基于云安全环境的蠕虫传播模型

张伟[1,2]，王汝传[1,2]，李鹏[1,2]

（1. 南京邮电学大学 计算机学院，江苏 南京 210003；2. 江苏省无线传感网高技术研究重点实验室，江苏 南京 210003）

摘 要：云安全体系的出现标志着病毒检测和防御的重心从用户端向网络和后台服务器群转变，针对云安全体系环境，基于经典 SIR 模型提出了一种新的病毒传播模型（SIR_C）。SIR_C 在考虑传统防御措施以及蠕虫造成的网络拥塞流量对自身传播遏制作用的基础上，重点分析了网络中云安全的部署程度和信息收集能力对蠕虫传播模型的影响。实验证明 SIR_C 模型是蠕虫传播研究在云安全环境下有意义的尝试。

关键词：蠕虫；云安全；传播模型；SIR

中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2012)04-0017-08

Worm propagation modeling in cloud security

ZHANG Wei[1,2], WANG Ru-chuan[1,2], LI Peng[1,2]

(1. College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China;

2. Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, Nanjing 210003, China)

Abstract: The emergence of cloud security changed the major virus-defensive position from client to network and server group. From the view of the cloud security, a novel worm propagation model, SIR_C (SIR in cloud security), which drives from SIR model was proposed. Based on considering the traditional human countermeasures and the network congestion traffic which is caused by worms and will curb the spread of worms, SIR_C model focused on the analysis of the impact of the degree of cloud security deployment and the information gathering capability on worm propagation model. The simulation results show that SIR_C model was a meaningful attempt to research worm epidemics in cloud security network.

Key words: worm; cloud security; propagation model; SIR

1 引言

现代意义上的恶意代码集合了扫描器、蠕虫、木马、Rootkit 等多种技术，蠕虫的传播手段被各类恶意代码用来实现其发布功能，蠕虫传播模型的研究可以帮助认识恶意代码的传播过程、造成的结果

收稿时间：2010-06-17；**修回日期**：2011-04-20

基金项目：国家自然科学基金资助项目（60973139, 60773041, 61003236）；江苏省科技支撑计划（工业）基金资助项目（BE2010197, BE2010198）；江苏省级现代服务业发展专项基金资助项目；高校科研成果产业化推进工程基金资助项目（JH10-14）；国家和江苏省博士后基金资助项目（20090451241）；江苏高校科技创新计划基金资助项目（CX10B-196Z）；江苏省六大高峰人才基金资助项目（2008118）；教育部高等学校博士学科点专项科研基金资助项目（20103223120007）

Foundation Items: The National Natural Science Foundation of China(60973139,60773041,61003236); Scientific & Technological Support Project (Industry) of Jiangsu Province (BE2010197, BE2010198); The Special Foundation for Development of Modern Service Industry of Jiangsu Province; Scientific Research & Industry Promotion Project for Higher Education Institutions(JH10-14) Postdoctoral Foundation (20090451241); Science & Technology Innovation Fund for higher education institutions of Jiangsu Province(CX10B-196Z); The Six Kinds of Top Talent of Jiangsu Province(2008118); Doctoral Fund of Ministry of Education of China(20103223120007)

以及各类因素在传播过程中的作用。蠕虫传播与生物传染病流行具有很多相似性，传统的传染病模型 SI[1]、SIR[2]、SEIR[3,4]被大量引入到蠕虫传播模型的研究中，另一方面蠕虫病毒具有很多不同于生物病毒的特性，如蠕虫的繁殖方式、使用者的安全观念和使用方式、网络的拓扑结构和网络通信状况等[5~9]。ZOU C C[5]等提出的双因素模型，考虑个体的主动免疫以及大量感染个体发送超出网络正常流量负荷的数据阻塞网络，限制了蠕虫的传播速度，解释了在红色代码蠕虫后期感染主机数量反而下降的现象。Dagon David[10]等考虑了网络的时区特性，把全世界时区按照计算机的聚集情况分成了亚洲、北美和欧洲 3 个主要区域，解释了蠕虫的感染效果具有显著的昼夜波动特性，统计得到的感染曲线呈现明显的波浪型下降。LI T[11]等对 SIR 传播模型进行了改进，加入了动态加入/退出和时滞概念。YAO Y[12]等提出的模型中结合隔离检疫策略，对模型的周期解和稳定性进行了分析。蠕虫的性质和网络特性也影响着蠕虫的传播方式，文献[13,14]分别分析了被动蠕虫病毒以及蠕虫在 P2P 网络中传播情况。传统的传播模型把网络看成是同构的，感染节点以均等的概率感染其他易感节点，文献[7,15]研究了在异构拓扑结构下的传播模型，如随机网络、网格和树形层次网络。

在蠕虫传播模型中，各类防御措施是其中的重要因素，经典的SIR模型中的第3种状态R(removed)就是对S(susceptible)和I(infective)状态的个体实现主动免疫的结果，传统的这类行为依赖于个体对病毒的检测和补丁安装，但是这种方式面临着病毒特征库不断更新、规模过大而客户端难以维系的问题，另外这种方式在面对 0 day 病毒处于极为不利的地位。为解决这种现状，各大厂商开始陆续推出云概念安全产品[16]。参加云计划的客户端收集可疑信息发送给数据处理中心，中心经过自动处理或人工分析识别出各类新威胁，并及时反馈到部署在网络中的服务器群组成的云端，这样不安全的链接或者恶意数据在云中直接被扼杀，从而阻止其进入用户端。在网络中而不是在客户端进行病毒的查杀，这种思想在 DDoS 防御上已经有体现，如在核心路由器设备上对 DDoS 造成的恶意流量进行过滤[17,18]和反向跟踪[19]，但检测恶意代码显然比检测具有一定流量规模和相关性特征的 DDoS 数据流要复杂很多。

本文研究云安全环境下的蠕虫传播模型，除了考虑蠕虫在云安全网络中的感染率受到个体主动免疫行为影响以及蠕虫在感染后期造成的网络拥塞带来的传播限制，重点分析其受到云环境对恶意行为检测和干预效果。云安全的病毒干预效果直接和参与可疑信息上报的用户规模相关，同时也和病毒当时的规模相关，病毒感染的个体越多，参与云安全的个体越多，就有越多的可疑信息上报，导致对特定病毒识别的准确性更高，过滤效果更好。云安全是对传统病毒防御方式的全新改变，也许某一天客户端不再需要安装杀毒软件，但是也应该看到云安全是在传统病毒防御方式遇到发展瓶颈时而不得不寻找新途径的选择，并且存在着网络依赖性问题，海量数据智能处理等相关技术没有达到理想的程度。因此研究在新的云安全环境中，云安全部署程度等因素的影响以及云安全在病毒控制上的效果正是本文关心的问题。

本文组织如下：第 2 节给出了云安全网络中的蠕虫传播模型 SIR_C；第 3 节对 SIR_C 模型进行了理论分析；第 4 节进行了仿真实验；最后总结全文。

2 SIR_C 模型

目前，蠕虫传播模型主要分为确定性模型和随机模型 2 大类，确定性模型使用平均场方法简化问题并用微分方程描述病毒传播的平均趋势，不考虑概率事件，此类模型无法表述传播过程中的概率事件，例如病毒消亡或突发事件，此外确定性模型忽视了个体之间的交互行为。本文研究的 SIR_C 模型选择 Kermack-Mckendrick 的 SIR 模型作为基本模型，在复杂网络背景下分析蠕虫病毒在大量主机上传播时表现出来的特征，由于基于大数量个体主机，可以使用平均场方法并用微分方程描述病毒传播的平均趋势，不需要考虑单个主机特殊事件的概率，SIR_C 模型属于确定性模型。SIR_C 有 3 个状态，分别为易感状态 S、感染状态 I 和移去状态 R，新增加的个体不继承母体的免疫因素和疾病，处于易感状态。SIR_C 模型中具体的个体不论其处于 3 种状态中的哪一种，其还存在另外一种附加属性，即其是否参加了云安全计划的成员，决定其是否会主动上报可疑信息。定义 $X1, X \in \{S, I, R\}$ 为没有参

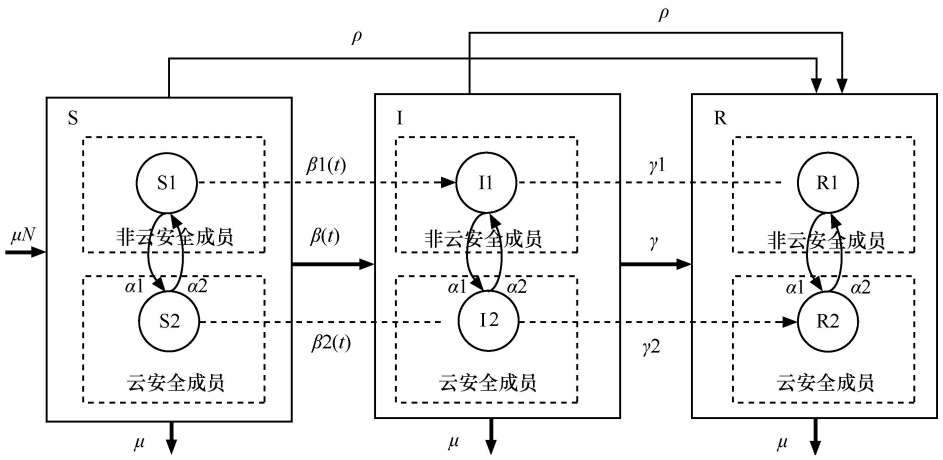


图 1　SIR_C 模型状态迁移

加云安全的个体，$X2, X \in \{S, I, R\}$ 为参加了云安全的个体。两者之间的区别只是是否主动上报可疑信息，在使用特征库防御病毒能力上没有差异，加入云计划完全是个体选择行为，图 1 是 SIR_C 模型的状态转换，基于如下假设。

1) 由于蠕虫涉及个体数目庞大，波动很小，系统个体总数 N 是不随时间变化的常数。

2) 模型主要考虑基于漏洞探测的主动传播型蠕虫，模型不考虑蠕虫的感染时间和潜伏期。

3) 蠕虫可以感染易感个体，使其状态变为感染个体，不区分个体对蠕虫的不同防御能力。

4) 云安全系统的样本收集来源主要来自成员个体的主动上报，而非蜜罐等系统的收集。

图 1 中 SIR_C 模型使用的参数描述如表 1 所示，其中，S、I、R 这 3 个状态中均被划分成了 2 个部分，分别表示参加了云安全计划和没有参加云安全计划的个体，由于加入云安全计划完全是用户行为，个体 S、I、R 这 3 个状态之间的变迁是由于蠕虫感染和主动免疫等动作导致的，并不会影响云安全成员状态的改变。从图 1 看出，云安全成员的状态的改变主要有 2 个来源：初始化状态设置和用户的动态修改，$\alpha 1$ 为云安全的加入率，$\alpha 2$ 为云安全的退出率。一次传播过程中的$\alpha 1$、$\alpha 2$ 相对于初始设置很小，可以忽略不计，所以 SIR_C 模型认为在整个蠕虫传播过程中云安全成员比例是一个固定的值 $k(0 \leqslant k \leqslant 1)$。既然云安全成员状态只是用于区别个体是否主动上报可疑信息，那么可得 SIR_C 模型中的云安全成员和非成员个体的接触率和移去率均相同，$\beta(t) = \beta 1 = \beta 2$，$\gamma = \gamma 1 = \gamma 2$。

表 1　　SIR_C 模型参数

符号	描述
S	易感个体 S= $S1$ + $S2$
$S1$	未参加云安全的易感个体
$S2$	参加了云安全的易感个体
I	感染个体 I= $I1$ + $I2$
$I1$	未参加云安全的感染个体
$I2$	参加云安全的感染个体
R	移去个体 R= $R1$ + $R2$
$R1$	未参加云安全的移去个体
$R2$	参加云安全的移去个体
N	全部个体总数 N= S + I + R
$\alpha 1$	云安全的加入率
$\alpha 2$	云安全的退出率
β	蠕虫接触率
γ	感染个体的移去率
ρ	易感个体和感染个体的主动免疫移去率
μ	个体的出生率和死亡率

易感主机的瞬间变化由出生率、死亡率、主动免疫移去率和蠕虫导致的感染率共同决定，假设出生率与系统个体总数目成正比，并且所有新增个体均为易感个体，死亡率和主动免疫移去率与易感个体成正比，可得式(1)。

$$S(t+\Delta t) - S(t) = \mu N - \beta(t)S(t)I(t) - \rho S(t) - \mu S(t) \quad (1)$$

式(1)中最复杂子项的就是蠕虫造成的感染发生率 $\beta(t)S(t)I(t)$，设云安全中的接触率为 $\beta(t)$，即单位时间内蠕虫导致的易感个体接触其他个体的数目。如果假设感染的个体接触率正比于个体总数，那么发生率为双线性模型 βSI，如果假设感染

的个体接触率是固定数值，那么发生率为标准模型 $\frac{\beta SI}{N}$，饱和模型介于两者之间 $\beta\times\frac{\alpha N}{1+\varpi N}\times\frac{SI}{N}$。但是这些模型均是假设接触率 β 为一个常数，在实际情况下这并不合理，蠕虫的感染效果受到网络情况和各类防御措施的影响，并且这种影响也会随着时间变化，在蠕虫的不同阶段体现出不同的影响。在云安全环境中，服务器群收集大量的可疑信息和网络流量来实时监控网络，蠕虫对易感个体的探测和具有特征信息的感染注入数据均可能被安全云检测出来，并在云中直接被过滤，从而降低蠕虫的感染效果。可以看到云安全的这种能力主要依赖于云安全成员的比例和蠕虫的规模这 2 个主要因素。越多的成员上报越多的蠕虫信息，那么就可能更快更准确地分析得出蠕虫特征加以遏制，SIR_C 模型定义的接触率见式(2)。

$$\beta(t)=\beta_0\theta_1(t)\theta_2(t) \tag{2}$$

$$\theta_1(t)=\left(1-\frac{I(t)}{N}\right)^{\eta 1} \tag{3}$$

$$\begin{cases}\theta_2(t)=\left(1-k^{\eta 2}\left(\dfrac{I(\mathrm{t})}{N}\right)^{\eta 3}\right), & t<t_{\max},\quad I(t)<I(t_{\max})\\ \theta_2(t)=\left(1-k^{\eta 2}\left(\dfrac{I_{\max}}{N}\right)^{\eta 3}\right), & t\geqslant t_{\max},\quad I(t)\geqslant I(t_{\max})\\ k=\dfrac{S2+I2+R2}{N}\end{cases} \tag{4}$$

式(2)中 β_0 为固定的基本接触率值，$\theta_1(t)$ 表示蠕虫自身传播导致对接触率的影响，$\theta_2(t)$ 表示云安全环境对接触率的影响。在蠕虫传播过程后期，感染状态个体剧增并产生大量数据，导致网络拥塞，反而制约了蠕虫的传播，本文采取文献[5]的策略，如式(3)。对第 2 个因素 $\theta_2(t)$，云安全的检测能力依赖于收集到的可疑信息的规模，因此，感染状态个体的增加在促进云安全能力上有正面作用，云成员比例 k 的增加也有同样的效果，支持更多信息的收集，增强云安全的杀毒能力，也会造成蠕虫发生率的下降。η 用来描述发生率对 3 种因素的敏感程度。式(4)表示云安全的影响分为 2 个阶段来分析，首先在感染个体数目达到顶峰前 $I(t)<I(t_{\max})$，即 $t<t_{\max}$ 阶段，随着 I 个体的增加，云安全可以收集更多的信息，更利于遏制蠕虫的传播，因此 $\theta_2(t)$ 下降；在蠕虫传播后期，感染个体的数量处于下降状态，但是 $\theta_2(t)$ 并不会转向上升，这是由于云安全在识别出该蠕虫后，会将防御能力处于最佳状态并一直保持，因此 $\theta_2(t)$ 也达到最佳值。综上，云安全中的蠕虫接触率为式(5)。

$$\beta(t)=\beta_0\left(1-\frac{\mathrm{I}(t)}{N}\right)^{\eta 1}\left(1-k^{\eta 2}\frac{\{\mathrm{I}(t),\mathrm{I}(t_{\max})\}}{N}^{\eta 3}\right),\quad k=\frac{S2+I2+R2}{N} \tag{5}$$

同理可以得出感染个体和移去个体的瞬时变化情况，SIR_C 模型的微分方程组如下：

$$\begin{cases}\dfrac{\mathrm{d}S(t)}{\mathrm{d}t}=\mu N-\beta(t)S(t)I(t)-\rho S(t)-\mu S(t)\\ \dfrac{\mathrm{d}I(t)}{\mathrm{d}t}=\beta(t)S(t)I(t)-\gamma I(t)-\rho I(t)-\mu I(t)\\ \dfrac{\mathrm{d}R(t)}{\mathrm{d}t}=\rho S(t)+\gamma I(t)+\rho I(t)-\mu R(t)\\ N=S(t)+I(t)+R(t)\end{cases} \tag{6}$$

严格意义上，蠕虫的传播是离散事件，但是本文将它作为连续过程看待，使用连续的微分方程组(6)来描述，这是因为蠕虫传播是涉及个体数目巨大的大规模事件，并且具体每个个体感染过程相互独立，这类方法在文献[20]也被使用，被证明是可行的和近似准确的。由于方程组(6)难以直接求出解，下面对 SIR_C 模型解的情况进行分析。

3 平衡点的稳定性分析

根据 SIR_C 模型的微分方程组(6)分析该模型的平衡点，并研究模型的稳定性。如果 SIR_C 模型是稳定的，则必须满足以下微分方程组：

$$\frac{\mathrm{d}S(t)}{\mathrm{d}t}=0,\frac{\mathrm{d}I(t)}{\mathrm{d}t}=0,\frac{\mathrm{d}R(t)}{\mathrm{d}t}=0 \tag{7}$$

令 $\frac{\mathrm{d}I(t)}{\mathrm{d}t}=0$，得到 $I(t)=0$ 或 $I(t)>0,S(t)=\frac{\gamma+\mu+\rho}{\beta(t)}$。

当 $I(t)=0$ 时，得到无病平衡点：

$$E_{q1}=(S_1^*,I_1^*,R_1^*)=\left(\frac{\mu N}{\mu+\rho},0,\frac{\rho N}{\mu+\rho}\right) \tag{8}$$

当 $I(t)>0,S(t)=\frac{\gamma+\mu+\rho}{\beta(t)}$ 时，得到地方性疾病平衡点：

$$E_{q2}=(S_2^*,I_2^*,R_2^*)$$
$$=\left(\frac{\mu+\rho+\gamma}{\beta(t)},\frac{\mu N}{\mu+\rho+\gamma}-\frac{\mu+\rho}{\beta(t)},\frac{(\rho+\gamma)N}{\mu+\rho+\gamma}-\frac{\gamma}{\beta(t)}\right) \tag{9}$$

3.1　无病平衡点及其稳定性

通过分析 SIR_C 模型在无病平衡点处的稳定性分析病毒传播的特性。根据微分方程组(6)，得到在无病稳定点处的 Jacobian 矩阵：

$$\boldsymbol{J}(E_{Q_1})=\begin{bmatrix}-\rho-\mu & -\beta(t)S_1^*(t) & 0\\ 0 & \beta(t)S_1^*(t)-\gamma-\rho-\mu & 0\\ \rho & \gamma+\rho & -\mu\end{bmatrix} \tag{10}$$

根据式（10），得到 $J(E_{q1})$ 的特征值

$$\begin{cases}\lambda_1=-\rho-\mu\\ \lambda_2=\beta(t)S_1^*(t)-\gamma-\rho-\mu\\ \lambda_3=-\mu\end{cases} \tag{11}$$

SIR_C 模型中所有的参数都假设为正值，有 $\lambda_1<0,\lambda_3<0$。若 SIR_C 模型在无病平衡点处是局部渐进稳定的，则要求 $\lambda_2<0$，即

$$\beta S_1^*-\gamma-\rho-\mu<0 \tag{12}$$

设基本再生数 R_0 为

$$R_0=\frac{\beta\mu N}{(\rho+\mu)(\gamma+\rho+\mu)}\ S_1^*=\frac{\mu N}{\mu+\rho} \tag{13}$$

根据以上在无病平衡点处的稳定性，可以得到以下引理。

引理 1　如果 $R_0<1$，SIR_C 模型在无病平衡点 E_{q1} 处是局部渐进稳定的；如果 $R_0>1$，SIR_C 模型在无病平衡点 E_{q1} 处是不稳定的。

证明　由稳定性定理知，微分方程组(6)渐进稳定的充分条件是其 Jacobian 矩阵的特征值 $\lambda_i<0,\ i=0,1,2$。由式(11)可知，在SIR_C模型中 $\lambda_1<0,\lambda_3<0$，如果令 $\lambda_2<0$，由已经计算出 $\lambda_2=(\gamma+\rho+\mu)\cdot\left[\frac{\beta\mu N}{(\rho+\mu)(\gamma+\rho+\mu)}-1\right]=(\gamma+\rho+\mu)(R_0-1)<0$ 得到 $R_0<1$，满足引理中的充分条件。证毕

定理 1　如果 $R_0\leqslant 1$，SIR_C 模型在无病平衡点 E_{q1} 处是全局渐进稳定的。

证明　由 SIR_C 模型的微分方程组(6)中的第一个微分方程得到

$$S'(t)\leqslant \mu N-\rho S(t)-\mu S(t)$$

解出

$$S(t)\leqslant\frac{\mu N}{\rho+\mu}+\left[S(0)-\frac{\mu N}{\rho+\mu}\right]\exp\left[-(\rho+\mu)t\right]$$

当 $t\to\infty$ 时，$S(t)\leqslant\frac{\mu N}{\rho+\mu}$

构造 Lyapunov 函数 $V(t)=I(t)$

$$V(t)'=I(t)'=\beta(t)S(t)I(t)-\gamma I(t)-\rho I(t)-\mu I(t)$$
$$=I(t)(\frac{\beta\mu N}{\rho+\mu}-r-\rho-\mu)<0$$

所以，得到无病平衡点 E_{q1} 是全局稳定的。　证毕

3.2　地方性疾病稳定点及其稳定性

根据微分方程组(6)，得到在地方性稳定点处的 Jacobian 矩阵：

$$\boldsymbol{J}(E_{Q_2})=\begin{bmatrix}-\beta(t)I_2^*(t)-\rho-\mu & -\beta(t)S_2^*(t) & 0\\ \beta(t)I_2^*(t) & \beta S_2^*-\gamma-\rho-\mu & 0\\ \rho & \gamma+\rho & -\mu\end{bmatrix}$$
$$=\begin{bmatrix}\frac{-\beta(t)\mu N}{\rho+\mu+\gamma} & -\rho-\mu-\gamma & 0\\ \frac{\beta(t)\mu N}{\rho+\mu+\gamma}-\rho-\mu & 0 & 0\\ \rho & \rho+\gamma & -\mu\end{bmatrix} \tag{14}$$

矩阵 $\boldsymbol{J}(E_{q2})$ 的特征值满足：

$$f(\lambda)=a_0\lambda^3+a_1\lambda^2+\ a_2\lambda+a_3$$

其中，

$$\begin{cases}a_0=1\\ a_1=\dfrac{\beta\mu N}{\rho+\mu+\gamma}+\mu\\ a_2=\dfrac{\beta\mu^2 N}{\rho+\mu+\gamma}-(\rho+\mu)(\rho+\mu+\gamma)+\beta\mu N\\ a_3=\mu\left[\beta\mu N-(\rho+\mu)(\rho+\mu+\gamma)\right]\end{cases}$$

引理 2　如果 $R_0>1$，则地方性稳定点 E_{q2} 是局部渐进稳定的。

证明　地方性稳定点 E_{q2} 的Routh-Hurwitz矩阵

$$\begin{bmatrix}a_0 & a_2\\ a_1 & a_3\\ (a_1a_2-a_0a_3)/a_0 & 0\\ a_3 & 0\end{bmatrix}$$

如果 $(a_1a_2-a_0a_3)/a_0$ 与 a_1 有相同的符号，则 3

个特征值具有负实部，则 Routh-Hurwitz 稳定性条件就满足。

因为 $R_0=\dfrac{\beta\mu N}{(\rho+\mu)(\gamma+\rho+\mu)}>1$, 则 $a_0>0, a_1>0, a_2>0, a_3>0$ 。

$$(a_1a_2-a_0a_3)/a_0=a_1a_2-a_0a_3$$

$$=\frac{\beta\mu N}{\gamma+\rho+\mu}a_2+\frac{\beta\mu^3N}{\gamma+\rho+\mu}>0$$

所以，地方性稳定点 E_{q2} 是局部渐进稳定的。

证毕

定理 2 如果 $R_0>1$, 地方性稳定点 E_{q2} 是全局渐进稳定的。

证明 构造 Lyapunov 函数 $V(t)$

$$V(t)=\int_{S_2^*}^{S}\frac{x-S_2^*}{x}dx+\int_{I_2^*}^{I}\frac{x-I_2^*}{x}dx$$

$$V'(t)=\left(\frac{S-S_2^*}{S}\right)S'+\left(\frac{I-I_2^*}{I}\right)I'$$

$$=\left(\frac{\mu N}{S}+\rho+\mu\right)(S_2^*-S)+$$

$$(\gamma+\mu+\rho)(I_2^*-I)-\beta SI_2^*\leqslant 0$$

所以，证明了地方性稳定点 E_{q2} 是全局渐进稳定的。

证毕

4 仿真实验

仿真实验使用 3 种不同的模型进行对比检测，SIR 模型、双因素模型和 SIR_C 模型，分别表示在 SIR 三仓室模型中不考虑网络流量加因素、考虑蠕虫导致的网络流量拥塞因素和云安全对网络蠕虫云过滤因素。3 组实验分别对蠕虫接触率、3 种状态个体数目比例变化和 SIR_C 模型的敏感系数进行检测，实验平台使用美国西北大学开发的 Netlogo 平台[21]，模拟 ER 随机网络和 BA 无标度网络这 2 种网络拓扑环境。

第 1 组接触率实验设置网络节点总数为 30 000，基本接触率β0 为 0.006，免疫移去率γ为 0.000 4，感染个体初始设置数值 10。根据式(5)设置网络拥塞敏感系数η1 为 3，云安全的敏感系数η2 和η3 均设置为 1，k 设置为 0.3，代表 30%的成员为云安全系统成员。图 2 和图 3 是在 ER 随机网络中的蠕虫接触率曲线，3 条曲线分别代表网络拥塞和云安全对蠕虫接触率的影响因子以及两者乘积形成的最终蠕虫接触率，图 2 和图 3 的区别是后者的云安全影响因子使用了分段函数，保证其是单调下降函数，即云安全对蠕虫的识别能力随着感染个体达到最高峰值时也达到其最佳状态，随着感染个体数目的继续下降，云安全影响因子并不下降而是保持在这个最优数值，这与双因素模型中基于网络拥塞的影响因子是不同的。在 SIR_C 模型中虽然也使用了和双因素模型中类似的网络拥塞影响因子，但是两者的实际运行值是不同的，双因素模型中该因子直接和感染个体的数目相关，但在 SIR_C 中，拥塞因子和云安全因子是会通过影响接触率而相互影响，可以通过图 4 和图 5 中的对应曲线对比看出，在 SIR_C 模型中，网络拥塞因子最小值达到了比双因素模型

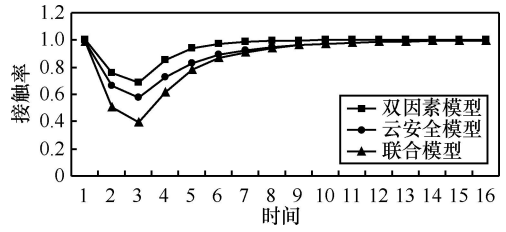


图 2 ER 随机网络中蠕虫接触率（不分段）

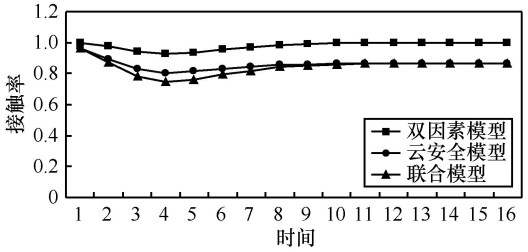


图 3 ER 随机网络中蠕虫接触（分段）

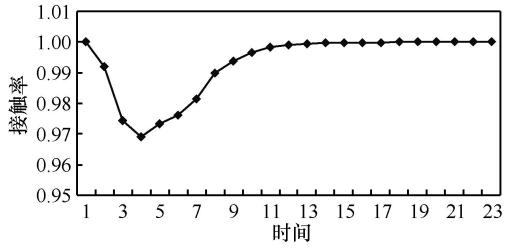


图 4 BA 无标度网络中蠕虫接触率（双因素）

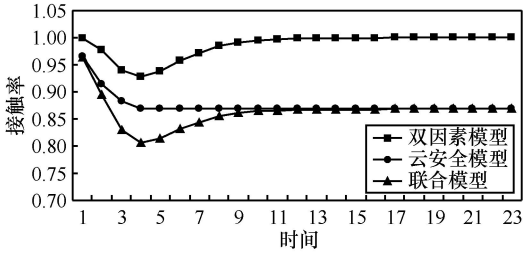


图 5 BA 无标度网络中蠕虫接触率（SIR_C）

中的更低的数值，并在最终状态双因素模型回复到初始状态，即对于同一类型蠕虫的再次爆发没有积累知识，而 SIR_C 却可以对同一类型蠕虫保持最佳遏制状态。

第 2 组实验的图 6~图 8 是在 ER 随机网络中的 3 种状态数目变迁，3 种模型得出的结果基本相似。图 9~图 11 是在无标度网络中的测试结果，无标度拓扑结构比较随机网络，蠕虫高峰的强度降低，到达时刻推迟，SIR_C 在无标度网络的指标介于 SIR 和双因素模型之间，并不是最佳，但这正是说明了 SIR_C 的优点。由于云安全的早期介入，降低了蠕虫的接触率，缓解了蠕虫自我的拥塞，可能导致感染过程缓慢，感染个体比例的峰值较高，但是在同样的一次蠕虫爆发周期后，SIR_C 在一次传播周期后可以保证更多的个体进入稳定的 R 状态。在面对精心构造的脉冲型传播蠕虫，SIR_C 模型充分利用首次冲击过程来保证生成更多免疫态的个体，在面对再次出现的同一类型蠕虫云安全会发挥积累的防御知识，这是另外 2 种模型所不具备的。

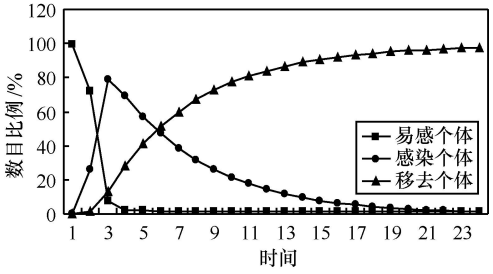


图 6　ER 随机网络中 SIR 模型结果

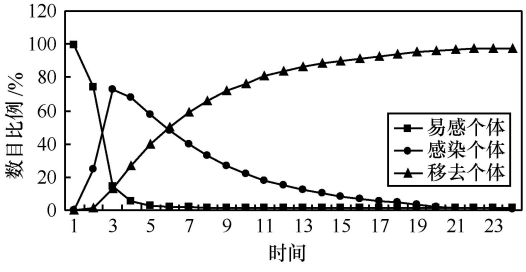


图 7　ER 随机网络中双因素模型结果

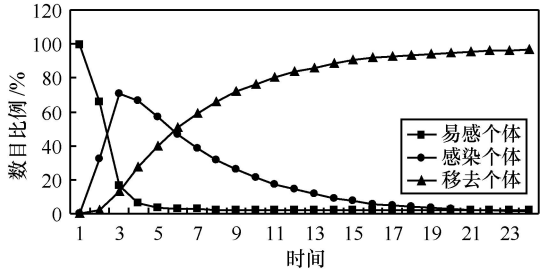


图 8　ER 随机网络中 SIR_C 模型结果

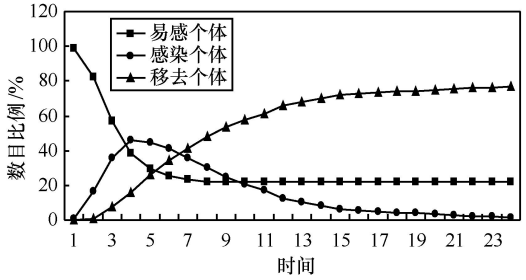


图 9　BA 无标度网络中 SIR 模型结果

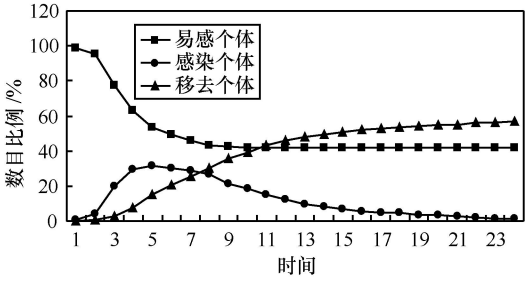


图 10　BA 无标度网络中双因素模型结果

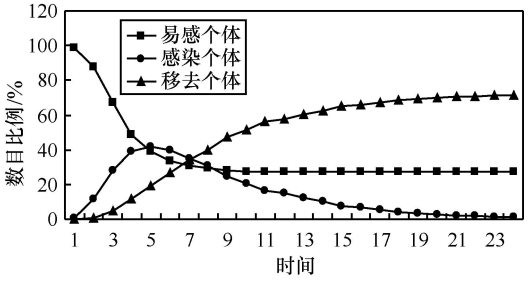


图 11　BA 无标度网络中 SIR_C 模型结果

第 3 组实验测试 SIR_C 模型参数的影响，设置网络拥塞因子系数η1 为 3，对云安全的成员比例 k 分别设置 0.1、0.5、1.0，敏感指数η3 设置为 1、2、4，观察其调整给蠕虫接触率带来的影响。从图 12 看出，云安全系统中参与成员比例 k 值越高，对提高整体网络的蠕虫防御能力提高帮助越大，但是最高也就在 65% 左右，因此一般网络中的云安全计划参与者超过 50% 就可以使接触率下降到 80%。图 13 说明，云安全的防御能力和网络中的流量并不是十分的敏感，一般不需要像双因素模型那样取η1 为 3，η3 一般可以取 1。

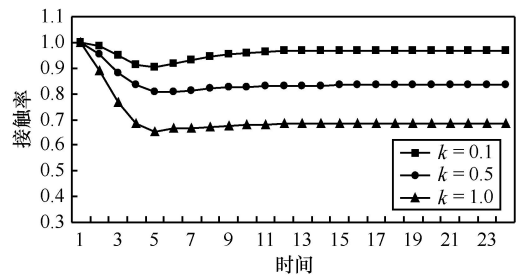


图 12　k 值调整 SIR_C 模型接触率变化

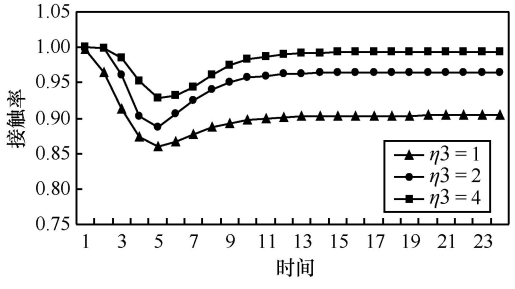


图 13 $\eta 3$ 值调整 SIR_C 模型接触率变化

5 结束语

云安全是一种全新的安全防御设计，不同于以往的个体免疫，是一种整体网络环境的免疫，但是这种新的架构如何影响蠕虫的传播行为，是否能够有效地遏制蠕虫的大规模爆发，目前在国内外文献未见相关报告。SIR_C 模型首次就云安全下的蠕虫传播所需要考虑的问题进行了分析和讨论，从云安全参与者比例和蠕虫信息收集能力的角度，结合蠕虫传播后期造成的网络拥塞现象，提出了 SIR_C 模型。云安全体系还存在很多不确定因素，如云安全的负面作用如何，如何防止病毒伪造上报可疑信息，云安全使用的实际效果如何等，这将是下一阶段的研究内容。

参考文献：

[1] PASTOR-SATORRAS R, VESPIGNANI A. Epidemic spreading in scale-free networks[J]. Phys Rev Lett, 2001, 86(14):3200-3203.

[2] HETHCOTE H W. The mathematics of infectious diseases[J]. SIAM Review, 2000, 42(4): 599-653.

[3] MISHRA B K, SAINI D K. SEIRS epidemic model with delay for transmission of malicious objects in computer network[J]. Applied Mathematics and Computation, 2007,188 (2): 1476-1482.

[4] EARN D J D, BRYAN P R, GRENFELL T. A simple model for complex dynamical transitions in epidemics[J]. Science, 2000, 287(5453): 667-670.

[5] ZOU C C, GONG W, TOWSLEY D. Code red worm propagation modeling and analysis[A]. Proc of the 9th ACM Conference on Computer and Communications Security[C]. New York, NY, USA, ACM Press, 2002.138-147.

[6] ZOU C C, TOWSLEY D, GONG W. Modeling and simulation study of the propagation and defense of Internet E-mail worms[J]. IEEE Transactions on Dependable Secure Computer, 2007, 4(2):105-118.

[7] SERAZZI G, ZANERO S. Computer virus propagation models[A]. MASCOTS Tutorials 2003, IEEE Computer Society[C]. 2003. 26-50.

[8] YUAN H, CHEN G Q. Network virus-epidemic model with the point-to-group information propagation[J]. Applied Mathematics and Computation, 2008, 206(1): 357-367.

[9] Frauenthal J C. Mathematical Modeling in Epidemiology[M]. Springer-Verlag, New York, 1980.

[10] DAGON D, ZOU C, LEE W. Modeling botnet propagation using time zones[A]. Proceedings of the 13th Annual Network and Distributed System Security Symp. (NDSS)[C]. San Diego, CA, USA, 2006. 235-249.

[11] LI T, GUAN Z H, WANG Y M. The stability of a worm propagation model with time delay on homogeneous networks[A]. Proceedings of the 2010 International Conference on Intelligent Control and Information Processing (ICICIP)[C]. Dalian, China, 2010. 753-755.

[12] YAO Y, GUO H, GAO F X, *et al*. The worm propagation model with pulse quarantine strategy[A]. Proceedings of the 2010 International Conference on Multimedia Information Networking and Security (MINES)[C]. Nanjing, China, 2010.269-273.

[13] LI H, ZHENG Q, Pan X H, *et al*. Propagation model of non-scanning active worm in unstructured P2P network[A]. Proceedings of the 2009 International Conference on Multimedia Information Networking and Security[C]. Wuhan, China, 2009.378-381.

[14] FENG C S, QIN Z G, YUAN D, *et al*. Modeling passive worm propagation in mobile P2P networks[A]. Proceedings of the 2010 International Conference on Communications, Circuits and Systems (ICCCAS)[C]. Chengdu, China, 2010.241-244.

[15] NIE X F, WANG Y W, JING J W, *et al*. Understanding the impact of overlay topologies on peer-to-peer worm propagation[A]. Proceedings of the 2008 International Conference on Computer Science and Software Engineering[C]. Wuhan, China, 2008.863-867.

[16] Guidance for critical areas of focus in cloud computing[EB/OL]. http://www.cloudsecurityalliance.org/guidance/csaguide.pdf, 2009.

[17] GABER M M, ZASLAVSKY A, KRISHNASWAMY S. Mining data streams: a review[J]. ACM SIGMOD Record, 2005, 34(2): 18-26.

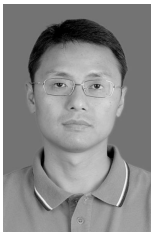
[18] ZHU L N, ZHU D Z. A Router-based technique to detect and defend against low-rate denial of service[A]. Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA)[C]. Xuzhou, China, 2009. 257-260.

[19] JOHN A, SIVAKUMAR T. DDoS: survey of traceback methods[J]. International Journal of Recent Trends in Engineering, 2009,1(2): 241-245.

[20] MISRA V, GONG W B, TOWSLEY D. A fluid based analysis of a network of AQM routers supporting TCP flows with an application to RED[A]. Proceedings of ACM/SIGCOMM[C]. Stockholm, Sweden, 2000. 151-160.

[21] WILENSKY U. NetLogo[EB/OL]. http://ccl.northwestern.edu/ netlogo/.

作者简介：



张伟（1973-），男，江苏泰兴人，博士，南京邮电大学副教授，主要研究方向为网络安全、计算机病毒分析、数据流检测等。

王汝传（1943-），男，安徽合肥人，南京邮电大学教授、博士生导师，主要研究方向为计算机软件、计算机网络和网格、对等计算、信息安全、无线传感器网络、移动代理和虚拟现实技术等。

李鹏（1979-），男，福建长汀人，南京邮电大学讲师，主要研究方向为计算机网络、信息安全等。