中国科学 : 信息科学 2026 年 第 56 卷 第 3 期: 491–522
SCIENTIA SINICA Informationis
中国科学院学部 科学与技术前沿论坛
《中国科学》杂志社
SCIENCE CHINA PRESS
卫星互联网安全专刊 · 评述

卫星互联网安全综述

曹进[1*], 孙钰[2], 张元玉[3], 马如慧[1*], 张田田[4], 苏洲[4], 苏璞睿[5], 李晖[1], 冯登国[5*]

1. 西安电子科技大学网络与信息安全学院, 西安 710071
2. 北京航空航天大学网络空间安全学院, 北京 100191
3. 西安电子科技大学计算机科学与技术学院, 西安 710071
4. 西安交通大学网络空间安全学院, 西安 710049
5. 中国科学院软件研究所, 北京 100190
* 通信作者. E-mail: jcao@xidian.edu.cn, rhma@xidian.edu.cn, fengdg@263.net

收稿日期: 2025–11–01; 修回日期: 2026–01–02; 接受日期: 2026–01–22; 网络出版日期: 2026–03–04

国家自然科学基金 (批准号: U23B2024) 资助项目

摘要 近年来, 随着通信技术的快速发展, 卫星互联网已成为全球信息基础设施的重要组成部分, 在军事、民用、经济和应急通信等领域的应用价值不断提升. 然而, 其网络架构开放、空间节点高动态、系统组成复杂且跨国跨域运营, 引入了多种安全挑战与威胁. 本文对卫星互联网安全进行系统性综述: 首先, 概述全球卫星互联网的发展态势及其重要意义, 阐明安全问题的重要性; 其次, 分析卫星互联网的体系特征与面临的基础性安全挑战; 再次, 梳理卫星互联网面临的多元威胁态势并结合典型案例分析; 随后, 总结安全防护技术并探讨了相关的政策与法律框架; 最后, 展望未来趋势, 旨在为卫星互联网安全领域的研究、产业实践与安全治理提供有价值的参考.

关键词 卫星互联网, 卫星互联网安全体系, 安全威胁态势, 安全防护技术, 政策与法律框架

1 引言

卫星互联网作为全球竞争的新兴领域与关键信息基础设施, 其理论价值与应用潜力日益凸显, 随之而来的安全问题也成为关键议题.

1.1 全球卫星互联网发展概况

卫星互联网通过在不同轨道部署一定数量的卫星, 构建面向全球的空间信息交换基础设施, 为地面、海洋和空中用户提供宽带接入等通信服务 [1]. 其广覆盖、低时延与宽带化特征, 可有效支撑能源、电力、应急救援等关键场景 [2], 进而推动该领域快速演进与应用扩展.

卫星互联网系统形态已由早期以地球同步通信卫星为主的少量大型卫星, 演进为中轨/低轨大规模星座网络 [3]. 早期系统主要用于广播、专网等, 覆盖范围大但链路时延高、灵活性有限. 近十年来, 微小卫星批量化制

引用格式: 曹进, 孙钰, 张元玉, 等. 卫星互联网安全综述. 中国科学: 信息科学, 2026, 56: 491–522, doi: 10.1360/SSI-2025-0463
Cao J, Sun Y, Zhang Y Y, et al. A survey of security in satellite Internet networks. Sci Sin Inform, 2026, 56: 491–522, doi: 10.1360/SSI-2025-0463

© 2026《中国科学》杂志社

https://www.sciengine.com/doi/10.1360/SSI-2025-0463

造、可复用火箭、相控阵终端、软件定义载荷与星间链路等技术不断成熟, 低轨与中轨星座开始大规模组网, 形成低时延、高弹性、易扩容的多轨协同、天地一体网络形态.

全球卫星网络正处于快速发展阶段, 国际竞争加剧 [4]. 美国企业依托发射 – 制造 – 运营的一体化能力率先规模化部署; 欧洲通过资本与产业整合推进多轨协同; 加拿大、日本、印度等国家亦加快布局并扩大其卫星网络覆盖范围. 我国正依托系统性的规划布局, 加速推进巨型星座建设. 随着各国卫星网络的迅速发展, 竞争的焦点已由频谱与轨道资源进一步延伸到发射能力、产业链协同、终端生态与标准话语权等, 监管合规与网络安全的重要性也在不断提升.

伴随着部署进程加快与市场竞争加剧, 卫星互联网商业化也在不断演进: 从地面通信补充逐步走向面向普通用户与行业的多样化服务, 例如, 偏远地区宽带接入、海上与航空移动通信、公共安全与应急指挥、能源矿业现场数据回传以及手机直连卫星等. 同时, 其仍面临设备功耗与成本高、大规模星座管理复杂、各国监管政策日趋严格以及数据安全与合规要求不断提升等多重挑战.

1.2　主要卫星互联网企业

全球卫星互联网企业围绕不同轨道类型加快布局, 形成以地球静止轨道 (geostationary orbit, GEO) 为基础保障、中地球轨道 (middle Earth orbit, MEO) 为性能补充、低地球轨道 (low Earth orbit, LEO) 为主力方向的多层次、差异化发展格局. 不同轨道体系在技术路线、市场定位与服务对象上各有侧重, 共同支撑全球空间通信网络 [5].

传统 GEO 运营商通过并购重组形成三大联盟: 欧洲通信卫星公司 (Eutelsat) 与一网 (OneWeb)、欧洲卫星公司 (SES) 与国际通信卫星公司 (Intelsat)、卫讯 (Viasat) 与国际海事卫星组织 (Inmarsat). Eutelsat 依托 36 颗 GEO 卫星提供多地区通信服务 [6]. SES 运营超 70 颗卫星 (含 GEO 和 MEO), 2024 年又以 31 亿美元收购 Intelsat, 组建了拥有超 100 颗 GEO 卫星、26 颗 MEO 卫星的混合轨道通信系统 [7~9]. Inmarsat (现属 Viasat 旗下) 运营的 Global Xpress (GX) 系统通过 5 颗 GEO 卫星构建了全球 Ka 频段高速宽带网络, 面向海事、航空、政府与企业提供高达 50 Mbps 下载与 5 Mbps 上传能力, 支持机上 Wi-Fi、海上连接及远程操作 [10]. 中国 GEO 卫星通信始于 1984 年东方红二号: 2017 年中星 16 号实现 Ka 频段高通量突破; 2020 年首颗 Ku 频段高通量宽带通信卫星亚太 6D 发射成功, 通信容量提升至 50 Gbps [11]; 2023 年中星 26 号容量进一步突破 100 Gbps [12].

MEO 卫星互联网研究相对较少: 其覆盖范围较 GEO 卫星窄且时延高于 LEO 卫星, 同时轨道维持与部署维护成本较高. 因而现有研究多聚焦于 GEO 或 LEO 卫星, 或将 MEO 卫星集成到与 LEO 或 GEO 卫星的混合网络中 [13]. SES 与 Intelsat 是全球唯一实际运营 MEO 宽带通信卫星星座的商业公司 [14]. 此外, 德国、日本、韩国均积极推进 MEO 卫星发展. 我国也稳步推进 MEO 卫星通信能力建设, 以构建自主可控的数据传输体系并支撑农业监测、物流调度与城市管理等领域的智能化升级. 在政策引导与投入下, 我国已逐步发展为全球 MEO 卫星市场中不可或缺的重要力量 [15].

LEO 卫星已成为全球新一代空间通信的重要方向 [16, 17]. 国际方面, 美国太空探索技术公司 (SpaceX) 计划发射 42000 颗低轨卫星, 且截至 2025 年 8 月已发射超过 9000 颗各代星链 (Starlink) 卫星, 服务全球超过 130 个国家/地区的 600 多万用户. OneWeb 已发射约 660 颗低轨卫星, 目前在轨运行约 654 颗. Eutelsat 于 2025 年 6 月宣布完成了新一轮 13.5 亿欧元的融资, 部分资金将用于升级 OneWeb 星座并计划发射至少 440 颗新低轨卫星. 亚马逊柯伊伯项目 (Project Kuiper) 计划发射 3236 颗卫星, 截至 2025 年 4 月 28 日已成功发射首批 27 颗卫星. 此外, 加拿大 Telesat Lightspeed、美国第二代铱星系统 (Iridium NEXT)、AST SpaceMobile 与 LynkGlobal 等项目, 分别在企业专网及直连手机通信领域展开布局 [18, 19]. 我国卫星互联网星座相继批量发射: 中国星网星座计划发射 12992 颗卫星, 至 2025 年 8 月共发射 9 组、累计 70 余颗卫星. 上海垣信的 “千帆星座” 计划发射 14000 颗卫星, 目前已发射 108 颗. 中国航天科技集团的 “鸿雁星座”、中国航天科工集团的 “行云星座” 及民营企业银河航天、九天微星等, 正在推进宽带与物联网星座研制 [20].

综上所述, 全球卫星互联网处于高速发展阶段, 高、中、低轨卫星各展所长、协同发力. 国际头部企业通过并购整合与技术创新持续扩大规模与服务范围; 我国在政策支持与技术突破下实现多轨道全面推进, 既实现了

https://www.sciengine.com/doi/10.1360/SSI-2025-0463

关键技术的自主突破, 也在星座规划与部署上展现出强劲势头, 共同推动全球空间通信网络向更高效、更广泛的方向快速迈进.

1.3　卫星互联网的关键价值与应用场景

卫星互联网作为新一代信息基础设施的重要组成部分, 已成为国家层面安全保障、产业数字化升级与全球信息连接体系的关键支撑 [21]. 相较于依赖基站和光缆的地面通信系统, 其可快速跨越地理障碍, 实现对山区、海岛、沙漠、海洋、高空以及极地等区域的无缝覆盖, 在突发灾害、战争冲突、自然阻断等极端场景下具备较强抗毁与恢复能力, 有效提升国家应急通信保障与立体通信网络的稳定性.

在国家层面, 卫星互联网被视为数字主权的重要组成, 在频谱轨道资源竞争、全球数据传输能力掌控以及网络安全与合规管理等方面具有显著地缘政治与技术博弈意义. 全球主要国家和地区 (尤其是中、美、欧等) 均将其纳入国家级新基建或主权网络布局. 中国在 “十四五” 规划和 2035 年远景目标纲要中将 “天地一体化信息网络” 列为重点发展方向 [22], 标志着卫星互联网已由技术可行迈向发展所趋.

在应用层面, 卫星互联网正由有限场景扩展至跨行业、多层次场景. (1) 公众通信方面, 可为偏远农村、边疆牧区、海岛渔村等提供基础网络接入服务. (2) 行业通信方面, 可支撑能源、电力、矿业、林业、海洋等野外站点与工程现场的宽带接入、视频回传与远程监控. (3) 交通运输方面, 可覆盖航空、船舶、铁路和高速公路等高移动性场景, 满足上网通信、远程监控、运营管理等多元化需求. (4) 应急通信与公共安全方面, 在地震、台风、洪灾、森林火灾等突发事件中, 可在地面网络瘫痪时快速恢复通信, 为指挥调度、灾情回传、舆情管控等提供可靠管道.

综上所述, 卫星互联网在维护国家网络主权与立体通信能力的同时, 也为产业升级提供关键支撑, 具备重要价值与商业前景.

1.4　卫星互联网安全问题研究的重要性

随着卫星互联网体系复杂化与规模化扩展, 其面临的安全风险与治理挑战也同步上升, 已成为制约其可持续发展与大规模部署的关键障碍.

在空间资源层面, 轨道和频谱资源争夺加剧, 大规模星座间潜在的电磁干扰、轨道碰撞和空间碎片生成风险持续上升 [21]; 全球尚缺统一有效的空间交通管理机制, 增加了长期安全运行的不确定性.

在网络安全层面, 星地链路、星间链路与终端接入均依赖无线连接, 易遭受身份伪造、链路干扰、信号窃听、篡改与欺骗等多重威胁. 尤其在空天地融合趋势下, 接入协议与地面网络趋同将扩大攻击面. 例如, KA-SAT 卫星网络遭攻击导致大量地面终端瘫痪, 造成大范围通信中断, 暴露了当前卫星系统的脆弱性.

在数据主权与隐私保护层面, 卫星覆盖跨越多国辖区, 当卫星飞过其他国家上空时, 用户的通信数据可能暂时处于不同国家管辖范围内, 存在被截获或审查风险. 若地面站建在国外, 还可能出现通信双方在本国而数据却在境外传输、存储或处理的情形.

综上所述, 卫星互联网关乎国家、企业与个人安全. 在推进星座建设、产业化与全球运营的同时, 需同步强化安全能力与机制创新, 从顶层设计、标准制定到协议选型、终端管理与数据合规等环节协同推进, 并兼顾关键基础设施脆弱性、网关/落地点集中与内部人员泄密等风险, 构建覆盖全生命周期、全链路、全场景的安全保障体系, 支撑卫星互联网的可信、可控与可持续发展.

2　卫星互联网安全体系特征与安全挑战

卫星互联网是空天地一体化网络的核心基础设施, 其安全体系建设是保障网络稳定运行与业务可靠服务的前提. 本节梳理其安全体系与架构特点, 概述空间段、地面段与用户段的核心模块及业务交互逻辑. 并结合卫星互联网广域覆盖、动态拓扑与异构融合等特征分析其面临的安全风险, 为后续安全防护技术研究提供依据.

2.1　卫星互联网典型体系

卫星互联网以互联网为底座融合地面移动通信网络, 通过星间链路 (inter-satellite link, ISL) 与网关地面站

https://www.sciengine.com/doi/10.1360/SSI-2025-0463

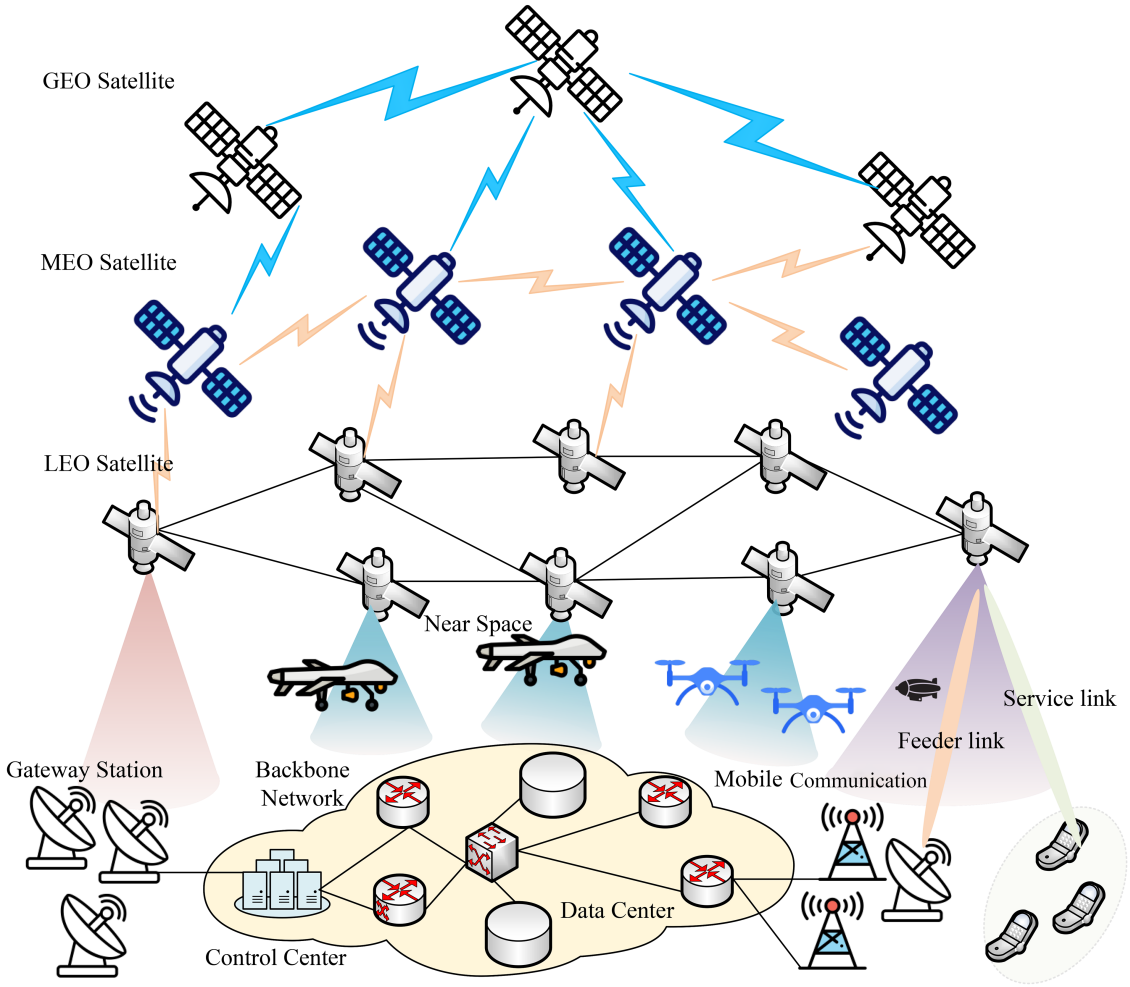


图 1　(网络版彩图) 卫星互联网典型架构图.

Figure 1　(Color online) The typical architecture diagram of satellite Internet.

(gateway station) 构建空天地一体化架构, 提供全球互联网接入服务. 如图 1 所示, 其主要包含空间段、地面段与用户段: 空间段由 LEO/MEO/GEO 等多层轨道星座组成, 通过 ISL 在时变拓扑上承载与转发核心数据业务, 并通过馈电/回传链路 (feeder link) 与网关地面站进行业务汇聚回传; 地面段由网关地面站、数据中心 (data center)、运营管控/控制中心 (control center) 及地面骨干网络 (backbone network) 等构成, 负责资源编排、策略下发与公网互通, 并可与地面移动通信网络 (mobile communication) 协同实现融合接入与业务分流; 用户段包括各类接入终端与边缘计算节点等, 通过业务/用户链路 (service link) 接入卫星网络, 完成同步、波束选择与接入等过程. 卫星互联网系统也可引入临近空间平台 (near space) 作为卫星与地面/用户侧之间的补充中继与边缘节点, 增强覆盖与承载能力.

不同轨道星座在覆盖、时延与切换特性上差异显著: GEO 覆盖广、下行传输容量大但时延较高; MEO 在覆盖与时延之间折中; LEO 通过大规模部署实现低时延与高吞吐量, 但过顶时间短导致接入终端需频繁波束/卫星切换. 实际建设中常采用 GEO/MEO/LEO 混合星座以增强网络覆盖与优化传输链路和网络性能. 星座运动形成了随时间演化的动态网络拓扑 (环形、星形、树形等), 可通过星间互联与路由优化提升卫星互联网节点间的传输效率. 若不支持星间链路, 则需选择最近网关将核心数据与任务进行落地, 并由地面骨干网络完成后续传输处理.

地面传输网络虽可支撑多协议网络融合与安全管控, 但远距离数据传输仍可能产生时延波动. 此外, 地面站

https://www.sciengine.com/doi/10.1360/SSI-2025-0463

部署规模、位置与冗余等直接影响卫星互联网的运行模式: 集中式网关部署便于统一运维但容灾能力较差; 分布式网关部署成本与运维压力更高, 但可提升终端接入与容灾能力. 因此, 卫星轨道、星间链路与网关地面站部署等共同影响卫星互联网资源调度与安全体系设计.

从实体功能角度, 卫星互联网可抽象为数据平面、控制平面与管理平面: 数据平面负责数据传输与多业务承载; 控制平面负责不同终端与卫星之间的接入、移动性管理、波束调优、路由与拥塞控制; 管理平面负责资源编排、计量与遥测管理等. 其协议栈与传统网络协议栈总体一致, 覆盖物理层/链路层多址与调制编码、网络层互连与分段路由、传输层控制与链路优化, 安全机制可按照协议栈不同层进行嵌入.

卫星载荷是实现通信、导航、感知等任务的核心模块, 与业务能力与组网模式密切相关; 除了卫星载荷外, 还包含能源、姿控、热控等公共模块以支撑卫星正常运行. 面向通信与数据传输业务, 卫星载荷主要包括通信载荷、导航载荷与信息安全载荷等. 通信载荷通常包含天线、射频链路、信号处理、星间链路处理与载荷管理和控制单元, 主要工作模式包括透明转发 (bent-pipe) 与再生处理 (regenerative). 透明转发模式以中继放大为主, 结构简单、时延低, 但链路资源利用率低且对地面网络依赖强, 常用于 GEO 以及对实时性要求高且流量集中的场景. 再生处理模式支持解调、译码、打包等星上处理, 并可提供 QoS (quality of service) 控制、多址调度与空间路由等能力, 有助于降低对单一地面站依赖, 但其对星载算力、功耗与在轨可信升级等提出了更高要求.

当前卫星互联网在接入与移动性管理中采用随机接入、半持久调度、波束级功率与频谱自适应策略, 并与移动通信核心网在身份鉴权、资源切片与安全策略控制上进行深度融合. 在网络资源管理与功能编排层面, 卫星互联网通过软件定义网络与网络功能虚拟化技术将频谱、功率、缓存与安全能力等抽象为可编排的虚拟资源, 由策略引擎实施跨域资源调度. 为缩短数据的传输路径与时延, 可在卫星轨道、地面站与边缘数据中心之间分层部署缓存、协议代理与数据加解密服务. 综上所述, 卫星互联网典型体系的本质是在多轨、多模式、多场景与多域资源编排约束下, 完成覆盖、时延、容量与服务的多目标折中, 并为后续安全体系设计提供结构化依据.

2.2　卫星互联网总体特点与挑战分析

本小节从空间轨道环境、体系结构复杂性与跨国跨域特性 3 个方面分析卫星互联网的总体特征与安全挑战, 并讨论大规模星座带来的安全管理难度, 为后续安全防护技术研究提供依据.

2.2.1　空间环境特点

卫星互联网以多轨道混合架构运行, 环境呈现高动态与异质性. 不同轨道在覆盖半径、传输时延与波束切换频率上差异显著: GEO 覆盖大且切换频率低, 但时延高达数百毫秒; LEO 传输路径短、时延低, 但因高速运动需频繁波束与网关切换; MEO 介于两者之间. 此外, 高速运动带来多普勒频移与相位变化, 叠加大气层与电离层时变特性, 易导致传输链路恶化, 使物理层与链路层呈现强时变特征. 同时, 星间/星地链路可见性受轨道与地形等因素影响, 难以持续稳定, 路由路径随时间呈周期性变化. 因此, 轨道条件、传播环境与系统动态特征共同构成卫星互联网体系设计与安全防护的基础约束条件.

空间环境主要挑战包含: (1) 终端接入与移动性管理需在高切换、高动态下保持稳定 [23]; (2) 跨域协同与协议适配需兼顾时延、误码与时变等约束; (3) 资源编排转向多域协同, 需将波束、频谱、功率与缓存等抽象为可观测、可编排对象以实现动态化资源保障; (4) 在星载算力与能耗约束下保障卫星节点的再生处理能力和业务可靠性. 综上所述, 多轨共存强化了卫星系统的动态性, 对路由策略、业务传输与资源编排等功能提出更高的要求.

2.2.2　体系结构复杂性

卫星互联网由空间段、地面站、用户终端与地面控制中心构成多层架构, 需要数据、控制与管理的跨平面协同. 空间段需综合评估星间链路与载荷能力以自适应生成路由; 地面段以地面站、数据中心与骨干网承载业务, 控制中心可借助 SDN (software-defined networking)/NFV (network functions virtualization) 将资源抽象为可编排单元, 并结合数字孪生开展全域测试与闭环优化. 低轨模式下, 终端因卫星高速移动频繁触发波束、卫星与网关切换, 要求终端接入与鉴权流程自适应完成切换并尽量降低端到端协议开销. 异构网络下, 不同厂商节点互操

https://www.sciengine.com/doi/10.1360/SSI-2025-0463

作、软硬件长期共存与在轨升级成为演进关键, 也使协议兼容与关键功能拆分更具挑战. 综上所述, 多轨互联结构使优化问题具有全局耦合与动态约束特征, 接入控制、路由选择与资源编排均需在时变拓扑、链路资源与业务策略之间进行全局协同优化. 因而需构建具备可观测、可预测与可编排能力的体系化机制, 以在覆盖、时延、容量与可靠性等关键指标间维持稳态平衡, 支撑卫星互联网长期可靠运行.

2.2.3　跨国跨域特性

卫星互联网运行于太空开放空间, 天然具有跨国属性, 不可避免涉及全球资源协调与政策约束. 2022 年 2 月, Viasat 卫星网络遭大规模恶意流量攻击, 使得网络中的调制解调器难以保持在线, 攻击者通过渗透到 KA-SAT 卫星网络的管理部分发起攻击, 影响了欧洲多个国家的卫星互联网服务. 此外, 受地面站部署与监管权限限制, 卫星系统需在全球协同与属地合规框架下运行. 频率与轨道资源由国际电信联盟 (International Telecommunication Union, ITU) 负责分配与协调, 而地面网关建设与运营需遵守各国无线电管理制度. 数据跨国传输还需满足各国在数据主权、加解密与合法审计等方面的差异化要求, 这进一步增加了身份认证、密钥分发与时间同步等环节的复杂性.

在跨国运营中, 卫星互联网安全不仅需要链路加密与抗干扰, 也高度依赖运营商侧账号体系、虚拟专用网络 (virtual private network, VPN)/远程运维、日志审计与事件响应. 2025 年 6 月, Viasat 确认出现 “未经授权访问”, 一旦服务商侧被入侵, 影响可能跨越多行业与多区域. 因此, 需在不同监管体系间实现标准与接口互操作以降低系统耦合与安全风险; 跨域策略、路由与密钥管理应具备可追溯、可回退及可审计能力, 以支撑安全事件的责任界定与应急响应; 同时建立可操作的供应链防护与审查机制, 在国际协同与主权安全之间取得平衡.

2.2.4　大规模星座安全管理难度

低轨卫星覆盖范围有限, 常需部署数千上万颗卫星以满足覆盖与业务需求, 节点规模显著增加安全管理难度. 可将大规模星座安全管理难点抽象为 “三层一闭环” 框架: 设备/软件层、策略/身份层与运行层, 以及贯穿其上的观测 – 评估 – 编排 – 验证闭环.

设备/软件层侧重版本与配置一致性, 避免因型号或软件版本差异导致同轨网络策略不一致. 策略/身份层需确保身份、密钥与访问控制在卫星、地面站与地面控制中心一致生效, 包括分层密钥管理、定期轮换、撤销同步等, 并将安全与业务策略按任务分片下发以提升其管理效率. 运行层需保障在轨升级可控可回退, 并实现异常的及时检测、预警与反馈. 闭环机制通过持续、可量化操作, 使安全控制策略具备可观测、可决策、可执行与可验证能力, 支撑从态势认知到策略落地的全流程管理.

实际部署中可采用中心策略集中控制、分布式代理实施的多级架构, 在网关侧就近执行相关安全策略与合规管控; 跨域协同策略执行则需基于零信任架构的标准化接口与最小权限控制. 因此, 大规模星座安全管理一方面要保持安全策略一致性与风险可控, 另一方面需提升卫星系统的运维自治能力与跨域协同能力.

3　卫星互联网安全威胁态势与典型案例

受开放架构、系统结构复杂与跨国运维等因素影响, 卫星互联网面临严峻且多元的安全威胁. 本节系统性梳理从通信链路、信令与数据传输到供应链与跨层攻击的威胁链条, 并结合典型事件说明其现实影响.

3.1　通信链路攻击

卫星通信链路开放, 其上下行信号极易遭干扰、截获、阻塞、欺骗等攻击, 对卫星通信安全甚至用户生命财产安全造成严重威胁.

3.1.1　信号干扰

如图 2 所示, 信号干扰通过在通信或导航频段发射高功率电磁干扰信号 (interference signal) 降低合法信号信噪比, 使其无法正确接收或中断, 从而导致通信业务中断并可能引发导航失效, 增加交通运输、物流与航空航海

https://www.sciengine.com/doi/10.1360/SSI-2025-0463

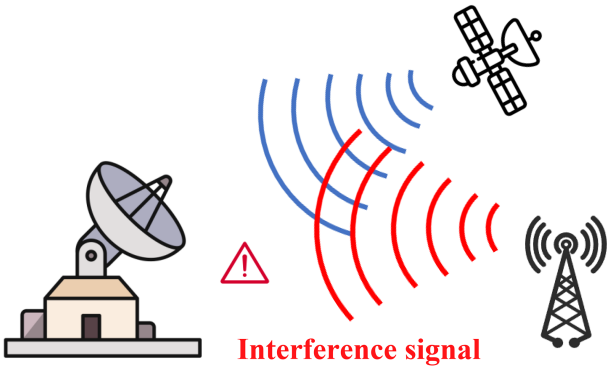


图 2　(网络版彩图) 信号干扰示意图.

Figure 2　(Color online) Illustration of signal interfering.

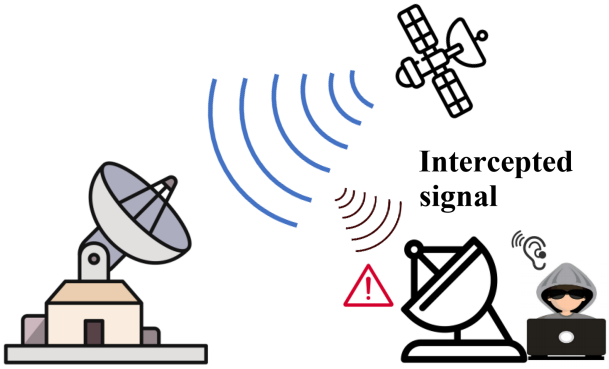


图 3　(网络版彩图) 信号截获示意图.

Figure 3　(Color online) Illustration of signal interception.

等安全风险 [24]. 卫星信号干扰的目标包括导航系统 (如 GPS、北斗)、通信卫星 (含地球同步与低轨星座)、卫星电视及遥感数据链路等. 由于卫星信号穿越大气层后功率极弱 (约 −160 dBW), 低功率地面干扰源也可能造成显著影响, 使卫星链路对干扰极为敏感. 威胁主体既包括国家级军事与情报机构的定向电子战压制, 也包括民用领域中非法干扰设备、商业竞争干扰及个人误用. 例如, 车载全球导航卫星系统 (global navigation satellite system, GNSS) 干扰器在机场、港口与交通枢纽等环境中即可造成定位失效并引发严重安全隐患. 冲突对抗场景中, 干扰常用于遮断敌方卫星通信、影响导航制导并阻断无人机与卫星互联网链路, 削弱对方的态势感知与作战指挥能力. 随着 Starlink, OneWeb 等低轨星座成为通信基础设施, 干扰活动从传统的对抗手段扩展至信息安全与网络攻防领域, 针对星座上行链路、地面终端与中继网关的干扰增多, 呈现由区域压制向更广域频谱威胁演化. 卫星信号干扰最典型的代表是导航信号干扰. 近年来, 欧洲多国报告了 GNSS 导航干扰现象. 根据欧空局 (European Space Agency, ESA) 和北约公开通报, 波罗的海 (Baltic Sea) 与黑海上空多次出现 GPS, GLONASS 信号中断, 影响民航与船舶航线安全. 例如, 2024 年一架空军飞机在飞越特定区域时报告 GPS 信号异常, 专家怀疑与战区附近电磁干扰有关 [25]. 同年, 一架飞机因广播式自动相关监视 (automatic dependent surveillance-broadcast, ADS-B) 系统遭 GPS 干扰导致导航辅助系统失效, 最终坠毁并导致重大人员伤亡 [26].

3.1.2　信号截获

如图 3 所示, 信号截获指攻击者在未授权情况下获取通信链路中传输的信息 (intercepted signal), 由于信号在开放空间传播, 攻击者只要处于信号传播范围内, 即可能利用地面高增益天线与软件定义无线电 (software-defined radio, SDR) 捕获传输信号. 信号截获通常不改变通信内容也不干扰信号传输, 而通过监听与分析获取信息; 未加密或弱加密系统的信息可能泄露 [27]. 该攻击门槛相对较低, 参与者广泛, 无论是国家的情报机构, 还是商业组织或黑客团体, 甚至个人研究者都可能通过信号截获对卫星通信安全造成威胁.

卫星信号截获的主要方式是被动监听: 在目标卫星波束覆盖区部署高灵敏度接收器接收下行信号并解调解码; 若采用加密, 还需具备密码破译能力以恢复内容. 德国研究团队 Chaos Computer Club München 基于软件无线电平台开发的 iridium-toolkit [28] 和 gr-iridium [29], 可实时截获铱星下行信号并解析 Iridium Ring Alert 等下行广播消息, 同时可配合密码破译工具窃听部分用户语音与短信数据 [30]. 还有研究指出 COSPAS-SARSAT 卫星下行链路存在明文可接收隐患, 攻击者可利用廉价 SDR 与开源解码工具实现被动截获与信息复原, 暴露国际搜救通信体系在链路保密与抗监听设计上的脆弱性 [31].

3.1.3　信号阻塞

如图 4 所示, 信号阻塞以链路可用性为目标, 通过遮挡、吸收信号或在特定频带注入高功率噪声、调制干扰等方式, 使合法信号持续、间歇或定向衰减至不可被可靠接收 (no signal), 导致链路不可用或严重降级. 信号阻

https://www.sciengine.com/doi/10.1360/SSI-2025-0463

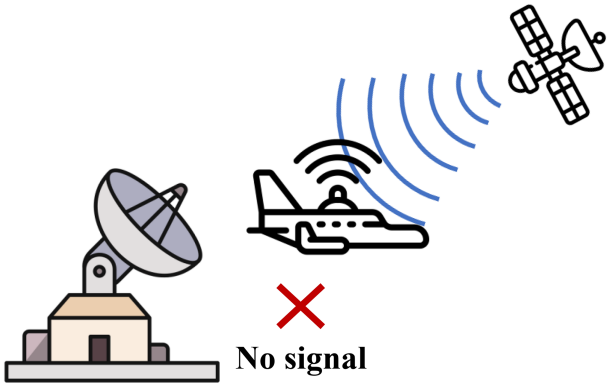


图 4　(网络版彩图) 信号阻塞示意图.

Figure 4　(Color online) Illustration of signal blocking.

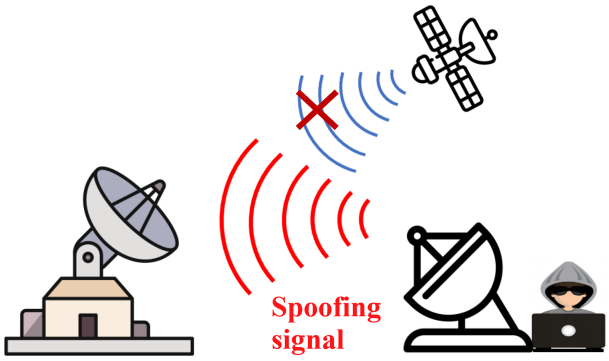


图 5　(网络版彩图) 信号欺骗示意图.

Figure 5　(Color online) Illustration of signal spoofing.

塞按形式可分为上行、下行与星间链路阻塞. 上行链路阻塞表现为地面站或终端发出的控制、命令或上报数据无法被卫星成功接收 [32]; 攻击者在地面部署高功率发射器或定向屏蔽即可以较低成本实现阻断. 下行链路阻塞是卫星向地面广播或点对点下行被覆盖或淹没; 由于到达地面的卫星信号经过长距离传输后已非常微弱, 攻击者无需巨大功率即可对局部区域造成有效干扰, 进而导致民用通信服务 (宽带、广播) 中断或导航信号失效. 星间链路阻塞可能来自针对星间链路频段的高功率干扰、定向激光遮挡或物理事件 (如空间碎片、太阳辐射或空间天气造成的噪声升高), 造成关键中继节点失联并引发区域服务崩溃. 大规模星座依赖星间链路实现分布式路由、跨地理区域中继以及降低地面中继依赖; 一旦星间链路被阻塞, 数据平面与控制平面可能隔离, 导致局部节点难以获取全网态势.

卫星信号阻塞已由简单干扰工具演变为能够影响战术成败、破坏经济稳定, 甚至争夺太空控制权的关键核心能力. 例如, 某地区冲突中, 针对作战方的通信阻塞频繁发生. 当地通信与电子战专家在接受采访时表示, 对方以大功率电磁手段在数十公里范围内阻塞卫星终端接收信号 [33]. 此外, 美军在原有的反卫星装置基础上, 进一步构建了 “梅多兰兹” 卫星通信对抗系统, 以阻塞式干扰阻断上行链路特定频率或者频段实现对卫星系统的全域攻击.

3.1.4　信号欺骗

如图 5 所示, 信号欺骗通过逆向解析协议并生成与合法信号格式一致但携带虚假内容的信号, 诱使接收端接收伪造信号 (spoofing signal), 解析出虚假时间、位置、控制或数据信息, 从而干扰系统的正常运行 [34]. 随着低成本 SDR 与自动化工具的普及, 构造和发射这种 “近似合法” 物理层信号的成本越来越低. 一些较早投入使用的卫星, 其通信协议在设计和部署的时候, 因过于强调效率与兼容性而忽视了安全认证机制, 导致其缺乏对信号来源真实性的验证, 更易被攻击者利用.

相比于信号干扰或阻塞, 信号欺骗的形式更加隐蔽且后果更严重: 可导致 GNSS 系统定位与时钟发生错误, 造成时空错乱, 诱导无人机、卫星或工业设备执行伪造指令, 甚至在 “中间人” 环节截取或篡改敏感会话. 在交通、航空、航海或金融等关键基础设施中, 一次成功的信号欺骗可能会引发事故, 产生人员伤亡, 造成巨大财产损失或服务大规模中断; 在重大安全领域则可能误导指挥决策、诱导兵力调动, 甚至蒙蔽战场感知, 从而改变全局态势. 例如, 2013 年德克萨斯大学的研究人员用低成本设备发送低功率 GPS 欺骗信号, 成功地让一艘正在航行的游艇偏离了预定航线 [35]; 2017 年黑海多艘船舶 GPS 定位系统集体偏差暴露了航运系统在依赖卫星导航时的脆弱性 [36]. 研究亦表明, 即便采用了消息验证码来检测信号完整性的伽利略系统, 其导航信号仍可能被成功欺骗 [37,38].

https://www.sciengine.com/doi/10.1360/SSI-2025-0463

3.2　信令与数据传输链路攻击

在卫星互联网中, 保障信令与数据的安全传输是卫星互联网的核心任务. 然而从链路层协议、网络层路由到应用层服务均可能遭受攻击, 导致服务中断、数据泄露甚至卫星系统被控制等风险.

3.2.1　链路层协议攻击

卫星互联网依赖无线信道, 使得链路层面临多重安全威胁. 尽管业界已提出多种链路层安全协议以增强通信保护, 但其设计往往优先考虑性能与兼容性, 安全性考量不足, 导致在实际部署中暴露出诸多缺陷, 难以有效应对卫星互联网复杂环境下的安全挑战.

首先, 若终端与卫星间以明文传输, 攻击者在链路范围内部署专用窃听设备即可窃听终端与卫星间的通信数据 [1]; 在窃听的基础上, 继而可篡改数据, 若卫星无法验证数据完整性则可能基于篡改信息做出错误判断并引发系统运行异常. 为确保数据传输安全, 系统可采用链路层加密与完整性保护, 但部署中仍存在缺陷: 早期 DVB-S 标准及部分私有协议采用弱加密且缺乏有效的完整性验证机制; Starlink 与 OneWeb 等在早期架构中引入了 LTE 网络, 但未对用户面数据提供完整性保护, 面临 ALTER 攻击 [39], 攻击者可实施选择密文攻击并进行域名系统 (domain name system, DNS) 欺诈, 诱导卫星终端访问仿冒的地面控制中心, 且可延伸至最新的 5G 非地面网络 (non-terrestrial network, NTN). 此外, 加州大学圣地亚哥分校和马里兰大学的研究团队近期发现并指出, 近半数 GEO 卫星传输未加密数据, 使大量敏感内容存在被第三方截获与窃听风险 [40].

其次, 由于信道开放与节点暴露等特性, 攻击者可能伪造合法终端或伪造网络节点提供虚假服务, 因而需部署身份鉴别机制. 但仍存在多种安全风险. (1) 若用户身份凭证未被安全保护, 攻击者可伪造或盗用合法用户身份标识发起注册与接入认证请求, 进而获取非法接入权限、占用链路资源、窃取数据等. (2) 若卫星接入协议在设计上存在缺陷, 如认证算法强度不足、密钥协商流程存在漏洞或缺乏抗重放机制, 攻击者可进行密码分析以破解密钥或重放截获的合法认证信令以绕过系统验证. 例如, 基于 2G 的 Globalstar 易受伪基站攻击, 攻击者利用单向认证缺陷仿冒地面控制中心向终端发送虚假指令短信. (3) 协议实现缺陷还可能使攻击者绕过鉴权直接接入. 例如, 2024 年, 宾夕法尼亚州立大学的研究团队揭示了主流 5G 基带芯片中存在的安全漏洞, 该漏洞可引发非接入层 (non-access stratum, NAS) 的 AKA 绕过与接入层 (access stratum, AS) 的安全绕过攻击 [41], 攻击流程如图 6 所示. 在 NAS AKA 绕过攻击中, 伪卫星伪造明文 “注册接受 (registration accept)” 消息绕过 NAS AKA 认证过程, 使受害终端建立无加密无完保的 N1 接口 (unprotected N1 interface); 在 AS 层安全绕过攻击中, 伪卫星通过伪造 “RRC 安全模式命令 (RRC security mode command)” 消息绕过终端与卫星间的空口加密, 使终端建立未受保护的 Uu 接口 (unprotected Uu interface) 并可在空口窃听卫星互联网传输的指控命令. (4) 攻击者可发起中间人攻击劫持整个认证与密钥协商过程, 导致后续所有会话数据被窃取或篡改. 例如, 2025 年缅甸境内电信诈骗园区通过非法渠道接入 “星链” 服务用于跨国犯罪活动, 引发美国国会相关委员会调查. 截至 2025 年 10 月, 美国太空探索技术公司声称已在缅甸电诈园区周边识别出超过 2500 台 “星链” 设备并使其不能运转 [42].

此外, 若接入过程中缺乏隐私保护, 终端将面临隐私泄露风险. 例如, 在 Iridium 等低轨卫星系统中, 攻击者即使完全不发射信号, 也可通过被动接收下行通信进行跨时间关联分析, 缩小目标用户的可能位置范围并实现持续跟踪与行为分析 [43]. 类似问题在 4G/5G 蜂窝网络中已被证实 [44]. 虽然 4G/5G 采用临时标识或加密机制来减少真实身份标识泄露, 但仍存在局限: 4G 终端首次接入或无法识别临时标识时需明文传输真实身份标识; 5G 虽采用加密方式隐藏用户真实身份标识, 但在紧急情况下仍可能回退至明文传输且可能遭受可链接性攻击 [45]. 更进一步地, 临时标识长期不变也会带来身份泄露风险. 例如, 名为 “黄貂鱼” 的 IMSI Catcher 设备曾被部署于大型公众集会、机场周边等区域, 通过伪基站诱骗终端并批量采集其 IMSI 等身份标识以实现无差别监控与定位 [46]. 研究还表明, 仅通过被动监听寻呼等空口信号即可在数秒内完成 4G 终端小区级定位验证, 并在 5G 网络中展示了利用 PIERCER 等攻击可实现标识关联与定向追踪, 进一步验证了隐私威胁的可行性 [47].

为应对上述攻击, 工业界已提出标准化接入安全机制. 2022 年, 第三代合作伙伴计划 (3rd Generation Partnership Project, 3GPP) Release 17 将 NTN 纳入 5G 标准, 明确卫星作为无线接入节点参与 5G 网络的标准化路

https://www.sciengine.com/doi/10.1360/SSI-2025-0463

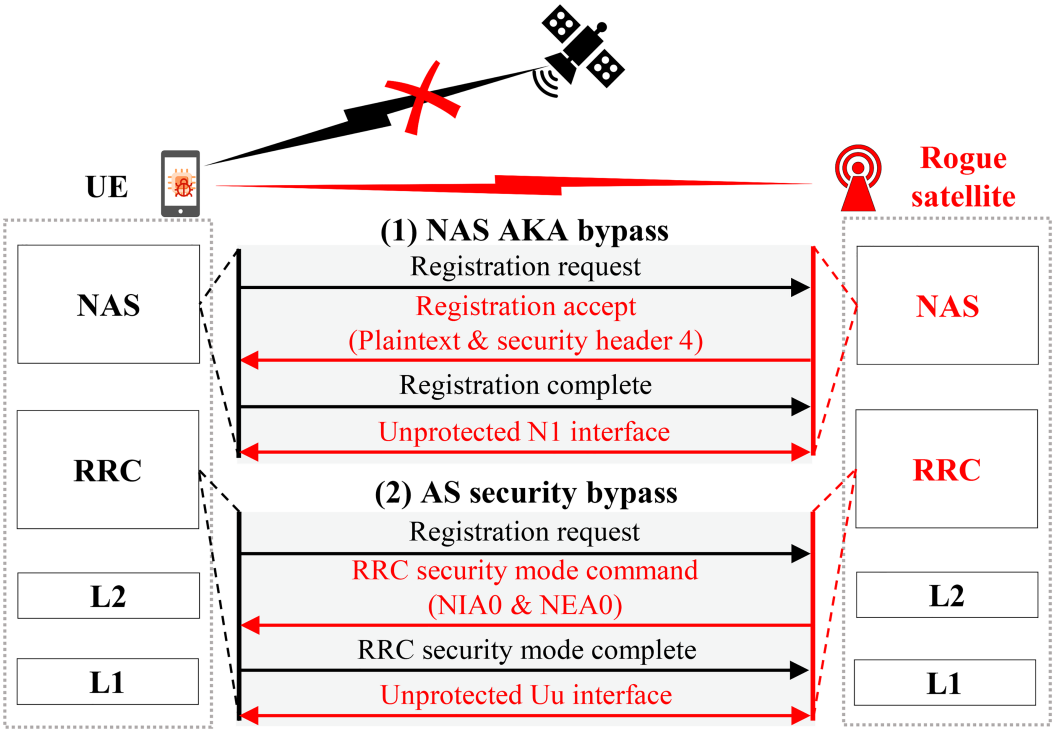


图 6　(网络版彩图) NAS AKA 绕过与 AS 绕过攻击流程.

Figure 6　(Color online) Attack procedures for NAS AKA bypass and AS bypass.

径 [48]. 复用标准化蜂窝网络有助于降低开发与部署难度, 但也可能将地面蜂窝网络长期存在的安全缺陷带入基于卫星互联网的指挥与控制链路. 目前, 3GPP 在制定终端通过存储转发卫星接入核心网的认证协议时, 考虑直接沿用地面网络接入认证协议 EPS-AKA/EAP-AKA/5G-AKA/EAP-AKA′ [49,50], 但卫星网络间歇连通与长时延可能导致超时使接入认证与算法协商无法或部分完成 [51]; 攻击者亦可利用长时延窗口对认证过程中的同步机制发起更有效的中间人攻击或重放攻击.

3.2.2　网络层路由攻击

路由协议是低轨卫星互联网的管控核心. 攻击者可通过篡改路由信息扰乱数据传输路径, 引发通信中断、数据泄露或资源滥用等安全问题.

在开放环境下, 攻击者可对路由协议发起欺骗攻击: 伪造探测报文并周期性广播给两端链路, 干扰卫星节点对链路状态的正确感知, 导致网络难以收敛; 通过注入伪造的链路状态更新消息, 宣称存在实际上不存在的优质路径, 在路由规模大、拓扑强动态条件下难以即时核验, 虚假信息可能在全网洪泛并导致路由表错误收敛, 使大量业务流量被误导 [52]. 若流量被引导至恶意节点, 可能出现选择性丢弃 (如丢弃大包或特定端口流量、仅发送探测类小包、或在卫星切换时间窗间歇性丢包以规避检测) [53], 导致通信连接中断、吞吐下降与时延抖动, 并诱发路由器错误拥塞判断与非必要降速/改路等.

此外, 受节点资源受限影响, 路由协议易遭受分布式拒绝服务 (distributed denial of service, DDoS) 攻击. 攻击者通过持续发送大量无效路由更新报文 [54], 迫使节点反复处理并重算路由, 消耗计算、内存与链路带宽, 进而导致合法路由更新无法处理、拓扑收敛缓慢甚至网络分裂, 影响全网稳定运行.

工业界已提出了一些网络层安全增强方案, 包括 IPSec (IP security) 机制以及空间数据系统咨询委员会 (Consultative Committee for Space Data Systems, CCSDS) 制定的 SCPS-SP (space communications protocol specifications-security protocol). 但将 IPSec 直接应用于卫星网络面临高时延/强抖动导致会话协商困难、连接不稳定; 高丢包引发数据包频繁重传并降低吞吐量, 同时封装头部带来额外带宽开销, 降低了有限带宽下的传输

https://www.sciengine.com/doi/10.1360/SSI-2025-0463

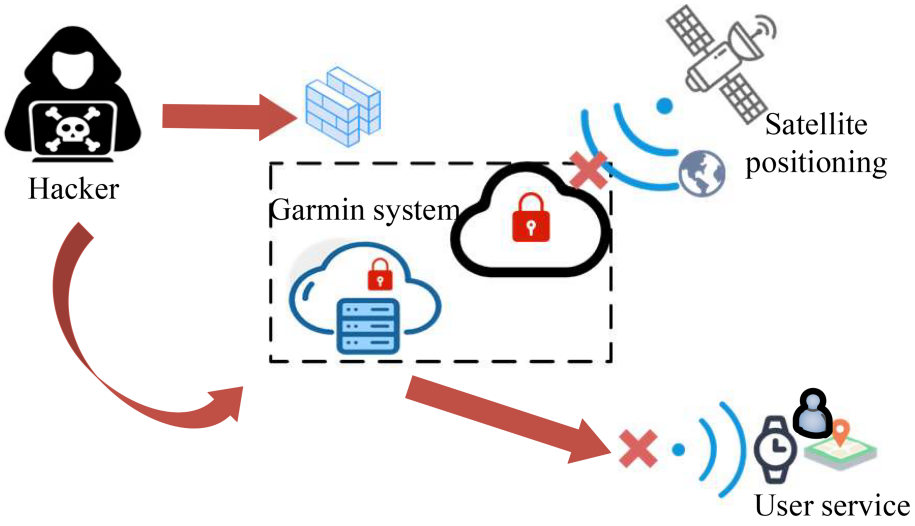


图 7　(网络版彩图) WastedLocker 勒索软件攻击.

Figure 7　(Color online) WastedLocker ransomware attack.

效率; 缺乏移动性管理使卫星切换时安全会话易中断, 影响业务连续性 [55~58]. SCPS-SP 与 IPSec 类似, 可为空间网络数据传输提供端到端保护并支持路由数据完整性、机密性检查与身份认证等 [59], 但其安全关联多依赖预置或地面站协助的一对一协商, 不支持群组密钥协商与切换认证, 且对信令内容缺乏统一规范, 导致不同航天器仍需大量定制化开发, 进一步引入安全风险 [60].

3.2.3　应用层服务攻击

应用层攻击可通过恶意代码植入与 DDoS 攻击造成服务中断、敏感数据泄露, 甚至触发系统级瘫痪风险.

卫星互联网天地一体架构下, 地面站服务器、网络管理系统与星上处理单元等设备的操作系统、运维软件或协议栈可能存在未修补的安全漏洞或配置缺陷, 攻击者可据此植入木马、后门等恶意代码并横向渗透, 建立隐蔽命令与控制信道以实现对基础设施的持久化控制; 即使部分安全弱点后续修补, 攻击者仍能通过已植入的恶意代码维持其对网络的访问权限. 星载计算机或关键固件一旦被植入恶意程序可引发服务中断与功能异常, 严重时干扰卫星运行; 地面站失陷可能导致用户数据被窃听/篡改或被用于向卫星下发未授权指令/恶意配置等, 导致星上运行异常; 用户终端失陷除导致其敏感数据泄露外, 还可能成为反向渗透地面站的跳板并干扰卫星业务等. 此类攻击具有隐蔽性与持久性, 若缺乏有效防护, 将对卫星互联网构成严重安全威胁. 例如, 2020 年 7 月, 如图 7 所示, 全球知名卫星定位设备 (satellite positioning) 制造商 Garmin 系统 (Garmin system) 遭遇 WastedLocker 勒索软件攻击. 黑客通过植入恶意代码加密其内部系统和大量云端数据, 直接导致云服务与卫星定位服务全面瘫痪, 全球用户服务 (user service) 无法正常使用 [61].

此外, 由于服务入口集中、无线信道开放且星上资源严格受限等特点, 卫星互联网易遭受 DDoS 攻击威胁. 攻击者控制大量主机可对地面站 (暴露的 IP 地址) 发送海量无效请求以耗尽带宽、计算资源或连接容量; 攻击者也可通过射频信号洪流直接针对卫星通信链路, 消耗星上资源 [62], 以较低成本造成服务退化甚至中断.

3.3　物理与供应链风险

物理安全与可信供应链是卫星互联网系统稳定运行的实体基础. 攻击者可利用地面设施的物理可接触性、全球化供应链的薄弱环节及卫星在轨运行的脆弱性等, 发起物理破坏、硬件篡改等攻击, 直接威胁系统完整性与服务连续性.

3.3.1　用户终端信任锚点安全威胁

随着 3GPP NTN 技术的普及, Starlink, OneWeb 等卫星通信系统支持用户通过标准 SIM 卡或嵌入式虚拟

https://www.sciengine.com/doi/10.1360/SSI-2025-0463

SIM (embedded SIM, eSIM) 卡直接接入网络, 终端身份认证机制与地面蜂窝网络深度耦合. SIM/eSIM 作为用户身份认证与密钥管理的核心组件, 存储包括国际移动用户识别码 (IMSI) 和长期共享密钥 (主密钥 K) 在内的多种敏感信息, 是用户接入卫星互联网的 “信任锚点”.

SIM/USIM 卡面临侧信道泄露风险: 攻击者可通过采集和分析密码算法在运行中泄露的功耗、电磁辐射与执行时间等物理信息, 恢复主密钥 K 并实现身份克隆. 2015 年有研究表明, 多款来自不同运营商和制造商的商用 USIM 卡对差分功耗分析攻击高度脆弱 [63], 攻击者无需物理破坏或特权访问, 仅监测 USIM 卡执行认证过程 MILENAGE 算法的功耗轨迹, 即可在数分钟至一小时内恢复 128 位主密钥 K 等核心安全参数. 该密钥一旦泄露, 用户身份可被永久克隆, 严重威胁通信系统的安全性.

eSIM 在逻辑层面继承了传统 SIM 的鉴权、密钥生成与存储能力且不依赖物理卡槽, 可缩减攻击者的接触面与篡改窗口, 但仍存在身份克隆风险. 2025 年波兰安全研究机构首次公开披露, 攻击者可对消费级 GSMA 合规 eUICC 与通过 EAL4 认证的安全芯片实施克隆攻击, 将同一运营商 eSIM 配置文件部署至两个独立 eUICC 并实现同时激活, 从而非法克隆 eSIM [64]. 恶意设备激活后可接收原本发送至合法用户的语音与短信, 对依赖短信进行双因素身份认证的应用场景构成严重威胁 (如邮箱、网银等动态验证码拦截).

卫星互联网终端的可信执行环境 (trusted execution environment, TEE) 通过在主处理器中构建与富执行环境 (rich execution environment, REE) 隔离的安全执行域提升安全性, 但大量研究表明, TEE 并非绝对安全, 仍面临软件栈漏洞、硬件架构缺陷、侧信道与微架构等攻击 [65~68].

综上所述, SIM/eSIM 与 TEE 的脆弱性可能导致信任锚点失效, 引发身份信息被非法复制、用户隐私数据泄露等严重后果.

3.3.2　供应链与固件篡改攻击

供应链与固件篡改攻击旨在通过修改或植入恶意硬件、替换固件或破坏关键电路实现系统控制、敏感信息窃取或功能破坏. 随着卫星通信体系日益软件化、商用组件与全球供应链的广泛应用, 网络攻击面显著扩大, 仅依赖网络边界防护的体系难以应对硬件层入侵.

卫星互联网供应链风险主要影响用户终端、卫星平台和地面系统等关键组成部分. 终端供应链攻击可在天线、调制解调器或基带芯片等终端核心组件的设计、制造或部署环节中植入恶意组件、篡改固件或预置后门, 抢先于设备启动建立持久化远程控制与数据外泄通道, 并可借此突破星地通信链路的安全防线, 致使通信数据泄露、指令篡改, 甚至以受控终端为跳板, 反向渗透地面控制网络. 例如, 2024 年宾夕法尼亚州立大学研究团队在 Black Hat 大会上公开的 5G Base Checker 工具, 首次系统性揭示了主流 5G 基带芯片 (如三星 Exynos 5123/5300) 存在的安全漏洞, 并介绍了由此引发的 NAS AKA 绕过攻击与 AS 安全绕过攻击 [41]. 攻击者发动上述攻击可仿冒基站、绕过认证流程, 建立未受保护的数据会话, 影响谷歌 Pixel、三星 Galaxy 等多款可直连卫星互联网的智能终端. 2025 年黑客组织 Lab Dookhtegan 对美国 ST Engineering iDirect 公司的 iDirect 卫星调制解调器发起网络攻击 [69]. 攻击者通过扫描暴露在公网的 iDirect 终端, 利用默认或弱口令漏洞获取 root 权限, 并部署自动化脚本使终端执行存储器擦除操作, 导致设备永久失效, 造成区域性卫星通信服务中断. 该事件暴露了卫星终端在部署过程中因配置不当 (如未修改默认凭证) 容易引发安全风险. 上述案例表明, 卫星终端的安全不仅依赖于网络边界防护, 更取决于设备底层组件的可信性, 如基带芯片、调制解调器固件等.

卫星供应链攻击可在设计、制造、集成、测试、分销及软件更新等供应链环节植入恶意硬件、固件和软件, 具有隐蔽性强、影响范围广与防御难度高等特点, 已成为威胁卫星通信、导航、遥感等关键空间基础设施的重大挑战. 美国新墨西哥大学研究提出了首个面向小型卫星的协同式硬件供应链攻击模型 SpyChain [70]. 该攻击模型利用商用现有组件在设计、制造或集成环节中的监管盲区, 将恶意逻辑植入非核心但具备高权限访问能力的辅助组件 (如电源管理、遥测接口模块), 在卫星发射前即建立持久化 “后门”. 由于系统默认信任这些组件, 恶意代码可在地面测试中规避检测, 并利用隐蔽信道绕过地面监控实现隐身通信; 入轨后则通过遥测数据窃取、运行指令干扰或拒绝服务 (denial of service, DoS) 攻击等方式破坏任务. SpyChain 攻击揭示了多组件协同执行的新型攻击向量, 其在美国国家航空航天局 (National Aeronautics and Space Administration, NASA) 的 NOS3 仿真

https://www.sciengine.com/doi/10.1360/SSI-2025-0463

平台上成功验证, 并已被纳入 SPARTA 攻击矩阵. 同理, 地面系统同样可能成为供应链攻击目标. 例如, 2022 年 Viasat KA-SAT 卫星遭受地面固件擦除攻击 [71], 攻击者首先利用 Viasat 运营网络中某台 VPN 设备的配置缺陷, 成功实现远程接入, 进入受信任的管理网络. 随后, 在内网中进行横向渗透, 逐步深入至管理 KA-SAT 卫星通信系统的核心操作区域. 最终, 通过执行底层管理命令, 深度擦除存储调制解调器固件的闪存, 致使数万台 VSAT 终端失联并引发服务大面积中断. 此次攻击不仅影响战区内的指挥通信, 还波及欧洲多国的能源、交通等关键民用基础设施, 凸显出卫星地面系统的脆弱性.

卫星终端的固件签名、安全启动与回滚保护机制构成递进式可信保障体系, 实现来源可信、执行可信和持续可信的核心目标. 固件签名通过非对称加密技术对固件映像进行数字签名, 终端在更新时验证签名的合法性, 确保固件来源的可信性, 防止攻击者伪造或篡改固件并注入恶意代码 [72]. 若缺失该机制, 攻击者可轻易刷入未经授权的固件, 植入持久化后门, 实现长期潜伏控制. 安全启动建立逐级验证的信任链, 从第一级引导程序开始, 逐层校验后续组件的完整性和真实性, 确保系统在启动过程中不被劫持, 确保执行可信 [73]. 一旦该机制缺失, 即便固件本身合法, 其加载过程仍可能被中间替换, 导致系统从启动之初即处于不可信状态. 回滚保护机制通过维护固件安全版本号或递增计数器, 禁止设备降级至已知存在漏洞的旧版本, 有效防范降级攻击, 保障系统在生命周期内的持续可信 [74]. 若缺乏此机制, 攻击者可利用历史漏洞绕过现有防护措施, 使已部署的安全补丁失效. 三者环环相扣, 共同构建卫星终端固件安全的纵深防御体系, 任一环节的缺失都将导致信任链断裂, 为供应链攻击、远程渗透和高级持续威胁 (advanced persistent threat, APT) 攻击暴露入侵攻击面并提供持久驻留条件. 例如, 2022 年比利时鲁汶大学的研究团队首次成功绕过 Starlink 用户终端安全启动 [75, 76]. 通过拆解终端的天线模组, 逆向分析其硬件架构与启动流程, 设计并开发了名为 Modchip 的破解装置. 该装置利用电压故障注入法成功绕过安全启动中的固件验签, 成功启动篡改后的不安全固件.

因此, 供应链与固件篡改不仅可能导致单设备控制, 还可能引发链路窃听、遥测数据伪造与系统级拒绝服务, 需前置防御.

3.3.3　空间物理威胁

卫星轨道环境拥挤、太空环境复杂使卫星互联网易遭受太空垃圾碰撞、恶意变轨碰撞等物理威胁, 影响卫星互联网的稳定运行 [77, 78]. 太空垃圾主要来源于废弃或者发生故障后未被妥善处理的卫星、火箭发射过程中产生的残骸、卫星碰撞产生的碎片等. 太空垃圾能够直接对在轨卫星、航天器和国际空间站的安全造成威胁, 尤其是随着商业卫星的不断增多, 空间轨道越来越拥挤, 太空垃圾的增多使得低地球轨道上的碰撞风险加大. 碰撞不仅会造成卫星或航天器的损失, 还可能产生大量碎片并触发 “碎片雪崩”, 进一步增加碰撞风险, 形成碎片链式反应.

近年来, 已有不少太空垃圾物理威胁的案例. 例如, 2009 年美国通讯卫星 “IRIDIUM 33” 与俄罗斯的废弃卫星 “Cosmos 2251” 发生碰撞并产生了约 2000 颗可追踪的碎片 [79]; 2007 年的一次反卫星试验通过摧毁废弃的气象卫星, 产生了大量碎片 [80]. 这些碎片至今依然存在, 增加了低地球轨道的垃圾密度并持续威胁在轨资产的安全.

除太空垃圾等非人为物理威胁外, 操纵卫星恶意变轨实施对目标卫星在轨碰撞也是主要的空间物理威胁之一. 例如, 2021 年和 2022 年, 美国 SpaceX 的 Starlink 卫星曾多次进行轨道调整, 导致与我国 “天宫” 空间站险些发生碰撞并引发关注 [81]. 随着轨道资源稀缺与对抗加剧, 在轨撞击威胁急需纳入空间安全治理与工程防护重点.

3.4　跨层攻击

跨层攻击可同时影响卫星互联网多个协议层或破坏层间协同, 通过干扰时空基准、篡改关键模型、渗透网络节点或破坏密码机制等方式, 导致网络同步失序、路由异常或信任体系崩塌. 典型场景包括导航信号攻击、人工智能 (artificial intelligence, AI) 模型篡改与操纵、APT 攻击等.

https://www.sciengine.com/doi/10.1360/SSI-2025-0463

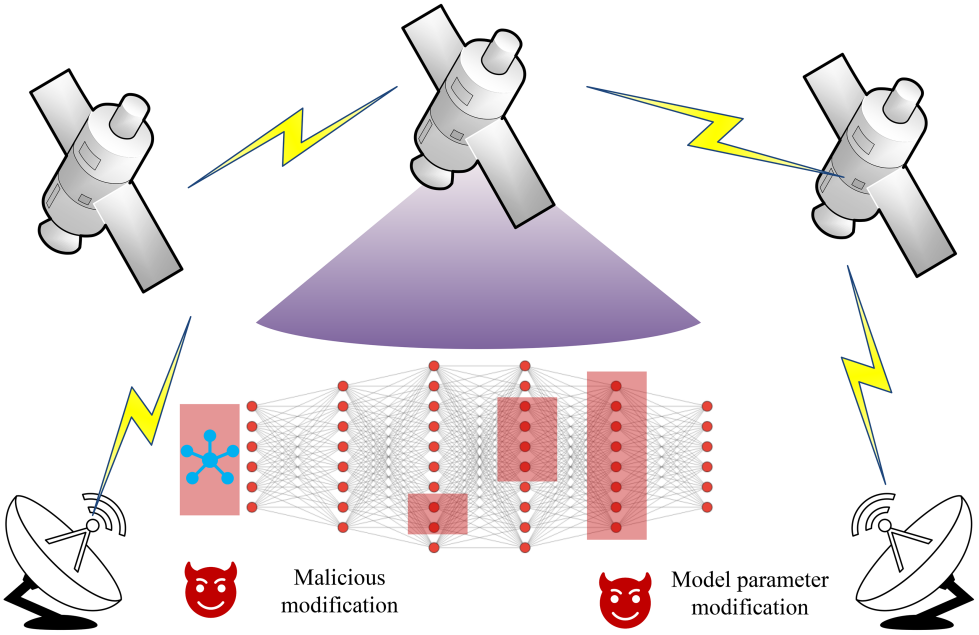


图 8　(网络版彩图) AI 模型篡改与执行结果操纵攻击.

Figure 8　(Color online) AI model tampering and execution result manipulation attacks.

3.4.1　针对导航信号的特定跨层攻击

授时/定位是网络拓扑构建、路由和密钥管理等关键环节的时间与空间基准. 一旦攻击者通过干扰、欺骗或操纵手段破坏该基准, 将从底层影响系统的同步性、连通性和信任机制, 进而在拓扑结构、路由及密钥管理等环节引发系统性风险 [82,83].

在路由层面, 节点依赖授时/定位信息感知网络结构并执行路由决策; 这些信息被干扰或篡改会导致节点对自身及邻居关系判断出现偏差, 并造成路由度量失真和控制面异常. 由于路由协议高度依赖距离、时延和链路寿命等参数, 而这些参数又高度依赖时间与位置的精度. 因此, 一旦授时或定位被篡改, 造成路径代价计算错误, 引发链路切换异常、路径失效或连接中断, 并进一步带来路由更新频繁、收敛速度下降等问题. 更严重的情况下, 攻击者可诱使流量经过自身, 实施监听或篡改, 从而破坏网络的可达性与安全性.

在密钥管理方面, 时间同步与位置信息影响密钥生成、分发与验证; 若攻击者通过伪造或干扰授时信号使系统时间发生偏移或节点位置错误, 可能导致密钥生成的随机性不足、时效验证失效与密钥轮换异常, 降低端到端加密的可靠性并放大中间人攻击或重放攻击风险.

授时与定位攻击呈现 “低层入侵、高层连锁” 特征: 攻击从信号物理层破坏时间和空间基准, 逐步影响到协议层的路由与密钥管理, 最终可能动摇整个网络的信任体系. 因此, 卫星互联网的安全设计需将授时与定位信号的真实性和完整性保护纳入核心防护框架, 结合多源时空校验、加密信号认证与跨层异常检测等技术手段形成互补防线.

3.4.2　AI 模型篡改与执行结果操纵攻击

近年来, 随着人工智能的快速发展, 卫星互联网正逐步引入相关 AI 模型用于实现通信资源调度、信号识别、入侵检测等功能, 支撑卫星互联网的异构多源数据处理与智能管控, 但模型参数修改与推理结果篡改会直接影响决策的可信性. 恶意攻击者可通过入侵地面站等方式篡改 AI 模型参数或输出结果 (如操纵资源分配模型来诱发传输链路拥塞), 其隐蔽性强、可溯性差且影响范围广.

如图 8 所示, 风险主要体现在两类篡改: (1) 对已完成训练的模型参数进行恶意修改 (model parameter modification), 降低模型的性能与准确性; (2) 对模型输出的恶意修改 (malicious modification), 误导执行策略

https://www.sciengine.com/doi/10.1360/SSI-2025-0463

并引发系统风险. 为了规避潜在风险, 可构建从模型训练到部署应用的全生命周期防护体系: 训练阶段引入模型签名与参数加密以确保模型权重的来源可验证; 部署阶段借助可信执行环境实现模型推理过程的硬件级隔离以提升模型推理结果的可信性. 此外, 可结合模型异常检测算法和分布式鲁棒优化算法动态识别执行偏差与潜在篡改行为, 形成可验证、可追踪的 AI 可信防护流程, 为卫星互联网的安全智能运行提供坚实保障.

3.4.3　APT 攻击

APT 是由国家级组织或受国家支持的黑客团体发起的复杂网络攻击模式, 具有高度隐蔽、长期潜伏和持续攻击等特征 [84]. 在卫星通信、导航与遥感等空间信息系统中, APT 攻击已成为威胁其安全运行的重要风险来源 [85]. 其通常通过多阶段、跨域协同手段, 综合运用社会工程学、零日漏洞与定制化恶意软件等, 逐步渗透卫星地面控制站、用户终端与星地通信链路, 实现对卫星系统的长期监控、数据窃取甚至功能破坏.

针对卫星互联网的 APT 攻击活动正日益增多. 例如, 2020 年全球著名的 APT 组织通过供应链攻击将恶意后门集成到 Orion 软件更新中, 影响包括美国航空航天局、多个联邦政府等关键机构. 2025 年国家互联网应急管理中心披露美国情报机构于 2024 年 7 月 ∼ 11 月对我国某通信与卫星互联网企业实施高级持续性威胁 (APT) 攻击 [86]. 攻击者通过多个境外跳板 IP, 利用该企业电子文件系统中存在的未授权访问和 SQL 注入漏洞, 植入内存驻留型后门程序, 并进一步部署窃密木马. 该木马将恶意载荷解码并注入 Tomcat Web 服务的 Filter 过滤器, 实现对特定网络流量的监听与隐蔽通信. 随后, 攻击者利用企业内部软件升级通道, 在内网中定向投递第二阶段载荷, 成功控制 300 余台终端设备, 并以 “军专网” “核心网” 等关键词为线索, 大规模搜索并窃取敏感技术资料与通信数据. 该事件充分暴露了 APT 攻击在关键基础设施环境中隐蔽渗透、持久驻留和定向窃密的典型行为模式, 也凸显了其对国家空间信息系统构成的实质性威胁.

3.4.4　SatOver 为代表的系列攻击

卫星通信系统在功能架构上与地面蜂窝网络高度同构, 普遍采用 LTE 或 NTN 协议栈并支持符合 3GPP 标准的终端直接接入. 协议栈复用降低了系统部署成本并显著简化了用户终端的接入复杂度, 已成为当前卫星互联网的主流设计范式 [87]. 然而, 这一融合架构在提升兼容性与经济性的同时, 也继承了地面蜂窝网络长期存在的信令安全缺陷.

SatOver 是典型的跨层控制面攻击, 首次针对承载卫星互联网的巨星座实现有效攻击 [87]. 其利用 NTN 与地面蜂窝系统在协议栈上的同源性, 构建了一条从物理层到 NAS 的跨层攻击路径, 其核心思想是: 在终端完成 NAS 认证与密钥协商 (AKA) 之前, 利用 RRC 子层未用加密与完整性保护的窗口期, 伪造初始控制信令, 实现对用户设备的劫持与长期控制.

通过修改开源协议栈并结合成品软件无线电设备 (如 USRP B210 等), SatOver 可对 3GPP IoT/NR-NTN 等网络发动攻击并持续阻断地面终端接入. 在攻击面、协议栈与攻击设备 3 个维度均具备原型化与实验复现可行性, 证明其硬件成本可控、部署方式灵活、结果复现稳定, 属于现实高危威胁.

3.5　网络战风险

卫星互联网在民用领域广泛应用的同时, 也逐渐成为支撑国家安全的重要基础设施 [88]. 其通过星座设计与地面站体系建设巩固数据与算力主权, 并提供广域、高带宽、低时延链路支撑多域联合作战的态势融合与快速决策; 此外, 多层次轨道星间链路与分布式网关构成的多层网络具备抗毁、抗干扰与自愈能力, 在地面骨干受损时可实现国家级关键信息的联通传输. 但其安全风险和隐患也可能对国家造成严重影响 [89, 90]. 本小节从关键设施脆弱性、频谱资源争夺与地面关口部署集中 3 方面分析其相关安全风险.

3.5.1　关键设施脆弱性风险

卫星互联网链路开放使其在对抗环境下不可避免面临干扰、监听与反制等. 例如, 2025 年 7 月 24 日约 15 时 (美国东部时间), Starlink 出现大范围故障, 全球逾 6.1 万名用户突遭断网, 中断持续约 2.5 h, 导致多地远程医疗

https://www.sciengine.com/doi/10.1360/SSI-2025-0463

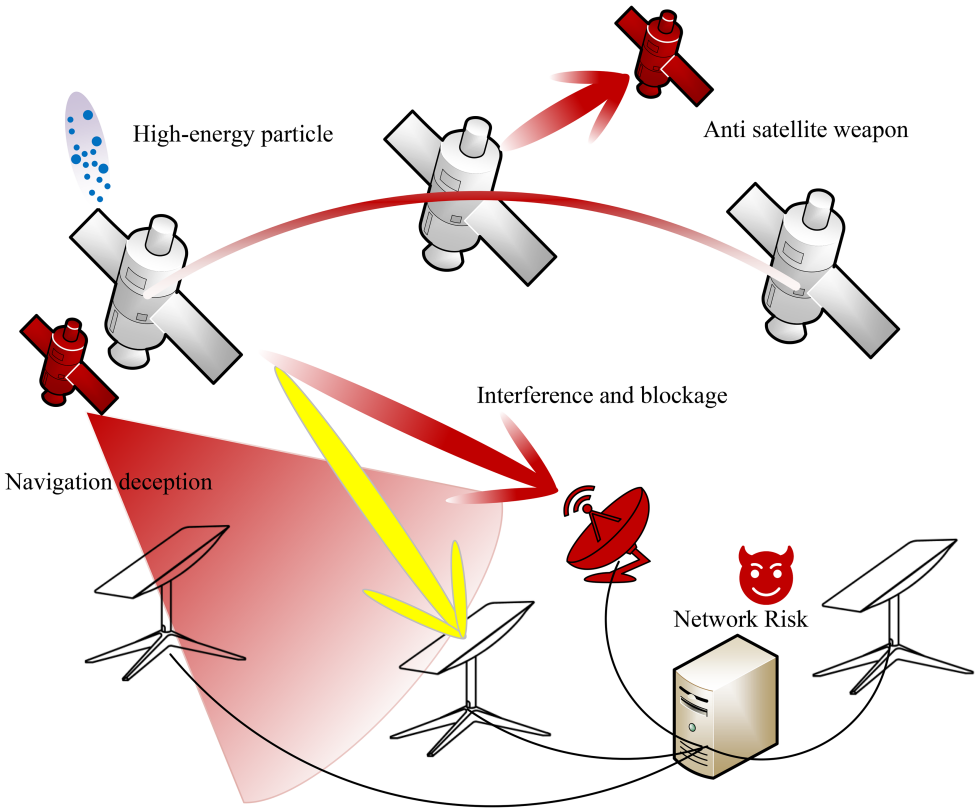


图 9　(网络版彩图) 关键设施脆弱性风险.

Figure 9　(Color online) Vulnerability risk of critical facilities.

服务中断、在线教育停摆与企业交易中断, 并对军用通信造成严重威胁. 此外, 美国太空军构建的 “梅兰多兹” 反卫星系统, 通过灵活的软硬件配置实现对不同卫星的精准干扰与电磁频谱的监控记录, 并结合上行阻塞式干扰阻断传输链路.

如图 9 所示, 关键设施的脆弱性可概括为多维攻防耦合与 “单点 – 双重” 风险.

(1) 物理/轨道层: 易受反卫星装置 (ASAT) 动能/软杀伤、太空碎片与空间天气影响, 星间链路对指向与热控极度敏感.

(2) 电磁频谱层: 星地/星间链路可被压制式干扰、欺骗式导航/测时扰动和波束侧瓣利用所破坏, 窄带 – 宽带相结合的机动式干扰可引发大范围服务退化 [91].

(3) 网络与控制面: 网关与地面控制中心的集中组件 (路由、编排、切片与密钥管理) 一旦被渗透或失配, 可能触发跨域策略失效、证书撤销滞后与路由劫持并引发连锁中断 [92].

(4) 软件与供应链: 星上载荷与地面系统的在轨升级、远程配置与第三方依赖扩大了后门与供应链攻击面.

(5) 地面侧与法律合规: 少量关键地面站、回传骨干与电力设施成为易打击目标, 跨国合规与数据主权限制也构成潜在风险.

综上所述, 在高时变拓扑与万级节点规模下, 上述脆弱性可能相互放大, 使局部干扰演化为跨域级联故障, 并直接威胁其体系的连续性与可信性.

3.5.2　频谱资源争夺风险

在国家级网络与电磁空间对抗风险不断升级的背景下, 卫星互联网频谱竞争已由传统 ITU 框架下的部门间协调, 扩展为贯穿政策、工程与对抗的多层面博弈. 在政策方面, 围绕轨道/频率的先占式申报、地面站落地许可, 逐步形成了 “准入 – 合规 – 执法” 的联动链条; 地面 5G 网络与多制式雷达部署也加剧了频谱拥塞, 需要多波束

https://www.sciengine.com/doi/10.1360/SSI-2025-0463

与动态频谱等方案提升复用效率. 在对抗环境中, 跨境定向压制、机动式骚扰与针对测时/测距链路的欺骗性扰动较为常见; 更隐蔽的方式是渗透网络并改写功率、波束、信道等参数, 在几乎无痕的情况下造成最大化的频谱干扰. 因此, 频谱安全已从单点抗干扰转向 “感知 – 决策 – 执行” 的闭环对抗. 针对该风险, 可通过以下方式来实现频谱安全: (1) 构建在轨与地面联合的射频态势感知, 持续更新认知频谱图谱, 实现毫秒级避让与窄带抑制; (2) 采用多域冗余、扩频与跳频等机制, 在强压制场景下保持链路生存性与业务连续性; (3) 在合规框架内, 将快速发现、动态规避、合法护航与弹性调度固化为运行常态.

3.5.3　地面关口集中风险

地面关口集中化部署可缩短建设与运维链路, 便于统一频谱合规与许可流程, 但在对抗环境下这种集中化部署易暴露为关键脆弱点: 各类地面站既是电磁压制与物理打击的关键目标, 也可能成为网络渗透的主要入口; 一旦关键节点失效, 可能触发服务面大幅退化甚至出现系统级中断. 因此, 卫星互联网架构需由 “集中 – 稳定 – 高效” 向 “分布式 – 冗余 – 可迁移” 转型: 部署上以多地点、小单元网关群替代集中式部署; 技术上引入可编排的网关资源池, 支持按负载、威胁与合规边界动态切换与再部署; 运维上以 “可观测 – 可编排 – 可回退” 的运维闭环固化变更路径, 将网关由单点转化为可替换、可迁移且留痕可证的分布式部署, 以在非合作对抗条件下保持生存性与服务连续性.

3.6　运维与人为因素威胁

星座规模化增长使维护与升级高度依赖专业运维人员与第三方协作, 在运维水平差异与人为因素主导的背景下, 卫星互联网呈现组织流程与技术机制耦合的系统性风险: 日常运维与运维轮班中身份与权限管理易失控, 系统配置与升级保障不足易触发系统性风险, 第三方承包商与外包也成为影响卫星互联网安全链条的关键薄弱环节.

3.6.1　内部人员泄密与社会工程学攻击

运维模式的高权限、自动化与第三方参与等特征, 提高了卫星地面站、载荷与密钥管理等关键资产与环节的暴露风险. 实践中, 基于零信任架构的最小权限与凭据生命周期管理常执行不到位, 共享账号与权限叠加仍然存在, 易导致越权访问与敏感数据泄露. 同时, 攻击者可在变更窗口或应急响应期间通过钓鱼邮件、伪装工单与恶意附件对内部人员实施信息欺骗以窃取口令与登录凭证. 为降低卫星互联网的潜在泄露风险, 可围绕身份、凭据、变更与分区 4 个环节重构运维基线: (1) 建立统一时间基线与不可篡改日志; (2) 对运维人员实施常态化反钓鱼演练与口令保密教育; (3) 对承包商坚持最小知情与数据脱敏原则; (4) 落实物理分区与设备网络微隔离措施. 综上所述, 通过可观测、可编排、可验证的可信运维闭环, 在不额外抬高日常操作风险的前提下, 显著降低内部泄露与社会工程学攻击导致的连锁后果.

3.6.2　误配置导致的安全事故

软件定义卫星、云端管控与智能化运维使对不同设备和软件系统的在线配置、升级、运维常态化. 因此, 对不同设备的误配置是卫星互联网中最常见的安全风险来源. 任一设备的误配置都可能使控制面、服务面与密钥体系的耦合配置风险快速扩散. 例如, 地面站或星地网关路由策略错误可能导致多轨道卫星构建的核心服务区失效; 星间/星地链路物理层关键参数误配置会导致信息传输链路质量波动与拥塞扩散; 密钥管理、证书撤销与基线参数漂移可触发跨域鉴权批量失效与会话掉线, 甚至被预警系统误判为攻击事件. LEO 过顶时间短也压缩了卫星在轨升级的有效窗口, 使微小参数配置差错更快传播且取证/纠偏成本更高. 因此, 面向卫星互联网的误配置预防是卫星互联网安全的核心问题之一, 需对卫星互联网设备配置策略开展充分评估, 并可借助卫星互联网数字孪生平台对关键配置进行预演, 验证路由收敛与传输容量/时延边界等.

3.6.3　第三方承包商与外包风险

第三方承包商与外包介入地面站运维、载荷升级、云端编排与密钥管理等高度敏感环节, 易导致权限外溢

https://www.sciengine.com/doi/10.1360/SSI-2025-0463

与凭据滥用, 并可能为恶意数据与软件病毒植入提供通道. 相关风险具有跨域可扩散、证据易缺失与回退成本高等共同特征, 易引发系统级联失效. 因此, 可通过最小权限抑制权限扩张, 以技术可验证机制保障取证链路, 并将零信任与最小权限等原则固化为外包准入与持续审计的硬约束, 将第三方风险压缩至可审计、可问责、可复原的范围内.

4　卫星互联网安全防护技术

针对卫星互联网面临的多重安全威胁态势, 需从多个维度构建全方位安全防御体系 [93]. 本节重点介绍通信加密与抗干扰、身份认证与访问控制、卫星态势感知与安全监测、AI 安全应用、量子安全密码以及 APT 对抗等核心防护技术.

4.1　通信加密与抗干扰技术

在卫星互联网安全体系中, 通信加密与抗干扰分别从信息逻辑层的机密性与物理信道的可用性两个维度, 构成防御外部信号攻击与威胁的关键防线 [94].

通信加密旨在降低卫星链路开放性带来的窃听、篡改与伪造风险. 受星上计算资源受限与链路高时延约束, 传统地面网络加密协议难以直接适配; 实际的卫星互联网体系中, 通常采用分层混合加密策略, 在计算开销与安全性之间折中. 通信系统中常结合对称与非对称加密技术以保障信息的机密性、完整性与身份认证 [95]. 对称加密 (如 AES, SM4 等) 依赖共享密钥实现高速加密, 适用于星上与地面网关间的大规模数据转发与实时通信场景; 非对称加密 (如 RSA, ECC 等) 主要用于初始链路握手阶段的身份认证、数字签名验证以及会话密钥的生成与分发, 防止未授权的终端或地面站加入网络 [96]. 实际系统通常先用非对称加密算法建立安全信道, 再切换至对称密码进行批量加密, 以兼顾计算效率与安全强度.

抗干扰技术旨在对抗复杂电磁环境下的恶意压制与欺骗, 通过物理层与信号处理手段提升系统鲁棒性 [97]. 典型方法包括扩频/跳频、多天线系统实现空间分集与自适应波束赋形. 直接序列扩频通过伪随机码扩展信号带宽以降低功率谱密度, 提升抗干扰能力; 跳频在伪随机序列控制下快速变更载波频率以规避定频干扰与窄带瞄准式干扰 [98]; 波束赋形结合多输入多输出技术与相控阵天线, 在干扰来波方向形成 “零陷” 并增强期望信号增益, 实现空间域上的物理隔离 [99]. 抗干扰技术能有效抑制恶意干扰与阻塞攻击, 显著提高通信系统的抗衰落与抗干扰性能, 增强信号在复杂电磁环境下的稳定性与抗干扰能力, 保障链路的通信可靠性 [100].

综上所述, 通信加密与抗干扰技术相互补充, 共同支撑卫星通信在复杂电磁环境下的安全与可靠运行.

4.2　身份认证与访问控制机制

在卫星互联网中, 身份认证与访问控制是防止网络资源被非法接入和滥用的基础. 受空口链路高度开放、终端能力差异与接入网多元异构等特征的影响, 需在保障安全的同时实现快速认证与动态授权.

已有研究提出多种卫星互联网身份认证机制. CCSDS 制定的 SCPS-SP 协议提供了身份认证、机密性检查与完整性保护等措施 [59], 但其密钥管理以隐式身份验证为主且可扩展性不足, 难以适配大规模星座. 3GPP NTN 直接沿用地面蜂窝网络认证标准 [49,50], 但在高时延与间歇连通条件下易出现超时失败并放大重放攻击等安全风险. 在此基础上, 除采用传统的公钥基础设施 (public key infrastructure, PKI) 体系 [101]、认证、授权与记账 (authentication, authorization, and accounting, AAA) 框架以及改进地面网广泛使用的 EAP/AKA [49,50] 等机制外, 可进一步引入基于零信任理念 [102] 的连续认证与风险自适应机制, 依据终端设备属性、位置信息、行为特征与风险等级动态调整认证强度与密钥生命周期. 面向差异化终端, 可建立能力标识与分级接入认证机制. 例如, 对低能力设备采用轻量化认证方案 [103,104]. 同时可采用经典与抗量子混合密码机制, 在兼容存量设备的同时提升整体抗量子安全性 [105,106], 支撑复杂异构环境下的统一身份、动态信任与高效安全接入. 此外, 为支撑高可靠认证机制, 需确保终端自身的安全可信. 为降低终端侧密钥泄露、设备克隆与固件篡改等风险, 可在终端侧部署硬件可信根 (如 TPM/eSIM/TEE) 并结合安全启动将密钥与启动状态绑定, 防止密钥被非法导出; 同时利用远

https://www.sciengine.com/doi/10.1360/SSI-2025-0463

程度量与远程证明校验固件及配置, 将终端可信状态作为接入网络的前置条件以防范冒用接入.

卫星互联网拓扑动态变化、场景复杂异构与节点移动性增强, 使静态访问控制规则难以适配. 可构建以属性为核心的动态自适应访问控制机制 [107], 结合用户角色、设备安全状态、实时位置与业务关键性等多维属性, 由策略控制点进行按需授权. 同时遵循零信任的最小权限原则, 实施细粒度会话级访问控制并引入持续评估与撤销授权机制, 随上下文属性与风险态势变化等动态调整访问权限, 必要时降权或终止会话 [102]. 对高安全等级星上操作可引入多级审批等机制, 形成在开放网络环境下闭环的、自适应的安全访问体系 [108].

4.3　卫星态势感知与安全监测技术

卫星态势感知通过目标探测、识别、跟踪、态势分析与预警决策等环节, 赋予卫星互联网对复杂太空环境的洞察与预判能力, 是保障其安全、智能、高效运行的重要技术支撑 [109,110]. 目标探测面向近地轨道、中地轨道、地球同步轨道及深空区域的失效/故障卫星与空间碎片等, 常用手段包括光学望远镜、雷达、射电望远镜与信号测量. 随高分辨率遥感技术发展, 探测精度与覆盖能力显著提升, 有助于精确地发现低轨道卫星和微小碎片并提高对空间物体的探测效率和准确度. 目标识别从类型、用途、状态 3 个维度对探测到的目标进行判断分析, 如确定目标类型为已知卫星、空间碎片、未知目标或者其他类型, 目标用途为通信卫星、侦察卫星、导航卫星或者其他, 以及目标状态为正常运行或者失控漂移等. 在探测与识别目标的基础上, 目标跟踪用于精算目标轨道参数并同构持续追踪目标的运动状态来预测目标未来位置; 现有轨道跟踪系统除依赖传统的地面雷达外, 也可结合星载传感器与卫星协同观测提升跟踪精度, 为空间任务规划提供决策支持.

态势分析面向目标分布与目标动态, 识别目标的碰撞风险、异常机动与敌对行为并评估目标对在轨资产的威胁; 同时, 可利用大数据分析技术和云计算平台, 对大量卫星和空间碎片数据进行实时处理, 使得风险评估更加动态、精准; 更进一步, 可监测宇宙环境变化、太阳活动等空间天气因素对卫星运行稳定性的影响. 在此基础上, 预警决策生成潜在碰撞预警、干扰/攻击风险预警、空间环境风险预警等, 并支持机动避碰、频率调度与链路切换等处置决策 [111]. 此类预警系统不仅关注即将发生的事故, 还能在潜在威胁出现之前进行预防性干预, 降低灾难性事件的发生概率.

基于卫星态势感知可构建安全监测机制, 对空间物理安全与网络空间安全进行实时监测: 一方面监测卫星硬件设备状态与星地/星间通信链路, 确保在轨稳定与数据传输可靠; 另一方面构建网络空间威胁表征、监测、传播路径刻画与威胁反制能力, 以在威胁出现前实现预判并提前采取处置措施.

4.4　基于 AI 的卫星异常检测与入侵防御技术

卫星互联网具有链路时延高、星座拓扑高动态、星间/星地链路异构、终端规模大且分布广泛等特征, 面临多类入侵攻击 (如 Coremelt [112], Crossfire [113] 与 ICARUS [114] 等). 随着卫星网络流量动态性与不确定性显著增强, 针对卫星互联网的入侵检测正由传统的规则/特征匹配型逐步演进为基于 AI 模型的智能检测. 基于 AI 的异常检测通常以多层特征 (如物理层 IQ 信号、RFF 指纹、MAC/网络流量、主机与应用日志、星座拓扑状态、时空业务画像等) 为输入, 利用数据驱动与先验约束相结合的模型学习正常态分布并刻画攻击态偏离, 将置信度与不确定性量化映射为联动处置策略与最终的风险置信度. 相关方法可基于深度学习 [115]、时序建模 [116] 与图神经网络等算法对通信流量、系统日志、遥测信号等多源异构数据进行高维特征提取与行为建模, 以识别异常通信模式、恶意指令注入与节点失陷等潜在攻击行为.

受星上算力、数据不均衡与对抗攻击等约束, 可采用 “星上部署轻量级模型用于实时监测、地面控制中心部署模型重训练与全局威胁分析” 的分层模式, 并通过联邦学习实现跨域知识共享. 在攻击强上下文依赖与跨时空关联场景下, 传统检测方法难以有效建模, 学术界逐渐探索基于大模型的攻击检测框架. 例如, 面向卫星互联网攻击检测的预训练大模型 PLLM-CS 通过 Transformer 自注意力机制强化上下文特征建模能力提升了检测性能 [117].

AI 引入在提升异常检测能力的同时也带来模型篡改、推理结果操纵等新的安全问题. 针对 AI 模型篡改攻击, 可依托硬件信任根实施安全启动, 对固件、推理框架与模型进行哈希度量与签名验真; 结合模型签名校验与

https://www.sciengine.com/doi/10.1360/SSI-2025-0463

哈希绑定策略并在可信执行环境中运行以降低模型运行时的注入与内存篡改风险. 针对 AI 模型执行结果被操纵风险, 可对输出结果进行签名并实施端到端加密, 防止在传输链路中被篡改.

在星地链路带宽与时延约束下, 安全防护能力往往以可插拔式部署且难以将全量任务与日志数据进行回传集中处理; 同时, 攻击面已由传统的链路攻击扩展至星上操作系统与协议栈等多个层面. 因此, 需在星上引入轻量化入侵检测能力实现风险在轨检测与干预, 并在多卫星协同应用场景下通过多维协同分析构建时空关联模型, 支撑全局态势感知与多层级联动防御策略生成. 在此基础上, 可结合轻量级入侵检测探针与区块链技术增强轨道态势感知的可信共享与追踪能力, 实现全局安全检测与处理策略时间线的不可抵赖、传播链可追溯及处置过程可审计, 显著提升星座态势共享与安全事件处置策略的可信度. 综上所述, 通过上述措施, 可显著提升卫星互联网在面对复杂网络攻击与异常行为时的智能检测能力与主动防御水平.

4.5　量子安全密码技术

随着量子计算技术的不断突破, 现用密码技术体制逐渐面临被破解的风险. 具体来讲, 量子计算削弱了传统对称密码的安全性, 并对现有非对称密码带来更严重威胁. 对量子与经典计算均安全的密码技术称为量子安全密码技术. 对称密码一般可通过增加密钥长度或杂凑值长度来提高安全性. 而非对称密码则需重塑密码体系.

当前主要有两条技术路线. (1) 量子密码: 基于量子力学原理, 可自然应对量子计算带来的安全威胁; 典型代表为 BB84 协议, 属于量子密钥分配 (QKD) 协议, 可用于卫星通信中实现密钥分发 [118]. (2) 抗量子密码/后量子密码 (PQC): 延续计算上可证明安全的传统方法, 其抵抗量子攻击的复杂度假设是保障抗量子密码安全的基础. 目前被普遍认可的基于数学的抗量子非对称密码主要包括下列 5 类: 基于格、基于编码、基于 Hash 或分组密码、基于多变量与基于同源 [119]. 当然, 也存在量子密码与抗量子密码结合的混合方案 [120].

美国、欧盟等国家和组织都从顶层进行设计和部署, 并积极推进抗量子密码迁移政策法规和指导性文件的制定. 美国国家标准与技术研究院 (National Institute of Standards and Technology, NIST) 于 2016 年底公开面向全球征集抗量子非对称密码算法, 并于 2024 年 8 月正式发布了 3 个抗量子非对称密码算法标准. 我国也在积极推进抗量子的密码算法标准的制定, 于 2025 年 2 月 5 日商用密码标准研究院发布开展新一代商用密码算法征集活动的公告 [121].

综上所述, 量子安全密码技术将成为未来网络安全体系的基石, 也将成为解决卫星互联网安全问题的重要技术手段.

4.6　APT 对抗技术

APT 攻击更易借助星地链路 “跳板” 实现长期潜伏与跨域渗透, 一旦控制星座关键节点即可对用户实施数据劫持. 因此, 构建面向卫星基础设施的 APT 对抗体系是卫星防御的核心环节之一. 尽管卫星高速运动、波束间断连接与资源受限使天地数据在时空上高度离散, 但基于溯源图的 APT 攻击检测方法 [122~124] 仍可通过缓解数据缺失对攻击链重建的影响来提升检测效果. 该方法通过汇聚地面控制中心、网络管理系统及各类用户终端中的细粒度审计日志 (如系统调用流、进程创建、文件读写、注册表修改与网络连接等), 构建覆盖 “地面 – 轨道 – 用户” 全链路的跨主机、跨时段因果依赖图谱, 以精确刻画从初始入侵 (如通过固件更新通道植入恶意代码)、权限提升、横向移动 (利用星地接口漏洞跳跃) 到经低轨中继节点外泄的数据回传等链条, 从而增强对隐蔽性强、周期长的 APT 攻击行为的发现能力与溯源精度.

此外, 基于大模型的 APT 溯源也逐渐成为新的检测范式 [125,126]. 其利用大模型强大的模式识别与语义关联能力, 将系统审计日志与威胁情报等异构信息转化为高层次威胁上下文, 并融合终端日志与星上遥测数据重构攻击时序逻辑; 基于重构结果可产出结构化告警并生成自然语言溯源报告, 以提升卫星互联网在面对 APT 攻击时的智能溯源与追踪能力.

https://www.sciengine.com/doi/10.1360/SSI-2025-0463

4.7　供应链安全

在卫星互联网中, 软硬件供应链安全是防止非法入侵与长期控制的关键基础. 然而, 由于卫星互联网系统软硬件高度依赖多厂商、跨地域协同开发与集成, 供应链安全防护面临较高复杂性与实施难度.

按照供应链所涉及的对象可分为软件供应链安全与硬件供应链安全. 软件供应链安全侧重代码、第三方依赖与开发流程完整性, 通过贯穿可信开发、代码加固、运行与分发的全流程治理, 防范恶意代码注入与隐蔽风险 [127]. 在可信开发阶段, 可结合数字签名与可信证书验证开发主体、关键信息完整性及第三方组件; 在代码层面, 通过安全加固设计与基于大模型的自动化漏洞检测降低潜在缺陷风险 [128]; 在运行与分发阶段, 依托可信执行环境保障软件加载、运行与升级的可验证性. 同时, 可构建基于区块链的软件供应链治理框架, 对开发主体、代码版本演化及第三方依赖关系进行链上存证, 实现软件开发与分发过程的可审计与可追溯, 降低恶意代码注入与供应链投毒风险 [129].

硬件供应链安全侧重芯片、固件与关键元器件的真实性与完整性, 通过固件签名、安全启动与回滚保护等机制建立硬件可信根以防止恶意篡改与后门植入; 结合区块链可实现硬件生产、交付与集成全过程的可追溯与可审计, 支持缺陷组件的快速定位与风险预警 [130].

综上所述, 融合区块链、可信执行环境与自动化漏洞检测等技术, 可提升供应链全生命周期追踪溯源能力与可审计性, 为卫星互联网长期可信运行与高可靠服务提供坚实支撑.

5　卫星互联网相关政策与法律框架

随着卫星互联网商业化应用场景的不断拓展, 其面临的网络安全威胁也日益加剧. 其覆盖范围广、技术架构复杂、应用场景多元, 一旦遭受网络攻击, 可能导致大范围服务中断、关键数据泄露甚至系统性失控, 影响范围远超传统地面网络. 为应对该挑战, 各国正加快制定政策法规, 推动安全标准与风险评估体系建设, 并探索数据主权归属与跨境传输安全等关键问题, 以提升空天信息系统的安全治理能力.

5.1　国际空间法与卫星互联网安全监管空白

卫星互联网兴起带来卫星网络安全与数据跨境流动等新型法律问题, 但早期国际法规 (如《外层空间条约》(Outer Space Treaty) [131]、《国际电信联盟组织法》(ITU Yearbook of Statistics) [132] 等) 难以形成强制性约束, 导致全球治理制度存在空白. 为健全卫星互联网法律监管体系, 各国都加快了立法速度与政策布局. 美国于 2020 年发布了《第五号太空政策指令》(Space Policy Directive-5) [133], 要求将网络安全纳入太空网络开发全生命周期; 2022 年发布的《卫星网络安全法》(Satellite Cybersecurity Act) [134], 要求面向美国卫星运营商提出网络安全建议并开放相关资源. 2023 年《国家近地轨道研究与发展战略》(National Low Earth Orbit Research and Development Strategy) [135] 提出组建低地球轨道国家实验室等举措以推进太空网络安全前沿研究.

与此同时, 我国也相继出台了一系列法律法规. 2017 年颁布的《中华人民共和国网络安全法》[136] 明确关键信息基础设施运行安全并强调要保护关键信息基础设施免受攻击、侵入、干扰和破坏. 2020 年, 我国将卫星互联网纳入 “新基建” 信息基础设施. 2023 年, 工业和信息化部发布的《关于电信设备进网许可制度若干改革举措的通告》[137] 中明确将卫星互联网设备纳入现行进网许可管理. 2025 年 4 月, 国家互联网信息办公室印发了《终端设备直连卫星服务管理规定》[138], 细化了对终端设备直连卫星服务的发展与促进、设备设施与服务管理、监督管理与法律责任等要求. 同年 8 月, 工业和信息化部发布了《工业和信息化部关于优化业务准入促进卫星通信产业发展的指导意见》[139], 提出要加强卫星通信监管并筑牢网络和数据安全防线.

总体而言, 主要航天国家已初步形成本国安全领域的基本法律体系, 但多为原则性与禁止性规定, 针对卫星互联网信息安全管理的专项法规仍不足, 亟需将安全管理需求与现行法规对标并细化落地路径.

https://www.sciengine.com/doi/10.1360/SSI-2025-0463

5.2　各国的安全标准与监管措施

面对卫星互联网快速发展, 主要国家正加速构建国内监管框架. 美国 NIST 针对商用卫星系统空间段、地面段、用户段及混合卫星网络等关键组成部分, 相继发布 4 项卫星网络安全风险管理框架, 用于帮助商用运营商识别太空系统的网络安全风险 [140]. 此外, 2023 年 5 月美国国务院在《太空外交战略框架》(A Strategic Framework for Space Diplomacy) [141] 中明确提出要持续强化以卫星互联网为代表的太空网络安全与信息通信技术能力, 提升关键基础设施的安全性与韧性. 我国于 2025 年发布的国家标准《空间数据与信息传输系统网络安全总体技术要求》[142], 系统性规定了空间网络安全总体需求、体系架构以及物理安全、控制安全和转发安全等方面的技术要求, 为我国空间网络建设与防护提供技术依据.

总体来看, 美国以 NIST 框架为核心强调基于风险识别与响应的动态管理, 体现 “过程导向” 的治理思路; 我国标准更侧重技术指标的统一性与可执行性, 体现 “顶层设计先行、技术规范托底” 的发展路径. 两种模式各有侧重, 反映了不同治理思路下的安全路径选择, 为未来国际规则协同提供对话基础.

5.3　数据主权与跨境安全问题

低轨星座等新型空间基础设施正在重塑全球信息传输格局. 其跨越国境、去中心化等特征推动空间 – 地面数据高速流动, 冲击传统以地理边界为基础的数据治理模式, 数据主权问题随之凸显. 然而, 现有国际法与国内法规对卫星互联网所引发的新型数据流动模式响应相对滞后, 亟需形成更契合太空网络特性的治理体系.

卫星互联网运行中, 数据主权与跨境安全面临双重挑战: 一方面, 数据主权边界模糊不清, 例如, 外国遥感卫星高分辨率成像、导航系统持续采集位置信息、通信数据经境外网关站落地处理等行为是否构成对我国数据主权的侵犯, 现行法律缺乏明确界定. 《中华人民共和国数据安全法》[143] 与《中华人民共和国网络安全法》[136] 主要面向地面网络设施, 难以有效覆盖空间段数据活动及由境外主体控制的数据处理行为. 另一方面, 数据跨境传输风险显著上升, 用户通过境外卫星终端 (如 Starlink) 接入互联网, 可能使敏感数据绕开地面网络监管直接传输至境外数据中心, 形成 “终端在内、数据在外” 的监管盲区. 尽管《中华人民共和国个人信息保护法》[144] 确立了 “属地 + 影响” 双重管辖原则并具备一定的域外适用效力, 但在执法实践中仍受制于卫星信号监测困难、境外运营商配合不足、星间链路端到端加密及密钥境外掌控等因素, 导致法律虽立而难以落地执行. 综上所述, 传统基于地理边界的监管体系难以有效应对跨域、动态、加密的太空数据流, 亟需构建兼顾国家安全、数据主权与技术创新的新型治理机制.

6　未来趋势与思考

本节将分析商业卫星网络开放性与安全困境, 探讨 AI 与自动化在卫星运维安全中的应用前景, 提出卫星地面数字孪生系统与卫星攻防演练靶场的建设要点, 并讨论未来可能出现的 “网络安全军备竞赛” 以及多国合作与安全联盟的可行路径.

6.1　商业卫星网络的开放性与安全困境

卫星互联网发展正在由政府主导逐步转向商业企业主导. 国外商业卫星互联网项目 (如美国的 Starlink、英国的 OneWeb 等) 与我国的千帆星座、吉利未来出行星座等共同推动了低轨卫星通信体系的规模化部署. 商业化的迅速推进降低了进入空间通信领域的技术与经济门槛, 加速了卫星网络与地面互联网的深度融合, 但也带来新的安全挑战: 多主体建设运营导致治理理念与安全策略不一致; 在成本、上市周期以及市场竞争压力下, 部分企业可能弱化早期安全研发投入, 致使认证、防篡改、链路隔离等基础防护环节存在薄弱点; 同时, 地面网关、用户终端与数据中心分布于不同的国家和地区, 各个国家的法规差异导致卫星互联网运行将同时受到不同国家的监管体系约束, 进一步增加了安全合规的复杂性. 因此, 如何在开放创新与统一安全标准、网络治理体系之间取得平衡, 将成为商业卫星互联网持续发展的关键问题.

https://www.sciengine.com/doi/10.1360/SSI-2025-0463

6.2　AI 与自动化在卫星运维安全中的前景

随着星座规模的持续增长与网络环境的高度动态, 依赖人工与静态规则的传统安全运维模式难以适配. AI 与自动化技术可在实时监控遥测、链路状态与通信流量的同时, 自动识别异常与潜在威胁, 并触发针对性处置. 例如, AI 模型可在链路层发现信号干扰、欺骗或链路异常, 结合自动化编排实现受攻击节点的主动隔离, 从而提升卫星网络自适应防御的检测与响应速度. 与此同时, 智能化防护也引入新的安全风险, 如数据投毒、模型篡改、对抗样本, 以及误报和可信度问题. 因此, 在利用 AI 与自动化技术提升防御效率的同时, 建立可验证、可控的模型安全与运行保障机制是未来演进的重要方向.

6.3　卫星地面数字孪生系统构建与应用

卫星地面数字孪生系统通过在地面实时模拟在轨卫星状态和环境, 为控制中心提供更精细的监测、管理与操作支撑, 并可作为安全可控的测试平台, 用于发现并修复卫星在轨系统中可能存在的漏洞和问题. 其核心价值在于: 在不影响实际业务运行的前提下, 开展长期、连续的安全测试, 通过模拟各种网络攻击、数据窃取与系统故障识别潜在缺陷, 形成针对性的安全补救措施. 卫星互联网数字孪生是未来发展的必然趋势, 但在数据同步精度、模型实时性与系统异构集成等方面仍存在关键挑战, 亟待进一步突破.

6.4　卫星攻防演练靶场建设路径

卫星互联网链路复杂、攻击隐蔽, 需构建专用卫星攻防演练靶场以验证卫星网络在高动态、大规模场景下的防护能力, 并进一步提升网络韧性. 卫星攻防演练靶场的建设可采用 “地面先行、在轨验证” 的渐进路径: 先建立模块化、可扩展的地面仿真与试验平台, 集成地面站、网关、用户终端及代表性卫星子系统, 形成测试方案与评价指标; 再设计小规模在轨试验单元, 验证防御器件的有效性; 最终实现地面与在轨协同联调能力. 系统化靶场建设既能够支撑实战化安全设计与攻防测试, 也有助于人才培养与工程化能力沉淀.

6.5　未来卫星互联网的 “网络安全军备竞赛”

各国在推动大规模星座部署的同时, 正加速构建空间网络攻防体系, 形成以安全为导向的研发与投入趋势, 拉开了未来卫星互联网 “网络安全军备竞赛” 的帷幕. 相较于电磁干扰与信号欺骗等传统的对抗方式, 未来空间对抗将更具多维化与智能化特征: 在 AI 与自动化技术的推动下, 网络渗透、链路劫持、控制信号篡改与数据截获等手段可能更具持续性、隐蔽性与破坏性; 量子通信、在轨数据处理等新兴技术也将重塑现有攻防体系, 推动安全防护从单个卫星节点防御转向整个网络系统级对抗. 在此趋势下, AI 与自动化运维、仿真验证与攻防靶场将成为提升体系韧性与风险应对能力的重要抓手. 但若持续存在技术壁垒、数据不互信与安全标准差异, 卫星互联网的开放性发展可能受限. 未来国际社会需要在开放与安全之间寻求平衡, 通过制定可验证的国际规则、提升安全透明度与信任建设, 避免良性竞争演变为新的对抗焦点.

6.6　多国合作与安全联盟的可能性

卫星互联网的全球覆盖属性决定了安全威胁具有跨国性, 任何单一国家难以独立应对全球级风险. 随着各国商业星座密集入轨, 未来可能形成面向卫星通信与网络防护的多国协作框架: 通过共享威胁或攻击情报、制定通用安全标准、联合攻防测试、入侵检测与应急响应等方式, 实现跨国卫星网络的安全共治. 现有国际电信联盟的频谱协调体系与联合国倡导的外空行为准则为这种合作提供了初步制度基础. 但受技术不共享、数据不公开、防务用途与商业竞争等因素影响, 合作推进仍较有限. 未来可从 3 方面积极推动全球卫星互联网安全协作 [145]: 一是加强沟通并主动参与或牵头建立卫星互联网安全协作机制, 推动威胁情报与应急响应信息共享; 二是参与空间网络安全标准制定, 推动安全技术与规范国际化; 三是鼓励科研机构与企业跨国联合研发, 构建开放可信的安全技术生态. 通过制度化的多国安全联盟与协同创新理念, 将推动防护体系由单点防御迈向全球共治, 为开放、安全与可持续服务铺平道路.

https://www.sciengine.com/doi/10.1360/SSI-2025-0463

6.7　智能安全卫星系统展望

面向安全威胁的多样化与持久化, 防御需求正从传统被动防护转向内生化、智能化与协同化. 智能安全卫星系统 [146~149] 通过融合人工智能等新兴技术, 将安全能力深度嵌入卫星系统运行全过程, 旨在形成全域感知、智能决策与自主协同的安全防护体系. 系统可通过 AI 驱动的自动编排、自修复与在轨自适应防御等机制, 结合联邦学习、强化学习与大模型等实现多域协同的智能决策; 面向大规模星座运行场景, 可通过智能路由重构、星间链路动态重配置与任务智能迁移提升服务连续性与鲁棒性; 并依托在线学习与数字孪生技术实现对干扰、欺骗等复杂攻击行为的持续建模与防御策略的动态调整.

但在实际部署中仍面临挑战: 多轨道、多协议、多业务叠加导致特征空间高度异构, 统一检测与态势评估模型构建困难; 星上算力、带宽与功耗受限以及星地链路高时延、易中断, 制约实时监测与快速响应能力; 端到端加密和隐私保护降低了业务内容的可观测性, 只能依赖更多元数据和行为特征; 真实攻击数据与基准样本匮乏, 以及在轨环境引发的概念漂移与对抗样本威胁, 严重制约模型的有效性与鲁棒性.

综上所述, 智能安全卫星系统已成为卫星互联网内生安全的重要支撑. 未来仍将进一步沿内生化、智能化与协同化方向持续演进.

7　结语

7.1　卫星互联网安全的重要性总结

卫星互联网正迅速成为未来全球信息基础设施的关键组成部分, 其意义已从通信服务延伸至支撑社会经济运行、民生福祉与国家安全等多重领域. 卫星互联网安全不仅关系单一星座系统的稳定可靠运行, 也将影响国家乃至全球网络空间安全格局. 相较于传统地面网络, 卫星互联网呈现更强的复杂性与开放性; 星地链路、终端跨域互联及空天地多层网络的紧密耦合, 使其在面对复杂隐蔽威胁或攻击时暴露出更高脆弱性. 威胁态势与典型案例表明, 风险已从电磁干扰、链路欺骗扩展到网络入侵、供应链攻击甚至国家级网络战, 卫星互联网安全风险已不再局限于技术层面, 而成为科技与战略、政策与法律等因素交织的综合性挑战.

作为天地一体化通信体系的核心, 卫星互联网与地面互联网、物联网及移动通信协同运行, 一旦任一关键链路或节点遭受恶意攻击或破坏, 可能引发跨网络连锁反应, 进而影响整个空天地一体化网络的整体运行, 甚至威胁到国家经济运行与社会安全. 在全球化、政治化和竞争化背景下, 单一国家封闭式管理与防护的模式难以奏效, 构建安全、可信、可持续的卫星互联网生态已成为全球卫星互联网发展中需要共同面对的重大命题. 为实现这一目标, 既需要在技术层面持续突破 (如强化加密与抗干扰、推进 AI 与自适应防御监测、构建卫星地面数字孪生系统与攻防演练靶场等), 也需在安全治理与运维层面推动安全标准化、协同化与国际互信机制建立.

安全应成为卫星互联网系统设计与运行的前置条件; 未来竞争不仅取决于其通信覆盖的广度, 更取决于安全防护纵深与治理体系的成熟程度, 谁能率先在卫星互联网安全体系中取得突破, 谁就将在未来的空间信息竞争中占据主动.

7.2　对科研、产业、政策制定者的建议

面向日益复杂且破坏性巨大的新兴威胁, 未来研究应聚焦构建系统化的卫星互联网安全防护技术体系: 针对星地通信高时延、卫星资源受限等特性, 设计新型接入认证、威胁检测、应急处置方案, 探索基于零信任架构的边界防护技术, 并攻克 AI 与自动化安全运维、卫星数字孪生、地面攻防演练等关键技术 [150]. 科研机构可重点推进卫星网络安全架构、人工智能自动化防护、量子安全密码与在轨可信计算等基础研究, 形成可验证、可迁移且具备演化与落地能力的安全理论体系.

产业侧需在星座设计、地面系统维护与供应链管理等环节落实 “安全为先” 的理念, 集成安全防护技术并完善安全评估标准, 通过测试入侵检测、攻击识别与应急响应能力评估各环节的安全性能, 持续加固卫星互联网安全防护的薄弱环节. 政策制定者应加快安全标准制定与推广, 推动跨国监管与共同设计、共同研发与共同治理

https://www.sciengine.com/doi/10.1360/SSI-2025-0463

框架建设, 构建具备韧性、自主性、持续性与可信度的安全生态, 保障卫星互联网长期安全运行.

参考文献

1 吕红伟, 吕金华, 张琦. 卫星互联网的安全威胁浅析. 科学与信息化, 2021, 5: 24, 26

2 Wang C, An J P, Xing C W, et al. A review of covert communication technologies for space information networks. Sci Sin Inform, 2024, 54: 1319–1349 [王超, 安建平, 邢成文, 等. 面向空间信息网络的隐蔽通信技术综述. 中国科学: 信息科学, 2024, 54: 1319–1349]

3 Gao Y Y, Wang N W, Lu Z. The development research and construction suggestion of satellite Internet constellations. J CAEIT, 2019, 14: 875–881 [高璎园, 王妮炜, 陆洲. 卫星互联网星座发展研究与方案构想. 中国电子科学研究院学报, 2019, 14: 875–881]

4 Huang T, Huo R, Liu J, et al. Development trends and prospects of future networks. Sci Sin Inform, 2019, 49: 941–948 [黄韬, 霍如, 刘江, 等. 未来网络发展趋势与展望. 中国科学: 信息科学, 2019, 49: 941–948]

5 Al-Hraishawi H, Minardi M, Chougrani H, et al. Multi-layer space information networks: access design and softwarization. IEEE Access, 2021, 9: 158587

6 APEC Telecommunications and Information Working Group. Fostering connectivity: the LEO satellite opportunities in APEC. 2025. https://www.apec.org/docs/default-source/publications/2025/8/225_tel_fostering-connectivity.pdf?sfvrsn=40fc7fd1_1

7 Hiemstra T, Hasler D, Paone D, et al. The European satellite-based QKD system EAGLE-1. In: Proceedings of Free-Space Laser Communications XXXVII, 2025. 216–222

8 Adnan M H, Ahmad Zukarnain Z, Harun N Z. Quantum key distribution for 5G networks: a review, state of art and future directions. Future Int, 2022, 14: 73

9 Chadalavada P, Farabi T, Dutta A. Sequential low-thrust orbit-raising of all-electric satellites. Aerospace, 2020, 7: 74

10 Yahia O B, Garroussi Z, Bélanger O, et al. Evolution of high-throughput satellite systems: a vision of programmable regenerative payload. IEEE Commun Surv Tut, 2024, 27: 1565–1597

11 Dong H W, Sun Z X. The satellite Internet industry is accelerating its development, opening up a new track for the Internet of everything. Commun World, 2024, 7: 26–29 [董宏伟, 孙灼昕. 卫星互联网产业加速发展开辟万物互联新赛道. 通信世界, 2024, 7: 26–29]

12 Zhang F, Chen X Q, Cao L, et al. Design and key technologies for space-based edge computing system. Aerospace Shanghai, 2022, 39: 139–146 [张飞, 陈小前, 曹璐, 等. 天基边缘计算系统设计及关键技术. 上海航天 (中英文), 2022, 39: 139–146]

13 Cui G, Duan P, Xu L, et al. Latency optimization for hybrid GEO-LEO satellite-assisted IoT networks. IEEE Int Things J, 2022, 10: 6286–6297

14 Beach M. O3B, the other three billion. STS-6664 Science and Technology in Development, 2020

15 Hein G W. Status, perspectives and trends of satellite navigation. Satell Navig, 2020, 1: 22

16 Fourati F, Alouini M S. Artificial intelligence for satellite communication: a review. Intell Converged Netw, 2021, 2: 213–243

17 Osoro O B, Oughton E J. A techno-economic framework for satellite networks applied to low Earth orbit constellations: assessing starlink, OneWeb and Kuiper. IEEE Access, 2021, 9: 141611

18 Kassas Z, Kozhaya S, Saroufim J, et al. A look at the stars: navigation with multi-constellation LEO satellite signals of opportunity. Inside GNSS, 2023. https://insidegnss.com/a-look-at-the-stars-navigation-with-multi-constellation-leo-satellite-signals-of-opportunity/

19 Zou C, Wang H, Chang J, et al. Optimal progressive pitch for OneWeb constellation with seamless coverage. Sensors, 2022, 22: 6302

20 Sun Y H, Peng M G. Low earth orbit satellite communication supporting direct connection with mobile phones: key technologies, recent progress and future directions. Telecommun Sci, 2023, 39: 25–36 [孙耀华, 彭木根. 面向手机直连的低轨卫星通信: 关键技术、发展现状与未来展望. 电信科学, 2023, 39: 25–36]

21 Purple Mountain Laboratory, Beijing University of Posts and Telecommunications. White paper on satellite Internet backbone network technologies (2025). In: Proceedings of Organizing Committee of the 9th Future Network Development Conference, 2025

https://www.sciengine.com/doi/10.1360/SSI-2025-0463

[紫金山实验室, 北京邮电大学. 卫星互联网承载网技术白皮书 (2025). 见: 第九届未来网络发展大会组委会, 2025]

22 Wan Y, Qian K C, Xing P. Review of controller deployment methods for space-ground integrated network based on SDN. Comput Meas Control, 2022, 30: 1–11 [万颖, 钱克昌, 邢鹏. 基于 SDN 的天地一体化网络控制器部署方法综述. 计算机测量与控制, 2022, 30: 1–11]

23 Xu X D, Han S J, Zhao Y, et al. 6G wireless coverage extension technologies. Sci Sin Inform, 2024, 54: 1144–1176 [许晓东, 韩书君, 赵芸, 等. 6G 无线覆盖扩展技术. 中国科学: 信息科学, 2024, 54: 1144–1176]

24 Wu D L, Csar C, Salinas J H. GPS jamming: a historical record from global radio occultation (RO) observations. In: Proceedings of the 37th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2024), 2024. 781–795

25 Seddon S, Adams P. Grant Shapps plane's GPS signal 'jammed' near Russia's Kaliningrad. BBC News, 2024. https://www.bbc.com/news/uk-68569676

26 Kirby P, Khalilova K. Azerbaijan says plane hit by 'external interference' over Russia before crash. BBC News, 2024. https://www.bbc.com/news/articles/cy4717j21kko

27 Zhang Y, Zhao S, He J, et al. A survey of secure communications for satellite Internet based on cryptography and physical layer security. IET Inf Secur, 2023, 2023: 5604802

28 Chaos Computer Club München. Iridium-toolkit: a set of tools to parse Iridium frames. https://github.com/muccc/iridium-toolkit

29 Chaos Computer Club München. Gr-iridium: iridium burst detector and demodulator. https://github.com/muccc/gr-iridium

30 YouTube. Iridium satellite hacking update—HOPE XI 2016 talk video. 2016. https://www.reddit.com/r/RTLSDR/comments/50ax1r/iridium_satellite_hacking_update_hope_xi_2016/

31 Hao J. The birdman and Cospas-Sarsat Satellites. In: Proceedings of Hack In The Box (HITB) Security Conference, 2019

32 Hudaib A A Z. Satellite network hacking & security analysis. Int J Comput Sci Secur, 2016, 10: 8–55

33 Wikipedia. Starlink in the Russian-Ukrainian War. https://en.wikipedia.org/wiki/Starlink_in_the_Russian-Ukrainian_War#:$\sim$:text=One%20document%20from%20the%202022,problems%20with%20the%20Starlink%20terminals

34 Psiaki M L, Humphreys T E. GNSS spoofing and detection. In: Proceedings of the IEEE, 2016, 104. 1258–1270

35 UT News. UT austin researchers successfully spoof an $80 million yacht at sea. 2013. https://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea/

36 Jones M. Spoofing in the Black Sea: what really happened? GPS World, 2017. https://www.gpsworld.com/spoofing-in-the-black-sea-what-really-happened/

37 Wang H, Zhang Y, Shen Y, et al. Novel replay attacks against Galileo open service navigation message authentication. In: Proceedings of the 36th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2023), 2023. 3897–3907

38 Wang H, Zhang Y, Zhu X, et al. OSNMA-SDR-SIM: an open-source tool for generating OSNMA-enabled galileo satellite signal. In: Proceedings of the 38th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2025), 2025. 3184–3192

39 Rupprecht D, Kohls K, Holz T, et al. Breaking LTE on layer two. In: Proceedings of IEEE Symposium on Security and Privacy (SP), 2019. 1121–1136

40 Zhang W M, Dai A, Ryan K, et al. Don't look up: there are sensitive internal links in the clear on GEO satellites. In: Proceedings of ACM Conference on Computer and Communications Security (CCS'25), 2025. 1–18

41 Tu K, Al Ishtiaq A, Rashid S M M, et al. Logic gone astray: a security analysis framework for the control plane protocols of 5G basebands. In: Proceedings of the 33rd USENIX Security Symposium (USENIX Security 24), 2024. 3063–3080

42 Shi G. SpaceX claims to have identified and cut off over 2500 Starlink devices around a telecom fraud park in Myanmar. Xinhuanet, 2025 [施歌. SpaceX 称识别并切断缅甸电诈园区周边逾 2500 台 "星链" 设备. 新华网, 2025] https://www.news.cn/20251022/87de393bf8994c00a73a829e5b3b197b/c.html

https://www.sciengine.com/doi/10.1360/SSI-2025-0463

43 Jedermann E, Strohmeier M, Lenders V, et al. RECORD: a RECeption-only region determination attack on LEO satellite users. In: Proceedings of USENIX Security Symposium (USENIX Security'24), 2024

44 Cao J, Ma M, Li H, et al. A survey on security aspects for 3GPP 5G networks. IEEE Commun Surv Tut, 2020, 22: 170–195

45 Basin D, Dreier J, Hirschi L, et al. A formal analysis of 5G authentication. In: Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS), 2018. 1383–1396

46 Electronic Frontier Foundation (EFF). Cell-site simulators (IMSI catchers). https://sls.eff.org/technologies/cell-site-simulators-imsi-catchers

47 Hussain S R, Echeverria M, Chowdhury O, et al. Privacy attacks to the 4G and 5G cellular paging protocols using side channel information. In: Proceedings of the Network and Distributed System Security Symposium (NDSS), 2019

48 Saad M M, Tariq M A, Khan M T R, et al. Non-terrestrial networks: an overview of 3GPP release 17 & 18. IEEE Int Things M, 2024, 7: 20–26

49 3rd Generation Partnership Project. 3GPP system architecture evolution (SAE); security architecture. TS 33.401 V19.1.0 (Release 19), 2025

50 3rd Generation Partnership Project. Security architecture and procedures for 5G system. TS 33.501 V19.4.0 (Release 19), 2025

51 3rd Generation Partnership Project. Study on security aspects of 5G satellite access in the 5G architecture phase 3. TR 33.700-29 V19.1.0 (Release 19), 2025

52 Xue W H, Pan T, Lu C C, et al. Research on inter-satellite routing security mechanisms in LEO satellite networks. Space-Integrated-Ground Inform Netw, 2023, 4: 13–23 [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. 天地一体化信息网络, 2023, 4: 13–23]

53 Li J C, Zhang W J, Qiu L C, et al. Security routing algorithm for space-air-ground integrated network based on probability game. Air Space Defense, 2024, 7: 74–78 [李嘉淳, 张唯炯, 邱令存, 等. 基于概率博弈的空天地一体化网络安全路由算法. 空天防御, 2024, 7: 74–78]

54 Li Z, Liu J. Research on secure routing in satellite networks. J Commun, 2006, 27: 113–118 [李喆, 刘军. 卫星网络安全路由研究. 通信学报, 2006, 27: 113–118]

55 Viega J, McGrew D. The use of Galois/counter mode (GCM) in IPsec encapsulating security payload (ESP). RFC Proposed Standard, 2005

56 Wan P, Lu Z, Zhu H. Study on the impact of IPSec on rate limiting strategies in satellite communications. In: Proceedings of the 4th International Conference on Information Technology, Big Data and Artificial Intelligence (ICIBA), 2024. 296–300

57 Mutlugun A, Hanna Y, Akkaya K. Performance evaluation of quantum-resistant IKEv2 protocol for satellite networking environments. In: Proceedings of IEEE Virtual Conference on Communications (VCC), 2024. 1–7

58 Frankel S, Krishnan S. RFC 6071: IP security (IPsec) and Internet key exchange (IKE) document roadmap. RFC Informational, 2011

59 Huang Z, Li L, Mi X M, et al. Space communication protocol specification (SCPS) and its applications: current status, issues and prospects. Telecommun Eng, 2007, 47: 7–11 [黄展, 李陆, 弥宪梅, 等. 空间通信协议 (SCPS) 及其应用: 现状、问题与展望. 电讯技术, 2007, 47: 7–11]

60 Consultative Committee for Space Data Systems. Space data link security protocol. Recommended Standard, Issue 2, CCSDS 355.0-B-2, 2022

61 Nanjing University of Aeronautics and Astronautics, Yuanjiang-Secbang Security Technology Group Co Ltd, Nanjing Sky-Easyreach Communication Technology Co Ltd. Annual report on satellite Internet security (2024). Nanjing: Nanjing University of Aeronautics and Astronautics. 2024 [南京航空航天大学, 远江盛邦安全科技集团股份有限公司, 南京天际易达通信技术有限公司. 卫星互联网安全年度报告 (2024). 南京: 南京航空航天大学. 2024]

62 Zhang C, Gao F. The future application scenarios and security analysis of satellite Internet. Inform Technol, 2022, 3: 120–126 [张聪, 高峰. 卫星互联网未来应用场景及安全性分析. 信息技术, 2022, 3: 120–126]

63 Liu J, Yu Y, Standaert F X, et al. Small tweaks do not help: differential power analysis of milenage implementations in 3G/4G

https://www.sciengine.com/doi/10.1360/SSI-2025-0463

USIM cards. In: Proceedings of European Symposium on Research in Computer Security, 2015. 468–480

64 Baran G. New eSIM hack lets attackers clone profiles and hijack phone identities. Cyber Security, 2025. https://cybersecuritynews.com/esim-hack/

65 Shang Y D, Hou X J, Wang Y Q, et al. Method for authenticating virtual eSIM card based on TEE, TEE terminal and management platform. CN 108848496 A, 2018-11-20 [尚一多, 侯晓军, 王跃强, 等. 基于 TEE 的虚拟 eSIM 卡的认证方法、TEE 终端和管理平台. CN 108848496 A, 2018-11-20]

66 Lapid B, Wool A. Navigating the samsung trustzone and cache-attacks on the keymaster trustlet. In: Proceedings of European Symposium on Research in Computer Security, 2018. 175–196

67 Lipp M, Kogler A, Oswald D, et al. PLATYPUS: software-based power side-channel attacks on x86. In: Proceedings of IEEE Symposium on Security and Privacy (SP), 2021. 355–371

68 van Bulck J, Moghimi D, Schwarz M, et al. LVI: hijacking transient execution through microarchitectural load value injection. In: Proceedings of IEEE Symposium on Security and Privacy (SP), 2020. 54–72

69 Balog O. Lab dookhtegan cyberattack—second wave findings (Aug 2025). CYDOME, 2025. https://cydome.io/lab-dookhtegan-cyberattack-second-wave-findings-aug-2025/

70 Vanlyssel J, Sobrados E, Anwar R, et al. SpyChain: multi-vector supply chain attacks on small satellite systems. 2025. ArXiv:2510.06535

71 Saunders N, Thummala R, Falco G. Space cybersecurity incident response framework: a viasat case study. In: Proceedings of IEEE Aerospace Conference, 2025. 1–15

72 Wu Y, Wang J, Wang Y, et al. Your firmware has arrived: a study of firmware update vulnerabilities. In: Proceedings of the 33rd USENIX Security Symposium (USENIX Security 24), 2024. 5627–5644

73 Busari M. Secure boot and firmware authentication policies in SoCs. 2025. https://www.researchgate.net/publication/394937608_Secure_Boot_and_Firmware_Authentication_Policies_in_SoCs

74 Matetic S, Ahmed M, Kostiainen K, et al. ROTE: rollback protection for trusted execution. In: Proceedings of the 26th USENIX Security Symposium (USENIX Security 17), 2017. 1289–1306

75 Jones R C. Survey of space professionals' perception of satellite cybersecurity from 2012 to 2022: decision-makers' thoughts on satellite cybersecurity evolving. New Space, 2024, 12: 259–272

76 Burgess M. The hacking of starlink terminals has begun. Wired, 2022. https://www.wired.com/story/starlink-internet-dish-hack/?utm_source=chatgpt.com

77 Kessler D J, Cour-Palais B G. Collision frequency of artificial satellites: the creation of a debris belt. J Geophys Res, 1978, 83: 2637–2646

78 Mason J, Stupl J, Marshall W, et al. Orbital debris-debris collision avoidance. Adv Space Res, 2011, 48: 1643–1655

79 Nicholas J. The collision of iridium 33 and cosmos 2251: the shape of things to come. In: Proceedings of the 60th International Astronautical Congress, 2009. 1–14

80 Wikipedia. 2007 Chinese anti-satellite missile test. 2025. https://en.wikipedia.org/wiki/2007_Chinese_anti-satellite_missile_test

81 Jones A. China's space station maneuvered to avoid Starlink satellites. Spacenews, 2021. https://spacenews.com/chinas-space-station-maneuvered-to-avoid-starlink-satellites/

82 Falletti E, Margaria D, Marucco G, et al. Synchronization of critical infrastructures dependent upon GNSS: current vulnerabilities and protection provided by new signals. IEEE Syst J, 2018, 13: 2118–2129

83 Fernandez-Hernandez I, Walter T, Neish A, et al. Independent time synchronization for resilient GNSS receivers. In: Proceedings of the International Technical Meeting of the Institute of Navigation, 2020. 964–978

84 Sharma A, Gupta B B, Singh A K, et al. Advanced persistent threats (APT): evolution, anatomy, attribution and countermeasures. J Ambient Intell Hum Comput, 2023, 14: 9355–9381

85 Langton M T, Yang Z, Pan G, et al. Security challenges in satellite ground stations and their risk mitigation techniques. In: Proceedings of the 13th International Conference on Communications, Circuits and Systems (ICCCAS), 2024. 508–513

https://www.sciengine.com/doi/10.1360/SSI-2025-0463

86 China Internet Society for Cyberspace Security. The US intelligence agencies frequently carry out cyber attacks and espionage against China's defense and military industry. 2025 [中国网络空间安全协会. 美情报机构频繁对我国防军工领域实施网络攻击窃密. 2025] https://mp.weixin.qq.com/s/MjIlXBYK0kK2ysU6a78BAg

87 Liu W, Li Y, Li H, et al. The dark side of scale: insecurity of direct-to-cell satellite mega-constellations. In: Proceedings of IEEE Symposium on Security and Privacy (SP), 2024. 445–464

88 Cao X, Nan G, Guo H, et al. Exploring LLM-based multi-agent situation awareness for zero-trust space-air-ground integrated network. IEEE J Sel Areas Commun, 2025, 43: 2230–2247

89 Rong Y, Nan G, Zhang M, et al. Semantic entropy can simultaneously benefit transmission efficiency and channel security of wireless semantic communications. IEEE Trans Inform Forensic Secur, 2025, 20: 2067–2082

90 Shao X, Wang W, Zhou B, et al. Joint bandwidth and spectrum usage zones flexible allocation for coexisting multiple UAV networks: an interference graph approach. IEEE Int Things J, 2025, 12: 31141–31153

91 Wu Q H, Wang W, Li Z G, et al. SpectrumChain: a disruptive dynamic spectrum-sharing framework for 6G. Sci China Inf Sci, 2023, 66: 130302

92 Xu D, Yu K, Ritcey J A. Cross-layer device authentication with quantum encryption for 5G enabled IIoT in Industry 4.0. IEEE Trans Ind Inf, 2022, 18: 6368–6378

93 Zhang Y, Zhao S R, He J, et al. Satellite Internet security: requirement, current status and trends. J Cybersecur, 2024, 2: 2–17 [张元玉, 赵双睿, 何吉, 等. 卫星互联网安全: 需求, 现状与趋势. 网络空间安全科学学报, 2024, 2: 2–17]

94 Tedeschi P, Sciancalepore S, Di Pietro R. Satellite-based communications security: a survey of threats, solutions, and research challenges. Comput Netws, 2022, 216: 109246

95 Abdelsalam N, Al-Kuwari S, Erbad A. Physical layer security in satellite communication: State-of-the-art and open problems. IET Commun, 2025, 19: e12830

96 Hamza A, Kumar B. A review paper on des, aes, rsa encryption standards. In: Proceedings of the 9th International Conference System Modeling and Advancement in Research Trends (SMART), 2020. 333–338

97 Pirayesh H, Zeng H. Jamming attacks and anti-jamming strategies in wireless networks: a comprehensive survey. IEEE Commun Surv Tut, 2022, 24: 767–809

98 Pickholtz R, Schilling D, Milstein L. Theory of spread-spectrum communications—a tutorial. IEEE Trans Commun, 2003, 30: 855–884

99 van Trees H L. Optimum Array Processing: Part IV of Detection, Estimation, and Modulation Theory. Hoboken: John Wiley & Sons, 2002

100 Jia Z. Anti-jamming technology in small satellite communication. J Phys Conf Ser, 2018, 960: 012013

101 Wang J, Zhang Y, Zhao S, et al. A survey on authentication in satellite Internet. J Netw Netw Appl, 2022, 2: 183–194

102 National Institute of Standards and Technology. Zero trust architecture. NIST SP 800-207, 2020

103 Internet Engineering Task Force (IETF). RFC 9200: Authentication and authorization for constrained environments using the OAuth 2.0 framework (ACE-OAuth). RFC Proposed Standard, 2022

104 Internet Engineering Task Force (IETF). RFC 9820: Authentication service based on the Extensible Authentication Protocol (EAP) for use with the constrained application protocol (CoAP). RFC Proposed Standard, 2025

105 National Institute of Standards and Technology. Module-lattice-based key-encapsulation mechanism standard. FIPS 203, 2024

106 ETSI. Quantum-safe hybrid key establishment (ETSI TS 103 744 V1.2.1). ETSI Technical Specification, 2025

107 National Institute of Standards and Technology. Guide to attribute based access control (ABAC) definition and considerations. NIST SP 800-162, 2014

108 Farrea K A, Baig Z, Doss R, et al. Zero trust-based authentication for inter-satellite links in NextGen low Earth orbit networks. Ad Hoc Netws, 2025, 174: 103817

109 Wang B, Li S, Mu J, et al. Research advancements in key technologies for space-based situational awareness. Space Sci Technol, 2022, 1: 176–207

https://www.sciengine.com/doi/10.1360/SSI-2025-0463

110 Oltrogge D L, Alfano S. The technical challenges of better space situational awareness and space traffic management. J Space Saf Eng, 2019, 6: 72–79

111 Oltrogge D L, Alfano S, Law C, et al. A comprehensive assessment of collision likelihood in geosynchronous Earth orbit. Acta Astronaut, 2018, 147: 316–345

112 Studer A, Perrig A. The coremelt attack. In: Proceedings of European Symposium on Research in Computer Security, 2009. 37–52

113 Kang M S, Lee S B, Gligor V D. The crossfire attack. In: Proceedings of IEEE Symposium on Security and Privacy, 2013. 127–141

114 Giuliari G, Ciussani T, Perrig A, et al. ICARUS: attacking low Earth orbit satellite networks. In: Proceedings of the 21th USENIX Annual Technical Conference, 2021. 317–331

115 Zeng Z, Jin G, Xu C, et al. Satellite telemetry data anomaly detection using causal network and feature-attention-based LSTM. IEEE Trans Instrumen Meas, 2022, 71: 1–21

116 Cheng F, Guo X, Qi Y, et al. Research on satellite power anomaly detection method based on LSTM. In: Proceedings of IEEE International Conference on Power Electronics, Computer Applications, 2021. 706–710

117 Hassanin M, Keshk M, Salim S, et al. PLLM-CS: pre-trained large language model (LLM) for cyber threat detection in satellite networks. Ad Hoc Netws, 2025, 166: 103645

118 Liao S K, Cai W Q, Liu W Y, et al. Satellite-to-ground quantum key distribution. Nature, 2017, 549: 43–47

119 中国科学院. 中国学科发展战略: 网络空间安全. 北京: 科学出版社, 2025

120 Yin J, Li Y H, Liao S K, et al. Entanglement-based secure quantum cryptography over 1120 kilometres. Nature, 2020, 582: 1–5

121 商用密码标准研究院. 新一代商用密码算法征集活动. 2025. https://www.niccs.org.cn/

122 Liu F, Wen Y, Zhang D, et al. Log2vec: a heterogeneous graph embedding based approach for detecting cyber threats within enterprise. In: Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, 2019. 1777–1794

123 Hossain Md N, Milajerdi S M, Wang J, et al. SLEUTH: real-time attack scenario reconstruction from COTS audit data. In: Proceedings of the 26th USENIX Security Symposium, 2017. 487–504

124 Hossain M N, Sheikhi S, Sekar R. Combating dependence explosion in forensic analysis using alternative tag propagation semantics. In: Proceedings of IEEE Symposium on Security and Privacy (SP), 2020. 1139–1155

125 Benabderrahmane S, Valtchev P, Cheney J, et al. APT-LLM: embedding-based anomaly detection of cyber advanced persistent threats using large language models. In: Proceedings of the 13th International Symposium on Digital Forensics and Security (ISDFS), 2025. 1–6

126 Cheng W, Zhu T, Xiong C, et al. SoK: knowledge is all you need: accelerating last mile delivery for automated provenance-based intrusion detection with LLMs. 2025. ArXiv:2503.03108

127 Ji S L, Wang Q Y, Chen A Y, et al. State of the art survey of open source software supply chain security. J Softw, 2023, 34: 1330–1364 [纪守领, 王琴应, 陈安莹, 等. 开源软件供应链安全研究综述. 软件学报, 2023, 34: 1330–1364]

128 Jiang Y, Liang J, Ma F, et al. When fuzzing meets LLMs: challenges and opportunities. In: Proceedings of the 32nd ACM International Conference on the Foundations of Software Engineering, 2024. 492–496

129 Nikitin K, Kokoris-Kogias E, Jovanovic P, et al. Chainiac: proactive software-update transparency via collectively signed skipchains and verified builds. In: Proceedings of the 26th USENIX Security Symposium (USENIX Security 17), 2017. 1271–1287

130 Bikos A N, Kumar S A P. SAT-IOTA: a cybersecurity reinforcement framework for blockchain-driven space satellites utilizing anomaly prediction. IEEE J Miniat Air Space Syst, 2025, 6: 378–391

131 United Nations. Treaty on principles governing the activities of states in the exploration and use of outer space, including the Moon and other celestial bodies (Outer Space Treaty). 1967. https://www.faa.gov/about/office_org/headquarters_offices/ast/media/treaty_Princi_Gov_Acti_States_OST.pdf

132 International Telecommunication Union (ITU). Yearbook of statistics. 1991, 2000: 2001

133 Zhang X Y. The United States places great importance on space cybersecurity. Civil-Mil Integr Cyberspace, 2021, 2: 29–33 [张

https://www.sciengine.com/doi/10.1360/SSI-2025-0463

晓玉. 美国高度重视太空网络安全问题. 网信军民融合, 2021, 2: 29–33]

134 United States Senate Committee on Homeland Security and Governmental Affairs. All information (except text) for S.1425—Satellite Cybersecurity Act. 2023. https://www.congress.gov/bill/118th-congress/senate-bill/1425/all-info

135 White House National Science and Technology Council (NTSC). National low Earth orbit research and development strategy. 2023. https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/NATIONAL-LEO-RD-STRATEGY033123.pdf

136 中华人民共和国全国人民代表大会常务委员会. 中华人民共和国网络安全法. 北京: 中国法治出版社, 2016

137 中华人民共和国工业和信息化部. 关于电信设备进网许可制度若干改革举措的通告. 北京: 中华人民共和国工业和信息化部, 2023

138 国家互联网信息办公室, 国家发展和改革委员会, 工业和信息化部, 等. 终端设备直连卫星服务管理规定. 北京: 国家互联网信息办公室, 2025

139 中华人民共和国工业和信息化部. 工业和信息化部关于优化业务准入促进卫星通信产业发展的指导意见. 北京: 中华人民共和国工业和信息化部, 2024

140 赛迪智库 (CCID). 美国商用卫星互联网安全管理的经验及对我国的启示. 2024. https://www.ccidgroup.com/info/1207/41151.htm

141 U.S. Department of State. A strategic framework for space diplomacy. 2023. https://www.state.gov/wp-content/uploads/2023/05/Space-Framework-Clean-2-May-2023-Final-Updated-Accessible-5.25.2023.pdf

142 Beijing Institute of Tracking and Telecommunications Technology, Tsinghua University, National Computer Network Emergency Response Technical Team/Coordination Center of China, et al. Space Data and Information Transfer Systems—General Technical Requirements of Network Security. Beijing: National Standardization Administration, 2025 [北京跟踪与通信技术研究所、清华大学、国家计算机网络与应急技术处理协调中心, 等. 空间数据与信息传输系统网络安全总体技术要求. 北京: 国家标准化管理委员会, 2025]

143 中华人民共和国全国人民代表大会常务委员会. 中华人民共和国数据安全法. 中华人民共和国全国人民代表大会常务委员会公报, 2021, 5: 951–956

144 中华人民共和国全国人民代表大会常务委员会. 中华人民共和国个人信息保护法. 中华人民共和国全国人民代表大会常务委员会公报, 2021, 6: 1117–1125

145 Deng P K, Hao Y R, Liu S S, et al. Analysis and suggestions on the security management of US commercial satellite Internet. China Inf Secur, 2025, 4: 74–76 [邓攀科, 郝依然, 刘思思, 等. 美国商用卫星互联网安全管理分析与建议. 中国信息安全, 2025, 4: 74–76]

146 Fontanesi G, Ortíz F, Lagunas E, et al. Artificial intelligence for satellite communication: a survey. IEEE Commun Surv Tut, 2025, 1: 1–61

147 Salim S, Moustafa N, Reisslein M. Cybersecurity of satellite communications systems: a comprehensive survey of the space, ground, and links segments. IEEE Commun Surv Tut, 2025, 1: 372–425

148 Du X K, Shu N, Liu C S, et al. Overview of security issues and defense technologies for low Earth orbit satellite network. J Electron Inform Technol, 2025, 4: 1609–1622

149 Aerospace. Cybersecurity in orbit: how aerospace is evolving defenses against emerging space threats. 2024. https://aerospace.org/article/cybersecurity-orbit-how-aerospace-evolving-defenses-against-emerging-space-threats

150 Feng D G. Research on the development trend of cybersecurity technology. J Inf Secur Res, 2025, 11: 2–4 [冯登国. 网络空间安全技术发展趋势研究. 信息安全研究, 2025, 11: 2–4]

https://www.sciengine.com/doi/10.1360/SSI-2025-0463

A survey of security in satellite Internet networks

Jin CAO[1*], Yu SUN[2], Yuanyu ZHANG[3], Ruhui MA[1*], Tiantian ZHANG[4], Zhou SU[4], Purui SU[5], Hui LI[1] & Dengguo FENG[5*]

1. *School of Cyber Engineering, Xidian University, Xi'an 710071, China*
2. *School of Cyber Science and Technology, Beihang University, Beijing 100191, China*
3. *School of Computer Science and Technology, Xidian University, Xi'an 710071, China*
4. *School of Cyber Science and Engineering, Xi'an Jiaotong University, Xi'an 710049, China*
5. *Institute of Software Chinese Academy of Sciences, Beijing 100190, China*

* Corresponding author. E-mail: jcao@xidian.edu.cn, rhma@xidian.edu.cn, fengdg@263.net

Abstract In recent years, with the rapid advancement of communication technologies, satellite Internet has become a critical component of the global information infrastructure, demonstrating growing strategic value in military, civilian, economic, and emergency communication domains. However, inherent characteristics such as its open network architecture, highly dynamic satellite nodes, complex system composition, and cross-domain operations have posed significant security challenges and threats. This paper aims to provide a systematic survey of security in satellite Internet networks. Firstly, it outlines the global development landscape of satellite Internet and its strategic significance, emphasizing the importance of security issues. Secondly, it analyzes the architectural characteristics of satellite Internet and the fundamental security challenges. Thirdly, the paper provides a detailed introduction of the diverse threat landscape, complemented with several concrete instances. Fourthly, it summarizes corresponding security protection technologies and explores relevant policy and legal frameworks. Finally, future trends are discussed to provide valuable insights for research, industrial practice, and security governance in this field.

Keywords satellite Internet, satellite Internet security architecture, security threat landscape, security protection technologies, policy and legal framework

https://www.sciengine.com/doi/10.1360/SSI-2025-0463