·安全技术· 文章编号：1000-3428(2018)08-0179-05 文献标志码：A 中图分类号：TP309

SDN 环境下的动态随机网络病毒传播模型及特性研究

刘 兰[1]，任光明[1]，林 军[2]

（1. 广东技术师范学院 电子与信息学院，广州 510655；2. 深圳赛宝工业技术研究院有限公司，广东 深圳 518071）

摘 要： 软件定义网络（SDN）提供了对网络的动态调控，但是安全性较差。为此，提出一种 SDN 下的动态随机网络模型。研究网络病毒随子网间节点迁移而扩散及爆发的过程，通过理论分析和数值模拟，发现网络病毒从源子网传播到目标子网的传播特性与子网间节点的迁移率相关。实验结果表明，该方法能有效找出病毒迁移阈值，并能实时发现病毒传播趋势。

关键词： 网络安全；软件定义网络；网络病毒；社团；随机网络；迁移率

中文引用格式： 刘 兰，任光明，林 军. SDN 环境下的动态随机网络病毒传播模型及特性研究[J]. 计算机工程，2018，44(8)：179-183.

英文引用格式： LIU Lan，REN Guangming，LIN Jun. Research on virus spreading model and characteristics of dynamic random network under SDN environment[J]. Computer Engineering，2018，44(8)：179-183.

Research on Virus Spreading Model and Characteristics of Dynamic Random Network Under SDN Environment

LIU Lan[1]，REN Guangming[1]，LIN Jun[2]

（1. School of Electronic and Information，Guangdong Polytechnic Normal University，Guangzhou 510655，China；
2. Shenzhen CEPREI Industry Technology Research Institute，Shenzhen，Guangdong 518071，China）

【Abstract】 The Software Defined Network（SDN）provides dynamic control of the network，but the security is poor. Therefore，a dynamic random network model of SDN is proposed to study the process of network virus spreading. Through theoretical analysis and numerical simulation，it is found that the propagation of network viruses from the source subnet to the target subnet is related to the mobility of the nodes between the subnetworks. Experimental results show that the method can effectively identify virus migration threshold and detect the trend of virus transmission in real time.

【Key words】 network security；Software Definition Network（SDN）；network virus；community；random network；mobility ratio

DOI： 10.19678/j.issn.1000-3428.0048127

0 概述

高速发展的互联网以及无处不在的互联互通使得网络空间安全成为一项关系到世界安全与稳定的国际性问题。网络互通有其优势，也同时为攻击者在全球网络的任意地点探测网络漏洞并发起攻击提供了方便之门。

软件定义网络（Software Defined Networking，SDN）[1]作为一种全新的网络架构，其安全性逐渐为网络空间安全领域发展热点和研究方向。SDN 采用全局视图，并通过控制器进行集中控制，这使大数据环境下的网络流量管理、入侵防御和隔离控制等变得容易，降低了管控难度。但 SDN 网络的集中架构也将给网络安全带来更大的风险[2]。随着 SDN 网络的安全应用的不断开发，信息安全领域中机遇与挑战并存[3-5]。一旦网络病毒在部分网络上传播，由于 SDN 的动态性和集中架构，可能对整个网络造成影响。为此，本文采用复杂网络的动力学模型描述异质性网络中的病毒传播过程，对 SDN 网络中的病毒路线进行溯源，进一步细化 SDN 管控机制，并使用随机模型作为初始模型。

1 研究背景

因为 SDN 网络控制与转发分离的思想，各类开

基金项目： 国家自然科学基金（61571141）；广东省教育厅特色创新类项目（2016KTSCX078）；广东省“质量工程”建设项目网络工程专业综合改革项目（2015133）。

作者简介： 刘 兰（1977—），女，副教授、博士，主研方向为信息安全、网络工程；任光明，副教授、博士；林 军（通信作者），高级工程师、硕士。

收稿日期： 2017-07-27 **修回日期：** 2017-09-15 **E-mail：** hust_ll@126.com

放的应用程序将带来的漏洞和由此产生的攻击不可避免[6-7],文献[8]对 SDN 网络的安全现状进行了分析,提出在 SDN 控制器上应建立异常检测平台,将收集的统计信息提供给异常检测模块使用。当发现异常时,应用程序将发出警报,采取相应措施并进行记录。文献[9]提出由 SDN 网络的控制器提供开发和部署安全应用的框架,管理员通过模块方式实现不同的异常检测。文献[10]分析云计算和 SDN 技术环境下的恶意代码攻击检测技术,提出相应的检测实验平台进行仿真处理。在各类安全事件中,网络病毒以其传播速度快、影响范围大和渗透力强等特点居于互联网安全问题的首位。目前 SDN 网络中第三方开发的应用软件均为不开源的,传统的基于源码的检测方式不再合适,这使得针对网络病毒的 SDN 网络攻击检测和防范成为了一个公开的问题。

网络病毒传播网络和其他社团网络一样是具有动态性的复杂网络,移动节点和移动介质在计算机网络中的广泛应用,使得网络病毒在不同子网之间得以传播。以前人们在网络病毒传播网络的研究中主要集中在静态复杂网络上,传统的防病毒、防火墙等技术都是静态安全防御技术,主要依赖于人工配置管理,对于大规模网络的管理和部署难度很大,当新的网络病毒出现时,很难掌握其规律,这给网络病毒检测造成了很大的困扰。

近年来,为了突破现有网络架构的制约,研究效率更高、效果更好的网络病毒防治技术,研究者们开始关注 SDN 的网络病毒检测方法。文献[11]在复杂网络中引入了一个有效的传染病传播理论模型,其研究工作为研究网络病毒在 SDN 网络中的传播特性提供了新的思路。文献[12]在改进的 SDN 架构上研究低通信开销的网络病毒检测方法。文献[13]提出一个无标度网络中恶意代码的传播模型,采取动态隔离疑似感染节点的方法来实现恶意代码的检测和防护。实验结果表明,可以通过调节系统感染结点可疑度的阈值,达到控制恶意代码传播的效果。文献[14]研究表明,网络拓扑对网络病毒传播速度是有影响的,越是处于网络中心的网络病毒传播速度越快,而且处于中心的网络节点重复感染的概率也较大。SDN 的控制器能够进行权限管理和应用隔离,从而实现网络逻辑控制。当新的网络病毒在某个子网爆发时,控制器可以根据网络状态改变流表策略,控制网络病毒传播到别的子网中去。本文分析 SDN 网络环境中网络病毒传播模型及动态随机网络中病毒传染的免疫策略,从而有效防御网络病毒传播。

2 数学模型

网络病毒的传播与生物疾病的传播具有相似性,可以采用相似模型来研究其传播特性[15]。这类模型有 2 个假设前提:1)网络内节点在任意的时刻 t 的状态是有限的,状态包括易感、潜伏、感染、恢复和隔离等,根据网络病毒的特性和建模目的不同,可以选择不同的状态集;2)感染类的节点会以一定概率感染网络中的其他节点,采用简单的概率关系来分析状态之间的转化。

这些数学模型一般以 SIR(Susceptible、Infected、Recovery)模型或者简化的 SIS(Susceptible、Infected、Susceptible)模型为基础的。SIR 模型采用 3 个状态,即易感 S(Susceptible)、感染 I(Infected)和恢复 R(Recovered),通过 3 个状态之间的转化及相互影响来分析网络中病毒的传播特性。其中,确定型模型比较适合描述易感节点数目很大情况,而随机型模型用来分析易感节点数目小的平均传播过程。因为计算机网络中节点因为自身的防护及各种安全措施,易感节点的数目不大,所以本文采用随机模型来研究 SDN 架构下节点的逻辑移动给网络病毒传播带来的趋势影响。

2.1 模型假设

在计算机网络中,不同的节点分属于不同的子网,子网的规模和网络病毒感染情况以及网络安全的防护措施存在着差异。在本文中以网络拓扑的逻辑子网作为社团划分依据,网络病毒在子网内部的传播速度比较快,而在不同的子网之间传播缓慢。为了简化模型,本文认为不同的子网之间网络病毒不能传播,也就是不同社团间的节点不存在感染路径。由于 SDN 网络对逻辑路由的灵活控制,当节点从一个子网转移到另外一个逻辑子网时,会将网络病毒扩散到目标子网。

为了简单明了并如实反映节点的转移对网络病毒传播的影响,本文建立模型前先做一些模型假设。

模型假设:

1)易感节点数 N 是一个常数,不随时间 t 的变化而变化,即没有新的易感节点进入或离开整个系统。

2)节点仅 2 个状态:易感 S 和感染 I,某一时刻 t 节点处于其中之一,不能再次感染已经感染的主机。初始感染主机数为 $I(0) = I_0$。

3)不同的子网之间网络病毒不能传播,也就是不同社团间的节点不存在感染路径。

数学模型中假设 t 时刻易感节点有 $k_{\inf}$ 个感染连边节点,每个易感节点被连边的感染节点感染的概率为 λ。$t+1$ 时刻易感节点被感染的概率为 $1-(1-\lambda)^{k_{\inf}}$。同时,因为网络中有的节点可以通过防火墙技术、打补丁、病毒查杀以及安装内容过滤器等方式使得感染节点从被感染状态 I 恢复成易感状态,本文假设某时刻节点的恢复率为 μ。

2.2 模型设立

在模型的假设基础上,可以构建一个动态随机

网络病毒传播模型。在此模型上,本文研究节点在子网间的转移对网络病毒传播的影响[11]。

1)N 个易感主机依概率 $n_i(i=1,2,\cdots,m)$ 分属于 m 个不同的子网:

$$\sum_{i=1}^{m} n_i = N \tag{1}$$

2)对于这 m 个子网,本文以 p_i 的概率在节点间加边来构造网络,使其满足式(2):

$$\sum_{i=1}^{m} p_i \cdot \frac{1}{2} n_i(n_i-1) = \frac{N \cdot \langle k \rangle}{2} \tag{2}$$

其中,$<k>$ 是整个随机网络的平均度。

3)当感染节点从一个子网迁移到另外一个逻辑子网时,会将网络病毒扩散到目标子网。本文假设每个节点 $j(j=1,2,\cdots,N)$ 以概率从一个子网迁移到另一个子网。在每一个时间步,删除社团之间的所有边,并以迁移率 q 表示社团节点之间的连边概率来描述动态传播过程。

设定一个病毒传播阈值 λ_c,当 $\lambda > \lambda_c$ 时,某类病毒会在网络中爆发。在随机网络病毒传播模型中,$\lambda_c = \mu/\langle k \rangle$。某个社团 i 子网内部的病毒传播阈值 λ_c^i 定义为:

$$\lambda_c^i = \frac{\mu}{\langle k_i \rangle} = \frac{\mu}{p_i(n_i-1)} \tag{3}$$

假设初始感染节点数为 $I(0)=1$,即开始时只有一个感染节点,此节点位于社团 i,那么当 $\lambda > \lambda_c^i$ 时,网络病毒将在社团子网 i 内部传播爆发,而不会影响到其他不同的社团子网。

因为 SDN 网络架构下实现网络节点(包括移动设备、各类网络设备和主机)的逻辑网络的重定向,所以社团子网间存在着节点的转移,即社团间节点的转移概率 $q>0$。当 $\lambda > \lambda_c^i(i=1,2,\cdots,m)$ 时,即使整个系统中初始感染节点为 1,经过足够的时间,网络病毒会在整个网络中传播开,而网络病毒的爆发时间与转移概率 q 相关。本文再讨论 $\lambda < \lambda_c^i(i=1,2,\cdots,n,n<m)$ 的情况,引入迁移率阈值 q_c,当转移概率 $q > q_c$ 时,网络病毒会在网络中传播开。

3　实验结果与分析

为了比较不同情况中网络病毒在动态随机网络中的传播特性,采用相同的实验环境,初始感染主机数 $I(0)=1$,网络节点数 $N=2\,000$,为了研究的简便性,设置 $m=2$, $n_1=800$, $n_2=1\,200$, $<k>=40$,连边数最大可以为 $n_1 \times n_2 = 960\,000$ 条,根据式(1)和式(2)得到 $p_1=0.020\,6$, $p_2=0.046\,4$。

3.1　$\lambda > \lambda_c^i(i=1,2)$ 的情况

假设某时刻节点的恢复率为 $\mu=0.1$,由式(3),计算可得 $\lambda_c^1=0.006\,1$ 和 $\lambda_c^2=0.001\,8$,取 $\lambda=0.04>\lambda_c^i(i=1,2)$。本文随机选取社团子网 1 中的某个节点为感染初始节点,社团子网 1 分别取转移概率 $q=0.000\,001 \sim 0.000\,01$ 向子网 2 进行迁移。图 1 表示在不同的转移概率下,社团子网内节点感染率 $\rho(t)$ 为时间 t 的曲线函数。

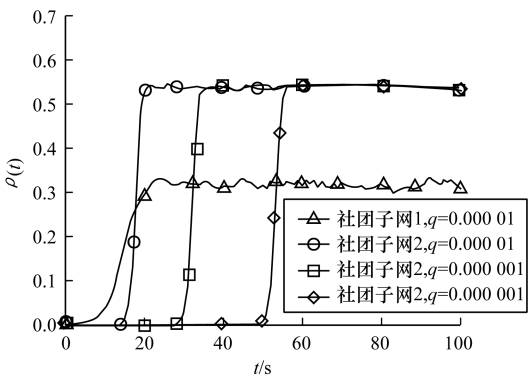

图 1　节点感染率 $\rho(t)$ 对 t 的函数

从图 1 可以看出,网络病毒首先在社团子网 1 中爆发,然后逐渐感染社团子网 2。转移概率越大,则子网 2 内病毒爆发的时间越短。因为子网 1 内病毒爆发的感染演化函数与迁移率关系不大,所以本文仅用 $q=0.000\,01$ 的曲线来表示各种不同的情况。图中的迁移率取值主要依据实验和经验值来获得。深入理解网络病毒传播的时间演化过程是寻找防止病毒爆发的管控策略的先决条件,因此,根据实验结论,由于 $\lambda > \lambda_c^2$,只有社团子网 1 中的某个感染节点依转移概率转移到社团子网 2,病毒才可能在子网 2 中传播。在每个时间步骤中,从社团子网 1 转移到社团子网 2 的感染节点的数目为 $n_1 q \rho_1(t)$,其中,$\rho_1(t)$ 表示在 t 时刻社团子网 1 内的感染率。q 表示社团间的迁移率,n_1 表示社团子网 1 中的节点数目。根据平均场理论,$\dot{\rho}_1(t)$ 满足 $\dot{\rho}_1(t) = -\mu\rho_1(t) + \lambda\langle k_1 \rangle \rho_1(t)(1-\rho_1(t))$。其中,$\rho_1(t)$ 表示网络中节点感染率,μ 表示感染节点的恢复概率,λ 表示易感节点跟一个感染节点相连时的感染概率。方程右边 $-\mu\rho_1(t)$ 表示感染节点减少量,$(1-\rho_1(t))$ 表示易感节点密度,$\langle k_1 \rangle$ 是一个易感点周围节点的数目,而 $\langle k_1 \rangle \rho_1(t)$ 是一个易感点周围感染节点的数目。根据乘法法则,$\lambda\langle k_1 \rangle \rho_1(t)(1-\rho_1(t))$ 是整个网络中感染点的增加数。当 $\dot{\rho}_1(t)>0$ 时,表示感染节点的增加,当 $\dot{\rho}_1(t)=0$ 时,表示感染节点数据增长率的临界值,由此可以化简为:

$$\rho_1(t) = \frac{a/b}{1+ce^{-at}} \tag{4}$$

其中,$a=\lambda\langle k_1 \rangle - \mu$, $b=\lambda\langle k_1 \rangle$,且:

$$c = \frac{a-\rho_1(0)b}{\rho_1(0)b} \tag{5}$$

其中,$\rho_1(0)$ 表示 $t=0$ 的时刻子网内网络病毒感染率,显然在这个简单模型中,$\rho_1(0)=1/n_1$。当在时间 t 时,社团子网 2 中节点感染的概率为 $n_1\rho_1(t)$ $n_2 q\lambda$,其中,$\rho_1(t)$ 表示第 t 步社团子网 1 中感染节点

数密度,q 是社团子网 1 中任意节点与社团子网 2 中节点的连边概率,λ 是整个系统中这类网络病毒的感染概率。假设社团子网 2 内的节点在时间 t_c 被感染的概率为 1,可以得到:

$$\int_0^{t_c} n_1\rho_1(t)n_2q\lambda\,\mathrm{d}t = 1 \tag{6}$$

由式(6)可得:

$$t_c = \frac{\ln(\mathrm{e}^{\ln(1+c)+b/(\lambda n_1 n_2 q)} - c)}{a} \tag{7}$$

因此,可以求得社团子网 2 的病毒爆发时间:

$$T_c = t_c + t_0 = \frac{\ln(\mathrm{e}^{\ln(1+c)+b/(\lambda n_1 n_2 q)} - c)}{a} + \frac{\ln c}{a} \tag{8}$$

其中,$t_0 = \ln c/a$ 表示社团子网 2 中感染节点数目从 1 增加到稳定值的中间时刻。

为了检验上述理论分析值,本文通过实验来模拟获得数据。T_c 为社团子网 2 中感染节点数目达到稳定值的一半的中间时刻。本文取不同的 λ 值 0.04 和 0.01,当转移概率 $q = 0.000\ 001 \sim 0.000\ 01$ 发生变化时,获得如图 2 所示的 2 条函数曲线。这 2 条曲线分别代表不同 λ 值 0.04 和 0.01 取值情况下,式(8)的 T_c 值。比较得知,数值模拟与理论结论是一致的。

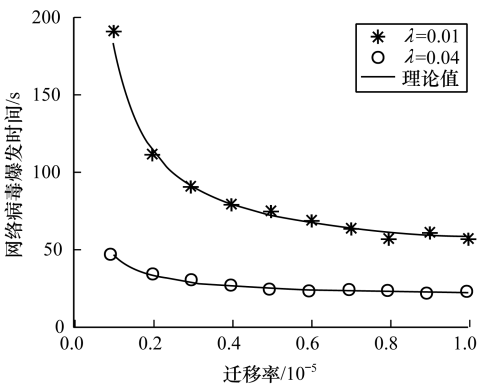

图 2 网络病毒爆发时间与迁移率的关系

3.2 $\lambda_c^2 < \lambda < \lambda_c^1$ 的情况

在 $\lambda_c^2 < \lambda < \lambda_c^1$ 情况下,如果社团子网间的节点迁移率太低,那么网络病毒在爆发前就会在社团子网 1 内部自动消亡了。而如果迁移率够高,那么网络病毒会转移到社团子网 2。本文采用图 1 类似参数,但取 $\lambda = 0.005$,其取值符合 $\lambda_c^2 < \lambda < \lambda_c^1$,在社团子网 1 内随机选取初始感染节点 $I(0) = 100$,计算可得 $\rho_1(0) = I(0)/n_1 = 0.125$,$\rho_2(0) = 0$,$\rho(0) = I(0)/N = 0.05$,其中,$\rho_1(0)$、$\rho_2(0)$、$\rho(0)$ 分别表示社团子网 1、社团子网 2 和整个社团中的病毒感染率。

图 3 为在不同的转移概率 $q = 0.000\ 1$ 和 $q = 0.000\ 01$ 的情况下,社团子网 1 和社团子网 2 内节点感染率 $\rho(t)$ 的演化函数曲线。星号点曲线表示社团子网 1,圆圈点曲线表示子网 2。由图 3(a)可以看出,当 $q = 0.000\ 1$ 时,大概在 t 为 60 时,网络病毒在社团子网 2 内爆发。由图 3(b)可以看出,当 $q = 0.000\ 01$ 时,社团子网 2 和社团子网 1 中病毒都不会爆发。

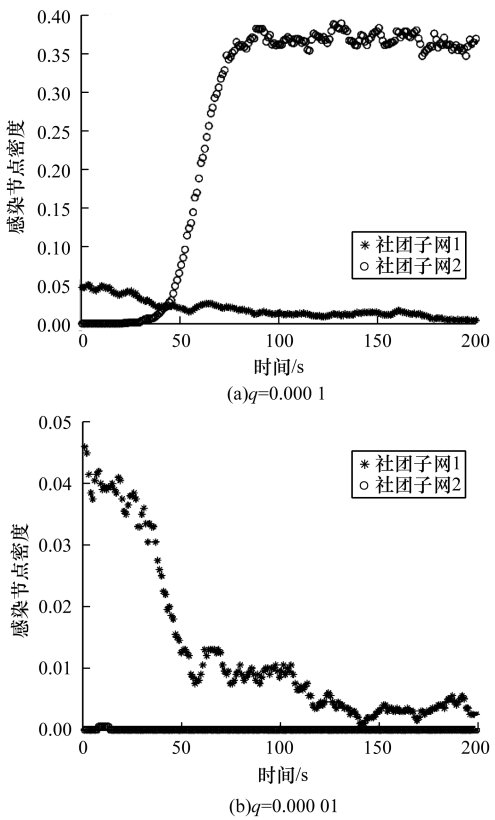

图 3 感染节点密度的演化曲线

由于 $\lambda < \lambda_c^1$,因此存在某个时间点 $t = t_1$ 使得社团子网 1 内的网络病毒最终死亡。那么只有在时间 $t = t_1$ 之前,有被感染的节点从社团子网 1 迁移到了社团子网 2,那么社团子网 2 内的网络病毒才有可能演化传播。根据式(4),当 $a < 0$ 时,$\rho_1(t_1)$ 会逐渐逼近于 0。本文取一个极小数,比如本例中 $\rho_1(t_1) = 0.000\ 1$,通过式(4)解得:

$$t_1 = \frac{\ln\left(\dfrac{10\ 000a - b}{bc}\right)}{-a} \tag{9}$$

又由式(7)和式(9),取 $t_1 = t$ 时 $q = q_c$,得:

$$q_c = \frac{b}{n_1 n_2\left(\ln\left(\dfrac{bc}{10\ 000a - b} + c\right) - \ln(1+c)\right)} \tag{10}$$

由式(5)获得 c 值。

在多组实验中,分别取 $I(0) = 50 \sim 100$,并取 $\lambda = 0.003 \sim 0.006$,然后从 0 开始逐渐加大迁移率 q 的取值。当迁移率增加到转移阈值 q_c 时,网络病毒在社团子网 2 中爆发。对每个组 $I(0)$ 和 λ 的取值,本文进行 100 次实验并取平均值。实验结果如图 4

所示,圆圈点和星号点分别代表 $I(0)=50$ 和 100 的实验结果,实线代表根据式(10)计算所得的理论值。实验结果表明,对于某个特定的 λ 值,迁移率阈值 q_c 与社团子网 1 中的初始感染数 $I(0)$ 成反比。而对于某个特定的 $I(0)$ 值,q_c 值随着感染率 λ 的增加而迅速减小。当 $I(0)=100$ 时,随着 λ 从 0.003 增加到 0.006,q_c 值迅速从 1.8×10^{-4} 减少到 7.8×10^{-5}。数值仿真实验证实了式(10)的理论值。

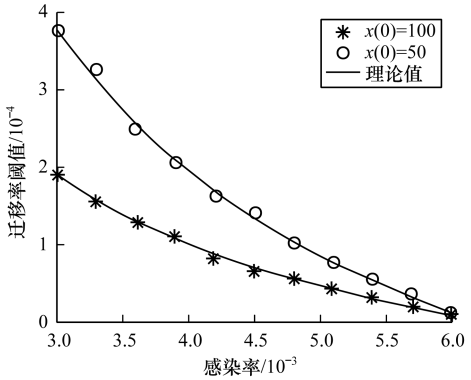

图 4　迁移率阈值与感染率的关系曲线

4　结束语

本文提出一种 SDN 环境下的动态随机网络模型,以网络拓扑的逻辑结构作为社团划分依据,采用随机模型研究网络病毒在节点迁移时的传播情况。实验结果表明,当社团间节点迁移率 q 大于迁移阈值 q_c 时,网络病毒会在社团子网间扩散和传播,这为 SDN 控制器管理策略的设置提供理论参考。由于实际的 SDN 网络环境更类似于无标度网络,后期研究将先从建立网络病毒在无标度网络模型中的模拟实验开始,分析不同标度网络节点的迁移率与网络病毒传播之间的数据关系,从而进一步研究其理论模型。

参考文献

[1] 张朝昆,崔　勇,唐胥祎,等. 软件定义网络(SDN)研究进展[J]. 软件学报,2015,26(1):62-81.

[2] 赵　涛,李　韬,孙志刚,等. REFINE:一种可重构的 SDN 转发平面实现模型[J]. 小型微型计算机系统,2015,36(10):2284-2288.

[3] AKHUNZADA A,AHMED E,GANI A,et al. Securing software defined networks:taxonomy,requirements,and open issues[J]. IEEE Communications Magazine,2015,53(4):36-44.

[4] 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.

[5] 郭春梅,张如辉,毕学尧. SDN 网络技术及其安全性研究[J]. 信息网络安全,2012(8):112-114.

[6] YOON C,PARK T,LEE S,et al. Enabling security functions with SDN[J]. Computer Networks,2015,85(C):19-35.

[7] 赵明宇,严学强. SDN 和 NFV 对未来移动通信网络的影响分析[J]. 电信网技术,2015(4):31-35.

[8] 左青云,张海粟. 基于 OpenFlow 的 SDN 网络安全分析与研究[J]. 信息网络安全,2015(2):26-32.

[9] SHIN S,PORRAS P,YEGNESWARAN V,et al. FRESCO:modular composable security services for software defined networks[EB/OL]. [2017-11-21]. https://www.mendeley.com/research-papers/fresco-modular-composable-security-services-softwaredefined-networks/.

[10] WANG Bing. DDoS attack protection in the era of cloud computing and software-defined networking[J]. Computer Networks the International Journal of Computer & Telecommunications Networking,2015,81(C):308-319.

[11] REN G,WANG X. Epidemic spreading in time-varying community networks[J]. Chaos:An Interdisciplinary Journal of Nonlinear Science,2014,24(2).

[12] LIN Y D,LIN P C,YEH C H,et al. An extended SDN architecture for network function virtualization with a case study on intrusion prevention[J]. IEEE Network,2015,29(3):48-53.

[13] HOSSEINI S,AZGOMI M A. A model for malware propagation in scale-free networks based on rumor spreading process[J]. Computer Networks the International Journal of Computer & Telecommunications Networking,2016,108(C):97-107.

[14] BRADLEY J T. Analyzing distributed Internet worm attacks using continuous state-space approximation of process algebra models[J]. Computer and System Sciences,2008,74(6):1013-1032.

[15] PELLIS L,BALL F,BANSAL S,et al. Eight challenges for network epidemic models[J]. Epidemics,2015,10(C):58-62.

编辑　刘　冰

(上接第 178 页)

[15] 王惠清,洪志全. 一种基于代数签名的远程数据完整性方案[J]. 计算机应用与软件,2016,33(2):302-306.

[16] HAO Z,ZHONG S,YU N. A privacy-preserving remote data integrity checking protocol with data dynamics and public verifiability[J]. IEEE Transactions on Knowledge and Data Engineering,2011,23(9):1432-1437.

[17] 李雪晓,叶　云,田苗苗,等. 基于格的大数据动态存储完整性验证方案[J]. 信息网络安全,2014,2(4):46-50.

编辑　吴云芳