

天地网络安全保障技术研究

李凤华^{1,2}, 张林杰³, 陆月明⁴, 耿 魁¹, 郭云川¹

(1.中国科学院信息工程研究所, 北京 100195;

2. 中国科学院大学网络空间安全学院, 北京 100049;

3. 中国电子科技集团公司第五十四研究所, 河北 石家庄 050081;

4. 北京邮电大学, 北京 100876)

摘要: 梳理天地网络的特征, 针对天地网络中的安全威胁, 系统地梳理测控/运控信息、终端接入、无线信道、传输、业务信息系统、运维管理等方面的安全风险, 提出融合安全支撑层、接入安全层、网络安全层、安全服务层及安全态势预警、统一安全管理等的天地网络安全保障架构, 设计统一安全管理与安全态势预警、实体认证与接入防护、多域网络互联安全控制、密码按需服务、安全服务动态重构等的实现机制, 为天地网络安全提供有效支撑。

关键词: 天地网络安全保障; 安全态势预警; 实体认证与接入防护; 安全互联控制; 密码按需服务; 安全服务动态重构

中图分类号: TN929

文献标识码: A

doi: 10.11959/j.issn.2096-8930.20200102

Research on Space-Ground Network Security Guarantee Technology

LI Fenghua^{1,2}, ZHANG Linjie³, LU Yueying⁴, GENG Kui¹, GUO Yunchuan¹

1. Institute of Information Engineering, Chinese Academy of Science, Beijing 100195, China;

2. School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China

3. The 54th Research Institute of China Electronics Technology Group Corporation, Shijiazhuang 050081, China

4. Beijing University of Posts and Telecommunications, Beijing 100876, China

Abstract: The characteristics of space-ground network was combed. Against security threats in space-ground network, the security risks faced by measurement control, operation control, terminal access, wireless transmission, transmission, business information system, maintenance management were analyzed. Further, by dividing space-ground network security into four layers: foundation layer, access layer, network layer and application layer, a security architecture to protect space-ground network was proposed. An implement mechanism (including unified security management and security situation aware, entity authentication and access protection, interconnection control, cipher on-demand service, dynamic reconstruction of security service) was designed to guarantee the security of space-ground network.

Key Words: space-ground network security guarantee, security situation aware, entity authentication and access protection, interconnection control, cipher on-demand service, dynamic reconstruction of security service

1 引言

随着人类足迹不断向深海、深空、沙漠等区域延伸, 地面信号无法覆盖区域的通信需求大幅增加。为了满足网络的随遇接入, 实现“全球覆盖、随遇接入、按需服务、安全可靠”的通信目标, 需构建由天基骨干

网、天基接入网、地基节点网构成的天地网络。天地网络将成为国家的战略性基础设施, 服务于全球用户, 带动通信等产业领域。毫无疑问, 天地网络将助力世界经济协调发展, 具有巨大的经济和社会价值。据Wccfttech报道, 具有典型天地网络特征的星链(Starlink)建成

收稿日期: 2020-08-15; **修回日期:** 2020-09-10

通信作者: 郭云川, guoyunchuan@iie.ac.cn

基金项目: 国家重点研发计划基金资助项目(No. 2016YFB0801001); 国家自然科学基金资助项目(No. U1836203)

Foundation Item: The National Key Research Project and Development Program of China (No. 2016YFB0801001), the National Natural Science Foundation of China (No. U1836203)

后,可为全球任意地区的任意用户提供至少1 Gbit/s带宽的互联网服务,预计每年收入可达300亿美元,10倍于为国际空间站发送卫星及有效载荷的收入。

不同于传统互联网络,天地网络具有如下特征。

信道开放、节点暴露:在天地网络中,卫星节点暴露在太空中,合法设备通过验证后可接入卫星中进行数据通信。攻击者可能利用这种特征,通过仿冒、伪造等手段对卫星网络进行攻击。虽然地面无线传感网络、Ad-Hoc网络也具有信道开放、节点暴露等特征,但由于天地网络的战略地位,其被攻击的可能性远高于无线传感等网络。

难以维护:卫星中失效的硬件资源无法替换,虽然从原理上可动态升级与更新其软件,但前提是在设计卫星时必须确保其具备软件重构能力;同时由于软件可能包含较多的交互接口,且存在内部逻辑复杂、网络传输丢包等问题,因此在更新软件模块时可能导致新的安全问题。

高方差、大时延:在天地网络中,高轨星间/星地通信链路具有数百毫秒的长时延(通常从关口站经卫星到另一关口站的传输时延为250~300 ms);同时,星间/星地物理距离高速动态变化导致链路通信时延方差增大。

全球覆盖、就近接入:天地网络将为包括南北极、沙漠、深空等在内的无人区提供通信服务,其通信范围覆盖全球;设备可采用就近接入方式接入卫星。这种方式导致“物理边界模糊、逻辑边界强化”,增加了信息监管的难度。

上述特征导致天地网络在物理层、网络层、数据层和内容层都面临巨大威胁。物理层存在物理损毁、物理信号窃听、拦截、注入、干扰等威胁;在网络层更易遭受重放攻击、跨网攻击、DDoS攻击等安全威胁;在数据层更容易遭受数据篡改、拦截等安全威胁;在内容层容易遭受数据失窃、虚假信息恶意传播等安全威胁。

2 相关工作

2.1 统一认证

XUE等^[1]提出了“用户—卫星接入点”间相互认证的身份验证系统模型,降低了认证过程中的等待时间,并且基于空间信息网络(SIN)的特点,确定了在SIN中进行身份认证的一些基本安全需求,设计了支持批量切换的高效安全切换认证机制。LIU等^[2]提出了基于椭圆曲线离散对数问题和区块链技术的动态匿名身份认证方案,该方案为移动节点提供了安全性和快速离线认证,保证了移动节点到基础设施认证过程的安全性。YOON等^[3]针对移动卫星通信系统的高效通信需求,基于安全的单向哈希函数,设计了匿名安全认证方案,在确保安全的同时避免移

动用户和网络控制中心的复杂计算。

朱辉等^[4]利用卫星时钟高度统一和运行轨迹可预测性的特点,提出了适用于双层卫星网络的星间组网方案。该方案可在无可信第三方参与的情况下,确保各个轨道间、卫星间安全通信,提高星间的组网认证效率。张子剑等^[5]针对低轨卫星间的认证需求,设计了一种轻量化的认证协议,并进行仿真验证其效率高于3GPP AKA协议。薛开平等^[6]基于安全凭证(Token),实现了用户与拜访域的双向快速认证增强方案,部分解决了运营商无缝切换与用户跨域漫游场景下的通信连续性问题。

2.2 威胁深度精准感知和智能联动管控

在威胁深度精准感知方面,美国等发达国家都对其高度重视。自1998年至今,美国政府先后提出了EINSTEIN、SHINE、X和TreasureMap等计划,具备对全球网络信息进行多维度主动探测的能力。BASS等^[7]在1999年首次提出网络安全态势感知的概念。SIATERLIS等^[8]基于数据融合范式,结合从多个简单指标生成的证据,为D-S推理引擎提供支持,并检测对单一网络元素(高带宽链路)的攻击,能够有效提高态势评估的效率。LU等^[9]基于最小二乘支持向量机(Fuzzy Least Squares Support Vector Machine)技术,整合多源多属性信息,进而得到网络安全态势值。POOLSAPPASIT等^[10]将贝叶斯网络运用到网络安全态势评估中,该方法可以动态量化各个层次上的网络安全风险。HU等^[11]基于隐藏信念规则库(BRB)模型,提出了一种网络安全态势的预测模型,该方法考虑到专家在进行参数初始化时具有一定的主观性,因此通过改进协方差矩阵适应进化策略(Covariance Matrix Adaption-Evolution Strategy, CMA-ES)来初始化参数,提高了网络安全状况预测的准确性。

国内网络安全态势评估的研究相对国外起步较晚。陈秀真等^[12]基于入侵检测产生的报警信息和网络性能评估指标结合网络系统组织结构等信息,提出了层次化安全威胁态势量化评估模型及计算方法,分别评估攻击/漏洞层、服务层、主机层和系统层的安全状况。层次分析法可有效把握网络安全态势,但其加权具有主观性。张勇等^[13]利用马尔可夫博弈模型建模安全威胁、管理人员和用户行为,构建三方参与的博弈模型,动态实时地评估网络的安全态势。胡静等^[14]结合模糊层次分析法和BP神经网络,评估网络安全态势。

在智能联动管控方面,由于卫星网络中星间、星地通信距离相对较远,通信过程产生高传播时延,一般的入侵检测研究方法不适用于卫星网络。早期,MELEK等^[15]设计了抗DoS安全协议,对数据包头的关键字段采用答题机

制,过滤恶意数据包。针对包头中关键字段缺少保护的问题,MA等^[16]采用Rabin加密算法对安全协议中的关键字段进行保护,防止攻击者通过猜测序号、伪造MAC地址等方式构造攻击数据包,断开已建立的连接。同时,MUHAMMAD等^[17]设计了卫星网络架构下针对ICMP Flooding攻击检测与响应的机制,在时间窗口内对ICMP Echo数据包进行统计与异常检测,若发现异常则选择禁用协议或限制速率的方式进行缓解。针对卫星网络高动态、自组织、随机拓扑的特点,关汉男^[18]设计了一种用于空间网络的协同入侵检测系统CIDS-S,通过划分安全域,设计基于有限状态机的异常检测算法及自适应黑洞攻击检测算法进行协同检测,使CIDS-S具有更好的检测效果。

2.3 资源弹性重构和密码按需服务保障

在资源弹性重构方面,目前研究主要聚焦于云计算、网络功能虚拟化和软件定义网络中的资源与服务编排,只有少部分工作研究卫星网络。LI等^[19]研究了卫星/地面网络中的服务功能链编排方案,提出了多域服务功能链编排框架和启发式服务功能链映射算法。FENG等^[20]考虑服务功能复用和服务功能链归并,提出了面向地面—卫星混合云网络的服务功能链高效映射机制,提高底层资源的利用效率。开彩红等^[21]研究了中继卫星任务调度方案,该方案综合考虑时窗、任务属性、卫星资源等约束,建立了任务调度模型,设计了基于人工蜂群的卫星任务调度算法,提高了资源利用率和任务执行的可靠性。针对卫星网络服务功能编排过程中服务请求接收率低、资源开销大的问题,潘成胜等^[22]基于流量缩放因子和虚拟网络功能间关系,提出面向空间信息网络的服务功能链映射算法。该算法通过预测函数来限制映射解的搜索范围,提升全局最优解求解速度,降低了时延和资源开销。

在密码按需服务保障方面,美国通用动力公司2009年开发了基于新型“现场可编程门阵列”芯片、加密速率高达40 Gbit/s的KG-530高速网络密码机。在学术界,易卓等^[23]针对密码服务的特性,将每个密码服务拆分成多个具有顺序关系的服务分块,在确保优先级高的分块执行时间不延迟的情况下,优先执行前置分块,缩短后续分块的等待时间。许英鑫^[24]提出基于分层调度的vFPGA迁移策略,通过全局调度和局部调度两个过程分层调度vFPGA,并标记FPGA的负载,降低SLA冲突概率,减少vFPGA的迁移频率。王泽武等^[25]综合考虑密码资源利用率、网络带宽资源占用比、CPU资源利用率和内存资源利用率等指标,利用熵权法给出了虚拟密码机的评价模型,设计了虚拟密码机迁移优化算法。

3 天地网络安全风险分析

3.1 测控/运控信息安全风险

测控和运控系统作为天地网络的测量和控制中心,主要负责卫星信号、观测数据、环境数据搜集,卫星轨道、工作状态、卫星钟差计算,卫星跟踪测量,航天器姿态、轨道控制等。测控和运控系统具有“心脏”和“大脑”的作用,因此成为攻击的重要目标。测控/运控系统的安全是保证卫星及业务系统正常运行的基本条件。测控网络终端的位置分布广,设备组件复杂,攻击者可进行内部攻击,也可经由测控/运控系统与互联网间的出入口发起攻击,并通过无线信道侦听、特定射频发送信息、重放攻击等多种方式实施入侵,从而破坏测控/运控指令/遥测信息(卫星载荷运行状态信息)等数据的机密性、完整性。

3.2 终端接入安全风险

卫星终端是天地网络为各类用户提供通信服务的重要载体,包括便携终端和固定终端等多种形式。终端的安全接入是终端间、终端与卫星/地面站间进行安全通信的前提,一旦用户身份被假冒,将给合法用户甚至天地网络造成重大损失和影响。

3.3 无线信道安全风险

天地网络中,星间/星地采用激光、微波等无线方式通信,地面终端间也可能采用无线方式传输数据。由于无线通信传输设备媒介的特殊性,使得其更容易遭受嗅探、中间人等攻击,数据传输过程中被拦截、篡改、恶意插入等的可能性大大增加。

3.4 业务信息系统安全风险

业务信息系统作为天地网络中各类业务运行的基本元素,存储了大量系统管理数据、鉴别信息和重要业务数据。一旦业务信息系统的身份鉴别信息被攻击者截获、假冒和重用,其内部数据可能会被盗用或破坏;同时,各类业务数据在传输、存储过程中也面临机密性和完整性被破坏的问题。

3.5 运维管理安全风险

运维管控中心主要承担天地网络运行中的网络管理、运营管理、卫星管理等任务,并与卫星、应用系统、上级网管等各类实体之间交互信令、控制状态等信息。一方面其面临各类信息在传输、存储过程中的机密性、完整性和可用性被破坏的问题;另一方面其面临系统管理员的身份被仿冒的问题,且需要防止网络中各类设备在远程管理过程中被假冒、被劫持。

4 天地网络安全保障体系

为了降低天地网络安全风险,提出安全保障技术体系,如图1所示。该技术体系由安全支撑层、接入安全层、网络安全层、安全服务层及安全态势预警、统一安全管理系统组成,最终形成完备柔性可重构的一体化纵横协同安全防护体系,为滚动建设的天地网络提供持续支撑。

安全支撑层为天地网络各层的安全保障服务提供基础的技术支撑,包括密码基础设施和认证管理两部分。其中,密码基础设施以接口调用方式提供对称加解密、非对称加解密、哈希计算等基本密码服务;认证管理对天地网络中的用户身份、访问权限等进行统一管理,包括证书签发、撤销、更新,以及权限授予、回收与更新等。

接入安全层确保设备接入到天地网络时的安全,包括接入防护、入网认证和接入链路保护等。确保非授权设备不能接入网络,授权设备只能接入相应的网络和接入网络的链路安全。

网络安全层针对星上处理设备、地面网关等多种实体动态组网,以及不同天基接入网用户间、天基信息网与地面网络用户间业务安全互通需求,结合网络构成、网络信息流程和控制流程,在低轨星座动态组网认证基础上,综合考虑链路时延方差大的特点进行安全动态组网控制,并依据用户的差异化安全需求进行骨干网的分级保护,通过对不同网络间的域间隔离交换和互联安全管控,实现天地互联网络运行的安全可控。

安全态势感知通过威胁驱动的内嵌式数据采集获得数据,依据网络可用资源(计算资源、存储资源和网络资源

等)评估数据的汇聚时机,基于当前环境、历史数据等对原始数据进行融合分析,动态整体地识别安全威胁,生成态势报警或预警;统一安全管理监测天地网络安全设备与系统的运行状态,依据安全威胁和运行状态等要素,动态配置安全策略,并对威胁进行分级智能管控。

5 天地网络安全保障关键技术

5.1 统一安全管理与安全态势预警

统一安全管理与安全态势预警的关键技术如图2所示。在威胁驱动的精准感知方面,安全威胁感知器/感知组件负责采集安全终端/网关/系统的运行状态数据。该层由多个不同系统的独立采集程序组成,完成设备、程序、数据库、中间件、服务等应用系统各组成方面的运行状态数据的采集。采集数据由威胁感知层从各类安全终端/网关/系统中获取,经预处理后传递到数据汇集层,数据汇集层对采集数据进行融合消冗等操作,经过逐级汇聚最终存入总的数据库。分析预警层从数据库获取全部采集数据,经过融合分析得到全网安全态势,发布威胁警告,并存入数据库。

在数据汇集方面,天地网络中汇集节点所关联的终端数量动态变化,致使单个汇集节点的并发压力随之变化。为了最大程度地利用计算和传输资源,需要根据网络拓扑结构的改变对汇集层次进行调整。威胁情报汇集系统负责对全网感知数据进行高并发汇聚,通过融合消冗、传输时机优化调度和差分传输控制实现数据的最小量有序传输。该系统采用可伸缩分级汇集策略使得汇集层具有管理规模

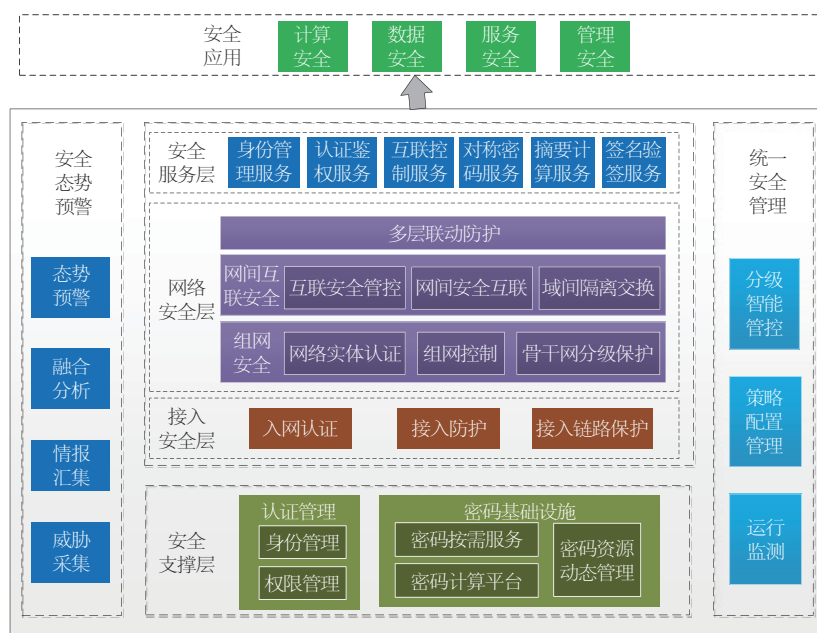


图1 天地网络安全保障技术体系

易拓展的特点，能够很好地适应天地网络规模的变化。

威胁融合分析与态势预警负责执行威胁要素提取、多维度基础数据分级统计、多层次网络安全事件分析和网络风险综合评估等任务。威胁报警由统一管理层从数据库中获取并进行展示，然后发送给智能管控层。智能管控层生成威胁处置指令，并通过管理系统逐级分解和下发，同时对威胁进行处置和效果评估。

全网安全设备统一管理系统负责对全网安全设备进行统一管理。该系统在构建网络拓扑的基础上，基于统一描述的安全策略对各类安全设备进行配置管理，并通过应急指挥调度与反馈研判对安全设备进行管控，实现威胁的及时处置。所有安全系统的配置和策略库均由统一管理层下发指令进行管理。采集指令由统一管理层的

感知策略生成功能进行管理，通过对数据库中最新威胁的分析，得到采集范围、采集内容和相关参数，生成采集指令并下发。汇集指令由统一管理层的汇集策略生成功能进行管理，通过对各级汇集状态的分析，制定汇集伸缩策略，生成汇集指令并逐级下发。

5.2 实体认证与接入防护

实体认证与接入防护是确保天地网络安全的基础之一，其关键技术如图3所示，主要包括随遇安全接入控制与安全切换、终端多域接入鉴权与漫游、高轨卫星组网实体认证及保持、低轨星座动态组网实体认证与控制、大规模实体统一身份与权限管理。

在大规模实体统一身份与权限管理方面，针对天地网络实体类型多、终端规模大、属性动态变化和信道开放等特点，研究大规模多样化实体统一身份管理、动态权限管理等内容，以实现海量身份和权限的动态关联和统一管理，确保实体高效组网认证与终端可信接入。

在高轨卫星组网实体认证及可信保持方面，针对高轨卫星相对位置固定、通信时延大、多链路并存、资源受限等特点，研究高轨卫星多链路组网实体认证、长时延链路下可信保持等内容，实现高轨卫星实体间链路自适应的安全认证和可信保持，为内嵌式安全认证模块和接入防护提供支撑。

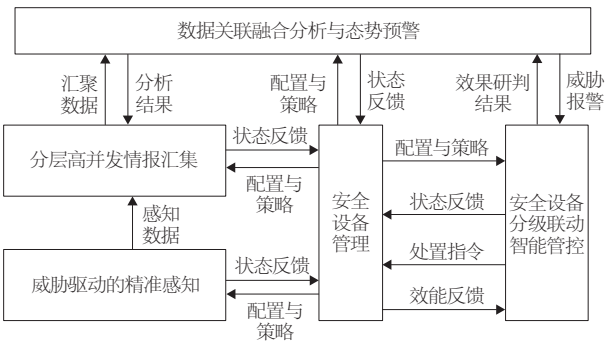


图2 统一安全管理与安全态势预警关键技术

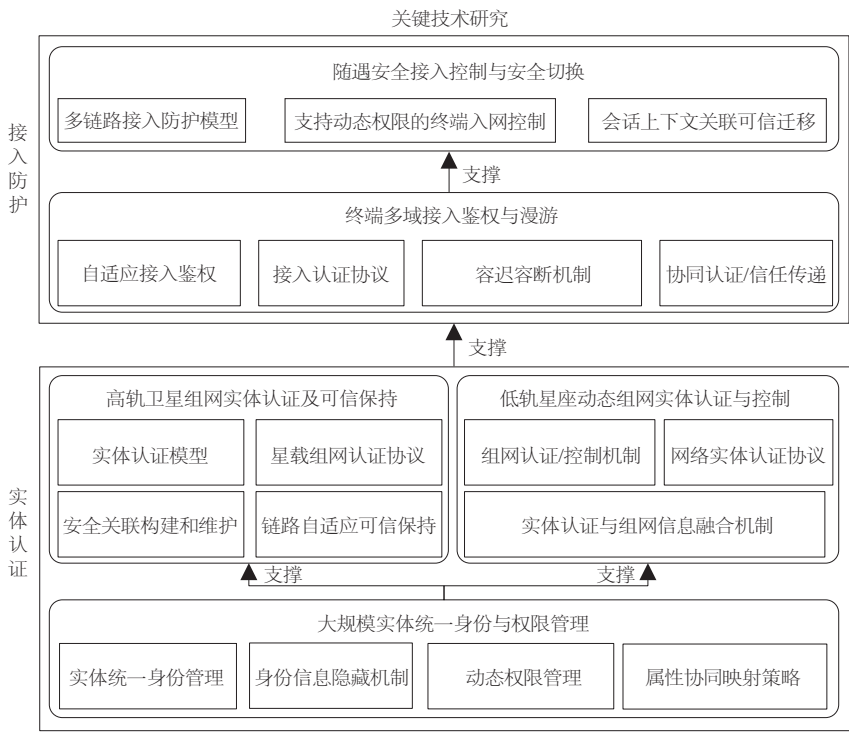


图3 实体认证与接入防护关键技术

在低轨星座动态组网认证与控制方面,针对低轨道星座网络拓扑高度动态变化、星际链路快速切换等特点,研究低轨星座动态组网认证、安全动态组网控制等内容,实现低轨卫星间的动态实体认证和弹性组网控制,为内嵌式安全认证模块和接入防护提供支撑。

在终端多域协同接入鉴权与安全漫游技术方面,面向天地网络的终端多域安全接入需求,研究终端协同接入鉴权、多域安全漫游等内容;提出支持大规模并发的接入鉴权模型,实现海量且多样化终端的多域统一接入鉴权和安全漫游。

在随遇安全接入控制与无缝安全切换方面,针对终端多模并存、链路频繁切换等特点,研究终端多链路随遇安全接入、基于切换流程的链路快速重建等内容,实现支持不同技术体制的终端、航天器、关口站等典型终端的安全接入控制和无缝安全切换。

5.3 多域网络互联安全控制

多域网络互联安全控制的关键技术如图4所示,主要包括天地网络多层联动安全防护机制、联动防护智能控制与管理、域间路由与拓扑隐藏和抗隐蔽通道的高速实时隔离交换。

在多层联动安全防护机制方面,针对天地网络安全威胁多样化、安全防护实体类型多、分区分域部署、节点自身防护能力不足等特点,基于安全接入网关和安全

互联网关的防护能力,通过对不同安全域、用户及数据类型的分析,制定差异化的过滤规则,以保证在受到攻击时,构建动态安全网关联动防护网,保证多种业务类型数据的安全传输。

在联动防护智能控制与管理方面,为保证天地网络的安全管理,需要及时有效处置所发现的安全威胁,避免威胁全网蔓延,提出管控策略动态选取与优化分解技术,根据威胁特征、被保护对象安全目标等动态选取管控策略,并结合网络拓扑和处置对象能力动态分解管控策略得到处置指令,实现安全设备联动管控。由于网络局势瞬息万变,难以保证安全策略的完全合理性,因此需在处置完成后进一步对威胁处置效果进行研判。为此提出威胁处置效果动态研判方法,实现威胁的闭环迭代处置。

在多网关联动与负载均衡方面,大规模DDoS攻击是目前常见的网络攻击手段,而大多数信息系统和中小网站都没有部署相关防御系统,因此需要在天地一体化骨干网络中对DDoS攻击进行检查和防御。在防御过程中,需要兼顾攻击检测与过滤的实时性、准确性和骨干网对高通量的要求。为此,需基于安全网关的联动防护系统架构,提出卫星通信资源受限下的联动与负载均衡技术,通过高通量精度自适应攻击流量的在线检测与过滤,在优先保证骨干网高通量的前提下,实现多网关联动与负载均衡。

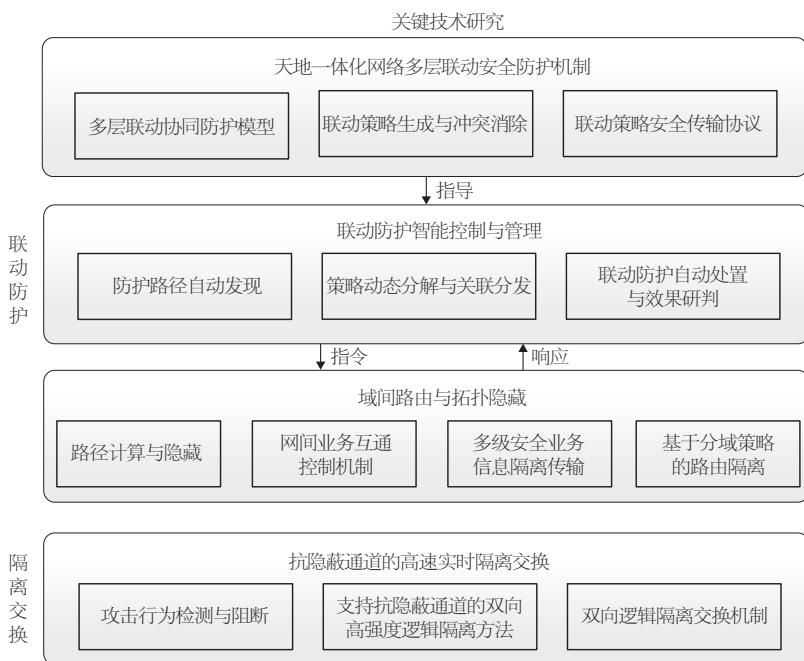


图4 多域网络互联安全控制关键技术

面向天地网络中资源受限的情形,需要为资源配置轻量级的通信协议。在密钥协商建立和已共享密钥两个阶段,分别提出了两种可组合使用的轻量级通信协议。在初始通信阶段,通过预先安装的公钥证书进行密钥协商,建立共享的安全密钥。再通过已经建立好的安全密钥实现以对称加密为基础的通信协议,进行数据传输。该方案能够兼顾轻量级通信需求和数据的安全快速传输,确保了数据的私密性、完整性和同步性。

在抗隐蔽通道的高速实时隔离交换方面,针对目前安全隔离交换技术存在的缺点和不足,如抗隐蔽通信能力不足等,提出抗隐蔽通道的数据交换方法,解决网络安全域由“物理隔离变逻辑隔离”所带来的安全隐患,为不同安全等级网络间的数据交换提供高强度的双向交换通道。

5.4 密码按需服务

在密码资源动态管理与协商方面,天地网络系统具有设备类型多、密码资源多、分区分域复杂、行政管理归属复杂等特点。不同用户域在业务类型、安全需求、网络资源状况等方面存在差异,不同用户域应配置不同的密码算法和密钥,其安全级别和密码服务类型不同,这导致多个用户域密码资源跨域管理复杂、管控信息种类多等问题。为解决以上问题,需突破跨网互联互通密码资源管理、多用户安全域动态组网密码资源分发、密码资源动态重构与加载等技术瓶颈,采用全网密码资源的动态识别、分发与配置机制,实现集中式与分布式相结合的分区分域密码资源动态管理,满足不同分区分域的业务安全隔离和防护需求,并提供与政府等密码基础设施的接口,为一体化网络密码按需服务提供密码资源管理保证。

在场景适应的高性能密码计算架构及平台方面,天地网络用户终端类型众多、用户业务多样、通信网络动态变化、用户连接并发频繁、不同安全等级用户互联互通,需要设计全新的计算服务架构,以适配星上、地面等各种应用环境。同时,天地网络中终端数量和网络业务的增长非常迅速,作为网络业务的支撑基础设施,密码计算平台需要具备容量可扩展、功能可重构的特点,以保证整个网络的持续发展。为此需提出适应天地一体化场景的高性能密码计算架构,并设计高性能的密码计算平台。在高性能密码计算架构中,需归一化密码计算及服务、高效管理密码运算状态、按需重构密码计算单元、服务状态全程跟随的密码服务调度、多核多密码算法高速数据透明交换等实现了密码计算性能线性可扩展、密码服务高并发、数据高吞吐率、功能可重构。

在密码装置安全防护方面,天地网络密码设备类型多、分布区域广、应用环境高度开放,易受到窃听、篡改等攻击。同时,空间环境下卫星节点密码设备易受高能粒子辐照影响,可能会对星上电子存储和运算数据形成高低电平的翻转,造成计算结果错误。针对以上威胁,需突破空间抗辐照的算法多核管理与调度等关键技术,保障天地网络系统中密码装置的安全性和可靠性。

5.5 安全服务动态重构

天地网络安全服务的动态重构的关键技术如图5所示,主要包括多粒度高并发用户行为仿真技术、差异化动态可配置的网络仿真技术、天地双骨干网络弹性重构技术。

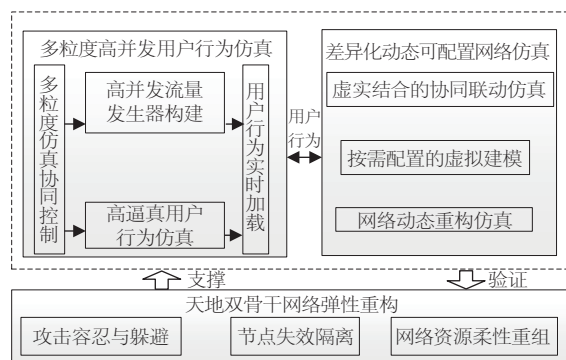


图5 动态重构关键技术

在多样化高并发用户行为仿真方面,针对天地网络中用户行为多样化的特点,研制用户行为仿真系统,实现对接入终端用户的行为仿真,并可部署和加载上述用户行为及可控制其仿真过程。

在差异化网元实体的大规模高逼真模拟方面,针对天地网络系统复杂、拓扑持续变化、网元类型多、差异大等特点,在分析天地网络中各类网元和终端设备等实体在通信体制、交换体制、交换容量等方面具有的差异性的基础上,研发差异化动态可配置的网络仿真系统。实现天地组网不同场景的差异化仿真、网元模拟器的安全功能嵌入、大规模虚拟网元的按需自动部署以及卫星链路高性能仿真等功能。

在场景适应的天地双骨干网络弹性重构方面,针对天地网络中各种故障和攻击、新的卫星资源加入等场景,突破弹性重构统一控制、联动弹性重构、可重构网络仿真等技术,提出基于场景适应的网络重构、安全能力重构等机制,构建虚实结合的可重构天地双骨干网络仿真系统,支持天地一体化安全防护能力的滚动建设。

参考文献：

- [1] XUE K, MENG W, LI S, et al. A secure and efficient access and handover authentication protocol for internet of things in space information networks[J]. IEEE Internet of Things Journal, 2019:1-1.
- [2] LIU Y N, LV S Z, XIE M, et al. Dynamic anonymous identity authentication (DAIA) scheme for VANET[J]. International Journal of Communication Systems, 2019, 32(5): e3892.
- [3] YOON E J, YOO K Y, HONG J W, et al. An efficient and secure anonymous authentication scheme for mobile satellite communication systems[J]. EURASIP Journal on Wireless Communications and Networking, 2011(1):86.
- [4] 朱辉, 武衡, 赵海强, 等. 适用于双层卫星网络的星间组网认证方案[J]. 通信学报, 2019, 40(3):1-9.
ZHU H, WU H, ZHAO H Q, et al. Efficient authentication scheme for double-layer satellite network[J]. Journal on Communications, 2019, 40(3):1-9.
- [5] 张子剑, 周琪, 张川, 等. 新的低轨星座组网认证与群组密钥协商协议[J]. 通信学报, 2018, 39 (6):150-158.
ZHANG Z J, ZHOU Q, ZHANG C, et al. New low-earth orbit satellites authentication and group key agreement protocol[J]. Journal on Communications, 2018, 39 (6):150-158.
- [6] 薛开平, 周焕城, 孟薇, 等. 天地一体化网络无缝切换和跨域漫游场景下的安全认证增强方案[J]. 通信学报, 2019, 40(6):138-147.
XUE K P, ZHOU H C, MENG W, et al. Secure authentication enhancement scheme for seamless handover and roaming in space information network[J]. Journal on Communications, 2019, 40 (6):138-147.
- [7] BASS T, GRUBER D. A glimpse into the future of ID[J]. login::the magazine of USENIX&SAGE, 1999, 24(4):40-45.
- [8] SIATERLIS C, MAGLARIS V. One step ahead to multisensor data fusion for DDoS detection[J]. Journal of Computer Security, 2005, 13: 779806
- [9] LU J, YANG X, ZHANG G. Support vector machinebased multisource multiattribute information integration for situation assessment[J]. Expert Systems with Applications, 2008, 34(2): 1333-1340
- [10] POOLSAPPASIT N, DEWRI R, RAY I. Dynamic security risk management using bayesian attack graphs[J]. IEEE Transactions on Dependable and Secure Computing, 2012, 9(1):61-74.
- [11] HU G Y, ZHOU Z J, ZHANG B C, et al. A method for predicting the network security situation based on hidden BRB model and revised CMA-ES algorithm [J]. Applied Soft Computing, 2016, 48:404-418.
- [12] 陈秀真, 郑庆华, 管晓宏, 等. 层次化网络安全威胁态势量化评估方法[J]. 软件学报, 2006, 17(4): 885897.
CHEN X Z, ZHENG Q H, GUAN X H, et al. Quantitative hierarchical threat evaluation model for network security[J]. Journal of Software, 2006, 17(4):885-897.
- [13] 张勇, 谭小彬, 崔孝林, 等. 基于 Markov 博弈模型的网络安全态势感知方法[J]. 软件学报, 2011, 22(3): 495508.
ZHANG Y, TAN X T, CUI X L, et al. Network security situation awareness approach based on Markov game model[J]. Journal of Software, 2011, 22(3):495-508.
- [14] HU J, TIAN M, WANG Y. Risk assessment and comparative analysis for technical standards alliance based on fuzzyahp method and bp neural network method[C]//2016 Portland International Conference on Management of Engineering and Technology, Honolulu, 2016, 597-605.
- [15] MELEK O, REFIK M. Denial of service prevention in satellite networks[C]//IEEE International Conference on Communications, 2004: 4387-4391.
- [16] MA T, LEE Y H, MA M D. Protecting satellite systems from disassociation DoS attacks[J]. Wireless Personal Communications, 2013, 69(2): 623-638.
- [17] MUHAMMAD U, MARWA Q. Mitigating distributed denial of service attacks in satellite networks[J]. Transactions on Emerging Telecommunications Technologies, 2020, 31(6).
- [18] 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: 上海交通大学, 2014.
GUAN H N. Research on key security technologies in LEO-based space network[D]. Shanghai : Shanghai Jiao Tong University, 2014.
- [19] LI G, ZHOU H, FENG B, et al. Horizontal-based orchestration for multi-domain SFC in SDN/NFV-enabled satellite/terrestrial networks[J]. China Communications, 2018, 15(5):77-91.
- [20] FENG B, LI G, LI G, et al. Efficient mappings of service function chains at terrestrial-satellite hybrid cloud networks[C]//2018 IEEE Global Communications Conference (GLOBECOM). IEEE, 2018: 1-6.
- [21] 开彩红, 肖瑶, 方青. 基于人工蜂群算法的中继卫星任务调度研究[J]. 电子与信息学报, 2015, 37(10):2466-2474.
KAI C H, XIAO Y, FANG Q. Relay satellite scheduling based on artificial bee colony algorithm[J]. Journal of Electronics & Information Technology, 2015, 37(10):2466-2474.
- [22] 潘成胜, 梁芷铭, 石怀峰, 等. 面向并发业务的卫星网络服务功

能链编排优化算法[J]. 计算机工程, 2020.

PAN C S, LIANG Z M, SHI H F, et al. Concurrent spatial information network service function chain quick scheduling method[J]. Computer Engineering, 2020.

- [23] 易卓, 孙慕明, 杜学绘. 基于服务映射与分块调度的天基接入点密码资源调度算法[J]. 信息安全研究, 2019, 5(9):805-811.

YI Z, SUN M M, DU X H. A cryptography resources scheduling algorithm for space-based access points based on service mapping and blocks scheduling[J]. Journal of Information Security Research, 2019, 5(9):805-811.

- [24] 许英鑫. 云密码资源池调度关键技术研究[D]. 郑州: 战略支援部队信息工程大学, 2019.

XU Y X. Research on key technique of cloud cryptographic resource pool scheduling[D]. Zhengzhou: Information Engineering University, 2019.

- [25] 王泽武, 孙磊, 郭松辉, 等. 密码云中基于熵权评价的虚拟密码机调度方法[J]. 计算机应用, 2018, 38(5):1353-1359.

WANG Z W, SUN L, GUO S H, et al. Scheduling method of virtual cipher machine based on entropy weight evaluation in cryptography cloud[J]. Journal of Computer Applications, 2018, 38(5):1353-1359.

[作者简介]



李凤华, 男, 博士, 中国科学院信息工程研究所研究员, 博士生导师, 主要研究方向为网络与系统安全、隐私计算、密码应用。



张林杰, 女, 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。



陆月明, 男, 博士, 北京邮电大学教授、博士生导师, 主要研究方向为分布式计算、区块链技术、网络空间安全。



耿魁, 男, 博士, 中国科学院信息工程研究所高级工程师, 主要研究方向为网络安全。



郭云川, 男, 博士, 中国科学院信息工程研究所正高级工程师、博士生导师, 主要研究方向为访问控制。