智慧标识网络动态防御机制与应用

Dynamic Defense Mechanism and Application for Smart Identifier Networks

摘要：介绍了智慧标识网络（SINET）的基本原理，重点分析了SINET的资源动态适配机制在安全性方面的解决方案，提出了动态适配安全防御总体架构和具体机制。理论研究和实验表明，智慧标识网络动态防御机制可灵活调度网络资源、智慧服务迁移，从而较好地应对一些网络安全攻击问题。

关键词：SINET；未来网络；动态安全防御；资源适配

Abstract: In this paper, the system model and design principles of smart identifier networks (SINET) are introduced, and the application of security in dynamic resource adaptation is analyzed. Then the dynamic adaptive defense architecture and mechanism are proposed. Theoretical research and practical deployment both prove that SINET dynamic defense mechanism can flexibly schedule network resources and intelligent service migration, so as to better cope with some network security attacks.

Key words: SINET; future networks; dynamic security defense; resource adaptation

于成晓/YU Chengxiao
刘刚/LIU Gang
张宏科/ZHANG Hongke
（北京交通大学下一代互联网互联设备国家工程实验室，北京 100044）
（National Engineering Lab on Next Generation Internet, Beijing Jiaotong University, Beijing 100044, China）

DOI：10.12142/ZTETJ.201901007
网络出版地址：http://kns.cnki.net/kcms/detail/34.1228.TN.20190129.1715.010.html

收稿日期：2018-12-28
网络出版日期：2019-01-29

现有互联网起源于20世纪60年代，采用“沙漏模型”的设计思想，具有“三重绑定”的特征，即服务的“资源和位置的绑定”、网络的“控制和数据绑定”以及“身份与位置绑定”。随着用户规模的增长和多媒体应用的增多，传统互联网已经逐渐暴露出来以上各种弊端。这种网络体系和机制是相对静态和僵化的，无法从根本上满足信息网络的高速、高效、海量、泛在等通信需求。

未来网络体系架构已成为世界各国信息网络领域的研究热点。美国自然科学基金委的全球网络创新环境（GENI）[1]、未来互联网设计项目（FIND）[2]计划，以及欧盟的未来互联网研究和试验（FIRE）[3]计划等。此外，美国自然科学基金委的未来互联网体系架构（FIA）项目资助的命名数据网络（NDN）[4]、泛在移动（MobilityFirst）[5]、星云（NEBULA）[6]、富有表现力的互联网架构（XIA）[7]等重大项目，美国开放网络基金会发起的软件定义网络（SDN）研究和欧洲

电信标准化协会发起的网络功能虚拟化(NFV)研究,都从不同方面研究未来网络架构。中国也非常重视对未来网络体系架构的研究,国家“973”计划先后启动了“一体化可信网络与普适服务体系基础研究”“可信可管可控的IP网基础研究”“面向服务的未来网络体系结构与机制研究”等项目。然而,未来网络架构需要支持对网络状态的实时感知并智慧地进行网络资源的动态适配,随着网络流量和网络状态自主地从全局角度考虑网络资源,动态提高网络资源利用率。

智慧标识网络(SINET)[8-12]作为一种新型网络架构,在解决现有网络存在的诸多弊端上,创造性地引入了“三层”“两域”的概念,纵向适配,横向解耦,并引入行为描述信息来实现内嵌于网络架构中的智慧性,使网络资源能够从根本上支持资源动态适配,实现网络资源高度优化利用。智慧标识网络的核心思想是实现网络资源资源优化适配,文中我们从网络动态适配角度对“智慧标识网络中网络动态防御”这一问题展开研究。

1 SINET研究背景

1.1 SINET体系模型与工作原理

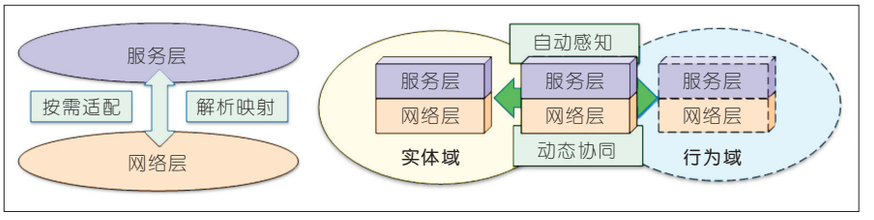
SINET针对导致互联网诸多弊端的本质原因设计了三层、两域为特征的网络体系架构,如图1所示。三层包括智慧服务层、资源适配层和网络组建层,具体功能为:智慧服务层主要负责服务的标识和描述,以及服务的智慧查找与动态匹配等;资源适配层通过感知服务需求与网络状态,动态地适配网络资源并构建网络族群,网络族群由一组网络节点或者相似功能的节点组成,负责决策优化、任务分配等,以充分满足服务需求进而提升用户体验,并提高网络资源利用率;网络组件层主要负责数据的存储与传输等实际操作,以及网络组件的行为感知与聚类等。两域指实体域和行为域。具体来说,实体域指各种各样的网络对象,是相对静态的,既包括硬件网络资源,又包括软件协议参数,本质上是指实际运行的网络。行为域指对实体域网络对象的处理逻辑和策略,是相对动态的,便于智能、适配、协同和决策等。

SINET的资源动态适配工作原理如图1所示,在智慧服务层和资源适配层之间,使用行为匹配机制:在行为域中根据服务需求行为描述和族群功能行为描述形成1次映射,为智慧服务寻求最佳的族群功能模块搭配组合,然后根据实体域内族群间的协作机制,控制指定的族群功能模块进行协同工作,从而实现服务标识到族群标识的映射过程。在资源适配层和网络组件层之间,使用行为聚类机制:在行为域中根据族群行为描述和组件行为描述形成另1次映射,为族群功能模块判定最合理的网络组件构成,然后再根据实体域的族群内联动机制,在族群功能模块内的网络组件之间建立相互联动关系,以完成族群功能模块的整体功能,实现由族群标识到组件标识的映射过程。通过这2次映射,网络资源可以依据服务需求动态适配,从而实现智慧服务。

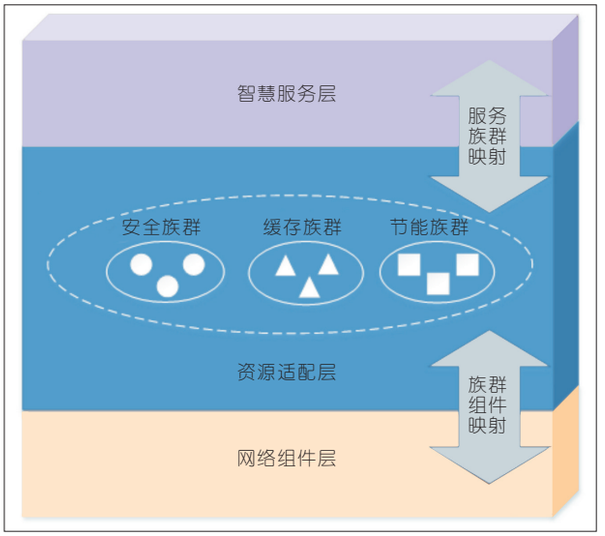
总之,智慧标识网络的三层、两域体系通过动态感知网络状态并智能匹配服务需求,进而选择合理的网络族群及其内部组件来提供智慧化的服务。同时,通过引入行为匹配、行为聚类、网络复杂行为博弈决策等机制来实现资源的动态适配和协同调度,大幅度提高网络资源利用率,降低网络能耗等,显著提升用户体验。

1.2 资源动态适配机制原理

资源适配层通过管理以及编排网络功能族群来满足动态的服务需求,其原理模型如图2



▲图1 智慧标识网络总体结构模型



◀图2
资源动态适配工作原理机制

所示。

资源适配层位于SINET3层结构中的中间层，负责感知来自上层服务需求和来自下层的网络状态，进而控制不同的网络组建形成最优化的网络族群，为上层提供特定的优质服务。资源适配层可以根据不同的服务编排不同的网络族群来支持不同类型的服务。基于上述设计，资源适配层可以更好地解决传统网络中存在的性能难题。

2 SINET动态安全防御管控

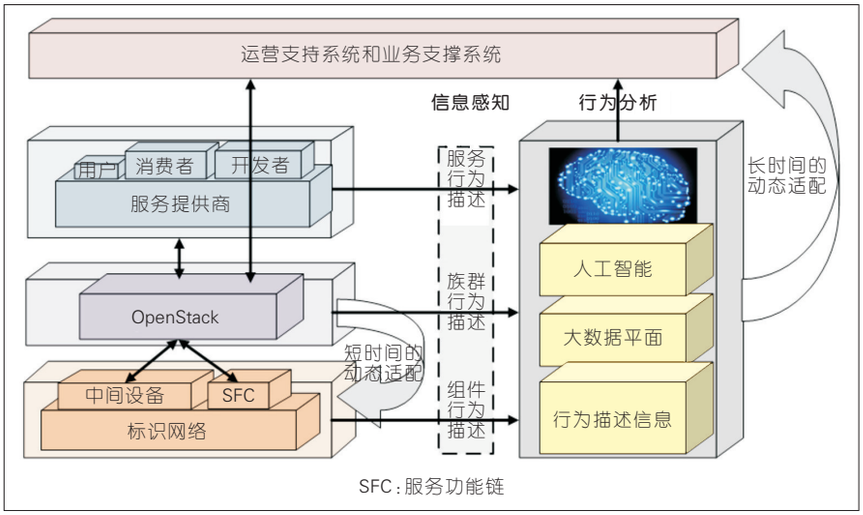
2.1 动态防御管控总体架构

SINET中资源适配层作为整体架构的中间层，是连接上层与下层实现网络的智慧化、自动化的重要组成部分。作为资源适配层的实体部分，族群是构建不同网络服务提供需求，并且根据不同族群的功能高效地管理网络组件。根据SINET总体架构以及SINET中资源适配层中的特点并结合网络功能服务链，我们提出了SINET动态防御管控架构，如图3所示。SINET动态防御管控架构是在OpenStack的平台下进行实现的。在短时间内的适配过程中，OpenStack平台下基于SINET中资源适配层族群的特点，与服务功能链（SFC）技术相结合，根据从上层感知到的服务需求，编排好对应的络族群，通过2次映射将服务需求与底层网络组件紧密地联系在一起，来实现不同的网络任务。在长时间内的适配过程中，通过日志数据收集，大数据分析平台以及人工智能技术等功能的引入，让网络更加智能化，提高网络流量的可预测性。基于SINET的动态安全防御架构的优势在于：

（1）实现动态资源适配。能够实时监测控制和分析网络中存在的网络资源和流量变化，对不用网络服务适配不同的网络族群来与网络组件对接，动态高效地管理网络，同时保证网络服务质量（QoS），优化网络能耗。

（2）动态网络防御。采用策略驱动的动态防御措施，利用SFC技术生成弹性安全功能服务链，快速察觉异常流量侵入，有效地抵御外来攻击，确保网络安全高效运行。

（3）加快网络自适应和动态感知。通过日志数据收集，以及大数据分析平台及人工智能技术等一系列功能的引入，让网络



▲图3 智慧标识网络动态防御管控架构

更加智能化，提高网络流量的可预测性。

2.2 SINET动态安全防御云平台

根据SINET的动态安全防御架构的特点和优势，基于OpenStack技术，将物理机的资源整合到一起形成虚拟资源池进行统一管理。图4为SINET动态安全防御管控云平台。OpenStack技术统一管理虚拟组件（包括虚拟计算组件、虚拟网络组件以及虚拟存储组件等），利用SINET提出的三层、两域架构，针对不同的动态安全防御措施，动态适配出不同的网络功能族群，然后通过SFC技术对每个功能族群里面的虚拟网络功能（VNF）进行编排从而达到对应的服务需求。SINET动态安全防御管控云平台基于OpenStack技术，可以支持多租户，可扩展性强，资源弹性伸缩；融合了容器与内核虚拟技术，根据不同的仿真场景灵活适配不同的技术，并且融合了Linux流量控制工具，实现了仿真网络特性的细粒度模拟。

动态安全防御云平台支持大规模拓扑动态变化的网络仿真。拓扑更新速度可达到毫秒级，规模可达100倍物理机个数；网络仿真链路信道实时模拟。每条仿真链路的误码率（10^{-4} ~ 10^{-9}）、时延（小于200 s、精度1 ms）可单独设置，支持延时抖动、延时与抖动相关性的设置；支持秒级的仿真场景快速复现，支持资源动态适配技术。

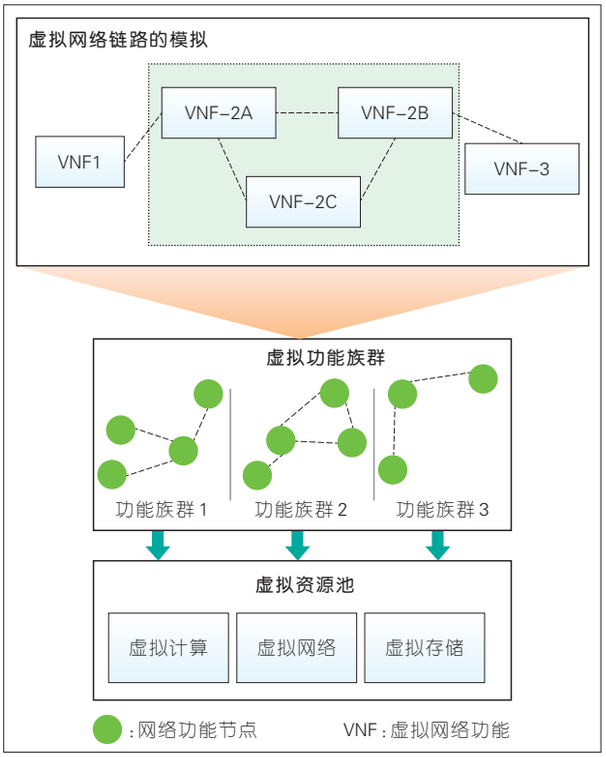
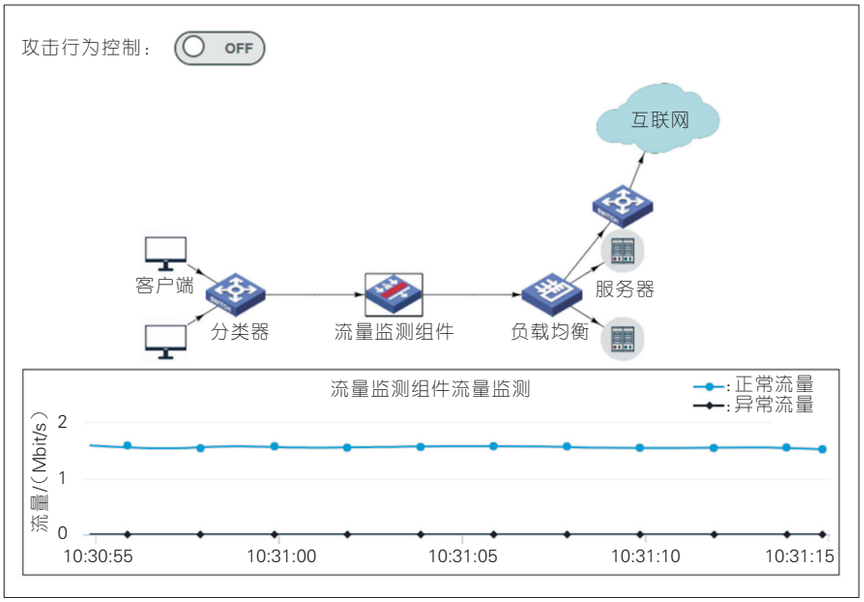
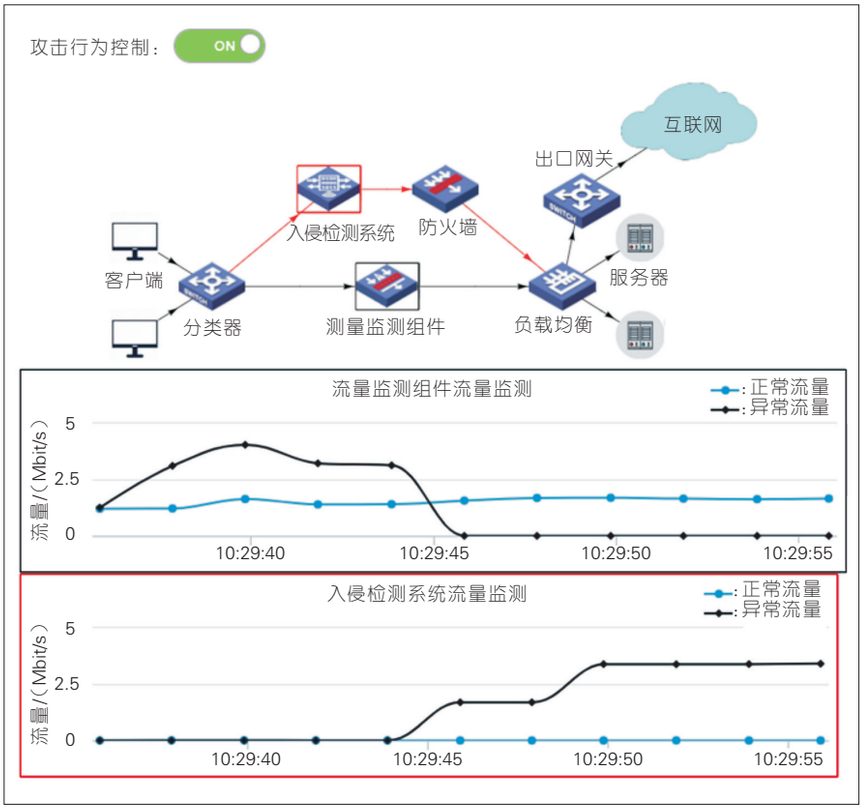


图4▶ 智慧标识网络动态安全防御管控云平台

图5和图6为SINET动态安全防御功能实例，其中分类器检测异常流量，筛选不同类型的流量，将经过不同SFC的数据包进行不同封装。图5是未发起恶意流连攻击时网络族群构成的网络组件拓扑，在流量监测控制组件中，正常流量为2 Mbit/s，异常流量几乎为零。当控制攻击



▲图5 未开启攻击时网络状态



▲图 6 开启攻击时网络状态

的行为开启后，网络中存在大数据量的异常流量，如图 6 所示。流量监测控制组件会感知异常流量的激增，从而智能化地适配新的网络族群，将生成的异常流量导入到新生成的网络族群链中，从而进行进一步的流量检测。当网络中的异常流量消失，又会自动更新为正常情况下的网络族群，实现高效地动态适配网络资源。

3 结束语

本文中，我们在简要介绍 SINET 体系结构的基础上，引入 OpenStack 和 SFC 技术，提出了基于 SINET 的动态安全防御总体架构。进一步地，我们还介绍了 SINET 动态安全防御管控云平台基本功能。通过实验，我们展示了智慧标识网络动态安全防御的效果，实现了动态地适配网络资源，从而缓解网络攻击行为造成的网络影响。SINET 作为一种新型网络架构和技术，有望应用于未来的 5G 核心网，使网络更高效、更灵活、更智能、更安全。

参考文献

[1] NSF. GENI: Global Environment for Network Innovations [EB/OL].(2018–04–28)[2019–12–28]. http://www.geni.net
[2] NSF. FIND: Future Internet Network Design. [EB/OL]. [2019–12–28]. http://www.nets–find.net/
[3] European Commission. FIRE [EB/OL]. [2019–12–28].http:///cordis.europa.eu/fp7/ict/fire/
[4] NSF. Named Data Networking [EB/OL]. [2019–12–28].http:///www.named–data.net/
[5] NSF. MobilityFirst [EB/OL]. [2019–12–28]. http://mobilityfirst.winlab.rutgers.edu/
[6] NSF. Nebula [EB/OL]. [2019–12–28]. http://nebula–fia.org/
[7] NSF. XIA–eXpressive Internet Architecture [EB/OL]. [2019–12–28].http://www.cs.cmu.edu/~xia/
[8] 张宏科, 罗洪斌. 智慧协同网络体系基础研究[J]. 电子学报, 2013, 41(7): 1249–1254. DOI: 10.3969/j.issn.0372–2112.2013.07.001
[9] ZHANG H K, DONG P, YU S, et al. A Scalable and Smart Hierarchical Wireless Communication Architecture Based on Network/User Separation [J]. IEEE Wireless Communications, 2017, 24(1): 18–24. DOI: 10.1109/mwc.2017.1600135wc
[10] ZHANG H K, LUO H B, CHAO H C. Dealing with Mobility–Caused Outdated Mappings in Networks with Identifier/Locator Separation [J]. IEEE Transactions on Emerging Topics in Computing, 2016, 4(2): 199–213. DOI:10.1109/tetc.2015.2449664
[11] ZHANG H K, QUAN W, SONG J Y, et al. Link State Prediction–Based Reliable Transmission for High–Speed Railway Networks [J]. IEEE Transactions on Vehicular Technology, 2016, 65(12): 9617–9629. DOI:10.1109/tvt.2016.2598473
[12] 权伟, 张宏科. 未来互联网体系的研究现状、热点与探索实践[J]. 中国科学:信息科学, 2017, 47(6): 804–810

作 者 简 介

于成晓，北京交通大学在读博士研究生；目前主要研究方向为未来网络架构、网络传输协议；已发表国际会议论文 1 篇。

刘刚，北京交通大学在读博士研究生；目前主要研究方向包括未来互联网、网络安全、软件定义网络和可编程数据平面等；已发表国际会议论文 1 篇。

张宏科，北京交通大学教授、下一代互联网互联设备国家工程实验室主任，电子学会理事，国家“973”项目首席科学家；目前主要从事未来网络体系理论及工程技术应用相关研究；曾获得 2014 年国家技术发明奖二等奖、2017 年国家技术发明奖二等奖、2017 年教育部技术发明一等奖等；已发表论文 100 余篇。