操作系统病毒时滞传播模型及抑制策略设计

王刚，冯云，马润年
（空军工程大学信息与导航学院，710077，西安）

摘要：为了有效抑制操作系统病毒在网络中的传播，针对操作系统病毒的目标性强和感染时滞等特点，提出了操作系统病毒的时滞传播模型及抑制策略。在经典 SIRS 模型基础上，考虑操作系统切换和感染阶段时耗因素，引入新的节点状态和感染时滞，构建了操作系统病毒的时滞模型，并给出了系统的平衡点和基本再生数；运用 Lyapunov 直接法，证明了网络系统在无病毒平衡点处的全局稳定性；根据 Hopf 分岔理论，计算了网络存在有病毒平衡点时出现分叉的阈值，分析了有病毒平衡点处的 Hopf 分岔行为；针对感染时滞过高时的振荡现象，设计了相应病毒传播抑制策略，通过微调操作系统切换频率消除振荡现象，在感染节点数稳定后，参照基本再生数重新调整操作系统切换频率，从而彻底消除病毒。理论和仿真结果表明：当基本再生数小于 1 时，网络能在无病毒平衡点处全局渐进稳定，此时网络可依赖自身免疫能力消除操作系统病毒；当基本再生数大于 1 且时滞大于对应阈值时，感染节点数存在周期性振荡，此时网络环境难以判定，通过微调操作系统切换频率可消除振荡；当基本再生数大于 1 且时滞小于对应阈值时，网络在有病毒平衡点处局部渐进稳定，此时网络安全态势明确，可根据基本再生数调整操作切换频率，彻底消除操作系统病毒。

关键词：感染时滞；病毒传播；稳定性；Hopf 分岔；抑制策略
中图分类号：TP393 **文献标志码**：A
DOI：10.7652/xjtuxb202103002 **文章编号**：0253-987X(2021)03-0011-09

OSID 码

Time-Delay Propagation Model and Suppression Strategy Design of Operating System Virus

WANG Gang, FENG Yun, MA Runnian
(Information and Navigation Institute, Air Force Engineering University, Xi'an 710077, China)

Abstract: To effectively suppress operating system virus propagation in the network, a time-delay propagation model and the suppression strategy of operating system virus are proposed aiming at the characteristics of operating system virus, such as strong target and delay of infection. Based on the SIRS model, a new state and the infection time delay are introduced. The time-delay model of the operating system virus is constructed. The equilibrium point and the basic regeneration number are given. The global stability of network system at the virus-free equilibrium point is proved by direct Lyapunov method. According to Hopf bifurcation theory, the threshold of bifurcation is calculated, and the Hopf bifurcation behavior is analyzed at the virus equilibrium point. To solve the oscillation in the case of too high infection time delay, the virus propagation suppression strategy is designed. The oscillation can be eliminated by fine-tuning the switching frequency of the operating system. When the number of infected nodes is stable, switching frequency of the operating system is renewed with reference to the basic

收稿日期：2020-08-16。 作者简介：王刚(1976—)，男，教授。 基金项目：国家自然科学基金资助项目(61573017)。
网络出版时间：2020-10-20 网络出版地址：http://kns.cnki.net/kcms/detail/61.1069.T.20201020.1401.002.html

regeneration number. to eliminate virus completely. The theoretical and simulation results show that when the basic regeneration number is less than 1, the network can be globally asymptotically stable at the virus-free equilibrium point. The network can eliminate the operating system virus relying on its own immunity. When the basic regeneration number is greater than 1 and the time delay is greater than the corresponding threshold, the number of infected nodes has periodic oscillation. It is difficult to determine the network environment at this time. The oscillation can be eliminated by fine-tuning the operating system switching frequency. When the basic regeneration number is greater than 1 and the time delay is less than the corresponding threshold, the network is locally asymptotically stable at the virus equilibrium point, and the network security situation is clear. At this time, the operation switching frequency can be adjusted according to the basic regeneration number to ensure network security.

Keywords: infection time-delay; virus propagation; stability; Hopf bifurcation; suppression strategy

操作系统病毒能利用操作系统漏洞攻击网络并在网络中传播,对网络及其用户造成重大损失。彻底查杀病毒需要消耗大量的时间和精力,难以在操作系统病毒入侵初期快速构建有效防御[1-3]。动态目标防御等新型防御手段[4-7]提供了主动防御的新思路,但考虑部署代价、对网络业务的负面影响等因素,在全网部署并持续运行成本过高。合理高效地部署防御并抑制操作系统病毒传播,已经成为网络安全领域亟待解决的问题。

计算机病毒传播研究借鉴了生物学病毒传播理论,经典病毒传播模型包括 SI、SIR 和 SIRS 等[8-11]。这些模型将网络抽象成图,以用户为节点,用户之间的联系为边,根据感染行为及用户对病毒的防御能力将节点划分为不同状态,研究不同状态之间的节点转化关系,通过动力学建模和稳定性分析推演网络中病毒可能的扩散规模。随着网络攻防对抗的升级,网络结构、病毒攻击机理、传播方式有新的特点,病毒传播模型和相关研究也出现了一些针对性改进[12-15]。一类是适应病毒传播特点,添加新的节点状态,修改状态转化关系,使模型更加契合病毒的传播模式,如 SEIR、SEIQR 等病毒传播模型;另一类则是考虑病毒传播过程中感染、免疫的耗时问题,在模型中添加时滞,研究带时滞的病毒传播模型[16-20]。通常而言,无时滞时病毒传播较为稳定,而时滞则可能造成网络中感染节点数的振荡,时滞病毒传播情况更复杂。

操作系统病毒利用的是特定操作系统的漏洞,通常只能在特定操作系统平台上运行,操作系统病毒传播主要受网络中多种类型操作系统和感染时滞等因素的影响。考虑操作系统病毒传播特性,本文主要研究操作系统病毒时滞传播模型及抑制策略,包括:①考虑网络中操作系统切换和感染过程耗时对操作系统病毒传播的影响,在 SIRS 病毒传播模型的基础上,引入新的状态和感染时滞,构建操作系统病毒的时滞传播模型;②研究网络在不同平衡点处的稳定性,分析网络消除病毒和出现分岔的条件,以及影响网络中感染节点规模和分岔的关键参数;③针对感染时滞造成的分岔问题,设计有感染时滞的操作系统病毒抑制策略;④仿真分析关键参数对操作系统病毒传播的影响和病毒抑制策略的有效性。

1 操作系统病毒时滞传播模型

按照计算机病毒传播机理,操作系统病毒扩散通常经历了侦察、传播和感染等阶段。侦察阶段,探查当前网段内有相应操作系统漏洞且未被感染的主机;传播阶段,病毒将用于传播的模块链接附着在正常程序中,随着正常程序的启动被加载入内存并执行,实现病毒的传播;感染阶段,操作系统病毒传播至用户计算机后,在造成危害之前需要完成侦查、复制和传播等工作,而后才会利用相应漏洞对用户造成危害。病毒感染由一系列行为组成,感染过程需要耗费一定时间,而这一过程中如果操作系统发生变化,则会导致目标和漏洞丢失,导致感染失败。为便于分析,做出如下假设:①网络中仅存在一种操作系统病毒,能感染主流操作系统 OS-A;②感染过程耗时为 τ,一旦被打断则感染失败。

在经典 SIRS 计算机病毒传播模型基础上,构建操作系统病毒传播的时滞 SIRO 模型,相应的节点状态转化关系如图 1 所示。

图 1 中:S 表示易感状态,该状态下的节点可以

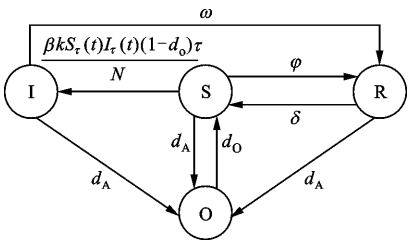


图 1　节点状态转化关系

被感染节点感染；I 表示感染状态，该状态下的节点已经被病毒危害，且具备感染其他节点的能力；R 表示免疫状态，该状态下的节点无法被感染；O 表示节点安装了其他操作系统的状态，该状态下的节点同样无法被感染节点感染；$S_\tau(t)=S(t-\tau)$，$I_\tau(t)=I(t-\tau)$状态的节点数，$S(t)$、$I(t)$分别表示 t 时刻易感、感染状态的节点数；k 表示网络的平均度；φ 表示易感节点获得免疫能力的概率；δ 表示免疫节点丧失免疫能力的概率；d_A 表示 OS-A 切换到其他操作系统的概率；d_O 表示从其他操作系统切换到 OS-A 的概率；N 表示网络中节点总数，在一段时间内保持稳定。易感节点在同感染节点通信过程中，可能被植入操作系统病毒，并在时间 τ 内被感染，β 表示易感节点单位时间内被其相邻的一个感染节点植入病毒的概率，一个节点被注入病毒的概率与其周围的感染节点数有关，当感染率较低时，可近似认为该节点被植入病毒的概率与其周围的感染节点数是线性相关的，易感节点周围感染节点数不完全相同，在动力学方程构建过程中，可采用平均场理论[8]，用 $\beta k I(t)/N$ 代替易感节点被植入病毒的概率。操作系统切换会打断操作系统病毒的感染和持续，在时间 τ 内，被植入操作系统病毒的易感节点未发生操作系统切换的概率为 $(1-d_A)^\tau$，易感节点的平均感染概率为 $\beta k I_\tau(t)(1-d_A)^\tau/N$。运用微分动力学方法，构建操作系统病毒传播的时滞微分方程为

$$\left.\begin{aligned}\frac{\mathrm{d}S(t)}{\mathrm{d}t}&=-\frac{\beta k S_\tau(t)I_\tau(t)(1-d_A)^\tau}{N}-\varphi S(t)-\\&\quad d_A S(t)+\delta R(t)+d_O O(t)\\\frac{\mathrm{d}I(t)}{\mathrm{d}t}&=\frac{\beta k S_\tau(t)I_\tau(t)(1-d_O)^\tau}{N}-\omega I(t)-d_A I(t)\\\frac{\mathrm{d}R(t)}{\mathrm{d}t}&=\varphi S(t)+\omega I(t)-\delta R(t)-d_A R(t)\\\frac{\mathrm{d}O(t)}{\mathrm{d}t}&=d_A S(t)+d_A I(t)+d_A R(t)-d_O O(t)\end{aligned}\right\}\tag{1}$$

式中 $R(t)$、$O(t)$分别为 t 时刻免疫、安装了其他操作系统状态的节点数。

令 $\mathrm{d}S(t)/\mathrm{d}t=0$，$\mathrm{d}I(t)/\mathrm{d}t=0$，$\mathrm{d}R(t)/\mathrm{d}t=0$，$\mathrm{d}R(t)/\mathrm{d}t=0$，求解可得平衡点 $P_0(S_0,I_0,R_0,O_0)$和 $P_1(S_1,I_1,R_1,O_1)$

$$\left.\begin{aligned}P_0(S_0,I_0,R_0,O_0)&=\Big(\frac{d_O(d_A+\delta)N}{(d_A+d_O)(d_A+\delta+\varphi)},0,\\&\qquad\frac{d_O\varphi N}{(d_A+d_O)(d_A+\delta+\varphi)},\frac{d_A N}{(d_A+d_O)}\Big)\\P_1(S_1,I_1,R_1,O_1)&=\\&\Big(\frac{(d_A+\omega)N}{\beta k(1-d_A)^\tau},I_1,\frac{\omega I_1+\varphi S_1}{d_A+\delta},\frac{d_A N}{d_A+d_O}\Big)\end{aligned}\right\}\tag{2}$$

式中

$$\begin{aligned}I_1=\{&[d_O(d_A+\delta)\beta k(1-d_A)^\tau-(d_A+d_O)\cdot\\&(d_A+\omega)(d_A+\delta+\varphi)]/[(d_A+\delta+\omega)\cdot\\&(d_A+d_O)\beta k(1-d_A)^\tau]\}N\end{aligned}\tag{3}$$

显然，无病毒平衡点 $P_0(S_0,I_0,R_0,O_0)$始终存在。根据文献[16]，由式(3)可得式(1)的基本再生数 $R_0=\dfrac{d_O(d_A+\delta)\beta k(1-d_A)^\tau}{(d_A+d_O)(d_A+\omega)(d_A+\delta+\varphi)}$。当 $R_0\leqslant 1$ 时，有病毒平衡点 $P_1(S_1,I_1,R_1,O_1)$不存在；当 $R_0>1$ 时，有病毒平衡点 $P_1(S_1,I_1,R_1,O_1)$存在。

2　稳定性分析

设 $A(t)=S(t)+I(t)+R(t)$，式(1)可进一步表示为

$$\left.\begin{aligned}\frac{\mathrm{d}A(t)}{\mathrm{d}t}&=-d_A A(t)+d_O O(t)\\\frac{\mathrm{d}O(t)}{\mathrm{d}t}&=d_A A(t)-d_O O(t)\end{aligned}\right\}\tag{4}$$

引理 1　式(4)表示的网络系统有唯一平衡点 $P(A,O)=\Big(\dfrac{d_O N}{d_A+d_O},\dfrac{d_A N}{d_A+d_O}\Big)$，且在该平衡点处局部渐进稳定。

证明　令式(4)中$\dfrac{\mathrm{d}A(t)}{\mathrm{d}t}=0$，$\dfrac{\mathrm{d}O(t)}{\mathrm{d}t}=0$，求解可得式(4)的唯一平衡点 $P(A,O)=\Big(\dfrac{d_O N}{d_A+d_O},\dfrac{d_A N}{d_A+d_O}\Big)$，该平衡点处的雅可比矩阵为

$$\boldsymbol{J}=\begin{bmatrix}-d_A & d_O\\ d_A & -d_O\end{bmatrix}\tag{5}$$

相应的特征方程为

$$\lambda(\lambda+d_A+d_O)=0\tag{6}$$

由式(6)可得式(5)的两个特征根为 $\lambda_1=0$ 和 $\lambda_2=-d_A-d_O$，均为非正根。由劳斯稳定判据，式(6)在唯一平衡点处局部稳定。证毕。

引理 2　当 $t\to\infty$时，$S(t)\leqslant S_0$。

证明 由引理 1 可知，当 $t\to\infty$ 时，有 $S(t)+I(t)+R(t)=d_{\mathrm{O}}N/(d_{\mathrm{A}}+d_{\mathrm{O}})$，进而可得 $R(t)=d_{\mathrm{O}}N/(d_{\mathrm{A}}+d_{\mathrm{O}})-S(t)-I(t)$，代入式(1)中 $\mathrm{d}S(t)/\mathrm{d}t$ 可得

$$\lim_{t\to\infty}\mathrm{d}S(t)/\mathrm{d}t=-\frac{\beta k S(t)I_{\tau}(1-d_{\mathrm{A}})^{\tau}}{N}-(d_{\mathrm{A}}+\delta+\varphi)S(t)+\frac{d_{\mathrm{O}}(d_{\mathrm{A}}+\delta)N}{d_{\mathrm{A}}+d_{\mathrm{O}}}-\delta I(t) \tag{7}$$

由微分方程比较定理可得

$$\lim_{t\to\infty}\mathrm{sub}(S(t))=-\frac{\beta k S(t)I_{\tau}(1-d_{\mathrm{A}})^{\tau}}{(d_{\mathrm{A}}+\delta+\varphi)N}+S_0-\frac{\delta I(t)}{d_{\mathrm{A}}+\delta+\varphi} \tag{8}$$

因此，$\exists\, T\in(0,+\infty)$，使得 $\forall\, t\in(T,+\infty)$，有 $S(t)\leqslant S_0-\dfrac{\beta k S_{\tau}I_{\tau}(1-d_{\mathrm{A}})^{\tau}/N+\delta I(t)}{d_{\mathrm{A}}+\delta+\varphi}$。

由于 $\beta k S_{\tau}I_{\tau}(1-d_{\mathrm{A}})^{\tau}N^{-1}+\delta I(t)\geqslant 0$，所以 $S(t)\leqslant S_0$。显然，当且仅当 $I(t)=I(t-\tau)=0$ 时，$S(t)\leqslant S_0$ 中的等号成立。证毕。

定理 1 当 $R_0\leqslant 1$ 时，式(1)表示的网络系统在无病毒平衡点 $P_0(S_0,I_0,R_0,O_0)$ 处全局渐进稳定。

证明 定义 Lyapunov 函数

$$f(t)=I(t)+\int_{t-\tau}^{t}\frac{\beta k S(x)I(x)(1-d_{\mathrm{A}})^{\tau}}{N}\mathrm{d}x \tag{9}$$

对式(9)求导可得

$$f'(t)=\frac{\mathrm{d}I(t)}{\mathrm{d}t}+\int_{t-\tau}^{t}\frac{\beta k S(t)I(t)}{N}\mathrm{d}x=\frac{\beta k S(t+\tau)I(t)(1-d_{\mathrm{O}})^{\tau}}{N}-\omega I(t)-d_{\mathrm{A}}I(t)=I(t)\left(\frac{\beta k S(t+\tau)I(t)(1-d_{\mathrm{O}})^{\tau}}{N}-(\omega+d_{\mathrm{A}})\right) \tag{10}$$

由引理 2 和式(2)可知

$$f'(t)\leqslant I(t)(\omega+d_{\mathrm{A}})(R_0-1) \tag{11}$$

当 $R_0\leqslant 1$ 时，$f'(t)\leqslant 0$，当且仅当 $I(t)=0$ 时等号成立。根据 LaSalle 不变原理，式(1)表示的网络系统在无病毒平衡点 $P_0(S_0,I_0,R_0,O_0)$ 处全局渐进稳定。证毕。

定理 2 当 $R_0>1$ 时，存在 τ_0，使得当 $\tau<\tau_0$ 时，式(1)表示的网络系统在有病毒平衡点处局部渐进稳定，当 $\tau\geqslant\tau_0$ 时，式(1)表示的网络系统在有病毒平衡点处振荡，出现 Hopf 分岔现象。

证明 根据引理 1，式(1)可简化为

$$\left.\begin{aligned}\frac{\mathrm{d}S(t)}{\mathrm{d}t}&=-\frac{\beta k S(t)I_{\tau}(t)(1-d_{\mathrm{A}})^{\tau}}{N}-S(t)-\delta I(t)+\frac{d_{\mathrm{O}}(\delta+d_{\mathrm{A}})N}{d_{\mathrm{O}}+d_{\mathrm{A}}}\\ \frac{\mathrm{d}I(t)}{\mathrm{d}t}&=\frac{\beta k S(t)I_{\tau}(t)(1-d_{\mathrm{O}})^{\tau}}{N}-\omega I(t)-d_{\mathrm{A}}I(t)\end{aligned}\right\} \tag{12}$$

对应的特征方程为

$$h(\lambda)=\begin{vmatrix}\lambda+m_1e^{-\lambda\tau}+n_1 & m_2e^{-\lambda\tau}+n_2\\ -m_1 & \lambda-m_2e^{-\lambda\tau}+n_3\end{vmatrix}=\lambda^2+(n_1+n_3)\lambda+n_1n_3+[(m_1-m_2)\lambda+m_1n_3-m_2n_1+m_1n_2]\mathrm{e}^{-\lambda\tau} \tag{13}$$

式中

$$\left.\begin{aligned}m_1&=\frac{\beta k I_1(1-d_{\mathrm{A}})^{\tau}}{N};\quad m_2=\frac{\beta k S_1(1-d_{\mathrm{A}})^{\tau}}{N}\\ n_1&=\varphi+d_{\mathrm{A}}+\delta;\quad n_2=\delta;\quad n_3=\omega+d_{\mathrm{A}}\end{aligned}\right\} \tag{14}$$

令 $\lambda=\mathrm{i}\mu$，利用欧拉公式，式(13)可化为

$$h(\lambda)=-\mu^2+c_2+c_3\mu\sin(\mu\tau)+c_4\cos(\mu\tau)+[c_1\mu+c_3\mu\cos(\mu\tau)-c_4\sin(\mu\tau)]\mathrm{i} \tag{15}$$

式中

$$\left.\begin{aligned}&c_1=n_1+n_3;\ c_2=n_1n_3;\ c_3=m_1-m_2\\ &c_4=m_1n_3-m_2n_1+m_1n_2\end{aligned}\right\} \tag{16}$$

分离式(15)的实部和虚部，可得

$$\left.\begin{aligned}\mu^2-c_2&=c_3\mu\sin(\mu\tau)+c_4\cos(\mu\tau)\\ c_1\mu&=c_4\sin(\mu\tau)-c_3\mu\cos(\mu\tau)\end{aligned}\right\} \tag{17}$$

进而可得

$$\mu^4+(c_1^2-2c_2-c_3^2)\mu^2+c_2^2-c_4^2=0 \tag{18}$$

当 $R_0>1$ 时，式(18)有正根 μ_0，式(13)存在一对共轭复根 $\pm\mu_0\mathrm{i}$，结合式(17)可得

$$\tau_0=\frac{1}{\mu_0}\arccos\left(\frac{c_4\mu_0^2-c_2c_4-c_1c_3\mu^2}{c_4^2+c_3^2\mu_0^2}\right) \tag{19}$$

根据 Hopf 分岔理论可知：当 $\tau<\tau_0$ 时，式(1)表示的网络系统在有病毒平衡点处局部渐进稳定；当 $\tau\geqslant\tau_0$ 时，式(1)表示的网络系统在有病毒平衡点处振荡，出现 Hopf 分岔现象。证毕。

由本节稳定性分析可知：①基本再生数是操作系统病毒持续存在的阈值，当 $R_0\leqslant 1$ 时，网络能够靠自身免疫能力和操作系统切换消除操作系统病毒；当 $R_0>1$ 时，无论是否出现分岔现象，操作系统病毒总能持续存在；②操作系统病毒在传播过程中的攻击过程耗时对其传播有两方面影响，一方面，攻击过程耗时越长，被操作系统切换打断的概率就越大，感染成功率越低，另一方面，攻击过程耗时导致感染节点数出现振荡，不利于用户或网络管理员对当前网络安全环境做出正确判断。

对于存在感染时滞的操作系统病毒，操作系统切换对操作系统病毒传播的影响体现在 3 个方面：①操作系统切换使部分感染节点中的操作系统病毒失去运行环境，从而无法运行；②操作系统的切换会打断感染过程，降低易感节点被感染的概率；③操作系统切换频率决定着网络中两类操作系统的比例，

OS-A 的数量越少，感染节点数也越少。

3　操作系统病毒抑制策略

抑制网络中操作系统病毒的传播，需要重点解决 2 个问题：①调整的度，现有平台动态目标防御技术虽然能实现异构平台之间的数据、应用迁移，但是非自发的操作系统切换会同步导致用户业务的损失，相关技术的部署和实施需要付出额外的成本，因此需要把握操作系统切换的度，尽量避免过高频率的切换；②当 $R_0>1$ 且 $\tau>\tau_0$ 时，网络系统在有病毒平衡点处振荡，出现 Hopf 分岔现象，网络环境安全状态难以判决，也无法根据网络安全状态实施针对性防御。本节结合基本再生数和稳定性分析，设计基于操作系统切换频率调整的病毒抑制策略。

操作系统切换频率参数 d_A 和 d_O 都能影响操作系统病毒的规模。其中，调整 d_O 仅改变了网络中不同操作系统所占的比例，而调整 d_A 则能加速感染节点平台的切换，使感染过程更大概率被打断以及改变不同操作系统的比例，本文通过调整 d_A 抑制操作系统病毒传播。根据定理 1，当 $R_0<1$ 时，网络能消除操作系统病毒，则参数 d_A 需要满足

$$d_O(d_A+\delta)\beta k(1-d_A)^{\tau}-(d_A+d_O)(d_A+\omega)(d_A+\delta+\varphi)<1 \quad (20)$$

当 $R_0>1$ 且 $\tau>\tau_0$ 时，感染节点数存在振荡，难以估计网络中的感染节点数，因此首先需要设法消除这种振荡，对网络安全环境进行估计，然后再根据式(20)计算抑制操作系统病毒传播所需的参数配置。由定理 2 的证明过程可知，τ_0 与操作系统切换频率相关，在抑制操作系统病毒传播过程中，可先对参数 d_A 进行小幅度调整并实时监测网络中病毒传播情况，一旦感染节点数相对稳定，则根据当前病毒传播情况进一步调整相关参数。基于此分析，设计抑制操作系统病毒传播的流程如下。

输入：微调值 m，振荡判定阈值 ΔI，反馈时间 ΔT。

步骤 1　获取一段时间(ΔT)内网络中感染节点数。

步骤 2　如果该时段内感染节点数的极差大于 ΔI，则认定存在振荡，采取步骤 3，否则采取步骤 4。

步骤 3　若 ΔT 内网络中感染节点数的极差大于 ΔIN，则认为仍存在振荡行为，$d_A=d_A+m$，返回步骤 1。

步骤 4　若 ΔT 内网络中感染节点数的极差不大于 ΔIN，则认为感染节点数基本稳定，根据当前感染节点数，估计参数，根据式(20)计算消除病毒所需阈值。

步骤 5　选取恰当的 d_A，对网络进行调整，直至网络恢复至安全状态。

4　仿真分析

通过仿真测试时滞 τ 和切换频率 d_A 对病毒传播的影响，验证所提病毒抑制策略的有效性。设基本参数如下：$N=2\ 000$，$k=16$，$\omega=0.08$，$d_A=0.01$，$d_O=0.09$，$\delta=0.1$，$\varphi=0.2$。设单位时间为 h，根据式(1)所示动力学方程模拟病毒传播过程的节点数变化时，会出现节点数为小数的情况，考虑实际病毒传播过程中，网络任意状态节点数均为整数，仿真结果中对节点数均做整数化处理。

4.1　时滞对病毒传播的影响

令 $\beta=0.015$，对任意的感染时滞 τ，均有 $R_0<1$，根据定理 1，网络在无病毒平衡点处全局渐进稳定。$\beta=0.015$ 时，不同感染时滞下感染节点数的变化曲线如图 2 所示。可以看出，当 $R_0<1$ 时，感染时滞仅造成感染节点数变化上的延迟，尽管不同时滞下的感染节点数变化趋势不同，但网络最终能够在无病毒平衡点处达到稳定。

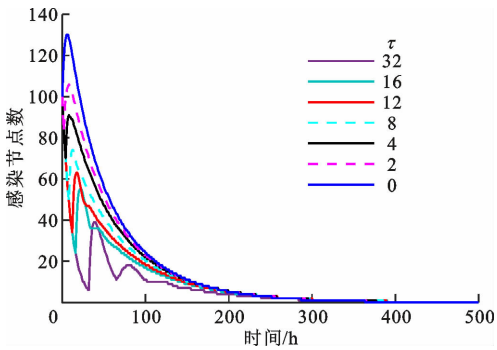


图 2　$\beta=0.015$ 时不同感染时滞下感染节点数的变化曲线

令 $\beta=0.08$，当 $\tau<150.6$ 时，$R_0>1$。当 $\tau\leqslant 7.9$ 时，$\tau<\tau_0$，网络在有病毒平衡点处局部渐进稳定；当 $\tau\geqslant 8$ 时，$\tau>\tau_0$，网络在有病毒平衡点附近振荡。$\beta=0.08$ 时，不同感染时滞下 τ_0 的变化曲线如图 3 所示，不同感染时滞下感染节点数的变化曲线如图 4 和图 5 所示。表 1 为不同感染时滞 τ 下[200,500]h 时间段内的平均感染节点数 $\bar{I}$。由图 3～5 可知，τ_0 随着 τ 的变化而变化。由图 4 和表 1 可知，感染时滞低于 τ_0 时，时滞仅影响网络中平衡点的位置和传播趋势，但网络最终仍可稳定在特定平衡点附近。由图 5 和表 1 可知，感染时滞 τ 会影响 $R_0>1$ 时的病毒传播，当感染时滞较高时，感染节点数会出现周

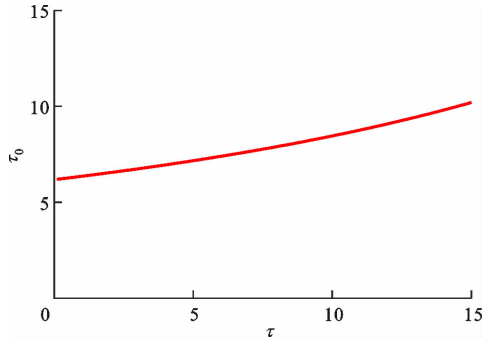


图 3 τ_0 随 τ 的变化曲线

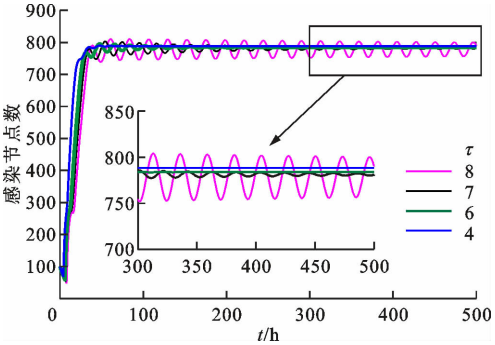


图 4 $\beta=0.08$ 时低感染时滞下感染节点数的变化曲线

期性振荡，随着感染时滞的降低，感染节点数会随之变大。综上可知，关于感染时滞 τ 的仿真结果与定理 2 的理论分析结果一致。

表 1 不同感染时滞下的平均感染节点数

τ	4	6	7	8	9	12	16	32
$\bar{I}$	789	784	781	779	772	742	728	711

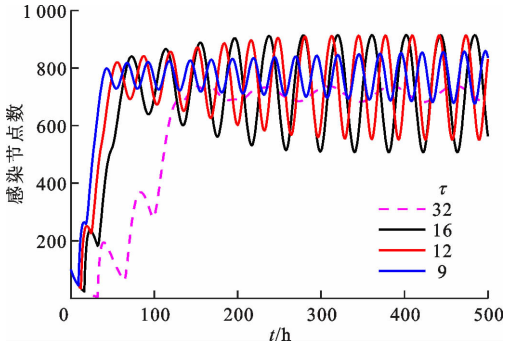
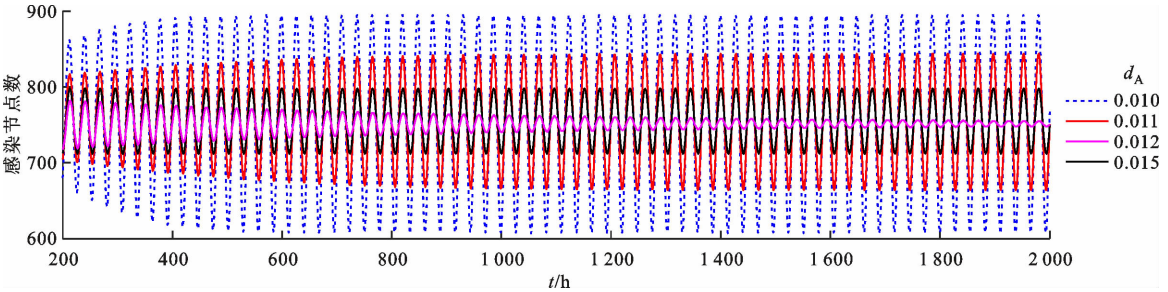


图 5 $\beta=0.08$ 时高感染时滞下感染节点数的变化曲线

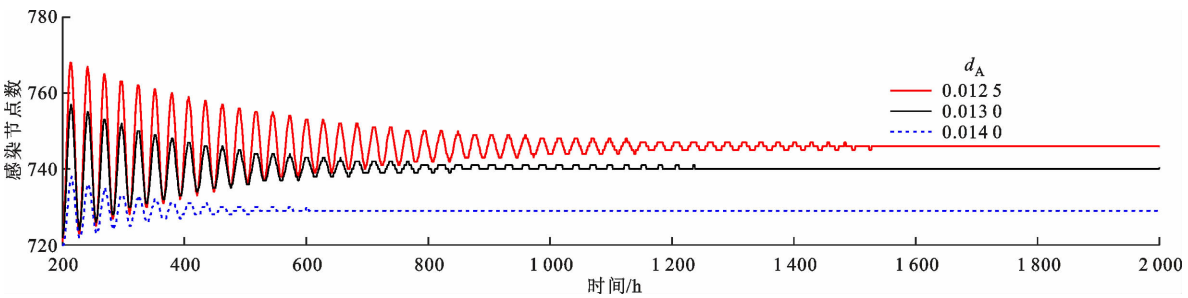
本小节仿真结果表明，R_0 和 τ_0 是网络中病毒传播的阈值，感染时滞对网络中病毒传播的影响有 2 个方面：①感染时滞会影响网络中感染节点的数量，感染时滞表示感染过程耗时，这一过程耗时越长，则被操作系统切换打断的概率越大，相应地感染成功率越低，感染节点数越低；②感染时滞较高时，即使感染率完全相同，平均感染节点数也相差不大，但由于存在振荡现象，无法根据某一时刻的感染节点数判定网络的安全环境，为抑制病毒传播带来困难。

4.2 操作系统切换频率对病毒传播的影响

令 $\beta=0.08$，$\tau=10$。结合定理 1、定理 2、式(19)(20)计算可得：当 $d_A\leqslant 0.012$ 时，感染节点数出现振荡；当 $0.012<d_A<0.070\ 4$ 时，网络在有病毒平衡点稳定；当 $d_A\geqslant 0.070\ 4$ 时，网络在无病毒平衡点稳定。$\tau_0<11$ 和 $R_0<1.1$ 时的感染节点数变化曲线如图 6 和图 7 所示。



(a)低切换频率



(b)高切换频率

图 6 $\tau_0<11$ 时感染节点数的变化曲线

由图 6a 可知，当 $d_A \leqslant 0.012$ 时，网络中感染节点数表现出周期性振荡，无法稳定在特定位置。由图 6b 可知：当 $0.012 < d_A < 0.070\ 4$ 时，网络中感染节点传播过程仍然会出现波动，但波动幅度不断减小，直至在相应平衡线位置稳定；当 $d_A \geqslant 0.070\ 4$ 时，网络能稳定在无病毒平衡点附近，仿真结果与理论推导一致。综合图 6 可知，当 $\tau > \tau_0$ 网络存在振荡现象时，通过调整参数 d_A 能够减小振荡幅度，直至消除振荡现象。由图 7 可知，通过调整参数 d_A 能够改变平衡点的位置，甚至消除病毒。参数 d_A 表示网络中 OS-A 切换至其他操作系统的频率，这种切换能够移除网络中的感染节点、打断感染过程并调整不同操作系统的数量，对网络中病毒的传播有着较大影响。

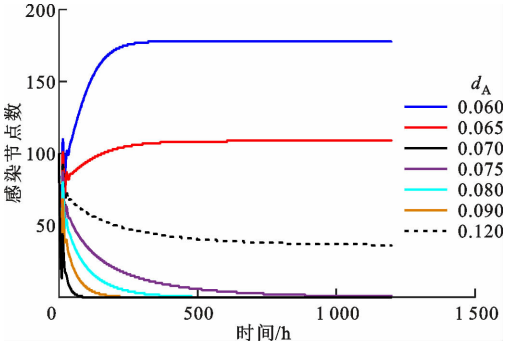


图 7　$R_0 < 1.1$ 时感染节点数的变化曲线

本小节仿真结果表明：①调整操作系统切换频率能够改变感染时滞的阈值 τ_0，当节点数存在振荡时，可调节操作系统切换频率增大 τ_0，使网络达到稳定状态，有利于对网络安全环境的判定；②调整操作系统切换频率能改变平衡点的位置，当病毒持续存在时，可增大操作系统切换频率，使网络平衡点从有病毒平衡点移动至无病毒平衡点，直至消除病毒。

4.3　病毒抑制策略有效性验证

根据感染节点在网络中的规模，可粗略估计相关参数，进而对网络进行相对精准的调整。对于存在感染时滞的操作系统病毒，根据理论分析和数值仿真可知，当 $\tau > \tau_0$ 时，感染节点数会发生振荡，不利于抑制操作系统病毒传播。取 $\beta = 0.08$，$\tau = 10$，此时 $R_0 = 4.107\ 6 > 1$，$\tau_0 = 8.459\ 8 < \tau$，仿真验证所提策略对病毒的抑制效果。未采取任何措施时，网络中病毒传播情况如图 8 所示，可以看出，操作系统病毒在网络中能够持续存在，且存在振荡现象。

考虑振荡对网络安全环境评估的负面影响，首先尝试消除网络中的振荡现象。按照所提策略，在当 $R_0 > 1$，$\tau > \tau_0$ 时，可首先对参数 d_A 进行微调，当

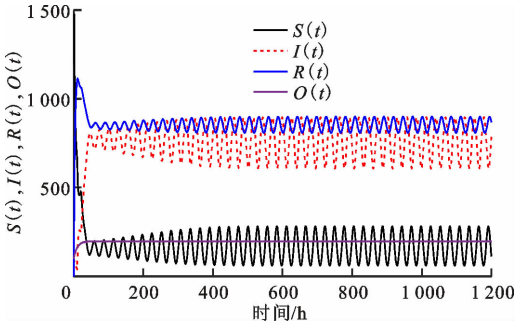


图 8　实施抑制策略前病毒传播情况

振荡消除后再根据式(20)进一步调整。设 $\Delta T = 200$，$m = 0.001$，$\Delta I = 1\%$，按照本文策略对参数 d_A 进行调整。d_A 的变化如图 9 所示，τ_0 随 d_A 的变化如图 10 所示，抑制策略执行过程中病毒传播情况如图 11 所示。

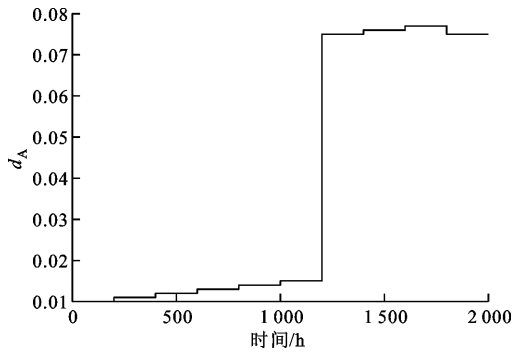


图 9　本文策略下 d_A 的变化曲线

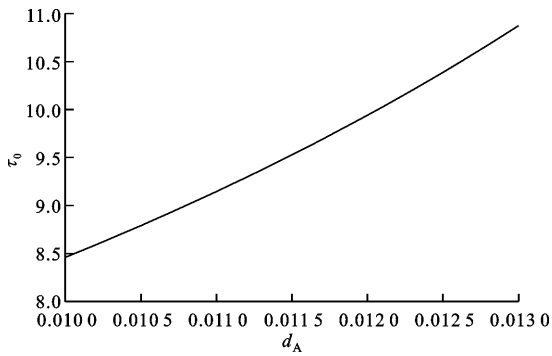
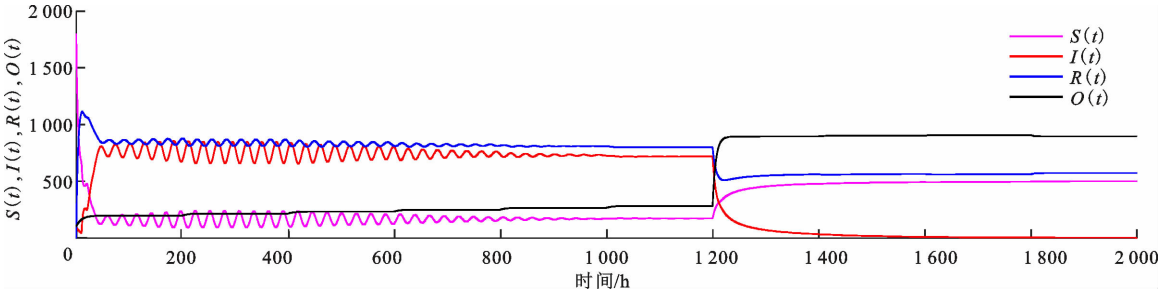
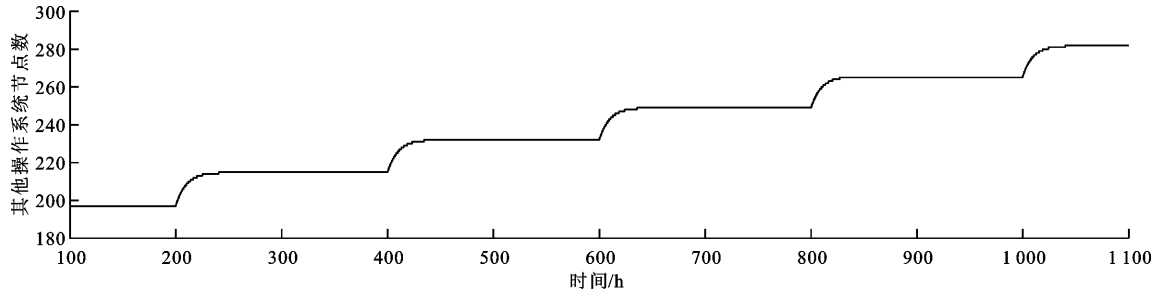


图 10　本文策略下 τ_0 随 d_A 的变化曲线

由图 10 可知，初始状态下，时滞阈值低于当前时滞，网络中节点数出现如图 11a 所示的周期性振荡，且振荡幅度大于设定的阈值。为消除振荡，进行了图 9 中[200，1 200] h 时间段所示的操作系统迁移频率的小幅度提升，使相应时间段内振荡幅度逐渐减小，如图 11a 所示，并且使其他操作系统节点呈阶梯变化，如图 11b 所示。3 次微调后，操作系统切换频率为 0.013，已经满足条件 $\tau < \tau_0$，能够消除网络中感染节点数的振荡。但是，振荡消除的表现为



(a)网络节点数变化



(b)[100,1100] h 时间段内其他操作系统节点数变化

图 11 本文策略下网络节点数的变化曲线

振荡幅度逐渐减小直至消失。因此,在振荡未完全消失且幅度仍大于所设定阈值时,网络依旧判定振荡存在,所以再次进行了两次操作系统切换频率的微调。振荡消除后,由式(20)计算可得,$d_A \leqslant 0.704$ 时网络理论上能够消除病毒。仿真中取 $d_A = 0.075$。抑制病毒传播过程中,感染节点数变化超过设定的阈值,这一过程中 d_A 存在小幅调整,但随着感染节点的消除再次恢复。

本小节结果表明,感染时滞和节点操作系统的切换影响着网络中病毒传播的稳定性。一方面,感染时滞和操作系统的切换频率影响网络平衡点的取值;另一方面,当网络存在有病毒平衡点时,感染时滞和操作系统切换频率共同影响着时滞阈值,当感染时滞高于这一阈值时会导致网络中 S、I 和 R 状态节点数的振荡,影响对当前网络安全态势的感知。因此,在网络中针对性部署平台动态目标防御技术,动态调整网络中不同操作系统之间的切换频率,有利于有效评估网络安全态势,抑制操作系统病毒的传播。

5 结 论

(1)基本再生数是病毒感染能力和网络免疫能力的综合体现,其阈值为 1,小于该阈值时,网络能消除病毒,否则病毒持续存在。基本再生数与感染时滞负相关,与操作系统切换频率正相关。

(2)感染时滞的阈值随操作系统切换频率和感染时滞动态变化,且正相关。在基本再生数大于 1 的情况下,当感染时滞小于该阈值时,网络稳定在特定平衡点附近,当大于该阈值时,网络在平衡点附近周期性振荡。

(3)操作系统病毒防御过程中,感染时滞无法人为调节,可调整操作系统迁移频率消除振荡,抑制操作系统病毒传播。

参考文献:

[1] WU Jiangxing, LI Jianhua, JI Xinsheng. Security for cyberspace: challenges and opportunities [J]. Frontiers of Information Technology & Electronic Engineering, 2018, 19(12): 1459-1461.

[2] SULTANA N, CHILAMKURTI N, PENG Wei, et al. Survey on SDN based network intrusion detection system using machine learning approaches [J]. Peer-to-Peer Networking and Applications, 2019, 12(2): 493-501.

[3] ALI M Q, AL-SHAER E, SAMAK T. Firewall policy reconnaissance: techniques and analysis [J]. IEEE Transactions on Information Forensics and Security, 2014, 9(2): 296-308.

[4] 周余阳, 程光, 郭春生, 等. 移动目标防御的攻击面动态转移技术研究综述 [J]. 软件学报, 2018, 29(9): 2799-2820.
ZHOU Yuyang, CHENG Guang, GUO Chunsheng, et al. Survey on attack surface dynamic transfer tech-

nology based on moving target defense [J]. Journal of Software, 2018, 29(9): 2799-2820.

[5] 仝青，张铮，张为华，等. 拟态防御 Web 服务器设计与实现 [J]. 软件学报，2017，28(4)：883-897.
TONG Qing, ZHANG Zheng, ZHANG Weihua, et al. Design and implementation of mimic defense web server [J]. Journal of Software, 2017, 28(4): 883-897.

[6] KANELLOPOULOS A, VAMVOUDAKIS K G. A moving target defense control framework for cyber-physical systems [J]. IEEE Transactions on Automatic Control, 2020, 65(3): 1029-1043.

[7] CHO J H, SHARMA D P, ALAVIZADEH H, et al. Toward proactive, adaptive defense: a survey on moving target defense [J]. IEEE Communications Surveys & Tutorials, 2020, 22(1): 709-745.

[8] EL-SAYED A M A, ARAFA A A M, KHALI M, et al. A mathematical model with memory for propagation of computer virus under human intervention [J]. Progress in Fractional Differentiation and Applications, 2016, 2(2): 105-113.

[9] 王刚，冯云，陆世伟，等. 多操作系统异构网络的病毒传播模型和安全性能优化策略 [J]. 电子与信息学报，2020，42(4)：972-980.
WANG Gang, FENG Yun, LU Shiwei, et al. Virus propagation model and security performance optimization strategy of multi-operating system heterogeneous network [J]. Journal of Electronics & Information Technology, 2020, 42(4): 972-980.

[10] LIU Lijun, WEI Xiaodan, ZHANG Naimin. Global stability of a network-based SIRS epidemic model with nonmonotone incidence rate [J]. Physica: A Statistical Mechanics and Its Applications, 2019, 515: 587-599.

[11] 张春明，陈冬垚. 广义网络上的计算机病毒传播模型 [J]. 数学物理学报，2019，39(2)：402-416.
ZHANG Chunming, CHEN Dongyao. Propagation of computer virus on generalized networks [J]. Acta Mathematica Scientia, 2019, 39(2): 402-416.

[12] 王刚，陆世伟，胡鑫，等. “去二存一”混合机制下的病毒扩散模型及稳定性分析 [J]. 电子与信息学报，2019，41(3)：709-716.
WANG Gang, LU Shiwei, HU Xin, et al. Virus propagation model and stability under the hybrid mechanism of “two-go and one-live” [J]. Journal of Electronics & Information Technology, 2019, 41(3): 709-716.

[13] 叶志勇，刘原，吴用. 具有非单调传染率的 SIQR 传染病模型的稳定性分析 [J]. 生物数学学报，2014，29(1)：105-112.
YE Zhiyong, LIU Yuan, WU Yong. Stability of a SIQR model with nonmonotone incidence rate [J]. Journal of Biomathematics, 2014, 29(1): 105-112.

[14] 苏飞，林昭文，马严，等. IPv6 网络环境下的蠕虫传播模型研究 [J]. 通信学报，2011，32(9)：51-60.
SU Fei, LIN Zhaowen, MA Yan, et al. Research on worm propagation model in IPv6 networks [J]. Journal on Communications, 2011, 32(9): 51-60.

[15] ZHOU Tao, LIU Jinguo, BAI Wenjie, et al. Behaviors of susceptible-infected epidemics on scale-free networks with identical infectivity [J]. Physical Review: E, 2006, 74(5): 056109.

[16] 王昕炜，彭海军，钟万勰. 具有潜伏期时滞的时变 SEIR 模型的最优疫苗接种策略 [J]. 应用数学和力学，2019，40(7)：701-712.
WANG Xinwei, PENG Haijun, ZHONG Wanxie. Optimal vaccination strategies for a time-varying SEIR epidemic model with latent delay [J]. Applied Mathematics and Mechanics, 2019, 40(7): 701-712.

[17] SONG Haitao, LIU Shengqiang, JIANG Weihua. Global dynamics of a multistage SIR model with distributed delays and nonlinear incidence rate [J]. Mathematical Methods in the Applied Sciences, 2016, 40(6): 21532164

[18] LI S S, LI X Z, CHAN S C. Chaotic time-delay signature suppression with bandwidth broadening by fiber propagation [J]. Optics Letters, 2018, 43(19): 4751-4754.

[19] 张晓潘，袁凌云. 具有时滞扩散作用的无线传感网络病毒传播模型的振荡动力学研究 [J]. 计算机科学，2017，44(S1)：390-394.
ZHANG Xiaopan, YUAN Lingyun. Oscillatory behaviors of malware propagation model in wireless sensor networks with time delays and reaction-diffusion terms [J]. Computer Science, 2017, 44(S1): 390-394.

[20] ZHU Linhe, GUAN Gui, LI Yimin. Nonlinear dynamical analysis and control strategies of a network-based SIS epidemic model with time delay [J]. Applied Mathematical Modelling, 2019, 70: 512-531.

（编辑　陶晴）