低轨卫星网络安全问题及防御技术综述

杜星葵[①] 束妮娜[①] 刘春生*[①②] 杨 方[①] 马 涛[①] 刘 洋[③]

[①](国防科技大学电子对抗学院 合肥 230037)

[②](合肥综合性国家科学中心人工智能研究院 合肥 230037)

[③](北京市遥感信息研究所 北京 100011)

摘 要：随着低轨卫星网络的快速发展，其应用领域日益广泛，与人工智能等技术融合程度日益趋深，但随之而来的安全问题也更加凸显。该文旨在综述低轨卫星网络面临的主要安全问题，并探讨相应的防御技术。该文首先概述低轨卫星网络的发展情况，不同于现有综述侧重于物理层安全的现状，该文针对低轨卫星网络安全问题，特别是网络层安全进行了系统性研究。该文详细介绍了低轨卫星网络的体系架构、独有的网络特征和脆弱性，并分析了其脆弱性机理，系统地介绍了低轨卫星网络面临的不同威胁手段的安全问题。在此基础上，对基于虚拟仿真、人工智能等先进技术的防御技术进行研究与分析，并对未来低轨卫星网络的安全发展方向提出了建议。

关键词：低轨卫星网络；网络安全；防御策略；人工智能

中图分类号：TN927.23; TP393.081 **文献标识码**：A **文章编号**：1009-5896(2025)06-1609-14

DOI: 10.11999/JEIT240957 **CSTR**: 32379.14.JEIT240957

1 引言

近年来，低轨卫星网络正迎来发展热潮，因其具有低延迟、高带宽、低成本、广覆盖等优势，在移动通信、物联网、海洋作业等方面应用广泛且前景广阔，也将成为未来6G网络架构的关键组成部分[1]。由于地理位置和运营成本的限制，传统的地面网络对于偏远山区或远海大洋等区域难以进行部署和维护，低轨卫星网络可通过卫星接入、多跳路由至地面站进而接入互联网服务，填补了此类区域的服务空缺[2]。可以预见，低轨卫星网络将突破地表地貌限制，在地面基站难以覆盖的沙漠、海洋、森林、山区以及偏远地区快捷、便利、低成本地构建宽带网络，有效弥补信息时代的数字鸿沟。除此之外，在应急救灾任务场景，低轨卫星网络可用于地面网络基础设施被破坏后，为灾区提供快速及时的应急网络接入服务，保障人民群众生命安全。

低轨卫星网络在国外发展非常迅速，SpaceX, OneWeb等商业公司均已建设规模庞大的低轨卫星星座项目，计划发射数万颗低轨卫星进行组网[3]。截止2024年10月，SpaceX已经发射7 010颗“星链”卫星，这些卫星分布在多组轨道上。首先部署的核心星座由1600颗卫星组成，均匀分布在32个轨道平面上，之后部署的卫星同样以类似的方式分布在不同高度的不同轨道平面[4]。与此同时，我国也在此领域制定了宏伟规划并稳步推进，“千帆星座”是我国首个进入正式组网阶段的巨型低轨商业卫星星座，将由超过1.5万颗低轨道卫星组成，旨在为全球提供移动通信和宽带互联网业务，为国家新型基础设施建设提供基础性条件[5]。

随着低轨卫星网络成为全球性的关键信息基础设施，其安全问题自然受到重视与关注。现已有一些综述文献对相关研究进行了总结和归纳，涉及了低轨卫星网络中物理层、网络层和应用层的安全问题。文献[6]从国家安全、网络安全和设备安全的角度，分析了卫星互联网的安全风险，总结出13个安全问题，但是相对而言没有聚焦具体技术。文献[7]聚焦空间信息网络的物理层安全，讨论了新兴的综合网络架构面临的相关研究挑战，对卫星通信系统中的物理层技术进行了详尽的总结，并按不同体系结构进行了分类，但该文献仅针对保密性相关问题关注物理层安全，对网络层安全问题涉及较浅。Wang等人[8]将虚假数据注入和拒绝服务(Denial of Service, DoS)以及分布式拒绝服务(Distributed Denial of Service, DDoS)等威胁分为5类，并聚焦应用层安全提出了利用区块链技术构建可靠可信网络的方法，但是他们没有提供物理层中的安全性解决方案，例如防御欺骗或干扰攻击。Guo等人[9]研究了包括陆地、海洋、海底和太空在内的天空地一体化网络的各个层面安全问题，他们讨论了这些层中的潜在威胁和解决方案，以及在此通信框架内可能发生的自然灾害。Yue等人[10]探讨了低轨卫星系统的整体安全性和可靠性问题，并提供了应对这些

收稿日期：2024-10-28；改回日期：2025-04-17；网络出版：2025-05-21

*通信作者： 刘春生 liuchunsheng17a@nudt.edu.cn

基金项目：高层次人才基金(22-TDRCJH-02-013, 2024-JCJQ-QT-039)

Foundation Items: The High-level Talent Fund (22-TDRCJH-02-013, 2024-JCJQ-QT-039)

挑战的解决方案，还涵盖了以前未得到充分解决的物理威胁，然而研究仅涵盖与低轨卫星网络相关的一般攻击和解决方案，并未根据明确的分类标准进行详细划分。Tedeschi等人[11]探讨了与网络的部署和运营相关的安全威胁、解决方案和挑战，特别是物理层威胁，主要关注物理层安全措施和加密方法。Manulis等人[12]对航天工业在新兴太空时代的背景下面临的网络安全威胁进行了全面分析，评估过去的安全威胁和事件，以了解对卫星的对抗性威胁，但他们没有明确提出针对攻击的应对策略。文献[13]对在网络层安全综述的基础上，还增加了对导弹等物理攻击对卫星网络的影响，并深入介绍了不同国家关于卫星利用及太空安全的政策，突出了卫星通信作为国家资产的战略重要性。

上述综述文献较为全面地概括了低轨卫星网络中物理层、网络层和应用层的安全问题与防御手段。总结而言，物理层是低轨卫星网络的基础，负责传输原始的比特流，因其广播特性容易受到窃听与信号干扰等威胁，物理层安全技术通过利用加密编码、波束成形和物理层秘钥技术等加强安全性和保密性；网络层负责数据包的路由和转发，涉及网络路由协议、拥塞控制和故障控制等，确保数据能够在低轨卫星网络中正确传输，可能面临路由攻击等安全威胁，因而提出了安全路由算法、故障恢复机制等来增强网络层的安全；应用层定义了用户直接使用的服务支持和安全机制，攻击者可能利用卫星系统的软硬件漏洞，通过欺骗等网络攻击手段，使星载工作设备陷入瘫痪，导致用户的重要数据面临泄密、丢失或篡改的风险。

但上述综述性文献仍存在值得关注与补充的地方：一是因侧重领域等原因，不够聚焦网络安全领域问题，如文献[6]视野较为宏观，对安全问题给出分类但没有聚焦到技术细节；二是综述主体关注天地一体化网络，并未凸显出低轨卫星网络独有特征，如文献[8,9]中对天空地一体化网络的安全问题探讨的技术细节非常丰富，虽然包含空间信息网络，但很大部分集中在无人机网络、传感器网络等方面；三是侧重物理层与链路层，对于网络层安全问题特点不够突出，低轨卫星网络与普通卫星通信最大的区别就在于其组网规模带来的网络层特性，文献[7,10–12]均主要聚焦物理层安全，分析总结了大量通信信道、频率等相关安全问题，对网络安全问题论述仍有完善空间。

在众多研究者的基础上，该文聚焦对低轨卫星网络安全问题及防御技术相关工作的系统全面综述。通过对低轨卫星网络的潜在脆弱性进行讨论，更深入地分析低轨卫星网络面临的安全问题特别是网络安全威胁。针对多类现实威胁，进一步剖析了为应对安全问题而发展的前沿防御技术。

2 低轨卫星网络概述

2.1 体系架构

如图1所示，低轨卫星网络一般由空间段、地面段和用户段3部分组成。空间段是指提供信息中继服务的卫星星座，由多颗低轨卫星组成，配备激光链路的卫星之间可以通过星间链路进行连接。地面段一般指地面站，包括卫星测控中心及其卫星测控网络、系统控制中心及各类信关站等，其中卫星测控中心及测控网络负责监控和管理卫星的轨道位置和姿态等；系统控制中心负责处理用户登记、身份确认、计费和其他的网络管理功能等；信关站负责呼叫处理、交换及与地面通信网的接口等。用户段指提供服务的移动设备、固定站点或车(舰、机)载终端等各种通信设备。

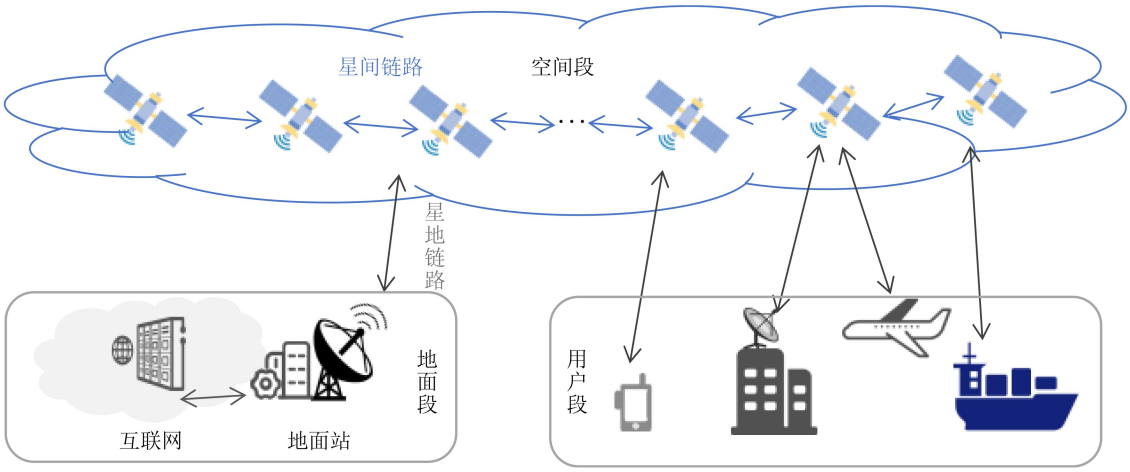


图 1 低轨卫星网络体系架构

当用户通过低轨卫星网络访问互联网服务时，来自用户段的设备通过一个或多个卫星的中继发送到地面站。如果用户与地面站同属一个卫星覆盖下，则通过“弯管”结构进行透明转发；对于远程用户，通过多跳卫星路由到达地面站。地面站接收到后，通过地面传统的光纤网络与互联网相连，用户得以访问网页内容、电子邮件等互联网服务。

2.2 低轨卫星网络特征

2.2.1 拓扑结构多层动态

与具有平面与固定结构的传统地面网络不同，低轨卫星网络的拓扑结构具有高动态性和立体多层等特点。低轨卫星轨道高度通常在500～2000 km，可分为不同的壳层，形成多层网络的结构，轨道周期相对较短，具有高动态性。这种立体多层高动态性的结构导致其网络拓扑在不断地改变，带来了网络管理和路由设计的挑战，要求网络能够适应频繁的拓扑变化[14]。

2.2.2 服务范围全球覆盖

传统地面网络如5G和光纤网络，可以提供非常高的带宽，适合高密度用户区域，但在偏远地区，地面网络的覆盖和容量受限于基础设施的建设和维护。低轨卫星网络能够提供全球范围内的覆盖，这对于海洋和山区等传统地面网络难以覆盖的区域尤为重要。根据文献[15]仿真分析，1.0版“星链”卫星全部部署后，在北纬53°至南纬53°之间已达到100%的覆盖效果，1.5版“星链”卫星也正在部署中，包括两极在内的全球覆盖率逐步提升。通过部署足够数量的卫星，可以实现对地球表面的连续覆盖，如图2所示的仿真验证表示，“星链”网络倾角为53°的单个壳层即可完成对中低纬度地区的多重覆盖。

2.2.3 数据传输低延迟

低轨卫星通信链路均为视距通信，传输时延和路径损耗相对较小且稳定，相比传统的地球同步轨道卫星，低轨卫星网络可以提供更高速的宽带连接，在轨道高度上，低轨卫星远低于同步卫星，信号不需要经过长距离传输，减少了延迟和信号丢失的问题[16]。低轨卫星网络能够提供低延迟与高带宽的连接，支持在线游戏、视频会议等众多实时应用服务。

2.2.4 资源分配弹性灵活

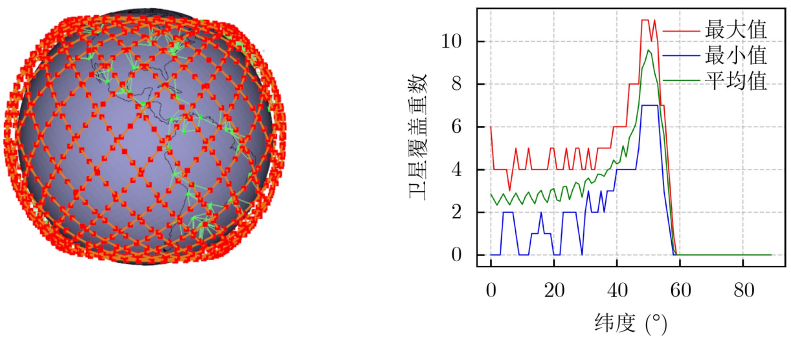
低轨卫星网络可以利用跳波束技术灵活分配系统资源，适用于业务分布不均匀的场景。这种技术可以根据业务需求动态调整波束，与传统地面网络的资源分配方式相比，更加灵活和高效。同时，其分布式特性和冗余设计使其具有较高的网络弹性，即使部分卫星或链路发生故障，网络仍能通过其他路径维持通信服务[17]。这种弹性对于确保关键通信服务的连续性至关重要，尤其是在自然灾害或其他紧急情况。

2.3 低轨卫星网络潜在脆弱性

2.3.1 节点脆弱性

低轨卫星网络中的卫星节点在复杂且开放的外层空间环境中运行，因此它们容易因自然原因而损坏或受到人为恶意攻击。首先，在外层空间中存在大量碎片可能导致碰撞事故，根据欧洲空间局数据，截至2024年9月，有大约40500个尺寸大于10 cm的空间碎片[18]，每颗卫星都面临着发生物理碰撞的风险，且一旦相撞，卫星可能会分裂更多碎片，从而加剧轨道拥堵并产生更高的风险。其次，宇宙环境中的磁暴等现象也会使卫星载荷失效。而且，人为恶意攻击也会造成低轨卫星网络节点失效，例如导弹或激光武器等能够破坏卫星设备，电子干扰和网络入侵能够致使其无法正常服务[13]。

在卫星自主控制过程中，卫星受到燃料变化和执行器故障的影响，导致执行效率下降。为了在执行器故障的情况下实现卫星姿态和轨道控制，学者们开发了各种控制方法，如滑模控制、自适应控制等。这些方法可以对故障进行鲁棒性修补，但它们只能处理预先考虑的故障，并且可能牺牲控制精



(a) “星链”网络仿真　　(b) “星链”卫星对北半球覆盖重数

图 2 “星链”网络单个壳层对地面的覆盖情况

度。运营商必须感知太空情况，校准卫星轨道，并在必要时通过轨道机动避免碰撞，现有研究低轨卫星星座的自动驾驶技术，提高了卫星节点的生存能力。

2.3.2 链路脆弱性

低轨卫星网络通过激光通信系统来建立星间链路，以无线电通信建立星地链路，均存在面对各种潜在威胁和干扰时可能导致通信链路中断或严重质量下降的链路脆弱性，这种脆弱性的来源之一是高动态性带来的链路切换。由于卫星的高速移动，某一颗卫星对于地面用户可见的时间非常短，用户终端可能需要在不同的卫星之间频繁切换，以保持连续的通信连接；同时，卫星间的相对速度很高，这要求星间链路能够快速建立和维护，以保持稳定的数据传输。卫星正常的轨道移动带来的链路切换是可以预先计算得到的，但还有一类预料之外的应急机动，如要避开提前观测到的空间碎片或陨石，则会放大链路的脆弱性。卫星在应急机动期间无法提供网络服务，机动中卫星的方向变化导致其天线暂时失去与地面站或终端的对准[19]；同样，机动也可能通过错位破坏光学卫星间链路，因此在实际情况中，每次机动引起的卫星连通性中断都可能持续数小时[20]。

2.3.3 协议脆弱性

协议脆弱性主要来源于两方面。首先，由于新兴的低轨卫星网络从本质上是建立在互联网协议栈上的，攻击者可以利用网络协议中的这些漏洞来发起攻击。联合利用空间路由信息、开放网络拓扑和地理分布式僵尸网络，通过在低轨卫星网络中的某些重要链路来注入恶意流量。

同时，低轨卫星网络的商业属性要求其追求时间延迟最低等特性，使其路由协议容易被推断出来，对合法协议的恶意利用也能起到破坏效果。当前学术界提出了多种适用于低轨卫星网络的路由协议，力求在有限的卫星计算/存储资源、星间链路带宽资源的限制下，实现全网路由收敛，但仍存在脆弱性威胁。基于卫星位置推算的路由协议和星座快照路由协议等，能够利用优化方法计算出转发路径，但均不能根据链路状态突发变化来过更新路由，网络抗毁性有待提高。

加密协议作为保证数据完整性和机密性的重要手段，也已有大量研究，如基于公钥签名的认证方案，实现了用户安全地接入卫星网络，但计算开销过大；基于对称密钥的认证方案，降低了计算开销，但不具有前向安全性，且需要保存海量的用户验证表等信息；基于哈希和异或运算的认证协议，能提供更高效的认证，但不足以抵抗欺骗攻击等安全威胁。

2.3.4 基础设施脆弱性

新兴的低轨卫星网络部署在很大程度上依赖于现有的网络基础设施和服务，文献[9]首次讨论了自然灾害对服务可靠性造成的威胁。即使不考虑小概率发生的天灾，恶劣的自然条件也会限制低轨卫星网络的服务能力，关注“星链”在野外服务效果的Ma等人[21]通过实际运营处于高纬度地区的用户终端，从而评估低轨卫星网络在恶劣自然条件以及不发达国家的服务质量，根据其统计数据，在高纬度地区的恶劣地形条件下，服务延迟高于正常水平的3～10倍，且在时间分布上有2%的完全阻塞率，验证了基础设施缺乏的恶劣自然环境对网络性能的重大影响。

其次，低轨卫星可以配备先进和智能的软硬件功能载荷，以便在轨道上执行多样任务，然而这些载荷也会带来新的脆弱性，比如运行在卫星系统上的软件的漏洞，攻击者可以利用这些漏洞来获得未经授权的访问或控制卫星。因此其可能会遭受诸如供应链威胁和基础设施DDoS攻击等风险。在低轨卫星网络服务的制造或部署过程中引入的任何恶意的软硬件都可能构成重大的安全风险，如恶意错误配置或数据泄露，应制定严格的控制和验证程序，以减轻这些风险。此外，卫星网络的空间网络段通过地面站连接到地面互联网，地面站在低轨卫星网络基础设施中的核心作用，导致其可能成为攻击的主要目标，地面站的失效会导致大量卫星服务中断。

3 低轨卫星网络安全问题

低轨卫星网络因其独特的优势带来广泛的应用前景，但其潜在脆弱性同样不容忽视，随着技术的发展，低轨卫星网络也面临着多种安全问题的威胁。这些安全威胁源自传统地面网络安全问题，同时利用低轨卫星网络的独有特点放大了脆弱性。如表1所示，本章按照安全威胁的行为手段，将低轨卫星网络面临的安全问题分为窃听攻击安全威胁、拒绝服务攻击安全威胁、路由攻击安全威胁和电子对抗干扰威胁等4类，并进行详细的分析梳理。

3.1 窃听攻击安全威胁

数据窃听是指非法组织使用复杂的设备或技术，通过无线链路非法接收和分析传输的流量数据或信令数据，从而破坏了通信的机密性。因为数据加密将增加卫星终端设备的成本，降低卫星链路资源的利用率，许多卫星通信网络不对传输的数据进行加密，因此很容易造成数据泄露。虽然窃听不会

表 1　低轨卫星网络安全问题总结

安全问题	具体手段	威胁描述	威胁影响
窃听攻击	窃听链路	窃听并破解传输的信息	数据泄露
拒绝服务攻击	链路阻塞	分布式恶意流量作用于目标链路	阻塞链路，增大时延
	节点失效	恶意流量占据节点服务	增大时延
	能量消耗	恶意流量消耗节点资源	降低可用性
路由攻击	伪造更新	引导进入攻击者控制的节点或网络路径	信息准确性
	篡改协议	篡改路由协议的控制消息或者数据包	改变路径，增大时延
	路由劫持	在控制的路径窃取或丢弃数据	数据泄露、降低可用性
电子对抗干扰	对卫星干扰	地面或空间设备对卫星进行干扰	降低可用性
	对终端干扰	地面或空间设备对用户终端进行干扰	降低可用性

影响数据的传输交互，但是窃听者不仅能分析和提取有用的信息，还能够分析指令构造以创建未来的攻击。

由于低轨卫星网络星地链路、星间链路均具有无线通信的开放性，通过其传输的数据容易被窃听，其窃听信道模型如图3所示，低轨卫星的全域覆盖也为窃听者提供了地理位置便利。潜在的攻击者可从公开渠道收集目标卫星网络的相关信息，包括卫星的轨道参数、通信频率、可能的通信协议等，由于其动态性可预测，可选择合适的地理位置进行提前部署，使用接收设备监听目标卫星的通信信号，并从解调的信号中提取有用信息。

文献[7]将通信安全作为关键目标，对涉及的安全指标进行详细归纳，工作聚焦窃听安全攻击，充分考虑卫星波束方向图和路径损耗，对卫星信道进行了详细的建模，并从物理层安全的角度提出了卫星通信网络的安全设计。文献[22]考虑了一种认知卫星-地面网络，其中窃听者非法地想要在卫星和基站发送针对主用户和次用户的信号的过程中窃听所发送的信号。文献[23]研究了如图4所示的存在多个窃听者的多用户多中继混合星地中继网络的物理层安全，位于卫星覆盖范围内的窃听者意图窃听卫星下行链路通过中继基站传输到地面终端的信息。

基于低轨卫星网络的数据传输过程中，用户设备的大量数据必须依赖网关或多个卫星进行交换转发，其中包含一些敏感信息，例如为了减少低轨卫星之间的切换的延迟以实现高精度连续用户跟踪，必须在网关或卫星之间共享的位置。一旦攻击者获得对用户位置信息的访问，这可能会触发随后不可逆转的攻击，甚至潜在的物理破坏。数据窃听通常与其他攻击相结合来破坏数据的完整性。攻击者通常会进行数据窃听，然后插入、修改、伪造被盗数据，最后将其发送给数据接收器，以达到破坏数据完整性的目的。

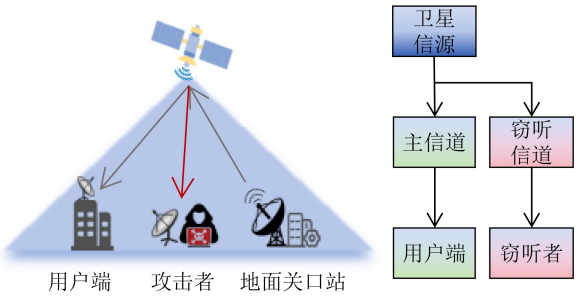


图 3 低轨卫星网络窃听场景

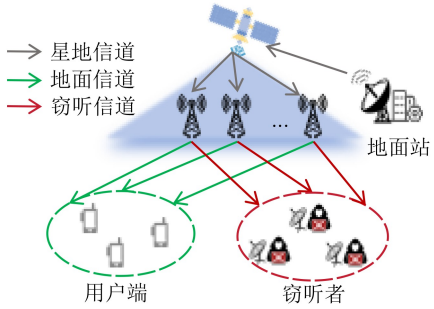


图 4 卫星网络多用户多窃听者场景

3.2　拒绝服务攻击安全威胁

在低轨卫星互联网中，拒绝服务攻击是一种常见的安全威胁，其原理与传统网络中的攻击类似，但其特定的技术和挑战性存在差异。在低轨卫星网络中，这可能涉及卫星或地面控制站遭受大量无效或恶意请求，导致服务性能下降或完全中断。低轨卫星网络的特点决定了其遭受DoS攻击的发生机制存在独特的原理和挑战，卫星网络中的用户设备由于卫星轨道的变动，需要频繁切换连接到不同的卫星，攻击者可以利用动态特性，通过频繁的请求或者制造大量的虚假连接请求，使得卫星或地面控制站无法正常处理合法用户的连接请求。卫星节点受有限内存资源的限制，不断涌入缓冲区的数据包可能会耗尽可用的内存资源。节点具有有限的缓冲区容量阈值，当未处理的负载变得太高时，可能会超

出该容量阈值。最终，缓冲区溢出导致系统崩溃，节点无法承载任何数据转发任务[24]。

目前，已经有较多针对低轨卫星网络进行DoS攻击的研究。文献[25]假设卫星网络中部分地面站已被攻击者控制，通过已控地面站对其它地面站进行DoS和DDoS攻击，模拟了DDoS攻击在卫星网络中使用互联网控制消息协议的回声请求洪泛攻击。卫星和地面设备的处理能力和带宽有限，具有资源有限性的特点，这使得其更容易受到拒绝服务攻击的影响。攻击者可以发送大量请求，消耗网络资源，导致服务质量急剧下降甚至服务中断。

地面传统网络拒绝服务攻击的一些方法也可应用到低轨卫星网络中，相应的研究中[26]，假设DDoS攻击者进行反射放大攻击，与接入空间骨干网的终端设备串通，耗尽带宽资源，导致数据传输和业务交付质量下降的攻击场景。文献[27]通过识别低轨卫星网络中的关键节点并进行拒绝服务攻击，通过对不同数量关键节点的攻击，分析网络在面对DDoS攻击下的安全性能，该工作验证了网络延迟和丢包率随被攻击的关键节点的数量成正比增加，对网络中关键节点的选择与防护有初步指导意义。

更进一步，通过两个特定的仿真场景展现拒绝服务攻击的影响。Giuliari等人[28]提出利用分布式的受控设备，针对链路容量的DDoS攻击——ICARUS，该工作对低轨卫星星座进行仿真，研究了分布式终端被控制后，通过规划多设备间合法流量路径，对卫星互联网中的链路进行拒绝服务攻击，攻击的目标包括星间链路和星地间上下行链路，具体研究了针对单条链路和面向区域间多条链路的DDoS攻击，简化场景如图5所示。通过对两个区域之间卫星互联网的所有链路进行计算分析，对连接两个区域的瓶颈链路进行攻击，从而达到区域通信阻断的目的。该方法同时启发进一步利用低轨卫星网络追求时间延迟小的特点，低轨卫星网络由于信号传播的时延，可能导致请求和响应之间的延迟增加，攻击者可以利用这种延迟，通过连续不断的请求或者利用时序的不稳定性，进一步加剧网络服务的不稳定性。

除了针对链路容量的泛洪攻击，还有研究者受到启发，设计了针对低轨卫星的能量消耗攻击机制[29]，通过来自不同的地理分布位置的受控主机，持续不断地向网络注入恶意流量，通过目标受害者卫星，阻止受害者卫星进入休眠状态，用这样的手段使卫星电池过度放电来缩短其寿命，实现对低轨卫星网络隐蔽的破坏与影响。

3.3 路由攻击安全威胁

路由攻击是地面互联网上最常见的网络攻击之一，攻击者利用协议漏洞修改数据包的原始转发路径，使其落入路由黑洞或通过窃听节点等高危区域[30]。随着星间链路的部署，低轨卫星网络真正具备了组网特性，同时也使其面临路由攻击的威胁。路由攻击将影响网络中数据包的传输路径，甚至导致敏感信息被攻击者获取或篡改。由于卫星节点的全球开放性和缺乏范围外的控制，低轨卫星网络比传统网络面临更多的潜在威胁。

由于低轨卫星高速移动，地面站和卫星之间的连接关系几分钟内就会发生改变，拓扑改变导致路由需要重新收敛，数据包报头中路由路径的节点序

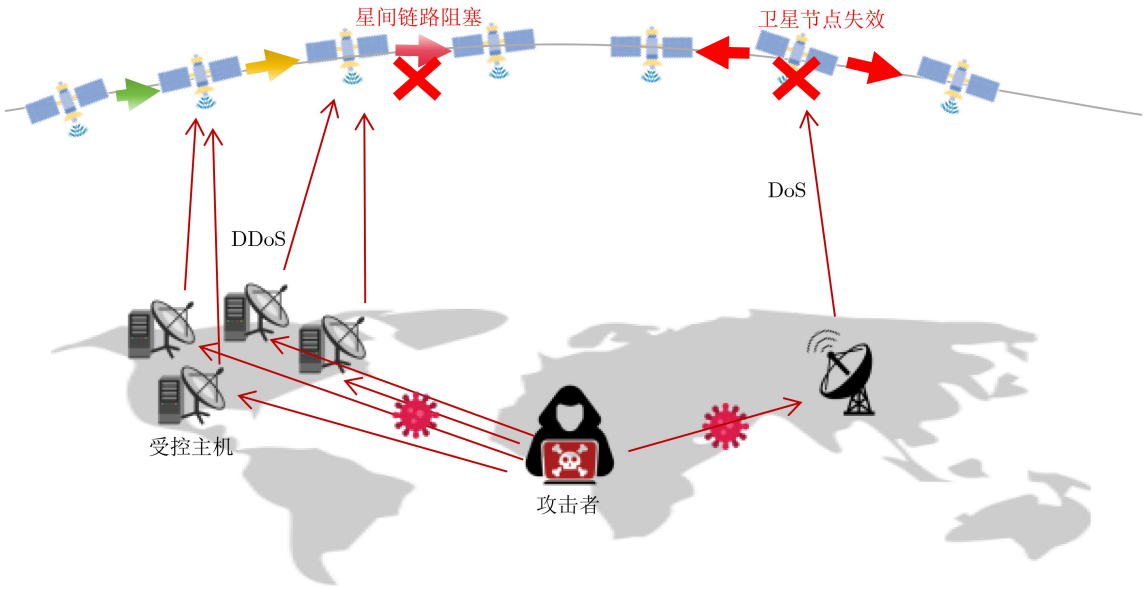


图 5 低轨卫星网络DDoS攻击场景

列将不再符合新收敛的路径，因此信息传递的路径需要重新计算，然后重新协商或导出节点之间的密钥，会给攻击者带来可乘之机。路由劫持后，利用黑洞攻击、虫洞攻击等方式，大量数据包将被丢弃，破坏低轨卫星网络的正常服务。

根据文献[31]，低轨卫星网络中的路由劫持攻击通常基于几种原理进行。伪造路由更新，攻击者可能发送虚假的路由更新消息，欺骗卫星或地面控制站，使其相信某个攻击者控制的路由路径是最佳路径，一旦攻击者的路由信息被接受并生效，合法数据包可能会被引导进入攻击者控制的节点或网络路径。篡改路由协议，攻击者可能通过直接篡改路由协议的控制消息或者数据包，来改变卫星网络中路由表的信息，使攻击者能够更为高效地控制或者影响卫星网络中数据包的传输路径。中间人攻击，攻击者可能伪装成合法的卫星节点或者地面控制站，从而使其能够截取和篡改通过它们的所有数据流量，这种方式使得攻击者能够实施更为隐蔽的攻击，避免被检测到。

3.4 电子对抗干扰安全威胁

电子对抗干扰是指通过发射大功率的噪声信号占用网络中节点的通信信道，掩盖或阻止接收所需信号，导致信噪比降低，无法与其他节点进行正常的通信从而失去可用性[32]。因为大多数低轨卫星采用的是没有经过数字信号处理的“弯管”结构进行透明转发，所以很容易遭遇基于信号功率的压制干扰，攻击者可以很容易地通过发射高功率干扰信号来干扰卫星的运行[6]。

根据干扰的对象可以分为针对卫星的上行干扰和针对地面用户端的下行干扰。上行干扰主要是从地面向卫星发射较强的信号，可能会对卫星转发器的某些信道产生干扰，使信道信号中断。干扰不仅仅能破坏通信的可用性，由于卫星依赖于来自地面的上行命令和控制信息来进行位置保持、有效载荷管理以及卫星健康和状态，因此在关键命令期间攻击卫星的上行链路可能会严重损害卫星的安全和降低使命性能。上行干扰可以在很大的区域内干扰卫星的传输，但其实施的难度和成本较大。特别是对于低轨卫星星座而言，针对卫星的干扰困难主要有以下原因：一是低轨卫星相对地面运动速度高达约 7 km/s，因此来自地面的干扰攻击面短暂；二是低轨卫星网络弹性高，星座中有多颗卫星同时覆盖同一地区，而干扰某颗卫星后，其业务可以切换至其他卫星承担。上行干扰实现后，卫星运营方也可以通过检测和修复，非常典型的案例是俄乌冲突期间，“星链”在受到电子干扰后快速应对恢复了服务[33]。下行干扰主要是从卫星到地面或移动站的信息流，各种不同平台的干扰机可用于干扰下行链路通信，但其影响仅限于特定的地面或移动的用户设备。下行干扰作用有限，只能干扰到干扰机作用范围内的用户。

文献[34]展现了一种特殊的天基干扰场景，通过低轨卫星星座对另一个低轨卫星星座进行干扰，着重针对星间链路干扰对单个星间链路性能和网络整体性能的影响进行研究，提出卫星干扰中主干扰区域的概念，设计了新的卫星网络容量计算方法来评估传输速率动态变化时巨型星座的网络容量。该工作实验结果表明，非合作干扰的干扰功率、星座尺度和倾角对巨型星座的网络容量具有显著影响，当干扰卫星星座和被干扰卫星倾角接近时，将发生最优干扰效果。

4 低轨卫星网络安全防御技术

4.1 基于加密手段的安全防护

与传统互联网安全体系相比较，低轨卫星网络更突出规模体系和太空环境的特殊性，现有工作通过提供与之相适应的安全策略和密码技术，进而设计基于密码的安全防护体系。文献[35]从物理设施、通信链路、计算机系统、数据业务和安全运营等方面，设计了全方位安全防护体系。

随着量子技术的快速发展，量子密码学利用量子力学的原理来实现安全通信，其难以通过数学方法解密，具有抗窃听的特性，窃听者在测量信号时任何微小的错误都会使其失真，导致接收器检测到信号已被拦截。基于这些特性，量子密码加密技术被认为是抗窃听的最佳解决方案。量子密钥分发是一种利用量子纠缠特性来安全分发密钥的技术，即使对于拥有无限计算能力的攻击者，也无法通过传统方法计算窃取密钥。早期的研究[36]已经发现了在近地轨道上产生量子纠缠现象，证明卫星能够具备量子通信的可能。国内潘建伟团队[37]设计了一种无需可信任中继节点，完全通过量子纠缠进行安全加密的方法，并计划在未来几年内发射低轨卫星并建立量子星座，这将极大地推动量子通信领域的发展。量子加密具有以下特点：一是对数学解密具有免疫性，基于不可逆的物理自然现象，其不受数学方法解密的影响；二是不可克隆性，由于量子不能被完美地复制，没有对原始信号的完美测量，就会失真从而无法获得信息；三是可检测是否被窃取，其能够抵抗欺骗攻击。

同时，区块链技术正成为低轨卫星网络安全分散管理的新兴解决方案，区块链是一种分布式账本

技术，它通过去中心化的方式集体维护一个连续增长的数据记录列表，这些数据记录被称为区块，每个区块通过密码学方法相互链接，确保数据的不可篡改性和透明性。在低轨卫星网络安全领域，能够确保卫星传输的数据不被非法修改，任何试图篡改数据的行为都会被网络中的其他节点检测到，从而保证数据的完整性。区块链技术可以为卫星网络中的每个设备创建独特的身份标识，并通过智能合约自动执行授权验证，增强系统的安全性，由于其分布式账本和共识操作，区块链可以追踪和验证每个请求的来源，有效对DoS和DDoS攻击进行识别。

低轨卫星受限于载荷能力、所处环境等相关因素，其运算处理能力弱，星上加密处理会耗费宝贵的资源。目前相关研究[38]已经聚焦于如何同时兼顾数据加密安全和低时延服务保障，对低轨卫星网络在内的多层卫星网络边缘模型进行构建，设计了一种基于强化学习的低轨卫星数据加密回传的决策方法。

4.2 基于弹性路由的安全防护

路由是无线通信的基础，因此制定有效且安全的路由策略在低轨卫星网络中至关重要。低轨卫星网络受到频繁的拓扑变化的影响，其路由比光纤网络路由更为复杂，弹性路由技术通过低轨卫星网络路由的建立、使用和维护来降低不利因素对于数据传输的影响，主要路由解决方法有以下几种。具体来说，在卫星网络中，卫星有限的计算资源和能源效率对路由产生了显著影响，从而促进增强路由安全方法的发展。

常用方法将软件定义网络(Software Defined Network, SDN)的思想引入低轨卫星网络中，从而分离网络的数据平面和控制平面，由控制平面来进行复杂的路由计算、资源管理等操作，剩余卫星节点只需要进行简单的硬件配置和数据报的转发，降低了对星上计算和处理能力的要求。在刘之莹等人[39]的工作中，地面和高轨卫星共同组成控制平面，地面和天基控制器的互补不仅缓解了星上计算压力，并且弥补了地面站无法实时监控的缺陷，地面控制中心基于地面用户数量与主机分布，构建地面流量请求模型来预测星上流量需求，基于预测结果设计预计算节能路由算法，在降低网络能耗的同时优化了路径决策。

基于弹性路由的路由策略，一方面能够应对网络中部分节点失效带来的影响，增强网络弹性；另一方面能够提高低轨卫星网络的服务质量，具体表现为更进一步降低时间延迟。为了应对DDoS针对链路的阻塞，文献[40]提出一种随机路由算法作为防御措施，该算法在最短路径等经典算法的基础上，引入随机性与加权概率分布算法来增加数据传输路径的不确定性，可有效且稳健地增大攻击者的攻击难度。文献[41]针对星间链路故障后存在的传输中断和数据安全问题，设计了一种快速响应链路损毁的路由算法，其引入了多优先级动态队列，在节点链路发生损毁后调整星间链路数据传输的优先级，通过动态优化进而重新计算路由，该方法克服了传统算法对故障情形适应性较差的问题。该方法经过利用OMNeT++进行建模仿真验证，相较于基于最短路径的随机选择路径路由算法，在网络中部分链路故障后该路由方法使网络的最大端到端时延降低了58%。

尽管基于SDN的低轨卫星网络路由方法研究已经有显著的进展，但是由于低轨卫星网络规模趋于巨型化发展，也给相关技术带来挑战，需要高效的网络监测与管理工具，对网络故障做出敏捷反应。Xie等人[42]在SDN 的框架上设计应对DoS攻击的检测方法，通过模拟网络中遭遇的各类DoS攻击场景构建攻击数据集，并对所提出的基于堆叠框架的集成学习检测方法进行验证，检出率达到99.7%，验证了其检测过程的有效性和可行性。Li等人[43]专注于基于安全信任的算法，该算法旨在保护低轨卫星网络中的路由免受内部恶意攻击。他们利用基于Dempster-Shafer理论的分布式信任评估模型，消除了对集中式基础设施的需求。该模型计算卫星之间的直接、间接和聚合信任值，以评估其可信度。

以上文献设计新的路由协议或算法不便于集成到已有的网络系统或协议中，同时也有工作设计适用性更广的机制来实现弹性安全路由。文献[44]设计的SLT算法可以与轨道预测最短路径优先路由协议集成，通过检测和隔离恶意节点来增强网络安全性，从而提高数据包传递率、减少数据包丢失，该算法在恶意节点数量较多的网络中显示出更高的效率，表明其在具有挑战性的环境中的鲁棒性和适应性。Jiang等人[45]设计了网络流过滤机制，该机制包括两个主要组件，流检测器和流调度器，流检测器能够过滤出网络中可疑的攻击流量，流调度器则根据恶意性来对队列中的流进行优先级排序，利用可编程的数据包调度来减轻攻击流量对良性业务流量的影响。

4.3 基于虚拟化技术的低轨卫星网络仿真平台

虚拟化技术是指通过软件将物理资源(如服务器、存储设备、网络资源等)抽象化，从而创建多个可以独立操作的虚拟资源。在低轨卫星网络仿真中，虚拟化技术可以用来模拟卫星网络的硬件和软

件环境，实现对网络的流量、路由、协议、传输策略等进行控制、配置、更新及优化。虚拟化技术在低轨卫星网络中的应用可以提高网络的灵活性和可扩展性，同时也能够降低成本和提高资源利用率。

Wang等人[46]设计了用于空间网络性能分析的仿真平台SNK (Space Networking Kit)，该分析架构能够对高速网络流量进行捕获和牵引，通过层次分析法和其他分析方法对网络性能进行综合评估，应用配置优化和并行处理来处理大量的高速网络流量。最后，通过分析系统的实验结果验证了所提架构的有效性，但在此工作存在较大的提升空间：一是工作中未验证大规模星座的仿真能力，实验所用卫星数量较少；而是其仿真效果实时性不足，下一步仿真系统工作的发展趋势，更倾向于支持不同规模和复杂性的真实网络条件下的测试，支持将真实世界的设备与虚拟仿真相结合。

面对低轨卫星网络中许多已知与未知的安全风险，数字孪生系统对网络优化领域极具价值性，能够帮助运营人员和研究人员进行安全评估、识别漏洞并设计有效的对策以提前迁移风险。Lai等人[47]为促进天地一体化网络的安全可靠，设计了空间数字孪生系统，将真实的网络中的实体进行数字化映射，对其特征、协议、行为、交互和潜在漏洞进行表示，能更好地识别、理解和监控各种空间网络的漏洞或威胁。该系统由物理空间到网络空间映射、虚拟网络生成、安全事件模拟、威胁和脆弱性评估4部分组成，进而能够实现模拟真实的卫星行为和卫星网络的操作系统和网络堆栈，从而便捷灵活地进行安全实验。该数字孪生系统进行了卫星链路泛洪攻击的案例测试，验证了系统对分析安全事件、提高防御效能的价值。

仿真平台的模块化也是重要的发展趋势，Gao等人[48]设计了命名为Plotinus的卫星互联网仿真数字孪生平台，并进行了验证实验。该系统采用模块化设计，可以轻松更换物理层，以模拟不同的飞行器并分析信道干扰。它还支持替换路径计算方法，以简化测试和部署算法，该平台允许对实时网络流量进行实时仿真，从而增强了实际的网络模型。评估结果表明，其能够有效地利用真实世界的设备仿真动态卫星网络，对各种通信模型和算法测试的适应性凸显了作为开发和分析低轨卫星网络的重要工具的作用，提供了一个跨层、实时和可扩展的数字孪生系统。该系统还具备可视化界面，将复杂的网络动力学和路由路径转换为3D视觉模型，将仿真结果更加直观展现。但在路径计算等仿真场景中，Plotinus需要处理更多的动态变化和失效的节点或链路，不如一些专业的仿真平台表现出色。在未来的工作中，对低轨卫星网络的虚拟仿真应当更加注重对故障场景的仿真，服务于优化故障恢复策略、提升网络规划的安全性。

4.4 AI赋能的卫星网络安全技术

对低轨卫星网络的攻击手段多种多样，且将随着网络的发展出现更多未知的安全威胁，传统的基于规则或行为的安全方法，可能难以应对更复杂隐蔽的攻击模式识别和入侵检测等挑战。但随着人工智能的发展，很多AI赋能的卫星网络安全技术已投入应用，并将在未来的安全检测中发挥更重要的作用。

文献[49]提出了一种基于深度学习的干扰管理系统，相较于传统的信号处理技术，文中设计的深度学习技术提高了在高信干比下检测干扰载波信号的准确性，这对于保护通信信道免受未经授权的访问和干扰至关重要。文献[50]利用机器学习方法来进行频谱占用检测和自动调制分类，能够检测出非法的干扰，利用卷积神经网络等技术，较少依赖专家特征选择等先验知识。使用深度强化学习方法优化星间与星地通信的业务调度和资源分配，低轨卫星网络复杂的网络拓扑结构增加了可用卫星和地面站的连续变化，资源分配决策非常重要。传统的方法如凸优化和进化算法等需要详细的模型，依赖大量的人工处理工作。然而，面向数据的人工智能方法可以提供急需的灵活性和自动化，以解决低轨卫星通信网络中的资源分配问题，文献[51]利用深度神经网络来学习网络参数与服务质量和效率水平间的复杂和动态关系，实现了相较传统方法约2.4倍的推理速度。此外，神经网络和其他人工智能模型有助于主动安全管理、动态适应新威胁，从而识别潜在的网络攻击、确保数据传输的完整性。例如，利用已经成熟应用在陆地网络中的网络入侵检测技术[52]，将现有的模型进行调整，可以用来预测和管理卫星网络中的流量数据。

近来，联邦学习已经成为网络安全技术的前沿方向，联邦学习作为一种保护用户隐私和数据隐私的新方法，有可能取代传统的机器学习和深度学习方法。文献[53]首先探索在低轨卫星网络中部署联邦学习，以实现星座内卫星之间关于规范的信息共享，例如在某些地理位置检测某些入侵威胁。文献[54]提出的FedSN框架通过一个新颖的子结构方案来处理异构的本地模型训练，同时提出了一种伪同步模型聚合策略来动态调度模型聚合，以补偿模型的陈旧性，解决了由于有限的稳定链路时间导致大量原始感知数据无法下载到地面站进行集中模型训练的

问题。联邦学习在低轨卫星网络上的部署会带来多方面优势：首先，数据处理和学习在低轨卫星网络中的设备更靠近用户，有效缩短了数据回传路径，显著降低端到端决策延迟；其次，联邦学习的参数更加灵活，在保障全局模型收敛性的同时，降低了对边缘节点持续连接的依赖性；此外卫星通信中各实体的数据隐私和安全得到加强，训练和预测可以在不共享数据的情况下完成，用户的敏感数据将不会暴露或导出到服务器或第三方。AI赋能的防御技术，有助于对低轨卫星网络进行优化，从而通过确保稳定和安全的卫星连接与减轻各类攻击的危害，增强整体安全态势。

5 总结与展望

本文回顾了低轨卫星网络的发展，指出了现有研究在系统性、全面性上的不足，并在此基础上，深入探讨了低轨卫星网络的体系架构和特点。通过对低轨卫星网络的潜在脆弱性进行分析，总结其由太空环境导致的节点脆弱性、由高动态性导致的链路脆弱性、由商业属性导致的协议脆弱性和与传统地面互联网耦合导致的基础设施脆弱性。该文揭示其可能遭遇的安全威胁并按物理层、网络层、应用层进行分类，研究了与每种安全威胁具体的攻击手段及相关的独特特征。针对这些安全问题，本文详细介绍了一系列正在蓬勃发展的技术，如基于量子密码的加密体制、基于弹性路由的故障恢复措施、基于虚拟化技术的仿真平台和深度学习、联邦学习等AI赋能的更多安全技术。这些技术在提高低轨卫星网络的安全性方面发挥了重要作用，同时也有广阔的发展和应用空间。

展望未来，低轨卫星网络的安全性研究将是一个长期而复杂的过程。随着量子通信、人工智能等新技术的融入，低轨卫星网络的安全防御技术将更加智能化、自动化，更多新兴技术将在低轨卫星网络领域发挥更重要的作用，如自适应智能组网技术和智能组网协议体系的发展，将为高效融合空天地海等多域网络提供支持，利用深度学习方法分析研究卫星网络的特性，创建相应的神经网络模型，进而提高网络适应性及协同性。同时，随着低轨卫星网络的商业化进程加快，如何平衡安全性与经济效益值得深入探讨，未来的研究应更加关注成本效益分析，以及如何在不同的应用场景下，实现网络安全与服务效率的最佳平衡。此外，国际合作在低轨卫星网络的安全治理中将扮演越来越重要的角色，共同制定国际标准和规则，以应对跨国界的安全威胁。

参 考 文 献

[1] 陈全, 杨磊, 郭剑鸣, 等. 低轨巨型星座网络: 组网技术与研究现状[J]. 通信学报, 2022, 43(5): 177–189. doi: 10.11959/j.issn.1000-436x.2022075.
CHEN Quan, YANG Lei, GUO Jianming, *et al*. LEO mega-constellation network: Networking technologies and state of the art[J]. *Journal on Communications*, 2022, 43(5): 177–189. doi: 10.11959/j.issn.1000-436x.2022075.

[2] LI Xiangling, FENG Wei, WANG Jue, *et al*. Enabling 5G on the ocean: A hybrid satellite-UAV-terrestrial network solution[J]. *IEEE Wireless Communications*, 2020, 27(6): 116–121. doi: 10.1109/MWC.001.2000076.

[3] DEL PORTILLO I, CAMERON B G, and CRAWLEY E F. A technical comparison of three low earth orbit satellite constellation systems to provide global broadband[J]. *Acta Astronautica*, 2019, 159: 123–135. doi: 10.1016/j.actaastro.2019.03.040.

[4] BHATTACHERJEE D and SINGLA A. Network topology design at 27, 000 km/hour[C]. The 15th International Conference on Emerging Networking Experiments and Technologies, Orlando, USA, 2019: 341–354. doi: 10.1145/3359989.3365407.

[5] 安建平, 李建国, 于季弘, 等. 空天通信网络关键技术综述[J]. 电子学报, 2022, 50(2): 470–479. doi: 10.12263/DZXB.20210029.
AN Jianping, LI Jianguo, YU Jihong, *et al*. Key technologies of space-air-ground communication networks: A survey[J]. *Acta Electronica Sinica*, 2022, 50(2): 470–479. doi: 10.12263/DZXB.20210029.

[6] CAO Huan, WU Lili, CHEN Yue, *et al*. Analysis on the security of satellite internet[C]. The 17th China Cyber Security Annual Conference, Beijing, China, 2020: 193–205. doi: 10.1007/978-981-33-4922-3_14.

[7] 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.

[8] WANG Yuntao, SU Zhou, NI Jianbing, *et al*. Blockchain-empowered space-air-ground integrated networks: Opportunities, challenges, and solutions[J]. *IEEE Communications Surveys & Tutorials*, 2022, 24(1): 160–209. doi: 10.1109/COMST.2021.3131711.

[9] 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.

[10] 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.

[11] TEDESCHI P, SCIANCALEPORE S, and DI PIETRO R. Satellite-based communications security: A survey of threats, solutions, and research challenges[J]. *Computer Networks*, 2022, 216: 109246. doi: 10.1016/j.comnet.2022.109246.

[12] MANULIS M, BRIDGES C P, HARRISON R, *et al*. Cyber security in new space[J]. *International Journal of Information Security*, 2021, 20(3): 287–311. doi: 10.1007/s10207-020-00503-w.

[13] KANG M, PARK S, and LEE Y. A survey on satellite communication system security[J]. *Sensors*, 2024, 24(9): 2897. doi: 10.3390/s24092897.

[14] CHEN Quan, GIAMBENE G, YANG Lei, *et al*. Analysis of inter-satellite link paths for LEO mega-constellation networks[J]. *IEEE Transactions on Vehicular Technology*, 2021, 70(3): 2743–2755. doi: 10.1109/TVT.2021.3058126.

[15] 李元龙, 李志强. 基于STK的Starlink星座覆盖仿真分析[J]. 指挥控制与仿真, 2023, 45(1): 119–129. doi: 10.3969/j.issn.1673-3819.2023.01.019.

LI Yuanlong amd LI Zhiqiang. Simulation analysis of Starlink constellation coverage based on STK[J]. *Command Control & Simulation*, 2023, 45(1): 119–129. doi: 10.3969/j.issn.1673-3819.2023.01.019.

[16] KLENZE T, GIULIARI G, PAPPAS C, *et al*. Networking in heaven as on earth[C]. The 17th ACM Workshop on Hot Topics in Networks, Redmond, USA, 2018: 22–28. doi: 10.1145/3286062.3286066.

[17] 朱沁雨, 曹延华, 陶海成, 等. 低轨星座网络拓扑的抗毁性研究进展[J]. 计算机工程与应用, 2022, 58(17): 1–12. doi: 10.3778/j.issn.1002-8331.2203-0316.

ZHU Qinyu, CAO Yanhua, TAO Haicheng, *et al*. Research progress on survivability of low-orbit constellation network topology[J]. *Computer Engineering and Applications*, 2022, 58(17): 1–12. doi: 10.3778/j.issn.1002-8331.2203-0316.

[18] ESA. Space debris by the numbers[EB/OL]. https://www.esa.int/Safety_Security/Space_Debris/Space_debris_by_the_numbers, 2024.

[19] Kepler Communications. Application of space exploration holdings, LLC, for modification of authorization for the SpaceX NGSO satellite system[EB/OL]. https://licensing.fcc.gov/myibfs/download.do?attachment_key=2638397, 2020.

[20] LI Yuanjie, LI Hewu, LIU Wei, *et al*. A networking perspective on Starlink's self-driving LEO mega-constellation[C]. The 29th Annual International Conference on Mobile Computing and Networking, Madrid, Spain, 2023: 17. doi: 10.1145/3570361.3592519.

[21] MA Sami, CHOU Y C, ZHANG Miao, *et al*. LEO satellite network access in the wild: Potentials, experiences, and challenges[J]. *IEEE Network*, 2024, 38(6): 396–403. doi: 10.1109/MNET.2024.3391271.

[22] AN Kang, LIN Min, OUYANG Jian, *et al*. Secure transmission in cognitive satellite terrestrial networks[J]. *IEEE Journal on Selected Areas in Communications*, 2016, 34(11): 3025–3037. doi: 10.1109/JSAC.2016.2615261.

[23] BANKEY V and UPADHYAY P K. Physical layer security of multiuser multirelay hybrid satellite-terrestrial relay networks[J]. *IEEE Transactions on Vehicular Technology*, 2019, 68(3): 2488–2501. doi: 10.1109/TVT.2019.2893366.

[24] ZHANG Le, DU Ye, and SUN Zhengyang. Modeling and analysis of cascading failures in LEO satellite networks[J]. *IEEE Transactions on Network Science and Engineering*, 2024, 11(1): 807–822. doi: 10.1109/TNSE.2023.3308610.

[25] NGUYEN T N, TRAN D H, CHIEN T V, *et al*. Security and reliability analysis of satellite-terrestrial multirelay networks with imperfect CSI[J]. *IEEE Systems Journal*, 2023, 17(2): 2824–2835. doi: 10.1109/JSYST.2022.3201128.

[26] AO Di, SHI Ruisheng, LAN Lina, *et al*. On the large-scale traffic DDoS threat of space backbone network[C]. 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), Washington, USA, 2019: 192–194. doi: 10.1109/BigDataSecurity-HPSC-IDS.2019.00045.

[27] ZHANG Yan, WANG Yong, HU Yihua, *et al*. Security performance analysis of LEO satellite constellation networks under DDoS attack[J]. *Sensors*, 2022, 22(19): 7286. doi: 10.3390/s22197286.

[28] GIULIARI G, CIUSSANI T, PERRIG A, *et al*. ICARUS: Attacking low earth orbit satellite networks[C/OL]. 2021 USENIX Annual Technical Conference, 2021: 317–331.

[29] ZHANG Yaoying, WU Qian, LAI Zeqi, *et al*. Energy drain attack in satellite internet constellations[C]. 2023 IEEE/ACM 31st International Symposium on Quality of Service, Orlando, USA, 2023: 1–10. doi: 10.1109/IWQoS57198.2023.10188709.

[30] KIM T H J, BASESCU C, JIA Limin, *et al*. Lightweight source authentication and path validation[C]. 2014 ACM conference on SIGCOMM, Chicago, USA, 2014: 271–282. doi: 10.1145/2619239.2626323.

[31] 薛文浩, 潘恬, 卢诚承, 等. 低轨卫星网络星间路由安全机制研究[J]. 天地一体化信息网络, 2023, 4(2): 13–23. doi: 10.11959/j.issn.2096-8930.2023015.

XUE Wenhao, PAN Tian, LU Chengcheng, *et al*. Research on LEO satellite network routing security[J]. *Space-*

Integrated-Ground Information Networks, 2023, 4(2): 13–23. doi: 10.11959/j.issn.2096-8930.2023015.

[32] PIRAYESH H and ZENG Huacheng. Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey[J]. *IEEE Communications Surveys & Tutorials*, 2022, 24(2): 767–809. doi: 10.1109/COMST.2022.3159185.

[33] LIU Wei, LI Yuanjie, LI Hewu, *et al*. The dark side of scale: Insecurity of direct-to-cell satellite mega-constellations[C]. 2024 IEEE Symposium on Security and Privacy, San Francisco, USA, 2024: 445–464. doi: 10.1109/SP54263.2024.00149.

[34] ZHANG Yunfan, HAN Chi, CHU Feihuang, *et al*. Jamming analysis between non-cooperative mega-constellations based on satellite network capacity[J]. *Electronics*, 2024, 13(12): 2330. doi: 10.3390/electronics13122330.

[35] 梁丽木, 姬少培, 金星虎, 等. 基于密码的卫星互联网安全防护体系研究[J]. 信息安全与通信保密, 2024(2): 31–39. doi: 10.3969/j.issn.1009-8054.2024.02.005.
LIANG Limu, JI Shaopei, JIN Xinghu, *et al*. Research on the security protection system of satellite internet based on cryptography[J]. *Information Security and Communications Privacy*, 2024(2): 31–39. doi: 10.3969/j.issn.1009-8054.2024.02.005.

[36] VILLAR A, LOHRMANN A, BAI Xueliang, *et al*. Entanglement demonstration on board a nano-satellite[J]. *Optica*, 2020, 7(7): 734–737. doi: 10.1364/OPTICA.387306.

[37] YIN Juan, LI Yuhuai, LIAO Shengkai, *et al*. Entanglement-based secure quantum cryptography over 1, 120 kilometres[J]. *Nature*, 2020, 582(7813): 501–505. doi: 10.1038/s41586-020-2401-y.

[38] 左珮良, 侯少龙, 郭超, 等. 基于强化学习的多层卫星网络边缘安全决策方法[J]. 通信学报, 2022, 43(6): 189–199. doi: 10.11959/j.issn.1000-436x.2022111.
ZUO Peiliang, HOU Shaolong, GUO Chao, *et al*. Security decision method for the edge of multi-layer satellite network based on reinforcement learning[J]. *Journal on Communications*, 2022, 43(6): 189–199. doi: 10.11959/j.issn.1000-436x.2022111.

[39] 刘之莹, 王兴伟, 徐双, 等. 基于预计算的软件定义卫星网络节能路由[J]. 网络空间安全, 2019, 10(11): 100–109. doi: 10.3969/j.issn.1674-9456.2019.11.016.
LIU Zhiying, WANG Xingwei, XU Shuang, *et al*. Precomputation based energy-saving routing for software defined satellite networks[J]. *Cyberspace Security*, 2019, 10(11): 100–109. doi: 10.3969/j.issn.1674-9456.2019.11.016.

[40] FRATTY R, SAAR Y, KUMAR R, *et al*. Random routing algorithm for enhancing the cybersecurity of LEO satellite networks[J]. *Electronics*, 2023, 12(3): 518. doi: 10.3390/electronics12030518.

[41] 崔荣芳, 徐湛, 职如昕. 低轨卫星星座快速响应链路损毁路由算法[J]. 电讯技术, 2023, 63(8): 1165–1172. doi: 10.20079/j.issn.1001-893x.220228001.
CUI Rongfang, XU Zhan, and ZHI Ruxin. A quick-response link destruction routing algorithm for LEO satellite constellation[J]. *Telecommunication Engineering*, 2023, 63(8): 1165–1172. doi: 10.20079/j.issn.1001-893x.220228001.

[42] XIE Nannan, XIE Lijia, YUAN Qizhao, *et al*. Research on dos attack simulation and detection in low-orbit satellite network[C]. The 23rd International Conference on Algorithms and Architectures for Parallel Processing, Tianjin, China, 2024: 240–251. doi: 10.1007/978-981-97-0811-6_14.

[43] LI Hui, SHI Dongcong, WANG Weizheng, *et al*. Secure routing for LEO satellite network survivability[J]. *Computer Networks*, 2022, 211: 109011. doi: 10.1016/j.comnet.2022.109011.

[44] PAN Tian, HUANG Tao, LI Xingchen, *et al*. OPSPF: Orbit prediction shortest path first routing for resilient LEO satellite networks[C]. 2019 IEEE International Conference on Communications, Shanghai, China, 2019: 1–6. doi: 10.1109/ICC.2019.8761611.

[45] JIANG Wei, JIANG Hao, XIE Yulai, *et al*. SatShield: In-network mitigation of link flooding attacks for LEO constellation networks[J]. *IEEE Internet of Things Journal*, 2024, 11(16): 27340–27355. doi: 10.1109/JIOT.2024.3397865.

[46] WANG Xiangtong, HAN Xiaodong, YANG Menglong, *et al*. Space networking kit: A novel simulation platform for emerging LEO mega-constellations[C]. IEEE International Conference on Communications, Denver, USA, 2024: 5590–5595. doi: 10.1109/ICC51166.2024.10622181.

[47] LAI Zeqi, DENG Yangtao, LI Hewu, *et al*. Space digital twin for secure satellite internet: Vulnerabilities, methodologies, and future directions[J]. *IEEE Network*, 2024, 38(1): 30–37. doi: 10.1109/MNET.2023.3337141.

[48] GAO Yue, QIU Kun, CHEN Zhe, *et al*. Plotinus: A satellite internet digital twin system[J]. *Journal of Communications and Information Networks*, 2024, 9(1): 24–33. doi: 10.23919/JCIN.2024.10494942.

[49] HENAREJOS P, VÁZQUEZ M Á, and PÉREZ-NEIRA A I. Deep learning for experimental hybrid terrestrial and satellite interference management[C]. The 2019 IEEE 20th International Workshop on Signal Processing Advances in Wireless Communications, Cannes, France, 2019: 1–5. doi: 10.1109/SPAWC.2019.8815532.

[50] AL HOMSSI B, DAKIC K, WANG Ke, *et al*. Artificial intelligence techniques for next-generation massive satellite networks[J]. *IEEE Communications Magazine*, 2024, 62(4):

66–72. doi: 10.1109/MCOM.004.2300277.

[51] YU Changgeun, KIM D, LEE H, *et al*. GPU-accelerated CNN inference for onboard DQN-based routing in dynamic LEO satellite networks[J]. *Aerospace*, 2024, 11(12): 1028. doi: 10.3390/aerospace11121028.

[52] LIRIM A and DAGLI C. Network intrusion detection system using deep learning[J]. *Procedia Computer Science*, 2021, 185: 239–247. doi: 10.1016/j.procs.2021.05.025.

[53] CHEN Hao, XIAO Ming, and PANG Zhibo. Satellite-based computing networks with federated learning[J]. *IEEE Wireless Communications*, 2022, 29(1): 78–84. doi: 10.1109/MWC.008.00353.

[54] LIN Zheng, CHEN Zhe, FANG Zihan, *et al*. FedSN: A federated learning framework over heterogeneous LEO satellite networks[J]. *IEEE Transactions on Mobile Computing*, 2025, 24(3): 1293–1307. doi: 10.1109/TMC.2024.3481275.

杜星葵：男，硕士生，研究方向为低轨卫星网络等.

束妮娜：女，教授，研究方向为无线网络优化、卫星互联网安全等.

刘春生：男，博士，副教授，研究方向为网络优化、数据补全等.

杨　方：男，博士生，研究方向为网络空间建模仿真与性能评估等.

马　涛：男，博士，教授，研究方向为卫星互联网安全与辅助决策等.

刘　洋：男，博士，工程师，研究方向为空间信息处理、电磁信号智能识别.

责任编辑：马秀强

Overview of Security Issues and Defense Technologies for Low Earth Orbit Satellite Network

DU Xingkui[①]　SHU Nina[①]　LIU Chunsheng[①②]　YANG Fang[①]
MA Tao[①]　LIU Yang[③]

[①](*College of Electronic Engineering, National University of Defense Technology, Hefei* 230037, *China*)
[②](*Institute of Artificial Intelligence, Hefei Comprehensive National Science Center, Hefei* 230037, *China*)
[③](*Beijing Institute of Remote Sensing Information, Beijing* 100011, *China*)

Abstract:

Significance　In recent years, Low-Earth Orbit (LEO) satellite networks have experienced rapid development, demonstrating broad application prospects in mobile communications, the Internet of Things (IoT), maritime operations, and other domains. These networks are poised to become a critical component of next-generation network architectures. Currently, leading global and domestic commercial entities are actively deploying mega-constellations to enable worldwide mobile communication and broadband internet services. However, as the scale of LEO constellations expands, the satellite networks are increasingly exposed to both anthropogenic threats (e.g., cyberattacks) and environmental hazards (e.g., space debris). Existing review studies have systematically summarized research on security threats and defense mechanisms across the physical, network, and application layers of LEO satellite networks. Nevertheless, gaps remain in prior literature: First, lack of technical granularity. Many studies provide taxonomies of security issues but fail to focus sufficiently on domain-specific cybersecurity challenges or delve into technical details. Second, overemphasis on integrated space-terrestrial networks. Existing reviews often prioritize the broader context of space-air-ground-sea integrated networks, obscuring the unique vulnerabilities inherent to LEO satellite architectures. Third, imbalanced layer-specific analysis: Current works predominantly address physical and link-layer security, while insufficiently highlighting the distinct characteristics of network-layer threats. Building upon prior research, this paper presents a comprehensive review of security challenges and defense technologies in LEO satellite networks. By analyzing the inherent vulnerabilities of these systems, we provide an in-depth exploration of security threats, particularly those targeting network-layer integrity. Furthermore, we critically evaluate cutting-edge defense mechanisms developed to mitigate realistic threats, offering insights into their technical principles and implementation challenges.

Progress　This paper first elaborates on the architecture of LEO satellite networks, systematically analyzing the composition and functional roles of three core components: the space segment, ground segment, and user segment. It then summarizes the operational characteristics of LEO networks, including their dynamic multi-

layer topology, globally ubiquitous coverage, low-latency data transmission, and resilient resource allocation mechanisms. These intrinsic characteristics fundamentally enable LEO networks to deliver high-quality communication services. Subsequently, this study identifies potential vulnerabilities across four dimensions: nodes, links, protocols, and infrastructure. Due to the open nature of satellite links, transmitted data are susceptible to eavesdropping, where adversaries may intercept satellite signals, predict orbital dynamics, and deploy surveillance systems preemptively. Prior research has addressed satellite communication security through physical-layer security designs and scenario-specific eavesdropping analyses. Through theoretical modeling and case studies, this work categorizes multiple Denial-of-Service (DoS) attack variants and explores routing attack risks inherent to the open architecture of LEO networks. Furthermore, it classifies electronic countermeasure interference types based on target scenarios and adversarial objectives. To counter these threats, the paper evaluates emerging defense technologies, including encryption-based security frameworks, resilient routing protocols, and digital twin-enabled virtualization platforms for network simulation and secure design optimization. Finally, it highlights cutting-edge AI-driven security solutions, such as machine learning-powered anomaly detection and federated learning for distributed threat intelligence.

Conclusions This review critically examines the evolution of LEO satellite networks, identifying critical gaps in systematic analysis and comprehensive threat coverage within existing studies. By establishing a four-dimensional vulnerability framework—node vulnerabilities arising from harsh space environmental conditions, link vulnerabilities exacerbated by high orbital dynamics, protocol vulnerabilities stemming from commercial standardization compromises, and infrastructure vulnerabilities due to tight coupling with terrestrial internet systems—the study systematically classifies security threats across physical, network, and application layers. The paper further dissects attack methodologies unique to each threat category and evaluates advanced countermeasures. Notable innovations include quantum cryptography-enhanced encryption systems, fault-tolerant routing algorithms, virtualized network emulation environments, and AI-empowered security paradigms leveraging deep learning and federated learning architectures. These technologies not only significantly enhance the security posture of LEO networks but also demonstrate transformative potential for future adaptive security frameworks. However, challenges persist in balancing computational overhead with real-time operational constraints, necessitating further research into lightweight cryptographic primitives and cross-domain collaborative defense mechanisms. This synthesis provides a foundational reference for advancing next-generation satellite network security while underscoring the imperative for interdisciplinary innovation in space-terrestrial converged systems.

Prospects Looking ahead, research on the security of LEO satellite networks will constitute a long-term and complex process. With the integration of emerging technologies such as quantum communication and artificial intelligence, security defense mechanisms in LEO satellite networks will evolve toward greater intelligence and automation. Emerging technologies are anticipated to play increasingly critical roles in this domain, particularly through advancements in adaptive intelligent networking technologies and intelligent networking protocol architectures. These developments will support the efficient convergence of space-air-ground-sea integrated networks. The application of deep learning methodologies to analyze network characteristics and construct corresponding neural network models will further enhance network adaptability and coordination. Concurrently, as commercial deployment of LEO satellite networks accelerates, the critical challenge of balancing security requirements with economic efficiency warrants in-depth investigation. Future research should prioritize cost-benefit analyses and explore optimal trade-offs between cybersecurity and service efficiency across diverse application scenarios. Furthermore, international collaboration is expected to assume a pivotal role in the security governance of LEO satellite networks, particularly through jointly establishing international standards and regulatory frameworks to address transnational security threats. This multilateral approach will be essential for maintaining the integrity and resilience of next-generation satellite infrastructures in an increasingly interconnected orbital environment.

Key words: Low Earth Orbit (LEO) satellite networks; Network security; Defensive strategies; Artificial Intelligence (AI)