

面向天地一体化信息网络的安全验证平台设计

秦智超, 张平, 范鑫鑫, 陆洲

(中国电子科技集团公司电子科学研究院, 北京 100041)

摘要: 天地一体化网络系统复杂、技术体制多样, 其中安全技术涉及系统的各个层面, 难以通过单项技术试验来实现系统层面的验证和评估, 需要构建具有一定网络规模的验证系统来完成安全技术体系的验证。基于通用开放、可重构的理念, 提出了一种天地一体化网络安全验证系统方案, 实现密钥管理、安全路由、安全切换、安全隔离、安全传输等安全保障技术的系统验证。

关键词: 空间信息网络; 天地一体化网络; 网络安全; 验证平台

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2016.00080

Design of security verification platform for the integrated space-ground network

QIN Zhi-chao, ZHANG Ping, FAN Xin-xin, LU Zhou

(China Academy of Electronics and Information Technology, Beijing 100041, China)

Abstract: The integrated space and terrestrial network is complex, having diversified technical specifications which involves all aspects of the system of security technology, so it is difficult to achieve system level verification and evaluation through individual technology test. It is necessary to construct a certain scale of network authentication system to verify the effectiveness of safety technology architecture. Based on the concept of general opening and reconstruction, a scheme of integrated network security verification system was presented to validate security technologies such as key management, secure routing, secure handoff, security isolation and secure transmission.

Key words: space information network, integrated space and terrestrial network, network security, demonstration platform

1 引言

当前, 空间信息系统建设呈现爆炸式发展形态, 根据美国 UCS 网站上公布的数据^[1], 截至 2015 年 12 月底, 全球总共有在轨各类航天器 1 381 颗, 其中低轨卫星 (LEO) 759 颗, 中轨卫星 (MEO) 92 颗, 高轨卫星 (GEO) 493 颗, 其他类型 37 颗。

然而, 目前各空间信息系统的建设仍然表现出各自为阵、独立建设的局面, 造成了空间资源的极大浪费。为此, 各国积极探索, 提出了诸如转型卫星计划 (TSAT)、下一代铱星 (Iridium NEXT)、太空互联网、空间激光高速公路等系统的建设计划, 从传统的“烟囱式”发展转向在任务层面多星协同发展、在信息层面网络化发展, 由此

收稿日期: 2016-07-11; 修回日期: 2016-08-02。通信作者: 秦智超, qzc0308@163.com

基金项目: 国家自然科学基金资助项目 (No.91338201); 国家高技术研究发展计划 (“863” 计划) 基金资助项目 (No.2015AA015701)

Foundation Items: The National Natural Science Foundation of China (No.91338201), The National High-Technology Research and Development Program of China (863 Program) (No.2015AA015701)

引出天地一体化信息网络的概念。

天地一体化信息网络规模庞大、结构复杂、支持业务种类繁多、网络伸缩性强、时空跨度大,网络拓扑结构不断变化^[2],并且涉及互联网、空间网络和无线移动网络等多种异质异构网络,加之天地一体化信息网络的空间段及天地间通信的空间暴露特性容易被攻击,因此必须重视天地一体化信息网络安全保障技术的研究,国内外在极高频段^[3]、跳扩频^[4]、多波束^[5]、天线调零^[6]、信息加密^[7]、结构增强^[8]等方面开展了大量工作。

鉴于各类安全保障技术研究较为分散,缺乏体系的验证,本文在提取空间信息网络典型特征的基础上,构建尽可能包含全部要素的最小原型系统,采用实物/半实物结合的网络安全验证系统,可以对安全保证技术的适用性、有效性进行实际验证。

2 相关工作

2.1 天地一体化信息网络安全威胁

我国天地一体化信息网络相关的研究和讨论已经持续了十多年,目前已经取得了一系列成果。2006年,沈荣骏院士^[9]首先提出了我国天地一体化航天互联网的概念及总体构想。2007年和2012年,中国宇航学会飞行器测控专业委员会先后两次召开学术年会,对航天互联网相关技术进行了专题研讨。2013年~2014年,工业和信息化部电子科学技术委员会组织了“天地一体化信息网络体系架构研究”重点课题,从发展战略、总体方案和关键技术3个方面对天地一体化信息网络开展研究^[10]。2013年和2015年,国内先后两次召开了天地一体化信息网络的高峰论坛,对凝聚国内天地一体化信息网络相关研究力量并形成统一的认识发挥了重要作用。2015年,张乃通院士^[11]发表了《对建设我国“天地一体化信息网络”的思考》一文,对天地一体化信息网络的定位、边界做了清晰的说明,并提出了网络基本架构的设想和对建设工作的建议。

根据以上研究工作,天地一体化信息网络是以地面网络为依托、天基网络为拓展,采用统一的技术架构、统一的技术体制、统一的标准规范,由天基信息网、互联网和移动通信网互联互通而

成。如图1所示,天基信息网包括天基骨干网、天基接入网、地基节点网3个部分。

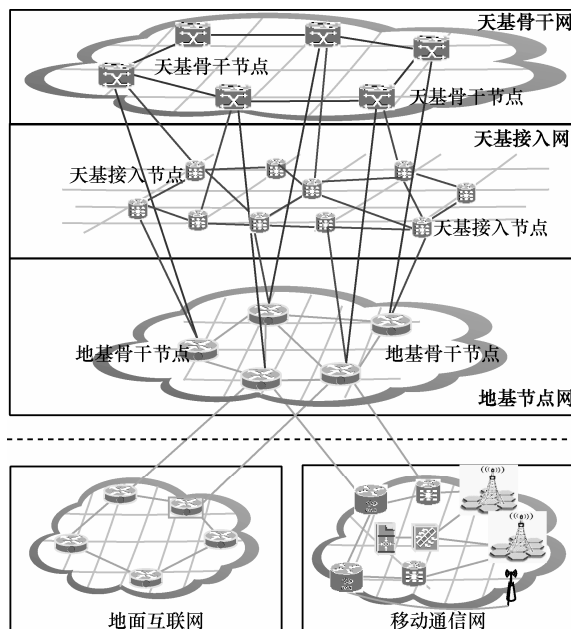


图1 天地一体化信息网络组成

安全保障技术作为天地一体化信息网络可靠运维的重要支撑,需要对天地一体化信息网络面临的各种威胁进行针对性和体系性设计。

目前天地一体化信息网络在各个层次中可能受到的攻击方法和防御手段总结如表1所示^[12]。

表1 天地一体化信息网络所面临的攻击

攻击类型	发生层次	预防机制
拥塞	物理层	扩频、较低占空比
篡改	物理层	有效密钥管理方案
窃听	物理层	加密
碰撞	数据链路层	错误检测
耗尽	数据链路层	传输率限制
通信量分析	网络层	链路加密、匿名通信
操控路由信息	网络层	认证、加密
选择性转发	网络层	冗余、探测
sybil 攻击	网络层	认证、加密
重放攻击	网络层	双向认证、3次握手
黑洞攻击	网络层	认证、监控、冗余
虫洞攻击	网络层	监控、灵活路由选择
Hello flood 攻击	网络层	双向认证、3次握手
Flooding 攻击	传输层	限制链接数目、客户难题
克隆攻击	应用层	唯一密钥对

2.2 天地一体化信息网络现代攻防

天地一体化信息网络由空间信息网络、地面互联网、移动网等组成，不可避免地涉及网络攻防。美国在网络攻防方面走在世界的前列，在保护本国通信方面，美国国家安全局曾经开展密码现代化计划（CMI），以达到保障军事卫星通信的信息安全要求。在 CMI 方面，必须要考虑通信卫星以下几类的主要功能。

传输安全（TRANSEC）：提供保障业务，防止被探测、干扰和物理层的拒绝服务。由此产生用来管理物理特性的跳组和密钥流，并将通信流量的保护层包括进来。

遥测、跟踪和控制：一是上行链路，解密、认证和验证卫星控制命令的完整性并认证来源；二是下行链路，加密遥测信息、业务信息，补充用来验证数据完整性和真实性的编码。

有效载荷和访问控制：认证并验证请求的完整性，该请求将由有效载荷控制处理。

通信安全：高保障因特网协议加密设备，加密解密于卫星上的所有秘密数据分组通信量。

IP 安全：加密解密卫星上所有的敏感数据分组通信量。

线路加解密：处理卫星所有的线路通信量。

跨域解决方案（CDS）或防护：用于桥接安全配置，保护本地网络，使其秘密信息与非密网络隔离。

英国军队为“天网-5”卫星安装了新型密码装置，为英国军队提供卫星通信保密服务。嵌入“天网-5”通信系统中的 CLERISY 采用美国的电

子密钥管理系统标准协议，能够满足多种目标。为通信保密管理人员提供能够自动管理、生成、分发、存储、统计和访问控制等功能。

日本防卫厅已完成卫星通信设施和数字微波线路的建设，并投入实际应用。目前正加紧构成一个地面、空间、有线、无线彼此协调的三军综合利用的立体化快速反应的信息安全保密体制。

在网络攻击方面，据报道，美国国家安全局曾发起代号为“攻坚克难”的研发项目，美国正投入巨资研发量子计算机，意欲攻破全球各类加密技术。

我国近年来在安全保密方面开展了大量的研究工作，成功研制了一系列用于卫星系统的安全设备，对链路、各种类型的语音/数据终端、网络等进行安全保护，以及密码密钥管理设备，为各种卫星和地面系统提供了一定的密码保护。2016 年 8 月 16 日升空的由我国自主研发的全球首颗科学实验量子卫星“墨子号”和即将建成的地面光纤量子通信网络，将初步形成“天地一体化”的量子通信网络，可应用于金融、政务等重要信息的保密传输。

2.3 空间演示验证系统

2012 年，NASA 成功将 SCaN Testbed^[13] 载荷运输到国际空间站（ISS）上，可长期在轨开展通信与导航相关的技术试验。SCaN Testbed 为未来空间任务提供了一个理想的测试平台，它利用最新的软件无线电技术，可在轨之后根据任务需求重新定义无线电功能。整个 SCaN Testbed 试验系统如图 2 所示，以国际空间站上搭载的 SCaN Testbed 软件定义无线电载荷为核心，通过 L、S、

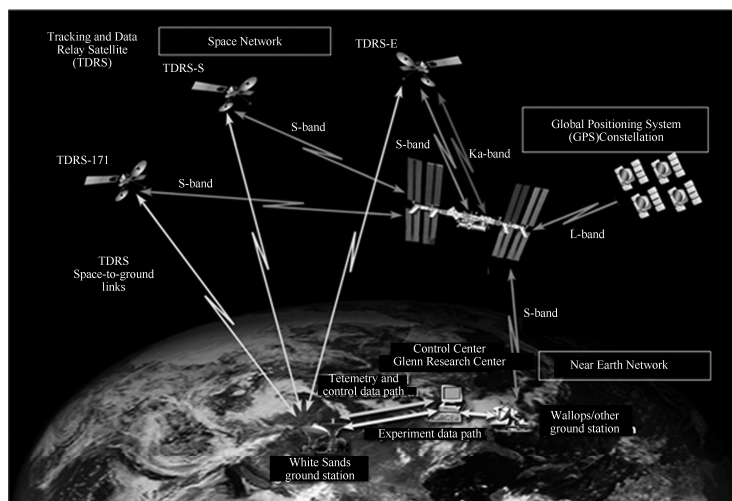


图2 美国空间通信与导航（SCaN）系统

Ka 等频段与 TDRS、GPS 等卫星系统以及地面网络构成一个天地一体的通用试验系统, 可开展各类通信/导航技术的空间在轨试验。

目前针对空间信息网络试验平台的研究主要集中在地面仿真或模拟试验系统模型的设计, 但也开始了空间试验平台建设, 尤其是 SCaN Testbed 这样的基于软件定义无线电的通用空间试验平台, 代表了未来空间试验平台的发展趋势, 值得借鉴。但 SCaN Testbed 空间试验平台侧重于通信和导航类的试验, 还不具备信息和网络多层次的试验支持能力, 构建功能可重构、能力可伸缩、具备信息和网络多个维度综合集成演示能力的空间试验平台将是未来充满挑战但意义重大的研究方向。

3 方案设计

3.1 设计原则

通用架构: 原型系统和空间等效试验平台的设计基于通用的硬件平台, 通过软件加载方式实现多种功能, 满足各项试验任务要求。

天地协同: 整个集成演示系统是天地一体的,

通过天地功能协同和资源配合完成试验, 提高试验的有效性和合理性。

迭代优化: 通过地面仿真模拟验证与空间在轨试验的比对和迭代, 根据试验评估结果不断优化、完善, 提高试验的科学性。

全面试验: 空间集成演示系统具备开展信息获取、处理、传输、分发与应用等各环节以及网络各层协议的全面验证能力。

开放联邦: 通过标准化开放接口, 可在其核心架构基础上不断吸纳各类试验资源, 并与其他试验系统建立联邦, 实现系统规模扩展和能力提升。

3.2 系统方案

如图 3 所示, 整个天地一体化安全验证系统由地面网络和空间网络两部分组成, 其中地面网络相比空间网络技术较为成熟, 在天地一体化信息网络中的主要作用是实现业务的互联互通, 可利用现有成熟资源开展演示验证, 包括中国教育和科研计算机网 (CERNET2)、LTE 试验网等试验网络; 而空间网络目前还没有实际系统可用, 采用地面模拟和半实物仿真等方式实现。

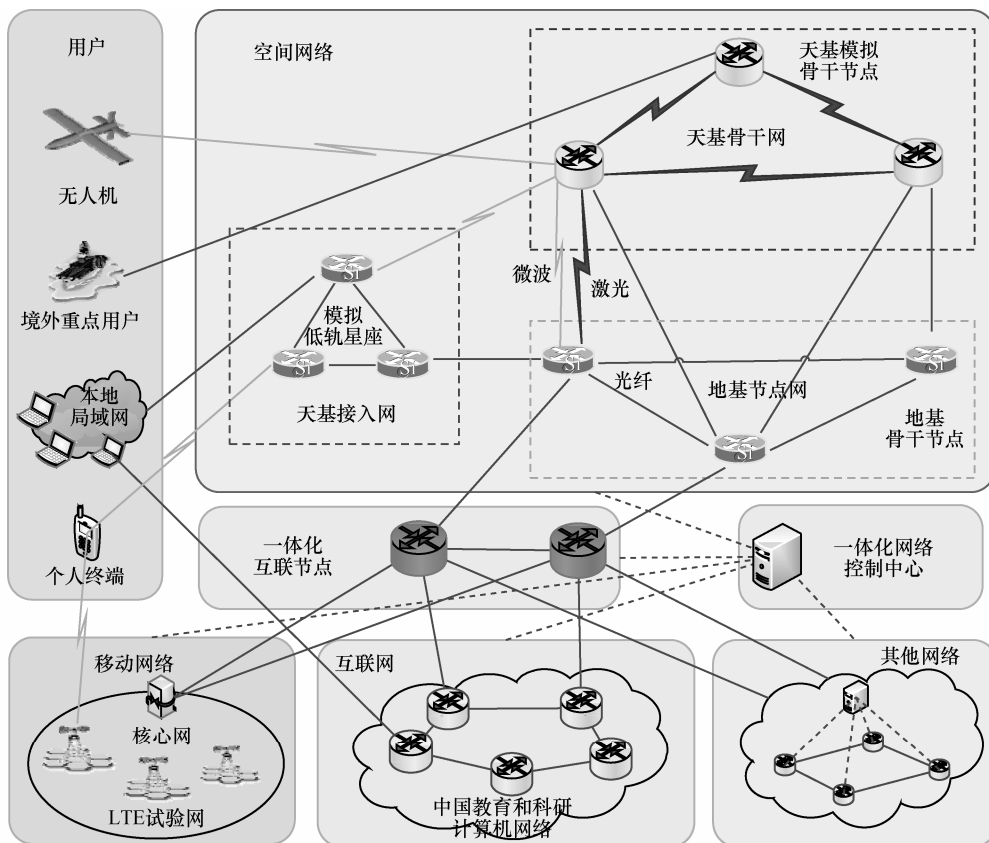


图3 天地一体化网络安全验证系统设想

1) 节点

在节点配置上,依据三点成网,天基骨干网、天基接入网、地基节点网 3 个网络至少需配置 3 个节点,并可根据系统需要不断扩展。

2) 链路

在链路配置上,天基骨干网为环状网,采用实激光链路模拟;地基骨干网为网状网,采用光纤链路模拟;天地互联采用实际激光/微波链路模拟;接入网低轨卫星之间、接入网与骨干网互联的微波链路采用计算机模拟实现;用户接入的微波或激光链路采用实际链路或者计算机模拟实现。

3) 一体化互联节点

一体化互联节点具备天地适配、骨干传输、异构互联等多种功能,实现空间网络与地面互联网、移动通信网等互联融合。

4) 控制中心

控制中心通过地面高速光纤与地面站连通,负责整个试验平台的运维管控等,具备网络资源管理、试验任务安排、试验数据采集与处理、试验性能评估等功能。

5) 用户

用户主要包括陆、海、空、天各类接入节点,

用于验证安全接入和用户管理等功能。

3.3 验证与测试用例

从攻击发起者的角度,安全威胁可能来自无线链路、核心网络实体或用户终端;从网络协议层次的角度,安全威胁可能来自物理层、链路层、网络层、传输层和应用层中的任意一个或多个层次。而且,网络设备的多样性和智能化、网络服务的易用性和可扩展性也使各种攻击行为的手段更加灵活,影响范围更加广泛,危害也更加严重。只有充分考虑各种可能的威胁来源和攻击方式,在每个协议层次均采用适当的安全机制和安全策略,制定合理高效的总体安全解决方案,才能抵御各种可能的网络攻击,推进天地一体化网络的渐进部署和应用,为天基信息系统提供可靠的安全保障。

1) 轻量级统一密钥管理试验

在一体化网络中选择若干动态可变节点组成一个服务节点集合,协助多播群密钥协商参数的生成和广播等操作,避免多播群的所有更新操作全部由一个服务节点来提供协助,避免单点失效并且实现负载均衡,试验示意如图 4 所示。

同时可设计基于身份的密码体制(IBC)方案。网络实体的公钥都可以由一个任意的字符串

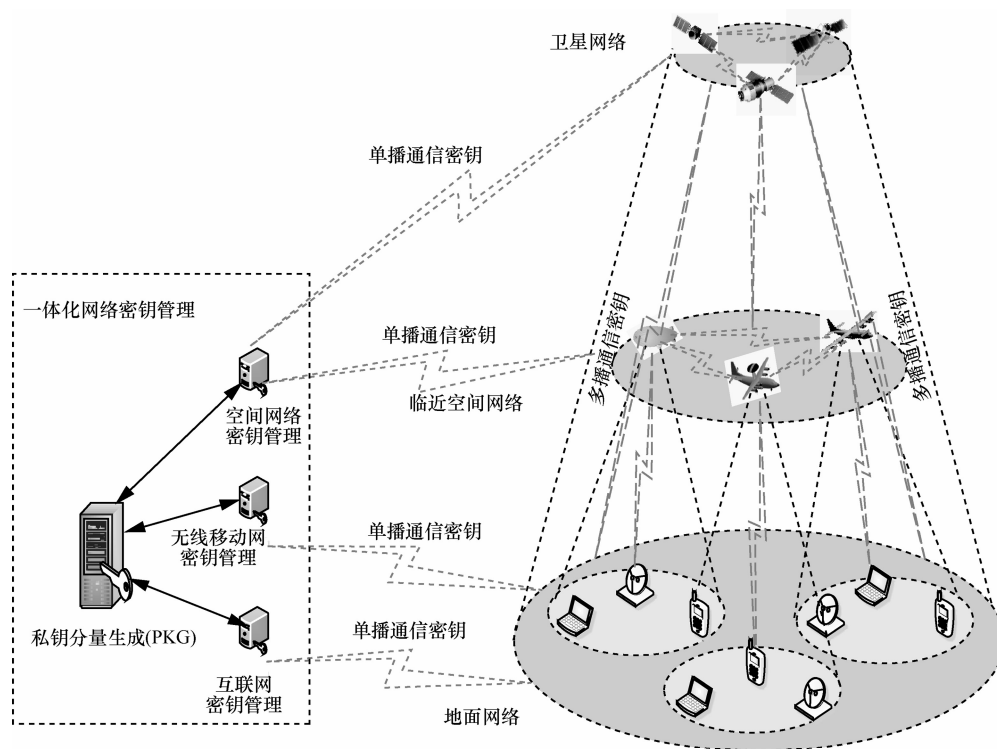


图4 统一密钥管理试验

(如 IP 地址或 MAC 地址)来定义,而不需要通过网络或其他方法额外地传输公钥。

2) 天地一体化网络安全路由试验

针对空间网络节点处理及存储能力受限、链路时延长、拓扑变化快等不利条件,采取跨层设计的思路和方法,从可靠性、QoS、负载均衡等角度对路由协议进行改进,从而降低路由建立时延和路由开销,并大幅度提高路由协议的整体性能。

试验示意如图 5 所示,该方案支持分等级的可信路由寻址体系。首先,根据设备及组件的自主研发程度,以及真实源地址验证、二维路由和轻量级统一密钥管理的部署情况,综合对路由设备的服务可控性分级。其次,利用优化理论,计算服务可控性最优路由,集中控制分组沿最优路由转发,达到优化路由服务分级可信的目的。最后,创设路由和转发一致性检测机制,达到入侵行为可检测、攻击者地址和身份可追查、被窃取资源可核对的目的。

3) 天地一体化网络安全切换试验

空间网络节点间相对位置是动态变化的,为了保证终端节点之间通过卫星或临近空间网络进行不间断的通信,必须使用移动性管理方案和协议以提供无缝网络接入服务。如图 6 所示,当移动终端 M 从当前位置移动到 M1 位置,其对应的通信卫星由 SATA 切换至 SATB。移动性管理主要包括位置管理和切换管理,其中的切换管理由于需要多个网络实体的参与而面临着更为严峻的安全挑战。

当节点之间尚未完成双向认证时,使用基于身份的签密方案来保证切换控制消息的机密性,只有指定的接收者才能够通过反签密算法获得消息的内容;当节点之间已经进行双向认证之后,双方根据实际情况协商会话密钥加密切换控制消息,保证切换控制消息的内容不被其他节点获得。另外,采用在切换报文中捎带认证信息、在认证信息中包含切换信息等方式,减少切换过程中安

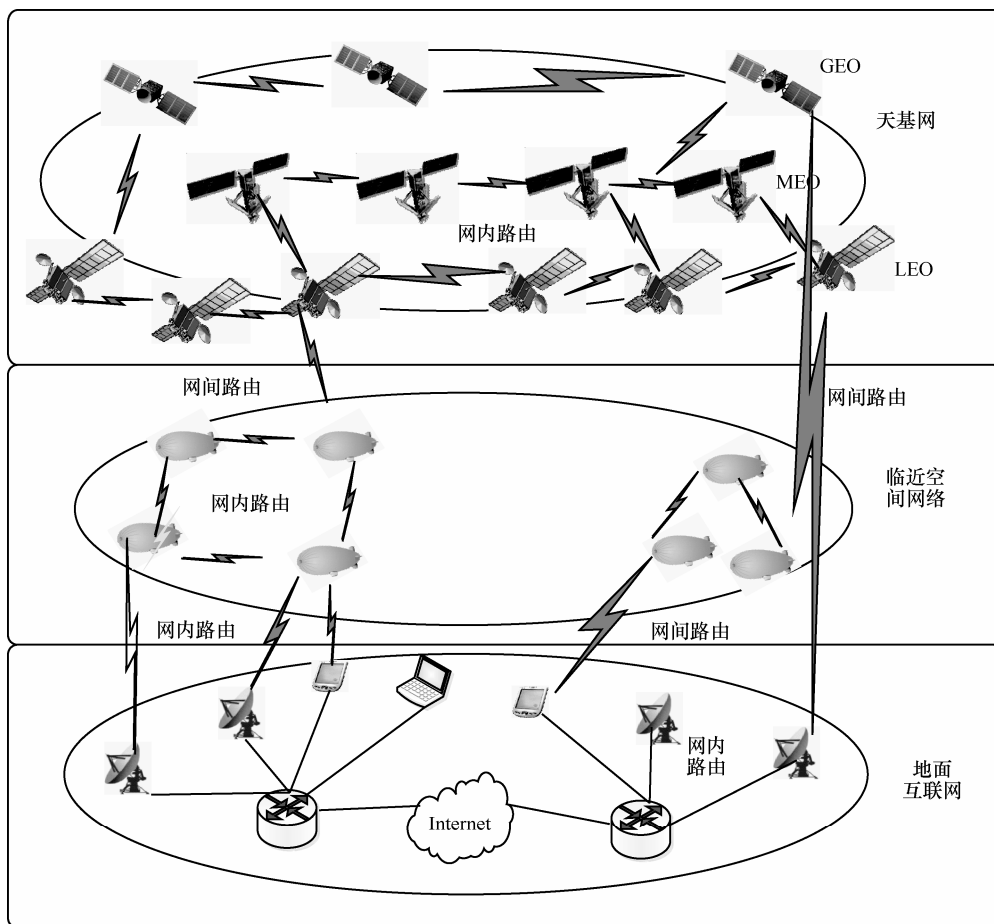


图 5 天地一体化网络安全路由试验

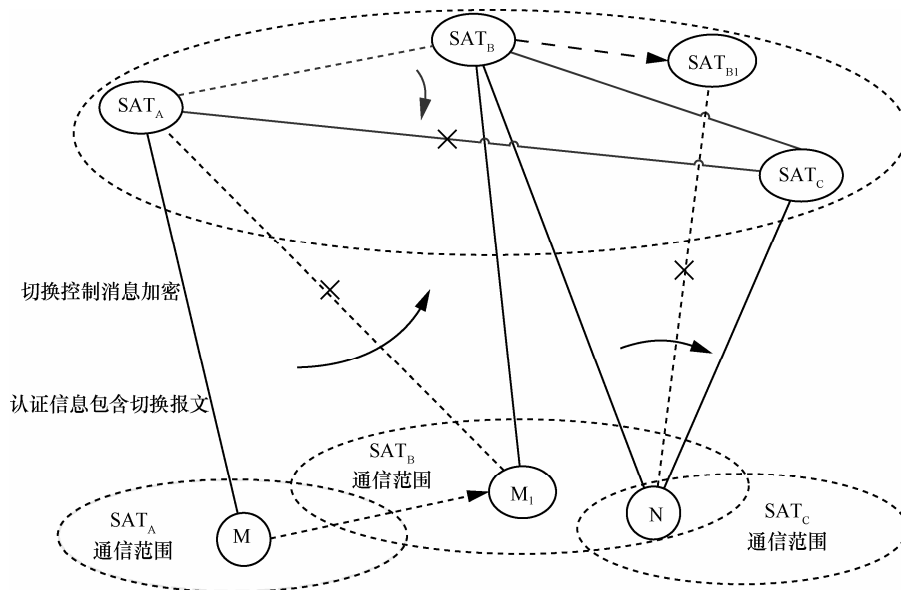


图6 天地一体化网络安全切换试验

全机制的处理开销，降低认证与切换并发时延。同时安全机制的引入不可避免地增加了切换延迟。由于空间网络拓扑的规律性和地面网络拓扑的稳定性，可以预先判断将要发生切换的目标接入节点。

4) 天地一体化网络安全隔离试验

通过空间隔离切断不同安全等级要求的网络间的直接连接，并借助时间隔离实现状态隔离与快速数据交换，既能阻止已知网络攻击，又能在机理上为未知攻击提供免疫，解决“安全隔离”与“安全通信”需求的矛盾。

试验示意如图7所示，在试验中所有不同安全等级网络间的信息交换都必须通过强双因子身份认证，登录基于可信计算平台设计的可信数据收发服务器。利用信任链的校验传递保证安全性，将基

于通信实体信息、用户信息、应用信息生成的可信标签附在数据上，传送到网间安全隔离网关。

网关使用可信计算模块中的错误检查和纠正密钥进行数字签名生成平台标签。通过安全令牌和平台标签的方式保证了终端身份的唯一性和不可伪造性。应用程序利用密码算法对终端上的数据交换系统的执行应用程序进行完整性校验并生成应用标签，将应用标签与平台标签进行绑定，最终形成数据终端的可信标签。

5) 天地一体化网络安全传输试验

为了适应天地一体化环境下对信息数据安全传输的要求，需要针对卫星信道的广播特性、卫星通信系统信道带宽资源受时空限制、数据缓存空间有限、数据处理能力有限、信道分组丢失率高、存在时延抖动等问题进行传输系统优化，改

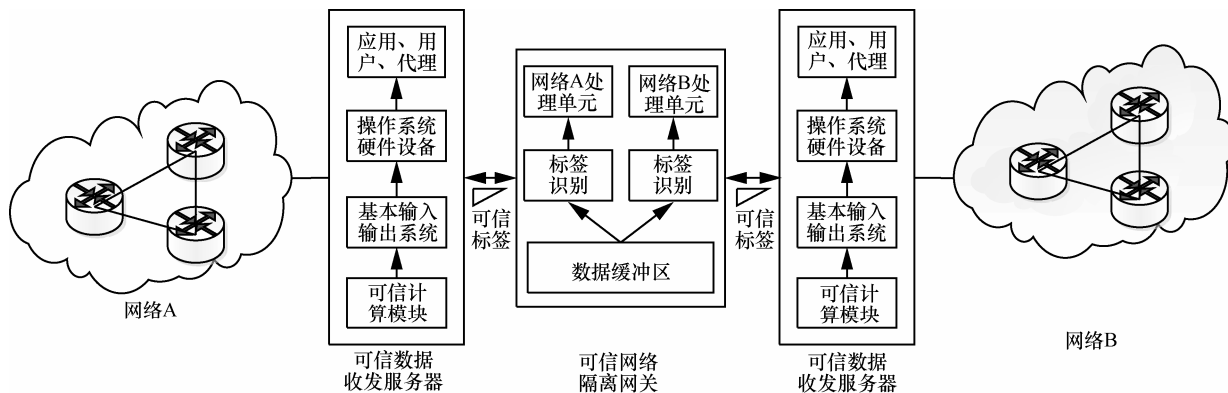


图7 天地一体化网络安全隔离试验

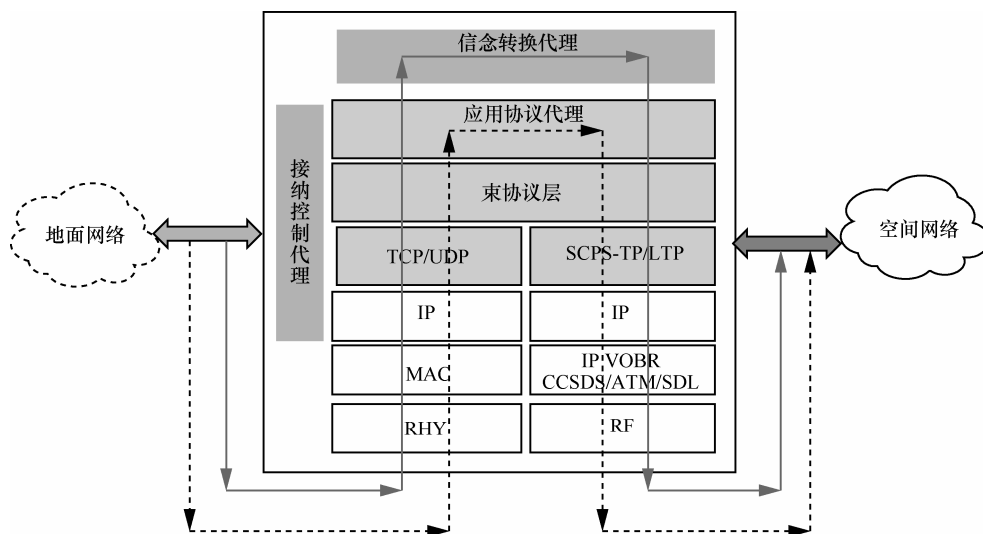


图8 天地一体化网络安全传输试验

善数据传输环境。

试验示意如图8所示,为了避免安全协议对传输协议和应用协议产生过多影响,通常会使用隧道机制实现上下层协议的透明。安全的传输层协议需要考虑真实性、机密性、完整性等安全服务,同时还应降低协议的交互次数和传输的消息量,在提高传输效率的前提下,达到安全和性能之间的平衡。

4 结束语

天地一体化网络具有电磁环境开放、网络设施暴露等特点,极易受到物理、电磁、网络等层面的安全威胁。安全是一个体系的概念,不仅仅是一个点或者一方面的安全,需要方方面面地考虑。本文基于通用开放、可重构的理念,提出了一种天地一体化网络安全验证系统的初步方案设计,并梳理了典型试验案例及流程。该系统具有动态可重构等特点,支持网络规模、拓扑动态可变等功能,并可随着后续试验任务要求升级扩展,基于该系统可开展天地一体化网络安全各方面技术的集成演示验证,为各项技术验证提供一个综合试验环境。

参考文献:

- [1] USC satellite database[EB/OL]. http://www.ucsusa.org/nuclear_weapons_and_global_security/solutions/space-weapons/ucs-satellite-database.html.
- [2] 彭长艳. 空间网络安全关键技术研究[D]. 长沙: 国防科技大学, 2010.
PENG C Y. Study of cyberspace security key technique[D]. Changsha: National University of Defense Technology, 2010.
- [3] SANCTIS M, CIANCA E, ROSSI T, et al. Waveform design solutions for EHF broadband satellite communications[J]. IEEE Communications Magazine, 2015, 53(3):18-23.
- [4] RONG L, RUIMIN L. An anti-jamming improvement strategy for satellite frequency-hopping communication [C]//International Conference on Wireless Communications & Signal. c2009:1-5.
- [5] UMEHIRA M, FUJITA S, GAO Z, et al. Dynamic channel assignment based on interference measurement with threshold for multi-beam mobile satellite networks[C]//The 19th Asia-Pacific Conference on Communications (APCC). c2013:688-692.
- [6] MAIARELLI D, GUIDI R, GALGANI G, et al. Numerical optimization of a satellite SHF nulling multiple beam antenna[C]//The 1st European Conference on Antennas and Propagation. c2006:1-5.
- [7] 王文华, 郑志明. 基于可变 S 盒的随机加密方案[J]. 北京航空航天大学学报, 2011, 37(7):811-816.
WANG W H, ZHENG Z M. Random encryption scheme based on alterable S case[J]. Journal of Beijing University of Aeronautics and Astronautics, 2011, 37(7):811-816.
- [8] DATASHVILI L, BAIER H. Derivation of different types of antenna reflectors from the principle of highly flexible structures[C]//The 8th European Conference on Antennas and Propagation (EuCAP 2014). c2014:4-8.
- [9] 沈荣骏. 我国天地一体化航天互联网构想[J]. 中国工程科学, 2006(10): 19-30.
SHEN R J. Sky-earth integrated space network idea of China[J]. Engineering Sciences, 2006(10):19-30.
- [10] CCF 2014-2015 中国计算机科学技术发展报告[M]. 北京: 机械工业出版社, 2015.

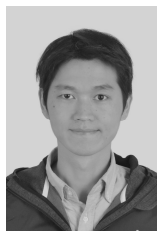
CCF 2014-2015 computer science and technology of China development report[M]. Beijing: China Machine Press, 2015.

- [11] 张乃通, 赵康健, 刘功亮. 对建设我国“天地一体化信息网络”的思考[J]. 电子科学研究院学报, 2015, 10(3):223-230.
ZHANG N T, ZHAO K L, LIU G L. Thinking of newly geographical information in China[J]. Electronic Journal of Academy of Sciences, 2015, 10(3): 223-230.
- [12] 闫大鹏, 赵军, 黄小红, 等. 基于天地一体化信息网络的安全防护系统建模及可靠性分析[C]//天地一体化信息网络高峰论坛. c2013.
YAN D P, ZHAO J, HUANG X H, et al. Security protection system reliability modeling and analysis based on the integration of heaven and earth information network[C]//The Integration of Heaven and Earth Information Network Peak BBS. c2013.
- [13] SCAN Testbed[EB/OL]. <http://spaceflightsystems.grc.nasa.gov/SOPO/SCO/SCaNTestbed>.

作者简介:



秦智超 (1981-), 男, 河北沧州人, 博士, 中国电子科技集团公司电子科学研究院高级工程师, 主要研究方向为物联网、天地一体化网络。



张平 (1981-), 男, 浙江临海人, 博士, 中国电子科技集团公司电子科学研究院高级工程师, 主要研究方向为空间信息网络、天地一体化网络。



范鑫鑫 (1984-), 男, 河南新乡人, 博士, 中国电子科技集团公司电子科学研究院高级工程师, 主要研究方向为网络空间安全。



陆洲 (1970-), 男, 河北石家庄人, 中国电子科技集团公司电子科学研究院研究员, 主要研究方向为宽带卫星通信、天基网络。