

基于星载网络探针的通信卫星信息安全监测系统设计

王明剑, 范丹丹, 徐潇申, 李孟
(北京空间信息传输中心, 北京 100023)

摘 要: 为提升通信卫星信息安全防护能力, 在星上资源受限的情况下, 实现系统信息安全监测, 在比较部分典型信息安全防护设计的基础上, 梳理通信卫星系统基本特性和面临的安全威胁, 分析并总结安全防护能力提升的制约因素, 提出一种利用星载网络探针技术采集卫星安全数据, 依托地面系统构建数据分析平台和综合监测系统的信息安全监测方法, 在资源占用度较低的前提下保证卫星业务正常运行, 实现系统安全监测和安全告警, 并对系统实际工作运行展开分析和验证。

关键词: 通信卫星; 星载探针; 信息安全; 安全监测

中图分类号: TN927

文献标识码: A

doi: 10.11959/j.issn.2096-8930.2023019

Design of the Monitoring System for Communication Satellite Information Security Based on Spaceborne Network Probe

WANG Mingjian, FAN Dandan, XU Xiaoshen, LI Meng
Beijing Space Information Transmission Center, Beijing 100023, China

Abstract: To enhanced the information security protection capability of communication satellites and solved the information security monitoring problem of the system under the condition of limited on-board resources, based on the comparison of some typical information security protection designs, this paper summarized the characteristics and security threats of the communication satellites, analyzed the constraints on improved security protection capabilities, then proposed a sort of collecting satellite security data by using space based probe technology, built data analysis platform and integrated monitoring system based on the ground system, which could realized the system security status monitoring and security alarm on the premise of ensuring the normal operation of the satellite business and low resource occupancy. At last the actual operation of the system was analyzed and verified.

Keywords: communication satellite, space based probe, information security, security monitoring

0 引言

通信卫星的暴露性和传输链路的开放性, 导致空间段已成为卫星通信系统安全防护最为薄弱的环节。随着电磁攻击、网络渗透及供应链漏洞^[1]等现实威胁的不断加剧, 通信卫星的信息安全问题更为凸显^[2]。与此同时, 以卫星互联网为代表的星座系统在遵循平台轻量化、接入便捷化、服务多样化等发展路径时, 信息安全防护机制和手段的部署及运用^[3]愈加受限于星上计算和存储能力、协议体制、业务传输需求等因素, 加深了其应对安全风险的难度。

当下卫星信息安全已直接关联卫星通信网络运维安全、传输安全和数据安全等各层面, 安全监测能力研究也已逐步从系统内部器件运行、外部空间环境影响及非自然因素应对处置等方面, 快速向卫星运行状态和承载业务的信息安全防护方向汇聚和延伸, 出现了各类以卫星运行和数据监测为基本手段的安全防护设计。比较和审视这些设计, 可发现其在实现系统安全性增强的同时, 仍存在一定的优化和提升空间。如参考文献[4]主要从网络信息安全视角提出了基于包含卫星测控信息在内的多源数据融合技术来实现网络安全态势的感知, 但未对卫星安全数据采集来源进行详细阐述。参考文献[5]提出了星载卫星信息安全

系统设计构想,主要关注物理层面对空间环境和外部威胁的感知,对卫星自身信息安全分析和防护欠缺考虑。参考文献[6]提出了综合利用遥感类卫星运行状态信息开展关键业务监控报警功能的设计与实现,但其安全关注对象仍以地面系统和业务数据为主。综上,卫星应用系统信息安全监测功能的设计和实现,应立足星上安全机制部署及安全数据采集、平台与业务安全监测数据融合、星地协同安全态势监测等方面实现深入和拓展。

聚焦卫星通信业务应用本身,由于其天然的信息传输功能特性,现有地面通信网络成熟的安全信息技术可在卫星通信网络中进行快速且充分的借鉴与移植。其中,星载网络探针作为网络探针技术在空间信息网络领域的重要拓展和应用,能够通过采集在轨卫星各类状态监视数据和运行控制数据,依托地面强大的数据处理和分析能力构建通信卫星信息安全监测系统,为高效、灵活、精准地解决空间段安全防护难题提供重要思路,在预警威胁实时性、安全监测精准性、安全态势系统性方面相较于基于测控的卫星信息安全监测均有较大程度提升。本文基于对通信卫星的安全威胁深入分析思考,提出了利用星载网络探针技术构建通信卫星信息安全监测系统,实现系统安全状态的有效监测和安全威胁的快速告警的设计理念,规范了系统运行模式和工作流程,并加以实验验证,旨在为后续卫星互联网信息安全保障建设提供解决思路。

1 通信卫星信息安全问题分析

1.1 系统安全特征分析

(1) 通信卫星的暴露性和传输链路的开放性

通信卫星运行于各类固定轨道,空间参数确定,定点位置和运转轨迹可测可循,客观上只要处于通信卫星波束照射覆盖范围内,利用同频段、同体制射频发送能力相当的终端均可以对卫星实施攻击。此外,由于各类星地、星间无线传输链路的开放性,如果缺乏合理有效的防护手段,极易出现通信载波受扰,通信信号被截获并进行分析^[7],信息遭篡改及系统被侵入等安全问题。

(2) 网络联通的多样性和网络拓扑的动态性

为保证通信传输服务的快捷灵活,卫星通信系统需要与分布在各物理域空间的异构网络实现互联互通^[8],传输业务多样,传输协议复杂,对跨网跨域间的网络接入、传输控制、数据交换和安全防护均提出了较高要求,工程层面解决难度较大。同时,由于各空间分散的网络节点和通信实体均处于快速移动状态,通联关系和业务切换频繁,卫星通信网络拓扑结构呈现高动态特征,网络安全接入和

安全切换的控制管理更为复杂困难。

(3) 星上计算和存储能力的受限性

出于卫星轻量化考虑,整星功耗、质量、体积等有限,加之空间恶劣环境制约,通信卫星,尤其是低轨星座通信卫星,在星上遥测遥控、数据管理和综合电子等分系统的资源配置上,有关运算处理、数据存储、传输速率、空间容积和功率分配等能力受限^[9],难以部署和运行较为复杂的信息安全监测机制及安全算法。卫星入轨后,星载信息系统软硬件相对固化,目前均难实现在轨功能的快速升级更新,系统安全风险防范的灵活性和可重构能力较弱。

1.2 主要安全威胁

(1) 内部系统网络受攻击

通信卫星主要利用星上数据传输网络实现卫星平台、有效载荷以及各功能组件间的信息通信。理论上,攻击者只要通过开放的无线信道就可以将攻击行为导入卫星内部网络及功能组件,进而对各分系统控制管理进行攻击并造成损伤。此外,通信卫星数据管理分系统包含与地面系统相近的路由和网络协议栈处理,属于多层链路,采用通用网络协议,面临与地面系统网络相同的安全威胁,更易遭受网络攻击。

(2) 信息失窃或遭控制接管

通信卫星使用的芯片有可能因供应链漏洞造成恶意预置后门、预设逻辑炸弹等安全威胁,对卫星平台和有效载荷的安全运行构成巨大风险。一方面,攻击者可利用信息产品的漏洞和后门程序,绕过系统安全管理控制,侵入星务系统,预设网络攻击工具,开展网络嗅探和侦收,为伺机实施网络攻击做准备;另一方面,攻击者利用预设逻辑炸弹,在预设逻辑条件满足时,自主启动,擦除或扰乱卫星运行数据,导致系统异常。

1.3 小结

综上,通信卫星的安全脆弱性极易引发攻击事件,已经严重威胁系统运行和数据传输安全,受制于星上有限的运算和存储能力,无法部署资源占用较大的既有成熟安全监测系统,一定程度上影响卫星信息安全状态的获取和分析效能,已经成为制约提升卫星安全防护能力的现实难题。

据此,本文提出设计和应用通信卫星专用信息安全网络探针,利用其部署便捷、功能灵活、资源占用小^[10]的优势,在不影响星上业务工作流程和减少星上资源耗用的同时,获取必要的信息安全数据,利用遥测链路将其发送至地面大数据分析平台。通过与地面孪生同构系统的信息关

联量进行对比,获得真实的卫星信息安全态势,解决卫星安全监测难题。此设计的优势在于:基于卫星数据开展监测,前移信息安全防护边线,提升了安全监测的时效性和灵活度。采用卫星采集和地面分析联合的工作模式,将数据处理分析重点部署在地面,减轻了星上数据运算和存储压力,同时又便于与卫星通信系统整体安全监测数据进行融合分析,拓展了安全监测的视野和范围。

2 基于星载网络探针的安全监测系统设计

2.1 星载网络探针方案

探针广泛应用于各种行业,应用于计算网络领域,即为网络探针,主要侦听网络数据包,区别于普通侦听模式,“探针”可集成数据包捕获、过滤、分析等多种功能^[1],分析结果存储在探针内存或磁盘之中,也可通过探针发送到后台数据库再次分析和存储。星载网络探针技术即是地面系统网络探针部署和运用于通信卫星信息系统及网络的技术,有别于地面系统,星载网络探针需要结合星上系统工作环境和功能架构,进行有针对性的特殊设计,才能实现对安全状态的有效监测。

考虑到卫星资源短缺特性,为减少能耗开销,提高工程实用性,针对星载安全探针的设计主要采用2种方式:桥式星载网络探针和插件接口式星载网络探针。其中,桥式星载网络探针以硬件设备形态部署在卫星星务系统关键部位,对数据包透明转发的同时,进行流量统计和必要

的内容分析,并将结果记录于缓存中,定时由载荷传输探针发送给地面大数据分析平台。插件接口式星载网络探针主要是在测控系统中部署定制化软件插件,定义标准接口,完成流量统计、日志信息以及必要的内容分析,并将分析及统计结果通过星载总线传输给载荷传输探针系统,定时传输给地面大数据平台。

2.2 安全监测系统组成

基于星载网络探针技术的通信卫星信息安全监测系统架构如图1所示。

系统采用星地一体设计,基于“星载安全探针+数据分析平台+安全监测系统”架构,协同实现通信卫星信息安全态势监测。其中,星载安全探针主要采集星上信息安全数据,通过测控系统将安全数据与遥测数据同步下发至地面测控系统。地面测控系统转发至数据分析平台进行分析和处理,并将处理结果传送至安全监测系统。安全监测系统基于攻击特性比和异常规则判定,利用各类算法和模型库,对安全数据进行关联分析、威胁判定、攻击监测及安全评估。需要说明的是,本设计安全监测功能与通用网络安全态势感知平台具有一定区别,本设计重点在于卫星信息安全状态:卫星访问信息流量较少,容易统计和分析;卫星传输协议较单一,组成类型简单;卫星信息来源和信息流向简单等特点。根据以上特点,针对卫星信息安全监测数据的分析模型主要关注卫星遥控指令收集整理和对比。

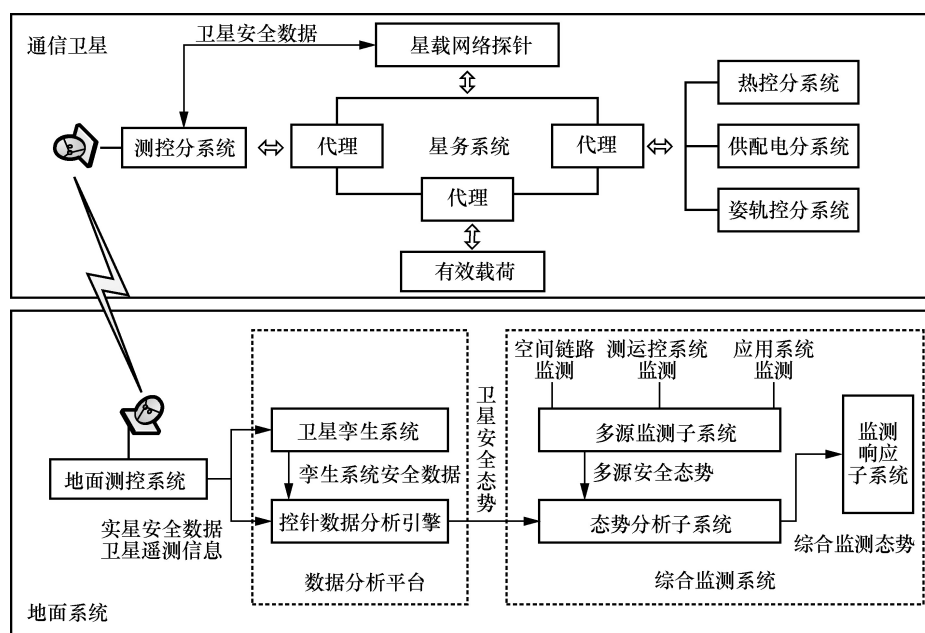


图1 通信卫星安全监测系统组成示意

在具体功能组成上,星载安全探针主要部署于卫星星务系统,利用安全代理(Agent)模块,分别采集星务与测控系统、通信载荷、姿轨控系统等之间的通信和异常数据。安全数据分析平台部署与地面测运控系统,采用星载同构孪生设计,利用系统镜像遥控响应数据与星上采集数据进行对比,判断卫星是否处于正常运行状态,初步诊断受到攻击的位置和类型。安全监测系统同步接收星上采集数据、安全数据分析平台分析结果,并汇总融合空间链路、地面测运控及应用系统中的终端数据、管理信息、网络流量、应用行为、轨道运行信息,开展联合安全监测。

2.2.1 星载网络探针

星载网络探针是实现卫星安全监测功能的核心部件,负责对卫星信息安全相关的原始数据进行采集,采集的数据类型包括测控协议数据流量、关键节点数据流量、关键节点数据摘要值信息、关键节点同步信息和关键部件日志信息等。星载网络探针整体由3部分组成。

(1)安全代理模块:主要由星务软件提供接口,也可直接并联于星载总线,完成对原始数据的处理、收集和捕获工作,包含基本摘要信息以及信息统计等方面的内容。

(2)运行管理模块:主要实现对网络探针的管理工作,包括性能监控、信息监测报告、数据信息储存以及日志生成等。

(3)数据传输模块:主要负责将探测到的信息按照指定策略传送给地面数据分析平台,可设计延迟发送功能,保证卫星与地面非通信时段监控数据的存储,在通信建立后及时发送到地面。

星载网络探针采取轻量级部署原则,以期尽量减少通信卫星软硬件资源消耗,具备针对星间、星地协议的检测分析能力,能够检测洪泛攻击、路由篡改攻击以及黑洞攻击等网络攻击行为。软件结构上具备可扩展性,探针各项功能以基础模块加载功能载荷的方式实现,可通过加载新载荷的方式扩展新功能。

2.2.2 数据分析平台

数据分析平台构建星载同构孪生系统,与在轨运行卫星采用相同架构及软硬件设计,同步接收和响应地面测控系统发送至卫星的指令信息,从而最大限度地实现星上安全数据的无差别判定。星载同构孪生可以采用物理孪生系统来实现验证比对,也可采用数字孪生技术来降低系统成本。数据分析平台包含2个系统。

(1)卫星孪生系统:主要负责接收和响应地面测控系统的遥控指令密文,保证输入的一致性和机密性,产生孪生系统遥测信息数据,并通过相同部署的网络探针进行数

据采集。在设计上,孪生卫星应与实体卫星保持严格的状态一致性,通过对在轨实体卫星各类实时状态数据的收集分析^[12],实现实体卫星与孪生卫星同步映射的目的,最终确保孪生系统能够对真实测控指令产生与在轨实体卫星一致的响应,并在在轨实体卫星状态异常后通过孪生卫星的响应差异性实现安全监测功能。

(2)探针数据分析引擎:主要接收卫星孪生系统网络探针采集的安全数据,并与实星网络探针采集的安全数据进行对比,并结合卫星遥测信息进行综合分析,得到卫星初步安全态势信息。探针数据分析引擎包含数据归并去重、数据简单筛选、数据优先处理、安全审计和安全数据解析等功能部件,可以实现对实体卫星和孪生卫星的探针采集数据的初始处理、全面比对和深度分析。

2.2.3 综合监测系统

综合监测系统主要利用数据分析平台输出的卫星初步安全态势结果,融合卫星通信系统内外部安全要素及威胁情报信息,实现安全监测信息体系化融合和集中化管控,并能够对复杂、高级威胁行为进行关联分析和溯源定位,提升全系统安全运维和管控的智能化水平,实现全域安全态势的集中监管和决策。综合监测系统包含3个子系统。

(1)多源监测子系统:主要负责收集和汇聚空间链路、地面测运控及应用系统中的终端监控、系统管控、网络流量、应用行为、轨道运行等各类状态监视信息,拓宽安全监测数据来源,形成多源、多维安全运维信息的高效融合和综合分析。多源监测的目的在于应对各类安全威胁来源的多样性,针对卫星通信系统的安全攻击途径可能起始于空间链路、地面测运控系统或业务应用终端,也有可能是以上几个领域的结合,因此对于多源数据的综合监测和融合分析是应对复杂性攻击的有效手段。

(2)态势分析子系统:主要基于数据分析平台提供的卫星安全态势初步分析结果,融合多源监测子系统形成的相关系统安全态势,依托各类攻击特征库、漏洞库、补丁库、恶意指令库、白名单库等,构建威胁分析模型、关联分析算法、机器学习算法、排序算法等分析算法模型,结合系统资产管理、安全事件、原始日志等信息的审计管理,开展关联分析、威胁判定、威胁监测和溯源定位,并对安全风险进行综合评估。同步对存在的安全风险进行策略制定和比对,预测系统的安全态势,并可实现安全态势数据的可视化展现。

(3)监测响应子系统:主要对监测到的安全事件进行及时响应,按应急任务处理进度分布、数量等进行统计分析,并对安全事件处理全过程及结果进行记录和管理,展

示监测响应工作的开展情况,针对安全态势分析的监测结果进行告警信息发布。在本设计中,监测响应的实现有赖于相关安全服务功能的配置和支撑,目前暂不属于安全监测范畴,需要在系统上进行进一步的系统功能扩展,在此不再展开讨论。

3 卫星信息安全监测运用

3.1 工作流程

卫星信息安全监测系统的基本工作流程如图2所示。

(1) 通信卫星在轨运行期间,星载网络探针采集卫星重要信息安全相关运行和状态数据,实时或暂时存储后,利用星地间遥测链路回传至地面测控站,实现卫星安全监测数据下传。

(2) 地面测控站根据工作计划,实时或定期接收星载网络探针下传数据,与地面卫星孪生系统产生的镜像遥控指令响应数据进行比对和分析,形成卫星初步安全态势,经过初步数据处理分析后,将信息数据传送至安全监测系统。

(3) 综合监测系统接收数据分析平台输出态势信息,同步汇集和分析相应空间链路、地面测控系统和应用系统安全运行态势数据,经过滤和处理后,开展行为关联分析、攻击检测分析、数据挖掘分析等,并对异常分析结果进一步开展威胁判定、追踪定位和风险评估,同步发布告警信息,指导应急处置。

3.2 运行模式

综合考虑卫星测控数据传输链路的可用周期、传输容量及地面测控系统站点配置等因素,减少安全监测功能对卫星正常测控业务的影响和资源占用,提升系统运行灵活性和可操作性。系统可采用数据驱动、人工驱动和定时驱动3种运行模式。

(1) 数据驱动模式:主要从异常数据的实时监测和判定出发,系统全时工作,一旦星载网络探针检测有异常出现,系统即采取最短周期、最优路径下传监测数据,地面系统即时响应并开展分析研判,发布告警信息。此种模式

下时效性最高,但资源占用也较大,适合高威胁场景下的系统安全监测。

(2) 人工驱动模式:主要由地面系统操作人员发起,根据需要配置星地间链路,并对各类检测和分析参数进行专门配置,主动操作和控制全系统开展有针对性的安全监测。此种模式下精准性最高,但需要进行详细任务规划和准备,适合对已知威胁场景下的系统安全监测。

(3) 定时驱动模式:主要根据卫星通信系统整体构建和安全防护要求,合理设计安全监测周期和检测标准,形成定时安全监测和告警机制,优化相关资源配置,定时开展安全监测。此种模式下稳定性最高,但对临时突发攻击等安全攻击的响应时效性较差,适合低威胁场景下常态化的系统安全监测。

在系统实际部署和运行过程中,应根据卫星通信系统体系架构、服务要求、资源配置,现实中安全威胁情况以及安全防护等级要求,合理设置和调整运行模式,以期实现对各类复杂应用场景的高效应对。

3.3 实验验证

针对本文提出的系统设计,采用实验系统模拟运行的方式对安全监测和安全告警开展模拟验证。系统基于“星载CPU+国产化主板+可信操作系统”架构,网络安全探针嵌入计算机主板。实验验证环境如图3所示。

实验系统构建了模拟通信卫星系统、模拟卫星攻击工具、模拟地面测控系统以及安全监测系统,利用计算机网络和中频信号传输线路模拟无线卫星测控信道连接各系统,实现卫星遥测遥控、攻击侦收接入和卫星安全监测等实验功能的模拟运行,并通过“安全监测态势展示”实时显示系统安全运行状态。实验过程如下。

(1) 攻击实施:模拟卫星攻击工具接入无线卫星测控模拟信道。对地面测控系统和模拟通信卫星系统展开系统扫描和信息收集,利用地面系统漏洞,绕过安全设备篡改遥控指令,影响卫星运行状态;或在模拟空间链路中截获遥控指令并篡改数据,上注木马或植入APT或重放遥控

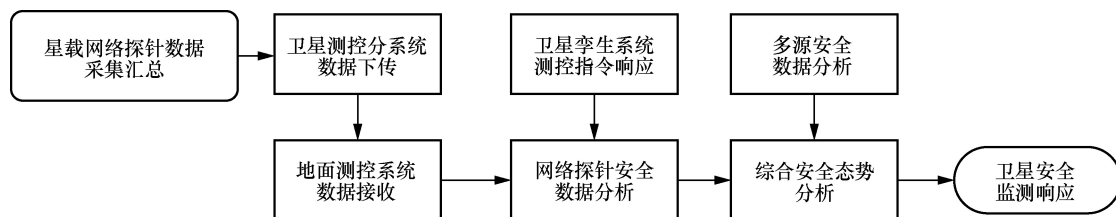


图2 系统基本工作流程

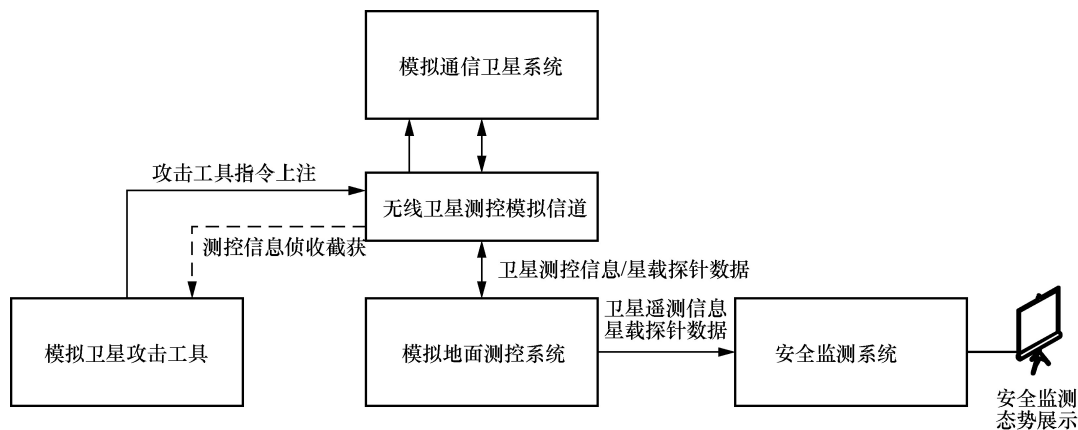


图3 实验验证环境示意

指令,使卫星重复调整姿势,偏离正常轨道;或对下传遥测数据进行篡改,导致无法及时判断卫星状态和调整卫星运行,影响业务正常进行。

(2)安全监测:攻击工具对地面测控系统进行扫描时,地面设备对嗅探包数据进行采集,利用安全监测系统进行对比分析,触发安全事件;星载网络探针对于卫星嗅探包数据进行采集,与遥测数据一起下发至安全监测系统,并与地面设备采集数据进行对比分析,触发安全事件。

(3)安全告警:当攻击展开时,安全监测系统实时探测地面测控系统用户异常行为、空间链路违法接入和星载网络探针采集异常数据,对相关安全事件进行监测分析后,及时发出安全告警信息。

4 结束语

将地面通信网络中较为成熟的信息安全技术应用于卫星通信网络,是快速提升卫星通信系统信息安全防御能力的有效途径,可以减轻重新设计、研发新技术的工作量,同时既有技术又具备较强的适应性和稳定度,但在工程实践过程中必须对卫星通信系统的基本特性和自身特点加以充分考虑。本设计中,采用天地一体结合和多域信息融合思路,可有效解决空间资源受限情况下网络安全机制部署及运用的难题,实现对卫星通信系统复杂安全事件的快速响应和有效应对。希望本文提出的基于星载网络探针技术的安全监测系统设计能为体系化解决卫星通信网络信息安全防御问题提供有益的借鉴和参考。

参考文献:

[1] 高恒伟,何辉,韩志钢,等. 卫星通信网络的安全威胁及防范策略[J]. 电子世界, 2021(4): 38-39.

GAO H W, HE H, HAN Z G, et al. The security threats of satellite communication network and preventive strategies[J]. Electronics World, 2021(4): 38-39.

[2] 李凤华,殷丽华,吴巍,等. 天地一体化信息网络安全保障技术研究进展及发展趋势[J]. 通信学报, 2016, 37(11): 156-168.

LI F H, YIN L H, WU W, et al. Research status and development trends of security assurance for space-ground integration information network[J]. Journal on Communications, 2016, 37(11): 156-168.

[3] 高瓴园,王妮炜,陆洲. 卫星互联网星座发展研究与方案构想[J]. 中国电子科学研究院学报, 2019, 14(8): 875-881.

GAO Y Y, WANG N W, LU Z. The development research and construction suggestion of satellite Internet constellations[J]. Journal of China Academy of Electronics and Information Technology, 2019, 14(8): 875-881.

[4] 董坤,张海霞,刘艳梅,等. 宽带卫星网络安全态势感知技术[J]. 信息网络安全, 2020(S2): 100-101.

DONG K, ZHANG H X, LIU Y M, et al. Situation awareness technology of broadband satellite network security[J]. Information Network Security, 2020(S2): 100-101.

[5] 李旻,姚方競. 星载信息安全保障系统构想[J]. 航天电子对抗, 2007, 23(6): 12-13.

LI M, YAO F J. Conception of satellite-carried information security assurance system[J]. Aerospace Electronic Warfare, 2007, 23(6): 12-13.

[6] 谢利子,赵现纲,郭强,等. 风云系列气象卫星关键业务监控报警系统的设计与实现[J]. 计算机应用, 2012, 32(S2): 192-195.

XIE L Z, ZHAO X G, GUO Q, et al. CBMS: Critical business monitoring system of Fengyun meteorological satellites[J]. Journal of Computer Applications, 2012, 32(S2): 192-195.

[7] YANG G X, YANG X. Design of adaptive anti-jamming antennas

- of direct sequence spread spectrum receiver[C]//Proceedings of the 2012 Second International Conference on Electric Technology and Civil Engineering. NewYork: ACM, 2012: 846-849.
- [8] YIN Z Z, ZHANG L, ZHOU X W, et al. QoS-guaranteed secure multicast routing protocol for satellite IP networks using hierarchical architecture[J]. International Journal of Communications, Network and System Sciences, 2010, 3(4): 355-363.
- [9] 韩笑冬, 叶勉. 通信卫星信息系统设计技术[M]. 北京: 中国宇航出版社, 2019.
- HAN X D, YE M. Design technology of communication satellite information system [M]. Beijing: China Aerospace Press, 2019.
- [10] 董帅, 莫皓颖, 户江民, 等. 基于探针的网络状态监测技术[J]. 通信技术, 2019, 52(4): 908-911.
- DONG S, MO H Y, HU J M, et al. Probe-based network status monitoring technology[J]. Communications Technology, 2019, 52(4): 908-911.
- [11] 吕金锁. 探针技术在网络信息监控系统中的应用[D]. 哈尔滨: 哈尔滨工程大学, 2006.
- LYU J S. Application of probe technology in network information monitoring system[D]. Harbin: Harbin Engineering University, 2006.
- [12] 刘蔚然, 陶飞, 程江峰, 等. 数字孪生卫星: 概念、关键技术及应用[J]. 计算机集成制造系统, 2020, 26(3): 565-588.
- LIU W R, TAO F, CHENG J F, et al. Digital twin satellite: concept, key technologies and applications[J]. Computer Integrated Manufacturing Systems, 2020, 26(3): 565-588.

[作者简介]



王明剑 (1979—), 硕士, 北京空间信息传输中心高级工程师, 主要研究方向为卫星通信系统网络安全。

范丹丹 (1982—), 博士, 北京空间信息传输中心高级工程师, 主要研究方向为卫星通信系统网络安全。

徐潇审 (1986—), 博士, 北京空间信息传输中心高级工程师, 主要研究方向为卫星通信系统网络安全。

李孟 (1988—), 硕士, 北京空间信息传输中心工程师, 主要研究方向为卫星通信系统网络安全。