“星链”卫星安全防护技术分析与研究

刘　奎[1,2]，赵宇轩[2]，徐国庆[1,2]，黄宇轩[1,2]，孔巍巍[2]

（1. 上海航天智能计算技术重点实验室，上海 201109；

2. 上海航天电子技术研究所，上海 201109）

摘要：在持续爆发的俄乌冲突中，“星链”卫星在乌克兰的应用引起全世界的强烈关注，其在其它网络通信手段中断的情况下提供战场局势、保持上下级联络、指挥前沿阵地作战中发挥重大作用。但在作战中暴露的安全性问题和采用的安全防护技术同样值得分析和研究。本文通过调研分析“星链”卫星信息网络系统软硬件架构、抗网络攻击能力、抗电子干扰能力，综合评估其安全防护技术现状及发展趋势，为我国卫星在核心元器件、操作系统、星上软件等设计开发方面的安全防护技术发展提供借鉴与参考。

关键词：卫星；星链；信息网络系统；网络安全；电子干扰

0　背景

截止2023年9月，“星链”卫星发射数量已超过5000余颗[1-2]。凭借传输速率高、延迟短、覆盖范围广、卫星数量多、成本低、整体生存能力强等优势，已在北美、欧洲、大洋洲等地的25个国家正式运营，并在俄乌战争中大放异彩，成为乌境内特别是政府、军方及部分普通民众内外通信的重要手段[3-4]。

SpaceX公司2月底向乌克兰发送“星链”地面终端后，“星链”卫星也受到网络攻击与干扰。马斯克3月5日表示，在乌克兰冲突周边地区的“星链”服务一度堵塞“数小时”，但在SpaceX公司对“星链”软件进行更新升级后，“星链”运行恢复正常。因此，SpaceX将“重新优先考虑网络防御和克服信号干扰”问题。马斯克3月25日再次表示，“星链”在乌克兰“抵住了所有黑客和干扰尝试”[5-6]。

2022年3月，俄军利用“提拉达－2s”移动式地基卫星干扰系统对“星链”星座进行干扰，部分乌军

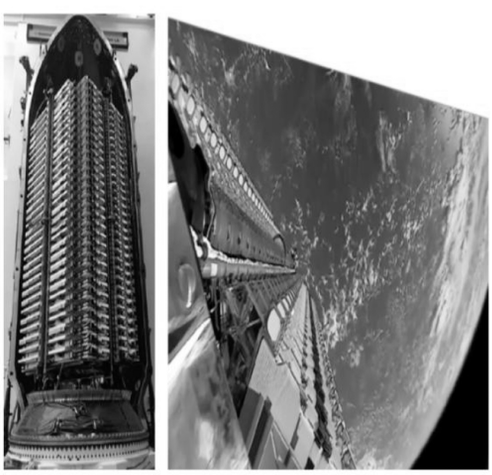

图1　“星链”航天器发射照片

图2　“星链”航天器遭网络攻击报道[6]

“星链”终端被堵塞干扰几个小时。虽然太空技术探索公司报道称通过及时更新软件成功修复星链，但是升级仍然造成“星链”通信的延迟。9月底，乌克兰上空“星链”系统再次出现故障，太空技术探索公司发出警告：“在乌克兰领土上将“星链”系统用于军事目的已不太可能。”相关专家认为，俄罗斯破解了“星链”系统程序代码，具备了对于情报截获与欺骗的能力[5-6]。

本文将从“星链”软硬件架构、抗电子干扰能力、抗网络攻击能力等方面进行研究，分析其安全防护技术的发展现状和未来趋势，为我国后续大规模建设的低轨卫星星座的安全防护技术提供参考。

1 “星链”信息网络系统软硬件架构

1）硬件级

CPU是计算机系统的基础和核心部件，决定了计算机本身的运算速度和数据处理能力。美国火星探测器上用的是IBM公司的RAD 6000，实际就是PowerPC系列。在一些大卫星上使用蓝宝石工艺的1750A，在一些小卫星领域，还会使用一些COTS器件，如工业级的386 EX。SpaceX公司自2019年5月启动组网发射以来，迄今已发射将数千颗“星链”组网卫星送入轨道，有资料显示卫星使用Sparc架构的SoC芯片，采用多级冗余提高可靠性。其引入低成本、工业化的芯片方案，大幅降低成本[2-4]。CPU复杂度极高，如IBM的power系列CPU的代码量已达到4000多万行，INTEL最新CPU的代码量也达到近6000万行。其中存在设计缺陷在所难免，因设计分工而引入的陷门也不可能彻底杜绝，主动隐匿复杂的后门功能也有充分的物质基础。

网络交换芯片是数据平面的承载核心，也是所有“星链”空间数据的汇聚中心，其本身的安全性至关重要。据资料显示，“星链”数据平台多采用赛林思Zynq系列芯片进行信息处理，虽说目前并无关于交换芯片器件漏洞导致的信息安全问题的相关报道，但是恶意厂商在交换机、路由器产品内植入恶意芯片、恶意代码的事件却屡见不鲜[7-8]。在航天领域，随着航天电子系统对运算性能、数据交换、数据传输需求的日益增加，交换芯片的广泛运用势在必行，因此发展信息安全交换技术是保障未来空间数据安全、防患于未然的必经之路。

2）操作系统级

SpaceX公司猎鹰火箭应用VxWorks和Linux，在龙飞船和地面设备大量应用实时加强的linux[9-11]。随着装备信息系统中计算机技术的快速发展，当敏感数据在武器系统中存储、处理、或传输时，原有的独立式、联合式计算机结构已不能够保护它们。它们已不能够满足现代复杂的军事和民用需求。计算机系统综合化后，在提高装备系统作战能力的同时，各子系统之间相互联网通信，资源高度共享、数据高度耦合、软件高度密集，同时也带来巨大的安全隐患。主要体现在：

① 由于资源高度共享，容易使其受到非法访问；

建立完整的资源访问控制技术，严格控制资源的访问权限，提高资源的安全性。

② 资源分布式缺乏有效管理；

系统资源分散在不同的系统之中，不同系统需要跨系统访问其他系统的资源对于目前来说还是有一定的难度。需要建立资源分布式管理的方法，有效整个分布式系统中各个资源，提高资源利用率。

③ 对于时间关键和安全关键的任务所需要的资源没有特别对待；

保证高级别任务及时高优先的获取资源的访问权限是建立安全可靠系统的关键之一。

④ 不同系统之间和系统内部之间不同安全等级的数据混杂传输，无法进行有效针对性的保护。

系统之间不同的数据传输有不同的安全要求，目前，对数据传输由于采用统一的数据传输方式，其数据之间无隔离，也没有区别对待。各个数据混杂在一个通道或链路中传输。不同安全等级的数据如果都采用高安全级别传输方式，则会造成开销浪费，如果都采用低安全等级的传输方式则无法保障高安全等级数据的安全[12]。以高效率通信手段，对不同安全级别的通讯数据进行隔离和分级保护是提高数据安全性和经济性急需的手段。

3）应用软件级

星上飞行控制系统软件的安全性问题是信息层面的问题，是通讯链路被物理介入，加密措施被破解失效或通过其他手段将后门、恶意代码等放置在飞行控制系统中引发的信息安全问题[13]。

飞行控制系统软件（由多个软件配置项和由软件定义的硬件联合组成）的安全性和健壮性是飞行器控制系统乃至飞行器平台设计和工程研制中要确保的首要问题之一。在过去，设计者面临的主要挑战是：

① 自主应对硬件系统的失效；

② 自主应对宇宙射线等环境应力造成的软件/数据错误；

③ 自主适应任务的变化（由环境摄动和地面指控共同构成的变化）。

2 “星链”抗电子干扰能力

“星链”卫星具备数量多、在低轨运行、电磁信号相对较强等优势。一方面，“星链”卫星具有对其他国家的军用卫星信号进行压制干扰甚至欺骗干扰的潜力，可用于降低对手卫星通信和卫星导航能力。另一方面，其部分地面站信号上传频谱范围与部分国家5G通信频谱接近/重叠，也可能导致部分国家的5G通信信号、其他近地轨道通信卫星的通信信道受到干扰。如果未来“星链”卫星上加装专用的电子战载荷，其太空电子战能力将显著增强，从而改变电磁频谱作战的形态和样式。

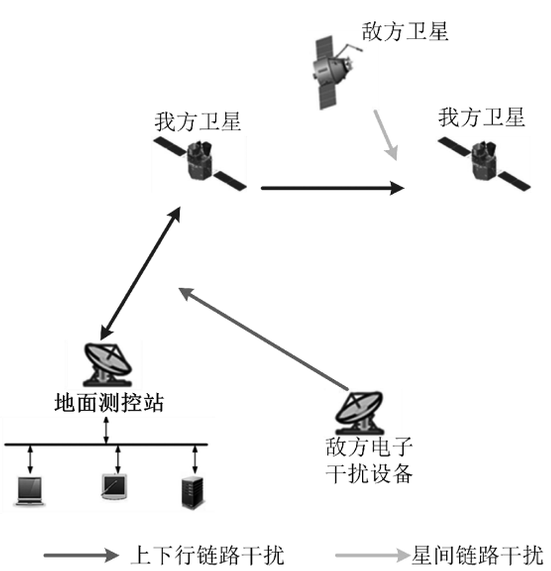

图3 卫星电子干扰主要途径

3 “星链”抗网络攻击能力

2022年2月24日俄乌冲突爆发前一小时，美国卫星运营商Viasat公司受到网络攻击，导致其曾被乌克兰军方频繁使用的KA-SAT卫星服务中断，乌境内数千名用户、欧洲其他国家数万名用户受到影响。而在SpaceX公司2月底向乌克兰发送“星链”地面终端后，“星链”卫星也受到网络攻击与干扰。马斯克3月5日表示，在乌克兰冲突周边地区的“星链”服务一度堵塞“数小时”，但在SpaceX公司对“星链”软件进行更新升级后，“星链”运行恢复正常。因此，SpaceX将“重新优先考虑网络防御和克服信号干扰”问题。马斯克3月25日再次表示，“星链”在乌克兰“抵住了所有黑客和干扰尝试”[4-6]。

SpaceX此次迅速、成功应对干扰的方式，对美军方造成强烈震动。美国国防部长办公室专门负责电子战的官员4月20日表示，在“星链”受到干扰的消息传出后第二天，SpaceX就“抛出一行代码并成功修复‘星链’”，使干扰突然失效，如果由美军来应对这一攻击行动将花费更长时间。该官员认为，美军电子战力量需要向SpaceX学习、拥有这种以（软件）升级方式快速应对新威胁的能力。从SpaceX此次快速、成功排除干扰以及美军的反应来看，美国高新技术企业在部分创新技术领域相对美军具备一定技术优势，并大大超出美军意料。

初步分析，美军有可能为SpaceX提供了俄军网络攻击手段、电子干扰能力、干扰频段与范围等情报资料，从而为SpaceX公司进一步加快卫星通信恢复速度、确保乌军战场指挥与通信能力提供了便利条件。

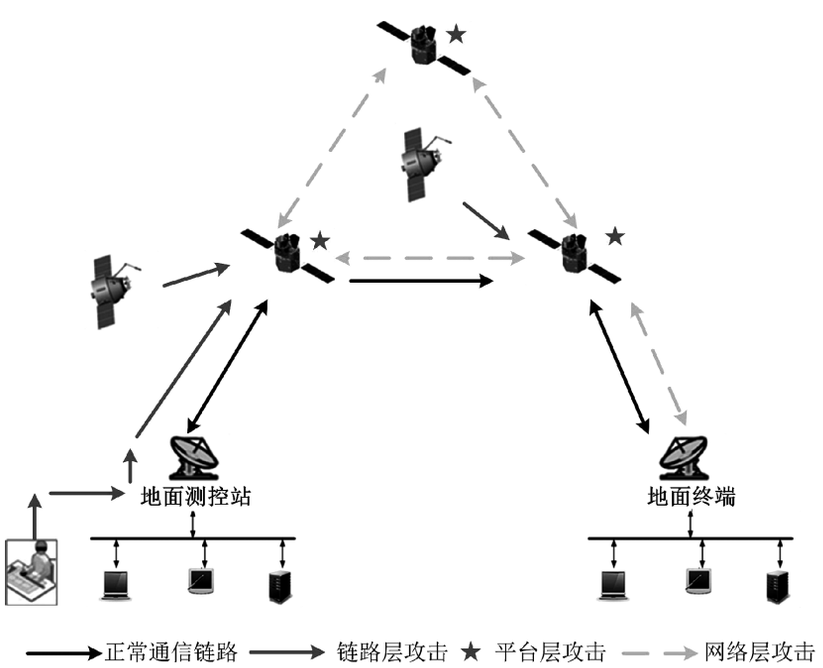

图4　卫星网络攻击主要途径

4 星链未来安全防护发展趋势

“星链”卫星具备数量多、在低轨运行、电磁信号相对较强等优势。一方面，“星链”卫星具有对其他国家的军用卫星信号进行压制干扰甚至欺骗干扰的潜力，可用于降低对手卫星通信和卫星导航能

力。另一方面，其部分地面站信号上传频谱范围与部分国家5G通信频谱接近/重叠，也可能导致部分国家的5G通信信号、其他近地轨道通信卫星的通信信道受到干扰。如果未来“星链”卫星上加装专用的电子战载荷，其太空电子战能力将显著增强，从而改变电磁频谱作战的形态和样式。

星间激光通信具有良好的通信隐蔽性和抗干扰性，由于目前不具备卫星间激光通信能力的1.0版本“星链”卫星仍占多数，卫星对位于其覆盖范围内的地面站网络接口依赖度高，对没有地面站的内陆、远海，尚不能实现全面覆盖。乌“星链”用户的上网应用，也需要通过波兰、立陶宛、土耳其境内地面站来实现网络接入。

对此，SpaceX公司采取的措施：一是加速推动卫星间激光通信，减少对地面站依赖。SpaceX把为“星链”加装卫星间激光通信设备作为发展关键，并最早应用于2021年1月发射的10颗极地轨道卫星，2021年9月后发射的1.5版本“星链”卫星则全部装备激光通信设备。二是增加卫星数量与覆盖范围。SpaceX公司采取以数量换质量策略，继续增加卫星数量，从而具备向同一地区多用户、高速率、大通量通信保障能力[13-14]。仅未来18个月该公司即计划再发射4200颗“星链”卫星。另外，SpaceX公司向美联邦通信管理局(FCC)提出申请，计划将用户天线最小可用仰角由原40°降为25°，从而扩大单颗卫星的通信服务覆盖范围。这是SpaceX公司在2.0版本卫星大量投入使用前，采取的临时性技术措施。

5 总结

通过对“星链”软硬件架构、抗电子干扰能力、抗网络攻击能力等方面进行研究可对我国卫星在核心元器件、操作系统、星上软件等方面的安全防护技术发展提供建议。

核心元器件方面，可开展可变结构执行体的设计技术研究。采用可变结构的设计技术，打破传统CPU系统架构中的静态性、相似性和确定性的现状，使得通过其上层的应用系统很难利用片上漏洞或陷门实现攻击之目的。为解决EDA工具链漏洞导致的信息安全问题，在IC设计、FPGA领域，配套国产自主研发器件制定专用化的EDA工具，是目前防范EDA工具链漏洞安全问题的一个解决途径。

操作系统方面，实现一种支持分布式资源管理、多级安全模式体系架构、对安全关键和时间关键任务的资源分级管理技术，实现资源安全隔离防护和访问控制和多安全等级的数据隔离传输。支持分布式资源访问、资源分级管理、资源安全隔离防护和访问控制技术，并对系统之间的传输数据进行分级隔离。克服空间环境影响造成的非法访问和空间网络信息系统中的安全隐患等。

星上软件方面，飞行控制系统软件信息安全设计技术、有利于信息安全的飞行控制系统软件架构设计技术、飞行器控制系统高可靠杀毒软件设计技术、多元信息融合的异常判别和隔离重构技术、硬件后门的测试识别技术、飞行控制系统软件信息安全的地面评测技术。建议采用在轨更换算法及密钥库的设计，提高在轨数据安全使用的可靠性和长寿命的需求。算法主要采用已通过相关资质认证的算法和密钥库，也可以考虑辅助采用国际通用的算法和生成相应的密钥库，通过上注通道进行在轨更新。

参 考 文 献

[1] 张煌，杜雁芸．“星链”军事化发展及其对全球战略稳定性的影响[J]．国际安全研究，2023，41(05)：157－158.

[2] 张睿健,颉靖,乔榕."星链"潜在威胁及网攻反制方法分析[J]. 中国电子科学研究院学报,2023,18(07):652-655.

[3] Smailes, Joshua, et al. "Dishing out DoS: How to Disable and Secure the Starlink User Terminal." arXiv preprint arXiv:2303.00582 (2023).

[4] 田丰."星盾":民用"星链"转身投军?[J]. 太空探索,2023(02):42-48.

[5] "星链"在俄乌冲突中的应用及启示[J]. 国防科技工业,2022(06):42-43.

[6] Rojas, Kevin M. Gonzalez. Threats to Satellite Cybersecurity in the 21 st Century. Diss. San Diego State University, 2023.

[7] 徐小涛,李建国,刘鹏."星链"卫星移动通信系统的发展现状及启示[J]. 国防科技,2022,43(02):15-19+117. DOI:10.13943/j.issn1671-4547.2022.02.03.

[8] 陈山. 俄"暗示"可能攻击"星链"卫星[N]. 环球时报,2022-09-21(008).

[9] 李元龙,李志强."星链计划"及其军事应用潜力研究[C]//中国指挥与控制学会(Chinese Institute of Command and Control). 第十届中国指挥控制大会论文集(上册). 兵器工业出版社,2022:85-91.

[10] 宋宇鸽,朱婕,程腾霄."星链"在俄乌冲突中的应用及未来军事发展分析[J]. 国际太空,2022(07):23-27.

[11] 何康,张洪忠. 从信息渠道到战略资源:俄乌冲突中星链卫星网络的功能跃升[J]. 湖南工业大学学报(社会科学版),2022,27(05):77-85.

[12] Topor, Sorin. "ELECTRONIC WARFARE-LESSONS LEARNED FROM RUSSIA'S ATTACK ON UKRAINE." Annals-Series on Military Sciences 15.1 (2023): 39-54.

[13] van Benthem, Tsvetelina J. "Privatized Frontlines: Private-Sector Contributions in Armed Conflict." 2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon). IEEE, 2023.

[14] Salkield, Edd, et al. "Satellite Spoofing from A to Z: On the Requirements of Satellite Downlink Overshadowing Attacks." Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks. 2023.

作者简介

姓名:刘奎,性别:男,出生年月:1993年12月,职务/职称:工程师,学历:博士研究生,研究方向:宇航计算机设计,工作单位:上海航天电子技术研究所,通信地址及邮编:上海市闵行区中春路1777号,邮编:201109,电子邮箱:liukui_804@163.com,联系电话:19921541535