

卫星互联网安全风险及应对措施分析

谷 欣¹, 单 超¹, 孙才俊², 李 珂³, 田 敏¹, 王瑞青¹

(1. 中国星网网络创新研究院有限公司, 北京 100029;

2. 之江实验室智能网络研究院, 浙江 杭州 311121;

3. 中电科网络安全科技股份有限公司, 北京 100043)

摘 要: 从阐述卫星互联网的系统组成和安全事件入手, 综合分析卫星和载荷、卫星终端、信关站、运控中心、运营中心等实体对象的安全风险, 接入链路、星间链路、馈电链路、测控链路、地面互联等通信链路安全风险, 运营数据、通信内容监管、公众隐私、数据违规出境等应用数据安全风险, 以及新兴技术带来的安全风险挑战, 并针对上述各种潜在的安全威胁提出相应的应对措施。最后对卫星互联网安全形势演变应关注的研究方向进行展望。

关键词: 卫星互联网; 安全挑战; 安全风险; 应对措施

中图分类号: TP393.08

文献标识码: A

doi: 10.11959/j.issn.2096-8930.2024010

Analysis of Satellite Internet Security Risks and Countermeasures

GU Xin¹, SHAN Chao¹, SUN Caijun², LI Ke³, TIAN Min¹, WANG Ruiqing¹

1. China Satellite Network Innovation Co., Ltd., Beijing 100029, China

2. Intelligent Network Research Institute Zhejiang Lab, Hangzhou 311121, China

3. CETC Cyberspace Security Technology Co., Ltd., Beijing 100043, China

Abstract: This paper was commenced with an exploration of the system composition and security events of satellite Internet, conducted a comprehensive assessment of risks associated with entities such as satellites, terminals, ground stations, mission control, and operation center, secondly extends to communication pathways, encompassing access links, inter-satellite links, feeder links, TT&C links, and ground networks, then delved into data-related risks, covering operational data, regulatory content, public privacy, and outbound data, furthermore, addresses challenges posed by emerging technologies. Finally, proposed corresponding countermeasures for potential threats and concludes by outlining crucial research directions for understanding the evolving security landscape of satellite Internet.

Keywords: satellite Internet, security challenges, security risk, countermeasures

0 引言

卫星互联网是一种利用通信卫星星座实现全球范围内地面、空中、海上用户等随遇接入互联网的新型信息基础设施^[1], 能为各种应用提供泛在、智能、协同、高效的广域空间网络支撑和保障。卫星互联网极大促进了移动设备向全场景协同、高可靠互联的方向迈进^[2-3], 有利于实现全球信息网络的高效互联与深度融合。

近年来, 卫星互联网在全球范围内高速发展, 极大促进了人类沟通和万物互联。作为全球化的关键信息基础设施, 卫星互联网面临着严峻的安全挑战, 这些挑战不仅直

接威胁着通信的机密性、完整性和稳定性, 还对数据安全、公众隐私甚至国家安全产生了潜在影响。因此, 亟须深入分析卫星互联网的安全风险和应对措施, 确保这一关键信息基础设施的可靠性和安全性, 为全球经济、社会的稳定和发展提供可靠保障。本文通过分析卫星互联网的安全风险及应对措施, 为卫星互联网安全体系设计提供借鉴和参考, 推动卫星互联网安全领域的深入研究和应用。

1 卫星互联网系统的组成

卫星互联网系统包括空间段、用户段及地面段^[4], 由实体对象及通信链路组成。空间段包括通信卫星及星

间链路,卫星通过星间链路进行互联;用户段包括各类卫星用户终端,用户终端通过接入链路与卫星进行互联;地面段包括信关站、运营中心及运控中心,信关站一方面通过馈电链路传输星地间数据,另一方面与地面互联网互联,实现卫星用户终端接入互联网的功能,此外,还通过测控链路传输对卫星的控制指令。信关站、运营中心、运控中心间采用地面链路进行互联,其系统的组成如图 1 所示。

2 卫星互联网安全事件分析

卫星互联网由卫星通信接入互联网演化而来,是一种通信和网络技术。近年来,针对卫星通信网络的攻击案例数量呈快速上升趋势,并且逐步从空间域的物理破坏向信息域的安全攻击发展^[5-6],这些攻击同样可以对卫星互联网造成破坏并产生不利后果。一些具有重大影响的卫星网络

安全事件见表 1。

从表 1 可以看出,针对卫星互联网的安全事件层出不穷,攻击者可以对卫星互联网中的实体对象、通信链路、应用数据等多个方面进行攻击。有关资料显示,网络战已经延伸到了太空领域^[7],出现了人类战争历史上首次围绕卫星进行太空攻防的案例。此外,人工智能、量子计算等技术的快速发展也将对卫星互联网的安全性产生深远影响,这些技术的引入可能导致卫星互联网系统面临更复杂、隐蔽和规模化的安全威胁。

3 卫星互联网安全风险分析

卫星互联网作为全球化的关键信息基础设施,为全球通信和互联网接入提供了无处不在的服务。然而,随着卫星互联网的快速发展和广泛应用,其安全风险也在日益增加,主要表现在实体对象、通信链路、应用数据(含卫

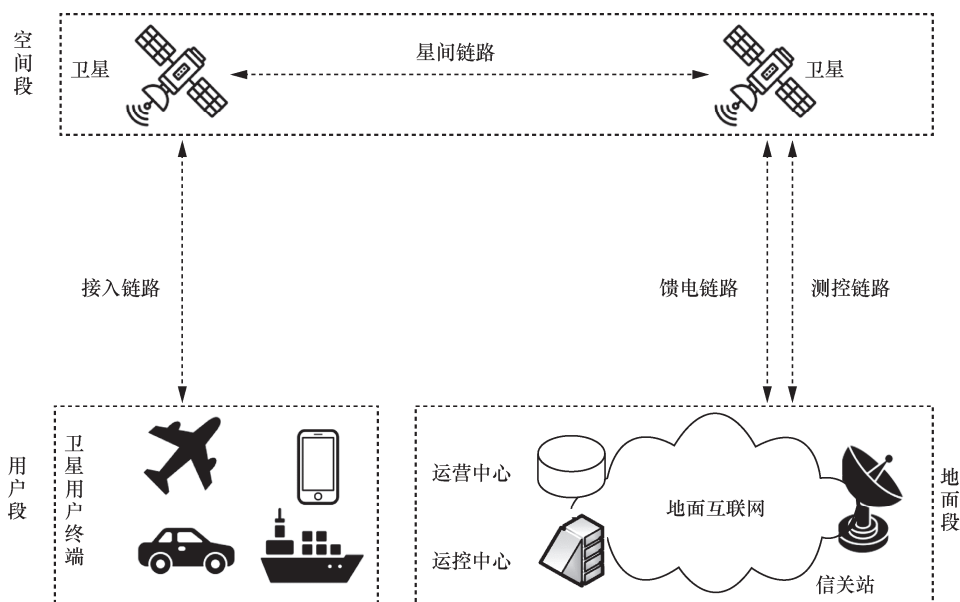


图 1 卫星互联网系统的组成

表 1 卫星网络安全事件

安全风险	安全事件			
实体对象安全风险	黑客入侵 X 射线科学卫星地面站,发布恶意指令控制卫星(1998 年)	美国铱星-33 与俄罗斯宇宙-2251 卫星相撞(2009 年)	SpaceX 40 颗卫星受地磁暴影响坠落(2022 年)	鲁汶大学安全研究员使用自制设备入侵星链卫星互联网服务(2022 年)
通信链路安全风险	黑客组织使用恶意软件劫持合法用户的 IP 地址来盗取卫星数据(2007 年)	NASA 和美国地质调查局的观测卫星受到干扰,卫星 C2 链路遭受攻击(2007 年)	牛津大学研究人员通过卫星天线和调谐器监听卫星互联网流量(2020 年)	Ka 频段卫星卫星网络中断,攻击者通过破坏管理网络关闭用户调制解调器(2022 年)
应用数据安全风险	NASA 电脑被盗,导致空间站密码和算法被泄露(2011 年)	攻击者通过外部合作商共享的网络环境进入 NASA 内网盗取约 500 MB 重要数据(2018 年)	黑客通过外部用户系统侵入 NASA 卫星天线网络,迫使 NASA 切断与该网络的连接(2018 年)	

星通信网访问互联网的数据)以及相关技术等几方面的安全风险,如图 2 所示。

3.1 实体对象安全风险

第一,卫星终端安全风险。随着手机直连卫星业务推向市场,直连终端作为普通电子产品进入千家万户,卫星终端进入了一个全新发展阶段。直连终端在为用户带来便利的同时也为攻击者提供了研究卫星工作机制、网络漏洞的机会。若终端自身防护措施不足,则可能存在终端与网络之间空中接口传输的信令和数据被窃取、被篡改的风险^[8]。此外,若终端 App 存在诸如软件漏洞、恶意代码等不安全因素,也可能增加用户个人隐私泄露的安全隐患。

第二,卫星和载荷安全风险。首先,攻击者可以利用恶意大功率上行干扰通过“卫星功率掠夺”使卫星通信业务信号无法正常传输,进而使卫星通信服务瘫痪。其次,卫星载荷作为资源受限系统,攻击者可以通过模拟海量卫星终端发送大量虚假请求,使卫星载荷无法为合法用户提供有效服务,引发拒绝服务攻击。最后,卫星和卫星载荷复杂、庞大的供应链可能存在安全漏洞,例如,某个器件或设备留有后门,攻击者可以利用该后门绕过或禁用安全策略,从而引发攻击事件^[9]。

第三,信关站安全风险。在物理环境方面,信关站选址不当可能遭受自然灾害(如地震、水灾、火灾、雷击等)的影响,机房环境保护欠佳可能遭受潮湿、静电、高温和电力供应中断等环境风险,安防措施不完善可能遭受非法人员入侵等安全威胁。在传输网络方面,信关站与外部互联网网元之间的通信网络可能穿越不可控区域,如数据未经加密进行传输,存在信息被攻击者监听、篡改或阻断的风险。在网络边界方面,信关站部署用户面功能(User Plane

Function, UPF)接入国际互联网,扩大了网络暴露面,存在被攻击者扫描和入侵的风险^[10]。

第四,运控中心安全风险。运控中心承载着多个关键系统,是被重点攻击的对象。首先,运控中心的应用系统和数据库若没有统一身份认证,则存在身份被冒用的风险,导致攻击者非法进入核心系统,偷窥核心数据,泄露重要信息。其次,运控中心的应用系统和数据库若缺乏必要的权限控制措施,则存在越权操作风险,导致攻击者进行违规操作,篡改核心数据,乱发操作指令,影响系统运行。最后,运控中心的应用系统和数据库若缺乏审计功能,则存在无法及时发现、分析和溯源攻击行为的风险。

第五,运营中心安全风险。运营中心部署运营支撑系统,用于对业务的运营维护。该系统提供大量对外服务,具有较大网络暴露面,极易遭受来自外部的攻击。首先,攻击者通过扫描开放的通信端口,获取设备软硬件信息,利用零日漏洞绕过安全防护措施入侵内部网络,再通过横向攻击、非法提权等操作获取重要系统权限,从而窃取和篡改系统数据。其次,攻击者利用操作终端一机多用、操作人员对外沟通频繁等特点,采用钓鱼、欺骗等手段,直接入侵操作终端,获取账号和权限后进入核心系统。最后,攻击者利用运营支撑系统存在频繁远程访问的特点,攻击运营支撑系统的身份验证和权限控制系统,通过“错误配置攻击”获得对运营支撑系统的远程访问权限,伪装成管理人员来篡改关键信息,实施违规和越权操作。

3.2 通信链路安全风险

第一,接入链路安全风险。接入链路是卫星终端与卫星之间的通信链路。由于接入链路信道开放、共享、易受干扰,因此极易受到各种安全攻击,主要体现在身份伪造、数据窃取、数据篡改和空中接口频率干扰等方面。首先,

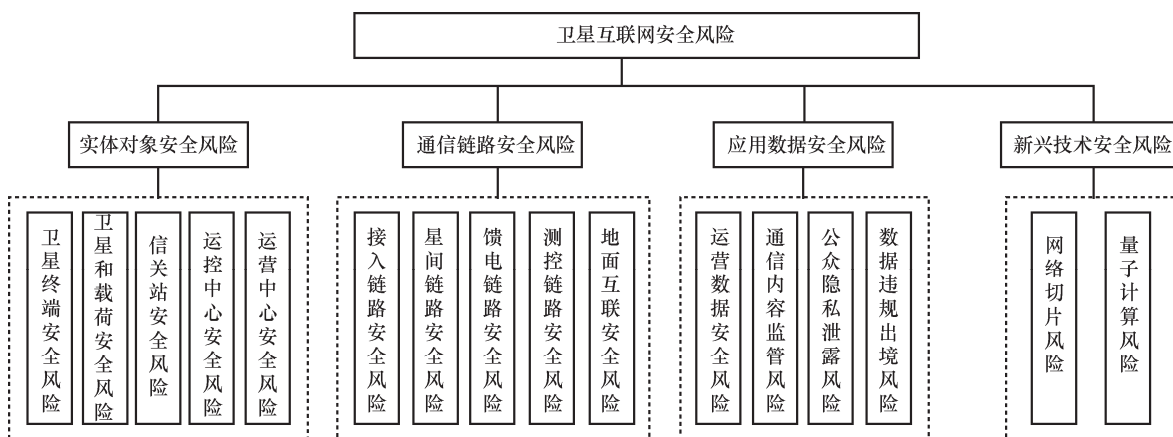


图 2 卫星互联网安全风险分类

地面终端与卫星之间的空中接口信道高度开放,攻击者可以假冒终端身份向卫星互联网发送恶意信息,进而对卫星互联网进行攻击。其次,如果终端与卫星之间的通信数据以明文方式进行传输,攻击者可以轻易窃听通信内容。再次,攻击者可以劫持和篡改卫星接入认证数据,并通过数据重放等手段欺骗认证系统,从而破坏身份认证的正确性。最后,由于卫星空间轨道的开放性,不同类型的卫星在共享的空间环境运行时不可避免地会引发信号杂波干扰、邻星干扰和相邻信道干扰^[11],这种干扰可能导致通信链路的可靠性下降、传输速率降低以及数据丢失风险增加,对卫星互联网系统的性能和可用性构成潜在威胁。

第二,星间链路安全风险。星间链路是卫星与卫星之间的通信链路。由于卫星节点的处理能力有限且星座拓扑结构动态变化,因此星间链路容易遭受身份伪造、数据窃取与篡改、数据重放等攻击^[12]。首先,星间可能未采取身份认证机制,使得攻击者可以伪造合法卫星身份加入组网链路,从而窃取卫星间的通信数据。其次,攻击者可以窃听星间通信的内容,一旦攻击者获得明文数据,可进一步伪造和篡改这些数据,并将篡改后的数据发送给接收方,使其接收到虚假的信息。最后,攻击者可以监听星间链路,将接收到的信息修改后重新发送给接收方的卫星,以致接收方卫星收到错误或无效的数据,数据完整性遭到破坏。

第三,馈电链路安全风险。馈电链路是卫星与地面站之间的通信链路,容易受到身份伪造、数据窃取与篡改、数据重放等攻击,产生的风险在星间链路中已进行分析。

第四,测控链路安全风险。测控链路是指卫星与地面测控站之间的链路。通过测控链路,测控站可以对卫星进行管理。测控链路安全风险主要体现在以下两个方面:一方面,攻击者接收卫星测控传输信号,通过专业的信号分析^[13],解析出卫星系统的通信编码体制;另一方面,若测控站与卫星间缺乏安全身份认证机制,攻击者可以伪造成合法的测控站并发送虚假测控指令,导致卫星控制权被接管。

第五,地面互联安全风险。地面互联链路指卫星地面站之间的通信链路。地面站主要包括信关站、运控中心、运营中心3部分,地面站之间需要租用运营商线路进行通信,攻击者可以通过运营商网络发起攻击,包括信息窃取、渗透攻击、恶意程序注入等,导致地面站信息被泄露、系统瘫痪。

3.3 应用数据安全风险分析

第一,运营数据安全风险。运营数据具有采集、传

输、存储、处理、交换和销毁的完整生命周期。在采集环节,若缺乏数据分级分类措施,且没有及时利用密码技术为数据打上不可篡改、不可分离的电子标签,数据可能存在源头不清、权属不清、类别混乱等问题,对数据生命周期后续环节造成无法弥补的影响;在传输环节,若缺乏加密措施和数据完整性验证机制,则存在被窃取或篡改的风险;在存储环节,若缺乏冗余备份措施和冷热多级备份能力,运营数据在断电、过温、火灾或人为误操作情况下可能遭受损毁;在处理环节,若缺乏身份认证和访问授权措施,攻击者可非法入侵运营系统,篡改重要数据;在交换阶段,若缺少密码保护措施,运营数据易被攻击者获取,导致数据所有权转移,未来可能被非法滥用;在销毁阶段,若无有效措施确保数据被完全销毁,则存在数据被部分或完全恢复,导致泄露、滥用的风险。

第二,通信内容监管风险。公众用户通过卫星互联网进行通信,如果对卫星互联网中的内容监管力度不足,则非法行为者可借助卫星互联网发布色情内容、交换恐怖信息、散布仇恨言论、传播虚假新闻、滥用消费者个人数据等,给国家安全、社会稳定、公众隐私带来严重挑战。

第三,公众隐私泄露风险。用户在卫星互联网中产生、存储、使用的数据(如身份信息、位置信息、通信信息、使用应用服务信息等)面临被非法采集、篡改、泄露等风险。

第四,数据违规出境风险。卫星互联网具有全球化的特点,某国用户产生的重要数据易借助卫星互联网发送到他国。目前,世界上主要国家都制定了约束重要数据出境的法律法规,对出境数据进行严格的管控和安全评估,未经评估的数据出境可能会导致重要数据泄露等风险。

3.4 相关技术安全风险分析

第一,网络切片风险。网络切片可以实现通信端到端的安全隔离,从而实现用户通信的隔离,但随着网络架构的演进,网络切片也引入了新的安全风险。首先,网络切片隔离措施不足,可能带来跨切片攻击和数据泄露风险。其次,网络切片为实现多业务场景承载,将引入更多的网络信令,如切片资源之间未做出合理的规划,网络将承载较大的调度负荷,存在信令风暴等安全隐患。

第二,量子计算风险。传统计算机使用二进制进行运算,而量子计算机则利用量子特性进行运算。与传统计算机相比,量子计算机的特点在于量子态和量子门操作,使其具有更高的运算速度和更强的计算能力。同时,量子算法充分发挥了量子比特的优势,针对特定的数学难题问题的解决效率实现指数级提升。未来,大规模量子计算机的

部署将会导致基于大整数分解、离散对数、椭圆曲线等数学困难问题的密码学方案面临被破解的风险^[14]。

4 安全风险应对措施

4.1 实体对象安全应对措施

第一，加强系统软硬件安全。通过代码审计、模糊测试和漏洞挖掘等防护手段，可以提高系统的抗攻击能力。这些措施有助于发现和修复潜在的安全漏洞，减少外部威胁对系统的影响。

第二，加强组网认证与密钥协商机制。卫星互联网需要研发轻量化安全组网认证与密钥协商机制，可用于卫星互联网系统中的节点身份认证^[15]，确保合法实体加入系统，防止未经授权的访问。

第三，加强安全审计。针对日常管理操作进行日志审计，设置不同级别的告警类型和告警触发阈值，及时检测异常行为和安全事件，提高事件溯源和调查取证的能力，保护系统免受内部和外部威胁的侵害。

4.2 通信链路安全应对措施

第一，提升密码算法能力。鉴于量子计算对传统密码算法的威胁，应考虑在非对称密钥体系中引入抗量子计算的密码算法，在对称密钥体系中通过增加密钥长度提升算法安全性。

第二，采用基于空间处理的抗干扰措施，包括自适应调零天线技术和点波束技术。自适应调零天线技术通过调整多个天线单元接收信号的加权值（相位和幅度），在天线接收波束中形成多个零陷，从而抑制干扰方向。点波束技术则利用 Ka 及以上频段波束较窄的特性，在空间上规避干扰。

第三，采用基于时间处理的抗干扰措施，包括猝发通信技术和跳时技术^[16]，有助于降低干扰对通信链路的影响，提高系统的抗干扰能力。猝发通信技术信号在传输过程中暴露的时间很短，大大降低了被侦察和截获的概率，从而有效对抗欺骗式干扰。跳时技术利用特定的码序列进行选择性的多时片的时移键控，使发射信号在时间轴上发生跳变。

4.3 应用数据安全应对措施

第一，加强数据全生命周期安全防护。在数据采集过程中，采取必要的分级分类措施，利用密码技术为电子文件和数据库打上标签，确保数据源头清晰、权属清晰，可追溯可审计；在数据传输过程中，采用加密技术和数据完整性验证机制保护数据的机密性和完整性，防止数据在传输过程中被窃取或篡改；在数据存储过程中，

进行介质管理和冗余备份，确保数据存储在安全可靠的环境中，并有同城、异地备份机制以应对意外情况；在数据处理过程中，采用身份认证、访问授权和行为审计，确保只有经过授权的用户可以访问数据，并对其访问行为进行监控和审计，同时，应遵循最小化和必要原则，只处理必要的数据，减少数据暴露的风险；在数据交换过程中，需要对敏感数据进行脱敏脱密处理，对数据进行风险评估，并采用密码保护措施，同时记录审批信息以确保数据使用符合管理要求；在数据销毁过程中，要确保对物理层和数据层进行完整销毁，防止数据被恶意获取或恢复。

第二，采用基于人工智能的敏感信息识别措施。利用人工智能算法，研究在海量数据中自动识别敏感字段，在大数据环境中对敏感数据的自动推理等功能。

第三，严格遵守数据出境法律法规。对于重要出境数据，需要进行全流程安全评估，以确保数据安全性。

4.4 相关技术安全应对措施

第一，采用基于人工智能的切片异常检测措施。采用基于机器学习的人工智能技术，对网络切片进行异常检测，以识别存在的安全风险，并建立基于自适应阈值的切片异常和隔离失败检测技术，及时发现并应对切片中的安全风险，提高系统的安全性和可靠性。

第二，采用抗量子密码算法。随着量子计算技术的发展，传统的加密算法可能面临被破解的风险，需要研究并采用抗量子的加密方法，以保护通信和数据的安全。其中，有两个重要的方向值得关注：基于密钥封装技术的对称抗量子加密方法，这种方法通过将加密密钥与特定参数绑定，实现密钥的安全交换和保护；基于格理论密码学的认证方案，格理论提供了一种抗量子攻击的数学基础，可用于设计具有强安全性的认证方案。

5 结束语

在当前全球互联网日益复杂的环境下，卫星互联网的安全也面临挑战。随着技术的发展，安全威胁在不断变化和增加，未来的研究应该关注以下几个方面。首先，应加强对相关技术安全性的研究。随着人工智能、物联网等相关技术在卫星互联网中的应用，需要深入研究这些技术带来的潜在安全风险，并提出应对措施。其次，需加强国际合作与信息共享。卫星互联网的安全问题是全球性的，需要各国和利益相关方的合作与协调，建立信息共享机制和跨国合作平台，以便及时共享安全威胁情报和最佳实践。最后，还需持续关注和研究卫星互联网安全方面的法律法

规,以应对不断演变的安全风险,为卫星互联网的未来发展提供坚实基础。

参考文献:

- [1] 沈学民, 承楠, 周海波, 等. 空天地一体化网络技术: 探索与展望[J]. 物联网学报, 2020, 4(3): 3-19.
- SHEN X M, CHENG N, ZHOU H B, et al. Space-air-ground integrated networks: review and prospect[J]. Chinese Journal on Internet of Things, 2020, 4(3): 3-19.
- [2] 李风华, 殷丽华, 吴巍, 等. 天地一体化信息网络安全保障技术研究进展及发展趋势[J]. 通信学报, 2016, 37(11): 156-168.
- LI F H, YIN L H, WU W, et al. Research status and development trends of security assurance for space-ground integration information network[J]. Journal on Communications, 2016, 37(11): 156-168.
- [3] 王子剑, 杜欣军, 尹家伟, 等. 低轨卫星互联网发展与展望[J]. 电子技术应用, 2020, 46(7): 49-52.
- WANG Z J, DU X J, YIN J W, et al. Development and prospect of LEO satellite Internet[J]. Application of Electronic Technique, 2020, 46(7): 49-52.
- [4] 徐永太. 卫星通信技术研究[J]. 电信网技术, 2015(1): 52-57.
- XU Y T. Research on satellite communication technology[J]. Telecommunications Network Technology, 2015(1): 52-57.
- [5] 吕红伟, 吕金华, 张琦. 卫星互联网的安全威胁浅析[J]. 科学与信息化, 2021(5): 24-26.
- LYU H W, LYU J H, ZHANG Q. Analysis of security threat of satellite Internet[J]. Science and Informatization, 2021(5): 24-26.
- [6] 张聪, 高峰. 卫星互联网未来应用场景及安全性分析[J]. 信息技术, 2022, 46(3): 120-126.
- ZHANG C, GAO F. The future application scenarios and security analysis of satellite Internet[J]. Information Technology, 2022, 46(3): 120-126.
- [7] 张雪松. “军民融合”的西方剧本--从俄乌战争看商业通信卫星的军事应用[J]. 兵器, 2022(6): 26-33.
- ZHANG X S. The Western script of "civil-Military Integration" - The military application of commercial communication satellites from the Russia-Ukraine War[J]. Weapon, 2022(6): 26-33.
- [8] 左赛春, 曹世博, 王阳阳. 全球低地球轨道互联网卫星星座竞争格局与面临的挑战[J]. 中国航天, 2018(5): 42-45.
- ZUO S C, CAO S B, WANG Y Y. Competitive landscapes and challenges of LEO Internet satellite constellations[J]. Aerospace China, 2018(5): 42-45.
- [9] 汪永明. 卫星通信安全风险与防御技术概述[J]. 保密科学技术, 2022(6): 30-36.
- WANG Y M. Overview of satellite communication security risks and defense technologies[J]. Secrecy Science and Technology, 2022(6): 30-36.
- [10] CAO H, WU L L, CHEN Y, et al. Analysis on the security of satellite Internet[C]//China Cyber Security Annual Conference. Singapore: Springer, 2020: 193-205.
- [11] 丁阳, 窦长江. 卫星导航 RDSS 业务下行频谱干扰故障树判定方法[J]. 测绘科学与工程, 2015, 35(2): 5.
- DING Y, DOU C J. Fault tree determination method for downlink spectrum interference of satellite navigation RDSS service[J]. Geomatics Science and Engineering, 2015, 35(2): 5.
- [12] 未央. 卫星: 黑客攻击的下一个“前线”警惕! 黑客的“魔爪”已经伸到了“天上”![J]. 信息安全与通信保密, 2016, 14(1): 62-63.
- WEI Y. Satellite-the next “front line” of hacking! The hacker’s “talons” have reached the “sky”![J]. Information Security and Communications Privacy, 2016, 14(1): 62-63.
- [13] 常亮. “新基建”下的卫星互联网安全态势分析[J]. 中国信息安全, 2020(7): 47-48.
- CHANG L. Analysis of satellite Internet security situation under “new infrastructure”[J]. China Information Security, 2020(7): 47-48.
- [14] NIST. Report on post-quantum cryptography[R]. 2016.
- [15] 孙煜, 徐俊峰, 王勇, 等. 基于国密算法的北斗短报文加密方案[J]. 数据通信, 2022(2): 1-3.
- SUN Y, XU J F, WANG Y, et al. Encryption scheme of Beidou Short Messages Based on National Secret Algorithm[J]. Data Communications, 2022(2): 1-3.
- [16] 杨松楠. 卫星通信系统的星地一体对抗技术[J]. 电子技术与软件工程, 2021(8): 9-10.
- YANG S N. Satellite-ground integrated countermeasure technology in satellite communication system[J]. Electronic Technology & Software Engineering, 2021(8): 9-10.

[作者简介]



谷欣（1980—），男，硕士，中国星网网络创新研究院有限公司高级工程师，主要研究方向为卫星互联网安全架构、安全标准。



李珂（1974—），男，硕士，中电科网络安全科技股份有限公司工程师，主要研究方向为网络安全架构。



单超（1977—），男，博士，中国星网网络创新研究院有限公司高级工程师，主要研究方向为卫星互联网系统总体和网络架构技术。



田敏（1983—），女，硕士，中国星网网络创新研究院有限公司工程师，主要研究方向为网络安全。



孙才俊（1990—），男，博士，之江实验室助理研究员，主要研究方向为网络攻防、移动安全、内生安全。



王瑞青（1984—），女，硕士，中国星网网络创新研究院有限公司工程师，主要研究方向为网络安全、数据安全。