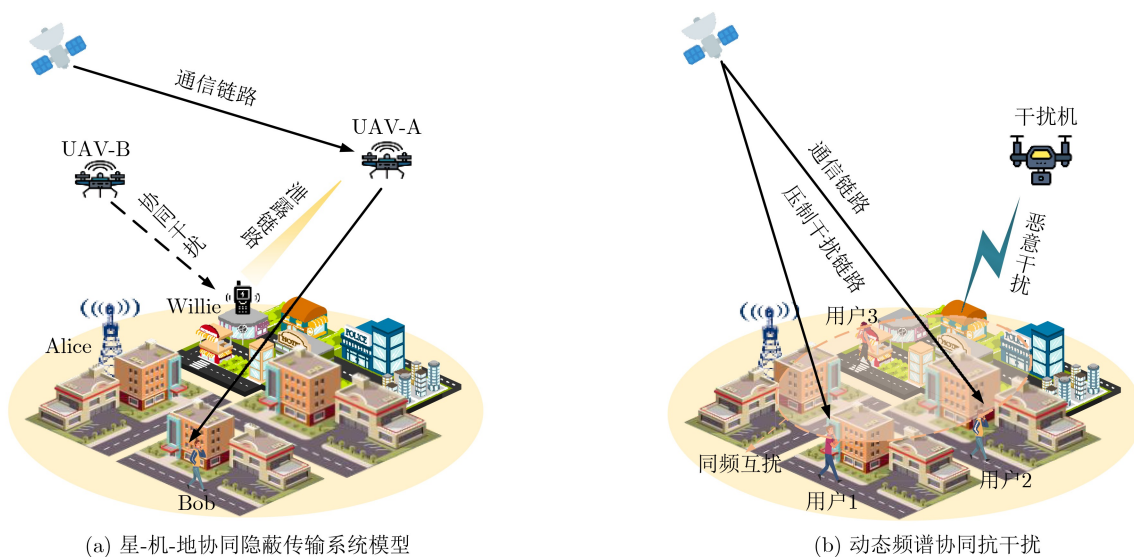


图3 双无人机协同的隐蔽通信及动态频谱协同抗干扰

协同等手段, 利用认知无线电技术实时探测频谱空穴。通过频谱捷变在规避强干扰频段的同时, 避免形成稳定可追踪的频谱与功率特征模式, 系统能够在高对抗电磁环境下有效兼顾通信生存能力与低可检测性。

3.4.2 人工噪声辅助隐蔽干扰技术

AN技术通过在发射信号中主动叠加干扰分量, 从信道容量层面扩大合法用户与窃听者之间的性能差异。与常规波束成形仅抑制旁瓣能量不同, AN技术利用多天线或协作节点^[30], 在合法信道的零空间方向发送人工噪声, 而该噪声对合法接收端保持正交或可知。这种策略使得Willie无法准确估计背景噪声功率, 从而打破其能量检测门限的收敛性, 在不显著增加信号暴露特征的前提下, 显著提升系统的隐蔽传输速率与安全区域边界。

通过优化信号与人工噪声之间的功率分配策略, 在满足合法通信质量约束的条件下尽量降低总发射功率, 可进一步减少信号被能量检测器发现的概率, 实现隐蔽性与通信可靠性的协同提升^[17]。

3.5 面向卫星场景的隐蔽增强技术

卫星通信固有的高速运动、长距离传播、全球广域覆盖以及独特的空间与大气信道特性, 使其在隐蔽通信设计上面临区别于地面系统的挑战。同时, 星载平台在功耗、计算能力与在轨升级方面的限制, 也进一步制约了复杂隐蔽机制的直接部署^[30]。已有文献针对卫星通信的运行环境特性, 从系统结构、信道利用和资源适配等多个维度, 提出并验证了一系列隐蔽增强思路。

3.5.1 轨道拓扑与频谱协同利用

多轨道卫星系统在轨道高度、覆盖范围和运动速度上的天然差异, 为隐蔽通信提供了可利用的结构多样性^[6]。相关研究通常构建由GEO、MEO与LEO卫星协同组成的多层网络^[5], 利用各轨道层间的异构频谱资源进行协同调度。这种机制不仅使通信拓扑随轨道运动持续演化, 还能通过跨层链路的动态频率捷变, 打破单一频段的持续辐射特征, 从而在一定程度上削弱Willie对稳定通信路径的感知能力。

3.5.2 卫星信道特性适配与利用

卫星信道所具有的方向性、多普勒效应和时变特性, 在部分研究中逐渐被视为隐蔽通信的潜在优势加以利用^[31]。以星间链路为代表的高方向性通信方式, 凭借其极窄波束和能量高度集中的特性, 有助于压缩信号在空间中的可截获区域^[32,33], 从物理层面降低非授权节点的截获概率, 为星间隐蔽传输提供天然支持。此外, 低轨卫星高速运动引入的可

预测多普勒频移, 为信号设计提供了额外的自由度。已有研究尝试利用分数域变换等手段对抗或利用多普勒频移^[10], 将跳频序列、载波偏移与轨道诱导的多普勒变化相匹配, 使非协作Willie难以区分通信信号与背景噪声或自然信道扰动。

3.5.3 受限星载资源的轻量化适配

受限星载平台的计算能力与功耗预算, 隐蔽通信机制在设计上需强调轻量化与可实现性^[34]。针对这一特点, 相关工作多从工程可实现性角度出发, 倾向于采用低复杂度的加密、跳频与信号伪装策略, 以避免复杂计算带来的能耗和时延负担。在下行链路中, 超宽带脉冲成形等低功率谱密度传输方式也被用于降低信号在频域上的可检测性^[22], 使其难以被地面高增益窄带接收设备有效捕获。

通过将隐蔽增强策略与星载资源约束相匹配, 可在不显著增加系统负担的前提下, 维持通信行为在功率、频谱和时间维度上的低可感知特性, 从而提升卫星隐蔽通信在实际部署环境中的可行性与鲁棒性。

4 隐蔽通信安全威胁与防御

4.1 主要安全威胁

尽管前述物理层技术提供了基础的隐蔽保障, 但卫星隐蔽通信的安全威胁源于空间环境的开放性、轨道运动的可预测性及多层架构的复杂性, 相较于地面隐蔽通信, 具有显著的场景特殊性。

4.1.1 全域多维监听威胁

卫星通信的开放性使得Willie能够构建全域覆盖的监听网络。为了严谨评估系统隐蔽容量的理论下界, 必须对这种全域多维威胁进行明确的物理与信息假设。相较于地面受限环境, 其多维威胁特性集中反映在拓扑协同、硬件边界与先验信息三个维度的非对称优势上。在拓扑协同方面, 有别于传统的单点孤立监听, 全域威胁通常表现为跨域多节点联合监听, Willie能通过空天地分布式节点进行软硬判决数据融合, 有效规避单一视距链路的非平稳衰落与遮挡盲区, 极大压缩了合法通信的隐蔽空间。在硬件参数边界上, 隐蔽性分析通常采用最恶劣的强Willie假设, 即假定监听方配备了孔径与增益均远超合法接收端的大规模天线阵列, 且具备逼近热噪声极限的极高接收灵敏度, 在此极值假设下, 其最终检测性能仅客观受限物理平台的底层热噪声与卫星高动态引起的残余多普勒频偏。在先验信息界定方面, 依据掌握信息的程度, 全域威胁可进一步划分为缺乏信号特征先验且只能依赖能量检测或高阶统计量提取的非协作盲侦测, 以及掌握

除加密密钥外所有公共通信参数和完美帧同步能力从而可实施最优匹配滤波检测的完全先验定向窃听。

4.1.2 轨道依赖型干扰威胁

基于可预测的卫星轨道星历与波束覆盖规律,传统隐蔽机制面临极具破坏性的轨道依赖型主动威胁。在前文界定的全域多维监听能力基础之上,攻击方可针对特定星地或星间链路进行精准的物理轨迹预判。利用这种时空先验性,攻击方不仅能实施高效的被动截获,更有能力在关键可见时间窗口内,有计划地定向部署大功率射频干扰与信号欺骗攻击。这种依托轨道可预测性发起的侦扰一体手段,能够对目标链路实施精准的压制,或诱导合法接收端产生判决错误,使得本就受限于极低发射功率与严苛信噪比的短时隐蔽传输面临极高的中断与失效风险。

4.2 多维协同防御方案

针对上述威胁,可构建涵盖物理层基础防护、网络层跨域协同和面向特定威胁的增强防护在内的广义分层防御体系。

4.2.1 物理层:空间-信道协同防护

根据3.2节所述的空间域波形与波束优化技术,在物理层安全增强方面,Jeon等人^[35]提出的物理层安全(Physical Layer Security, PLS)框架在卫星场景中可与随轨动态波束成形结合,通过利用GEO卫星全局监测数据及LEO卫星轨道预报,动态调整波束指向和形状,一方面自适应星地链路的多普勒频移和信道快变特性,另一方面将信号能量尽可能限制在合法覆盖区域,从而为广域覆盖下的低可检测性提供基础支撑。

针对星载功耗与算力受限约束,文献^[36]提出轻量化协同方案,在资源分配时优先考虑卫星轨道周期与信道时变性,加密模块采用适配星上边缘计算的简化算法,在保障隐蔽性和抗干扰性的同时控制计算和功耗开销。

此外,新兴技术如RIS可与卫星多波束技术协同,通过动态调控信号传播路径,将能量定向汇聚到合法接收端并对潜在监听方向形成空间“阴影区”,有效降低旁瓣泄漏风险。结合具有极窄波束和高度定向性的星间链路,可在星间建立高保密性隐藏通道,从空间域物理特性上减小被截获的空间范围。

4.2.2 网络层:跨域动态协同防护

在多域协同防护方面,现有两种核心技术范式适配卫星场景,一是基于空频资源协同的跨域隐蔽传输,利用LEO星座的快速重访特性与认知无线电

技术,动态探测频谱空穴,实现频段、轨道位置甚至中继路径的联合跳变,从而削弱Willie和干扰者的时空预测能力。二是基于智能赋能的跨层协同防护,典型代表为Guo等人^[37]近期提出的星地联邦学习架构,创新性地将星载边缘计算节点、地面信关站、空基无人机作为联邦节点,通过分布式模型训练实现威胁特征跨域共享,在无需集中上传原始数据的前提下构建全局防御模型,既降低星上数据暴露风险,又提高对全域多源威胁的适应性。

4.2.3 面向典型威胁的增强防护

针对主动监听威胁,可采用多维度防护策略。在第3.4节人工噪声技术的基础上,文献^[17]提出协同干扰机制,通过博弈论激励自私的干扰设备生成人工噪声,干扰窃听者的信号接收。该方法采用两阶段Stackelberg博弈框架优化干扰功率与激励策略,并将安全路由建模为最短加权路径问题,优先选择干扰增强路径以提升整体PLS性能。文献^[38]进一步引入通信质量(Quality of Service, QoS)约束,采用拉格朗日乘数法优化各节点发射功率,在满足连接中断概率(Connection Outage Probability, COP)阈值要求的前提下,最小化路由的保密中断概率(Secrecy Outage Probability, SOP),构建安全与服务质量的双目标优化模型。此外,文献^[39]利用双极化卫星信道的正交特性,提出了基于极化滤波的物理层安全传输方案,从信号维度隔离窃听威胁。

在多接收器协同防护方面,文献^[40]通过联合优化多波束系统的波束成形向量,实现多用户信号的协同管理,使合法用户的中断概率(Outage Probability, OP)满足约束,同时抑制窃听者的截获概率(Intercept Probability, IP)。文献^[41]提出,在卫星多播场景中采用XOR网络编码,将用户A和B的数据异或后统一广播,各用户通过自身已知信息完成解码,从而减少冗余信息暴露、增强链路隐蔽性,并通过联合优化返回链路与前向链路的时间分配在保密性和系统容量之间实现权衡。

通过以上物理层、网络层及针对性防护方案的有机结合,可构建多层次、多维度的卫星隐蔽通信安全防护体系,在星载资源受限的前提下显著提升系统的抗干扰能力与整体安全性。

5 未来研究方向与挑战

面对日益严峻的空天安全挑战,单一技术的优化难以满足需求,未来的研究需要在多个核心领域同步推进。如图4所示,这四个维度共同构成了下一代卫星隐蔽通信的技术蓝图。



图 4 卫星隐蔽通信未来发展的关键技术方向

5.1 动态环境下的鲁棒性传输

在CSI非理想化情形下，噪声和信道的不确定性将严重制约隐蔽通信的系统性能，如何提升复杂环境下的可靠性与传输速率是亟待突破的瓶颈。特别是低轨卫星的高速运动造成了信道快速时变、大多普勒频移以及时延的不确定性，这对隐蔽通信的稳定性构成了严峻挑战^[42]。未来的研究重点不应仅局限于静态模型，而需聚焦于高精度动态信道预测模型的开发以及资源的自适应分配机制。通过建立基于实时轨迹信息和运动特性的传输优化策略，实现对动态干扰的主动适应，从而有效增强隐蔽通信在非理想信道条件下的抗干扰能力和隐蔽性。

然而在非平稳信道下，维持高精度的信道追踪通常依赖于发送密集的导频序列或进行高频次的状态反馈，但这会产生极具辨识度的周期性电磁特征，从而破坏系统隐蔽性。因此，未来的核心科学问题在于如何破解预测精度与隐蔽性暴露之间的固有冲突。亟须探索基于数据驱动、无需依赖已知导频信号的盲信道估计技术，或深入挖掘卫星轨道等物理先验信息，实现以极低开销甚至无额外信号开销的方式，从系统内部推断信道状态。

5.2 AI赋能卫星隐蔽通信

AI凭借非线性挖掘与决策能力，为隐蔽通信提供了极具前景的技术路径。已有研究展示了深度强化学习在空天网络多维资源联合调度中的强大潜

力^[36]。基于此类智能动态编排机制，通过引入隐蔽性约束，可进一步支持发射功率、波束指向及频谱资源的自适应联合优化，从而在复杂动态环境下实现智能化的频谱伪装与隐蔽传输。在此基础上，文献^[14]基于深度强化学习算法联合优化了无人机的飞行轨迹与发射功率，在无需先验信道信息的条件下显著提升了隐蔽传输速率。同时，AI在空间维度的应用也至关重要，文献^[29]指出基于AI的动态轨迹规划与三维波束成形联合设计，有助于提升非平稳信道下的链路鲁棒性。

然而，现有研究常忽略工程落地的核心矛盾。深度强化学习等复杂模型在优化过程中需要进行海量的数据状态交互和庞大的参数计算，这与星载平台在功耗、体积、重量及散热等方面的严苛物理限制存在根本冲突。未来的关键科学问题在于如何突破高算力需求与低功耗平台之间的工程壁垒。具体而言，亟须探索面向受限星载资源的轻量化AI模型，通过移除神经网络冗余连接的网络剪枝技术，或将大模型知识迁移至小模型的知识蒸馏技术来压缩模型。更为根本的解决思路在于改变计算范式，构建星地协同的分布式学习架构。文献^[43]将耗能高的模型训练任务放在算力充足的地面云中心完成，而低轨卫星作为雾节点仅执行低功耗的推理任务。这种架构被认为是实现星地集成网络中原生智能的关键，能够有效调和星上算力与能耗的约束，

这为从工程上破解星载AI的算力能耗瓶颈提供了可能。

5.3 面向6G NTN的隐蔽通信

6G NTN通过多维异构架构实现了全球无缝连接,但节点的高动态移动与信道频繁快变导致了网络拓扑的高度不确定性。这种复杂环境要求隐蔽通信机制必须具备极高的动态适应与重构能力,需结合机器学习算法实时感知网络状态,利用多普勒效应补偿与动态信道预测技术确保传输的鲁棒性。为应对这一挑战,多通信节点的协同机制显得尤为关键:无人机^[44]、低轨卫星与RIS^[45]的深度融合可显著提升系统韧性。利用卫星集群的协同工作与分布式控制优势,不仅能有效克服组网带来的冲突与干扰,还能通过隐蔽信号的分布式传输与联合处理,构建通感算一体化^[46]的广域隐蔽网络,并结合动态资源共享机制进一步增强安全性。

尽管多节点协同与分布式控制能有效提升广域网络的隐蔽性,但其工程落地受制于严苛的时空同步与信令交互瓶颈。在6G NTN大规模异构组网中,无人机、低轨卫星与RIS间的深度融合高度依赖于微秒级的节点间同步与频繁的控制面状态交互。这种海量的协同信令本身即构成了极易被非授权方截获的辐射特征。为缓解这一暴露风险,现有研究开始引入多用户通感一体化联合波束赋形与协作干扰技术^[47],或利用可移动天线主动重构空间信道以兼顾探测精度与隐蔽容量^[48]。然而这些物理层面的前沿技术在跨域节点扩展时仍难以彻底摆脱对交互信令的依赖。因此,未来的具体科学问题在于如何设计极低开销甚至无连接的隐蔽同步协议,以及如何在缺乏全局瞬时交互的条件下,基于感知通信一体化实现异构节点的多用户联合波束赋形与静默资源调度。

5.4 融合量子通信技术的卫星隐蔽通信

量子通信技术为突破经典隐蔽通信的理论极限带来了全新的物理层安全路径。现阶段研究多聚焦于量子密钥分发技术,文献^[49]系统评估了包含有限密钥效应的卫星量子密钥分发实用架构,并深入分析了指向误差与大气湍流对密钥生成率的严重制约。但长距离自由空间损耗、低轨星地链路复杂传播环境的影响^[50],以及太阳背景光子噪声都是量子隐蔽通信在空天地链路中面临的物理瓶颈。因此该领域未来的核心科学问题在于如何突破强背景噪声下的高保真度单光子探测边界,以及如何在极低信噪比下精准区分微弱的量子隐蔽信号与背景噪声。相应的关键技术瓶颈包括如何设计抗大气湍流的鲁棒性量子态波形,以及如何突破极短卫星可见窗口

内有限统计起伏效应导致的隐蔽吞吐量衰减。这些底层物理难题的突破将是量子隐蔽机制从实验室内理想光纤迈向全天时星地复杂组网的关键。

6 结论与展望

本文系统综述卫星隐蔽通信的理论基础、关键技术及未来挑战。首先,基于Alice-Bob-Willie模型,分析卫星信道特性对隐蔽通信容量的制约机制,讨论适用于非理想信道的修正型平方根定律,揭示多普勒频移、大气衰减等因素对隐蔽性能的双重影响。其次,围绕“天基、空基、地基”三层协同架构,系统梳理隐蔽编码、智能波束成形、频谱分集、动态频谱接入等核心技术,并总结抗监听与抗干扰的多层级防护机制。进一步地,本文还探讨人工智能、量子通信等新兴技术在提升卫星隐蔽通信智能性与安全性方面的潜力。尽管卫星隐蔽通信在架构设计、信号处理和资源调度等方面已取得显著进展,但仍面临低轨动态组网、非理想信道鲁棒传输、星载资源受限等多重挑战。未来研究应聚焦于发展高精度信道预测与多普勒补偿模型,提升高速移动环境下的通信稳定性;推动AI与量子技术的深度融合,构建智能协同的跨层隐蔽传输机制;突破轻量化星上处理与低功耗编码算法,增强系统在资源约束下的实战能力;建立跨域协同的安全评估与标准化体系,促进卫星隐蔽通信在6G天地一体化网络中的规模化应用。

综上所述,卫星隐蔽通信作为空天信息安全的战略性技术,其发展不仅依赖于传统通信与信号处理技术的进步,还需与人工智能、量子科技等前沿领域交叉融合,推动安全机制从仅强调内容保密向兼顾低可探测性、抗干扰与可部署性的综合防护演进,为构建高可靠、高隐蔽的空天通信网络提供支撑。

参考文献

- [1] KODHELI O, LAGUNAS E, MATURO N, *et al.* Satellite communications in the new space era: A survey and future challenges[J]. *IEEE Communications Surveys & Tutorials*, 2021, 23(1): 70–109. doi: [10.1109/COMST.2020.3028247](https://doi.org/10.1109/COMST.2020.3028247).
- [2] 邓娜, 邢成文, 赵楠. 卫星隐蔽通信技术综述[J]. 中兴通讯技术, 2024, 30(5): 55–67. doi: [10.12142/ZTETJ.202405009](https://doi.org/10.12142/ZTETJ.202405009).
DENG Na, XING Chengwen, and ZHAO Nan. A review of satellite covert communication technologies[J]. *ZTE Technology Journal*, 2024, 30(5): 55–67. doi: [10.12142/ZTETJ.202405009](https://doi.org/10.12142/ZTETJ.202405009).
- [3] 陈全. 面向低轨巨型星座的星地一体化网络关键技术研究[D]. [博士论文], 国防科技大学, 2021. doi: [10.27052/d.cnki.gzjgu.2021.000477](https://doi.org/10.27052/d.cnki.gzjgu.2021.000477).

- CHEN Quan. Towards LEO mega-constellation: Study on integrated satellite-terrestrial networks[D]. [Ph. D. dissertation], National University of Defense Technology, 2021. doi: [10.27052/d.cnki.gzjgu.2021.000477](https://doi.org/10.27052/d.cnki.gzjgu.2021.000477).
- [4] PAN Gaofeng, YE Jia, AN Jianping, *et al.* Latency versus reliability in LEO mega-constellations: Terrestrial, aerial, or space relay?[J]. *IEEE Transactions on Mobile Computing*, 2023, 22(9): 5330–5345. doi: [10.1109/TMC.2022.3168081](https://doi.org/10.1109/TMC.2022.3168081).
- [5] YUE Pingyue, AN Jianping, ZHANG Jiankang, *et al.* Low earth orbit satellite security and reliability: Issues, solutions, and the road ahead[J]. *IEEE Communications Surveys & Tutorials*, 2023, 25(3): 1604–1652. doi: [10.1109/COMST.2023.3296160](https://doi.org/10.1109/COMST.2023.3296160).
- [6] 于季弘, 蔡雨庭, 刘家豪, 等. 空天隐蔽通信技术综述[J]. 重庆邮电大学学报(自然科学版), 2023, 35(5): 775–788. doi: [10.3979/j.issn.1673-825X.202212110360](https://doi.org/10.3979/j.issn.1673-825X.202212110360).
- YU Jihong, CAI Yuting, LIU Jiahao, *et al.* Space-air covert communication: A survey[J]. *Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition)*, 2023, 35(5): 775–788. doi: [10.3979/j.issn.1673-825X.202212110360](https://doi.org/10.3979/j.issn.1673-825X.202212110360).
- [7] ALIBERTI G, DI PIETRO R, and GUARINO S. Reliable and perfectly secret communication over the generalized Ozarow-Wyner's wire-tap channel[J]. *Computer Networks*, 2016, 109: 21–30. doi: [10.1016/j.comnet.2016.06.034](https://doi.org/10.1016/j.comnet.2016.06.034).
- [8] DING Haichuan, WANG Wenjing, MA Ying, *et al.* Adaptive covert communications in time-varying environments with multi-slot covertness constraints[J]. *IEEE Transactions on Wireless Communications*, 2025, 24(12): 9978–9988. doi: [10.1109/TWC.2025.3576095](https://doi.org/10.1109/TWC.2025.3576095).
- [9] BASH B A, GOECKEL D, and 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. doi: [10.1109/JSAC.2013.130923](https://doi.org/10.1109/JSAC.2013.130923).
- [10] WANG Zhaoqi, ZHOU Peiyuan, LIU Xiqing, *et al.* Fractional domain waveform design for covert downlink communication with signal overlay in integrated satellite-terrestrial networks[J]. *IEEE Journal on Selected Areas in Communications*, 2026, 44: 1751–1764. doi: [10.1109/JSAC.2025.3639194](https://doi.org/10.1109/JSAC.2025.3639194).
- [11] HE Biao, YAN Shihao, ZHOU Xiangyun, *et al.* On covert communication with noise uncertainty[J]. *IEEE Communications Letters*, 2017, 21(4): 941–944. doi: [10.1109/LCOMM.2016.2647716](https://doi.org/10.1109/LCOMM.2016.2647716).
- [12] WANG Shuai, YE Jia, CHEN Chao, *et al.* Safeguarding inter-satellite transmissions: A viewpoint from covertness[J]. *IEEE Wireless Communications*, 2025, 32(1): 221–228. doi: [10.1109/MWC.002.2400042](https://doi.org/10.1109/MWC.002.2400042).
- [13] HU Jinsong, GUO Mingqian, YAN Shihao, *et al.* Deep reinforcement learning enabled covert transmission with UAV[J]. *IEEE Wireless Communications Letters*, 2023, 12(5): 917–921. doi: [10.1109/LWC.2023.3251357](https://doi.org/10.1109/LWC.2023.3251357).
- [14] ZHOU Xiaobo, YAN Shihao, HU Jinsong, *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. doi: [10.1109/TSP.2019.2928949](https://doi.org/10.1109/TSP.2019.2928949).
- [15] SONG Zhe, ZHANG Xuyang, WANG Shuai, *et al.* Adaptive redundancy CRDSA in UAV-LEO satellite covert communication networks[J]. *IEEE Transactions on Communications*, 2026, 74: 5879–5892. doi: [10.1109/TCOMM.2026.3668167](https://doi.org/10.1109/TCOMM.2026.3668167).
- [16] GUO Zewei, SUN Ranran, SHEN Yulong, *et al.* Covert communication in satellite-terrestrial systems via beamforming and jamming[J]. *IEEE Transactions on Vehicular Technology*, 2026, 75(5): 8030–8047. doi: [10.1109/TVT.2025.3630218](https://doi.org/10.1109/TVT.2025.3630218).
- [17] XU Yang, LIU Jia, SHEN Yulong, *et al.* Incentive jamming-based secure routing in decentralized internet of things[J]. *IEEE Internet of Things Journal*, 2021, 8(4): 3000–3013. doi: [10.1109/JIOT.2020.3025151](https://doi.org/10.1109/JIOT.2020.3025151).
- [18] WANG Shuai, ZHANG Xiaorui, SONG Zhe, *et al.* Generative AI empowered covert communications: Autonomy, efficiency, and suitability[J]. *IEEE Wireless Communications*, 2026, 33(2): 208–216. doi: [10.1109/MWC.2025.3596961](https://doi.org/10.1109/MWC.2025.3596961).
- [19] YU Xinchun, WEI Shuangqing, and LUO Yuan. Finite blocklength analysis of gaussian random coding in AWGN channels under covert constraint[J]. *IEEE Transactions on Information Forensics and Security*, 2021, 16: 1261–1274. doi: [10.1109/TIFS.2020.3032292](https://doi.org/10.1109/TIFS.2020.3032292).
- [20] CHEN Xinying, AN Jianping, XIONG Zehui, *et al.* Covert communications: A comprehensive survey[J]. *IEEE Communications Surveys & Tutorials*, 2023, 25(2): 1173–1198. doi: [10.1109/COMST.2023.3263921](https://doi.org/10.1109/COMST.2023.3263921).
- [21] 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. doi: [10.11959/j.issn.1000-436x.2020137](https://doi.org/10.11959/j.issn.1000-436x.2020137).
- LIN Yuda, JIN Liang, ZHOU You, *et al.* Performance analysis of covert wireless communication based on beam forming with noise uncertainty[J]. *Journal on Communications*, 2020, 41(7): 49–58. doi: [10.11959/j.issn.1000-436x.2020137](https://doi.org/10.11959/j.issn.1000-436x.2020137).
- [22] 安建平, 倪子涵, 王帅, 等. 基于扩维域能量弥散的隐蔽通信[J]. 中国科学: 信息科学, 2024, 54(8): 1940–1969. doi: [10.1360/SSI-2024-0012](https://doi.org/10.1360/SSI-2024-0012).
- AN Jianping, NI Zihan, WANG Shuai, *et al.* Covert

- communications based on energy dispersion in extended dimensions[J]. *Science China Information Sciences*, 2024, 54(8): 1940–1969. doi: [10.1360/SSI-2024-0012](https://doi.org/10.1360/SSI-2024-0012).
- [23] MAO Haobin, PI Xiangyu, ZHU Lipeng, *et al.* Sum rate maximization for movable antenna enhanced multiuser covert communications[J]. *IEEE Wireless Communications Letters*, 2025, 14(3): 611–615. doi: [10.1109/LWC.2024.3514199](https://doi.org/10.1109/LWC.2024.3514199).
- [24] HUA Zizheng, KE Ying, CHEN Su, *et al.* Computer vision target detection-aided high-frequency satellite-ground communications[J]. *IEEE Internet of Things Journal*, 2024, 11(18): 29321–29334. doi: [10.1109/JIOT.2024.3385424](https://doi.org/10.1109/JIOT.2024.3385424).
- [25] LIN Zhi, NIU Hehao, AN Kang, *et al.* Refracting RIS-aided hybrid satellite-terrestrial relay networks: Joint beamforming design and optimization[J]. *IEEE Transactions on Aerospace and Electronic Systems*, 2022, 58(4): 3717–3724. doi: [10.1109/TAES.2022.3155711](https://doi.org/10.1109/TAES.2022.3155711).
- [26] ZHENG Gan, ARAPOGLOU P D, and OTTERSTEN B. Physical layer security in multibeam satellite systems[J]. *IEEE Transactions on Wireless Communications*, 2012, 11(2): 852–863. doi: [10.1109/TWC.2011.120911.111460](https://doi.org/10.1109/TWC.2011.120911.111460).
- [27] MA Yuanyuan, ZHANG Ge, XU Zhan, *et al.* Secrecy capacity of SWIPT-based cognitive satellite-terrestrial network with artificial noise and noncolluding ERs[J]. *IEEE Transactions on Aerospace and Electronic Systems*, 2024, 60(6): 9029–9044. doi: [10.1109/TAES.2024.3440270](https://doi.org/10.1109/TAES.2024.3440270).
- [28] QING Chaojin, SUN Yu, YANG Yuqiao, *et al.* Sensing information-assisted CSI feedback for UAV communication systems[J/OL]. *IEEE Sensors Journal*, <https://ieeexplore.ieee.org/document/11164535>, 2025.
- [29] YU Jihong, CAI Yuting, YAN Shihao, *et al.* Joint 3D beamforming-and-trajectory design for UAV-satellite uplink covert communication[J]. *IEEE Transactions on Communications*, 2025, 73(5): 3469–3481. doi: [10.1109/TCOMM.2024.3480979](https://doi.org/10.1109/TCOMM.2024.3480979).
- [30] FANG Xinran, FENG Wei, WEI Te, *et al.* 5G embraces satellites for 6G ubiquitous IoT: Basic models for integrated satellite terrestrial networks[J]. *IEEE Internet of Things Journal*, 2021, 8(18): 14399–14417. doi: [10.1109/JIOT.2021.3068596](https://doi.org/10.1109/JIOT.2021.3068596).
- [31] LEI Hongjiang, MU Shunkai, ZHENG Shiyu, *et al.* Achieving covertness in cooperative systems with power allocation[J]. *IEEE Internet of Things Journal*, 2025, 12(9): 12527–12537. doi: [10.1109/JIOT.2024.3521051](https://doi.org/10.1109/JIOT.2024.3521051).
- [32] LI Bin, FEI Zesong, ZHOU Caiqiu, *et al.* Physical-layer security in space information networks: A survey[J]. *IEEE Internet of Things Journal*, 2020, 7(1): 33–52. doi: [10.1109/JIOT.2019.2943900](https://doi.org/10.1109/JIOT.2019.2943900).
- [33] QI Bin, YE Neng, LI Jianguo, *et al.* Shrinking the insecure area for satellite downlink using multi-beam intersection[J]. *IEEE Transactions on Communications*, 2025, 73(2): 921–937. doi: [10.1109/TCOMM.2024.3445276](https://doi.org/10.1109/TCOMM.2024.3445276).
- [34] AN Jianping, KANG Bichen, OUYANG Qiaolin, *et al.* Covert communications meet 6G NTN: A comprehensive enabler for safety-critical IoT[J]. *IEEE Network*, 2024, 38(4): 17–24. doi: [10.1109/MNET.2024.3379864](https://doi.org/10.1109/MNET.2024.3379864).
- [35] JEON S, KWAK J, and CHOI J P. An integration of cryptography and physical layer security for multibeam satellite systems[J]. *IEEE Transactions on Communications*, 2025, 73(2): 1087–1099. doi: [10.1109/TCOMM.2024.3440873](https://doi.org/10.1109/TCOMM.2024.3440873).
- [36] ZHANG Yue, HOU Gaopan, LIU Jingmin, *et al.* Energy-efficient resource allocation for satellite-UAV-ground integrated compute first networking[J]. *IEEE Transactions on Consumer Electronics*, 2025, 71(4): 10986–11000. doi: [10.1109/TCE.2025.3610868](https://doi.org/10.1109/TCE.2025.3610868).
- [37] GUO Hongzhi, LI Jingyi, LIU Jiajia, *et al.* A survey on space-air-ground-sea integrated network security in 6G[J]. *IEEE Communications Surveys & Tutorials*, 2022, 24(1): 53–87. doi: [10.1109/COMST.2021.3131332](https://doi.org/10.1109/COMST.2021.3131332).
- [38] XU Yang, LIU Jia, SHEN Yulong, *et al.* QoS-aware secure routing design for wireless networks with selfish jammers[J]. *IEEE Transactions on Wireless Communications*, 2021, 20(8): 4902–4916. doi: [10.1109/TWC.2021.3062885](https://doi.org/10.1109/TWC.2021.3062885).
- [39] LUO Zhangkai, WANG Huali, and ZHOU Kaijie. Polarization filtering based physical-layer secure transmission scheme for dual-polarized satellite communication[J]. *IEEE Access*, 2017, 5: 24706–24715. doi: [10.1109/ACCESS.2017.2762726](https://doi.org/10.1109/ACCESS.2017.2762726).
- [40] ZHAO Bai, LIN Min, LI Fei, *et al.* Robust frame-based beamforming scheme to enhance secure multigroup multicast transmission for multibeam satellite systems[J]. *IEEE Transactions on Vehicular Technology*, 2024, 73(3): 4407–4411. doi: [10.1109/TVT.2023.3324437](https://doi.org/10.1109/TVT.2023.3324437).
- [41] KALANTARI A, ZHENG Gan, GAO Zhen, *et al.* Secrecy analysis on network coding in bidirectional multibeam satellite communications[J]. *IEEE Transactions on Information Forensics and Security*, 2015, 10(9): 1862–1874. doi: [10.1109/TIFS.2015.2432732](https://doi.org/10.1109/TIFS.2015.2432732).
- [42] 李德政. 低轨遥感卫星组网关键技术研究[D]. [博士学位], 中国科学技术大学, 2020. doi: [10.27517/d.cnki.gzkju.2020.002097](https://doi.org/10.27517/d.cnki.gzkju.2020.002097).
- LI Dezheng. Research on key networking technologies for low earth orbit remote sensing satellites[D]. [Ph. D. dissertation], University of Science and Technology of China, 2020. doi: [10.27517/d.cnki.gzkju.2020.002097](https://doi.org/10.27517/d.cnki.gzkju.2020.002097).
- [43] YUAN Shuo, PENG Mugen, and SUN Yaohua. Satellite-terrestrial integrated fog networks: Architecture,

- technologies, and challenges[J]. *IEEE Wireless Communications*, 2025, 32(4): 208–215. doi: [10.1109/MWC.011.2400262](#).
- [44] 胡杨林, 张天魁, 李博, 等. 无人机使能的通信感知一体化组网与技术研究综述[J]. 电子与信息学报, 2025, 47(4): 859–875. doi: [10.11999/JEIT241116](#).
- HU Yanglin, ZHANG Tiankui, LI Bo, *et al.* A survey on UAV-enabled integrated sensing and communication networking and technologies[J]. *Journal of Electronics & Information Technology*, 2025, 47(4): 859–875. doi: [10.11999/JEIT241116](#).
- [45] YANG Ziyi, NI Zihan, YUE Pingyue, *et al.* RIS-aided Space-terrestrial secure communication under multieavesdropper and malignant interference[J]. *IEEE Transactions on Aerospace and Electronic Systems*, 2025, 61(3): 6733–6747. doi: [10.1109/TAES.2025.3528387](#).
- [46] 朱政宇, 欧阳泽彬, 潘高峰, 等. 低轨卫星通感一体化系统中的隐蔽通信传输方案[J]. 电子与信息学报, 2025, 47(10): 3538–3548. doi: [10.11999/JEIT250208](#).
- ZHU Zhengyu, OUYANG Zebin, PAN Gaofeng, *et al.* Covert communication transmission scheme in low earth orbit satellite integrated sensing and communication systems[J]. *Journal of Electronics & Information Technology*, 2025, 47(10): 3538–3548. doi: [10.11999/JEIT250208](#).
- [47] WANG Yutao, YANG Weiwei, NI Xue, *et al.* Covert communication in multi-user ISAC systems: Joint beamforming and jamming optimization[J]. *IEEE Transactions on Vehicular Technology*, 2026, 75(2): 2927–2938. doi: [10.1109/TVT.2025.3607485](#).
- [48] YANG Hanyu, GONG Shiqi, LIU Heng, *et al.* MA-aided integrated sensing and covert communication systems[J]. *IEEE Journal on Selected Areas in Communications*, 2026, 44: 3690–3704. doi: [10.1109/JSAC.2026.3669141](#).
- [49] JORDAN-PARRA J, GARCIA-ROMERO M, GIL-LOPEZ J, *et al.* Satellite quantum key distribution: Analysis, modeling, performance evaluation, and validation[J]. *IEEE Open Journal of the Communications Society*, 2025, 6: 8241–8271. doi: [10.1109/OJCOMS.2025.3614698](#).
- [50] 苏昭阳, 刘留, 艾渤, 等. 面向低轨卫星的星地信道模型综述[J]. 电子与信息学报, 2024, 46(5): 1684–1702. doi: [10.11999/JEIT230941](#).
- SU Zhaoyang, LIU Liu, AI Bo, *et al.* Survey of satellite-ground channel models for low earth orbit satellites[J]. *Journal of Electronics & Information Technology*, 2024, 46(5): 1684–1702. doi: [10.11999/JEIT230941](#).
- 邓 浩: 男, 副教授, 研究方向为5G/B5G信号处理、无线物理层安全传输等.
- 孙维远: 女, 硕士, 研究方向为卫星隐蔽通信技术、语义通信等.
- 朱政宇: 男, 教授, 研究方向为智能超表面、通感一体化、语义通信等.
- 潘高峰: 男, 教授, 研究方向为空天信息网络、无线安全通信等.
- 孙钢灿: 男, 教授, 研究方向为宽带无线通信、智能物联网系统等.

Survey of Satellite Covert Communications: Status, Key Technologies, and Future Challenges

DENG Hao^① SUN Weiyuan^② ZHU Zhengyu^③ PAN Gaofeng^④ SUN Gangcan^③

^①(School of Physics and Electronics, Henan University, Kaifeng 475004, China)

^②(School of Future Technology, Henan University, Zhengzhou 450046, China)

^③(School of Electrical and Information Engineering, Zhengzhou University, Zhengzhou 450001, China)

^④(School of Cyberspace Science and Technology, Beijing Institute of Technology, Beijing 100081, China)

Abstract:

Objective This survey comprehensively integrates the theoretical foundations, key technologies, and future challenges in the field of satellite covert communications. Based on the classic Alice-Bob-Willie model, it analyzes the impact of satellite channel characteristics on covert communication capacity, laying the theoretical groundwork. It summarizes the covert communication network model under the space-based, air-based, and ground-based three-layer architecture (Fig. 1), and systematically reviews core technologies and their optimization methods, including signal camouflage coding, beamforming, spectrum diversity, quantum encryption, and AI-assisted techniques. The main security threats faced by satellite covert communications are outlined, and multi-layered defense strategies, such as physical layer security and intelligent collaborative protection, are summarized. This provides theoretical and technical support for promoting highly secure and intelligent development in this field.

Significance The research significance of this survey lies in its systematic integration of the theoretical framework and technological systems in the field of satellite covert communications. Addressing the threats of detection, interference, and eavesdropping in the vast, open satellite environment, it summarizes representative space-air-ground architectures reported in the literature. These architectures overcome the limitation of traditional encryption technologies that only protect information content, supporting low probability of detection by reducing statistical distinguishability at the physical layer. By elucidating the constraints of satellite channels on covert capacity through the refined square root law, and reviewing enhancement strategies reported in prior work centered on core technologies such as dynamic encoding, beamforming, and spectrum diversity, it provides theoretical and technical foundations for constructing highly survivable space-air-ground integrated secure communication networks. This holds significant strategic value for national defense, emergency communications, and the security assurance of 6G integrated space-terrestrial networks.

Progress Existing studies reveal the dual impact of Doppler spread on satellite covert capacity: while increasing the missed detection probability, it simultaneously causes signal distortion, necessitating reliance on adaptive coding for compensation. The research further quantifies the detection characteristic differences among terrestrial, aerial, and orbital wardens (Willie) (Table 1), providing a theoretical basis for hierarchical defense design. In terms of covertness enhancement techniques, existing schemes propose multi-level strategies. AI-driven dynamic camouflage combined with sparse coding integrates background noise, inter-satellite links, and dynamic beamforming, improving covert throughput. At the network level, cooperative UAV-assisted transmission and dynamic spectrum coordination are summarized as typical network-level enhancement schemes (Fig. 3). Based on representative studies, a hierarchical defense framework for satellite covert communications is summarized. This combines reconfigurable intelligent surface control, Stackelberg game-theoretic incentives for jamming cooperation, and XOR network coding, and utilizes federated learning to achieve cross-domain threat signature sharing. These systematic advances provide innovative solutions for the covertness and security of satellite communications.

Conclusions This paper systematically investigates the foundations and advancements of satellite covert communication, highlighting the integration of multi-layer satellite constellations, dynamic aerial relays, and quantum-encrypted, software-defined networks to establish resilient global covert channels. By adapting the Alice-Bob-Willie model to real-world satellite channel imperfections, it guides covert throughput and security optimization. The infusion of AI into coding and waveform design enables adaptive, environment-aware concealment strategies. Future research should focus on robust covert links in dynamic LEO environments, scalable constellation management, and the deep integration of AI and quantum technologies for 6G NTN systems, as the convergence of programmable satellites, intelligent surfaces, and advanced machine learning is expected to further influence secure space communications.

Prospects Future research challenges and development trajectories focus on four critical domains: robust transmission under non-ideal channels, AI-enabled intelligent decision-making, 6G NTN integrated networking, and quantum-communication integration (Fig. 4). High-precision Doppler compensation models must be developed to mitigate rapid channel variations in LEO satellites. Concurrently, robust transmission mechanisms should be developed under non-ideal CSI conditions, potentially leveraging deep reinforcement learning for real-time resource optimization. Research should prioritize synergistic advancement of AI and quantum technologies. This entails integrating cross-layer Quantum Key Distribution (QKD) designs with covert transmission protocols, while utilizing Software-Defined Satellite (SDS) capabilities for dynamic strategy deployment. Key opportunities include exploiting Reconfigurable Intelligent Surfaces (RIS) for enhanced spatial-domain signal control and implementing blockchain solutions to address trust constraints in multi-node cooperative networks. Essential objectives encompass deploying efficient lightweight onboard algorithms and establishing optimized international coordination frameworks for spectrum and orbital resource allocation.

Key words: Satellite Covert Communications; Covert Encoding; Beamforming; Spectrum Agility