面向网络攻击态势的 SDN 虚拟蜜网

廉　哲，殷肖川✉，谭　韧，卞洋洋
(空军工程大学信息与导航学院，西安，710077)

摘要　针对现有网络态势感知研究无法按需获取态势信息，不能根据网络攻击态势威胁情况对网络结构进行动态调整等问题，利用 SDN 对网络流量灵活控制的基本原理，并结合 OpenDaylight 控制器良好的扩展性和可管控性等性质，提出一种基于 SDN 的虚拟蜜网架构。通过构建 SDN 虚拟蜜网，实现了数据控制层与数据传输层的分离，解决了传统蜜网在网络态势获取方面存在的流量控制困难以及物理机部署不方便、动态调整部署复杂的问题。最后，利用 Mininet 平台搭建 SDN 虚拟蜜网进行仿真验证，实验结果表明 SDN 虚拟蜜网能够实现按需获取态势信息、动态调整网络结构等功能，从而减少网络攻击态势威胁。

关键词　攻击态势；软件定义网络；虚拟蜜网；按需获取；动态调整
DOI　10.3969/j.issn.1009-3516.2017.03.014
中图分类号　TP393.08　　**文献标志码**　A　　**文章编号**　1009-3516(2017)03-0079-06

Research on SDN Virtual Honeynet for Network Attack Situation

LIAN Zhe, YIN Xiaochuan, TAN Ren, BIAN Yangyang
(Information and Navigation College, Air Force Engineering University, Xi'an 710077, China)

Abstract: Aimed at the problems that the existing network situation awareness cannot acquire on-demand situation information and cannot adjust the network structure according to situational threat of network attacks dynamically, a SDN-based virtual honeynet architecture is proposed on the basis of flexible traffic control principle with the combination of good scalability and manageability of OpenDaylight controller. Through constructing a SDN-based virtual honeynet, the separation between data control layer and data transmission layer is realized. Simultaneously, traffic controlling difficulty and inconvenience of deploying or dynamically adjusting physical machines are solved compared to traditional honeynets. At last, the paper utilizes Mininet platform for building SDN virtual honeynet. The experiment results show that the SDN-based virtual honeynet can achieve on-demand access to situation information and dynamic adjustment of network structure etc. , thus reducing the network attack threat.

Key words: attack situation; software defined networking; virtual honeynet; on-demand acquisition; dynamic adjustment

当今网络环境日趋复杂，网络信息安全成为人们关注的焦点，网络态势感知研究对于当前网络安

收稿日期：2016-12-14
基金项目：陕西省工业科技攻关项目(2016GY-087)
作者简介：廉　哲(1994—)，男，山西万荣人，硕士生，主要从事网络与信息安全研究. E-mail：lianzkgd@163.com
通讯作者：殷肖川(1961—)，男，陕西西安人，教授，主要从事网络与信息安全研究. E-mail：byy0902@163.com

引用格式：廉哲，殷肖川，谭韧，等. 面向网络攻击态势的 SDN 虚拟蜜网[J]. 空军工程大学学报(自然科学版)，2017，18(3)：79-84. LIAN Zhe，YIN Xiaochuan，TAN Ren，et al. Research on SDN Virtual Honeynet for Network Attack Situation[J]. Journal of Air Force Engineering University (Natural Science Edition)，2017，18(3)：79-84.

全状态具有较深的认知,可以对网络状态做出评估与预测,从而为决策者提供数据支撑。蜜网[1-2]采用一种主动防御机制,通过引诱攻击者进入提前设计好的蜜罐网络,监控攻击者行为,引诱攻击者进行操作,一方面可以起到保护真实网络的作用;另一方面可以通过引诱攻击者进而获取更多的态势信息,通过进一步对获取到的态势信息进行分析评估预测,从而进行有效防御。然而,网络环境是实时变化的,为了能够实现按照需求来获取攻击态势信息[3],并能灵活应对网络遭受的各类攻击,本文提出了一种基于 SDN[4-5](Software Defined Networking,简称 SDN)的虚拟蜜网架构,该架构较传统的蜜网系统成本较低,部署快速,通过软件来定义逻辑上的网络拓扑,利用虚拟化技术[6]来构建网络拓扑,以满足对网络资源的不同需求,无需关心底层网络的物理拓扑结构并且可以实现动态部署。一方面可以动态改变网络结构来减少网络安全威胁,提高网络安全性;另一方面可以通过动态部署进而获取有针对性、有价值的态势信息,并且可以结合流表信息,为决策提供数据支撑并实现主动防御。

1 相关研究

蜜罐技术最早提出是由于互联网存在太多安全问题[7]:安全基础薄弱、攻击工具较多、网络攻防处于非对称博弈,为了改变这种攻防博弈的非对称性,蜜罐技术得以使用。蜜网技术实质上是一种研究型、高交互型的蜜罐技术[8]。之前人们的研究主要集中于蜜网系统的 5 类关键技术[9]:网络欺骗、数据捕获、数据控制、攻击分析与特征提取、预警预防技术,提出了大量高效的算法。目前蜜网已经发展到第 3 代,其核心技术在于其昂贵的蜜墙设备,这使得安全防护成本较高[10]。但是,传统的蜜网存在系统流量控制困难,物理机部署不方便,动态调整复杂,蜜墙设备昂贵的问题,无法应对态势多变的网络环境,不能对网络态势进行有针对性的调整从而获取有效的态势信息[11]。胡毅勋[12]在 2015 年提出了基于 Openflow 协议的虚拟蜜网系统,运用 Openflow 交换机验证了蜜网系统转发时延低、动态性强的特性和叠加虚拟蜜网系统的有效性。赖积保[13]等人提出的基于简单加权法和灰色理论的网络安全态势感知模型能够较方便地量化直观反映当前网络攻击态势。本文在前人研究基础上,进一步对网络攻击态势进行分析处理,构建 SDN 虚拟蜜网,实现按需获取态势信息,应对网络态势状况动态调整网络结构,降低网络攻击态势威胁状况。

2 预备知识

2.1 SDN 架构

SDN[14-16]提出了一种软件定义网络的网络架构,它可以通过软件对专用的网络设备进行部署,通过特定的控制器对网络中的流量实现实时控制,达到数据控制层与数据传输层的分离,能够节约网络部署成本,方便动态调整控制网络状态,提高了网络的灵活性与可管控性,见图 1[17-19]。基于此,可以开发各种应用程序,通过软件来定义逻辑上的网络拓扑,以满足对网络资源的不同需求,且无需关心底层网络的物理拓扑结构,通过 SDN 控制器对网络中的流量进行控制,实现按照用户需要控制网络结构和功能的特性。

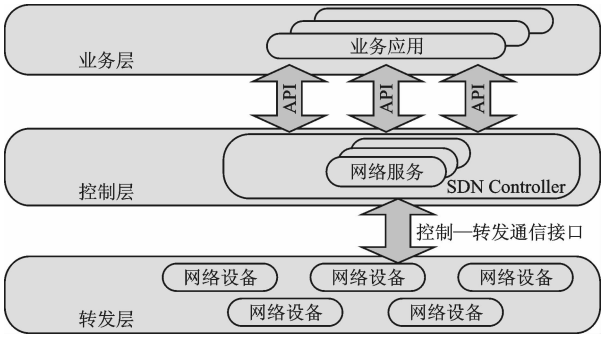

图 1 SDN 基本架构

Fig. 1 SDN basic architecture

2.2 对文献[13]模型的分析与改进

文献[13]依据网络所提供的各类服务数量以及遭受到的不同类别威胁,提出了一种基于简单加权法的攻击态势评估模型。相关符号意义、参数说明、具体模型详见文献[13]。文中定义当前网络安全态势状况由

$$F=(S,A,C,N,T)=\sum_{i=1}^{n}\beta_i\left(\sum_{j=1}^{m}10^{T_{ij}}C_{ij}\right) \quad (1)$$

来表示,F 越大,网络受到的威胁程度越大。

通过实验利用模型对网络态势情况进行了获取与评估,得到 2 组数据:表 1 为网络中服务运行状况,表 2 为服务受到的攻击次数以及威胁程度,其中空白处表示在该时间段内该服务未运行,“0”表示该时段内该服务未受到攻击,用{威胁程度(攻击次数)}表示服务受到的威胁状况。

依据表 1、2 和模型公式可以计算出各个时间段的攻击态势,文献[13]仅是对攻击态势进行了计算与预测,并未应对攻击态势进行处理。本文通过对表 1、2 中不同的服务遭受到的攻击次数以及威胁程度的情况分析,设计基于 SDN 的动态虚拟蜜网,改

变网络结构，从而可以通过减少或者停止高危服务来降低攻击威胁态势；并可以针对当前态势，按需获取更多信息，提供更多易于攻陷利用的服务，达到按需获取态势信息的目的。

表 1　服务运行状况

Tab. 1　Service operation condition

时间	服务名称	β_i	n
T_1	{FTP,RPC,SOCKET}	{0.335,0.375,0.29}	3
T_2	{FTP,RPC,DNS,SOCKET,HTTP}	{0.265,0.282,0.103,0.295,0.155}	5
T_3	{FTP,RPC,SOCKET,TELNET}	{0.192,0.391,0.306,0.111}	4
T_4	{FTP,RPC}	{0.564,0.436}	2
T_5	{FTP,RPC,SOCKET,HTTP}	{0.079,0.295,0.237,0.389}	4

表 2　服务受到攻击次数及威胁程度

Tab. 2　Number of service attack and threat level

时间	FTP	RPC	DNS	SOCKET	HTTP	TELNET
T_1	{1(2)}	{1(3)}		{1(5)}		
T_2	{1(1)}	{2(2)}	{2(2)}	{1(1)}	0	
T_3	{2(2),1(2)}	{1(1)}		{2(1)}		{2(2)}
T_4	{2(1),1(6)}	{1(1)}				
T_5	{3(1),1(3)}	{1(4)}		0	{1(2)}	

3　基于 SDN 的虚拟蜜网

3.1　虚拟蜜网架构

利用 SDN 控制器 OpenDaylight，简称 ODL，与轻量级软件定义网络测试平台 Mininet[20] 相结合，通过 mininet 部署虚拟蜜网，ODL 控制网络流量转发实现虚拟蜜网功能，蜜网架构见图 2。

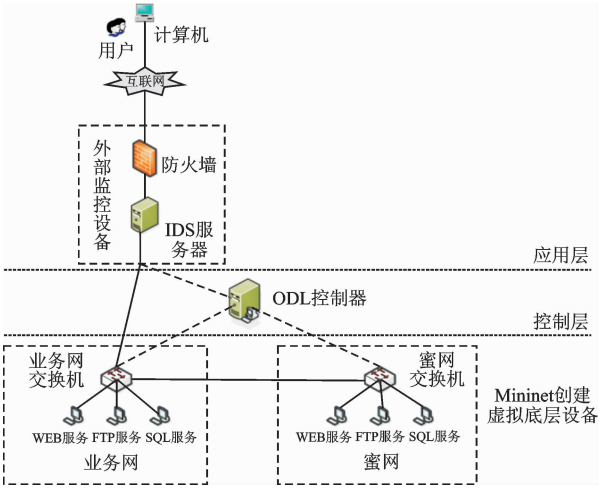

图 2　基于 SDN 的虚拟蜜网

Fig. 2　Virtual honeynet based on SDN

基于 SDN 架构，将网络共分为 3 层：应用层供外部用户进行访问或者诱导攻击方对蜜网实施攻击；控制层利用 ODL 控制器对虚拟蜜网实施流量转发控制并搜集网络流表信息，可以作为态势信息获取的一个途径；虚拟底层设备用于搭建业务网与虚拟蜜网，虚拟蜜网通过诱导攻击者进行访问攻击，一方面可以保护真实系统免遭攻击；另一方面可以按照需求动态调整网络结构，引诱攻击者攻击，进而获取更多有效态势信息。

3.2　网络流量转发过程

当攻击方对 SDN 虚拟蜜网进行攻击时，通过防火墙、IDS 设备监控可以通知 ODL 控制器对网络流量进行控制转发，引诱攻击方对蜜网实施攻击，实现蜜网功能，获取态势信息。流量转发过程见图 3。

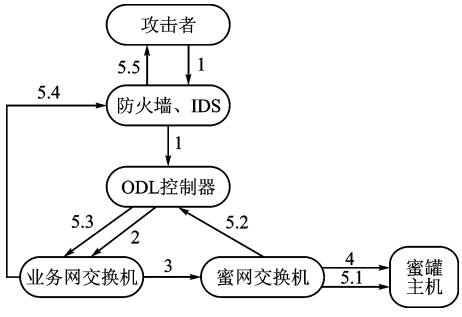

图 3　攻击流量转发过程

Fig. 3　Attack flow forwarding process

Step1　当攻击方访问业务时，首先经过防火墙与 IDS 设备的监测分析，当检测到有攻击行为时，向 ODL 控制器进行通报。

Step2　ODL 控制器将流量转发命令通过流表的形式发送给业务网虚拟交换机。

Step3　业务网交换机解析流量控制命令以后将攻击者请求内容转发至蜜网。

Step4　蜜网交换机根据接收到的请求，对流量进行控制转发至相应服务中。

Step5　蜜网将响应流量发送至 ODL 控制器，

ODL 控制器通过改变流表信息将响应流量通过业务交换机转发至外部网络,完成信息交互。

Step6 ODL 控制器通过监控与分析蜜罐系统中流量的 shell 命令或者特权行为等来判断攻击行为,分析攻击方的时空信息等,达到蜜网诱骗获取网络态势信息的目的。

整个网络架构通过防火墙、IDS、ODL 控制器对网络中的流量、日志等信息进行监控、记录,可以在攻击者未发现被诱骗的情况下更多的捕获网络态势信息,分析攻击行为,评估预测态势状况,从而做出相应对策。

3.3 与传统蜜网比较

运用 SDN 架构结合 ODL 控制器构建虚拟蜜网,能解决传统蜜网流量控制困难以及物理机部署不方便、动态调整部署复杂的问题。利用 SDN 架构实现流量转发与控制的分离,运用 Mininet 构建虚拟化蜜罐主机,能够实现动态调整网络结构、保护真实主机与按需获取态势信息的功能。

构建 SDN 虚拟蜜网采用当前比较流行的一种可扩展、通用化的大型控制器架构 OpenDaylight 并结合虚拟机等虚拟化技术来实现动态虚拟蜜网的部署。与其它控制器相比,ODL 设计灵活,扩展性好;在功能上,ODL 支持更多的协议,具有更为全面的服务功能,ODL 还得到微软、思科、IBM 等公司的支持,更有可能在实际中得到广泛的应用[21-22]。目前主流开源控制器对比见表 3。由表 3 可以看出 ODL 控制器较其它控制器支持更多的南向协议,且版本更新速度较快(平均每 6 个月有较大的更新),应用前景更好。

表 3 主流开源控制器对比

Tab. 3 Mainstream open source controller comparison

控制器	开发语言	支持的协议	多平台支持	更新频率
Floodlight	Java	OpenFlow 1.0	Linux/Win	较低
Ryu	Python	OpenFlow1.0/1.3 等	Linux	较低
OpenDaylight	Java	OpenFlow1.0/1.3、BGP 等	Linux/Win	较高
Beacon	Java	OpenFlow 1.0	Linux/Win	较低
OpenContrail	C++	BGP、XMPP	Linux	较低

4 仿真实验

4.1 实验部署

本文利用虚拟机软件 VMware 12,一共构建 2 台虚拟机。一台虚拟机安装 Ubuntu 系统,在其上面安装 ODL 控制器 Beryllium 版本;另一台虚拟机安装 Ubuntu server 版本,并安装 Mininet-2.2.1。将 2 台虚拟机互联,利用 Mininet 建立虚拟蜜网,通过 ODL 控制器对蜜网进行流量控制。利用虚拟机进行部署可以比较方便的实现虚拟蜜网的构建,设施简单,成本较低。通过 Mininet 部署 SDN 网络,可以实现跟实体机同样的工作效果,还可以支持复杂拓扑,使用方便,功能强大,易于还原。

4.2 仿真测试与分析

测试目的是为了验证基于 SDN 架构与 ODL 控制器的蜜网动态调整部署的便利性以及对于网路态势状况的应对调整,提高网络安全性。利用 Mininet 创建 2 个交换机节点,每台交换机配置 2 个主机,分别代表 HTTP 服务与 MySQL 服务。图 4 为 ODL 控制器监控到的拓扑结构,其中左交换机为业务系统,对外提供 2 个服务,右交换机为蜜罐系统,用来诱导攻击者实施攻击行为。

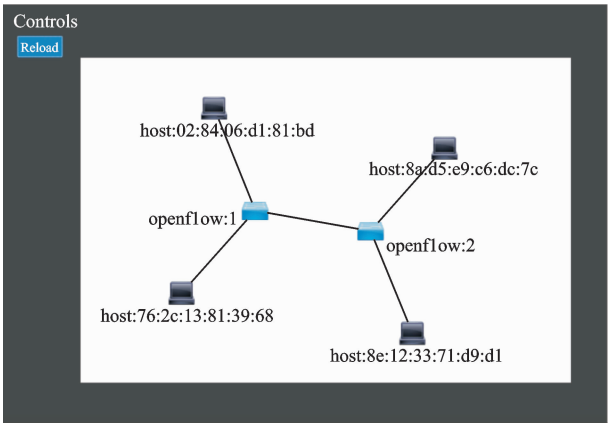

图 4 虚拟蜜网拓扑图

Fig. 4 Virtual honeynet topology

动态虚拟蜜网相比较静态蜜罐具有难识别、成本低等优点,应用前景很广,且利用虚拟化技术更符合未来网络发展环境。该架构可以通过自定义 Python 脚本定义网络拓扑结构,核心代码见图 5,可以按照需要增加删除服务主机,动态调整网络结构,降低网络态势威胁,提高网络安全性。

利用文献[13]所得实验数据,以 T_2 和 T_5 时间段为例,这 2 个时间段的安全态势为 $F_2=83.2$,$F_5=100.95$。通过表 1、2 可以看出,在 T_2 时间段 RPC 与 DNS 服务受到的攻击次数与威胁程度相对

较多，但 RPC 服务所占比重相对较大，可以通过 SDN 虚拟蜜网实现快速改变网络结构，停止 RPC 服务。当停止 RPC 服务之后，系统服务所占权重发生变化：

$$\beta'_1 = \frac{\beta_1}{\sum_{i=1,i\neq 2}^{n} \beta_i} \tag{2}$$

图 5　定义拓扑核心代码图

Fig. 5　Define topology core code

改变网络拓扑结构后，各服务权重见表 4。

表 4　调整后各服务权重

Tab. 4　Adjusted each service weight

时间	服务名称	β_i	n
T_2	{FTP，DNS，SOCKET，HTTP}	{0.324，0.126，0.361，0.189}	4

此时网络安全态势 $T'_2 = 32.05 < 83.2 = T_2$，通过虚拟蜜网调整网络结构后可以降低网络安全态势，提高网络安全性。

对于 T_5 来说，当时网络 FTP、RPC、HTTP 服务遭受到攻击较为严重，为了获取更多有关攻击手段、方式、时空信息等，可以通过动态调整网络结构，增加更多诱饵蜜罐主机等用来获取态势信息，实现按需获取态势信息的目的。并为实际服务提供更加针对性的保护与防御。当攻击方攻击一段时间之后，再次对蜜网系统进行动态调整，时刻转变网络状态，只有将网络状态时刻处于变化中，才能保证网络的不透明性，使网络得到有效保护。

通过实验验证了基于 SDN 的动态虚拟蜜网可以解决传统蜜网流量控制困难以及物理机部署不方便、动态调整部署复杂的问题，结合简单加权法网络攻击态势评估模型进一步验证了 SDN 动态虚拟蜜网可以实现按需获取态势信息，能够按照态势需要动态调整网络结构，从而减少网络态势威胁状况，并获取更多有效态势信息。

5　结语

本文在前人研究的基础上，综合网络攻击态势感知研究与 SDN 相关技术，利用 SDN 架构，通过 ODL 控制器与 Mininet 相结合，设计了动态虚拟蜜网。该架构可实现传统意义上的蜜网系统的基本功能，可以方便地进行蜜网部署，添加或者删除各类服务，更节约成本，部署更加方便，系统更加容易还原。通过实验验证了基于 SDN 动态虚拟蜜网对于网络攻击态势研究的意义：一方面可通过动态停止高危服务，降低网络安全态势状况，提高网络系统安全性；另一方面，可以通过分析网络态势，按需动态部署蜜罐服务，获取更多态势信息，为决策提供支撑。

由于 Mininet 属于轻量级软件定义网络测试平台，功能服务有限，在后期研究工作中，可以利用多台虚拟机实现软件定义网络架构，在此基础上部署更复杂与功能服务更完善的虚拟蜜网。其次可以对 ODL 控制器进行更充分的利用，结合流表信息与传统的网络态势感知分析算法，进行威胁性分析、态势评估、态势预测等分析网络安全态势，提供态势信息支撑。

参考文献(References)：

[1] GAUTAM R, KUMAR S, BHATTACHARYA J. Optimized Virtual Honeynet with Implementation of Host Machine as Honeywall [C] // 2015 Annual IEEE India Conference. IEEE, 2015: 1-6.

[2] 胡双双. 基于蜜网的攻击行为分析 [D]. 北京：北京邮电大学, 2015.
HU S S. Analysis of attack based on honeynet [D]. Beijing: Beijing University of Posts and Telecommunications, 2015. (in Chinese)

[3] 陈珍，夏靖波，陈婉，等. 基于关联规则的态势预测方法 [J]. 空军工程大学学报(自然科学版)，2016，17(4)：85-89.
CHEN Z, XIA J B, CHEN W, et al. A Situation Forecast Method Based on Association Rules [J]. Journal of Air Force Engineering University (Natural Science Edition), 2016, 17(4): 85-89. (in Chinese)

[4] YAN Q, YU R, GONG Q, et al. Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: a Survey, Some Research Issues, and Challenges [J]. IEEE Communications Surveys & Tutorials, 2016, 18(1): 602-622.

[5] FEAMSTER N, REXFORD J, ZEGURA E. The

road to SDN: An Intellectual History of Programmable Networks [J]. Acm Sigcomm Computer Communication Review, 2014, 44(2): 87-98.

[6] 陈靖, 黄聪会, 孙璐, 等. 应用虚拟化技术研究进展[J]. 空军工程大学学报(自然科学版), 2013,14(6): 54-58.
CHEN J, HUANG C H, SUN L, et al. Survey of the Research on Application Virtualization Technology [J]. Journal of Air Force Engineering University (Natural Science Edition), 2013,14(6): 54-58. (in Chinese)

[7] KIZZA J M. Guide to Computer Network Security [J]. Computer Communications & Networks, 2015.

[8] 诸葛建伟, 唐勇, 韩心慧, 等. 蜜罐技术研究与应用进展 [J]. 软件学报, 2013, 24(4): 825-842.
ZHUGE J W, TANG Y, HAN X H, et al. Honeypot Technology Research and Application [J]. Journal of Software, 2013, 24(4): 825-842. (in Chinese)

[9] STOCKMAN M, HEILE R, REIN A. An Open-Source Honeynet System to Study System Banner Message Effects on Hackers [C]// Proceedings of the 4th Annual ACM Conference on Research in Information Technology. ACM, 2015: 19-22.

[10] FAN W, FERNÁNDEZ D, DU Z. Adaptive and Flexible Virtual Honeynet [C]// International Conference on Mobile, Secure and Programmable Networking. Paris, 2015: 1-17.

[11] JI F Z, ZHOU Y T, TANG Q J, et al. Network Security Situation Assessment Based on FAHP [C]// International Conference on Automation, Mechanical Control and Computational Engineering. 2015.

[12] 胡毅勋, 郑康锋, 武斌, 等. Openflow 下的动态虚拟蜜网系统 [J]. 北京邮电大学学报, 2015(6): 104-108.
HU Y X, ZHENG K F, WU B, et al. A Dynamic Virtual Honeynet System Using Openflow [J]. Journal of Beijing University of Posts and Telecommunications, 2015(6): 104-108. (in Chinese)

[13] 赖积保, 王慧强, 朱亮. 网络安全态势感知模型研究 [J]. 计算机研究与发展, 2006, 43(S2): 456-460.
LAI J B, WANG H Q, ZHU L. Research on Network Security Situation Awareness Model [J]. Journal of Computer Research and Development, 2006, 43(S2): 456-460. (in Chinese)

[14] ZHENG Y R, SHI G W, LUO W B, et al. Software Defined Networking: a New Trend of Networking [C]// Applied Mechanics and Materials. 2014: 685-688.

[15] DUAN Q, ANSARI N, TOY M. Software-Defined Network Virtualization: An Architectural Framework for Integrating SDN and NFV for Service Provisioning in Future Networks [J]. IEEE Network, 2016, 30(5): 10-16.

[16] WOOD T, RAMAKRISHNAN K K, HWANG J, et al. Toward a Software-Based Network: Integrating Software Defined Networking and Network Function Virtualization [J]. IEEE Network, 2015, 29(3): 36-41.

[17] 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.
ZUO Q Y, CHEN M, ZHAO G S, et al. Research on Open Flow-Based SDN Technologies [J]. Journal of Software, 2013, 24(5): 1078-1097. (in Chinese)

[18] 王蒙蒙, 刘建伟, 陈杰, 等. 软件定义网络: 安全模型、机制及研究进展 [J]. 软件学报, 2016, 27(4): 969-992.
WANG M M, LIU J W, CHEN J, et al. Software Defined Networking: Security Model, Threat and Mechanism [J]. Journal of Software, 2016, 27(4): 969-992. (in Chinese)

[19] 王鹃, 王江, 焦虹阳, 等. 一种基于 OpenFlow 的 SDN 访问控制策略实时冲突检测与解决方法 [J]. 计算机学报, 2015, 38(4): 872-883.
WANG J, WANG J, JIAO H Y, et al. A Method of Open Flow-Based Real-Time Conflict Detection and Resolution for SDN Access Control Policies [J]. Chinese Journal of Computers, 2015, 38(4): 872-883. (in Chinese)

[20] OLIVEIRA R L S, SHINODA A A, SCHWEITZER C M, et al. Using Mininet for Emulation and Prototyping Software-Defined Networks [C]// IEEE Colombian Conference on Communications and Computing. IEEE, 2014: 1-6.

[21] MEDVED J, VARGA R, TKACIK A, et al. Opendaylight: Towards A Model-Driven Sdn Controller Architecture [C]// 2014 IEEE 15th International Symposium on A World of Wireless, Mobile and Multimedia Networks. Sydney: IEEE, 2014: 1-6.

[22] 房秉毅, 张歌, 张云勇, 等. 开源 SDN 控制器发展现状研究 [J]. 邮电设计技术, 2014(7): 29-36.
FANG B Y, ZHANG G, ZHANG Y Y, et al. Research on the development of open source SDN controller [J]. Designing Techniques of Posts and Telecommunications, 2014(7): 29-36. (in Chinese)

(编辑: 徐楠楠)