Security and Verification in Space Networks

空间网络

安全与验证

唐朝京 鲁智勇 等著

国防工业出版社
National Defense Industry Press

空间网络安全与验证

Security and Verification in Space Networks

唐朝京　鲁智勇　彭长艳
冯　超　张　磊　由春华　著

国防工业出版社

·北京·

内容简介

空间信息网络集成了各种空间信息获取、传输、处理、分发和应用系统，能够实现快速智能的信息共享和综合利用，极大地促进了制信息权优势的获得，是未来信息化战争的核心技术支撑，并将对军事现代化产生巨大的推动作用。本书内容分为三部分：介绍了空间网络及架构；论述了空间网络安全策略、空间网络安全体系结构、安全路由、安全传输控制、密钥管理和安全切换等关键技术；探讨和研究了空间网络安全协议建模、协议安全定量验证方法和协议安全定性验证方法等技术。

本书可作为从事空间网络安全和对抗人员的必备参考资料，也可作为高等院校学生和教师参考书以及工程实践用书。

图书在版编目(CIP)数据

空间网络安全与验证 / 唐朝京等著. —北京：
国防工业出版社，2014.7
ISBN 978-7-118-09359-9

Ⅰ. ①空… Ⅱ. ①唐… Ⅲ. ①计算机网络-安全技术 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2014)第 142724 号

※

国防工业出版社出版发行
(北京市海淀区紫竹院南路 23 号 邮政编码 100048)
北京嘉恒彩色印刷有限责任公司
新华书店经售

*

开本 710×1000 1/16 **印张** 19 **字数** 360 千字
2014 年 7 月第 1 版第 1 次印刷 **印数** 1—3000 册 **定价** 48.00 元

(本书如有印装错误，我社负责调换)

国防书店：(010)88540777 发行邮购：(010)88540776
发行传真：(010)88540755 发行业务：(010)88540717

前　言

由部署在不同轨道、执行不同任务的多种类型的卫星、临近空间飞行器及相应地面系统和终端连接起来，并与传统地面有线和无线网络相融合的空、天、地一体化网络（简称空间网络），能够实现快速智能的信息获取、传输、处理、分发和应用。然而，空间网络的复杂性、异构性、信道开放性等特点对空间组网，特别是空间网络的安全带来了巨大的挑战。如何设计满足空间网络应用要求和特点的安全解决方案是空间网络中的基本问题，也是当前该领域的研究热点之一。

全书内容分为三部分，共计12章。第一部分共有2章，对空间网络及架构进行了描述；第二部分共有6章，对空间网络安全策略、空间网络安全体系结构、安全路由、安全传输控制、密钥管理和安全切换等关键技术开展了研究；第三部分共有4章，对空间网络安全协议建模、协议安全定量验证方法和协议安全定性验证方法和网络安全验证等技术进行了研究。

本书作者近些年一直致力于通信网络安全和对抗技术的研究和应用，取得了一些研究成果。在撰写此书的过程中，查阅了大量的文献和资料，并将近几年来我们在理论和工程应用的成果融入到有关章节中。撰写本书的目的是促进空间网络技术的应用，同时也为空间网络防护和验证技术的研究和开发提供应用思想和可操作性技术。通过空间网络防护和验证等相关技术的研究，可为空间网络信息安全提供有力的技术支持。

本书由国防科技大学电子科学与工程学院唐朝京教授组织和策划。中国洛阳电子装备试验中心的鲁智勇高级工程师和由春华工程师、空军第一航空学院航空电子工程系的彭长艳博士及国防科技大学电子科学与工程学院的冯超博士、张磊博士参与了部分工作，本书的完成体现了团队精神。

由于空间网络安全与验证是一个崭新的领域，涉及的内容范围又比较广，书中难免有不妥之处，敬请广大读者提出宝贵意见，并给予批评指正。

作　者

2013年12月于长沙

目　录

第一部分　空间网络和架构

第二部分　空间网络安全策略和技术

第三部分 空间网络安全验证

第一部分　空间网络和架构

在介绍空间网络的基本概念和特点的基础上，针对空间网络中的安全问题所涉及的关键技术，分析对地观测、导航定位、通信三类卫星和临近空间信息系统的发展趋势，总结网络融合和综合军事应用对空间组网的需求，研究网络的拓扑结构、节点构成、协议栈的各个层次可能使用的网络协议以及空间网络架构。

第1章　空间网络

随着航天技术、移动通信技术和网络技术的迅速发展和信息化建设的逐渐深入，空间信息系统正向着网络化的趋势加速发展。利用先进的空间链路技术，将地球轨道空间和临近空间中各种类型的飞行器连接起来实现互联互通，并与相应的地面设施和网络相融合，共同组成具有自主信息获取、传输、处理、分发与应用功能的空间信息网络，可在通信、导航、定位、监视、侦察、预警、遥感、探测、气象、广播、电子对抗等军事应用领域发挥越来越大的作用，为国家安全提供强大的信息支持，并对国防现代化建设产生巨大而深远的影响。

空间网络的广阔应用前景使其得到了国内外学术界、工业界、特别是军方的高度关注和重视。近年来，研究人员针对空间网络的体系结构、网络融合、网络管理、路由、移动性管理、传输控制等技术开展了大量的工作，取得了丰硕的成果，促进了空间网络的发展和应用。然而，现有的研究在空间网络的安全方面还很不够，要么没有充分考虑空间网络可能面临的安全问题，要么机械地照搬地面网络中的安全解决方案。由于空间网络具有复杂性、异构性、高动态性、长延迟等迥异的特点，地面网络中的传统安全解决方案并不完全适用于空间网络。因此，针对空间网络的特点，设计合理高效的安全体系结构和安全机制，是空间网络的研究、设计、部署和应用中极其重要的课题。本书主要针对空间网络中的安全体系结构、安全路由、安全切换、安全传输控制和密钥管理等关键技术开展研究。

本章首先介绍了空间网络的基本概念和特点，总结了卫星网络和临近空间网络的典型应用以及国内外的研究现状；然后针对空间网络中的安全问题所涉及的关键技术，分析了现有的研究工作及其存在的不足；最后介绍了本书的主要研究内容。

1.1　概　述

1.1.1　基本概念

20世纪50年代末期，苏联和美国先后发射了以军事应用为目标的首颗人造地球卫星。此后，在军事需求的强力推动下，空间技术得到了迅速的发展，并广泛应用于对地观测、导航定位和军事通信等领域。发展军用卫星技术从而夺取空间优势，成为世界各国增强军事航天力量的首要任务。

早期的单星模式卫星系统仅仅通过“弯管”式透明转发进行信息的传输，在覆盖地域和覆盖时间上存在很大的局限性。相比之下，星座模式的卫星系统由多颗分布在相同或不同轨道上的同类型卫星共同完成信息获取和传输的任务，能够克服单星模式的缺陷，在保证时间性要求的同时可提供较好的覆盖性能，已经得到了广泛的军事应用。

然而，随着卫星系统种类的迅速增加和功能的日益完善，系统之间自成体系、条块分割的局面也逐渐形成。不同卫星系统之间的互联互通非常困难，频繁的协议转换导致互操作效率低下，并且资源浪费和重复建设现象也十分严重。这些问题都使得空间信息不能得到有效共享和综合利用，制约了空间系统效益的充分发挥。

因此，空间信息系统从单星模式和星座模式，逐步发展到网络化模式，对航天资源进行统筹规划、优化设计和综合建设，进而提高空间系统的整体效益，成为未来军事航天技术发展的必然趋势。目前，只有美国和俄罗斯的航天系统具备星座应用模式，美国正在为进入网络化模式做准备。我国的空间系统还以单星模式为主，即将进入星座模式，迫切需要向网络化模式演进，从而满足日益增长的军事应用需求。

临近空间是指处于现有飞机最高飞行高度和卫星最低轨道高度之间的空域（距地面 20 ~ 100km），也可称亚轨道、空天过渡区或简称为近空间。近年来，临近空间飞行器的军事应用得到了广泛的关注，各军事大国均已开展了相关领域的研制、部署和应用工作。通过在临近空间部署不同种类的飞行器，并利用平台间链路组成网络，可实现区域侦察监视、导航定位、通信中继等多种功能。因此，临近空间网络也将成为未来空、天、地一体化网络的重要组成部分。

根据对空间信息系统的研究现状和发展趋势的分析，可以看到，未来空、天、地一体化网络是由不同轨道上多种类型的卫星、临近空间飞行器及相应地面系统和终端连接起来组成的综合信息网络。空间信息网络集成了各种空间信息获取、传输、处理、分发和应用系统，能够实现快速智能的信息共享和综合利用，极大地促进了制信息权优势的获得，是未来信息化战争的核心技术支撑，并将对军事现代化产生巨大的推动作用。

1.1.2 网络特点

空间网络由多种不同类型的异构网络互联而成，与传统无线网络在拓扑动态性、自组织性等方面存在一些相似之处；然而，空间网络在节点构成、部署环境、链路特性和典型应用等方面却存在显著差异，具有很多非常鲜明的特点。

（1）网络拓扑结构高动态变化。空间网络是由位于不同轨道平面上的各种卫星以及空间飞行器组成的立体层次化网络。网络中的卫星节点按照预定的轨道运行，节点之间的相对位置不断变化；同样，临近空间节点也可能处于高速运动状态

中，使得空间网络的拓扑结构随着时间不断地变化。另外，由于空间链路的开放性，空间网络中各组成子网的物理边界比较模糊，不存在地面固定网络那样确定的内、外部网络边界。

（2）各种异构网络紧密融合。卫星通信、临近空间平台通信等空间无线通信网络，与地面传统的各种无线和有线网络进一步融合，形成一个遍布地面、海上、空中和空间，无处不在、无时不在的空、天、地一体化网络，将给空间网络的网络融合技术带来新的挑战。由于不同的网络可能使用不同的通信协议，需要协议转换网关以实现互操作，对各种组网技术的网络性能提出了更高的要求。

（3）通信方式多种多样。空间网络中子网与节点的高度异构性，使得整个平台的构造、网络的链路和系统的整合都异常复杂。各种网络节点之间存在着点对点通信、广播通信、组播通信、单向通信、双向通信、面向连接的通信、无连接的通信、直接通信和间接通信等不同种类的通信方式，可能对应不同的网络协议，因此，协议的共存、切换、融合都需要进行深入的研究。

（4）空间链路传输距离远、时延长。空间和天地间的传输路径远比地面网络长，因此具有较长的传输延迟，在深空通信中更是如此。这样一来，原有的地面网络中广泛使用的传输协议不再适用，必须改进或者设计新的空间网络传输协议。除了数据传输协议以外，在设计或实现实时性要求较高的网络应用时也必须充分考虑链路的时延因素。

（5）空间链路误码率高，带宽非对称。空间和天地间的微波或激光链路与地面有线或无线链路相比，受空间环境和电磁干扰的影响较大，链路性能不稳定，误码率高，甚至经常中断，给空间通信协议的研究带来很多困难。另外，天地间链路还存在非对称的特点，下行链路的带宽一般远大于上行链路，也会给传统网络传输协议的应用带来较大的影响，必须采取一定的机制或策略对协议进行改进，以适应空间链路的特点。

（6）可靠性和安全性要求高。空间网络系统成本高，应用的领域均非常重要，远程维护和管理非常复杂，这些特点决定了空间网络必须具有高可靠性和高安全性。组成空间信息网络的不同子系统、子网与节点由于自身数据的敏感性、信息价值的大小、面临的安全威胁和安全风险的大小存在差异，具有不同的安全需求。因此，必须对系统的可靠性和安全需求进行客观而全面的分析，针对不同空间应用和信息的安全等级，采用不同的安全防护机制和安全策略。

空间网络的上述特点给各种网络技术特别是网络安全技术的研究带来了很多不利的影响，使空间网络的研究工作面临十分严峻的挑战。在进行空间网络关键技术的研究时，必须适应高动态拓扑、大规模网络、不可靠通信、无固定基础设施、有限的计算处理能力等方面的限制，采取各种措施和机制应对这些挑战，从而提高空间网络的性能和效率。

1.1.3 典型应用

从系统功能的角度，空间信息网络主要由信息获取、信息传输、导航定位、信息处理、网络管理和安全防御等子系统组成。本书在典型应用中主要分析对地观测、导航定位和通信三类处于核心地位的空间系统，而较少考虑其他处于辅助地位的系统。主要由各类卫星系统组成的空间信息系统，当前的发展极为迅速，并将逐步演进到网络化模式，在军事和民用领域正发挥日益重要的作用；相比之下，临近空间信息系统的应用尚处于研究论证和演示验证等较为初级的阶段，然而由于其具有性价比高、时延小、灵活性强、链路损耗小等突出的优点，在未来空间网络的应用中将存在广阔的发展空间。

1. 卫星网络

卫星系统按照轨道情况，可分为地球静止轨道（Geosynchronous Earth Orbit，GEO）卫星和非地球静止轨道（NGEO）卫星，NGEO 卫星又可分为低地球轨道（Low Earth Orbit，LEO）卫星（700～1500km）、中地球轨道（Middle Earth Orbit，MEO）卫星（10000km 左右）和高椭圆轨道（Highly Elliptical Orbit，HEO）卫星等。卫星及其地面基础设施共同组成卫星网络，也称为天基网络或天基综合信息网。

卫星网络系统在作战指挥决策、行动实施、效果评估和国土防御等方面发挥着极其重要的作用，给军事行动带来了革命性的影响，是主宰战场空间和确保军事优势的关键因素之一，将成为信息化战争的核心基础设施。

1）对地观测

卫星对地观测系统是空间网络信息系统中主要的信息获取平台。典型的对地观测卫星包括气象卫星、资源卫星、海洋目标监视卫星、照相侦察卫星、雷达成像卫星、电子侦察卫星、导弹预警卫星和核爆炸探测卫星等。依靠对地观测卫星系统强大的观测能力，能够实现对地面、空中、海洋目标的实时监控、侦察、跟踪，对指定区域内多种战略性政治、经济和军事目标进行详查侦察和精确定位，对战略、战术导弹发射进行预警、防御，提供气象、环境、水文、测绘等信息，对核爆炸进行探测，从而为军事行动提供决策支持。

2）导航定位

卫星导航定位系统被称为“太空中的指南针”。通过接收卫星发出的导航信号，可实现全天候、全球性、高精度的导航、定位、测速和授时等功能。卫星导航定位系统能够为陆、海、空等军兵种提供导航定位服务，为单兵、武器平台提供导航支持，也能为战略核武器、运载工具、各种精确制导武器提供精确的导航定位能力以提高其打击能力和命中精度，推动了机械化战争向信息化战争精确打击的转变。

3）通信

卫星通信系统是天基网络的核心，是未来信息化战争中指挥信息系统 C^4ISR 的重要组成部分。按照应用类型，通信卫星分为固定通信卫星、移动通信卫星、宽

带多媒体卫星、直播卫星、数据中继卫星等，已广泛应用于指挥控制、信息传输等军事通信任务中。卫星通信系统能够为多军兵种联合作战提供实时、全球覆盖的语音、图像、数据、多媒体、广播等通信服务，使各军兵种用户能够获得迅速、准确、保密、稳定的通信保障，实现作战单元之间各种进攻和防御所需信息的共享与分发，大大提高了多军兵种协同作战、联合作战的效能。

2. 临近空间网络

临近空间飞行器按照速度可分为低速飞行器、亚声速飞行器和高超声速飞行器等。低速飞行器主要包括传统浮空器（飞艇和气球）、升浮一体化飞行器等，亚声速飞行器主要包括太阳能平流层飞机、高空无人机等，而高超声速飞行器则指快速达到天对地精确打击的各种飞行器，如空天飞机。准静止的临近空间飞行器有时也称为高空平台（High Attitude Platform Station，HAPS）。

临近空间飞行器具有性价比高，可携带载荷重量大，灵活性强，使用持久，安全性强等突出的优势，非常适应于空间网络应用的需求，具有较为广阔的军事应用前景。低速临近空间飞行器能够在确定区域内实施持久的信息获取、信息对抗等军事任务，既可实现战术/战役级别的侦察、监视、导航、预警和电子对抗系统，也可实现高分辨率对地观测、信息中继和导航定位系统。高速临近空间飞行器则适用于实现目标远程侦察平台，或者远程精确打击武器系统。

1）对地观测

相比于卫星，临近空间飞行器具有距离地面近、机动灵活等优点，更适合执行特定条件下的对地观测任务，如侦察、监视和预警。临近空间侦察与监视系统利用光电遥感器或无线电设备，可对地面、海洋或空中目标进行实时侦察、监视或跟踪。低速的侦察与监视系统可在特定区域上空长时间驻留，且覆盖区域较大，侦察分辨率高；而高速的侦察与监视系统具有部署速度快、突防能力强、被拦截概率小、可纵深进行侦察等特点，能快速监测战场情况的变化。临近空间预警系统以导弹预警为目标，部署在临近空间较高的位置，能监视地球上的特定区域，用于及时发现弹道导弹的发射并粗略地预报其弹道和落点。

2）导航定位

准静止的临近空间飞行器能够作为全球卫星导航定位系统的增强基础设施，提高导航和定位服务的精度和可用性，增强定位过程的可靠性。应用高空飞艇或高空无人机有可能实现独立于卫星导航系统的一种区域导航系统，当卫星导航系统受到干扰时，这种导航方式可以暂时代替卫星系统，为武器装备系统提供导航、定位和导引等服务。

3）通信

临近空间通信系统具有容量大，频率利用率高，通信时延小，链路损耗小，机动性强，建设周期短，管理、维护和升级容易等突出的优势，具有向地面、海上、低空节点提供高宽带、抗干扰及超视距通信的能力，能满足战役、战术级别的军事行动中