

卫星互联网安全仿真测试技术研究

李皓^{1,2}, 张林杰^{1,2}, 张翼飞^{1,2}

(1. 通信网信息传输与分发技术国家级重点实验室, 河北 石家庄 050081;

2. 中国电科网络通信研究院, 河北 石家庄 050081)

摘 要: 针对卫星互联网安全仿真测试面临的系统的持续演进、海量攻防数据管控及多样化测试任务的灵活实施等挑战, 提出基于软件定义网络和云平台的系统架构和技术体系。分别就高逼真大规模网元模拟、高并发流量发生、基于 SDN 的安全服务链动态编排等关键技术进行深入研究, 并提出解决途径。实验结果证明这 3 项技术具备一定的创新性, 可应用于卫星互联网仿真测试平台的构建。

关键词: 卫星互联网; 网络仿真; 海量数据; 安全测试

doi: 10.11959/j.issn.2096-8930.2023018

Research on Satellite Internet Security Simulation Test Technology

LI Hao^{1,2}, ZHANG Linjie^{1,2}, ZHANG Yifei^{1,2}

1. Science and Technology on Information Transmission and Dissemination in
Communication Network Laboratory, Shijiazhuang 050081, China

2. China Electronics Technology Group Corporation Network Communication Research Institute, Shijiazhuang 050081, China

Abstract: Aiming at the challenges of continuous evolution of large-scale systems, massive attack data management and control, and flexible implementation of diversified test tasks, a system architecture and technical structure based on software-defined network and cloud platform were proposed. Key technologies such as high-fidelity large-scale network element simulation, high concurrent traffic generation, and dynamic choreography of security service chain based on SDN were studied in depth, and solutions were proposed. The experimental results showed that these three technologies were innovative and could be applied to the construction of the integrated simulation test platform.

Keywords: satellite internet, network simulation, big data, security test

0 引言

卫星互联网作为国家战略性公共信息基础设施^[1-3], 为陆海空天各类用户提供全球网络信息服务。卫星互联网安全防护涉及多系统不同要素间的信息交互^[4], 系统复杂, 测试场景建立困难, 在真实环境中对卫星互联网进行网络攻防等安全测试困难且危险。网络仿真以其安全性、经济性和可重复性优点而成为网络安全测试的一种重要手段。美国 PCTE 平台、英国 FCR 网络靶场、春秋云境网络靶场、360 新一代实网攻防靶场、浙江大学工业互联网安全试验网等网络安全仿真测试平台主要针对地面网络的攻防演练, 对卫星互联网安全仿真方面的研究较为缺乏^[5]。因此, 需开展卫星互联网安全仿真测试关键技术研究, 构建支持

增量升级、动态部署与柔性重构的半实物仿真系统, 满足安全防护设备/系统功能性能测试、安全防护系统体系化防御效能定量分析与测试评估、网络扩展演进发展等需求。

1 卫星互联网安全仿真测试技术面临的挑战

卫星互联网建设周期长, 安全防护技术要随着通信系统技术体制的演化而调整^[6], 在卫星互联网技术体制尚未完全确立的条件下, 网络安全仿真测试技术面临巨大挑战。

(1) 在仿真体系架构方面, 面向卫星互联网的迭代演进和安全防护技术的不断更新^[7], 要构建适应网络安全技术飞速发展的卫星互联网仿真平台, 必须采用先进、合理、高性能的仿真技术体系架构, 既支持现有网络安全技术的模拟, 又兼容未来新技术的引入。

(2) 为应对卫星互联网中各类网元实体在通信体制、安全试验需求等方面的差异性,以及终端规模大等特点,需要构建差异化的网元模型,并基于模型建立大规模仿真测试与评估平台。利用仿真技术的安全性、经济性和可重复性的优点为安全设备/系统提供仿真测试环境,对安全设备/系统的技术指标、技术体制和关键技术进行测试与评估。

(3) 在海量攻防数据的管控方面^[8],面向卫星互联网海量网元模型的管理,解决网元模型的逼真度和大规模网络运行效率的矛盾问题,以及海量仿真模型的管理维护、动态部署、协同调度和模型间高效的数据分发是关键。

(4) 在安全测试的实施方面,卫星互联网地基节点间存在被实体假冒、渗透入侵和拒绝服务等安全风险,需要构建安全测试工具链,实现测试数据在服务链式的安全测试工具间动态调整。

2 安全仿真测试系统架构与技术体系

2.1 系统架构

卫星互联网安全防护仿真测试系统体系架构如图1所示。由卫星互联网仿真分系统、试验管理网、安全测试工具、安全测试评估系统和安全测试管理控制系统共同组成。

卫星互联网仿真分系统和试验管理网共同构建安全测试网络环境。卫星互联网仿真分系统提供基础网络模拟

环境,集成业务应用、运维管理和安全防护仿真系统,为安全防护仿真测试提供逼真的测试试验环境。试验管理网为安全防护仿真测试过程中的管理、协调、控制和数据采集等业务提供管理控制通道。卫星互联网仿真分系统、被测安全防护设备、安全测试工具和安全测试评估系统在安全测试管理控制系统的统一控制下,开展测试试验任务。

安全测试工具从卫星网络对抗的视角,提供从情报搜集、威胁建模、漏洞分析到网络攻击的安全测试工具,构建面向卫星互联网中操作系统、路由交换设备、典型应用服务器的安全自动测试平台,体现网络对抗环境下卫星互联网的生存性和运维支撑能力。

安全测试评估系统提供评估模型、指标算法、多模型多方法综合评估等功能,支持在不同运维样式、不同组织应用条件下,卫星互联网安全防护设备/系统防御效能的评估分析。

安全测试管理控制系统负责安全防护仿真测试和评估任务从场景设计、过程策划、过程管理、信息探测、态势呈现到数据管理的全过程管理和控制。

2.2 技术体系

卫星互联网安全防护仿真测试系统基于云平台、软件定义网络(SDN)和虚拟化技术构建。虚拟化技术采用全虚拟化KVM(Kernel-Based Virtual Machine)与轻量级虚

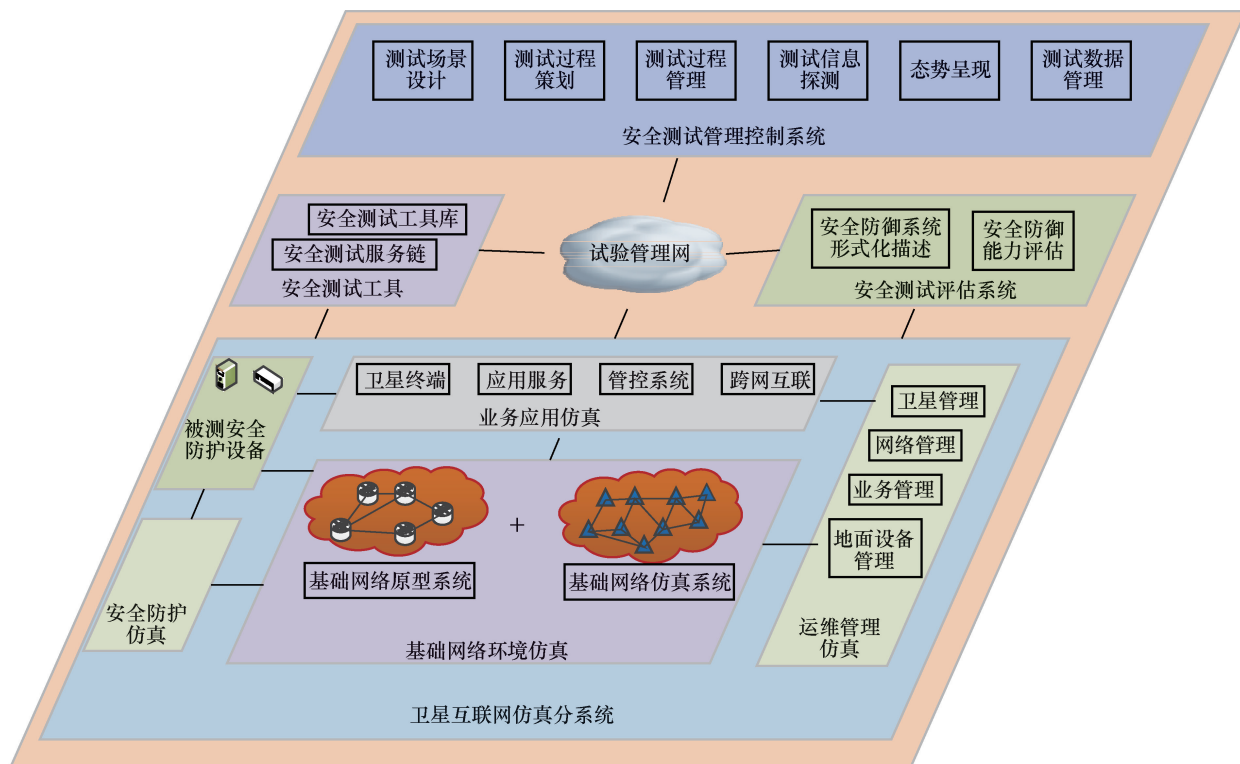


图1 卫星互联网安全防护仿真测试系统体系架构

拟化 Docker 相结合的方法;使用 KVM 保证网络安全试验环境的真实性,使用 Docker 实现海量网元设备的虚拟化仿真建模;使用开源的、企业级的虚拟交换机 Open vSwitch 技术搭建灵活可扩展的仿真测试网络。卫星互联网安全防护仿真测试与评估平台技术体系如图 2 所示。

整个架构主要分为 4 层。

(1) 基础设施层

基础设施层包括计算、存储、网络、镜像、认证等物理资源,通过一系列的虚拟化技术,在该基础设施的基础上,提供给卫星互联网安全防护仿真测试与评估平台进行资源使用。

(2) 资源层

资源层使用虚拟化技术,实现卫星互联网网元模型、安全测试工具的资源池化,并通过安全测试管理控制与 SDN 控制器的协同,对流量按需调度。根据应用所需就可以从资源池中找到相应资源,而不用关心设备部署在哪里。

(3) 控制层

控制层主要包括两个模块:一是安全测试管理控制,实现安全测试任务的管理和控制;二是云平台控制管理和 SDN 控制器。云平台控制管理主要实现对云计算环境的管理。SDN 控制器主要实现业务网络、管理网络等相关网络功能设计。

(4) 应用层

应用层利用控制层提供的北向接口,以及卫星互联网

安全防护仿真测试与评估存储的相关数据,提供一系列安全测试用例,包括单安全设备的安全测试与评估以及安全系统的安全测试与评估。

3 关键技术及解决途径

3.1 高逼真大规模网元模拟技术

针对卫星互联网拓扑持续变化,网元类型多、差异大等特点,需研究多类型实体高逼真模拟算法、按需配置的虚拟建模、虚实结合的协同联动仿真等内容,实现卫星互联网中各类网元设备的差异化安全仿真。而网络安全仿真最本质的问题^[9]是解决抽象建模与逼真模拟、模型差异定制与物理性能固定、场景灵活构建与承载环境僵化等一系列矛盾。因此,高逼真大规模网元模拟包括差异化天地网元模拟和卫星链路高动态仿真两项关键技术。

(1) 差异化天地网元模拟

卫星互联网的安全测试仿真^[10]从整体和全局的角度,完整地对于一个安全通信网络系统进行配置和部署。在搭建的卫星互联网仿真分系统中,实现对卫星节点、卫星终端等 5 类网元模型的覆盖,支持虚拟化网元节点的快速部署和参数配置,可以模拟天地各类网络设备^[11]、安全设备的操作系统环境,实现包含认证、密码、态势感知等各类安全设备的虚拟化 I/O 端口,真实模拟出卫星互联网、安全设备的资源受限环境,实现网络层及上层应用软件的无缝加载。支持安全功能嵌入的差异化网元模拟如图 3 所示。

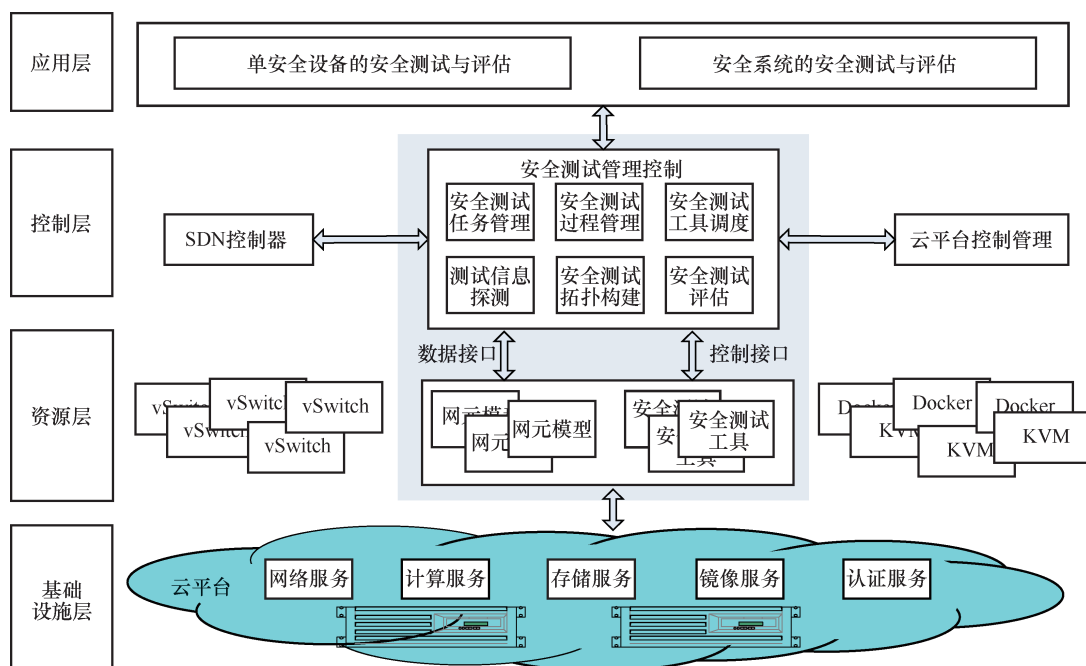


图2 卫星互联网安全防护仿真测试与评估平台技术体系

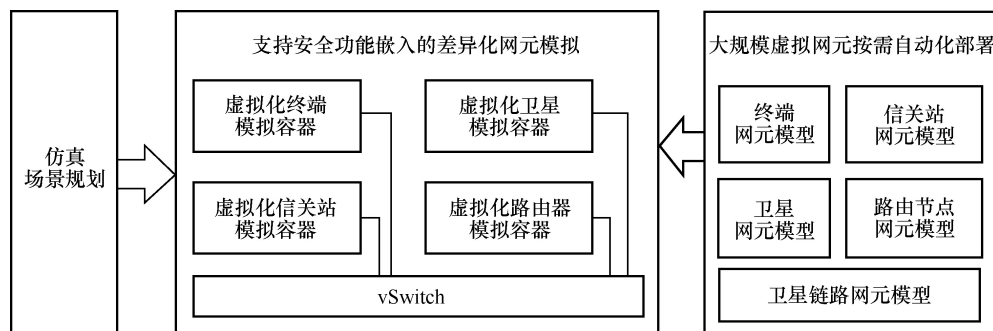


图 3 支持安全功能嵌入的差异化网元模拟

在仿真粒度方面,结合不同分辨率仿真模型的机理和特点,采用实物系统模拟小规模卫星互联网环境;采用全虚拟化仿真模拟不同体制的星上处理设备、信关站设备;采用轻量级虚拟化仿真模拟海量、多类型卫星终端;采用数字仿真模拟动态的低轨星座和地基网络。仿真过程中,实现实体模型与仿真模型的快速转换,支持操作系统级的安全仿真验证。在仿真试验管理阶段,能够根据试验任务和仿真网络的需求,实现各网络分片建模方式以及建模粒度的决策和动态配置。

(2) 卫星链路高动态仿真

针对主流卫星链路仿真逼真度与吞吐量不足的缺点,在链路发送端设置报文匹配规则,在链路接收端对链路时延误差进行动态差分补偿,实现卫星链路动态时延的高逼真仿真。在全虚拟化卫星节点内部署高通量路由协议,且支持卫星协议的自动配置,显著提升了天基骨干网间链路的吞吐量,能够满足卫星激光链路高吞吐量仿真需求。此外,通过融合 STK 仿真软件的卫星轨道精确测算优势,实现各种卫星链路可见性、时延、误码率及带宽的动态高逼真仿真。

卫星互联网空间段采用轻量级虚拟化和全虚拟化模拟卫星节点和地面节点,采用虚拟交换机模拟卫星链路。多层虚拟交换机 Open vSwitch 主要分为二层交换机 br-int 以及 OpenFlow 交换机两种。如图 4 所示,计算节点 1 采用轻量级虚拟化方式,计算节点 2 采用全虚拟化方式。网络内部通信主要通过二层交换机进行转发,跨网络通信主要通过 OpenFlow 交换机及相连的物理交换机进行转发。当报文经过二层交换机 br-int 时被打上内部标签,二层交换机根据报文目标 MAC 地址决定是否直接转发;在报文经 OpenFlow 交换机转发时将内部标签转变为外部 VLAN 标签,并依据流表匹配规则进行转发。

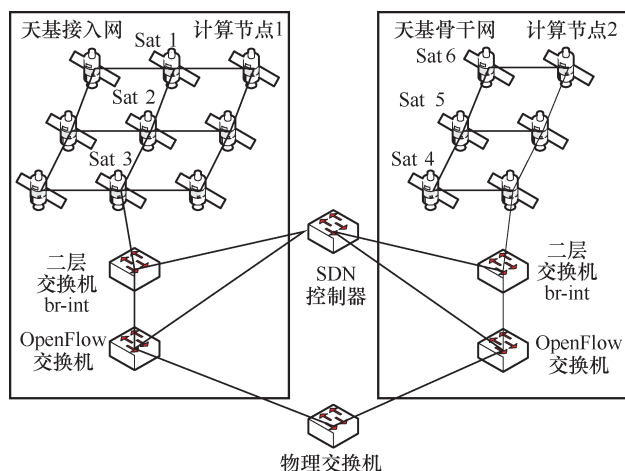


图 4 卫星链路仿真实现

高逼真大规模网元模拟技术能够支持安全实物设备无缝接入、差异化安全场景的灵活构建,支撑持续发展的安全技术测试任务,提高卫星互联网安全环境构建和综合试验能力。

3.2 高并发流量发生技术

针对卫星互联网的用户种类多、行为多样化、业务流量大、事件高并发等特征,需研究多样化、高并发、大流量业务生成,以及网络协议级、操作系统级用户行为仿真技术等内容,实现粒度可控、亿级用户行为的仿真模拟。如何在保证仿真逼真的前提下,构建群体业务行为表述模型,实现在有限计算资源下高并发生成业务流量^[15]是关键问题。因此,本文针对高并发流量生成,从高并发仿真架构、高效数据处理等方面开展研究。

高并发流量发生器分为通信层和作业处理层。通信层执行会话连接维护、数据接收、数据发送。作业处理层执行并发数据的仿真生成、数据后台维护。利用多线程使得通信层和作业处理层并行执行。为通信层创建线程数量为 N 的多个线程,为作业处理层创建线程数量为 M 的线程

池。尽量为每个线程绑定一个 CPU 核，充分发挥多核的优势，提高并发效率。

通信层和作业处理层之间通过待处理队列和待传输队列实现数据传递。多线程高并发仿真架构如图 5 所示。本架构针对高并发海量连接的业务需求进行处理，采用固定数目的线程进行业务数据的处理，不会随着前端仿真应用请求数量的增加而增加，避免在高并发海量连接的情况下，线程数量大幅度增加而导致处理性能下降的问题。

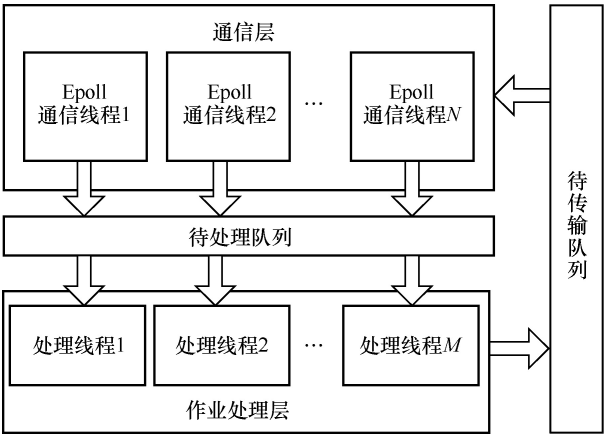


图 5 多线程高并发仿真架构

通信层的数据接收、发送使用 Epoll 接口。Epoll 接口是 Linux 下多路复用 I/O 接口 poll 的增强版本。它支持一个进程打开大批量的 socket 描述符，且 I/O 效率不随文件描述符（FD）数目增加而线性下降，并能显著提高程序在大量并发连接中只有少量活跃情况下的系统 CPU 利用率。在使用 Epoll 接口时，采用了边缘触发（Edge-Triggered，ET）的模式。边缘触发是高速工作方式，它能使用户空间程序缓存 I/O 状态，减少 epoll_wait 的调用，提高应用程序效率。

千万条数据的后台维护采用状态跟随方法，维护每条数据的连接标识 ID 和序列号 SEQ 用于索引。ID 是通信线程对应的线程号。ID 和 SEQ 具有 3 个作用：一是用于保证作业包的有效处理和正确返回到相应的通信线程；二是在需要数据先后顺序的业务处理中作为数据的先后顺序标识；三是用于作业包的排序和组合。ID 和 SEQ 在作业包生命周期中全程跟随，在拆分作业包时进行填写，在进行业务数据的处理时及给仿真应用返回处理后的作业包时使用。

作业包及包头结构示意图如图 6、图 7 所示。

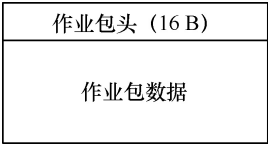


图 6 作业包结构示意图

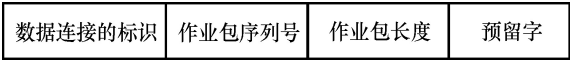


图 7 作业包的包头结构示意图

高并发流量发生技术能满足卫星互联网海量用户和瞬时的海量业务需求，构建高并发流量发生器，采用支持高并发海量连接的通信方法，满足高并发海量连接的高性能要求。

3.3 安全测试工具链智能编排技术

当前安全测试工具具有多源、异构特点，每种测试工具能力相对固定，难以进行灵活调度和编排，无法适应卫星互联网大规模复杂场景的安全测试需求。为此，在资源层采用虚拟化分层解耦方法；在应用层采用能力与属性定义相剥离的技术路线，将安全测试能力抽象为软件可定义的功能组件，实现上层测试任务与底层具体测试工具的隔离，并基于安全测试编排引擎实现安全测试能力的灵活重组和按需调度。研究工具属性定义和多维度关联技术、工具标准化封装和动态调用技术、面向卫星攻防的技术和技术知识库技术等，形成针对卫星互联网的标准化、灵活化、精准化动态安全测试能力，为自动安全测试子系统提供底层的全方位测试能力支撑，大幅度提升安全测试的质量和效率。

安全测试工具链智能构建流程如图 8 所示。

- （1）首先安全测试人员针对目标测试网络详细信息进行输入，包括网络拓扑、设备连接关系、安全防护设备部署等网络要素信息。
- （2）自动安全测试子系统通过网络安全测试模型分析，对测试环境进行解构、拆分，获取目标测试环境的重点要素信息，如安全网关、安全态势感知系统、关键路由节点信息等内容，生成理论推导的测试方案。
- （3）自动安全测试子系统抽取、合并、简化目标网络典型要素，梳理目标测试系统设备节点要素信息，构建面向各设备节点的安全测试任务。
- （4）自动安全测试子系统针对单点设备开启安全测试流程，包括漏洞探测、安全测试工具载荷选择、渗透测试、后渗透测试、安全测试工具评分等全流程环节。
- （5）自动安全测试子系统在安全测试理论推导方案的

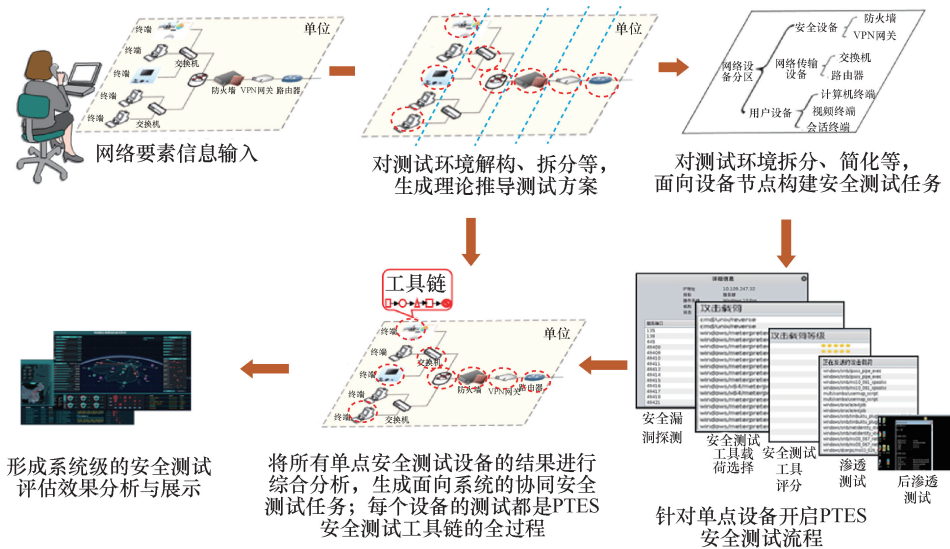


图 8 安全测试工具链智能构建流程

指导下, 将所有单点安全测试设备的结果进行综合分析, 生成面向系统的协同安全测试任务; 每个设备的安全测试都采用渗透测试执行标准 (PTES) 安全测试工具链的全流程, 各环节之间相互衔接, 依据前一测试效果动态生成后续安全测试流程的工具。

(6) 通过对各设备安全测试工具效果的评估, 形成系统级的安全测试效果分析与展示。

在 PTES 安全测试任务的全过程管理的基础上, 从资源和工具调度、流程自动化等角度出发, 研究安全测试任务一键式构建、基于测试目标的安全测试任务自动分解、子任务独立资源调度和并发处理、安全测试任务自动化编排等技术, 设计任务自动化编排引擎, 实现安全测试任务灵活构建、安全测试任务自动执行、多任务独立并发执行, 极大地降低了网络安全测试的复杂度, 提高了网络安全测试的效率。

4 实验结果

(1) 高逼真大规模网元模拟技术

如图 9 所示, 实测构建的场景中包含 217 个节点, 其中 6 个天基骨干卫星节点, 120 个低轨天基接入卫星节点, 16 个信关站节点, 15 个路由节点, 3 个天通一号卫星, 6 个 Ka 卫星, 6 个 Ku 卫星, 41 个卫星终端, 3 个低速航天器和 1 个高速航天器。

(2) 高并发流量发生技术

从思博伦测试仪向安全试验演示与验证平台发起千万并发数据测试, 抓取被攻击节点的数据包保存为 .pcap 文件, 通过 Wireshark 打开, 可查看并发安全事件条数为 11 995 条。

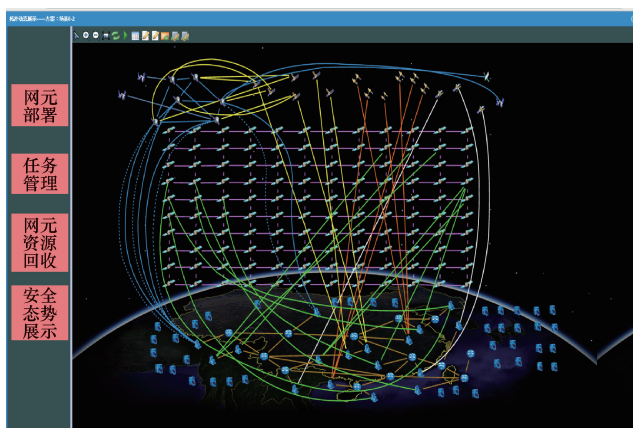


图 9 拓扑部署完成

查看用户通信情况, 通过安全态势展示图可以看出实时通信链路数达到 10.4 万条左右。

(3) 安全测试工具链智能编排技术

根据测试人员在前期交互阶段选择的测试目的, 生成相应的测试流程, 根据测试流程和测试中间结果, 动态选择一组合适的测试工具, 并将前驱工具的输出与后继工具的输入有效衔接, 最终将测试结果以简单易懂的形式返回给测试人员。

例如, 在威胁建模阶段, 可根据情报搜集阶段的结果对目标进行漏洞扫描, 扫描结果与可用的攻击载荷进行匹配, 并对攻击载荷的攻击能力进行等级评判, 将攻击载荷按等级从高到低排序。在接下来的渗透攻击过程中, 优先使用等级较高的攻击载荷, 以便更容易攻破目标系统。

5 结束语

本文开展了卫星互联网安全仿真测试平台技术研究,提出了高逼真大规模网元模拟技术、高并发流量发生技术和安全测试工具链智能编排技术并进行验证实验。实验结果显示,高逼真大规模网元模拟技术支持对卫星终端节点、星载节点、信关站节点、路由交换设备、运维管理系统、应用服务系统等节点/设备/系统的仿真,能够为卫星互联网安全防护系统提供仿真验证环境;高并发流量发生技术能够支撑千万级并发数据的实时通信仿真,1万条以上安全事件并发仿真和10万条以上通信链路实时仿真,实现了有限资源下海量数据的管理调度;安全测试工具链智能编排技术可根据不同需求构建包含不同虚拟安全功能的安全服务链,针对不同的业务流量进行按需编排处理,支持安全功能的按需动态加载,支持安全服务链的动态重构以及安全服务链动态重构过程中流量的无损编排。

参考文献:

- [1] 虞志刚, 冯旭, 黄照祥, 等. 通信、网络、计算融合的天地一体化信息网络体系架构研究[J]. 电信科学, 2022, 38(4): 11-29.
YU Z G, FENG X, HUANG Z X, et al. Research on the architecture of space-ground integrated information network: integration of communication, networking and computing[J]. Telecommunications Science, 2022, 38(4): 11-29.
- [2] 亓玉璐, 江荣, 荣星, 等. 基于网络安全知识图谱的天地一体化信息网络攻击研判框架[J]. 天地一体化信息网络, 2021, 2(3): 57-65.
QI Y L, JIANG R, RONG X, et al. Attack analysis framework of space-integrated-ground information network based on cybersecurity knowledge graph[J]. 2021, 2(3): 57-65.
- [3] 马方舒, 王岩, 张国威, 等. 天地一体化信息网络中物理层安全方案[J]. 天地一体化信息网络, 2020(2): 73-80.
MA F S, WANG Y, ZHANG G W, et al. Physical layer security schemes in space-integrated-ground information network[J]. Space-Integrated-Ground Information Networks, 2020(2): 73-80.
- [4] 韩孟达, 曹利峰, 雷依翰, 等. 空天网络安全切换技术研究综述[J]. 计算机工程与应用, 2022, 58(16): 56-70.
HAN M D, CAO L F, LEI Y H, et al. Overview on technology of security handover in aerospace network[J]. Computer Engineering and Applications, 2022, 58(16): 56-70.
- [5] 王晨. 天地一体化网络数据安全聚合关键技术研究[D]. 南京: 南京信息工程大学, 2022.
- WANG C. Research on key technologies of data security aggregation in space-earth integration network[D]. Nanjing: Nanjing University of Information Science & Technology, 2022.
- [6] 景文强, 余波, 李昂阳, 等. 天地一体化信息网络主动防御安全体系研究[J]. 信息技术与网络安全, 2019, 38(8): 17-21.
JING W Q, YU B, LI A Y, et al. Research on active defense security system of space-ground information network[J]. Information Technology and Network Security, 2019, 38(8): 17-21.
- [7] 李凤华, 郭云川, 耿魁, 等. 天地一体化信息安全动态赋能研究[J]. 无线电通信技术, 2020, 46(5): 561-570.
LI F H, GUO Y C, GENG K, et al. Dynamically empowering security for space-terrestrial integrated information network[J]. Radio Communications Technology, 2020, 46(5): 561-570.
- [8] 万颖, 钱克昌, 邢鹏. 基于 SDN 的天地一体化网络控制器部署方法综述[J]. 计算机测量与控制, 2022, 30(11): 1-10.
WAN Y, QIAN K C, XING P. Review of controller deployment methods for space-ground integrated network based on SDN[J]. Computer Measurement & Control, 2022, 30(11): 1-10.
- [9] 张晓凯, 郭道省, 张邦宁. 空天地一体化网络研究现状与新技术的应用展望[J]. 天地一体化信息网络, 2021, 2(4): 19-26.
ZHANG X K, GUO D X, ZHANG B N. Research status of space-air-ground integrated network and application prospects of new technologies[J]. Space-Integrated-Ground Information Networks, 2021, 2(4): 19-26.
- [10] 沈学民, 承楠, 周海波, 等. 空天地一体化网络技术: 探索与展望[J]. 物联网学报, 2020, 4(3): 3-19.
SHEN X M, CHENG N, ZHOU H B, et al. Space-air-ground integrated networks: review and prospect[J]. Chinese Journal on Internet of Things, 2020, 4(3): 3-19.
- [11] 刘龙龙, 张建辉, 杨梦. 网络攻击及其分类技术研究[J]. 电子科技, 2017, 30(2): 169-172.
LIU L L, ZHANG J H, YANG M. Research on network attacks and their classification[J]. Electronic Science and Technology, 2017, 30(2): 169-172.
- [12] 周磊. 计算机网络虚拟仿真技术的研究与应用[J]. 电子质量, 2022(7): 122-129.
ZHOU L. Research and application of computer virtual simulation technology[J]. Electronics Quality, 2022(7): 122-129.
- [13] 陈新宇, 王晓锋, 刘渊. 天地一体化卫星网络拓扑场景仿真技术[J]. 计算机工程与应用, 2022, 58(20): 87-97.

CHEN X Y, WANG X F, LIU Y. Topological scenario emulation technology of space-ground integrated satellite network[J]. Computer Engineering and Applications, 2022, 58(20): 87-97.

- [14] 叶海洋, 张桂珠, 王晓锋, 等. 面向天地一体化卫星网络的高性能仿真技术[J]. 计算机工程与应用, 2019, 55(17): 82-88.

YE H Y, ZHANG G Z, WANG X F, et al. High-performance emulation technology for space-ground integrated satellite network[J]. Computer Engineering and Applications, 2019, 55(17): 82-88.

- [15] 文奕, 陈兴蜀, 曾雪梅, 等. 面向安全分析的大规模网络下的DNS流量还原系统[J]. 信息安全, 2019(5): 77-83.

WEN Y, CHEN X S, ZENG X M, et al. DNS protocol restore system for security analysis based on large-scale network[J]. Netinfo Security, 2019(5): 77-83.

[作者简介]



李皓 (1987—) 男, 博士, 中国电科网络通信研究院工程师, 主要研究方向为内生安全、深度学习、网络通信系统。

张林杰 (1972—), 女, 研究员, 中国电科网络通信研究院副总工程师, 主要研究方向为网信体系、网络安全、通信网络与系统。

张翼飞 (1996—) 男, 硕士, 中国电科网络通信研究院助理工程师, 主要研究方向为网络安全、网络攻击追踪溯源等。