专题：内生安全

网络空间内生安全试验场管理技术

朱泓艺，陆肖元，李毅
（上海宽带技术及应用工程研究中心，上海 200436）

摘　要：网络靶场（CR）已被广泛认可为一种研究网络攻防技术与网络架构脆弱性的有效途径，网络空间内生安全试验场是一种面向网络空间内生安全技术的网络靶场，近年来受到了高度关注。基于以 5G 发展为核心的网络空间新形势，提出了面向虚实结合网络环境的试验场管理技术，设计了基于内生安全软件定义网络控制器的试验场管理架构。同时提出了一种内生安全网络控制系统的架构设计，采用中间层转发代理实现数据安全隔离，支持多种异构开源控制器。最后，基于一种试验场组网方案提出试验场场景重构与资源编排方法。

关键词：网络空间；内生安全；网络靶场；软件定义网络
中图分类号：TP393
文献标识码：A
doi:10.11959/j.issn.1000−0801.2021048

Management technologies of cyberspace endogenous safety and security test site

ZHU Hongyi, LU Xiaoyuan, LI Yi
Shanghai Engineering Research Center for Broadband Technologies and Applications, Shanghai 200436, China

Abstract: The cyber range has been widely recognized as an effective way to study the technologies of network attack/defense and the vulnerability of network architecture. The endogenous safety and security test site that receives high attention recently is a type of cyber range for cyber space endogenous safety and security technologies. Based on the new situation of cyberspace with 5G development, a test site management technology for virtual-real network settings was proposed, and a test site management architecture based on the endogenously secured software defined network controller was designed. A design of the endogenously secured network control system was also proposed, which used a middle layer forwarding agent to achieve data isolation and supported multiple heterogeneous open-source controllers. Finally, a test site scenario reconfiguration and resource orchestration method was proposed based on a test site networking scheme.

Key words: cyberspace, endogenous safety and security, cyber range, software defined network

收稿日期：2021−02−15；**修回日期**：2021−03−14
通信作者：朱泓艺，hyzhu@bnc.org.cn
基金项目：国家重点研发计划项目（No.2020YFB1805101）；上海市科技创新行动计划高新技术领域项目（No.20511102102）
Foundation Items: The National Key Research and Development Program of China（No. 2020YFB1805101），Shanghai Science and Technology Innovation Action Plan（No. 20511102102）

1　引言

随着互联网技术与垂直行业的紧密结合，网络空间安全作为国家安全的组成部分，其重要性日益凸显。尤其是在云网融合、车联网、工业互联网、天地一体化等技术发展的加速推进下，移动通信、智能网联汽车、工业系统、卫星通信均逐渐暴露在网络攻击的风险之下。网络空间安全造成的影响，也从个人隐私、企业机密的泄露，提升到危害人民财产、生命安全以及国家利益的高度。快速迭代的网络架构、设备以及应用场景，使传统的网络安全防御技术和传统的网络信息产品安全性能检测技术捉襟见肘，难以承担维护国家网络空间安全的重要任务。

在网络安全防御技术方面，“内生化”的网络安全在近年来已成为研究热点。由于网络攻防态势的普遍不对称性，被动式的防御技术与产品仅依靠阻挡、检测和修复[1-2]等手段存在一定的滞后性。因此，在面对未知的系统漏洞后门与恶意网络攻击时，往往无法及时有效地发现威胁，只能在网络受到攻击造成损失后进行修补，无法满足如今工业互联网、车联网等领域的高安全性要求。采用主动防御技术，为系统引入动态随机性使之呈现不可预知的特点，从而减少对网络攻击先验知识的依赖，成为网络安全领域新的主流观点。基于此，拟态防御原理引入动态异构冗余架构[3-4]，从网络空间的根本结构上为系统提供“内生”的安全性能。拟态防御作为目前实现网络空间内生安全的一种最具有可行性的技术体系，已被广泛应用于网络架构与软硬件设备的设计之中[5-6]。

在网络安全检测技术方面，网络靶场[7]（cyber range，CR）和试验床（test-bed，TB）作为一种网络空间安全研究的信息基础设施，可承担网络信息产品安全性能的评估、网络安全性策略的制定和在典型网络应用场景进行网络攻防演练等任务，为新型网络技术与设备提供一个具有高度可操作性的试验环境。因此，CR 技术已受到国际社会的高度重视，世界各国均将 CR 作为体现国家安全实力的重要信息基础设施。

作为两者的融合，网络空间内生安全试验场是一种主要面向网络空间内生安全技术的 CR/TB。参考文献[8]重点探讨了基于面向对象设计思想的网络空间先进防御技术试验场构建方法，为网络空间内生安全试验场的设计与建设提出了一种可行的方法。

在我国，CR/TB 的研究主要以科研院所如国防科学技术大学、中国科学院计算技术研究所、北京邮电大学等机构牵头建设，在网络攻防演练、场景仿真、数据采集等多个方面均有重大突破。同时，在南京紫金山实验室的支持下，全球首个网络内生安全试验场在南京落地，主要面向全球提供真实的人机对抗环境，提供网络设备的安全测试与网络安全人员的技能培训。

国外关于 CR/TB 的研究情况见表 1，国外关于 CR/TB 的相关研究于 20 世纪初已经开始，其中美国的起步相对较早。各国 CR/TB 的主要建设机构分为两类，分别为国家政府部门与科研机构，前者如美国国防部更侧重于网络攻击防御技术与网络武器有效性评估等，后者例如各世界著名高校与非营利科研组织则更侧重下一代网络体系架构研究。无论出于何种建设目的，所有的 CR/TB 均具有大规模网络环境模拟以及构建可重复实验的需求。

本文基于对 CR/TB 的全球趋势研究与 5G 新形势下对于网络安全试验的需求分析，提出了一种网络空间内生安全试验场管理技术，针对先进防御技术的模拟测试、内生安全设备的部署验证以及攻防演练场景的快速构建与切换等需求，设计了以内生安全软件定义网络控制器为核心的虚实结合试验场管理架构，通过双层隔离的方式，在保障试验环境独立安全的前提下，提供网络信息可视化、场景快速重构、多场景并行运行以及

表 1　国外关于 CR/TB 的研究情况

区域	名称	机构	国家	启动时间	主要任务
北美	National Cyber Range（NCR）[9-10]	DARPA	美国	2008 年	网络攻击防御技术与武器的有效性评估、网络攻防人员培训、网络攻防演练等
	GENI[11]	NSF	美国	2005 年	研究网络核心技术如交换、寻址、网络管理等，提高网络性能，研究新的网络体系结构等
	PlanetLab[12]	休斯顿大学	美国	2003 年	研究资源虚拟化应用和分布式覆盖网络，构建面向全球访问的虚拟化覆盖网试验
	DETERlab[13]	NSF、DHS、DARPA	美国	2003 年	研究下一代高级网络安全技术，构建一个通用的网络安全实验平台
	CASElab[8]	维多利亚大学	加拿大	2010 年	在完全可重复的实验条件下研究真实世界大规模网络系统的行为建模，支持对互联网的新技术/武器的鉴定和评估
欧洲	FP7[14]	欧盟成员国和相关国家	欧盟	2007 年 2013 年	研究信息通信技术，包括数字图书馆与资源、数字存储、网络保存、信息检索及运用等多个主题
	FCR[15]	Northrop Grumman	英国	2010 年	研究大型复杂网络的模拟，在安全可控的试验环境进行基础设施生存能力和可靠性方面的网络试验及评估
	G-LAB[16-17]	BNBF	德国	2008 年	研究未来网络技术，主要针对新型网络技术与新型网络应用需求之间的交互与配合
日韩	AKARI[18]	JAXA	日本	2006 年	主要面向小型机构，提供研究下一代网络架构的试验环境
	U-Korea[19]	韩国政府	韩国	2004 年	主要研究无线传感网络

信息资源可编排等功能。同时，提出了一种内生安全网络控制系统的架构设计，采用中间层转发代理实现数据安全隔离，支持多种异构开源控制器执行体构建拟态资源池，并采用了基于关键字段流一致策略的裁决算法。最后，基于一种试验场组网方案提出试验场场景重构与资源编排方法。考虑到篇幅问题，在下文中，主要以试验场来指代网络空间内生安全试验场。

2　虚实结合的试验场管理架构

本节基于以 5G 为核心的网络空间安全新形势，重点分析了建设虚实结合的试验场管理体系架构的必要性以及需要实现的技术要求，最终提出一种以内生安全软件定义网络控制器衔接实体网络与虚拟网络的试验场管理架构，实现对于虚实结合试验场的统一控制管理与资源编排。

2.1　需求分析

5G 的到来不仅强化了网络功能虚拟化（network function virtualization，NFV）与软件定义网络（software defined network，SDN）的重要性，更使得两者紧密结合。一方面，随着云计算的发展，许多新型高科技企业与电信服务运营商都青睐部署于原生云中的虚拟网络功能（virtual network function，VNF）。容器与微服务技术的发展更促进了 NFV 技术的应用，以容器运行 VNF 可以提供自动扩/缩容、编排等功能，对于新型企业而言，是较为高效的业务部署方式，也是摆脱传统设备商软硬一体化限制的重要手段；另一方面，随着分布式计算、边缘计算等技术的发展，SDN 技术重新被广泛应用于数据中心网络，通过解耦网络设备的控制层与数据层，在控制层实现了网络管理的标准化与可编程，从而更有效地分配东西向网络资源。5G 在核心网控制面实现全面的虚拟化，而在用户面则基于 SDN 技术实现高效的转发与分流，通过以 NFV/SDN 融合技术为代表的网络结构转型，满足多种垂直行业不同应用场景的差异化用户体验保障要求。

5G 技术的发展也为网络安全问题带来了巨大的挑战：（1）由于 5G 建设过程中大量应用了支持通用白盒设备以及通用接口的 NFV/SDN 技术，

与过去的传统移动网络相比，与固定宽带网络联系更为紧密，同时也为恶意网络攻击者提供了方便之门；（2）VNF 的部署与应用为网络控制层带来了具有较高复杂度的程序构成与底层操作系统，大幅提升了网络控制层中存在漏洞或后门的概率；（3）在 5G 技术应用于垂直行业的过程中，NFV/SDN 技术也逐渐渗透至例如工业互联网、车联网、卫星网络等，而这些场景过去未曾考虑网络攻击的风险，部分基础设施安全防护措施薄弱、业务系统复杂，安全等级要求却远高于传统互联网。

为了应对网络空间安全新形势，本文提出的试验场的构建方法与管理架构以面向虚实结合网络空间的大规模多场景攻防演练为目标，从试验场管理层面实现对于虚实网络的统一控制管理与资源编排；在面向用户的应用平台层面则需要消除对于虚实网络差异的感知，从而支持内生安全虚拟/实体网元的联合测试验证以及可重构的攻防演练场景。

2.2　架构设计

在试验场管理方面涉及大规模虚实网络的互联组网、高可靠高安全的网络控制、高效率的资源编排、可重构切换的攻防演练场景等多项关键技术。本文所提出的试验场管理架构如图 1 所示，主要分为试验场平台、SDN 控制器、虚拟/实体网络 3 部分，其中实线表示数据链路，虚线表示管理链路。试验场平台作为整个试验场的应用层，提供网络拓扑可视化、动态信息资源编排、攻防演练场景构建与切换以及先进防御技术与设备的测试评估等功能。SDN 控制器为统一网络控制的关键网元，通过动态异构冗余架构以及异构 SDN 控制器执行体池的构建，为 SDN 控制层提供内生安全保护。虚拟网络主要提供大规模组网场景的快速构建以及内生安全虚拟网元的部署；实体网络主要部署内生安全实体网元以及攻击、测试等专业设备。整个试验场在 SDN 控制层与物理硬件设备管理接口采用了双层隔离的设计思路保障试验场平台的安全可靠。整个试验场管理架构在设计中遵循以下原则。

- 先进性：针对先进防御技术与设备的部署需求提供模拟环境建立的功能，以满足测试评估需求。
- 可重构性：支持攻防演练场景的快速构建、释放、切换，提供高效灵活的测试验证环境；
- 可扩展性：支持新增设备与硬件资源，可支持大规模分布式试验场部署。
- 规范性：以先进防御技术标准体系为导向，保障先进防御技术测试验证的规范性。
- 安全性：试验场管理系统需要与试验场环境进行高度隔离。

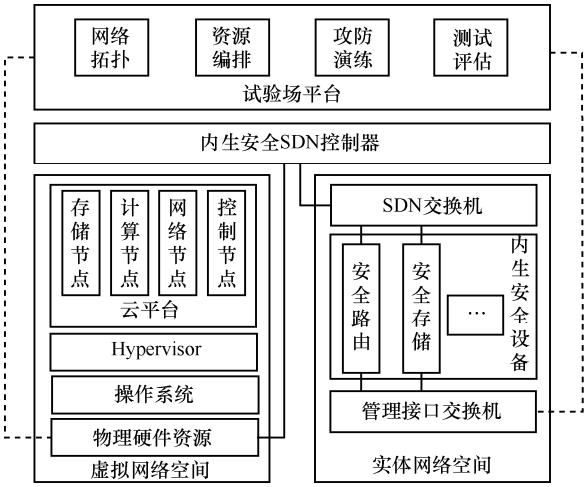

图 1　虚实结合的网络空间内生安全试验场管理架构

根据上述设计原则与需求，本架构具备如下特点。

在虚实网络的高速互联方面，SDN 使用软件应用程序对虚实网络进行集中控制编程，北向支持开放的 RESTconf API，使得试验场网络管理无须考虑底层网络技术的复杂性。南向则通过 NETconf 协议，在虚拟网络侧与云平台的网络节点进行对接，例如在基于 OpenStack 平台的虚拟网络中，SDN 控制器可与 Neutron 模块对接，用以管理虚拟网络中所有的计算、存储和控制节点，实现虚拟网元的组网；实体网络侧对接 SDN 交换

机，作为实体网元的数据汇聚节点。SDN 控制器具备大规模网络拓扑发现、高速信息处理和流表下发的能力，采用流表聚合和标签路由算法，可以解决实体 SDN 交换机流表数量限制和查询效率，从而实现大规模二层组网和高效率的二层交换，最终实现虚实网络的万兆高速互联。

安全可靠的网络控制方面，在 SDN 控制层引入动态异构冗余的架构，首先在数据层和应用层之间加入中间层与拟态层，其中中间层不进行路由计算仅作为数据采集、报文上传、流表下发等任务的中间节点，拟态层则维护支持多个异构 SDN 控制器执行体的资源池，将报文信息同时转发给多个执行体，通过流表一致性裁决强化路由信息安全可靠性，同时实现对于异常执行体的发现与清洗重启。

在统一信息资源编排方面，网络拓扑信息的维护由 SDN 控制器统一管理，在虚拟网络侧通过路由器、端口、子网、主机与链路等元素的映射，将基于云平台的虚拟网络拓扑与实体网络拓扑进行整合，提供统一的网络拓扑展示，简化试验场网络运维管理，提高试验场管理平台可视化效果；承载虚拟网络的云服务器以及构成实体网络的实体网元额外设置了管理接口与链路，将承载试验场攻防演练的数据链路和实现各设备配置管理与数据采集的管理链路进行安全隔离，避免试验场中的攻击数据流直接影响到试验场管理平台。

在支持攻防演练场景的快速构建与切换方面，试验场支持的独立管理链路可以快速生成或释放虚拟网元、启动或停止实体网元，并通过 SDN 控制器调整组网结构，大幅简化攻防演练场景构建的流程，同时支持不同设备组成多个测试环境并行试验，实现高效的测试评估。

3 内生安全软件定义网络控制系统

在虚实结合的试验场管理架构体系中，实现虚实网络集中控制的SDN控制层为整个试验场的核心部位，需要承载虚拟网络中与云平台的对接、在实体网络中控制SDN交换机实现拓扑变更以及虚实网络的高速互联等功能，其安全性能需要最高级别的保障。

本节提出基于动态异构冗余架构的内生安全软件定义网络控制系统架构保障 SDN 控制层安全，实现多异构 SDN 控制器执行体动态调度、流表对比裁决、快速调度下线重启控制器等关键性技术。

3.1 异构开源 SDN 控制器执行体

基于拟态防御的SDN控制层安全机制在参考文献[20]中进行了充分的讨论，研究了基于语义层面的异构控制器流表项对比裁决。在实验中，选用了 ODL（Open Day Light）控制器作为主控制器，而 POX 和 ONOS（Open Network Operating System）作为等价异构控制器提供对比裁决的流表数据。在本文中，选用自研的 DCFabric 开源 SDN 控制器作为中间层，本身并不提供路由功能，仅为多个异构 SDN 控制器执行体提供报文上传、网络拓扑信息更新以及流表转发的功能，构成拟态防御架构中的代理节点。在安全性上，该部分仅作为透传通道，其功能具有简单可靠的特点，难以出现故障或被网络攻击。在功能性上，提供了与云平台对接和可视化的能力，可以满足虚实结合的试验场组网需求。

在异构执行体的选取方面，本文提出的内生安全SDN控制器采用三大主流开源SDN控制器 ODL、ONOS、Ryu 构成异构资源池，其各项特点对比见表 2。其中，ODL 控制器由 Linux 基金会主导开发推进，主要面向数据中心网络支持 SDN/NFV 分布式框架和平台；ONOS 控制器则由非营利性组织 ONLab 主导推出，主要聚焦控制器平台层，业务组件则提供开放接口供使用者自行开发；Ryu 控制器由日本 NTT 公司负责设计研发，完全采用 Python 语言实现，具有轻量化的优点。

表 2　开源 SDN 控制器对比

控制器名称	启动时间/s	内存占用/KB	代码量/行	主要编写语言
ODL	180	976 004	111 737	Java
ONOS	55	461 132	791	Go
Ryu	7	45 712	1451	Python

根据测试对比可见，本文所引用的 3 种开源 SDN 控制器分别采用不同的语言进行编写，在执行体的异构度上有足够的保障。与 ONOS 和 Ryu 相比，ODL 控制器由于功能模块丰富，不仅代码量为另外两种控制器的上百倍，同时在启动时需要占用更多的时间。这一点在内生安全 SDN 控制器运行过程中，将会较大地影响 ODL 控制器下线清洗后恢复上线所需要的速度。而 Ryu 控制器属于轻量级系统，在代码量与 ONOS 相当的情况下，可以实现 10 s 以内的快速启动，并且内存占用也远低于其他两种控制器。

3.2　控制器架构

SDN 控制器整体架构如图 2 所示，包括应用层、中间层、数据层以及拟态层；应用层与中间层之间使用 RESTful API 进行消息传递，包括拓扑信息获取、配置下发等消息；中间层和数据层之间使用 OpenFlow 协议进行消息交互，包括数据层的请求以及流表下发等消息；拟态层主要作为中间层的一部分，包括裁决器、调度器以及各种异构控制器。

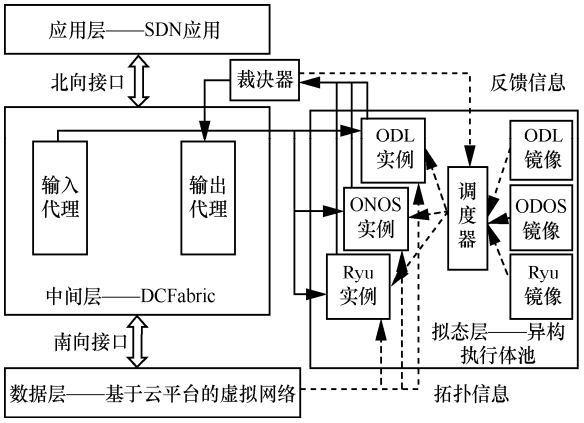

图 2　内生安全 SDN 控制器架构

其中，中间层和拟态层是内生安全 SDN 控制器的两个重要组成部分，中间层使用 DCFabric 与数据层的 SDN 交换机或云平台中的网络节点建立连接，数据层中的数据发生交换时，向中间层请求路由策略。在初始化完成之后，拟态层中的各个异构控制器会各自独立获取并更新数据处理中整体网络状态，中间层收到交换发送的策略请求之后，通过输入代理模块将请求信息分发到层中的各个异构控制器，各个控制器分别进行路由策略计算。各个控制器计算得到的转发策略会统一发到裁决器进行汇总，裁决器将策略统一汇总发送到输出代理，最后下发到 SDN 交换机。

拟态层中的各个控制器以虚拟机或容器的方式运行，可以根据需求快速地创建或释放一个控制器实例。其中裁决器不只是对策略进行裁决，还会将裁决的结果向调度器反馈，调度器收到裁决结果后，对有安全风险的控制器执行体进行清洗。

应用层主要是对网络的可视化管理，包括可视化的查看以及配置，前端页面向应用层服务端获取网络当前状态数据，并将其展现在前端页面，包括网络拓扑信息、当前各种异构控制器的运行状态、当前 SDN 交换机的流表信息等。应用层服务端通过 RESTful API 向 DCFabric 控制器获取状态信息，不同的用户拥有不同的配置管理权限以及查看权限，从而增强网络管理的安全性。

3.3　拟态裁决的流程设计

内生安全 SDN 控制器的拟态裁决主要针对“流一致”的要求进行设计，即多个异构 SDN 控制器执行体流表的路由策略保持一致。在裁决器收到多个控制器发送的流表信息后，开始裁决过程，主要由同步、折分、比较和裁定 4 个步骤组成。

同步：本步骤为了保证拟态裁决的对象是异构控制器，是针对同一路由策略请求后下发的流表信息，该过程可通过报文标识符 Packet_ID 完成。

拆分：由于逐比特比较计算量大，且无法处

理异构控制器私有的控制规则信息，难以在裁决器进行流表的逐位匹配。因此，在本步骤对流表的关键信息进行提取，按照路由策略的语义规则，将其分为多个关键字段。

比较：根据关键字段拆分结果，对多个流表每个字段进行分别匹配比对，例如分别就源地址、目标地址、转发端口等字段进行比对。

裁定：在比较过程结束后，根据比对结果裁定具有多数优势的流表信息为真，转发至代理节点，并将流表信息裁定为假的控制器信息反馈至调度器进行处理。

在本系统设计中，除了采用细粒度的流一致裁决算法，还添加了带容忍阈值的自清洗机制强化内生安全 SDN 控制器的可靠性与稳定性。由于多个控制器执行体的路由策略可能有一定的不一致，同时考虑到部分控制器执行体的重启时间较长，裁决器在经过裁定之后可以记录控制器执行体的错误次数：在初始状态时，所有控制器执行体的错误次数均为 0，每当发现有错误消息出现将相应控制器执行体的错误次数加 1。当错误次数达到某个预设的容忍阈值时，裁决器将信息反馈至调度器，相应控制器执行体进入自清洗阶段——重启/替换控制器执行体。完成自清洗阶段之后，该控制器执行体的错误次数重置。

基于动态异构冗余架构的内生安全SDN控制系统由于采用了多个异构控制器执行体与流一致的拟态裁决算法，在少于半数的控制器执行体被攻击时，仍能保证正确的流表输出。同时裁决器能够识别这些具有安全风险的执行体，并进行调度清洗消除网络攻击对控制器执行体的影响，大幅强化了 SDN 控制层的安全能力。

4　可快速切换场景的试验场部署管理技术

建设网络空间内生安全试验场的主要目的是对网络空间内生安全原理、技术、方法进行全面的系统研制，从而促进内生安全理论体系的完善和深化，为内生安全技术、设备提供测试认证，支撑基于虚实结合网络空间环境的攻防演练、人员培训和能力评价，最终实现相关产业链的标准化与商业化。本节提出一种可支持场景快速重构、切换的试验场部署管理技术，以一个典型的组网方案为例，充分介绍面向服务、动态充足、按需分发等能力的试验场管理策略。

4.1　虚实结合的试验场典型组网方案

网络空间内生安全试验场组网案例如图 3 所示，一个典型的虚实结合试验场主要分为 5 个主要组成部分：试验场平台、外部互联网接入、虚拟网络、实体网络和管理接口链路。

试验场平台是面向测试及运维人员的用户接口，也是整个试验场的应用层，通过对接 SDN 控制器获取全网信息感知，并通过管理接口链路获得试验场各设备资源信息与管理配置能力，从而支持网络可视化、场景构建切换等功能；外部互联网接入处首先完成用户接入认证以提供不同级别的测试服务，在接入侧旁挂攻击/背景流量生成器模拟网络攻击与杂讯干扰；虚拟网络主要由例如 OpenStack 的云平台支持，可基于镜像实现虚拟网元的快速生成，并通过云平台网络节点与 SDN 控制器对接；实体网络主要部署网络空间内生安全设备，如内生安全路由、内生安全存储等系统，以一个或多个 SDN 控制器作为数据链路通道进行互联；管理接口链路独立于试验场数据链路，通过管理接口交换机汇聚全试验场各网络设备、服务器、主机的管理配置信息与资源信息数据。

4.2　场景重构与资源编排

基于物理设备和物理链路构建的传统网络安全防御试验场，存在实验规模有限和场景重构缓慢等缺陷。在虚实结合的试验场环境中，以基于云平台构建的虚拟网络可以极快的速度提供大规模虚拟网元互联的复杂网络试验环境，可以较低的成本满足多种大规模复杂网络试验场景构建的需求，强化了试验场针对异构网络架构进行试验

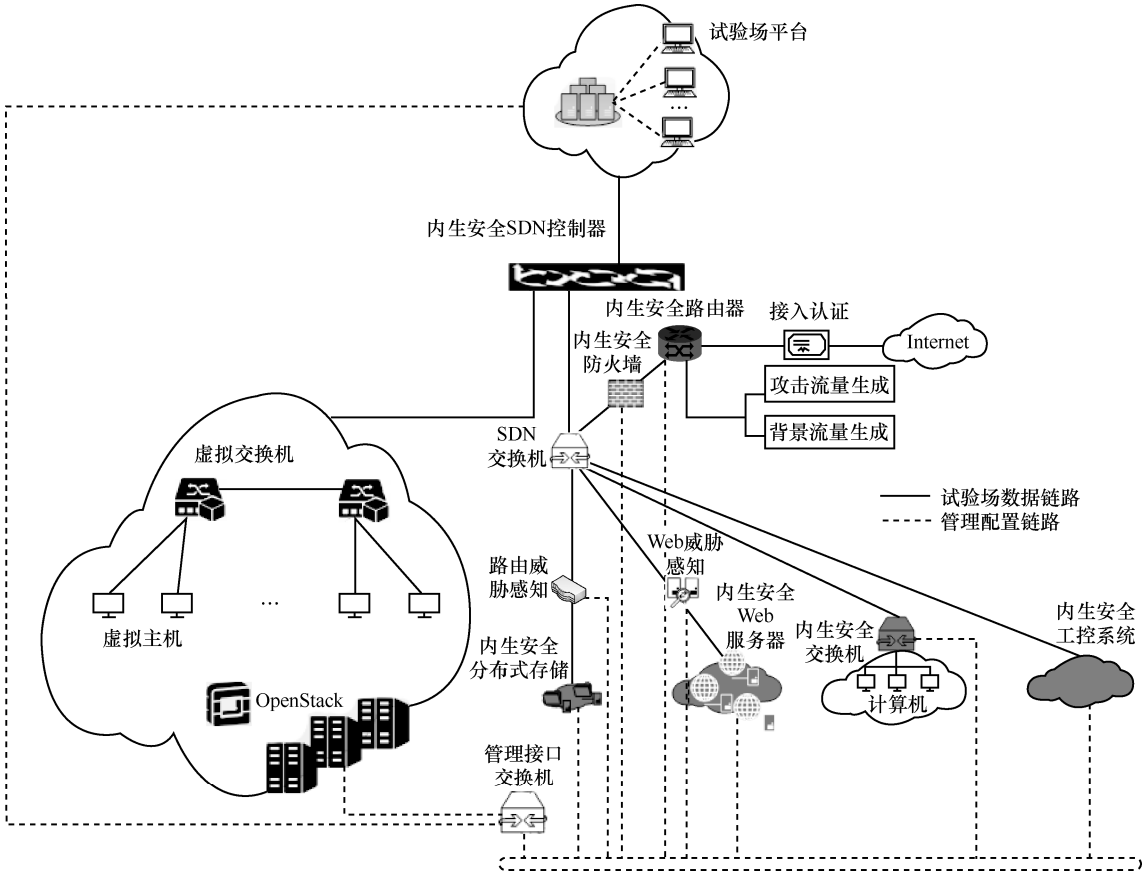

图 3　网络空间内生安全试验场组网案例

测试与攻防演练的能力。同时，虚拟网络在重构网络场景方面相对于实体网络具有较高的优势，基于镜像的虚拟网元具有快速生成、释放实例的能力，并且部分云平台支持蓝图功能，可以更为简便地实现场景切换。

在实体网络方面，通过 SDN 控制器也可以相对快速地调整网络拓扑结构，实现实体网络场景的重构。如图 3 所示的试验场组网方案中采用多网口的云平台服务器设备与 SDN 交换机，以多重标签流量牵引的 SDN 动态组网方式实现实体网元之间以及实体和虚拟网元的虚拟网络链路动态可定义，从而实现试验场应用层与物理网络环境的解耦。同时，这样的组网方式支持多种场景的并行试验测试，通过内生安全 SDN 控制器控制多个 SDN 交换机与虚拟网络，隔离出多个互不影响的网络场景，可供多个测试团队同时在试验场中针对不同的网络技术与设备进行攻防演练，提升了试验场的工作效率。

在大规模复杂组网条件下，试验场运维人员对全网设备资源的感知、配置与调度存在困难。本组网部署方案在试验场测试环境的数据链路外，独立部署管理接口链路汇聚至试验场平台。通过试验场资源编排器管理维护全网设备资源信息数据，并基于此执行试验场资源编排。试验场编排器可部署人工智能引擎，在长期运行中采集分析试验场数据，提供智能化的资源优化能力。

5　结束语

本文提出面向虚实结合的试验场管理架构与组网部署技术，可以针对性地满足网络空间安全新形势下，对于内生安全技术、设备的测试验证与人员技能的培训要求，有效利用了内生安全 SDN 控制器与数据管理链路的隔离设计为试验场提供了安全可

靠的可编排可重构能力。该管理架构基于人工智能编排器，有望发展为智能化的网络空间内生安全试验场。

参考文献：

[1] XU H, CHEN X, ZHOU J M, et al. Research on basic problems of cognitive network intrusion prevention[C]//Proceedings of 2013 Ninth International Conference on Computational Intelligence and Security. Piscataway: IEEE Press, 2013: 514-517.

[2] CHUNG C J, KHATKAR P, XING T Y, et al. NICE: network intrusion detection and countermeasure selection in virtual network systems[J]. IEEE transactions on dependable and secure computing, 2013, 10(4): 198-211.

[3] 邬江兴. 网络空间拟态防御研究[J]. 信息安全学报, 2016, 1(4): 1–10.
WU J X. Research on cyber mimic defense[J]. Cyber Security, 2016, 1(4): 1-10.

[4] 邬江兴. 拟态计算与拟态安全防御的原意和愿景[J]. 电信科学, 2014, 30(7): 1-7.
WU J X. Meaning and vision of mimic computing andmimic security defense[J]. Telecommications Science, 2014, 30(7): 1-7.

[5] 仝青, 张铮, 张为华, 等. 拟态防御 Web 服务器设计与实现[J]. 软件学报, 2017(4): 883-897.
TONG Q, ZHANG Z, ZHANG W H, et al. Design and implementation of mimic defense Web server[J]. Journal of Software, 2017(4): 883-897.

[6] 朱泓艺, 陆肖元, 李毅. 基于拟态防御原理的分布式多接入边缘计算研究[J]. 物联网学报, 2019(10): 80-87.
ZHU H Y, LU X Y, LI Y. Distributed multi-access edge computing based on mimic defense theory[J]. Chinese Journal on Interner of Things, 2019(10): 80-87.

[7] 方滨兴, 贾焰, 李爱平, 等. 网络空间靶场技术研究[J]. 信息安全学报, 2016, 1(3): 1-9.
FANG B X, JIA Y, LI A P, et al. Cyber ranges: state-of-the-art and research challenges[J]. Cyber Security, 2016, 1(3): 1-9.

[8] 刘正军, 徐锐, 李春林, 等. 面向先进防御技术的网络安全试验场构建方法[J]. 通信技术, 2020, 53(2): 450-455.
LIU Z J, XU R, LI C L, et al. Construction method of network security experimental platform foradvanced defense technology[J]. Communication Technology, 2020, 53(2): 450-455.

[9] FERGUSON B, TALL A, OLSEN D. National cyber range overview[C]//Proceedings 2014 IEEE Military Communications Conference. Piscataway: IEEE Press, 2014: 123-128.

[10] URISA V E, STOUT W M S, VANan L B, et al. Cyber range infrastructure limitations and needs of tomorrow: a position paper[C]//Proceedings 2018 International Carnahan Conference on Security Technology (ICCST). Piscataway: IEEE Press, 2018: 1-5.

[11] PETESON L, WROCLAWSKI J. Overview of the GENI architecture[J]. GENI Design Document, 2007(2): 06-11.

[12] PETERSONE L, MUIR S, ROSCOE T, et al. Planetlab architecture: an overview[J]. PlanetLab Consortium May, 2006, 1(15): 1-4.

[13] BENZEL T, BRADEN R, KIM D, et al. Experience with deter: a testbed for security research[C]//Proceedings of 2nd International Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities. Piscataway: IEEE Press, 2006: 10 .

[14] SUNE M, BERGESIO L, WOSENER H, et al. Design and implementation of the OFELIA FP7 facility: The European OpenFlow testbed[J]. Computer Networks, 2014, 61: 132-150.

[15] WINTER H. System security assessment using a cyber range[C]//Proceedings of IET International Conference on System Safety. [S.l.: s.n.], 2013.

[16] SCHWERDEL D, REUTHER B, ZINNER T, et al. Future internet research and experimentation: the G-Lab approach[J]. Computer Networks, 2014(61): 102-117.

[17] MULLER P, SCHWERDEL D. A novel approach towards sustainable testbeds: ToMaTo on cloudLab[J]. PIK-Praxis der Informationsverarbeitung und Kommunikation, 2017, 39(3-4): 87-102.

[18] MIYAJI T. X-ray-Infrared relation of AGNs and search for highly obscured accretion in the AKARI NEP Field[J]. Proceedings of the International Astronomical Union, 2019, 15(S341): 172-176.

[19] BAIK K H, SUK Y K. A Study on the ubiquitous industryz's effects on Korean economy using interindustry analysis[J]. Journal of the Korea Academia-Industrial Cooperation Society, 2006, 7(3): 494-505.

[20] 丁绍虎, 李军飞, 季新生. 基于拟态防御的 SDN 控制层安全机制研究[J]. 信息安全学报, 2018, 4(4): 84-93.
DING S H, LI J F, JI X S. Research on SDN control layer security based onmimic defense[J]. Cyber Security, 2018, 4(4): 84-93.

[作者简介]

朱泓艺（1990− ），男，博士，上海宽带技术及应用工程研究中心副研究员，主要研究方向为下一代无线通信技术、边缘计算、智能网联汽车及信息安全技术等。

陆肖元（1975− ），男，上海宽带技术及应用工程技术研究中心教授级高级工程师，上海浦东临港智慧城市发展中心主任，主要研究方向为宽带网络与智慧城市应用等。

李毅（1965− ），男，上海宽带技术及应用工程研究中心主任、博士生导师，主要研究方向为宽带网络与大数据技术及应用等。