“去二存一”混合机制下的病毒扩散模型及稳定性分析

王 刚* 陆世伟 胡 鑫 马润年
(空军工程大学信息与导航学院 西安 710077)

摘 要：随着网络信息系统的发展，网络病毒扩散方式及免疫策略成为网络安全领域研究的热点之一。该文研究了一类新型混合攻击病毒，并根据其特点将这类病毒定义为“去二存一”型病毒。通过分析新型病毒的攻击方式，构建了“去二存一”混合机制下病毒的SEIQRS信息扩散模型。在此基础上，求解对应系统的平衡点，并运用Routh-Hurwitz判据分析了系统基本再生数R_0及其对系统稳定性的影响。最后，仿真验证了模型的有效性和稳定性。

关键词：病毒扩散；混合机制；稳定性分析
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1009-5896(2019)03-0709-08
DOI: 10.11999/JEIT180381

Virus Propagation Model and Stability Under the Hybrid Mechanism of “Two-go and One-live”

WANG Gang LU Shiwei HU Xin MA Runnian
(*Institute of Information and Navigation*, *Air Force Engineering University*, *Xi'an* 710077, *China*)

Abstract: With the development of network information system, virus propagation and immunization strategy become one of the hot topics in the field of network security. In this paper, a new virus with hybrid attacking is introduced, which can attack network in two modes. One is to attack and infect the network nodes directly, and the another is to hide itself in the nodes by hiding its viral characteristic. According to its characteristics, this type of virus is defined as “Two-go and One-live” and the corresponding virus propagation model is established. Moreover, the stability of the system is studied by solving the equilibrium points and analyzing the basic reproduction number R_0. Numerical simulations are presented to verify effectiveness and stability of the novel model.

Key words: Virus propagation; Hybrid mechanism; Stability analyzing

1 引言

攻击和防御是网络安全博弈的一对孪生子，尽管目前出现了动态目标防御、集体防御等策略和技术，但是网络安全总体上仍处于易攻难守的态势。在这种易攻难守的态势下，网络安全组织通常专注于解决单种病毒的防御问题，这种针对单一病毒攻击的防御设计在多数情况下也相对有效[1,2]。与此同时，网络安全博弈同步加速了混合攻击[3]等新型攻击策略和技术的发展。2017年6月出现的Not-Petya勒索病毒，能够在加密文件实现勒索的同时秘密清除内部数据，实施“二次破坏”；10月出现的“坏兔子”勒索病毒，可以利用恶意软件感染媒体网站，同时隐藏强大的鱼叉式网络钓鱼攻击。相对而言，这些新型病毒强调利用显式攻击分散防御方注意力，从而将另一种具有隐藏特性的病毒注入目标网络，并寻找合适的激活时机实施2次攻击。在攻击过程中，两种方式同时展开，一种攻击方式下的病毒直接攻击感染网络节点单元，但易被网络防御系统检测并查杀；另一种则利用免杀技术，如加壳，花指令，修改特征码等，隐藏病毒表征特性，避免被杀毒软件检杀，从而潜伏到网络节点单元中等待激活。综合这类病毒的发展和特征，我们将其定义为“去二存一”型病毒，即两种病毒同时展开攻击，而最终只有一种病毒大规模存活于网络中。据“趋势科技”预测，这类病毒在2018年网络安全领域将相对普遍[3]。

针对“去二存一”型病毒入侵，防御方需要对新型病毒的扩散方式和免疫策略有所研究。当现实

收稿日期：2018-04-25；改回日期：2018-09-13；网络出版：2018-09-25
*通信作者： 王刚 wglxl@nudt.edu.cn
基金项目：国家自然科学基金(61573017, 61703420)
Foundation Items: The National Science Foundation of China (61573017, 61703420)

网络遭受普通病毒入侵时，如网络中的节点遭到攻击感染，导致网络节点失效和网络系统瘫痪，通常采用信息/病毒扩散建模分析的方法研究病毒传播规律、影响因素和免疫策略。如文献[4]应用SIE(Susceptible-Infected-External)模型研究了外部因素影响下的计算机病毒扩散问题，文献[5]构建SIR(Susceptible-Infected-Removed)模型研究蠕虫病毒扩散方式，并运用数值逼近法分析其稳定性，文献[6]研究了相关异构感染率下的SIS(Susceptible-Infected-Susceptible)病毒传播模型。考虑到实际网络中免疫节点会衰退为易感节点，文献[7,8]构建SIRS(Susceptible-Infected-Removed-Susceptible)信息扩散模型，运用李雅普诺夫函数分析其平衡点的稳定性，并引入状态概率转移法研究病毒传播规律。基于网络行动的时延和内部节点的损伤特性，文献[9]提出SLBS(Susceptible-Latent-Breaking-Susceptible)模型，重点分析非线性感染率对病毒传播的影响。借鉴传染病模型中隔离者概念，文献[10]构建SIQRS(Susceptible-Infected-Quarantine-Removed-Susceptible)复杂网络病毒扩散模型，并提出与度相关的更加准确的病毒传播率。考虑到现实网络对病毒的查杀，文献[11]构建SIVRS(Susceptible-Infected-Variant-Recovery-Susceptible)病毒扩散模型，并对病毒扩散控制问题进行探索。针对网络结构与功能的不同，文献[12－14]研究了不同网络下病毒传播模型及系统的稳定性。考虑网络中多种不确定因素对病毒传播的影响，文献[15－18]研究了不同因素影响下病毒扩散的免疫控制方法。这些成果为开展网络病毒扩散、稳定性分析和免疫控制提供了理论和方法参考，但主要限定于单种病毒的扩散研究，对于“去二存一”型病毒而言，扩散机理和相应的查杀免疫机制都有了新的变化，具体而言：(1)新型病毒存在两种并行攻击手段，一种是直接以病毒的形式入侵目标网络，攻击和感染目标网络的易感节点，另一种通过隐藏自身的病毒特性，避开目标网络防御系统的检测，达到潜伏的目的。(2)攻击方通常会选择在合适的时机激活潜伏的病毒，然后迅速大幅度感染目标网络中的易感节点，达到“奇袭”的目的；因特殊原因无法激活或行动结束后尚未激活的潜伏病毒，可以再次转化为易感节点。(3)网络防御系统会加大对病毒的检杀力度，使得病毒/受病毒感染的节点尽可能地恢复到健康状态，再次转化为易感节点；对于很难在有效时间内清除所有病毒的情况，防御方会选择对部分病毒节点/受病毒感染节点实施物理隔离，防止病毒进一步感染其它节点，并在隔离阶段完成对隔离节点的免疫修复。基于以上分析，需要构建新的病毒扩散模型来研究“去二存一”混合机制下网络病毒扩散机理，通过稳定性分析研究病毒入侵后网络系统的演化过程，并寻找可能的防御途径及方法。

2 模型构建

在传统的SIRS信息扩散模型[7,8]基础上引入潜伏状态E，并根据新型病毒的攻击方式，完善易感状态向潜伏状态和感染状态的双重转化过程：易感状态S→潜伏状态E，易感状态S→感染状态I。其中，S→E过程表示网络易感节点被潜伏型病毒入侵，进入待激活状态；S→I过程表示网络易感节点被直接攻击型病毒感染为感染节点，并具备感染其他易感节点的能力。考虑到网络中部分易感节点在未被感染时也会具备抗病毒能力，免受网络病毒攻击感染，即存在易感状态S→免疫状态R。另外，处于潜伏状态的节点E，会以一定的概率被激活，从而转变为感染节点I，即E→I。同时，一部分潜伏状态节点E无法被激活或到行动结束也未激活，从而失去被激活的意义，再次转化为易感节点S，即E→S。考虑到网络防御系统对病毒节点查杀效果的不彻底性，根据文献[9,19,20]中传染病模型隔离者概念及复杂网络渗流理论，对部分受感染的节点进行物理隔离，断开与其它节点的连接。在此基础上，引入隔离状态Q，并根据系统防御机制，完善感染状态向易感状态和隔离状态的双重转化：感染状态I→易感状态S，感染状态I→隔离状态Q。其中，I→S表示受感染节点被网络防御系统检测并清除其中病毒，重新转变到易感状态；I→Q表示对未能被清除病毒的节点进行隔离，断开与外界的传播途径。考虑到大部分病毒传播速度十分迅速，需要将病毒节点先进行隔离，再进行免疫处理，避免免疫期间感染其他节点。因此，这里免疫过程只针对被隔离的节点，不再单独考虑对感染节点直接进行免疫的情况，即只存在隔离状态Q→免疫状态R。其次，考虑到病毒在扩散过程中可能会存在变异等行为，使得免疫节点对变异后病毒失去免疫能力，即存在免疫状态R→易感状态S。

基于以上考虑，构建“去二存一”混合机制下的SEIQRS病毒扩散模型，如图1所示。

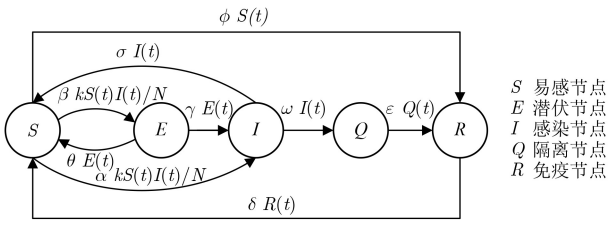

图 1 “去二存一”混合机制下的SEIQRS病毒扩散模型

其中，N为网络总节点数，k为网络节点平均度。$S(t)$, $E(t)$, $I(t)$, $Q(t)$和$R(t)$分别表示t时刻易感节点、潜伏节点、感染节点、隔离节点和免疫节点的数量。感染节点可分为两部分，一部分为被潜伏型病毒感染的节点，处于激活状态，具备感染能力，记作I_1；另一部分为被直接攻击型病毒感染的节点，记作I_2。假设I_1在感染节点中所占比例为β_0，则I_1的数量为$\beta_0 I(t)$，每次接触感染的概率为β_1，单位时间内一个感染节点与其他易感节点接触的次数为U，则平均有效接触率为$\beta_1 US/N$，即每个被潜伏型病毒感染的节点的感染率表达式为$\beta_1 US/N$。根据关治洪等人[10]的研究得知，接触次数U与节点度k成正比，即$U=\beta_2 k$，从而得到单个I_1节点的感染率为$\beta_1\beta_2 kS(\mathrm{t})/N$，则单位时间内所有潜伏型感染节点$I_1$的感染数为$\beta_0\beta_1\beta_2 kS(\mathrm{t})I(\mathrm{t})/N$，记$\beta=\beta_0\beta_1\beta_2$为$I_1$的感染系数，则感染数可简化为$\beta kS(\mathrm{t})I(\mathrm{t})/N$。同理，可得$I_2$的感染数为$\alpha kS(\mathrm{t})I(\mathrm{t})/N$，其中$\alpha$为$I_2$的感染系数。假设单位时间单个潜伏节点在网络行动中未被激活的概率为θ，则总的潜伏节点未被激活数量为$\theta E(\mathrm{t})$。同理，单位时间内其余状态节点之间的转移数量依次可得。

根据微分动力学原理，参照文献[6－8]，可得扩散模型对应的数学模型：

$$\left.\begin{aligned}
\frac{\mathrm{d}S(t)}{\mathrm{d}t} &= \theta E(t)+\sigma I(t)+\delta R(t)\\
&\quad -(\alpha+\beta)kS(t)I(t)/N-\varphi S(t)\\
\frac{\mathrm{d}E(t)}{\mathrm{d}t} &= \beta kS(t)I(t)/N-(\theta+\gamma)E(t)\\
\frac{\mathrm{d}I(t)}{\mathrm{d}t} &= \alpha kS(t)I(t)/N+\gamma E(t)-(\omega+\sigma)I(t)\\
\frac{\mathrm{d}Q(t)}{\mathrm{d}t} &= \omega I(t)-\varepsilon Q(t)\\
\frac{\mathrm{d}R(t)}{\mathrm{d}t} &= \varepsilon Q(t)+\varphi S(t)-\delta R(t)
\end{aligned}\right\} \tag{1}$$

假设网络节点状态仅在5类状态间转化，节点总数恒定为$N=S(t)+E(t)+I(t)+Q(t)+R(t)$，其中免疫状态节点数量$R(t)$可表示为$R(t)=N-S(t)-E(t)-I(t)-Q(t)$，则式(1)可进一步表示为

$$\left.\begin{aligned}
\frac{\mathrm{d}S(t)}{\mathrm{d}t} &= \theta E(t)+\sigma I(t)-(\alpha+\beta)kS(t)I(t)/N\\
&\quad -\varphi S(t)+\delta\,(N-S(t)-E(t)\\
&\quad -I(t)-Q(t))\\
\frac{\mathrm{d}E(t)}{\mathrm{d}t} &= \beta kS(t)I(t)/N-(\theta+\gamma)E(t)\\
\frac{\mathrm{d}I(t)}{\mathrm{d}t} &= \alpha kS(t)I(t)/N+\gamma E(t)-(\omega+\sigma)I(t)\\
\frac{\mathrm{d}Q(t)}{\mathrm{d}t} &= \omega I(t)-\varepsilon Q(t)
\end{aligned}\right\} \tag{2}$$

3　稳定性分析

网络系统稳定是指网络中不同状态的节点数量随时间变化逐步趋于稳定，可通过求解分析系统方程平衡点得到网络系统稳定时各状态节点的数量和性能。令式(2)中$\frac{\mathrm{d}S(t)}{\mathrm{d}t}=0$, $\frac{\mathrm{d}E(t)}{\mathrm{d}t}=0$, $\frac{\mathrm{d}I(t)}{\mathrm{d}t}=0$, $\frac{\mathrm{d}Q(t)}{\mathrm{d}t}=0$，可得网络系统的一个平衡点为$P^0(S^0,E^0,I^0,Q^0)=\left(\frac{\delta N}{(\varphi+\delta)},0,0,0\right)$。

式(2)存在另一个平衡点$P^1(S^1,E^1,I^1,Q^1)$，其中，

$$S^1=\frac{N(\sigma+\omega)(\gamma+\theta)}{k(\alpha\theta+\alpha\gamma+\beta\gamma)}$$

$$I^1=\frac{\varepsilon N[k\delta(\alpha\theta+\alpha\gamma+\beta\gamma)-(\varphi+\delta)(\sigma+\omega)(\theta+\gamma)]}{k[\beta\delta\varepsilon(\sigma+\omega)+(\alpha\theta+\alpha\gamma+\beta\gamma)(\delta\varepsilon+\delta\omega+\varepsilon\omega)]}$$

$$E^1=\frac{\beta(\sigma+\omega)}{(\alpha\theta+\alpha\gamma+\beta\gamma)}I^1,\ Q^1=\frac{\omega}{\varepsilon}I^1$$

分析可得，I^1存在一个阈值，决定网络系统中感染节点是否完全被清除。借鉴文献[10,11]中基本再生数概念和病毒传播理论，定义基本再生数$R_0=\frac{k\delta(\alpha\theta+\alpha\gamma+\beta\gamma)}{(\varphi+\delta)(\sigma+\omega)(\theta+\gamma)}$。显然，当且仅当$R_0\le 1$时，$I^1\le 0$，考虑实际病毒扩散过程中，各节点数量非负，因而，对应平衡点P^1处的感染节点数为0，系统中感染节点被完全清除。

令$P^*(S^*,E^*,I^*,Q^*)$为式(2)的任意平衡点，根据式(2)可得任意平衡点的Jacobi矩阵为

$$\boldsymbol{J}(P^*)=\begin{pmatrix}
\frac{-(\alpha+\beta)kI}{N}-\varphi-\delta & \theta-\delta & \frac{(\alpha+\beta)kS}{N}+\sigma-\delta & -\delta\\
\frac{\beta kI}{N} & -(\gamma+\theta) & \frac{\beta kS}{N} & 0\\
\frac{\alpha kI}{N} & \gamma & \frac{\alpha kS}{N}-\sigma-\omega & 0\\
0 & 0 & \omega & -\varepsilon
\end{pmatrix} \tag{3}$$

定理 1　当$R_0\le 1$时，式(2)在平衡点P^0局部渐近稳定；当$R_0>1$时，在平衡点P^0处不稳定。

证明　由式(3)可得平衡点P^0处的Jacobi矩阵为

$$\boldsymbol{J}(P^0)=\begin{pmatrix} -\varphi-\delta & \theta-\delta & -\dfrac{(\alpha+\beta)k\delta}{\varphi+\delta}-\delta+\sigma & -\delta \\ 0 & -(\gamma+\theta) & -\dfrac{\beta k\delta}{\varphi+\delta} & 0 \\ 0 & \gamma & \dfrac{\alpha k\delta}{\varphi+\delta}-\sigma-\omega & 0 \\ 0 & 0 & \omega & -\varepsilon \end{pmatrix} \tag{4}$$

矩阵$\boldsymbol{J}(P^0)$对应的特征多项式为

$$(\lambda+\varepsilon)(\lambda+\varphi+\delta)\left[(\lambda+\gamma+\theta)\times\left(\lambda+\sigma+\omega-\frac{\alpha k\delta}{\delta+\varphi}\right)-\frac{\beta k\delta\gamma}{\varphi+\delta}\right]=0 \tag{5}$$

解得特征根$\lambda_1=-\varepsilon$，$\lambda_2=-(\psi+\delta)$，等式$(\lambda+\gamma+\theta)\left(\lambda+\sigma+\omega-\dfrac{\alpha k\delta}{\delta+\varphi}\right)-\dfrac{\beta k\delta\gamma}{\varphi+\delta}=0$的解是多项式的另外两个特征根，设为$\lambda_3$, λ_4。分析可知：当$R_0\le 1$时，$\lambda_3+\lambda_4<0$, $\lambda_3\cdot\lambda_4\ge 0$，则$\lambda_3$, λ_4实部均为负，平衡点P^0处局部稳定；当$R_0>1$时，λ_3, λ_4至少有一个特征根为正，平衡点P^0处局部不稳定。 证毕

定理 2 当$R_0>1$时，式(2)在平衡点P^1局部渐近稳定；当$R_0\le 1$时，在平衡点P^1处不稳定。

证明 由式(3)可得平衡点P^1处的Jacobi矩阵为

$$\boldsymbol{J}(P^1)=\begin{pmatrix} -\dfrac{(\alpha+\beta)kI^1}{N}-\delta-\varphi & \theta-\delta & -\dfrac{(\alpha+\beta)kS^1}{N}-\delta+\sigma & -\delta \\ \dfrac{\beta kI^1}{N} & -(\gamma+\theta) & \dfrac{\beta kS^1}{N} & 0 \\ \dfrac{\alpha kI^1}{N} & \gamma & \dfrac{\alpha kS^1}{N}-\sigma-\omega & 0 \\ 0 & 0 & \omega & -\varepsilon \end{pmatrix} \tag{6}$$

设矩阵$\boldsymbol{J}(P^1)$对应的特征多项式为

$$\lambda^4+\mu_1\lambda^3+\mu_2\lambda^2+\mu_3\lambda+\mu_4=0 \tag{7}$$

计算可得，$\mu_1=\varepsilon+M_1$，$\mu_2=\varepsilon M_1+M_2$，$\mu_3=\varepsilon M_2+M_3$，$\mu_4=\varepsilon M_3$。其中，

$$\begin{aligned} M_1&=\delta+\varphi+\theta+\sigma+\omega+\frac{\beta}{\alpha}\gamma+\frac{2\alpha k}{N}I^1-\frac{\alpha k}{N}S^1,\\ M_2&=\left(\theta+\frac{\alpha+\beta}{\beta}\gamma\right)\left(\varphi+\delta+\sigma+\omega-\frac{\alpha k}{N}S^1\right)\\ &\quad+\frac{\alpha kI_1}{N}\left(\sigma+2\omega+2\delta+\theta+\frac{\alpha+\beta}{\alpha}\gamma\right)\\ &\quad+(\varphi+\delta)\left(\sigma+\omega-\frac{\alpha k}{N}S^1\right)\\ &\quad-\gamma(\varphi+\delta+\sigma+\omega),\\ M_3&=(\varphi+\delta)\left[\left(\theta+\frac{\alpha+\beta}{\alpha}\gamma\right)\left(\sigma+\omega-\frac{\alpha k}{N}S^1\right)\right.\\ &\quad\left.-\gamma(\sigma+\omega)\right]+\frac{\alpha k}{N}I^1\\ &\quad\cdot\left[\delta(\sigma+\omega)+(\delta+\omega)\left(\theta+\frac{\alpha+\beta}{\alpha}\gamma\right)\right] \end{aligned} \tag{8}$$

计算可得，当$R_0>1$时，$\mu_1,\mu_2>0$，$\mu_1\mu_2-\mu_3>0$，且$\mu_1\mu_2\mu_3-\mu_3^2-\mu_4>0$。根据Routh-Hurwitz稳定判据[11−13]，式(7)对应的Routh表第一列元素均为正值，因此，在平衡点$P^1(S^1,E^1,I^1,Q^1)$处局部稳定。 证毕

由上述分析可知，系统的稳定性与基本再生数R_0有紧密联系。当$R_0\le 1$时，系统在无病毒平衡点P^0处局部渐近稳定，即网络系统中不存在病毒节点；当$R_0>1$时，系统在感染源平衡点$P^1(S^1,E^1,I^1,Q^1)$处局部渐近稳定，即网络系统中存在病毒节点。通过分析基本再生数$R_0=\dfrac{k\delta(\alpha\theta+\alpha\gamma+\beta\gamma)}{(\varphi+\delta)(\sigma+\omega)(\theta+\gamma)}$可知，网络节点平均度$k$及“去二存一”混合机制下的感染系数$\alpha$, β对基本再生数的影响是正向的，即3个参数值越大，R_0越大，病毒在网络系统中扩散规模越大；防御机制下的3个转移参数φ, σ, ω对基本再生数的影响是反向的，即3个参数值越大，R_0越小，病毒在系统中扩散规模越小。换言之，如果“去二存一”病毒的两种攻击强度不超过防御门限值，则防御方可通过检杀-隔离-免疫机制修复感染节点，使网络系统将恢复到健康状态，并趋向稳态；反之，如果攻击强度超过防御门限值，防御方未能完全清除系统内病毒节点，最终网络系统会趋向于一种有病毒节点的稳态，且系统中待激活的病毒节点、受病毒感染节点以及被隔离的病毒节点将以一定比例持续存在。“去二存一”病毒的攻击能力由两种攻击方式共同决定，相对而言，它的潜在威胁力可能更大。

4　仿真分析

定理1和定理2表明，当$R_0 \le 1$时，系统在无病毒平衡点P^0处局部渐近稳定；当$R_0 > 1$时，系统在感染源平衡点$P^1(S^1, E^1, I^1, Q^1)$处局部渐近稳定。为验证理论分析的合理性，围绕基本再生数$R_0 = \dfrac{k\delta(\alpha\theta + \alpha\gamma + \beta\gamma)}{(\varphi+\delta)(\sigma+\omega)(\theta+\gamma)}$，重点对网络节点度$k$、两种感染方式下感染系数$\alpha$, β以及查杀参数σ仿真。由于Matlab组件Simulink可以仿真求解非线性微分方程组，适用于病毒传播动力学模型求解分析，以下使用该工具分析4个参数对系统稳定性的影响，进而验证模型的有效性以及网络系统的演进关系。通过平衡点分析可知，在系统最终稳定时，潜伏节点E、感染节点I和隔离节点Q的数量存在正比例关系。为反映系统状态随时间的变化，以$S(t)$, $E(t)$和$I(t)$为轴建立3维坐标系，并参照文献[8－10,12－14]设置相关参数，令节点数量初始值$(S(0), E(0), I(0), Q(0))$=(980, 0, 20, 0), $\alpha = 0.1$, $\beta = 0.3$, $\theta = 0.1$, $\gamma = 0.6$, $\sigma = 0.4$, $\omega = 0.5$, $\varepsilon = 0.4$, $\varphi = 0.4$, $\delta = 0.2$, N=1000, k=10。若无特殊说明，3维仿真图中自变量t在[0, 200]之间取值。

4.1　网络平均度k

考虑网络平均度对流通性的影响较大，先仿真分析网络平均度k对新型病毒传播的影响。令基本再生数$R_0 = 1$，对应网络平均度$k_{\lim} = \dfrac{(\varphi+\delta)(\sigma+\omega)(\theta+\gamma)}{\delta(\alpha\theta+\alpha\gamma+\beta\gamma)} = 7.56$。分别取$k$=5和$k$=10进行仿真，各状态节点数量随时间的变化结果如图2所示。令k在区间[0, 15]内取值，步长为5，观察感染节点数量$I(t)$在不同k值下的变化情况，结果如图3所示。

由图2和图3分析可知，当$k \le k_{\lim}$时，$R_0 \le 1$，系统局部渐近地稳定在平衡点P^0处；当$k > k_{\lim}$时，$R_0 > 1$，系统局部渐近地稳定在P^1处。仿真结果表明，在网络系统演化中，网络平均度越大，病毒节点数量峰值越大，病毒在网络中扩散规模越大，稳定后的网络系统中感染节点越多。特殊地，当网络平均度$k = 0$时，即网络中节点都处于断开连接状态，病毒会在系统自身防御机制下被清除，感染节点数量趋于0。

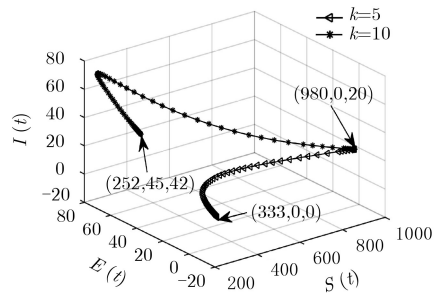

图 2　k=5和k=10时各状态节点数量

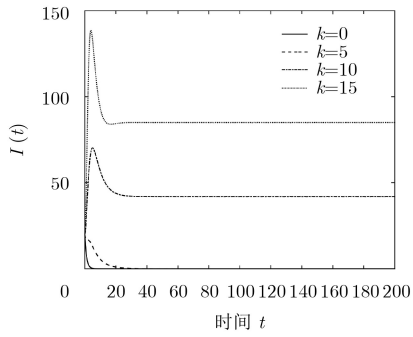

图 3　不同k值下$I(t)$随时间的变化

4.2　感染系数α

考虑“去二存一”混合机制下易感节点被双重感染的特点，仿真分析两种感染方式下的感染系数α, β对新型病毒传播的影响。首先，对感染系数α进行仿真验证。令基本再生数R_0=1，对应的感染系数$\alpha_{\lim} = \dfrac{(\delta+\varphi)(\sigma+\omega)}{k\delta} - \dfrac{\beta\gamma}{(\gamma+\theta)} = 0.013$。分别取$\alpha = 0.01$和$\alpha = 0.10$进行仿真，仿真时间取[0, 800]，各状态节点数量随时间的变化结果如图4所示。令α在区间[0, 0.03]内取值，步长为0.01，观察感染节点数量I(t)在不同α值下的变化情况，仿真结果如图5所示。

由图4和图5分析可知，当$\alpha \le \alpha_{\lim}$时，$R_0 \le 1$，系统局部渐近地稳定在平衡点P^0处；当

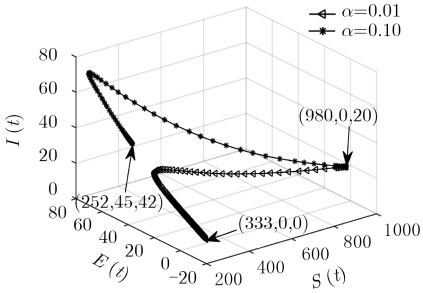

图 4　$\alpha = 0.01$和$\alpha = 0.10$时各状态节点数量

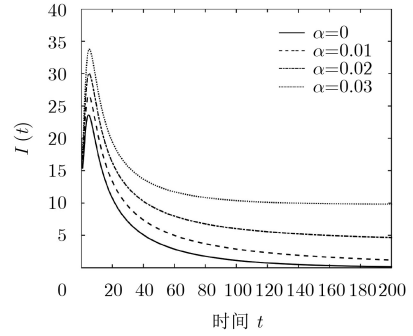

图 5　不同α值下$I(t)$随时间的变化

$\alpha > \alpha_{\lim}$时，$R_0 > 1$，系统局部渐近地稳定在P^1处。仿真结果表明，I_1型感染节点的感染系数越大，病毒节点数量峰值越大，病毒扩散规模越大，稳定后感染节点越多。此外，对图5的进一步分析表明，当接触率$\alpha = 0$，即不存在直接攻击时，网络系统可通过自身防御机制快速清除病毒节点。

4.3 感染系数β

仍然令基本再生数R_0=1，对应的感染系数$\beta_{\lim} = \dfrac{(\delta+\varphi)(\gamma+\theta)(\sigma+\omega)}{k\delta\gamma} - \dfrac{\alpha(\gamma+\theta)}{\gamma} = 0.2$。取$\beta = 0.1$和$\beta = 0.5$分别进行仿真，各状态节点数量变化如图6所示。令$\beta$在区间[0, 0.45]内取值，步长为0.15，观察感染节点数量I(t)在不同β取值下的变化情况，结果如图7所示。

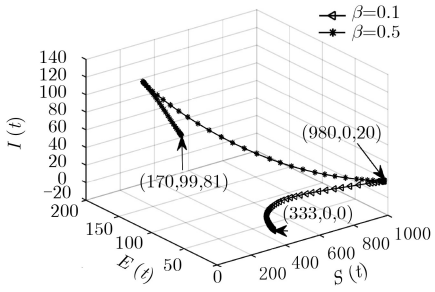

图 6 $\beta = 0.1$和$\beta = 0.5$时各状态节点数量

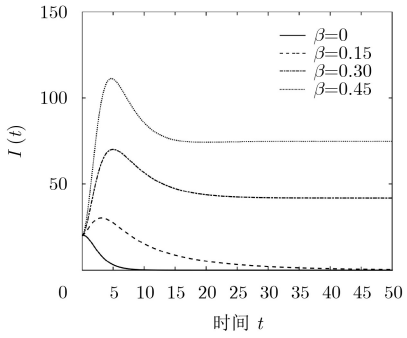

图 7 不同β值下$I(t)$随时间的变化

由图6和图7分析可知，当$\beta \le \beta_{\lim}$时，$R_0 \le 1$，系统局部渐近地稳定在平衡点P^0处；当$\beta > \beta_{\lim}$时，$R_0 > 1$，系统局部渐近地稳定在P^1处。仿真结果表明，I_2型感染节点的感染系数越大，病毒扩散规模越大，稳定后感染节点越多。此外，对图6的进一步分析表明，当感染系数$\beta = 0$时，即系统中不存在潜伏机制病毒时，防御系统可以在病毒入侵初期就迅速清除感染节点，并使网络系统稳定在健康状态。

4.4 查杀参数σ

考虑病毒入侵后网络防御系统的检杀-隔离-免疫机制，依次分析转移参数σ, w, φ对新型病毒传播的影响。令基本再生数R_0=1，对应的查杀参数$\sigma_{\lim} = \dfrac{k\delta(\alpha\theta+\alpha\gamma+\beta\gamma)}{(\varphi+\delta)(\theta+\gamma)} - \omega = 0.69$。取$\sigma = 0.3$和$\sigma = 1.2$分别进行仿真，各状态节点数量随时间的变化结果如图8所示。令σ在区间[0, 1.2]内取值，步长为0.4，观察感染节点数量I(t)在不同σ取值下的变化情况，结果如图9所示。

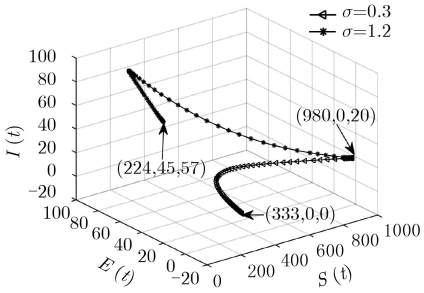

图 8 $\sigma = 0.3$和$\sigma = 1.2$时的各状态节点数量

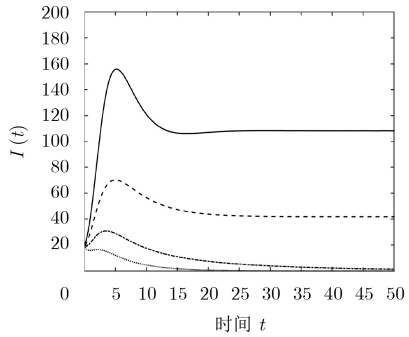

图 9 不同σ值下$I(t)$随时间的变化

由图8和图9分析可知，当$\sigma > \sigma_{\lim}$时，$R_0 \le 1$，系统局部渐近地稳定在平衡点P^0处；当$\sigma \le \sigma_{\lim}$时，$R_0 > 1$，系统局部渐近地稳定在P^1处。仿真结果表明，网络防御系统对感染病毒的节点检测查杀比例越小，病毒扩散规模越大，稳定后的网络系统中感染节点越多。当$\sigma = 0$，即网络防御系统不具备病毒检杀机制时，系统中病毒数量会迅速上升，在系统稳定时存在大量病毒节点。通过对基本再生数$R_0 = \dfrac{k\delta(\alpha\theta+\alpha\gamma+\beta\gamma)}{(\varphi+\delta)(\sigma+\omega)(\theta+\gamma)}$的分析，得知转移参数$\varphi, \sigma, w$都与再生数$R_0$成反比，仿真结果验证免疫参数$\varphi$和隔离参数$\omega$对系统稳定性的影响与参数$\sigma$相似，这里不再分析。

5 结论

理论分析和仿真结果表明：(1)在网络行动的起始阶段，“去二存一”型病毒攻击网络系统并潜伏于网络节点中，防御系统未检测到潜伏病毒的节

点，系统中病毒节点数量逐渐增加，并在激活后感染其他网络节点；一旦防御系统检测到病毒节点，便启用有效防御手段，迅速清除病毒。但最终网络中是否存在病毒节点，取决于网络系统自身的防御能力。(2)在网络安全防御行动中，可以通过改变复杂网络的节点度来有效控制病毒在网络系统中的扩散规模，从而维护网络空间安全。通过减小网络节点度，来减缓病毒在网络系统中的扩散速度，使其感染能力不超过网络防御门限，从而将网络系统稳定在无病毒状态，维持网络空间的健康。(3)网络防御系统针对病毒入侵存在3种防御机制——隔离、免疫、检测查杀，3种防御手段对系统的稳定性具有同向作用。防御方可通过增大这3种机制下的转移参数，来提高网络系统防御能力，维护网络空间安全。

参 考 文 献

[1] 张书奎, 崔志明, 龚声蓉, 等. 传感器网络病毒感染传播局域控制研究[J]. 电子学报, 2009, 37(4): 877–883. doi: 10.3321/j.issn:0372-2112.2009.04.038.
ZHANG Shukui, CUI Zhiming, GONG Shengrong, *et al*. An investigation on local area control of compromised nodes spreading in wireless sensor networks[J]. *Acta Electronica Sinica*, 2009, 37(4): 877–883. doi: 10.3321/j.issn:0372-2112.2009.04.038.

[2] 王田, 吴群, 文晟, 等. 无线传感网中移动式蠕虫的抑制与清理[J]. 电子与信息学报, 2016, 38(9): 2202–2207. doi: 10.11999/JEIT151311.
WANG Tian, WU Qun, WEN Sheng, *et al*. The inhibition and clearup of the mobile worm in wireless sensor networks[J]. *Journal of Electronics & Information Technology*, 2016, 38(9): 2202–2207. doi: 10.11999/JEIT151311.

[3] E安全. 黑客战术三十六计之“声东击西”[OL]. https://www.easyaq.com/news/1538639872.shtml, 2017, 11.

[4] ZHANG Zizhen and BI Dianjie. Bifurcation analysis in a delayed computer virus model with the effect of external computers[J]. *Advances in Difference Equations*, 2015, 2015(1): 317–330. doi: 10.1186/s13662-015-0652-y.

[5] VALDEZ J, GUEVARA P, and AUDELO J. Numerical approaching of SIR epidemic model for propagation of computer worms[J]. *IEEE Latin America Transactions*, 2015, 13(10): 3452–3460. doi: 10.1109/TLA.2015.7387254.

[6] QU Bo and WANG Huijuan. SIS epidemic spreading with correlated heterogeneous infection rates[J]. *Physica A: Statistical Mechanics and its Applications*, 2017, 472(1): 13–24.

[7] TANG Qian and TENG Zhidong. A new Lyapunov function for SIRS epidemic models[J]. *Bulletin of the Malaysian Mathematical Sciences Society*, 2017, 40(1): 237–258. doi: 10.1007/s40840-016-0315-5.

[8] 顾海俊, 蒋国平, 夏玲玲. 基于状态概率转移的SIRS病毒传播模型及其临界值分析[J]. 计算机科学, 2016, 43(6): 64–67. doi: 10.11896/j.issn.1002-137X.2016.6A.014.
GU Haijun, JIANG Guoping, and XIA Lingling. SIRS epidemic model and its threshold based on state transition probability[J]. *Computer Science*, 2016, 43(6): 64–67. doi: 10.11896/j.issn.1002-137X.2016.6A.014.

[9] YANG Luxing and YANG Xiaofan. The impact of nonlinear infection rate on the spread of computer virus[J]. *Nonlinear Dynamics*, 2015, 82(2): 85–95.

[10] 关治洪, 亓玉娟, 姜晓伟, 等. 基于复杂网络的病毒传播模型及其稳定性[J]. 华中科技大学学报, 2011, 39(1): 114–117.
GUAN Zhihong, QI Yujuan, JIANG Xiaowei, *et al*. Virus propagation dynamic model and stability on complex network[J]. *Journal Huazhong University of science & Technology*, 2011, 39(1): 114–117.

[11] XU Degang, XU Xiyang, XIE Yongfang, *et al*. Optimal control of an SIVRS epidemic spreading model with virus variation based on complex networks[J]. *Communications in Nonlinear Science and Numerical Simulation*, 2017, 48(1): 200–210.

[12] KHANH G H and HUY N B. Stability analysis of a computer virus propagation model with antidote in vulnerable system[J]. *Acta Mathematica Scientia*, 2016, 36(1): 49–61. doi: 10.1016/S0252-9602(15)30077-1.

[13] WANG Xu, NI Wei, ZHENG Kangfeng, *et al*. Virus propagation modeling and convergence analysis in large scale networks[J]. *IEEE Transactions on Information Forensics and Security*, 2016, 11(10): 2241–2254. doi: 10.1109/TIFS.2016.2581305.

[14] TIAN Daxin, LIU Chao, SHENG Zhengguo, *et al*. Analytical model of spread of epidemics in open finite regions[J]. *IEEE Access*, 2017, 5(2): 9673–9681.

[15] LIU Siyu, JIN Jiyu, and WANG Zhisen. Influence of node mobility on virus spreading behaviors in multi-hop network[J]. *EURASIP Journal on Wireless Communications and Networking*, 2016, 2016(1): 172–182. doi: 10.1186/s13638-016-0667-4.

[16] ZHANG Chunming and HUANG Haitao. Optimal control strategy for a novel computer virus propagation model on scale-free networks[J]. *Physica A*: *Statistical Mechanics and Its Applications*, 2016, 451(1): 251–265.

[17] HAN Dun, SUN Mei, and LI Dandan. The virus variation model by considering the degree-dependent spreading rate[J]. *Physica A*: *Statistical Mechanics and Its Applications*, 2015, 433(1): 42–50.

[18] XU Qichao, SU Zhou, and YANG Kan. Optimal control theory based epidemic information spreading scheme for mobile social users with energy constraint[J]. *IEEE Access*, 2017, 5(1): 3536–3547.

[19] 王小娟, 宋梅, 郭世泽, 等. 基于有向渗流理论的关联微博转发网络信息传播研究[J]. 物理学报, 2015, 64(4): 4502–4510. doi: 10.7498/aps.64.044502.

WANG Xiaojuan, SONG Mei, GUO Shize, *et al*. Information spreading in correlated microblog reposting network based on directed percolation theory[J]. *Acta Physica Sinica*, 2015, 64(4): 4502–4510. doi: 10.7498/aps.64.044502.

[20] LI Ming and WANG Binghong. Percolation on networks with dependence links[J]. *Chinese Physics B*, 2014, 23(7): 6402–6411.

王 刚：男，1976年生，博士，教授，硕士生导师，主要研究方向为网络空间安全和复杂网络.

陆世伟：男，1995年生，硕士生，研究方向为网络空间安全.

胡 鑫：男，1993年生，硕士生，研究方向为网络空间安全.