doi:10.11887/j.cn.201806017 http://journal.nudt.edu.cn

潜伏-隔离机制下的信息扩散拓展模型及稳定性*

王 刚[1],胡 鑫[1,2],陆世伟[1],马润年[1]
(1. 空军工程大学 信息与导航学院,陕西 西安 710077;2. 中国人民解放军95507部队,贵州 贵阳 550031)

摘 要:为适应信息扩散中病毒传播的复杂性和不确定性,在传统病毒传播模型和信息扩散模型基础上,引入潜伏状态和隔离状态,研究潜伏-隔离机制下的信息扩散模型及其稳定性。构建基于潜伏-隔离机制的信息扩散模型;运用劳斯稳定性判据,论证系统平衡点的局部稳定性,分析基本再生数 R_0 及其对网络感染源和系统状态的影响;通过仿真实验,分析节点连通半径、节点分布密度和节点接触率对信息扩散的影响。仿真结果表明:通过调整节点连通半径、节点分布密度和节点接触率等参数,可实现对信息扩散的有效控制。

关键词:网络安全;信息扩散;稳定性;潜伏-隔离机制
中图分类号:TP393 **文献标志码**:A **文章编号**:1001-2486(2018)06-124-05

Information diffusion extended model and stability based on escape-quarantined mechanism

WANG Gang[1], *HU Xin*[1,2], *LU Shiwei*[1], *MA Runnian*[1]
(1. Information and Navigation Institute, Air Force Engineering University, Xi'an 710077, China;
2. The PLA Unit 95507, Guiyang 550031, China)

Abstract: In order to meet the complexity and uncertainty of virus diffusion in cyberspace operation, escape status and quarantined status were introduced into the virus diffusion model based on a traditional diffusion model, and its stability was discussed. The escape and quarantined mechanism of cyberspace operation was introduced. Via Routh stability criterion, the local stability of system equilibrium point was demonstrated as well as the basic reproductive number R0. Simulations were given to illustrate the influence of node connectivity, node distribution density, and node contact ratio on information diffusion. The results show that the information diffusion can be effectively controlled by changing the parameter regulations on node connectivity, node distribution density, and node contact ratio.

Key words: cyber security; information diffusion; stability; escape-quarantined mechanism

在复杂网络环境中,网络节点通过多级多类型节点之间的连接链路和信息流程关系,实现网络信息的针对性扩散和传播[1-2]。信息扩散具有典型的流通性、影响性和被影响性等特点,与病毒传播过程所具有的传播性、感染性和被感染性特点相似,通常借助病毒传播模型研究网络的信息扩散机理和性能,如基于易感-感染-易感(Susceptible-Infected-Susceptible,SIS)模型的网络病毒延迟及其影响因素[3]、基于易感-感染-免疫(Susceptible-Infected-Remove,SIR)模型的无标度网络最大传染能力分析[4]、基于易感-感染-免疫-易感(Susceptible-Infected-Remove-Susceptible,SIRS)模型的移动自主网络传播特性分析[5]、基于易感-感染-隔离-免疫-易感(Susceptible-Infected-Quarantined-Remove-Susceptible, SIQRS)模型的病毒传播机制分析[6]。

在网络安全领域,信息网络攻防技术的发展,使得网络行动隐蔽高效、高边疆和深度攻防等特点更加凸显,网络信息节点性质和作用关系较SIQRS等模型有了新的变化,"潜伏-隔离"成为复杂网络中信息扩散的新机制和攻防策略与技术研究的焦点[1,7]。网络信息节点在遭受病毒攻击感染后,病毒外在的特征会暂时隐藏潜伏起来;按照某种需求和触发机制,攻击一方在特定时机激活启动该病毒。从网络安全防御角度看,当侦察到节点遭受入侵病毒感染后,通常采用集体防御策略和技术对感染节点进行隔绝[8]。

针对网络行动特点,本文在SIRS模型基础上,引入潜伏状态E和隔离状态Q,构建了基于潜伏-隔离机制的信息扩散模型,即易感-潜伏-

* 收稿日期:2017-08-30
基金项目:国家自然科学基金资助项目(61573017,61401499)
作者简介:王刚(1976—),男,湖北武汉人,教授,博士,硕士生导师,E-mail:wglxl@nudt.edu.cn

感染 - 隔离 - 免疫 - 易感(Susceptible-Escape-Infected-Quarantined-Remove-Susceptible,SEIQRS)模型,给出了模型稳定性的理论分析和仿真验证。

1　信息扩散拓展模型

从网络病毒传播角度分析,先进网络武器(如网络飞行器、网络病毒)通常采用隐蔽方式注入对手的网络链路和节点单元后潜伏下来,并根据需要选择合适的时机和手段激发网络病毒,实施网络感染和攻击行动,“潜伏”是网络行动中信息扩散的重要因素。从网络安全防御角度分析,立体深度和集体防御已成为新的趋势。简而言之,防御方通过集体协同行动检测受感染情况,然后采取一定策略和技术手段实现对受感染节点的隔绝处置,自主或强制断开与其他节点的连通,待完成修复后,重新接入网络节点,其中的“隔离”是网络行动和信息扩散的关键因素。因此,在网络安全领域的研究中,应综合考虑网络攻防行动中的“潜伏”和“隔离”因素,在传统病毒扩散模型基础上增加潜伏、隔离状态和相应的信息扩散关系。

将网络节点状态分为 5 类,即易感染状态 S、潜伏状态 E、感染状态 I、隔离状态 Q 和免疫状态 R。记 N 为网络节点总数,$S(t)$ 为 t 时刻网络节点中未受感染的节点数量,$E(t)$ 为 t 时刻潜伏于网络中的携带病毒信息的节点数量,$I(t)$ 为 t 时刻受病毒感染成网络病毒的节点数量,$Q(t)$ 为 t 时刻受病毒感染节点经检测后自主隔离的节点数量,$R(t)$ 为 t 时刻经治愈后自身具有抗病毒能力的节点数量。若易感节点与感染节点接触概率为 β_0,单位时间内单个感染节点与其他节点的接触次数为 C,接触次数与节点度 k 正相关,即 $C=ak$,则易感节点的感染率为 $\beta kS(t)I(t)/N$(令 $\beta=\beta_0 a$)[6]。节点连通性与节点接触半径 r 以及节点分布密度 ρ 有关,其有效传播区域为以该节点为中心、半径为 r 的圆,即该区域面积为 πr^2。考虑节点度分布的计算不包括节点自身[1,6],节点度可表示为:

$$k=\rho\pi r^2-1 \tag{1}$$

构建的信息扩散拓展模型如图 1 所示。

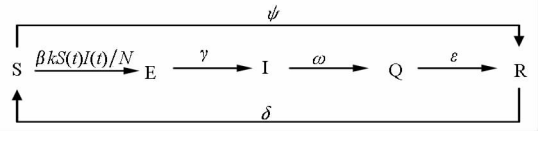

图 1　信息扩散拓展模型

Fig. 1　Information diffusion extended model

对应的数学式为:

$$\begin{cases}\dfrac{\mathrm{d}S(t)}{\mathrm{d}t}=-\dfrac{\beta kS(t)I(t)}{N}-\psi S(t)+\sigma R(t)\\ \dfrac{\mathrm{d}E(t)}{\mathrm{d}t}=\dfrac{\beta kS(t)I(t)}{N}-\gamma E(t)\\ \dfrac{\mathrm{d}I(t)}{\mathrm{d}t}=\gamma E(t)-\omega I(t)\\ \dfrac{\mathrm{d}Q(t)}{\mathrm{d}t}=\omega I(t)-\varepsilon Q(t)\\ \dfrac{\mathrm{d}R(t)}{\mathrm{d}t}=\varepsilon Q(t)+\psi S(t)-\sigma R(t)\end{cases} \tag{2}$$

其中:ψ 为易感状态转化为免疫状态的概率,表示部分节点自身具有抗病毒能力,在遭受网络入侵行动后受到激活直接转化为具有抗病毒能力节点的概率;γ 为潜伏状态转换为感染状态的概率,表示病毒攻击感染网络中其他节点,并使其携带病毒信息的概率;ω 为感染状态转换为隔离状态的概率,表示受病毒攻击感染的网络节点采取防御措施并断开通信连接,避免攻击感染其他网络节点的概率;ε 为隔离状态转换为免疫状态的概率,表示断开通信连接的受感染节点进行自愈修复,使其具有抗病毒能力的概率;δ 为免疫状态转换为易感状态的概率,表示节点的抗病毒能力在网络安全防御过程中逐渐减弱,使其最终转变为不具有抗病毒能力节点的概率。

2　稳定性分析

网络信息扩散的稳定性是指网络中处于不同状态的节点数逐渐趋于稳定,且不受时间和网络中其他因素(感染源)的影响。网络总节点数 $N=S(t)+E(t)+I(t)+Q(t)+R(t)$。假设在信息扩散过程中,$N$ 保持不变,则免疫节点数可表示为 $R(t)=N-S(t)-E(t)-I(t)-Q(t)$。为求解平衡点,将式(2)调整为:

$$\begin{cases}\dfrac{\mathrm{d}S(t)}{\mathrm{d}t}=-\dfrac{(\rho\pi r^2-1)\beta S(t)I(t)}{N}-\psi S(t)+\\ \qquad\qquad \delta[N-S(t)-E(t)-I(t)-Q(t)]\\ \dfrac{\mathrm{d}E(t)}{\mathrm{d}t}=\dfrac{(\rho\pi r^2-1)\beta S(t)I(t)}{N}-\gamma E(t)\\ \dfrac{\mathrm{d}I(t)}{\mathrm{d}t}=\gamma E(t)-\omega I(t)\\ \dfrac{\mathrm{d}Q(t)}{\mathrm{d}t}=\omega I(t)-\varepsilon Q(t)\end{cases} \tag{3}$$

令 $\dfrac{\mathrm{d}S(t)}{\mathrm{d}t}=0,\dfrac{\mathrm{d}E(t)}{\mathrm{d}t}=0,\dfrac{\mathrm{d}I(t)}{\mathrm{d}t}=0,\dfrac{\mathrm{d}Q(t)}{\mathrm{d}t}=0$,当 $t\to\infty$ 时,系统各状态节点数趋于平稳,且与时间无关。由式(3)可得平衡点 $\boldsymbol{P}^0(S^0,E^0,I^0,$

$Q^0)=\left(\frac{\delta}{\psi+\delta}N,0,0,0\right)$，对应的潜伏、感染和隔离状态的节点数均为0。

令基本再生数 $R_0=\frac{(\rho\pi r^2-1)\beta\delta}{\omega(\delta+\psi)}$，当且仅当 $R_0>1$ 时，式(3)存在另一个平衡点 $\boldsymbol{P}^1(S^1,E^1,I^1,Q^1)$。其中：$S^1=\frac{\omega N}{(\rho\pi r^2-1)\beta}$，$E^1=\frac{\omega\varepsilon N[(\rho\pi r^2-1)\beta\delta-\omega(\delta+\psi)]}{\beta(\rho\pi r^2-1)[\delta(\omega\varepsilon+\gamma\omega+\gamma\varepsilon)+\gamma\varepsilon\omega]}$，进一步转化可得基于 R_0 的对应表达式 $E^1=\frac{\omega\varepsilon N\delta(1-1/R_0)}{\delta(\omega\varepsilon+\gamma\omega+\gamma\varepsilon)+\gamma\varepsilon\omega}$，$I^1=\frac{\gamma}{\omega}E^1$，$Q^1=\frac{\omega}{\varepsilon}I^1=\frac{\gamma}{\varepsilon}E^1$。

定理1 当 $R_0\leqslant1$ 时，系统在平衡点 $\boldsymbol{P}^0(S^0,E^0,I^0,Q^0)$ 处局部渐近稳定；当 $R_0>1$ 时，平衡点 $\boldsymbol{P}^0$ 局部不稳定。

证明：$\boldsymbol{P}^0$ 处的 Jacobian 矩阵 $J(\boldsymbol{P}^0)$ 为：

$$\begin{pmatrix}-\psi-\delta & -\delta & -(\rho\pi r^2-1)\beta\frac{\delta}{\delta+\psi}-\delta & -\delta\\ 0 & -\gamma & (\rho\pi r^2-1)\beta\frac{\delta}{\delta+\psi} & 0\\ 0 & \gamma & -\omega & 0\\ 0 & 0 & \omega & -\varepsilon\end{pmatrix} \tag{4}$$

对应特征多项式为：

$$(\lambda+\varepsilon)(\lambda+\psi+\delta)[(\lambda+\gamma)(\lambda+\omega)-\beta\gamma\frac{\delta}{\delta+\psi}(\rho\pi r^2-1)]=0 \tag{5}$$

可得特征根 $\lambda_1=-\varepsilon$，$\lambda_2=-(\psi+\delta)$，另两特征根为等式 $\lambda^2+(\gamma+\omega)\lambda+\frac{\gamma}{\delta+\psi}[\omega(\delta+\psi)-\delta\beta(\rho\pi r^2-1)]=0$ 的解。结合等式分析可知：当 $R_0\leqslant1$ 时，式(5)的根实部均为负，平衡点 $\boldsymbol{P}^0$ 局部稳定；当 $R_0>1$ 时，存在一个特征根为正，平衡点 $\boldsymbol{P}^0$ 局部不稳定。□

定理2 当 $R_0>1$ 时，系统在平衡点 $\boldsymbol{P}^1(S^1,E^1,I^1,Q^1)$ 处局部渐近稳定。

证明：$\boldsymbol{P}^1$ 处的 Jacobian 矩阵为：

$$\boldsymbol{J}(\boldsymbol{P}^1)=\begin{pmatrix}\frac{-(\rho\pi r^2-1)\beta I^1}{N}-\psi-\delta & -\delta & -\omega-\delta & -\delta\\ \frac{(\rho\pi r^2-1)\beta I^1}{N} & -\gamma & \omega & 0\\ 0 & \gamma & -\omega & 0\\ 0 & 0 & \omega & -\varepsilon\end{pmatrix} \tag{6}$$

矩阵 $\boldsymbol{J}(\boldsymbol{P}^1)$ 所对应的特征多项式为：

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

式中：

$$\mu_1=\frac{(\rho\pi r^2-1)\beta I^1}{N}+\gamma+\varepsilon+\psi+\delta+\omega$$

$$\mu_2=\frac{(\rho\pi r^2-1)\beta I^1}{N}(\varepsilon+\gamma+\omega-\delta)+\varepsilon(\psi+\delta+\gamma+\omega)+(\psi+\delta)(\gamma+\omega)$$

$$\mu_3=\frac{(\rho\pi r^2-1)\beta I^1}{N}(\varepsilon\gamma+\varepsilon\omega-\varepsilon\delta-\omega\delta-\omega\gamma-\gamma\delta)+\varepsilon(\psi+\delta)(\gamma+\omega)$$

$$\mu_4=-\frac{(\rho\pi r^2-1)\beta I^1}{N}(\omega\delta\varepsilon+\gamma\omega\varepsilon+\gamma\delta\varepsilon-\gamma\omega\delta)$$

其中，$\mu_1,\mu_2>0$，由劳斯稳定性判据[9-10]计算得，$\mu_1\mu_2-\mu_3>0$，$\mu_3(\mu_1\mu_2-\mu_3)-\mu_1^2\mu_4>0$。可判断其特征根全部位于坐标轴的左半平面，对应 $\boldsymbol{J}(\boldsymbol{P}^1)$ 的特征值实部为负。可得结论：当基本再生数 $R_0>1$ 时，感染源平衡点 $\boldsymbol{P}^1$ 局部渐近稳定。□

上述稳定性分析显示网络病毒入侵和防御中的“潜伏-隔离”规律。当网络病毒攻击未超出网络安全防御能力阈值时，即便网络节点受到病毒入侵，但由于具有网络安全免疫机制和技术，受病毒信息感染的节点和携带病毒信息的节点均被隔离后修复，全部网络节点最终都转化为具有抗病毒攻击感染能力的节点(即免疫节点)，整个网络逐渐趋于稳定；反之，如果病毒入侵超过网络安全防御能力阈值，网络中网络病毒节点、受病毒攻击感染的网络节点以及断开通信连接的网络病毒节点将持续存在，并以一定的节点数目比例逐渐趋于稳定。

3 仿真分析

选取节点有效连通半径 r、节点分布密度 ρ 和节点接触率 β 三个参数，仿真验证其对信息扩散的影响。参照文献[6,11]选取仿真参数，设置节点总数 $N=10\ 000$，各状态节点数量初始值为 $(S(0),E(0),I(0),Q(0))=(9800,0,200,0)$，$\delta=0.1$，$\psi=0.9$，$\beta=0.2$，$\rho=0.01$，$r=30$，$\gamma=0.6$，$\omega=0.5$，$\varepsilon=0.8$。

3.1 节点连通半径 r

调整节点连通半径，分析其对信息扩散的影响。令 $R_0=1$，得对应节点连通半径传播阈值 $r_{\lim}=28.8$。即当 $r\leqslant r_{\lim}$ 时，系统局部渐近稳定在平衡点 $\boldsymbol{P}^0$ 处；当 $r>r_{\lim}$ 时，系统局部渐近稳定在平衡点 $\boldsymbol{P}^1$ 处。图2和图3分别表示不同连通半径对应易感状态S和感染状态I的变化曲线。r 在区间[10,50]内取值，步长为10。

当 r 取10,20且小于 $r_{\lim}$ 时，系统局部渐近稳定在平衡点 $\boldsymbol{P}^0(1000,0,0,0)$ 处；当 r 取30,40,50

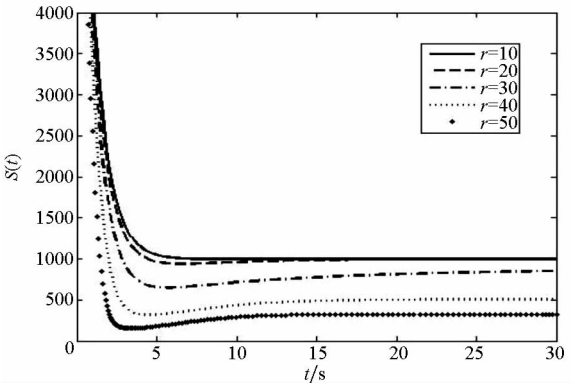

图 2　不同 r 下 $S(t)$ 随时间的变化曲线

Fig. 2　Curve of $S(t)$ varies with t under different r

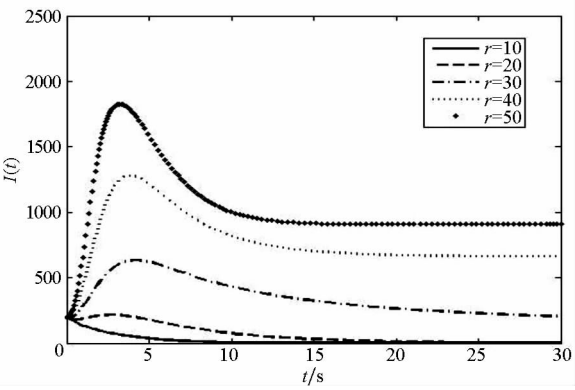

图 3　不同 r 下 $I(t)$ 随时间的变化曲线

Fig. 3　Curve of $I(t)$ varies with t under different r

且大于 $r_{\lim}$ 时,系统局部渐近稳定在平衡点 $\boldsymbol{P}^1$ 处。当系统在局部渐近稳定平衡点 $\boldsymbol{P}^1$ 处时,易感状态 S 的节点数随着 r 的增大而减小,感染状态 I 的节点数随着 r 的增大而增大。可见,节点连通半径越大,入侵病毒越容易攻击感染网络信息节点,并在网络实施安全防御后逐渐趋于稳定。通过调节 r 值,可实现对网络信息扩散的有效控制。

3.2　节点分布密度 ρ

调整节点分布密度,分析其对信息扩散的影响。令 $R_0 = 1$,得节点分布密度的传播阈值 $\rho_{\lim} = 0.009$。即当 $\rho \leqslant \rho_{\lim}$ 时,系统在平衡点 $\boldsymbol{P}^0$ 处局部渐近稳定;当 $\rho > \rho_{\lim}$ 时,系统在平衡点 $\boldsymbol{P}^1$ 处局部渐近稳定。图 4 和图 5 分别表示不同 ρ 对应易感状态 S 和感染状态 I 的变化曲线。ρ 在区间[0.002,0.018]内取值,步长为 0.004。

当系统在局部渐近稳定平衡点 $\boldsymbol{P}^1$ 处时,易感状态 S 的节点数随着 ρ 的增大而减小,感染状态 I 的节点数随着 ρ 的增大而增大。可见,节点分布密度越大,入侵病毒越容易攻击网络信息节点,并在网络实施安全防御后逐渐趋于稳定。通过调节 ρ 值,可实现对网络信息扩散的有效控制。

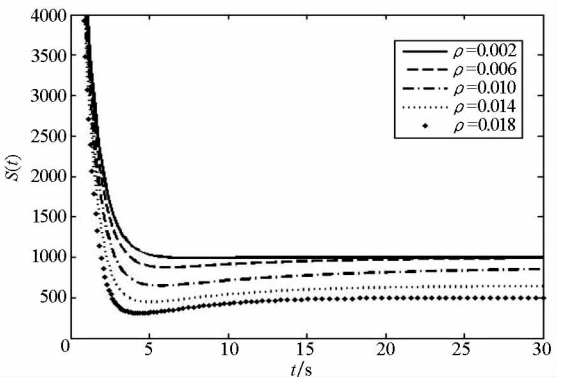

图 4　不同 ρ 下 $S(t)$ 随时间的变化曲线

Fig. 4　Curve of $S(t)$ varies with t under different ρ

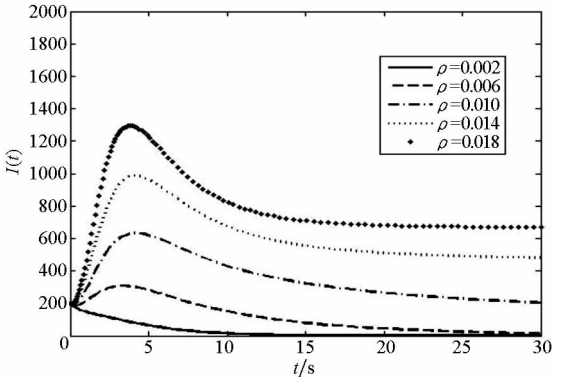

图 5　不同 ρ 下 $I(t)$ 随时间的变化曲线

Fig. 5　Curve of $I(t)$ under different ρ

3.3　节点接触率 β

调整节点接触率,分析其对信息扩散的影响。令 $R_0 = 1$,得节点接触率的传播阈值 $\beta_{\lim} = 0.183$。即当 $\beta \leqslant \beta_{\lim}$ 时,系统在平衡点 $\boldsymbol{P}^0$ 处局部渐近稳定;当 $\beta > \beta_{\lim}$ 时,系统在平衡点 $\boldsymbol{P}^1$ 处局部渐近稳定。图 6 和图 7 分别表示不同 β 对应易感状态 S 和感染状态 I 的变化曲线。其中,β 在区间[0.1,0.3]内取值,步长为 0.05。

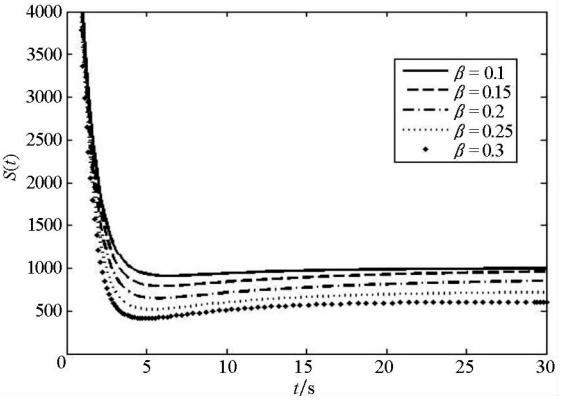

图 6　不同 β 下 $S(t)$ 随时间的变化曲线

Fig. 6　Curve of $S(t)$ varies with t under different β

当 β 取 0.1,0.15 且小于 $\beta_{\lim}$ 时,系统局部渐近

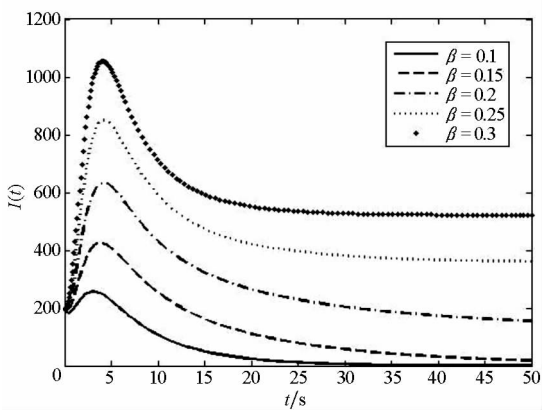

图7 不同β下$I(t)$随时间的变化曲线

Fig. 7 Curve of $I(t)$ varies with t under different β

稳定在平衡点$\boldsymbol{P}^0$(1000,0,0,0)处;当β取0.2,0.25,0.3且大于$\beta_{\lim}$时,系统局部渐近稳定在平衡点$\boldsymbol{P}^1$处。当系统在局部渐近稳定平衡点$\boldsymbol{P}^1$处时,易感状态S的节点数随着β的增大而减小,感染状态I的节点数随着β的增大而增大。可见,节点接触率越大,入侵病毒越容易攻击感染网络信息节点,并在网络实施安全防御后逐渐趋于稳定。通过调节β值,可实现对网络信息扩散的有效控制。

按照以上仿真步骤,调整仿真参数中的各状态节点数量初始值,多组仿真结果与以上给出的仿真结果大体相似。仿真结果表明:①通过降低网络信息节点的连通半径、节点分布密度和节点接触率,可有效减少网络病毒与网络中其他节点的通信连接,从而降低病毒攻击感染网络节点的概率。②如果网络侦察鉴别能力较弱,病毒感染节点将迅速增加,而隔离节点数相对较少。③如果网络防御和病毒侦察鉴别能力较强,隔离节点数在一段时间内将持续且相对缓慢增长,一旦掌握了病毒入侵特征和免疫手段,网络病毒将可能被迅速消除,潜伏节点数迅速降低至稳态,隔离节点数目在动态变化中趋向稳态。

4 结论

本文借鉴病毒传播理论研究信息扩散问题,在经典的病毒传播模型基础上,构建了基于复杂网络的信息扩散SEIQRS模型,分析了系统的稳定性。以阈值门限R_0为基准,分析了R_0对系统平衡点的稳定性的影响:当$R_0 \leqslant 1$时,系统的无病毒平衡点局部渐进稳定,网络空间安全防御占据优势;当$R_0 > 1$时,系统的感染源平衡点全局渐进稳定。同时,仿真分析了节点连通半径、节点分布密度和节点接触率对信息扩散的影响。

参考文献(References)

[1] Argonne National Laboratory. Enabling distributed security in cyberspace: building a healthy and resilient cyber ecosystem with automated collective action [R]. Department of Defense, 2011.

[2] Tsigkanos C, Kehrer T, Ghezzi C. Architecting dynamic cyber-physical spaces [J]. Computing, 2016, 98(10): 1011-1040.

[3] Li C C, Jiang G P, Song Y R. Comparative effects of avoidance and immunization on epidemic spreading in a dynamic small-world network with community structure [J]. Wuhan University Journal of Natural Sciences, 2016, 21(4): 291-297.

[4] 裴伟东, 刘忠信, 陈增强, 等. 无标度网络中最大传染能力限定的病毒传播模型问题研究[J]. 物理学报, 2008(11): 6777-6785.
PEI Weidong, LIU Zhongxin, CHEN Zengqiang, et al. Study of epidemic spreading on scale-free networks with finite maximum dissemination [J]. Acta Physica Sinica, 2008(11): 6777-6785. (in Chinese)

[5] 赵焱鑫, 张丹, 王小明, 等. 移动自组网病毒传播模型及稳定性分析[J]. 计算机应用与软件, 2015, 32(11): 297-300.
ZHAO Yanxin, ZHANG Dan, WANG Xiaoming, et al. Virus propagation model of manet and its stability analysis [J]. Computer Application and Software, 2015, 32(11): 297-300. (in Chinese)

[6] 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(自然科学版), 2011, 39(1): 114-117.
GUAN Zhihong, QI Yujuan, JIANG Xiaowei, et al. Virus propagation dynamic model and stability on complex networks [J]. Journal of Huazhong University of Science and Technology(Natural Science Edition), 2011, 39(1): 114-117. (in Chinese)

[7] 刘效武, 王慧强, 吕宏武, 等. 网络安全态势认知融合感控模型[J]. 软件学报, 2016, 27(8): 2099-2114.
LIU Xiaowu, WANG Huiqiang, LYU Hongwu, et al. Fusion-based cognitive awareness-control model for network security situation [J]. Journal of Software, 2016, 27(8): 2099-2114. (in Chinese)

[8] Wu G Y, Sun J, Chen J. A survey on the security of cyber-physical systems [J]. Control Theory and Technology, 2016, 14(1): 2-10.

[9] Yu G T, Gao J, Luo J H. Stability analysis method considering non-parallelism: EPSE method and its application [J]. Applied Mathematics and Mechanics, 2016, 37(1): 27-36.

[10] Menacer T. Control of a fractional jerk equation using the fractional Routh-Hurwitz criteria [C]//Proceedings of 4th International Conference on Systems and Control, 2015: 351-356.

[11] 鲁延玲, 蒋国平, 宋玉荣. 自适应网络中病毒传播的稳定性和分岔行为研究[J]. 物理学报, 2013, 62(13): 130202.
LU Yanling, JIANG Guoping, SONG Yurong. Stability and bifurcation of epidemic spreading on adaptive network [J]. Acta Physica Sinica, 2013, 62(13): 130202. (in Chinese)