零日病毒时滞传播模型及稳定性分析

仇铭阳，王　刚*，孟庆微，马润年
(空军工程大学信息与导航学院，西安，710077)

摘要　考虑感染时滞因素对零日病毒传播的影响，研究平台动态防御背景下零日病毒时滞传播模型及其稳定性。首先，分析了时滞因素对零日病毒传播的影响，引入平台动态防御模式，建立了零日病毒时滞传播 SIZRO 模型；其次，根据 Lyapunov 稳定性判据，给出了系统平衡点的局部稳定性证明，分析了基本再生数 R_0 及其对零日病毒传播的影响。最后，将 SIZDR 模型与 SIZRO 模型中感染节点数量进行比对，证明利用平台动态防御解决零日病毒传播问题的可行性。理论分析与仿真结果表明，所提模型能客观反映零日病毒时滞传播及免疫规律，平台动态防御可有效提升系统对零日病毒的防御效果。

关键词　零日病毒；时滞；传播模型；平台动态防御；稳定性
DOI　10.3969/j.issn.1009-3516.2022.02.014
中图分类号　TP309.5　　**文献标志码**　A　　**文章编号**　1009-3516(2022)02-0090-07

An Analysis of Zero-Day Virus Transmission Model with Time-Delay and Stability

QIU Mingyang, WANG Gang*, MENG Qingwei, MA Runnian
(Information and Navigation School, Air Force Engineering University, Xi'an 710077, China)

Abstract　In consideration of the influence of infection time-delay on the transmission of zero-day virus, the time-delay transmission model of zero-day virus and its stability under the background of platform dynamic defense are studied, the following measures should be taken in the research. Firstly, the influence of time-delay on the propagation of zero-day virus is analyzed, and the Dynamic Platform Defense model is introduced, and a SIZRO model of zero-day virus propagation is established. Secondly, according to the Lyapunov stability criterion, the local stability of equilibrium point in system is proved, and the basic reproduction number and its effect on the zero-day virus transmission are analyzed. Finally, the number of infected nodes in SIZDR model being compared with that in SIZRO model, the feasibility of using platform dynamic defense to solve zero-day virus transmission problem is demonstrated. The theoretical analysis and simulation results show that the proposed model can objectively reflect the time-delay propagation and immune law of zero-day virus, and the Dynamic Platform Defense can effectively improve the defense effect of the system against zero-day virus.

Key words　zero-day virus; time-delay; propagation model; dynamic platform defense; stability

零日病毒是利用计算机平台中存在的零日漏洞　　发起攻击的一种网络病毒，和一般网络病毒相比，具

收稿日期：2021-07-13
作者简介：仇铭阳(1997—)，男，陕西西安人，硕士生，研究方向为网络空间安全。E-mail：1048087698@qq.com
通信作者：王　刚(1976—)，男，湖北黄冈人，教授，博士生导师，研究方向为网络空间安全，复杂网络建模。E-mail：wglxl@nudt.edu.cn

引用格式：*仇铭阳，王刚，孟庆微，等. 零日病毒时滞传播模型及稳定性分析[J]. 空军工程大学学报(自然科学版)，2022，23(2)：90-96. QIU Mingyang, WANG Gang, MENG Qingwei, et al. An Analysis of Zero-day Virus Transmission Model with Time-Delay and Stability[J]. Journal of Air Force Engineering University (Natural Science Edition), 2022, 23(2): 90-96.*

有潜伏性强和信息不对称的特点[1]。在零日病毒攻击中，攻击方可以利用对手计算机平台存在的零日漏洞，事先设计和部署网络攻击行动，较之防御方具有建立在信息优势基础上的决策和攻击优势，同时，由于传统防御工作周期长、工作量大，零日攻防中攻击方的优势更加明显[2-4]。此外，和多数传统病毒的“直接”“无差别”感染模式相比较，零日病毒攻击通过分析目标主机的资源信息，可选择满足特定条件的主机和恰当时机发起攻击，具有隐蔽性和针对性。零日病毒从存在到激活都存在时间差，也就是目前高级持续性威胁中普遍存在的潜伏性和潜伏周期，因此时滞问题也是零日病毒需要重点关注的。

从近年来零日攻击相关研究情况分析，相关成果主要集中两个方面。一是零日病毒传播机理和传播行为建模。文献[5]分析了零日病毒作用机理和基本流程，在经典 SIR(susceptible infected recovered, SIR)模型[6-7]基础上，提出了零日病毒传播 SIZDR(susceptible infected zero-day damaged recovered, SIZDR)模型。文献[8]借鉴传染病动力学理论以不同安全状态网络节点密度定义网络攻防态势，分析网络节点安全状态转移路径；以网络勒索病毒攻防博弈为例，使用 NetLogo 多 Agent 仿真工具开展不同场景下攻防态势演化趋势对比实验。针对零日病毒在内的新型病毒潜伏特性。文献[9]引入潜伏和隔离状态，提出了 SEIQRS(susceptible escape infected quarantine remove susceptible)模型，研究了潜伏隔离机制下的病毒传播规律。二是零日病毒的防御方法和策略。文献[10]引入沙盒技术，提出了一种基于信息系统状态概率排序的分析模型，通过模型分析、跟踪和评估系统状态从而识别并阻止可能的零日攻击。文献[11]将低级操作码、应用程序许可和专有的 Android API 包作为输入值，利用深度学习神经网络进行训练，实现了可在无须了解恶意特征的情况下，发掘疑似零日攻击行为。文献[12]考虑文档类型零日漏洞检测效果不佳，提出了一个以恶意文档检测为核心，漏洞特征判断为辅助的文档类型 0Day 漏洞检测模型，通过该模型大大提高了对文档类零日漏洞的检测准确率。文献[13]为解决零日攻击破坏性强的这一特点，提出了基于 NIDPS 和蜜罐的零日攻击伤害最小化混合系统，实现了防御效果的最大化。以操作系统病毒为例，文献[14]分析了病毒的时滞特性和感染力强等特点，引入动态防御理念和平台动态防御模式，提出了操作系统病毒的时滞传播模型及抑制策略，研究了时滞导致的系统演化分叉行为和操作系统跳变对病毒传播抑制的有效性。总体上，前期研究主要关注零日病毒传播的一般规律和防御模式，对零日病毒传播和防御的研究还存在需要持续深入。考虑到零日病毒的潜伏特性和时滞因素的影响，通过传播机理分析和时滞模型求解，研究时滞可能造成的系统演化分叉行为和条件。文献[15]提出了一类具有 2 种不同时滞的病毒传播模型，分析了模型稳定性及系统 Hopf 分岔行为产生条件。文献[16]在 SEIR(susceptible escape infected remove)模型[17]的基础上，考虑感染及恢复过程中存在时延的情况，提出了 SEIR-KS(susceptible exposed infected kill signals recovered)模型，通过模型稳定性分析及 Hopf 分岔行为分析，给出了病毒防御方法。其次，适应网络攻防发展趋势，借鉴操作系统病毒传播抑制策略和操作系统跳变模式[14]，将动态防御渗透到病毒传播和免疫的行为建模和具体防御实践中。文献[18]在 SIQRS(susceptible infected quarantine remove susceptible)模型的基础上，考虑防病毒软件杀死病毒的过程存在时滞，提出了时滞 SIQRS 传播模型并研究了模型稳定性。张子振等人[19]考虑隔离病毒节点存在时滞这一情况，引入处理时滞，研究了无线传感网络中蠕虫病毒的传播问题。

基于此，论文研究平台动态防御背景下零日病毒时滞传播模型及其稳定性。

1　零日病毒时滞传播模型

根据对零日病毒传播机理[5]的分析，结合平台动态防御的思想，零日病毒扩散及免疫过程可简化为初始感染、病毒传播、病毒发作及损毁和平台迁移 4 个阶段。与零日病毒传播机理不同，零日病毒时滞传播及免疫的过程有所变化。在病毒传播阶段，目标主机感染零日病毒的过程中存在耗时 τ。在零日阶段，将毁损状态转化为易感状态的过程融入到零日状态转化为易感状态的过程中。在平台迁移阶段，防御方利用平台迁移技术以一定的概率将目标主机中原有平台迁移至其他平台。由于平台的转变，使得针对原有平台的零日攻击无法正常进行，从而达到了免疫的效果。结合以上论述，做出如下假设：①网络仅存在一种零日病毒，且该病毒仅能感染一种特定运行平台下的目标主机；②感染耗时为 τ。感染过程一旦中断，零日病毒无法成功感染该目标主机。

SIZDRS 模型[5]是针对零日病毒传播机理提出的模型，在对零日病毒传播及免疫过程的分析基础

上,对 SIZDRS 模型进行了改进。本文重新定义了零日病毒执行阶段,同时引入了异构平台状态。提出了 SIZRO 模型,其状态转移关系见图 1。

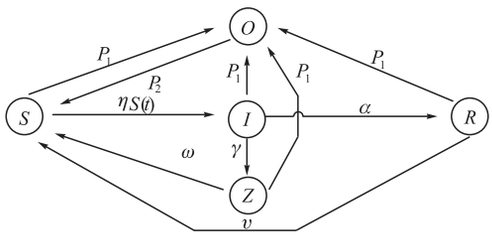


图 1 SIZRO 病毒传播及免疫模型

在 SIZDRS 模型的基础上,针对新模型改进部分进行说明:

1)易感状态 S→初始感染状态 I。易感状态 S 节点与零日状态 Z 节点接触,经过一定时间间隔 τ 后,转化为初始感染状态。其中,$Z(t-\tau)$表示考虑零日病毒感染时滞 τ 的情况下在 t 时刻零日状态节点数量。

2)零日状态 Z→易感状态 S。由于部分计算机核心系统被控制或部分由计算机操控的工控系统被破坏导致整个网络的性能下降,因此目标主机在被损毁后,相关操作人员将对已损坏的设备进行翻新或者使用新的设备。ω 代表了由毁损状态恢复为易感状态的恢复率。

3)易感状态 S、初始感染状态 I、零日状态 Z、免疫状态 R→其他平台状态 O。在平台迁移的过程中,防御方并不知悉网络中每一节点的感染情况。因此,防御方为了防御效益最大化,将对整个网络中的每一主机进行平台迁移。由于运行平台及环境的不同,针对原平台的零日攻击在其他平台上无法进行,从而达到免疫的效果。定义由原平台迁移至其他平台的迁移成功率为正向切换成功率 P_1。

4)其他平台状态 O→易感状态 S。处于其他平台状态的节点,在成功阻止零日病毒的攻击后,防御方将其他平台状态迁移至原平台状态,定义该过程中平台迁移成功率为反向切换成功率 P_2。

5)免疫状态 R→易感状态 S。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,或者由于用户更新系统等使具有免疫功能的节点重新转化为易感节点。υ 代表了免疫状态转化为易感状态的转化率。

设网络中节点总数 N 为各状态节点数量和,在病毒传播及免疫过程中保持不变,新增变量 $O(t)$表示 t 时刻其他节点状态节点的数量。根据条件可知,各状态数量之间满足:$R(t)=N-S(t)-I(t)-Z(t)-O(t)$。根据微分动力学原理,可得模型对应的动力学方程:

$$\begin{cases}\dfrac{\mathrm{d}S(t)}{\mathrm{d}t}=\dfrac{-\beta KS(t)Z(t-\tau)}{N}+\upsilon R(t)+\omega Z(t)+P_2O(t)-P_1S(t)\\ \dfrac{\mathrm{d}I(t)}{\mathrm{d}t}=\dfrac{\beta KS(t)Z(t-\tau)}{N}-\alpha I(t)-\gamma I(t)-P_1I(t)\\ \dfrac{\mathrm{d}Z(t)}{\mathrm{d}t}=\gamma I(t)-\omega Z(t)-P_1Z(t)\\ \dfrac{\mathrm{d}R(t)}{\mathrm{d}t}=\alpha I(t)-P_1R(t)-\upsilon R(t)\\ \dfrac{\mathrm{d}O(t)}{\mathrm{d}t}=P_1[S(t)+I(t)+Z(t)+R(t)]-P_2O(t)\end{cases} \tag{1}$$

2 稳定性分析

由式(1)求解可得平衡点 $\boldsymbol{P}^0(S_0,I_0,Z_0,R_0,O_0)$和 $\boldsymbol{P}^1(S_1,I_1,Z_1,R_1,O_1)$

$$\boldsymbol{P}^0(S_0,I_0,Z_0,R_0,O_0)=\left(\frac{P_2N}{P_1+P_2},0,0,0,\frac{P_1N}{P_1+P_2}\right)$$

$$\boldsymbol{P}^1(S_1,I_1,Z_1,R_1,O_1)=\left\{\frac{(P_1+\alpha+\gamma)(P_1+\omega)N}{\beta K\gamma},I_1,\frac{\gamma}{P_1+\omega}I_1,\frac{\alpha}{P_1+\upsilon}I_1,\frac{P_1N}{P_1+P_2}\right\} \tag{2}$$

式中:

$$I_1=\frac{P_1P_2\beta K\gamma-(P_1+\alpha+\gamma)(P_1+\omega)(P_1+P_2)P_1}{[(P_1+\upsilon)(P_1+\omega)(P_1+\alpha+\gamma)-(P_1\upsilon\alpha+\omega\upsilon\alpha+P_1\omega\gamma+\upsilon\omega\gamma)]}\cdot\frac{(P_1+\upsilon)(P_1+\omega)\cdot N}{\beta K\gamma(P_1+P_2)} \tag{3}$$

显然,无病毒平衡点始终存在。由式(3)可得式(1)的基本再生数 $R_0=\dfrac{P_2\beta K\gamma}{(P_1+\alpha+\gamma)(P_1+\omega)(P_1+P_2)}$。当 $R_0\leqslant 1$ 时,有病毒平衡点 $\boldsymbol{P}^1(S_1,I_1,R_1,Z_1,O_1)$不存在;当时 $R_0>1$,有病毒平衡点存在 $\boldsymbol{P}^1(S_1,I_1,R_1,Z_1,O_1)$。

引理 1 当 $t\to\infty$时,$S(t)\leqslant S_0$。

证明:设 $A(t)=S(t)+I(t)+R(t)+Z(t)$,式(1)可进一步表示为:

$$\begin{aligned}\frac{\mathrm{d}A(t)}{\mathrm{d}t}&=-P_1A(t)+P_2O(t)\\ \frac{\mathrm{d}O(t)}{\mathrm{d}t}&=P_1A(t)-P_2O(t)\end{aligned} \tag{4}$$

令$\dfrac{\mathrm{d}A(t)}{\mathrm{d}t}=0$,$\dfrac{\mathrm{d}O(t)}{\mathrm{d}t}=0$,求解可得式(4)的唯一平衡点 $\boldsymbol{P}(A,O)=\left(\dfrac{P_2N}{P_1+P_2},\dfrac{P_1N}{P_1+P_2}\right)$,对应的雅克比矩阵为:

$$\boldsymbol{J}=\begin{bmatrix}-P_1 & P_2\\ P_1 & -P_2\end{bmatrix} \tag{5}$$

相应的特征方程为：

$$\lambda(\lambda+P_1+P_2)=0 \tag{6}$$

由式(6)可得式(5)的 2 个特征根 $\lambda_1=0$ 和 $\lambda_2=-P_1-P_2$。显然，特征根为非正根，由劳斯稳定性判据可知，式(6)在平衡点处局部稳定。因此，当 $t\to\infty$ 时，有 $S(t)+I(t)+R(t)+Z(t)=P_2N/(P_1+P_2)$，进而可得 $S(t)=P_2N/(P_1+P_2)-I(t)-R(t)$，从而 $S(t)\leqslant S_0$。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 $P^0(S_0,I_0,R_0,Z_0,O_0)$ 处全局渐进稳定。

证明：定义 Lyapunov 函数

$$L(t)=\frac{\gamma}{P_1+\alpha+\gamma}\left[I(t)+\int_{t-\tau}^{t}\frac{\beta KS(x+\tau)Z(x)}{N}\mathrm{d}x\right]+Z(t) \tag{7}$$

对式(7)求导可得：

$$L'(t)=\frac{\gamma}{P_1+\alpha+\gamma}\left[\begin{aligned}&I'(t)+\frac{\beta KS(t+\tau)Z(t)}{N}\\&-\frac{\beta KS(t)Z(t-\tau)}{N}\end{aligned}\right]+Z'(t)=$$

$$\frac{\gamma}{P_1+\alpha+\gamma}\left[\begin{aligned}&\frac{\beta KS(t)Z(t-\tau)}{N}-(\alpha+\gamma+P_1)I(t)\\&+\frac{\beta KS(t+\tau)Z(t)}{N}-\frac{\beta KS(t)Z(t-\tau)}{N}\end{aligned}\right]+$$

$$\gamma\cdot I(t)-(P_1+\omega)Z(t)=$$

$$\frac{\gamma}{P_1+\alpha+\gamma}\cdot\frac{\beta KS(t+\tau)Z(t)}{N}-(P_1+\omega)Z(t)=$$

$$\left[\frac{\gamma}{P_1+\alpha+\gamma}\frac{\beta KS(t+\tau)}{N}-(P_1+\omega)\right]Z(t) \tag{8}$$

由引理 1 可知：

$$L'(t)\leqslant Z(t)(P_1+\omega)(R_0-1) \tag{9}$$

当 $R_0\leqslant 1$ 时，$L'(t)\leqslant 0$，当且仅当时等号成立。根据 LaSalle 不变原理，式(1)表示的网络系统再无病毒平衡点 $\boldsymbol{P}^0(S_0,I_0,R_0,Z_0,O_0)$ 处全局渐进稳定。证毕。

定理 2　当 $R_0>1$ 时，系统在有病毒平衡点处局部渐进稳定。

证明：根据引理 1，式(1)可化简为：

$$\begin{cases}\dfrac{\mathrm{d}S(t)}{\mathrm{d}t}=\dfrac{-\beta KS(t)Z(t-\tau)}{N}+\\\upsilon\left[\dfrac{P_2}{P_1+P_2}N-S(t)-I(t)-Z(t)\right]+\\\omega Z(t)+\dfrac{P_1P_2}{P_1+P_2}\cdot N-P_1S(t)\\\dfrac{\mathrm{d}I(t)}{\mathrm{d}t}=\dfrac{\beta KS(t)Z(t-\tau)}{N}-\alpha I(t)-\gamma I(t)-P_1I(t)\\\dfrac{\mathrm{d}Z(t)}{\mathrm{d}t}=\gamma I(t)-\omega Z(t)-P_1Z(t)\end{cases} \tag{10}$$

对应的特征方程为：

$$\boldsymbol{h}(\lambda)=\begin{vmatrix}\lambda+P_1+\upsilon & \lambda+\alpha+\gamma+P_1+\upsilon & \upsilon-\omega\\\dfrac{-\beta KZ_1}{N} & \lambda+\alpha+\gamma+P_1 & \dfrac{-\beta KS_1}{N}e^{-\lambda\tau}\\0 & -\gamma & \lambda+\omega+P_1\end{vmatrix}=$$

$$\lambda^3+(e+f+a)\lambda^2+(ef+ae+af+bm)\lambda+aef+bmf+mc\gamma-(n\gamma\lambda+an\gamma)e^{-\lambda\tau} \tag{11}$$

式中：

$$\begin{cases}m=\beta KZ_1/N,n=\beta KS_1/N\\a=P_1+\upsilon,b=\alpha+\gamma+P_1+\upsilon\\c=\upsilon-\omega,\ e=\alpha+\gamma+P_1\\f=P_1+\omega\end{cases} \tag{12}$$

令 $\lambda=\mathrm{i}\mu$，利用欧拉公式并分离实部和虚部，式(11)可化为：

$$\begin{cases}c_3-c_1\mu^2=c_4\mu\sin(\mu\tau)+c_5\cos(\mu\tau)\\c_2\mu-\mu^3=c_4\mu\cos(\mu\tau)-c_5\sin(\mu\tau)\end{cases} \tag{13}$$

式中：

$$\begin{cases}c_1=e+f+a\\c_2=ef+ae+af+bm\\c_3=aef+bmf+mc\gamma\\c_4=n\gamma,\ c_5=an\gamma\end{cases} \tag{14}$$

进而可得：

$$\mu^6+(c_1^2-2c_2)\mu^4-(2c_1c_3+c_4^2-c_2^2)\mu^2+c_3^2-c_5^2=0 \tag{15}$$

令 $k=\mu^2$，式(15)可化为：

$$k^3+(c_1^2-2c_2)k^2-(2c_1c_3+c_4^2-c_2^2)k+c_3^2-c_5^2=0 \tag{16}$$

令 $f(k)=k^3+(c_1^2-2c_2)k^2-(2c_1c_3+c_4^2-c_2^2)k+c_3^2-c_5^2$，对 $f(k)$ 求导得：

$$f'(k)=3k^2+2(c_1^2-2c_2)k-(2c_1c_3+c_4^2-c_2^2) \tag{17}$$

结合式(1)中参数取值范围计算可知，$c_1^2-2c_2>0$，$-(2c_1c_3+c_4^2-c_2^2)>0$。因此，当 $k>0$ 时，方程 $f'(k)>0$，对应式(16)单调递增；由于 $\lim\limits_{k\to+\infty}f(k)\to+\infty$，$c_3^2-c_5^2>0$，式(16)无正实根，式(1)在有病毒平衡点处不存在 Hopf 分岔现象。因此，当 $R_0>1$ 时，系统在有病毒平衡点处局部渐进稳定。证毕。

由以上分析可知：①基本再生数决定了网络系统中零日病毒存在与否。当 $R_0\leqslant 1$ 时，网络中不存在零日病毒，此时网络系统在无病毒平衡点 $\boldsymbol{P}^0(S_0,I_0,R_0,Z_0,O_0)$ 处局部渐近稳定；当 $R_0>1$ 时，零日病毒存在于网络之中且最终感染病毒计算机数量趋于稳定，此时系统在有病毒平衡点 $\boldsymbol{P}^1(S_1,I_1,R_1,Z_1,O_1)$ 处局部渐近稳定。②零日病毒的感染时滞对网络系统稳定时的传播规模没有影响。③网络中两类平台的数量仅取决于平台切换概率(正、反向切

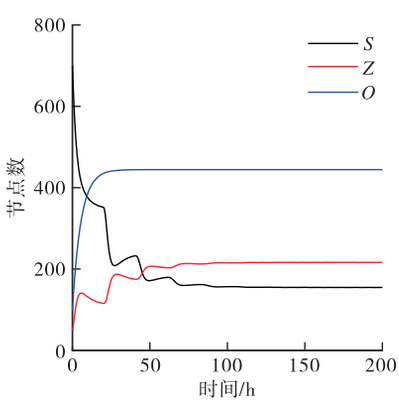
换率),无论网络中是否存在病毒,处于原有平台和其他平台的节点数量始终保持不变。

3 仿真分析

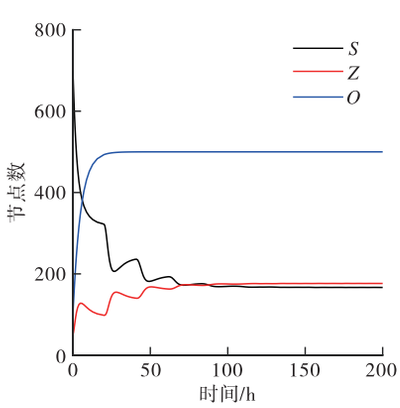
仿真分析平台迁移成功率和时滞因子对零日病毒传播的影响,验证模型及其稳定性。平台迁移成功率可通过完善硬件及软件来进行调节,感染时滞因子主要是病毒自身特性。参照实验[5],本文实验采用 MATLAB2019 进行模拟仿真,利用仿真软件中求解时滞微分方程的工具 ODE45,对动力学方程组进行求解,并成图表示结果。其中,微分方程求解间隔为 50,模型中各个参数的设置如下:$\beta=0.6$, $K=6$, $\alpha=0.2$,$\upsilon=0.5$,$\gamma=0.6$,$P_1=0.08$,$P_2=0.15$,$\omega=0.3$,设节点总数 $N=1\ 000$,初始状态下不同状态节点数为$(S_0,I_0,Z_0,R_0,O_0)=(700,50,50,100,100)$。在仿真验证过程中,用易感状态、零日状态和异构平台状态等 3 类状态的节点数量变化,动态演示零日病毒传播规律及平台迁移的免疫效果。

3.1 平台切换成功率

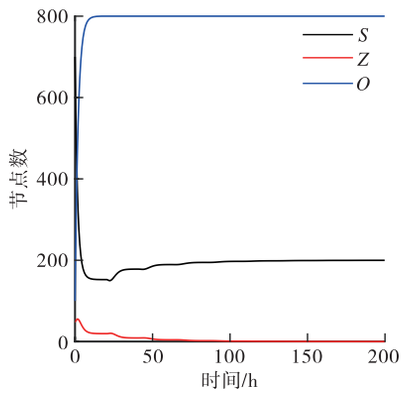
调整平台切换成功率 P_1 和 P_2 验证其对病毒传播的影响及免疫效果。分别令 $P_1=0.08,0.1,0.4$,图 2 所示为不同正向切换概率对应的系统状态。



(a) P_1=0.08



(b) P_1=0.1

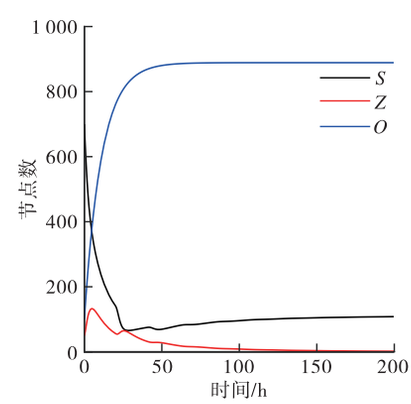


(c)P_1=0.4

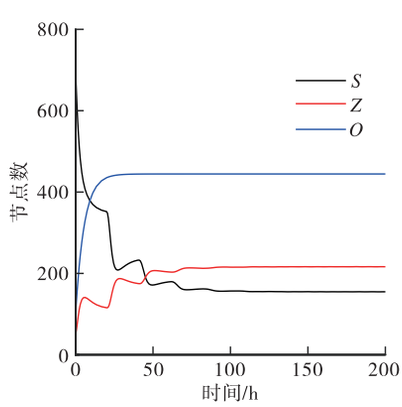
图 2 不同 P_1 对应的系统状态

图 2(a)、(b)、(c)分别对应 $P_1=0.08,0.1,0.4$ 的系统状态。仿真结果表明,当 $P_1=0.4(R_0<1)$ 时,系统在平衡点 $\boldsymbol{P}^0(200,0,0,0,800)$ 处局部渐进稳定;当 $P_1=0.1(R_0>1)$ 时,系统在 $\boldsymbol{P}^1(167,118,176,39,500)$ 处局部渐进稳定;当 $P_1=0.08(R_0>1)$ 时,系统在 $\boldsymbol{P}^1(155,137,216,47,445)$ 处局部渐进稳定;当系统在局部渐进稳定平衡点 $\boldsymbol{P}^1$ 处时,零日状态节点数随着 P_1 的增大而减小。可见,正向切换率越大,零日病毒在传播及免疫过程中成功入侵目标主机的概率越小,通过调节正向切换率 P_1,可以有效抑制零日病毒的传播,达到较好的免疫效果。

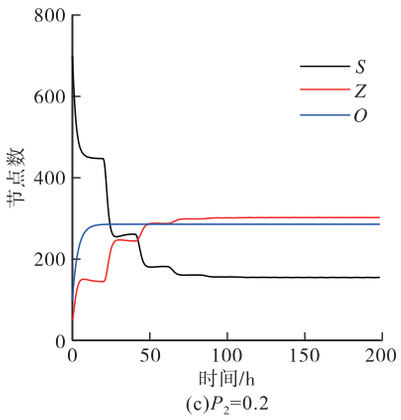
其他参数保持不变,分别令 $P_2=0.01,0.1,0.2$。图 3 为不同反向切换率对应的系统状态,图 3(a)、(b)、(c)分别对应 $P_2=0.01,0.1,0.2$ 的系统状态。



(a) P_2=0.01



(b) P_2=0.1



(c)P_2=0.2

图 3　不同 P_2 对应的系统状态

仿真结果表明，当 $P_2=0.01(R_0<1)$ 时，系统在平衡点 $\boldsymbol{P}^0(108,0,0,1,891)$ 处局部渐进稳定；当 $P_2=0.1(R_0>1)$ 时，系统在 $\boldsymbol{P}^1(155,137,216,47,445)$ 处局部渐进稳定；当 $P_2=0.2(R_0>1)$ 时，系统在 $\boldsymbol{P}^1(155,191,302,66,286)$ 处局部渐进稳定；当系统在局部渐进稳定平衡点 $\boldsymbol{P}^1$ 处时，零日状态节点数随着 P_2 的增大而增加。可见，反向切换率越大，零日病毒在传播及免疫过程中成功入侵目标主机的概率越大，通过调节反向切换率 P_2，可以有效抑制零日病毒的传播，达到较好的免疫效果。

3.2　感染时滞 τ

图 4 中不同颜色的曲线代表不同时滞下的零日节点状态数，由上至下 $\tau=0.1,0.2,0.3,1,2,3,10,20,30$。

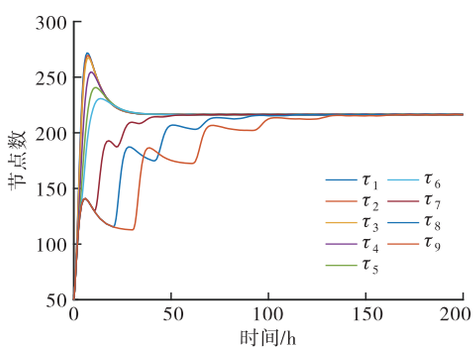
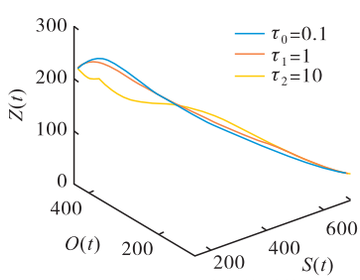


图 4　不同时滞 τ 对应的零日状态节点数

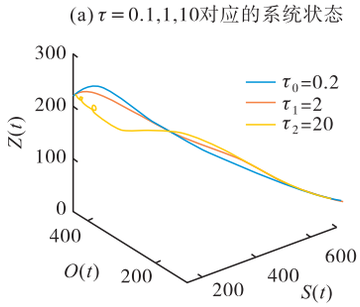
仿真结果表明，当 τ 取不同的数值时，最终零日状态节点数为 216，网络系统在 $\boldsymbol{P}^1(155,137,216,47,445)$ 处达到平衡。因此，感染时滞的改变不影响零日病毒在网络系统传播的最终状态；但不同的感染时滞情况下，病毒扩散至平衡状态所需要的时间不同，零日病毒由初始状态扩散至平衡状态所需时间随着感染时滞的增加而增大。

当 $\tau=10,20,30$ 时，病毒在传播过程中出现了明显的类周期现象。当 $\tau=10$ 时，零日节点数变化曲线的第 1 个极小值出现在 $t=10$ 时，此时网络系统中各节点数为(354，89，131，28，398)。当 $t=20$ 时，到达变化曲线的第 2 个极小值点，此时网络系统中各节点数为(212，121，188，41，438)。当 $t=30$ 时，变化曲线出现第 3 个极小值，此时网络系统中各节点数为(171，132，208，45，444)。当 $\tau=20(30)$ 时，网络系统分别在 $t=20(30)$、$40(60)$、$60(90)$、$80(120)$ 时出现极小值。综合以上分析，在系统达到平衡状态前，网络系统分别在 $t=n\tau(n=1,2,\cdots)$ 时出现极小值；当 $\tau=0.1,0.2,0.3,1,2,3$ 时，病毒传播过程中未出现明显的类周期现象。因此，感染时滞一方面影响了整个网络系统从初始感染阶段到平衡阶段的病毒扩散规模。另一方面，在感染时滞较大时，感染时滞精准刻画了类周期变化的规律。

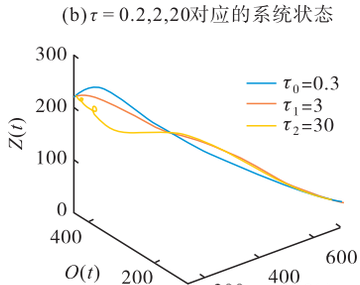
图 5 为不同时滞 τ 对应的系统状态。仿真结果表明，随着感染时滞因子逐渐增大，节点数量变化越明显。同时，在时滞较大的情况下，随着感染时滞的增加，曲线卷曲的情况越明显，即零日状态节点数出现类周期变化的现象越明显。



(a) $\tau=0.1,1,10$对应的系统状态



(b) $\tau=0.2,2,20$对应的系统状态



(c) $\tau=0.3,3,30$对应的系统状态

图 5　不同时滞 τ 对应的系统状态

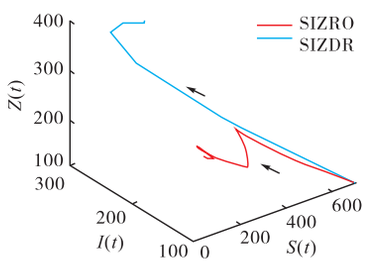
3.3　传播及免疫效果对比

实验[5]针对 SIZDR 模型进行了模拟仿真。本节通过模拟相同或相似的环境，对比 SIZRO 模型与 SIZDR 模型对于零日病毒的免疫效果，验证 SIZRO 模型的免疫效果优于 SIZDR 模型。根据文献[5]中的模型及本文设置的参数，令 SIZDR 模型中各参数

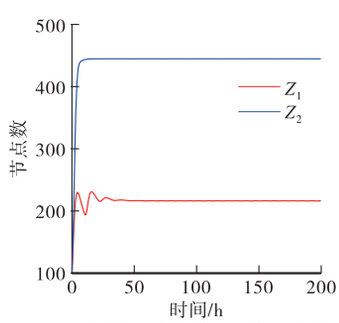
取值分别为:$\beta=0.6$,$K=6$,$\alpha=0.2$,$\upsilon=0.5$,$\gamma=0.6$。设置节点总数 $N=1\ 000$,初始状态下,不同状态节点数为$(S_0,I_0,Z_0,D_0,R_0)=(700,100,100,0,100)$。为了构建相似的网络环境,需要通过参数设置将 SIZDR 模型中零日状态到毁损状态并最终转化为易感状态的过程简化为 SIZRO 模型中零日状态转化为易感状态的过程。因此,令 $\omega=1$,意味着毁损状态节点最终全部转化为易感状态。同时,为了满足 SIZRO 模型中 $\omega=0.3$ 这一条件,令 SIZDR 模型中 $\sigma=0.3$。SIZRO 模型中各参数取值不变,初始状态下,不同节点数为$(S_0,I_0,Z_0,R_0,O_0)=(700,100,100,100,0)$。

在整个网络系统达到平衡状态时,零日节点数量的多少直接反映了整个网络中处于高风险状态的用户主机数量的多少。零日节点数量越多,网络系统的风险就越大;反之,整个网络的风险就越小。因此,网络系统达到稳定状态时,零日节点的数量与总结点数量的比值定义为网络风险率,记为 ψ。

图 6 为不同病毒传播模型的传播及免疫效果对比图。仿真结果表明,在相同条件下,SIZRO 模型最终在有病毒平衡点 $\boldsymbol{P}^1(155,137,216,47,445)$处局部渐近稳定,SIZDR 模型在有病毒平衡点 $\boldsymbol{P}^2(111,222,445,133,89)$处局部渐近稳定。在网络系统达到稳定状态时,SIZRO 模型中零日节点数量为 216,SIZDR 模型中零日节点数量为 445。因此,两个模型的网络风险率分别为 $\psi_1=0.212$,$\psi_2=0.445$,$\psi_1<\psi_2$。综上,在相同条件下,SIZRO 模型能够更好的抑制零日病毒的传播。针对零日病毒,平台动态防御的思想可以起到良好的免疫效果。



(a)不同模型三维对比图



(b) 不同模型零日节点数对比图

图 6 不同模型传播及免疫效果对比图

4 结语

本文在 SIZDR 模型的基础上,考虑感染时滞因素并结合平台层动态目标防御的思想,提出了 SIZRO 模型,通过稳定性分析,讨论了相关因素对病毒传播及免疫效果的影响,对正向切换成功率、反向切换成功率及感染时滞 3 个参数开展了仿真,同时对比了 SIZRO 模型与 SIZDR 模型对零日病毒的免疫效果。理论分析和仿真结果表明,不同的感染时滞导致病毒扩散规模到达稳定状态的时间不同。利用平台动态防御思想,可以有效抑制零日病毒的传播。改变平台切换成功概率可以有效抑制零日病毒的传播规模,起到较好的免疫效果。论文中还存在一定的不足之处,下一步工作将围绕零日病毒传播及免疫模型,提出并分析相应的免疫策略。

参考文献

[1] SUN X Y, DAI J, LIU P. Using Bayesian Networks for Probabilistic Identification of Zero-Day Attack Paths[J]. IEEE Transactions on Information Forensics and Security, 2018,13(10): 2506-2521.

[2] CUI M, WANG J. Deeply Hidden Moving-Target-Defense for Cybersecure Unbalanced Distribution Systems Considering Voltage Stability[J]. IEEE Transactions on Power Systems, 2021, 36(3): 1961-1972.

[3] 王刚,陆世伟,冯云,等. 基于社团网络的网络协同防御[J]. 空军工程大学学报(自然科学版), 2021, 22(2):68-76.

[4] 刘小虎,张玉臣. 网络空间安全保密困境与移动目标防御[J]. 保密工作, 2019(2):69-70.

[5] 孟庆微,仇铭阳,王刚,等. 零日病毒传播模型及稳定性分析[J]. 电子与信息学报, 2021, 43(7): 1849-1855.

[6] VALDEZ J, GUEVARA P, AUDELO J. Numerical Approaching of SIR Epidemic Model for Propagation of Computer Worms[J]. IEEE Latin America Transactions. 2015, 13(10): 3452-3460.

[7] YONATHAN A. Analysis of Twitter-Based Malware Propagation Using SIR Epidemic Model[J]. Journal of Applied Information Communication and Technology, 2020, 5(1):11-19.

[8] 刘小虎,张恒巍,张玉臣,等.基于博弈论的网络攻防行为建模与态势演化分析[J]. 电子与信息学报, 2021, 43(12): 3629-3638.

[9] 王刚,陆世伟,胡鑫,等. 潜伏机制下网络病毒传播SEIQRS模型及稳定性分析[J].哈尔滨工业大学学报, 2019,51(5):131-137.

(下转第 105 页)

据集上进行多分类比较实验。实验结果证明，该方法显著提高了入侵检测的正确率。在准确度、精确度、TPR、FPR、F 值和 AUC 等方面的综合表现要优于原始 SVM 和 GWO-SVM，具有更好的检测性能。

由于 PSOGWO-SVM 算法中参数的初始值对寻优能力和收敛速度有很大影响，因此后期工作将研究如何产生合适的参数初始值，从而提高 PSOGWO-SVM 的分类性能。

参考文献

[1] FERRAG M A, MAGLARAS L, MOSCHOYIANNIS S, et al. Deep Learning for Cyber Security Intrusion Detection: Approaches, Datasets, and Comparative Study[J]. Journal of Information Security and Applications, 2020, 50: 102419.

[2] ALSAADI H I, ALMUTTAIRI R M, BAYAT O, et al. Computational Intelligence Algorithms to Handle Dimensionality Reduction for Enhancing Intrusion Detection System[J]. Journal of Information Science and Engineering, 2020, 36: 293-308.

[3] 柯钢. 改进粒子群算法优化支持向量机的入侵检测方法[J]. 合肥工业大学学报(自然科学版), 2019, 42(10): 1341-1345.

[4] 汪生，金志刚. 基于模糊 SVM 模型的入侵检测分类算法[J]. 计算机应用研究, 2020, 37(2): 501-504.

[5] HALIM Z, YOUSAF M N, WAQAS M, et al. An Effective Genetic Algorithm-Based Feature Selection Method for Intrusion Detection Systems[J]. Computers & Security, 2021, 110: 102448.

[6] 刘静，杨正校. 改进 ACO-SVM 在网络入侵检测中的应用[J]. 软件, 2018, 39(10): 57-59.

[7] DAVAHLI A, MAHHOUBEH S, GOLNOUSH A. Hybridizing Genetic Algorithm and Grey Wolf Optimizer to Advance an Intelligent and Lightweight Intrusion Detection System for IoT Wireless Networks[J]. Journal of Ambient Intelligence and Humanized Computing, 2020, 11(11): 5581-5609.

[8] ALMOMANI O. A Feature Selection Model for Network Intrusion Detection System Based on PSO, GWO, FFA and GA algorithms[J]. Symmetry, 2020, 12(6): 1046.

[9] 曹源，高丙朋，张振海. 一种基于 PSO-GWO 的电网故障诊断方法[J]. 电测与仪表, 2021, 58(9): 35-40.

[10] IOANNOU C, VASOS V. Network Attack Classification in IoT Using Support Vector Machines[J]. Journal of Sensor and Actuator Networks, 2021, 10(3): 58.

[11] HU J J. Network Security Situation Prediction Based on MR-SVM[J]. IEEE Access, 2019, 7: 130937-130945.

[12] 杨越翔. 基于日志数据的 U2R 和 R2L 入侵检测研究[D]. 兰州：西北师范大学, 2020.

[13] 全亮亮. 基于数据挖掘算法的入侵检测研究[D]. 武汉：武汉科技大学, 2013.

（编辑：徐敏）

(上接第 96 页)

[10] SUPRUN O, YUDIN O, ZIUBINA R, et al. Devising a Method of Protection Against Zero-Day Attacks Based on an Analytical Model of Changing the State of the Network Sandbox[J]. Eastern-European Journal of Enterprise Technologies, 2021, 109: 50-57.

[11] MILLAR S, MCLAUGHLIN N, RINCON J M D, et al. Multi-View Deep Learning for Zero-Day Android Malware Detection[J]. Journal of Information Security and Applications, 2021, 58(3): 102718.

[12] 白鹏. 文档类型 0 Day 漏洞检测技术的研究与实现[D]. 北京：北京邮电大学, 2015.

[13] JEONG J H, CHOI S G. Hybrid System to Minimize Damage by Zero-Day Attack based on NIDPS and Honey Pot[C]// 2020 International Conference on Information and Communication Technology Convergence. Nanjing: [s. n.], 2020.

[14] 王刚，冯云，马润年. 操作系统病毒时滞传播模型及抑制策略设计[J]. 西安交通大学学报, 2021, 55(3): 11-19.

[15] 张志双. 一类具有双时滞计算机病毒传播模型的动力学性质[D]. 哈尔滨：哈尔滨工业大学, 2013.

[16] YANG F, ZHANG Z. Hopf Bifurcation Analysis of SEIR-KS Computer Virus Spreading Model with Two-Delay[J]. Results in Physics, 2021, 24: 104090.

[17] 王超，杨旭颖，徐珂，等. 基于 SEIR 的社交网络信息传播模型[J]. 电子学报, 2014, 42(11): 2325-2330.

[18] 宋磊，王春雷. 一类时滞网络病毒传播模型的 Hopf 分支[J]. 计算机与现代化, 2016(11): 79-82.

[19] 张子振，储煜桂，KUMARI S，等. 一类具有非线性发生率的无线传感网络蠕虫传播模型的延迟动力学行为[J]. 浙江大学学报：理学版, 2019, 46(2): 168-186, 199.

（编辑：徐楠楠）