doi:10.11959/j.issn.1000-436x.2016229

天地一体化信息网络安全保障技术研究进展及发展趋势

李凤华[1]，殷丽华[1]，吴巍[2]，张林杰[2]，史国振[3]
（1. 中国科学院信息工程研究所信息安全国家重点实验室，北京 100093；
2. 中国电子科技集团公司第五十四研究所，河北 石家庄 050000；3. 北京电子科技学院信息安全系，北京 100070）

摘 要：天地一体化信息网络由天基骨干网、天基接入网、地基节点网、地面互联网、移动通信网等多种异构网络互联融合而成，对实现国家安全战略目标具有重要意义。首先，介绍了天地一体化信息网络架构，以及卫星节点暴露、信道开放、异构网络互连等特征，并从物理层、运行层、数据层 3 个层面分析了天地一体化信息网络面临的威胁；其次，从物理安全、运行安全、数据安全 3 个层面对抗损毁、抗干扰、安全接入、安全路由、安全切换、安全传输、密钥管理等安全保障技术的研究现状进行了阐述；最后，针对天地一体化信息网络特点和安全保障需求，指出了天地一体化信息网络安全保障技术发展趋势和研究方向。

关键词：天地一体化信息网络；威胁；安全保障；安全架构
中图分类号：TP302 **文献标识码**：A

Research status and development trends of security assurance for space-ground integration information network

LI Feng-hua[1], YIN Li-hua[1], WU Wei[2], ZHANG Lin-jie[2], SHI Guo-zhen[3]
(1. State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China;
2. CETC 54, Shijiazhuang 050000, China;
3. Department of Information Security, Beijing Electronic Science and Technology Institute, Beijing 100070, China)

Abstract: Space-ground integration information network consists of space-based backbone network, space-based access network, the node net of foundation, Internet, mobile communication network, which has important significance for the realization of the target of national security strategy. Firstly, the characteristics of space-ground integration network, such as exposed channel, heterogeneous network integration, etc, were analyzed. Also, the corresponding threats from the physical layer, operation layer, data layer were introduced. Secondly, a comprehensive study on current status of survivability, anti-jamming, secure access, secure routing, secure handoff, secure transmission and key management were made. Finally, combined with research status, the important trends were proposed.

Key words: space-ground integration information network, threats, security assurance, security architecture

1 引言

随着卫星研制、火箭发射、运载、多星发射等各类技术的不断进步和应用，卫星网络迅速发展。借助于卫星网络，人类的“足迹”得以在太空的各个地方出现。同时，随着国家安全、航空航天、灾害预警等需求的不断增强，以及空间探索等任务的逐渐深入，各种战略信息任务在陆、海、空、天等不同维度空间不断开展，使原先相互独立的网络根据需要进行信息共享，实现跨地域、跨空域通信和网络各节点协同工作，这促使卫星网络进一步发展，并要求卫星网络与空间飞行器、地面网络等有

收稿日期：2016-08-24；**修回日期**：2016-09-27
通信作者：李凤华，lfh@iie.ac.cn
基金项目：国家重点研发计划基金资助项目（No.2016YFB0800303）；国家“核高基”科技重大专项基金资助项目（No.2015ZX01029101）
Foundation Items: The National Key Research and Development Program of China (No.2016YFB0800303), The National Science and Technology Major Project of China (No.2015ZX01029101)

机融合，形成天地一体化信息网络，从而更好地服务于国家安全和国计民生。

网络空间安全是反恐、社会服务和治理之基[1]，天地一体化信息网络安全作为其组成部分，重要性不言而喻。然而，天地一体化信息网络有别于传统网络，存在信道开放、拓扑高度动态变化、间歇链路等特征，面临着网络攻击、数据窃取等众多威胁和挑战，需研究具有针对性的抗损毁、抗干扰、防窃听、安全路由、安全切换、安全传输、安全接入和密钥管理等安全技术，构建天地一体化信息网络安全架构，以保障网络的安全运行。

2　天地一体化信息网络的特征及安全威胁

天地一体化信息网络由多种异构网络融合而成，由于其多维建设和卫星网络的特性，面临诸多安全威胁。

2.1　天地一体化信息网络架构

天地网络从架构层面划分，大致可以分为 3 类，1) 通过布设在全球的地面站实现网络的全球服务，天上卫星不进行网络组建的“天星地网”，如国际海事卫星组织管理的国际海事卫星通信系统（Inmarsat）等；2) 不依靠地面网络，仅通过天上卫星进行网络独立组建的“天基网络”，如美国的先进极高频卫星通信系统（AEHF）、民用低轨个人移动通信系统铱星系统（Iridium）等；3) 由地面网络和空间网络相互连接、融合，共同构成天地一体化信息网络的“天网地网”，如美国的转型卫星通信系统（TAST）计划等。其中，天网地网方式为未来天地网络架构的主要组网方式，因此，本文以“天网地网”作为天地网络的架构（即天地一体化信息网络），在此基础上对相关各类安全技术进行分析。

天地一体化信息网络由包括天基骨干网、天基接入网和地基节点网在内的天基网络、地面互联网、地面移动通信网等多种异构网络互联、融合而成，采用统一的技术体制和标准规范，如图 1 所示。

天基骨干网由若干个处于对地静止轨道（GEO, geostationary orbit）的高轨卫星节点联网组成，承担着网络中数据转发/分发、路由、数据传输等重要功能，可实现网络的全球、全时覆盖。

天基接入网由若干个处于高轨或低轨的卫星节点联网而成，包括高轨卫星移动接入网、低轨星座接入网等，为陆基、海基、空基、天基多维度用户提供网络接入服务。

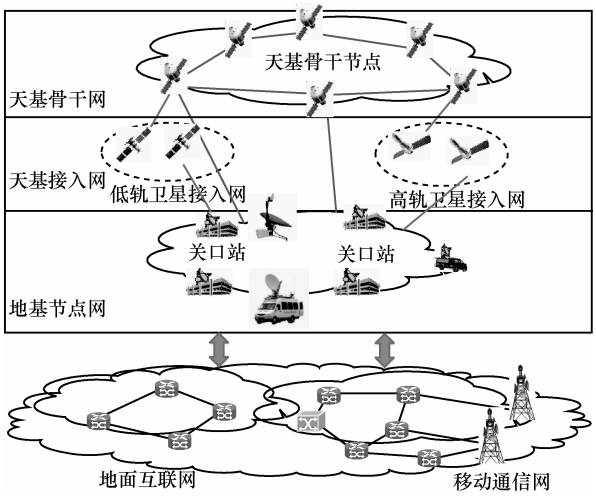


图 1　天地一体化信息网络示意

地基节点网由关口站、一体化网络互联节点等地基节点联网组成，主要实现对天基网络的控制管理、信息处理，以及天基网络与地面互联网、移动通信网等地面网络的互连等。

除天基骨干网、天基接入网、地基节点网之外，天地一体化信息网络还包括地面互联网、移动通信网等地面网络，主要为互联网用户提供接入卫星网络的服务等。

2.2　天地一体化信息网络特征

天地一体化信息网络跨陆、海、空、天的多层级建设以及天基网络的特殊性导致其具有卫星节点暴露、信道开放、异构网络互连、拓扑高度动态变化、传输高时延、时延大方差及星上处理能力受限等特点，因而面临诸多安全挑战。

1) 卫星节点暴露且信道开放。天地一体化信息网络中，卫星节点直接暴露于空间轨道上，长期处于恶劣的自然环境中，容易遭受非法截获、无意/蓄意干扰甚至摧毁。网络传输链路开放，且合理有效的物理保护手段缺失，造成星间、星地等链路极易受到恶意电磁信号、大气层电磁信号及宇宙射线等的干扰，并可能遭受恶意用户的窃听。

2) 异构网络互连且网络拓扑高度动态变化。天地一体化信息网络由涵盖陆、海、空、天在内的多种异构网络互联融合而成，导致对传统的路由、网络接入等的性能和安全性要求进一步提高，且存在军民共用的实际需求，需对不同安全等级的网络实施不同级别的防护，实施对各网络的互联控制，保证多级安全。天地一体化信息网络的节点包含卫星

节点、地面节点等多种类型，而卫星节点始终处于高速运转状态，可能频繁地加入或退出网络，导致网络拓扑时刻发生变化。拓扑的不断变化致使通信往返时延方差大，难以准确预测往返时延，造成不必要的数据重传。

3) 高时延、大方差、间歇链路。由于链路传输距离远长于传统地面网络，天地一体化信息网络中的数据传输存在高时延的问题。且由于卫星始终处于变化的恶劣自然环境中，如太阳黑子爆发、暴雨天气等，将导致链路的连通难以像传统网络一样保持时间连通性，进而造成通信时延极易大幅变化。此外，因卫星始终处于高速运动状态，加之地球的自转与公转，使星间通信无法长时间处于各自的信号覆盖范围内，进一步加大了通信链路持续保持的难度和通信时延抖动的幅度，因而，呈现连通间断性、时延方差大等特点。

4) 星上节点能力受限。受卫星有效载荷技术及太空自然恶劣环境等因素的影响，如功耗要求、宇宙射线等，卫星节点的计算、存储、带宽、物理空间等资源均受到较大限制，处理能力非常有限，在现有技术条件下卫星发射后，硬件层面几乎没有升级改造的可能，难以实现能力的有效扩展。一旦有非法用户接入卫星，并采用拒绝服务等方式对卫星进行攻击，其破坏效果将数倍强于对传统网络的攻击。

2.3 天地一体化信息网络面临的安全威胁

根据方等[2]提出的信息安全模型，信息安全包括物理安全、运行安全、数据安全、内容安全 4 个层面，结合天地一体化信息网络安全实际，以下主要从前 3 个层面对天地一体化信息网络面临的威胁展开论述。

2.3.1 物理层面的威胁

物理层面的安全主要针对系统的可用性和机密性等方面，天地一体化信息网络在这一层面面临的威胁主要包括物理损毁、信号干扰等。

物理损毁主要指对网络中卫星、地面站等基础设施的物理破坏。在太空环境下，诸多不可抗的自然因素，如太阳黑子爆发等突发性自然活动将对卫星等造成严重的威胁和破坏，影响网络的正常运转。不仅如此，由于天地一体化信息网络的重要性，卫星等设施还可能遭受反卫星武器的打击，特别是在军事领域，卫星等设施极有可能成为敌方首要打击的对象。除此之外，卫星自身的硬件系统发生的故障也可能造成网络的瘫痪。

信号干扰指传输链路信号受到人为或自然的电磁干扰。由于天地一体化信息网络处于复杂的电磁环境下，极易遭受恶意电磁信号、大气层电磁信号及宇宙射线等各类干扰，导致正常的数据传输受到影响甚至发生中断。目前，信号干扰技术主要包括欺骗干扰、压制干扰等。欺骗干扰技术指通过卫星信号转发、模拟伪造等方式使用户做出错误判断的干扰技术。抗欺骗干扰主要可通过角度鉴别、认证加密等方式进行。压制干扰技术指卫星信号被同频段大功率噪声干扰，导致信噪比降低从而使可用性降低或失去的干扰技术。相较于欺骗干扰抵御技术，压制干扰技术具有成本低廉、操作性强等特征。

2.3.2 运行层面的威胁

运行层面的安全主要针对系统运行的可控性、可用性等方面，天地一体化信息网络在接入、切换、访问等运行过程中面临的威胁主要包括欺骗攻击、恶意程序攻击等。

欺骗攻击指由于天地一体化信息网络中卫星节点的动态接入的特点，真实节点存在被冒充的可能，从而造成非法节点接入到天地一体化信息网络中，导致系统发生异常甚至瘫痪。

恶意程序攻击指通过利用天地一体化信息网络中可能存在的脆弱点、安全漏洞、无效配置等缺陷，在系统中植入病毒、木马等各类恶意代码或程序，从而造成系统被远程操控，最终造成天地一体化信息网络被破坏，后果严重。

2.3.3 数据层面的威胁

数据层面的安全主要针对数据在传输、处理等过程中的机密性、完整性等方面，天地一体化信息网络在路由、数据传输等运行过程中面临的威胁主要包括路由伪造/篡改、数据窃取等。

数据在路由过程中可能面临篡改攻击、伪造攻击等威胁。一方面，攻击者可能假冒合法节点加入网络，使原有合法节点的数据传递失常或数据被泄露；另一方面，攻击者可能伪造路由消息，在网络中恶意篡改路由，造成无效路由的产生，从而导致数据传输延时、传输开销等大幅增加，严重降低网络的性能。

与传统网络类似，天地一体化信息网络在数据传输过程中也面临 SYN 攻击、中间人攻击等各类威胁。除此之外，由于天地一体化信息网络高时延、大方差以及间歇链路等特性，致使数据传输可靠性较低，严重影响数据传输效率。

3　物理安全技术

物理安全[2]主要指对网络中物理装置或设备的防护。针对天地一体化信息网络物理安全的保障技术主要包括抗毁技术、抗干扰技术、人工噪声、多波束通信等。

3.1　抗毁技术

抗毁技术[3,4]指当卫星节点、通信链路等发生故障、面临人为无意、恶意攻击或遭受恶劣自然环境挑战时，网络维持自身功能的技术。目前的研究包括多站备份、优化网络结构等。

例如，张方明[5]针对 TDMA 卫星系统采用网状网络结构导致的对主站高度可靠性要求的问题，采用双主站的方式搭建 TDMA 主站，并采用主备间实时信号互检测方法实现异地备份和主备间在线热切换，保证了切换过程业务无感型，大幅提高了卫星通信系统的抗毁性和可靠性。董等[6]从空间网络架构的顽健性出发，将图论中自然连通度的概念引入空间网络以描述其抗毁性测度，在此基础上，提出一种基于免疫审查的优化人工免疫算法的空间网络结构设计方法，较大程度地提高了空间网络的抗毁性和健壮性。

3.2　抗干扰技术

现有针对卫星网络的干扰技术主要包括欺骗干扰和压制干扰等，对应的抵抗技术分别针对这 2 类技术。

在抗欺骗干扰方面，黄等[7]针对欺骗干扰的信号特征设计了一种适用于卫星导航接收机的抗欺骗干扰方法，该方法利用残留信号检测、到达角检测、电文加密认证检测及信号传输延迟检测等手段从信号体制设计与信号处理 2 个层面对欺骗进行识别，可直接用于 SNSS 接收机的设计。Fan 等[8]提出了一种抗欺骗攻击的跨层防御机制，该机制包含物理层和其他层 2 个层次的防护，其中，在物理层引入 GPS 载波噪声比（C/No，carrier-to-noise ratio）的概念，通过计算各接收器 C/No 的标准差，得到欺骗的先验概率，并嵌入计数器实现同步相量测量单元（PMU, phasor measurement unit）的识别；在其他层引入状态估计的检测方法，对欺骗攻击引起的坏数据注入进行动态检测，以识别欺骗的概率，提高了一对多同时攻击或一对一攻击的检测效率。韩雪谦[9]针对恶劣环境下卫星通信系统的单一抗干扰技术效果不佳的问题，提出了多域协同抗干扰技术，该技术利用凸集投影理论将时域、空域、频域的多种抗干扰技术进行融合，对各域的参数和变量进行统一处理，并设计了不同技术在域内/域间的切换机制，大幅增强了技术的抗干扰效果。

在抗压制干扰方面，最简单的抗击压制干扰的手段是提高卫星信号的发射功率，但由于星载系统的供电能力非常有限，致使该种技术效果不佳。可通过伪卫星技术、扩频技术来弥补上述缺陷。伪卫星技术[10,11]的主要优势在于其与用户距离远小于卫星与用户的距离，可将卫星信号强度增强数百倍，从而抵抗压制干扰。

除以上 2 类技术外，抗干扰技术还有扩频技术等。扩频技术通过对干扰信号进行“稀释”的手段达到抗干扰目的。Yang 等[12]通过设计了一种自适应接收天线，通过引入抗干扰矩阵技术将信号频带扩展，一定程度上提高了直序扩频信号的捕捉能力。

3.3　其他技术

其他针对卫星网络物理安全的技术研究还包括人工噪声、多波束通信等。

Goel 等[13]提出通过人工噪声（AN，artificial noise）的方式实施窃听反制，在确保原始信源质量不受影响的前提下通过在其冗余频段添加人为信号，干扰其解析真实信号能力，从而提高其窃听信道的疑义速率。Lei 等[14]设计了一种联合多波束和功率控制的物理层安全通信技术，利用迭代算法获取功率分配策略，并通过消除同信道干扰和窃听者信号趋零方式得到波束形成加权值，从而确保数据的保密传输率。Zheng 等[15]基于多波束通信和 AN 等技术，提出了一种最大化窃听者信道干扰率的防护策略，大幅增强了抗干扰效果。

4　运行安全技术

运行安全[2]主要指对网络的运行过程、状态等的保护。针对天地一体化信息网络运行安全的保障技术研究主要包括安全接入、安全切换、入侵检测、访问控制等。

4.1　安全接入

天地一体化信息网络星上节点能力受限、异构网络互连等特点使对节点接入的安全性、吞吐率等要求比传统网络接入更高。

Hwangt 等[16]针对移动卫星通信系统提出了一种用户接入认证方案，该方案使用对称加密方式，并使用集中式认证方式，通过链路加密传输认证信

息，既保证了接入安全，又降低了计算开销。Zheng 等[17]针对移动卫星通信网络提出了一种接入认证方案，该方案采用双向认证方式，强调认证网关的作用，并将 SOV 逻辑公理的概念引入网络控制中心（NCC）的设计，在保证防篡改、重放等攻击的同时，降低了身份认证的计算负载。Bayrakdar 等[18]提出了一种基于认知无线电的时隙 ALOHA 方案，其中主体用户在认证后利用 TDMA 技术接入信道，无线电用户采用时隙 ALOHA 技术随机接入空闲信道，大幅提高了信道利用率。House[19]将知识管理的概念引入卫星网络的接入过程，提高了网络对恶意终端的识别能力。肖等[20]从卫星网络信道固定分配导致其利用率低下的问题入手，提出一种基于认知无线电的信道接入策略，通过构建具有捕获效应和基于频谱感知的信道接入模型，获取认知用户的最佳频谱感知时间，从而接入空闲卫星信道，大幅提高低负载情况下卫星网络吞吐率。

现有卫星通信系统大多各自独立采用地面通信网的接入认证体制，未考虑天基组网时复杂异构多域互联场景的统一认证与互联控制，尤其在高低轨卫星系统互联组网时面临的长时延变化、间歇链路、多链路接入和复杂动态网络结构等场景下缺乏安全接入的考虑。

4.2 安全路由

鉴于天地一体化信息网络多种异构网络互联而成，在数据发送、转发、接收等过程中需安全高效的路由协议，以保证数据以最优路径实现安全传输。

Hou 等[21]提出一种高可靠性的路由算法，该算法利用时间感知的数据挖掘算法预测每个节点对联系的动态变化，并使用时空图模型进行拓扑的刻画，既降低了总链路开销，又保证了路由的可靠性。Yin 等[22]在考虑 3 层卫星网络体系架构的基础上，利用逻辑位置的概念对 LEO 和 HEO 卫星进行隔离区分，提出一种服务质量保证的安全多播路由协议，该协议采用非对称密码技术保护密钥预分发过程，并利用最低成本树构造 QoS 约束下的多播树构造，在保证安全的同时降低了端到端延时和多播连接失败率。Lu 等[23]设计了一种可以保证路由拓扑一致性的双层卫星网络的拓扑控制策略，并在此基础上将集中式和分布式路由策略相结合，提出了一种具有较强健壮性的路由协议，加强了路由与卫星节点失效的无关性，提高了路由的安全能力，并降低了路由延时。李等[24]结合卫星运动的可预知性特点，提出了一种针对卫星网络的基于安全机制的路由协议 SODV（satellite networks on-demand distance vector routing），该协议采取静态配置与动态调整相结合的策略，以较小开销实现路由的动态变化，并通过引入信任机制，以检测并响应网络中其他节点的恶意行为，实现部分攻击行为的防范，然而该协议未明确信任度量的时间，并可能出现高信任度的节点导致网络拥塞的情况。为此，潘等[25]综合考虑网络负载特性、节点利用率、信任值及跳数等条件，通过引入滑动窗口机制提出了一种信任评估模型，基于该模型对现有路由协议进行了安全性改进，设计了一种适用于卫星网络的按需安全路由协议，可实现多种常见内部行为的攻击的有效防范。杨等[26]设计了一种基于最小值的时间虚拟化策略，对卫星运行周期进行分割，避免了过短时间片所导致的难以完成路由无法收敛问题，在此基础上引入分层管理策略，并在各时间片开始获取链路状态信息，以进行路由计算与更新，降低了节点管理难度，从而提高了路由性能。Kuo 等[27]提出一种基于分布式的安全增强动态路由算法，该算法基于区域路由协议 ZRP 的思想，通过随机化分组传输过程和优化扩展的路由表，在增强数据传输的安全性的同时，可兼容包含 RIP 和 DSDV 协议的多数现有协议。Yu 等[28]提出了一种多层卫星网络安全路由协议，该协议利用卫星运行轨迹的可预见性，并引入信任机制和身份验证机制，进行节点历史行为的评估和信任值的动态调整，以及源和目的节点间的互认证，达到抵抗 DoS 攻击和端到端信息可靠传输的效果，同时利用时间戳、签名、路由维护等技术，可抗重放、自私行为和黑洞等攻击，并实现非正常节点的安全隔离。

由于天地一体化信息网络拓扑高度动态变化、节点处理能力有限等特点，现有方案多集中在降低链路开销、保证路由可靠性等方面，很少有方案将路由协议的安全性纳入考虑范畴。表 1 对现有相关安全路由研究工作进行了比较。

4.3 安全切换

天地一体化信息网络中节点相对位置不固定，网络一直处于高度动态变化状态，为保证节点间的不间断通信，需进行安全高效的网络切换机制。

徐等[29]提出了一种适用于卫星网络的安全切换机制，该机制使用上下文传递的方法，将包含切换节点标识、通信加密/认证算法及切换会话密钥等信息进行封装并预先发送给切换基站，同时，设置

表 1　　**现有相关安全路由研究工作对比**

路由方案	设计策略	是否跨层	是否按需	QoS 保障	安全性
文献[21]方案	基于时间感知的预测	否	否	一般	较低
文献[22]方案	基于逻辑位置	是	是	较高	较高
文献[23]方案	基于拓扑刻画/分层	是	否	一般	一般
文献[24]方案	基于信誉度	否	是	较低	较高
文献[25]方案	基于信任机制	否	是	较低	较高
文献[26]方案	基于时间虚拟化策略和分层管理	否	否	一般	一般
文献[27]方案	基于分布式路由信息	否	否	一般	较高
文献[28]方案	基于信任机制	是	是	一般	较高

了切换次数和切换时间的阈值，当超过该阈值时需重新进行接入认证，从而保证了切换的可靠性和安全性。He 等[30]提出了一种新型安全切换认证协议 PairHand，通过使用双线性加解密方式保障切换过程的安全，该方式仅需 MN（mobile node）和 AP（access point）间的握手操作，无需传输和验证证书信息，并设计了一个高效的批量签名验证方案，实现单个 AP 对多个签名的同时验证，既保证了切换验证的安全性，又降低了切换的计算和通信开销。孟等[31]针对 LEO（low earth orbit）卫星网络切换中频率高、切换点受限等问题，提出了一种安全高效的任意点切换方案，该方案通过记录已发生切换行为和上下文传递过程等内容，将历史信息引入安全上下文中，使切换后的密钥不会泄露以往会话密钥信息，确保了前向安全，并对切换过程中指令消息进行新鲜度和完整性保护，同时提供原地址证明，从而提高了切换过程的安全性。Korçak 等[32,33]从虚拟卫星节点入手，在研究卫星系统的通用虚拟拓扑和固定轨迹的基础上，设计了一种多态虚拟网络拓扑结构及其数学建模，基于该拓扑并首次利用回归算法处理定点低轨卫星网络的安全切换问题，提高了切换过程的流畅性。Deng 等[34]基于 WCDMA 系统软切换算法和借助位置信息计算的停留时间提出了一种针对 GEO 卫星通信系统的改良软切换算法，该算法通过对接收到的信号强度、终端的停留时间、所处位置与运行速度进行加权，基于该加权值进行切换频率的动态调整，有效降低了系统负担、切换次数及切换时延。Rahman 等[35]提出了一种适用于 LEO 卫星网络的自适应切换方案，该方案利用不同无线信道最大化频谱效率的变化调整资源分配策略，并通过将连接阻塞和下降概率保持在一个可接受水平来保证 QoS。Wu 等[36]利用 GPS 和卫星的多样性属性进行针对 LEO 卫星网络的简单实时切换算法的设计，该算法能有效减少卫星间切换次数。Zhang 等[37]提出了一种针对 LEO 卫星网络的具有预测机制的切换方案，该方案利用卫星网络的星历信息和移动终端上的 GPS 模块计算卫星的位置，提前对终端执行地址自动配置，并基于 SIGMA 机制预测终端的切换时间，降低了切换延迟和分组丢失率。Chen 等[38]从基于预留策略的自适应概率角度出发，设计了一种切换管理方案，利用终端位置信息和切换概率计算预留带宽，降低了新连接阻塞的概率，从而增强了切换的平滑性。

现有星间切换方案多从切换开销、切换时延等角度考虑对切换性能的优化，仅有部分方案利用签名、加密等技术对切换的安全性进行保障。表 2 对现有相关安全切换研究工作进行了比较。

4.4　其他技术

针对天地一体化信息网络运行安全的保障技术研究还包括入侵检测、访问控制等。

入侵检测[39]技术通过对天地一体化信息网络的内外部行为进行监控，在危害发生前及时拦截和响应入侵，从而保证系统的可控性、可用性、可确认性及稳定性。Zhang 等[40]根据卫星节点的功能特征，并基于登入登出机制对安全域进行划分，在此基础上设计了一个分层的分布式入侵检测模型，及安全域内/间的入侵检测代理协作机制，有效提高了入侵检测效率。关等[41]结合网络空间结构特性，并借鉴自组织网络的入侵防御技术，设计了一种入侵

表 2 现有相关安全切换研究工作对比

切换方案	切换方向	切换层次	切换策略	切换延迟	安全性
文献[29]方案	水平切换	网络层切换	基于上下文	较低	较高
文献[30]方案	水平切换	链路层切换	基于签密	一般	较高
文献[31]方案	水平切换	网络层切换	基于上下文和历史信息	较低	较高
文献[32,33]方案	水平切换	链路层切换	基于虚拟拓扑	较高	一般
文献[34]方案	垂直切换	链路层切换	基于位置信息	较高	较低
文献[35]方案	水平切换	网络层切换	基于频谱变化效率	较高	较低
文献[36]方案	水平切换	网络层切换	基于属性	一般	一般
文献[37]方案	水平切换	网络层切换	基于位置信息	较高	一般
文献[38]方案	水平切换	网络层切换	基于位置信息	较高	一般

检测系统，并提出了基于状态机的异常检测算法和跨层自适应黑洞攻击检测算法，通过基于 DSR 协议的状态机对节点进行实时监测，实现了对洪泛攻击、路由篡改攻击以及黑洞攻击等多种攻击类型的同时检测。

访问控制[42]的主要功能是允许合法用户访问和使用系统受保护的资源和服务，并防止非法用户的访问和合法用户的非法访问。封等[43]引入访问控制的连续性、主动性等概念，设计了一种适用于卫星网络的控制模型，该模型与基于角色、上下文的访问控制模型相结合，通过将动态的偏好知识应用于用户授权与访问过程，实现对用户的连续访问控制。Qi 等[44]基于 RBAC（role-based access control）模型和 ABAC（attribute-based access control）模型设计了一种分布式访问控制框架，通过 RBAC 模型管理静态属性，ABAC 模型管理动态属性，动态地添加用户—角色关系和角色—权限关系，同时提出了访问控制工作流模型，减少了角色和访问控制规则的数量，降低了管理的复杂性，并保证了访问控制的灵活性。

此外，天地一体化信息网络运行安全还应考虑全网统一安全管理、全网安全威胁态势感知与预警等技术。目前，在安全管理等方面，杨等[45]提出了一种针对微纳卫星的星载设备管理办法，可在卫星上自主完成设备的故障检测和管理等功能。在态势感知方面，国防科大研发了大规模网络安全态势分析 YHSAS 等系统[46]，实现了多维度实时的网络安全态势分析、基于特征事件序列频繁情节的网络安全态势预测等技术。然而，现有安全管理技术通常存在“各自为政”的问题，缺乏统一的管理体系，且由于天地一体化信息网络的时延大、间歇链路等独有特征，现有态势感知技术难以直接用于天地一体化信息网络，亟待进一步研究。

5 数据安全技术

数据安全[2]主要指对数据在收集、处理、传输等过程中的保护。针对天地一体化信息网络数据安全的保障技术研究主要包括安全传输、密钥管理等。

5.1 安全传输

天地一体化信息网络中端到端的传输需跨越多个异构网络，传输链路长，且存在大方差、高时延、星上处理能力受限等问题，为加强数据的机密性和可用性，需保证传输的可靠性、安全性等。

Yavuz 等[47]提出一种基于签密方案的卫星多播安全协议，该协议采用 N 层架构，将密钥更新带来的影响局部化，保证了前向和后向安全，大幅降低了带宽消耗和计算、存储开销，并采用分批生成密钥的方式，有效降低了卫星的工作负载，同时采用多方签密方案，提供了比传统单方签密方案更高的机密性、认证能力和不可抵赖性，适用于高安全性和高可靠性要求的大型卫星广播系统。张等[48]对传统 TCP 协议进行改进，提出了一种针对空间网络的可靠信息传输控制协议，该协议借鉴预处理和预先探测的思想，在保持原 TCP 首部格式和有限状态机不变的前提下对原 TCP 协议中慢启动、拥塞避免、快速重传及快速恢复等算法进行改进，既保证了传输的安全可靠，又大幅提高了传输性能。王等[49]提出了一种针对卫星网络的基于跳到跳信息的数

据传输控制协议，该协议使用异步逐跳确认重传机制，以快速恢复整段丢失的数据，并通过基于检测窗口的 SNACK（selective negative ACK）机制及时恢复上述重传逐跳机制无法恢复的数据，从而加强了卫星网络中数据传输的可靠性。Roy-Chowdhury 等[50]提出了一种针对混合卫星网络的性能感知的安全单播通信方案，该方案包含新型分层 IPSec 协议和双模 SSL（DSSL, dual-mode SSL）协议，其中新型分层 IPSec 协议通过对密钥交换协议 IKE 进行优化以生成分层 IPSec 协议所需的额外密钥得到，DSSL 协议通过在 SSL 协议中增加代理 SSL 字段以实现对 HTTP 代理服务器更好的支持，既实现了混合卫星网络中的端到端安全通信，提高了协议的安全性，又降低了传输时延。Roseti 等[51]对 IPSec 协议进行扩展，提出了一种跨层 IPSec 协议，该协议获取 UDP-lite 协议首部中的负载长度，并根据该长度为数据域的敏感部分提供安全服务，从而增强了数据的完整性保护。Zhang 等[52]设计并实现了一种适用于卫星网络的新型透明 TCP PEP 协议，该协议结合集中式 PEP 和分布式 PEP 性能增强代理实现，在保证安全性的同时显著提高了传输效率。Gulzar 等[53]在详细分析卫星网络中 TCP PEPs 和 IPSec 协议冲突的本质原因，通过区分 PEPs 可信度提出了完全可信 PEPs、半可信 PEPs 和不可信 PEPs 3 种不同的方式进行 PEPs 能力和 IPSec 方式的分配，以使该 2 种协议共存，提供了数据传输安全性和传输性能的不同权衡。Sun[54]等提出了一种适用于卫星网络的增强型端对端 TFRC 协议，该协议使用微分算法 LDA，通过计算基于 RTT 测量的等候延时进行分组丢失区分，避免传统 TFRC 协议的错误分类，可更精确地计算损失事件率，从而以更合适的速率发送数据，在保证提高数据传输可靠性的同时，显著提高瓶颈链路利用率。然而，该协议比传统 TFRC 协议的收敛事件长。Pradhan 等[55]提出一种卫星集群环境下的安全传输机制，该机制通过使用格标签来表示安全分类和实施多级安全(MLS)策略，以确保严格的信息分区，在此基础上，设计了一种新型发现服务系统，该系统通过 OpenDDS 扩展集中式发现服务，实现实体授权，保证了传输安全。

现有的传输协议包括 SCPS、空间 IP 改进协议等，安全传输主要基于对传统的 TCP 和 IPSec 协议的改进等方式实现。已有卫星系统大多采用链路加密机制保护星地链路的数据传输安全，实现了遥测数据加密和部分数传加密，民用卫星通信一般采用 IP 机密技术体制，实现卫星通信的端到端加密。

5.2　密钥管理

密钥管理是实现天地一体化信息网络一系列安全手段的重要基础。目前，密钥管理的研究一般从提高密钥的灵活性、安全性等方面展开。

罗等[56]提出了一种空间网络中基于身份的组密钥管理方案，该方案使用公钥密码体制进行组成员密钥协商，由卫星节点组成动态可调整的动态服务节点集合，辅助群组公共参数与密钥参数的生成、更新及广播操作，解决了组成员计算、存储和通信等开销失衡的问题，避免了由单个服务节点故障、离线导致的单点失效问题，从而保证了较高的安全性。针对网络空间中 1-affect-*n* 问题，Zhou 等[57]基于一对多加密机制，提出了一种一对多映射的密钥协商协议，使网络中成员的加入或退出只需更新该成员的解密密钥和公共加密密钥，实现了网络中各实体之间私钥的无关性，保证了安全性的同时，也提高了密钥管理方案的效率和灵活性。针对原有卫星网络管理协议中密钥更新由地面测控站依次进行易导致的单点失效问题，周等[58]提出一种针对卫星网的分层式组密钥管理方案，该方案采用层簇式结构，以高轨卫星作为密钥协商树的根节点，各组成员根据三叉密钥树自主进行密钥树计算，有效减少协商过程的通信开销，并将身份认证机制和双线性对引入密钥协商过程，进一步提高了方案安全性。Jiao 等[59]提出了一种基于阈值技术的卫星网络组密钥管理方案，该方案利用椭圆曲线密码技术带认证功能的优势，无需建立安全信道，并独立于第三方，通过使用阈值机制提高系统健壮性，避免了单点失效问题，同时在发送处理过程中认证组共享密钥，加强了常见攻击行为的抵抗能力，从而进一步提高了安全性。Wang 等[60]基于网络分层、多域等特征提出了一种新型组密钥管理方案，该方案采用代理重加密技术，并限定核心骨干网络节点只参与新的组密钥分配，不能获得新的组密钥，解决了单点故障问题，同时对网络中成员关系的变化所带来的影响进行了限制，提高了密钥管理方案的可伸缩性。Sun 等[61]提出了一种卫星多群组密钥管理方案，该方案根据用户的访问能力对其进行分组，并将子组控制器密钥作为叶节点，管理数据密钥作为根节点，通过二叉树的方式将上述节点连接，并合并相同的部分，基于此进行多组密钥管理图的构

建，在满足前向/后向安全的同时，大幅减少了存储和通信开销。Elmasri 等[62]设计了一种针对战术卫星的高性能组密钥管理算法，该算法要求卫星终端参与组密钥管理，使用密钥管理器认证终端操作，并通过证书验证证书共享机制有效降低时间开销，以防止在对抗过程中静止的卫星终端的位置不发生变化，从而防止终端被敌方窃取。Hu 等[63]根据传输速率、可移动性、资源限制等条件对空间网络中的元素进行分类，基于该分类将空间网络划分为卫星—空间传感器网络、空间传感器—地面传感器网络、地基节点网络等，针对各网络特性提出了各自的密钥管理方案，实现了适应各网络的高效密钥管理方案。

现有关于天地一体化信息网络中密钥管理方案主要可分为集中式、分布式、集中式与分布式结合 3 种类型，多数方案在考虑计算、存储、通信开销的同时，会考虑抗单点失效的问题，但多数方案存在可扩展性一般的问题。表 3 对现有相关密钥管理研究工作进行了比较。

6 结束语

本文针对天地一体化信息网络中卫星节点暴露且信道开放、异构网络互连、网络拓扑高度动态变化、传输高时延、时延方差大、链路间歇性、星上节点处理能力受限等独有特点，并阐述了各特点对网络带来的安全威胁。在此基础上，从物理安全、运行安全、数据安全等 3 个层面对目前天地一体化信息网络中相关安全技术的国内外研究现状进行了分析。现有天地一体化的研究多针对单一卫星网络展开，为了实现今后天地网络的真正完全融合，应开展天地一体化信息网络安全架构研究，如图 2 所示。在研究物理安全、运行安全、数据安全等技术的基础上，进一步对威胁感知与联动管控技术、安全仿真验证技术展开研究，实现天地一体化信息

表 3　现有相关密钥管理研究工作对比

密钥管理方案	计算开销			通信开销			存储开销	可扩展性	抗单点失效
	密钥协商	成员加入	成员离开	密钥协商	成员加入	成员离开			
文献[59]	–	$tP+M$	$tP+M$	–	$2n+1$	$n+1$	–	一般	是
文献[61]	–	–	–	–	–	–	–	较高	是
文献[62]	–	–	–		$5n$-4		–	一般	否
文献[56]	$(2+\log n)M+(1+\log n)P$	$(2n+2)(M+P)$	$(2n-\log n)(M+P)$	$3n-1$	$\log n+3$	$\log n-1$	$1+2\log n$	一般	是
文献[58]	$(n\log k+8n-2)M+(n\log k+n-2)P$	$(3k+8)M+(k\log k+\frac{11}{2}k+\frac{3}{2})P$	$3kM+(k\log k\frac{11}{2}k-2\log k-\frac{19}{2})P$	n	2	2	–	一般	否
文献[60]	–	–	–	–	$2+\log n$	$2\log n$	$\log n+1$	较高	是

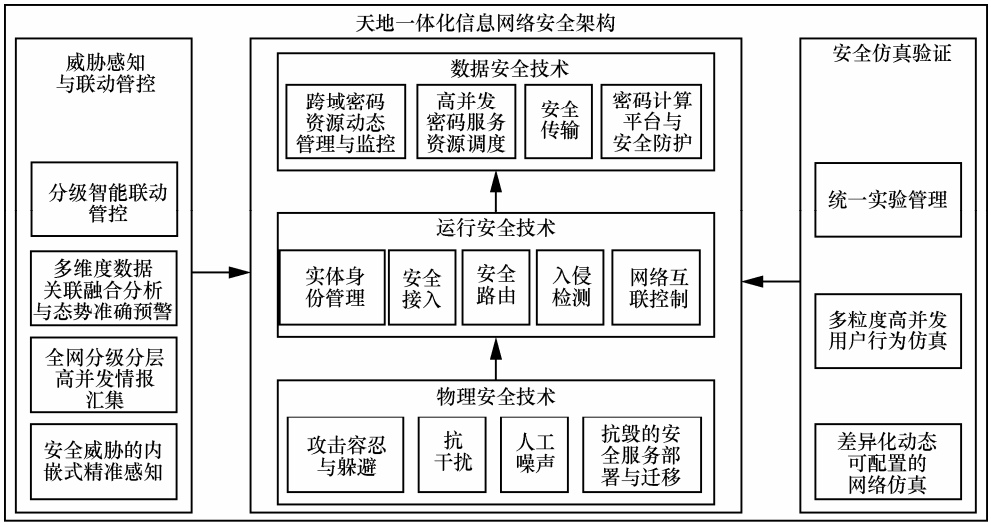


图 2　天地一体化信息网络安全架构

网络安全的全面保护。具体研究内容如下。

1) 物理安全。针对天地一体化信息网络面临的各种攻击技术不断增强的特点，在抗损毁、抗干扰、人工噪声等技术研究基础上，需从提高攻击容忍能力和躲避能力等角度出发，以多攻击源、攻击长时持续等为切入点，研究多源持续攻击容忍与躲避、节点自动失效隔离技术；探讨威胁态势与网络服务能力的关系，设计基于威胁态势的服务能力调整方法，研究抗毁的安全服务快速部署与迁移等。

2) 运行安全。针对天地一体化信息网络实体类型多、终端规模大、属性状态变化、低轨星座网络拓扑高动态变化、星际链路速度快频率高、网络中断多模并存等特点，研究大规模实体统一身份及权限管理、高轨卫星组网实体认证及可信保持、低轨星座动态组网认证与控制、终端多域协同接入鉴权与安全漫游、随遇安全接入与无缝安全切换等技术；未来天地一体化信息网络的复杂异构多域互联场景，需从多安全域、多安全等级等角度出发，针对一体化网络安全威胁多样化、空间节点自身防护不足等特点，研究联动防护的智能控制与管理、支持网络动态扩建的互联安全控制与重构、资源受限下的域间路由与拓扑隐藏、抗隐蔽通道的高速实时隔离交换等技术。

3) 数据安全。针对天地一体化信息网络设备类型多、密码资源多、分区分域复杂、行政管理归属复杂等特点，研究跨域密码资源动态管理与监控方法，具体包括域内域间密码资源动态分发与参数配置、密码算法与协议重构策略、密码计算动态调度等。针对天地一体化信息网络因为动态扩展、亿级终端数量等特点，研究高并发密码服务资源调度方法，具体包括密码计算资源虚拟化、密码服务高并发调度、亿级密钥管理、密码作业服务管理与迁移等。针对密码计算平台高效运行、资源可重构以及安全防护等需求，研究密码计算平台与安全防护技术，具体包括密码计算平台高效管理机制、密码算法快速切换、密码算法动态重构等。

4) 威胁感知与联动管控。针对星上/终端计算能力受限导致难以实现威胁的精准感知，研究安全威胁的内嵌式精准感知技术，具体包括威胁指数动态度量、资源受限下威胁驱动的动态组合采集、威胁信息联动分析等。鉴于卫星链路带宽资源有限，针对威胁数据传输时带宽占用受限的问题，研究全网分级分层高并发情报汇集技术，具体包括威胁信息归一化描述、数据智能压缩与消冗、数据差分传输控制、传输时机与传输链路优化调度等。针对一体化网络安全威胁种类多、语义关系复杂等特点，研究多维度数据关联融合分析与态势准确预警技术，具体包括威胁态势要素提取、多维度数据融合分析、异构威胁信息逐级关联发现、多层次多维度威胁情报综合研判与智能预测等。针对天地一体化信息网络亿级终端、脆弱点分布广等特点，研究分级智能联动管控技术，具体包括联动管控策略生成与智能选取、采集命令/控制命令细粒度分级分解、联动处置范围优化确定、基于效果反馈的处置命令智能调整、安全威胁实时阻断等。

5) 安全仿真验证。针对天地一体化网拓扑持续变化、网元类型多、差异大等特点，研究差异化动态可配置的网络仿真方法，具体包括多类型实体高逼真模拟算法、高性能大规模模拟器设计方法、模拟器按需动态配置机制、安全协议嵌入技术等。针对用户种类多、行为多样化、业务流量大、事件高并发等特征，研究多粒度高并发用户行为仿真技术，具体包括高并发流量发生器构造、高逼真用户行为仿真、多粒度仿真协同、用户行为实时加载等。针对安全测试任务复杂多样、联合仿真环境动态部署等特点/需求，研究统一实验管理方法，具体包括仿真模型按需配置管理、安全能力综合评估分析、基于测试任务的实验预案生成等。

参考文献：

[1] 李凤华. 信息技术与网络空间安全发展趋势[J]. 网络与信息安全学报, 2016, 1(1): 8-17.
LI F H. Development trends of the information technology and cyberspace security[J]. Chinese Journal of Network and Information Security, 2016, 1(1): 8-17.

[2] 方滨兴, 殷丽华. 关于信息安全定义的研究[J]. 信息网络安全, 2008 (1): 8-10.
FANG B X, YIN L H. Research on the definition of information security[J]. Netinfo Security, 2008 (1): 8-10.

[3] CLEMENT D M, JOHNSON A W. Satellite survivability estimates[J]. IEEE Transactions on Nuclear Science, 1981, 28(6): 4198-4203.

[4] SEGNER S M, GIORDANO F A. Surrogate satellite applications and survivability[C]//Military Communications Conference, 1984. MILCOM 1984. IEEE. IEEE, 1984, 2: 267-270.

[5] 张方明. 一种基于信号互检测的 TDMA 系统主站热备份方法[J]. 电子技术与软件工程, 2016, 13: 47-48.
ZHANG F M. A hot backup method for TDMA system master station based on signal mutual detection[J]. Electronic Technology & Soft-

ware Engineering, 2016, 13:47-48.

[6] 董飞鸿, 吕晶, 巩向武,等. 空间信息网络结构抗毁性优化设计[J]. 通信学报, 2014, 35(10): 50-58.
DONG F H, LYV J, GONG X W, et al. Optimization design of structure invulnerability in space information network[J]. Journal on Communications, 2014, 35: 50-58.

[7] 黄龙, 唐小妹, 王飞雪. 卫星导航接收机抗欺骗干扰方法研究[J]. 武汉大学学报: 信息科学版, 2011, 36(11): 1344-1347.
HUANG L, TANG X M, WANG F X. Anti-spoofing techniques for GNSS receiver[J]. Geomatics and Information Science of Wuhan University, 2011, 36(11): 1344-1347.

[8] FAN Y, ZHANG Z, TRINKLE M, et al. A cross-layer defense mechanism against GPS spoofing attacks on PMUs in smart grids[J]. IEEE Transactions on Smart Grid, 2015, 6(6): 2659-2668.

[9] 韩雪谦. 卫星通信系统多域协同抗干扰技术[J]. 现代雷达, 2016, 38(5): 78-81.
HAN X Q. Multi-domain collaborative anti-jamming technique for satellite communication system[J]. Modern Radar, 2016, 38(5): 78-81.

[10] DAI L, RIZOS C, WANG J. The role of pseudo-satellite signals in precise GPS-based positioning[J]. Journal of Geospatial Engineering, 2001, 3(1): 33-44.

[11] GREJNER-BRZEZINSKA D A, TOTH C K, SUN H, et al. A robust solution to high-accuracy geolocation: quadruple integration of GPS, IMU, pseudolite, and terrestrial laser scanning[J]. IEEE Transactions on Instrumentation and Measurement, 2011, 60(11): 3694-3708.

[12] YANG G, YANG X. Design of adaptive anti-jamming antennas of direct sequence spread spectrum receiver[C]//The 2012 Second International Conference on Electric Technology and Civil Engineering. IEEE Computer Society, 2012: 846-849.

[13] GOEL S, NEGI R. Guaranteeing secrecy using artificial noise[J]. IEEE Transactions on Wireless Communications, 2008, 7(6): 2180-2189.

[14] YANG G, YANG X. Design of adaptive anti-jamming antennas of direct sequence spread spectrum receiver[C]//The 2012 Second International Conference on Electric Technology and Civil Engineering. IEEE Computer Society, 2012: 846-849.

[15] ZHENG G, ARAPOGLOU P D, OTTERSTEN B. Physical layer security in multibeam satellite systems[J]. IEEE Transactions on wireless communications, 2012, 11(2): 852-863.

[16] HWANG M S, YANG C C, SHIU C Y. An authentication scheme for mobile satellite communication systems[J]. ACM SIGOPS Operating Systems Review, 2003, 37(4): 42-47.

[17] ZHENG G, MA H T, CHENG C, et al. Design and logical analysis on the access authentication scheme for satellite mobile communication networks[J]. IET Information Security, 2012, 6(1): 6-13.

[18] BAYRAKDAR M E, ATMACA S, Karahan A. A slotted Aloha based random access cognitive radio network and its performance evaluation[C]//Software, Telecommunications and Computer Networks (SoftCOM), 2012 20th International Conference. IEEE, 2012: 1-5.

[19] HOUSE T C. Client\server access: satellite-ATM connectivity using a knowledge management approach[C]//International Conference on Information Technology: New Generations. 2007:863-867.

[20] 肖楠, 梁俊, 张衡阳, 等. 一种基于认知无线电的卫星网络信道接入策略[J]. 宇航学报, 2015, 36(5): 589-595.
XIAO N, LIANG J, ZHANG H Y, et al. A channel access strategy based on cognitive radio for satellite communication network[J]. Journal of Astronautics, 2015, 36(5): 589-595.

[21] HOU W, XIAN B, GUO L, et al. Novel routing algorithms in space information networks based on timeliness-aware data mining and time-space graph[C]//Wireless Communications & Signal Processing (WCSP), 2015 International Conference. IEEE, 2015: 1-5.

[22] YIN Z, ZHANG L, ZHOU X, et al. Qo-guaranteed secure multicast routing protocol for satellite IP networks using hierarchical architecture[J]. Int'l J. of Communications, Network and System Sciences, 2010, 3(04): 355.

[23] LU Y, ZHAO Y, SUN F, et al. A survivable routing protocol for two-layered LEO/MEO satellite networks[J]. Wireless Networks, 2014, 20(5): 871-887.

[24] 李喆, 刘军. 卫星网络安全路由研究[J]. 通信学报, 2006, 27(8): 113-118.
LI Z, LIU J. Research on secure routing algorithm in satellite networks[J]. Journal on Communications, 2006, 27(8): 113-118.

[25] 潘艳辉, 王韬, 吴杨, 等. 基于信任的低地球轨道卫星网络路由安全机制[J]. 计算机工程, 2011, 37(20): 149-151.
PAN Y H, WANG T, WU Y, et al. Route security mechanism based on trust for low earth orbit satellite network[J]. Computer Engineering, 2010, 37(20): 149-151.

[26] 杨力, 杨校春, 潘成胜. 一种 GEO/LEO 双层卫星网络路由算法及仿真研究[J]. 宇航学报, 2012, 33(10): 1445-1452.
YANG L, YANG X C, PAN C S, et al. A GEO /LEO double-layered satellite network routing algorithm and its simulation[J]. Journal of Astronautics, 2012, 33(10): 1445-1452.

[27] KUO C F, PANG A C, CHAN S K. Dynamic routing with security considerations[J]. IEEE Transactions on Parallel and Distributed Systems, 2009, 20(1): 48-58.

[28] YU Z, ZHOU H, WU Z. A trust-based secure routing protocol for multi-layered satellite networks[C]//2012 IEEE International Conference on Information Science and Technology. IEEE, 2012: 313-317.

[29] 徐国愚, 陈性元, 杜学绘. 一种新的基于上下文传递的临近空间安全切换机制[J]. 计算机科学, 2013, 40(4): 160-163.
XU G Y, CHEN X Y, DU X H, et al. New near space security handoff scheme based on content transfer[J]. Computer Science, 2013, 40(4): 160-163.

[30] HE D, CHEN C, CHAN S, et al. Secure and efficient handover authentication based on bilinear pairing functions[J]. IEEE Transactions on Wireless Communications, 2012, 11(1): 48-53.

[31] 孟梦, 陈性元, 徐国愚, 等. 一种安全高效的 LEO 卫星网络任意点切换方案[J]. 计算机工程, 2015, 41(3): 1-6.
MENG M, CHEN X Y, XU G Y, et al. A secure and efficient LEO satellite network switching scheme at any point[J]. Computer Engineer-

ing, 2015, 41(3): 1-6.

[32] KORCAK O, ALAGOZ F. Virtual topology dynamics and handover mechanisms in earth-fixed LEO satellite systems[J]. Computer Networks, 2009, 53(9): 1497-1511.

[33] KORCAK O, ALAGOZ F. Link-layer handover in earth-fixed LEO satellite systems[C]//2009 IEEE International Conference on Communications. IEEE, 2009: 1-5.

[34] DENG Z, LONG B, LIN W, et al. GEO satellite communications system soft handover algorithm based on residence time[C]//Computer Science and Network Technology (ICCSNT), 2013 3rd International Conference on IEEE, 2013: 834-838.

[35] RAHMAN M, WALINGO T, TAKAWIRA F. Adaptive handover scheme for LEO satellite communication system[C]//AFRICON, 2015. IEEE, 2015: 1-5.

[36] ZHAOFENG W, GUYU H, SEYEDI Y, et al. A simple real-time handover management in the mobile satellite communication networks[C]//Network Operations and Management Symposium (APNOMS), 2015 17th Asia-Pacific. IEEE, 2015: 175-179.

[37] ZHANG Z, GUO Q, GAO Z. A prediction based SCTP handover scheme for ip/leo satellite network[C]//2010 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM). IEEE, 2010: 1-4.

[38] CHEN L M, GUO Q, WANG H Y. A handover management scheme based on adaptive probabilistic resource reservation for multimedia LEO satellite networks[C]//Information Engineering (ICIE), 2010 WASE International Conference. IEEE, 2010, 1: 255-259.

[39] ANDERSON J P. Computer security threat monitoring and surveillance[R]. Technical Report, James P. Anderson Company, Fort Washington, Pennsylvania, 1980.

[40] WEN-BO Z, PEIGEN S, ZHI-GUO L, et al. An intrusion detection model for satellite network[C]//Information Management and Engineering (ICIME), 2010 The 2nd IEEE International Conference. IEEE, 2010: 167-170.

[41] 关汉男. 基于 LEO 的空间网络安全体系及关键技术研究[D]. 上海交通大学, 2014.
GUAN H N. Research on key security technologies in LEO-based space network[D]. Shanghai Jiao Tong University, 2014

[42] 李凤华, 熊金波. 复杂网络环境下访问控制技术[M]. 北京:人民邮电出版社, 2015.
LI F H, XIONG J B. Access control technology for complex network environment[M]. Beijing: Posts & Telecom Press, 2015

[43] 封孝生, 刘德生, 乐俊, 等. 临近空间信息资源访问控制策略初探[J]. 计算机应用研究, 2008, 25(12): 3702-3704.
FENG X S, LIU D S, YUE J, et al. Exploration on access control to near space information resources [J]. Application Research of Computers, 2008, 25(12): 3702-3704.

[44] QI H, MA H, LI J, et al. Access control model based on role and attribute and its applications on space-ground integration networks[C]// 2015 4th International Conference on Computer Science and Network Technology (ICCSNT). IEEE, 2015, 1: 1118-1122.

[45] 杨磊, 刘鹏飞, 赵勇,等. 微纳卫星星载设备管理方法[J]. 仪器仪表学报, 2014(s2): 141-145.
YANG L, LIU P F, ZHAO Y, et al. Equipment management of nano-satellite[J]. Chinese Journal of Scientific Instrument, 2014(s2) : 141-145.

[46] HAN W H, WANG Q G. Security situation analysis and prediction system for large-scale network SSAP[C]//Computing and Convergence Technology (ICCCT), 2012 7th International Conference. IEEE, 2012: 1125-1129.

[47] YAVUZ A A, ALAGZ F, ANARIM E. SAT05-6: NAMEPS: *n*-tier satellite multicast security protocol based on signcryption schemes[C]//IEEE Globecom 2006. IEEE, 2006: 1-6.

[48] 张民, 罗光春, 王俊峰, 等. 空间信息网络可靠传输协议研究[J]. 通信学报, 2008, 29(6): 63-68.
ZHANG M, LUO G C, WANG J F, et al. Reliable transmission control protocol for spatial information networks[J]. Journal on Communications, 2008, 29(6): 63-68.

[49] 王路, 胡月梅, 刘立祥, 等. 基于跳到跳信息的卫星网络传输控制协议研究[J]. 通信学报, 2012, 33(6): 91-102.
WANG L, HU Y M, LIU L X, et al. Transmission control protocol based on hop-by-hop for satellite networks[J]. Journal on Communications, 2012, 33(6): 91-102.

[50] ROY-CHOWDHURY A, BARAS J S. Performance-aware security of unicast communication in hybrid satellite networks[C]//2009 IEEE International Conference on Communications. IEEE, 2009: 1-6.

[51] ROSETI C, LUGLIO M, PROVENZANO S, et al. A cross-layer architecture for satellite network security: CL-IPsec[C]//2008 4th Advanced Satellite Mobile Systems. IEEE, 2008: 82-87.

[52] ZHANG Y, PENG H, GU J. Design and implementation of a TCP performance enhancement gateway for satellite networks[C]// Communications and Intelligence Information Security (ICCIIS), 2010 International Conference. IEEE, 2010: 252-255.

[53] GULZAR W A, KHAN Z A, NAWAZ R. Implementation of IPsec on performance enhancing proxies for long distance wireless and satellite networks[C]//Multitopic Conference (INMIC), 2012 15th International. IEEE, 2012: 395-402.

[54] SU N Y, JI Z, WANG H. TFRC-satellite: a TFRC variant with a loss differentiation algorithm for satellite networks[J]. IEEE Transactions on Aerospace Electronic Systems, 2013, 49(2): 716-725.

[55] PRADHAN S, EMFINGER W, DUBEY A, et al. Establishing secure interactions across distributed applications in satellite clusters[C]// Space Mission Challenges for Information Technology (SMC-IT), 2014 IEEE International Conference on. IEEE, 2014: 67-74.

[56] 罗长远, 李伟, 霍士伟. 基于身份的空间网络组密钥管理方案[J]. 通信学报, 2010, 31(12): 104-110.
LUO C Y, LI W, HUO S W. Identity-based group key management scheme for space networks[J]. Journal of China Institute of Communications, 2010, 31(12): 104-110.

[57] ZHOU J, ZHOU X. Autonomous shared key management scheme for space networks[J]. Wireless Personal Communications, 2013, 72(4): 2425-2443.

[58] 周林, 矫文成, 吴杨, 等. 一种基于层簇式的卫星网络组密钥管理方案[J]. 宇航学报, 2013, 34(4): 559-567.
ZHOU L, JIAO W C, WU Y, et al. A group key agreement protocol based on layer-cluster for satellite network[J]. Journal of Astronautics, 2013, 34(4): 559-567.

[59] JIAO W, HU J, LU Z, et al. A threshold value-based group key management for satellite network[C]//2013 IEEE Third International Conference on Information Science and Technology (ICIST). IEEE, 2013: 718-721.

[60] WANG Z, DU X, SUN Y. Group key management scheme based on proxy re-cryptography for near-space network[C]//Network Computing and Information Security (NCIS), 2011 International Conference on IEEE, 2011, 1: 52-56.

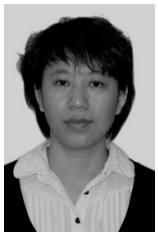
[61] SUN Y, MA H. Satellite multi-group key management[C]//2013 IEEE Third International Conference on Information Science and Technology (ICIST). IEEE, 2013: 894-899.

[62] ELMASRI M H, MEGAHED M H, ELAZEEM M H A. Design and software implementation of new high performance group key management algorithm for tactical satellite[C]//2016 33rd National Radio Science Conference (NRSC). IEEE, 2016: 149-158.

[63] HU S M X. Classification and key management approaches for space networks security[C]//International Conference on Anti-counterfeiting, Security and Identification. Guiyang, China, 2008:127.

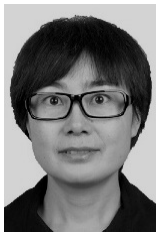
作者简介：

李凤华（1966-），男，湖北浠水人，博士，中国科学院信息工程研究所副总工、研究员、博士生导师，主要研究方向为网络与系统安全、信息保护、隐私计算。



殷丽华（1973-），女，辽宁朝阳人，博士，中国科学院信息工程研究所副研究员、硕士生导师，主要研究方向为信息安全、安全性评估。

吴巍（1956-），男，重庆人，中国电子科技集团公司第五十四研究所总工程师、研究员、博士生导师，主要研究方向为网络与信息系统、网络安全。



张林杰（1972-），女，河北乐亭人，中国电子科技集团公司第五十四研究所研究员，主要研究方向为网络安全、通信网络与系统。

史国振（1974-），男，河南济源人，博士，北京电子科技学院副教授、硕士生导师，主要研究方向为网络与系统安全、嵌入式安全。