ISSN 1002-4956
CN11-2034/T

实 验 技 术 与 管 理
Experimental Technology and Management

第35卷 第11期 2018年11月
Vol. 35 No. 11 Nov. 2018

DOI:10.16791/j.cnki.sjg.2018.11.028

基于软件定义网络的安全攻防虚拟仿真实战平台

叶福玲[1,2]，张 栋[1,2]，林为伟[1,2]

(1. 福州大学 数学与计算机科学学院，福建 福州 350116；
2. 福州大学 网络信息安全与计算机技术国家级实验教学示范中心，福建 福州 350116)

摘 要：为解决传统网络安全攻防虚拟仿真实验教学产品网络拓扑不够灵活、攻防模式切换困难、较难与其他开源产品融合的问题，提出建设基于软件定义网络的安全攻防虚拟仿真实战平台。介绍了平台的设计思路、关键技术和网络拓扑。平台设计基于SDN和虚拟化，利用OpenStack开源云平台构建虚拟网络部件和SDN网络拓扑，并有效实施网络隔离。攻防实战环境的设置过程展现出支持网络拓扑和攻防模式的多样化和灵活性，提高了平台的可扩展性，降低了建设成本，促进了网络攻防虚拟仿真实战教学水平的提高。

关键词：软件定义网络；网络攻防；虚拟仿真；OpenStack

中图分类号：TP393；G434 **文献标识码**：A **文章编号**：1002-4956(2018)11-0125-05

Virtual simulation actual-combat platform for security attack and defense based on software defined network

Ye Fuling[1,2], Zhang Dong[1,2], Lin Weiwei[1,2]

(1. College of Mathematics and Computer Science, Fuzhou University, Fuzhou 350116, China;
2. National Experimental Teaching Demonstration Center of Network Information Security and Computer Technology, Fuzhou University, Fuzhou 350116, China)

Abstract: To solve the problems that the virtual simulation experimental teaching products for the traditional network security attack and defense are not flexible in the network topology, and it is difficult for them to switch between offensive and defensive modes and integrate with other open source products, a virtual simulation platform for the network security attack and defense based on software definition network is proposed, and the design idea, key technology and network topology of the platform are introduced. The platform design is based on SDN and virtualization. By using the OpenStack open source cloud platform, the virtual network components and SDN network topology are constructed, and network isolation is effectively implemented. The process of setting up the offensive and defensive environment shows that this platform supports the diversification and flexibility of the network topology and attack and defense mode, improves the scalability of the platform, reduces the construction cost, and promotes the improvement of the virtual simulation actual-combat teaching level of the network attack and defense.

Key words: software defined network; network attack and defense; virtual simulation; OpenStack

随着互联网飞速发展，网络安全问题日益凸显。作为信息安全及相关专业的核心课程，计算机网络安全类课程具有较强的实践性，特别是网络安全攻防实战课程，只有通过系统实验、实训，才能让学生掌握网络安全攻防的能力。然而，由于网络安全攻防实验的特殊性和破坏性，网络安全攻防的实验教学主要依赖于虚拟仿真环境。构建网络安全攻防虚拟仿真平台对于网络安全实验教学具有重要意义[1-4]。

近年来，虚拟仿真实验教学产品在一定程度上满足了网络安全攻防实战教学的需要，但却存在一些共性问题，主要是：(1)产品网络拓扑相对固化，实现拓扑

收稿日期：2018-07-20
基金项目：教育部产学合作协同育人基金项目(201602012018)；福建省高等学校服务产业特色专业建设项目(50009437)；福州大学学科特色创新创业课程建设项目
作者简介：叶福玲(1974—)，女，福建永春，本科，实验师，示范中心副主任，主要研究方向为软件定义网络、实验室建设与管理
通信作者：张栋(1981—)，男，福建福州，博士，副教授，主要研究方向为软件定义网络.
E-mail：hangdong@fzu.edu.cn

的灵活变化困难；(2)产品提供的攻防环境模式相对单一，攻防环境设置和切换困难；(3)产品的技术细节被屏蔽，较难实现与其他开源软件融合。随着软件定义网络(software defined networking，SDN)的发展，上述问题有望得到解决。

作为新型网络架构，SDN 将转发与控制相分离。控制平面负责数据转发策略的制定和下发；数据平面由交换机等网络元素组成，负责数据包的转发操作。控制平面与数据平面间通过南向 OpenFlow 协议实现通信[5-7]。SDN 通过集中式管理、网络可编程、网络虚拟化等方式，使网络能被灵活控制，支持各类应用场景的定制，为解决网络安全攻防虚拟仿真产品的共性问题提供了可行的方案。

1 网络安全攻防虚拟仿真实战平台的设计

1.1 总体思路

网络安全攻防虚拟仿真实战平台基于 SDN 架构，具有数据平面与控制平面分离、控制器集中控制网络，并可用全局视野对网内资源进行集中调度等特点。平台引入 OpenStack 开源云服务，在网络拓扑构建中按需、可度量、快速、弹性地对资源池中的计算、网络、存储等资源进行管理和分配[8-10]。在实体控制器和数据存储的基础上，平台虚拟化部署交换机、防火墙、应用服务器等，通过 SDN 控制器集中配置虚拟网拓扑，并保证虚拟网的有效隔离。平台的设计基于 SDN 和虚拟化，支持包括网络拓扑和攻防模式等实战环境的多样化和灵活变更，以适应不同的实验场景。平台基于开源技术，相对容易与其他开源软件实现融合扩展，无需产品许可，建设成本较低。

1.2 关键技术

(1) 软件定义网络 SDN。SDN 将控制功能从网络设备分离，数据平面仅维护流表结构，而流表管理归控制器负责，实现逻辑控制和数据转发相分离的网络架构。在这种架构下，控制器管理和配置网络的逻辑控制策略，交换机根据控制器下发的流表完成数据包的转发。随着 SDN 概念的提出，OpenFlow 成为 SDN 网络可编程思想的载体，代表了 SDN 的实现原型和部署实例，也是目前 SDN 控制平面和数据平面相互通信最常用的协议标准[7,11]。攻防实战平台使用 OpenFlow 1.3 实现控制平面和数据平面的通信。

(2) Open vSwitch。Open vSwitch 是一种虚拟交换机，通过编程扩展，使大规模的网络自动化成为现实，并支持标准管理接口和协议。OpenvSwitch 支持多种 Linux 虚拟化技术，是云计算平台中虚拟交换机的首选[12]。攻防实战平台使用 Open vSwitch 作为虚拟交换机。

(3) OpenStack。OpenStack 既是云计算平台项目，也是开源的云计算操作系统，它包含计算节点、控制节点、存储节点和网络节点。OpenStack 的核心服务组件包括 Nova(计算)、Neutron(网络)、Swift(对象存储)、Cinder (块存储)、Glance (镜像)、Keystone(认证)等。OpenStack 通过一个 Dashboard 控制面板为服务提供可视化的 UI 接口[13-15]。攻防实战平台使用 OpenStack 构建操作平台，实现 SDN 控制设备和转发设备等网络资源的虚拟化。

1.3 网络拓扑

平台的实体设备包括控制服务器和数据服务器。平台引入虚拟化技术，虚拟出 SDN 控制器、交换机、防火墙、实战靶机服务器、渗透主机等设备，构建 SDN 攻防实战网络拓扑。用户登录攻防平台，连接渗透主机，按照事先划分的网络拓扑渗透相应的靶机服务器，展开攻击。平台网络拓扑如图 1 所示。

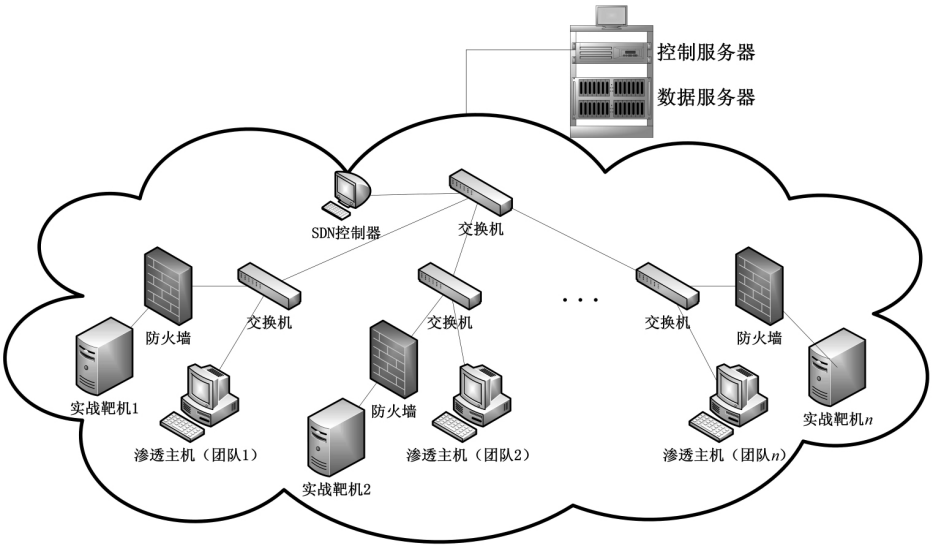

图 1 基于 SDN 的网络安全攻防虚拟仿真实战平台网络拓扑图

（1）控制服务器：攻防平台的控制节点，同时部署攻防实战管理系统和答题系统。首先，控制服务器作为 OpenStack 的控制节点，安装 Nova、Neutron、Swift 等组件，分别负责计算、网络和存储，其中 Neutron 的 L2 Agent 代理选用 Open vSwitch 实现虚拟交换，也是 SDN 交换机。控制节点的所有管理在 Dashboard 提供的 Web 界面进行。其次，控制服务器部署实战管理系统和答题系统，分别由教师（管理员）和学生使用。

（2）数据服务器：平台的数据存储，保证数据的保密性、完整性和可用性，负责对系统各类信息的统一存储和控制。

（3）SDN 控制器：OpenStack 创建的虚拟部件。下发流表，数据平面各转发设备根据流表规则完成数据包转发，使各个虚拟部件配置形成网络拓扑，并保证各组网络的相互隔离，用户只能连接相对应的靶机。

（4）交换机：OpenStack 创建的虚拟部件。控制器下发流表到虚拟交换机，由交换机连接各种攻防设备。

（5）实战靶机：OpenStack 创建的虚拟部件。根据攻防实战难度的不同，提供不同安全漏洞的系统镜像，渗透难度越大，靶机等级越高。实验时，先创建不同等级的镜像实例，再分配给相应团队。在单向攻击的模式下，每个团队渗透自己的靶机，在对战互攻模式下，两个团队可互相攻击对方的靶机，并且可以给自己的靶机设置防御措施。

（6）防火墙：OpenStack 创建的虚拟部件，主要用于隔离实战靶机，保证虚拟实战环境的隔离性。

（7）渗透主机：OpenStack 创建的虚拟部件，可连接靶机，实现渗透攻击和安装防御工具。

2 网络安全攻防虚拟仿真实战环境的设置

在开始虚拟攻防实战之前，教师或管理员需根据实验要求，提前设置实战的网络环境，学生在实战环境中开始实验。传统攻防实战平台和 SDN 的攻防实战平台在实战环境设置上有明显区别。

2.1 传统攻防实战环境设置

传统攻防实战平台采用实体设备，这些设备在部署时已人为划分好各子网，并在设备上设置了对应端口。平台在安装部署时，只需将对应的主机连接至相应的设备端口即可。这样的设计虽然简化了安装配置过程，但攻防实战的网络环境固化，扩展困难，因而不支持实战环境的多样化和灵活变更，难以适应多样化的实验场景。

现在有部分攻防实战平台采用虚拟化技术，在一定程度上解决了实体设备固化、网络扩展困难等问题。通过虚拟化技术可以方便地添加和删除网络设备。但在传统网络环境中，网络数据转发机制缺少集中控制和全局视野，一旦平台网络拓扑发生变化，就需要更改所有转发设备，同样难以支持实战环境的多样化和灵活变更，较难适应不同的实验场景。

2.2 SDN 攻防实战环境设置

引入 SDN 后的平台系统架构如图 2 所示，可以看出攻防实战平台的实战环境变得灵活，可从攻防实战环境设置的 3 个步骤体现。

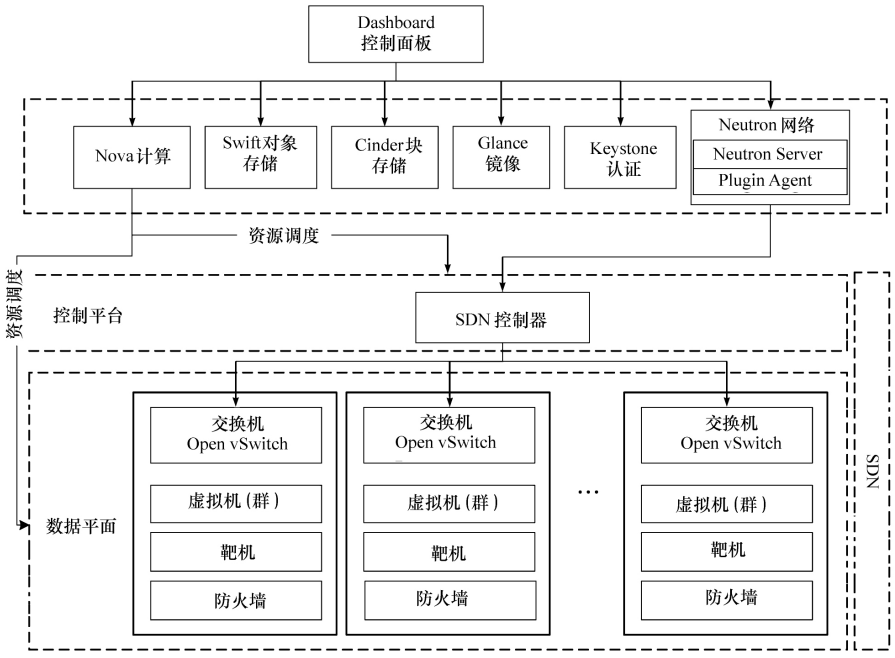

图 2 基于 SDN 的网络安全攻防虚拟仿真实战平台系统架构图

2.2.1 构建网络部件

平台利用 OpenStack 的 Neutron 组件提供虚拟网络功能，全过程通过 Nova 组件实现资源调度。OpenStack 由 NeutronServer 提供 API 给 Plugin 插件调用，实现攻防实战所需控制器、交换机、防火墙、靶机等各种部件。Plugin 访问数据库获取逻辑网络的配置信息以及同物理网络的对应关系。Plugin Agent 对 Neutron Server 端的各类 Plugin 提供代理，和各类 Plugin 完成信息交互。

在 SDN 网络下，Plugin 的选择具有多样性。以交换机为例，当 Neutron 的 Plugin 配置成 Open vSwitch 时，控制平面通过 OpenFlow 流表进行转发控制，数据平面使用 VXLAN 技术进行隧道封装，这样构建出来的网络将支持灵活的 API 调用。

此外，攻防实战平台支持在现有网络下，根据实战用户数量变化，在硬件配置允许的范围内新增或删除网络部件，实现实战环境的灵活配置。

2.2.2 构建 SDN 网络拓扑

在构建网络部件时，平台选择装有 OpenDayLight (ODL)开源控制器的虚拟机，通过北向接口连接攻防实战平台的控制软件，使用 OpenFlow 1.3 作为和交换机通信的南向接口，连接各个 Open vSwitch 交换机。

在数据包发送前，控制器需提前向交换机下发流表。流表包含所有 OpenFlow 预设或用户自定义的规则。当数据包到达交换机时，交换机根据规则匹配和处理实现转发或丢弃数据包。交换机内包含一张或多张流表，从 0 开始编号和匹配。每张流表包含了多条规则，按规则优先级先后匹配。当数据包在流表匹配到某一条规则时，交换机将更新计数器，执行 Flow Entry 设置的指令，再跳转至其他流表或直接执行匹配动作。当数据包在该流表内没有任何匹配，就进入优先级最小 Table-miss 规则，数据包默认被丢弃、发给控制器或另一张流表。

基于 SDN 的攻防实战平台能灵活定制网络拓扑。数据包匹配的内容可以是报文的任意字段，并且由 ODL 集中控制流表的下发，设置流表规则，实现任意网络部件的连通或隔离。当需要修改时，只需集中修改规则，下发新的流表。例如，在单向攻击模式中，控制器设置每台客户端虚拟机和分配靶机的连接，实现单向渗透攻击。改成互攻模式后，控制器设置客户端虚拟机可以连接防护自己的靶机，同时也可连接至对手团队的靶机进行渗透攻击。另一方面，当实战队伍数量变化时，平台支持在硬件配置能力范围内灵活新增或删减网络部件，再通过控制器向新增交换机下发流表，制定数据包的处理机制。

2.2.3 实现网络隔离

在 SDN 网络下，可用基于隧道封装模式的 Overlay 技术实现数据平面上不同用户在同一物理网络的相互隔离。攻防实战平台基于 SDN 网络，使用 VXLAN 这一典型的 Overlay 技术。如图 3 所示，虚拟机 VM1 和 VM2 经 qbr、br-int、br-tun 等 3 个虚拟网元实现 VXLAN 隧道通信。

平台的虚拟交换机 Open vSwitch 对应于 VXLAN 的 VTEP(VXLAN tunnel end point)类型的网络设备，在 Open vSwitch 上搭建 VXLAN 网络。以图 3 为例，在 VM1 上设置 VXLAN，远端 IP 设置为 VM2 能对外通信的 IP，命令格式为：

ovs-vsctl add-port [VM1 的网桥] vx1 -- set interface vx1 type=vxlanoptions:remote_ip=[VM2 能对外通信的 ip]。

VM2 设置过程同 VM1，只需将 IP 改成 VM1 能对外通信的 IP。设置完毕后，VM1 和 VM2 之间就能实现 VXLAN 隧道通信。以上设置可实现对实战链路的有效隔离，保证控制链路不受实战环境的破坏。

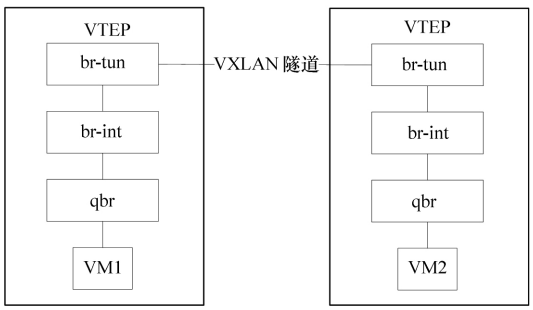

图 3 VTEP 类型的 VXLAN 示意

引入 SDN 后，实战环境设置更加便捷灵活。图 4 展示了攻防实战环境设置的流程。实战环境设置完毕，用户登录实战系统，平台分配相应的虚拟主机。用户可以连接实战环境设置时配置的靶机，进行渗透攻击和防御实验，实现单向攻击或互相攻防。整个配置过程灵活多变，并且支持在硬件配置许可的范围内随时新增或删减实战团队。表 1 总结了各种攻防实战平台的组网方案，可以看出基于 SDN 的组网方案带来的便捷。此外，整个平台设计均使用开源软件，提高了可扩展性并降低建设成本。

表 1 各种攻防实战平台组网方案比较

组网方案	新增部件	修改拓扑
传统网络+实体设备	成本高、周期长	逐台配置修改
传统网络+虚拟化	虚拟化，快捷便利	逐台配置修改
SDN+虚拟化	虚拟化，快捷便利	数控分离，集中控制，全局视野

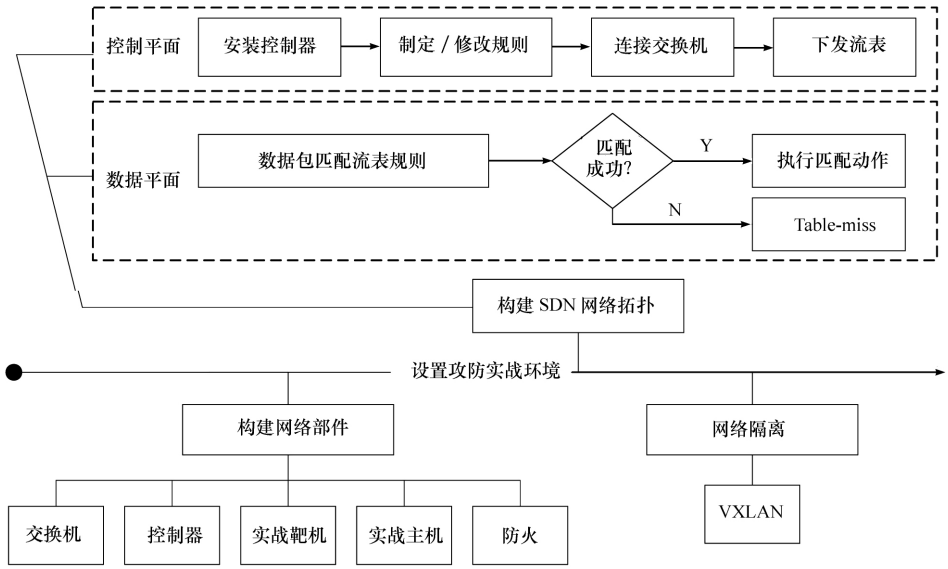

图 4　设置攻防实战环境流程

3　结语

本文提出的基于 SDN 和虚拟化的网络攻防实战虚拟仿真实验平台，实战环境的设置能够支持网络拓扑和攻防模式等实战环境的多样化和灵活变更，以适应不同的实验场景。除此之外，平台使用开源软件，提高了可扩展性，并且节省了购买产品技术许可的成本，有利于平台的推广和使用，并促进网络攻防虚拟仿真实验教学水平的提高。

参考文献(References)

[1] 黄建忠，张沪寅，裴嘉欣. 网络安全虚拟仿真实验教学体系设计[J]. 实验室研究与探索，2016，35(10)：170-174.

[2] 黄晓芳. 网络攻防实验平台开发与实现[J]. 实验技术与管理，2017，34(5)：73-76.

[3] 周敏. 网络攻防实验平台的设计[J]. 实验技术与管理，2016，33(5)：139-142.

[4] 鲁先志，胡海波. 基于开源架构的虚拟网络安全实验平台[J]. 实验技术与管理，2015，32(7)：120-123，155.

[5] 张朝昆，崔勇，唐骞骞，等. 软件定义网络(SDN)研究进展[J]. 软件学报，2015，26(1)：62-81.

[6] 柳林，周建涛. 软件定义网络控制平面的研究综述[J]. 计算机科学，2017，44(2)：75-81.

[7] McKeown N，Anderson T，Balakrishnan H，et al. OpenFlow：enabling innovation in campus networks[J]. ACM SIGCOMM Computer Communication Review，2008，38(2)：69-74.

[8] 吴怡晨，王轶骏，薛质. 面向网络空间的攻防靶场设计[J]. 通信技术，2017，50(10)：2349-2356.

[9] 底晓强，张宇昕，赵建平. 基于云计算和虚拟化的计算机网络攻防实验教学平台建设探索[J]. 实验技术与管理，2015，32(4)：147-151.

[10] 周敏. 网络攻防实战教学系统的设计与实现[J]. 实验技术与管理，2016，33(6)：154-156，171.

[11] 左青云，陈鸣，赵广松，等. 基于 OpenFlow 的 SDN 技术研究[J]. 软件学报，2013，24(5)：1078-1097.

[12] Open vSwitch. What is Open vSwitch[EB/OL]. [2018-05-27]. http://www.Open vSwitch.org/.

[13] OpenStack. What is OpenStack[EB/OL]. [2018-05-27]. https://www.openstack.org/software/.

[14] 任晶晶，戴锦友，刘琼，等. 基于 OpenStack 的 SDN 相关技术研究[J]. 光通信研究，2016(1)：11-14.

[15] 刘瑛. SDN 在 Openstack 云数据中心的技术研究[J]. 移动通信，2016，40(22)：56-60.

(上接第 124 页)

[9] 冒建亮，李奇，朱海荣. 一种连续非奇异快速终端滑模控制方法[J]. 控制与决策，2016，31(10)：1873-1878.

[10] 李升波，李克强，王建强，等. 非奇异快速的终端滑模控制方法及其跟车控制应用[J]. 控制理论与应用，2010，27(5)：543-550.

[11] 周硕，王大志，高庆忠. 永磁同步电机的非奇异快速终端滑模控制[J]. 电气传动，2014，44(11)：51-54.

[12] 华玉龙，孙伟，迟宝山，等. 非奇异快速终端滑模控制[J]. 系统工程与电子技术，2017，39(5)：1119-1125.

[13] 侯利民，李勇，孙钊. PMSM 混沌运动的非奇异快速终端滑模控制[J]. 控制工程，2017，24(11)：2206-2210.

[14] 薛定宇. 控制系统计算机辅助设计：MATLAB 语言与应用[M]. 3 版. 北京：清华大学出版社，2012.

[15] 赵海滨. MATLAB 应用大全[M]. 北京：清华大学出版社，2012.

[16] 石良臣. MATLAB/Simulink 系统仿真超级学习手册[M]. 北京：人民邮电出版社，2014.