

王军,杨璐,杨子钰,等.基于动态隔离的工业互联网恶意软件传播模型研究[J].辽宁工程技术大学学报(自然科学版),2025,44(2): 226-236.DOI:10.11956/j.issn.1008-0562.20240090
WANG Jun,YANG Lu,YANG Ziyu,et al.Research on malware propagation model of industrial internet based on dynamic isolation [J].Journal of Liaoning Technical University(Natural Science),2025,44(2):226-236.DOI:10.11956/j.issn.1008-0562.20240090

基于动态隔离的工业互联网恶意软件传播模型研究

王 军, 杨 璐, 杨子钰, 付 强*

(沈阳化工大学 计算机科学与技术学院, 辽宁 沈阳 110142)

摘 要: 为更真实地描述恶意软件在工业互联网中的传播动态行为, 基于动力学系统理论, 引入时延因素, 构建可变隔离率的时延恶意软件传播模型。针对恶意软件感染早期阶段感染节点数量较小的特点, 模型根据感染主机数量的变化动态调整隔离率; 对模型进行数值分析和仿真实验, 结合理论推导得出Hopf分岔的阈值。研究表明: 时延的存在导致系统出现Hopf分岔现象, 当时延小于阈值时, 系统保持稳定; 当时延超过阈值时, 系统呈现不稳定状态。表明该模型能够更准确地预测恶意软件传播的动态过程。研究结论为工业互联网安全防护策略的制定提供理论依据。

关键词: 网络安全; 工业互联网; 恶意软件传播模型; 动态隔离; 时延系统; Hopf分岔阈值

中图分类号: TP399

文献标志码: A

文章编号: 1008-0562(2025)02-0226-11

Research on malware propagation model of industrial internet based on dynamic isolation

WANG Jun, YANG Lu, YANG Ziyu, FU Qiang*

(College of Computer Science and Technology, Shenyang University of Chemical Technology, Shenyang 110142, China)

Abstract: To more accurately describe the dynamic behavior of malware propagation in the industrial internet, this paper constructs a delay malware propagation model with a variable isolation rate, based on the theory of dynamical systems and incorporating delay factors. This model dynamically adjusts the isolation rate with the change in the number of infected hosts, addressing the characteristic of a small number of infected nodes in the early stages of malware infection. By performing numerical analysis and simulation experiments, and combining theoretical derivation, the Hopf bifurcation threshold is obtained. The research results show that the presence of delay leads to the occurrence of Hopf bifurcation. When the delay is below the threshold, the system remains stable; when the delay exceeds the threshold, the system becomes unstable. This proves that the model can more accurately predict the dynamic process of malware propagation. The research conclusions provide a theoretical basis for the formulation of security protection strategies in the industrial internet.

Keywords: network security; industrial internet; malware propagation model; dynamic isolation; time-delay system; Hopf bifurcation threshold

0 引言

工业互联网作为工业数字化与智能化转型的

重要基础^[1-4], 所面临的安全威胁日益严峻。网络攻击带来的生产中断和数据泄露等问题, 对制造业构成巨大威胁^[5-8]。由于现有的恶意软件传播模

收稿日期: 2024-04-12 修回日期: 2024-05-13 接受日期: 2024-05-23 责任编辑: 朱含露

基金项目: 辽宁省自然科学基金项目(2022-MS-291) 辽宁省教育厅高校基本科研项目(LJKMZ20220781; JYTMS20231488; LJKQZ20222457)

作者简介: 王 军(1978-)男, 辽宁沈阳人, 博士, 教授, 主要从事工业网络安全的研究。E-mail: 382134224@qq.com

通信作者: 付 强(1990-)男, 辽宁沈阳人, 博士, 讲师, 主要从事工业网络安全的研究。E-mail: 562833467@qq.com

型普遍存在固定隔离率、忽略时延、节点异质性考虑不足、网络拓扑结构过于简化等问题,如何利用传播动力学模型描述恶意软件在工业互联网中的传播过程,并结合工业互联网中的具体情况,设计具有针对性的防控策略,已经成为当前研究的重点问题。

针对现有恶意软件模型无法适用于所有工业中的细节等问题,学者们提出了SIS模型^[9-11]和SIR模型^[12-14]等用于研究。XIAO等^[15]研究恶意软件在网络理系统中的传播动力学特性及其临界点预测方法,为理解复杂系统中的恶意软件传播机制奠定了理论基础。REY等^[16]基于个体的数学模型,提出一种专门用于研究工业关键基础设施中的恶意软件传播行为。MAHBOUBI等^[17]对异构移动恶意软件进行了系统性分析,识别出影响传播过程的关键参数。上述研究虽然能够初步揭示恶意软件传播的基本特性,但未能充分考虑传播过程中参数的动态演化特征。工业互联网环境下的恶意软件传播往往伴随着参数的动态变化过程,单一的静态分析方法难以准确预测传播趋势。YAO等^[18]提出考虑时滞效应和可变感染率的蠕虫传播模型,探讨动态传播过程中变量的演化规律,通过引入可变感染率提升预测精度。YU等^[19]在此基础上进一步改进包含双感染率的SEI2RS模型,实现了对网络物理系统中双感染率恶意软件传播的建模,但该模型未考虑时延效应。YANG等^[20]提出一种双时延SIDQR模型,在文献[19]的基础上强调了时间延迟在传播过程中的作用,提升了动态传播模型的复杂度。综上可知,现有的模型虽然在一定程度上可以模拟恶意软件传播行为,但忽略了隔离率的动态变化在实际工业系统安全防护中的重要价值。

因此,本文基于动力学系统理论,结合时延因素和可变隔离率,构建一个更符合工业互联网场景的恶意软件传播模型。采用动力学系统理论描述恶意软件的传播过程,将节点状态转化为数学变量,分析其动态演化规律;引入时延因素,反映出工业互联网中存在的时间延迟情况;并通过数值分析和仿真实验,研究系统的稳定性条件,推导Hopf分岔阈值。结合理论推导和仿真数据实

验,验证模型对恶意软件动态传播的预测能力。

1 模型设计

设工业互联网上主机的总数为 N ,SIQVD模型的状态转换见图1。

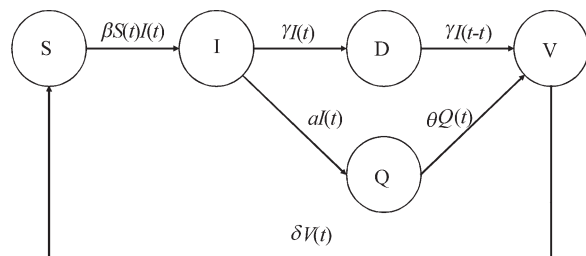


图1 SIQVD模型的状态转换

Fig.1 state transition of the SIQVD model

该模型中,易感主机在遭受恶意软件攻击后会转变为感染主机,模型采用动态隔离策略来控制恶意软件在易感主机间的传播。网络管理员可根据实时情况动态调整感染主机的隔离率,而被隔离的主机可以通过安装补丁等方式转变为恢复态。假设所有主机存在易感(S)、感染(I)、隔离(Q)、恢复(V)和延迟(D)5种状态。SIDQV模型为

$$\begin{cases} dS/dt = -\beta I(t)S(t) + \delta V(t) \\ dI/dt = \beta I(t)S(t) - \gamma I(t) - aI(t) \\ dQ/dt = aI(t) - \theta Q(t) \\ dV/dt = \theta Q(t) + \gamma I(t-\tau) - \delta V(t) \\ dD/dt = \gamma I(t) - \gamma I(t-\tau) \end{cases}, \quad (1)$$

式中: t 为时间; s ; S 为易感者的台数; I 为感染者的台数; Q 为被隔离者的台数; V 为接受疫苗的个体台数; D 为延迟状态的个体台数; a 为感染者的被隔离率; β 为感染率; γ 为感染者的恢复率; θ 为被隔离者向接受疫苗者的转化率; δ 为接受疫苗者失去免疫的速率; τ 为时间延迟。

假设 a 为 t 的函数,记为

$$a(t) = a_0 f_1(I(t)),$$

式中: a_0 为初始感染率; $f_1(\cdot)$ 为感染宿主 I 的非线性函数,表达式为

$$f_1(I(t)) = \frac{I}{1+al}, \quad (2)$$

满足:① $f_1(0) = 0$; ② $f_1'(I) > 0$; ③ $f_1''(I) < 0$; ④ $\lim_{I \rightarrow \infty} f_1(I) = C < +\infty$ 。

采用微分方程组表示 SIDQV 模型为

$$\begin{cases} \frac{dS}{dt} = -\beta I(t)S(t) + \delta V(t) \\ \frac{dI}{dt} = \beta I(t)S(t) - \gamma I(t) - \alpha_0 f(I(t)) \\ \frac{dQ}{dt} = \alpha_0 f(I(t)) - \theta Q(t) \\ \frac{dV}{dt} = \theta Q(t) + \gamma I(t-\tau) - \delta V(t) \\ \frac{dD}{dt} = \gamma I(t) - \gamma I(t-\tau) \end{cases}, \quad (3)$$

式中, $f(I(t)) = f_1(I(t))I(t)$ 。

2 平衡稳定性与分岔分析

为分析系统平衡点的稳定性条件, 探讨在时延参数变化下系统是否出现分岔现象, 揭示系统的内在动态特性, 进行如下分析。

为验证系统的平衡稳定性, 需证明式 (3) 有且只有 1 个正平衡点。基本再生数 R_0 可以衡量恶意软件传播的临界条件, 当 $R_0 > 1$ 时, 恶意软件会持续传播, 而当 $R_0 < 1$ 时, 恶意软件最终会消失。

根据式 (3) 可得

$$R_0 = \frac{\beta N}{(\gamma + \alpha f'(0))}。$$

定理 1 当 $R_0 \geq 1$ 时, 式 (3) 有 1 个独特正平衡点为 $E^* = (S^*, I^*, D^*, Q^*, V^*)$, 其中,

$$S^* = \frac{\alpha_0 f(I^*) + \gamma I^*}{\beta I^*}, I^* = I^*, Q^* = \frac{\alpha_0 f(I^*)}{\theta},$$

$$V^* = \frac{\alpha_0 f(I) + \gamma I^*}{\delta}, D^* = \gamma \tau I^*。$$

证明: 当式 (3) 稳定时, 满足

$$\begin{cases} -\beta I(t)S(t) + \delta V(t) = 0 \\ \beta I(t)S(t) - \gamma I(t) - \alpha_0 f(I(t)) = 0 \\ \alpha_0 f(I(t)) - \theta Q(t) = 0 \\ \theta Q(t) + \gamma I(t-\tau) - \delta V(t) = 0 \\ \gamma I(t) - \gamma I(t-\tau) = 0 \end{cases}, \quad (4)$$

令 $I(t) > 0$, 则有

$$S^* = \frac{\alpha_0 f(I^*) + \gamma I^*}{\beta I^*}, Q^* = \frac{\alpha_0 f(I^*)}{\theta},$$

$$V^* = \frac{\alpha_0 f(I) + \gamma I^*}{\delta}, D^* = \gamma \tau I^*。$$

由于式 (4) 中的主机总数为二进制, 系统平衡条件 (即所有主机台数的总和始终保持恒定) 为

$$H(I) = \frac{\alpha_0 f_1(I(t)) + \gamma I}{\beta I} + I + \frac{\alpha_0 f_1'(I(t))}{\theta} + \frac{\alpha_0 f_1'(I(t)) + \gamma I}{\delta} - N = 0。 \quad (5)$$

对式 (5) 求导得

$$H'(I) = \frac{\alpha_0 f_1'(I(t))}{\theta} + 1 + \frac{\alpha_0 f_1'(I(t)) + \gamma}{\delta} + \frac{\alpha_0 f_1'(I(t)) + \gamma}{\beta I} - \frac{\gamma I + \alpha_0 f_1'(I(t))}{\beta I^2}。 \quad (6)$$

将式 (2) 以及各参数代入式 (6) 得

$$H'(I) = \frac{\beta \delta \theta I^2 + \beta \gamma \theta I^2 + 10 I \beta \gamma \theta}{\beta \theta \delta (I^2 + 10 I + 25)} + \frac{25 \alpha \beta \delta + 25 \alpha \beta \theta - 5 \alpha \delta \theta}{\beta \theta \delta (I^2 + 10 I + 25)} + \frac{25 \beta \delta \theta + 25 \beta \gamma \theta}{\beta \theta \delta (I^2 + 10 I + 25)}。 \quad (7)$$

由于参数均为正值, 故 $H'(I) > 0$, 函数单调递增。若存在 $H(I) = 0$ 的正根, 则 $H(0) < 0$, 基于此可得

$$\begin{aligned} H(0) &= \lim_{I \rightarrow 0} H(I) = -N + \frac{\alpha_0 f_1'(0)}{\theta} + \\ &\frac{\alpha_0 f_1'(0)}{\delta} + \frac{\alpha_0 f_1'(0)}{\beta} + \frac{\gamma}{\delta} + I = \\ &\frac{I \beta \delta \theta - N \beta \delta \theta + \alpha \beta \delta f_1'(I)}{\beta \delta \theta} + \\ &\frac{\alpha \beta \theta f_1'(I) + \alpha \theta \delta f_1'(I) + \beta \gamma \theta}{\beta \delta \theta}。 \end{aligned} \quad (8)$$

将参数代入式 (8) 可得 $H(0) < 0$, 表明系统存在 1 个正平衡点。证毕。

由于 $Q(t) = N - S(t) - I(t) - V(t) - D(t)$, 将式 (3) 简化为

$$\begin{cases} \frac{dS}{dt} = -\beta I(t)S(t) + \delta V(t) \\ \frac{dI}{dt} = \beta I(t)S(t) - \gamma I(t) - \alpha_0 f(I(t)) \\ \frac{dV}{dt} = \theta(N - S(t) - I(t) - V(t) - D(t)) + \\ \gamma I(t-\tau) - \delta V(t) \\ \frac{dD}{dt} = \gamma I(t) - \gamma I(t-\tau) \end{cases}。 \quad (9)$$

求式 (9) 关于平衡点 E^* 的雅可比矩阵为

$$J(E^*) = \begin{pmatrix} -\beta I & -\beta S & \delta & 0 \\ \beta I & \beta S - \gamma - \alpha_0 f'(I) & 0 & 0 \\ -\theta & -\theta + \gamma e^{-\lambda \tau} & -\theta - \delta & -\theta \\ 0 & \gamma - \gamma e^{-\lambda \tau} & 0 & 0 \end{pmatrix}。 \quad (10)$$

令 $J(E^*) = 0$, 得到其特征方程为

$$P(\lambda) + B(\lambda)e^{-\lambda \tau} = 0, \quad (11)$$

式中,

$$\begin{cases} P(\lambda) = \lambda^4 + p_3\lambda^3 + p_2\lambda^2 + p_1\lambda + p_0 \\ B(\lambda) = b_1\lambda + b_0 \end{cases} \quad (12)$$

由式(10)可得

$$\begin{aligned} p_3 &= I\beta - S\beta + \alpha f'(I) + \delta + \gamma + \theta, \\ p_2 &= I\alpha\beta f'(I) + I\beta\delta + I\beta\gamma + I\beta\theta - \\ &\quad S\beta\delta - S\beta\theta + \alpha\delta f'(I) + \alpha f'(I)\theta + \\ &\quad \delta\gamma + \delta\theta + \gamma\theta, \\ p_1 &= I\alpha\beta\delta f'(I) + I\alpha\beta f'(I)\theta + I\beta\delta\gamma + \\ &\quad I\beta\delta\theta + I\beta\gamma\theta - S\beta\delta\theta + \alpha\delta f'(I)\theta + \delta\gamma\theta \\ p_0 &= I\beta\delta\gamma\theta, b_1 = -I\beta\delta\gamma, b_0 = -I\beta\delta\gamma\theta. \end{aligned}$$

定理2 如果模型满足条件A(1):

① $p_3 > 0$; ② $p_3 p_2 - (p_1 + b_1) > 0$; ③ $(p_1 + b_1) > 0$,

则正平衡点 E^* 是稳定且局部范围内没有时延的。

证明: 当 $\tau = 0$ 时, 式(9)可化简为

$$\lambda^4 + p_3\lambda^3 + p_2\lambda^2 + p_1\lambda + p_0 + (b_1\lambda + b_0)e^{-\lambda\tau} = 0. \quad (13)$$

根据Routh-Hurwitz准则, 式(13)所有根都有负实部。因此, 正平衡点 E^* 是局部无时滞渐近稳定的。证毕。

令 $\lambda = i\omega$, 代入式(11), 分离实部和虚部, 其中, 实部为

$$\omega^4 - p_2\omega^2 + p_0 + b_0\cos(\omega\tau) + b_1\omega\sin(\omega\tau) = 0, \quad (14)$$

虚部为

$$-p_3\omega^3 + p_1\omega - b_0\sin(\omega\tau) + b_1\omega\cos(\omega\tau) = 0. \quad (15)$$

将式(14)和式(15)平方后相加得

$$\begin{aligned} b_0^2 + (b_1\omega)^2 &= (\omega^4 - p_2\omega^2 + p_0)^2 + \\ &\quad (-p_3\omega^3 + p_1\omega)^2. \end{aligned} \quad (16)$$

化简式(16)得

$$\omega^8 + D_3\omega^6 + D_2\omega^4 + D_1\omega^2 + D_0 = 0, \quad (17)$$

式中: $D_3 = p_3^2 - 2p_2$; $D_2 = 2p_0 + p_2^2 - 2p_1p_3$; $D_1 = p_1 - 2p_0p_2 - b_1^2$; $D_0 = p_0^2 - b_0^2$ 。

令 $\omega^2 = z$, 将式(17)简化为 z 的多项式, 得

$$h(z) = z^4 + D_3z^3 + D_2z^2 + D_1z + D_0. \quad (18)$$

定理3 假设式(18)满足A(2): ① $D_0 \geq 0$, $\Delta \geq 0$, $z_1 > 0$ 或 $h(z_1) > 0$; ② $D_0 \geq 0$, $\Delta < 0$; ③不存在 $z^* \in (z_1, z_2, z_3)$ 使 $z^* > 0$ 和 $h(z^*) \leq 0$, 则系统的正平衡点 E^* 是绝对稳定的。也就是说 E^* 对任何 $\tau \geq 0$ 都是渐近稳定的。

定理3中 Δ 为特征多项式(18)的判别式, 用于判断根的实虚性质; z_1 、 z_2 、 z_3 表示特征方程

的实数根。

证明: 假设式(18)中的模型满足条件A(2), 确保式(11)的根满足稳定性条件。

由前文推导可知, 式(18)至少有1个正实根 ω_0 , 式(11)有1对纯虚根 $\pm i\omega_0$ 。这意味着系统存在周期性振荡。将纯虚根 $\pm i\omega_0$ 代入式(14)和式(15)进行联立, 可得时延阈值 $\tau_k > 0$, 使系统满足稳定性条件。

$$\begin{aligned} \tau_k &= \frac{1}{\omega_0} \arccos \left[\frac{b_0(\omega_0^4 - p_2\omega_0^2 + p_0)}{b_0^2 + (b_1\omega_0)^2} + \right. \\ &\quad \left. \frac{(p_3\omega_0^3 - p_1\omega_0)b_1\omega_0}{b_0^2 + (b_1\omega_0)^2} + \frac{2k\pi}{\omega_0} \right]. \end{aligned} \quad (19)$$

令 $\lambda(\tau) = v(\tau) + i\omega(\tau)$ 为式(11)的根, 当 $\tau = \tau_k$ 时, 满足 $v(\tau_k) = 0$, $\omega(\tau_k) = \omega_0$ 。

由上述推导可知, 式(11)所示特征方程在一定的范围内存在1对纯虚根, 可以证明存在1个时延使系统保持一定的稳定性。证毕。

定理4 设 $h'(z_0) \neq 0$ 。若 $\tau = \tau_0$, 则 $\pm i\omega_0$ 为式(11)所示特征方程的一对纯虚根, 且满足条件A(2), 则

$$\frac{d\operatorname{Re}\lambda(\tau_0)}{d\tau} > 0. \quad (20)$$

因此, 当时延 $\tau > \tau_k$ 时, 式(11)存在至少1个实部为正的实特征根, 此时系统不稳定。对式(11)两边求导, 结合 b_1 和 b_0 的相关项, 可得

$$\begin{aligned} \left(\frac{d\lambda}{d\tau} \right)^{-1} &= \frac{4\lambda^3 + 3p_3\lambda^2 + 2p_2\lambda}{(b_1\lambda + b_0)\lambda e^{-\lambda\tau}} + \\ &\quad \frac{p_1 + b_1e^{-\lambda\tau} - (b_1\lambda + b_0)\tau e^{-\lambda\tau}}{(b_1\lambda + b_0)\lambda e^{-\lambda\tau}} = \\ &\quad \frac{(4\lambda^3 + 3p_3\lambda^2 + 2p_2\lambda + p_1)e^{\lambda\tau}}{(b_1\lambda + b_0)\lambda} + \\ &\quad \frac{b_1}{(b_1\lambda + b_0)\lambda} - \frac{\tau}{\lambda}. \end{aligned} \quad (21)$$

用式(14)和式(15)简化式(11)的实部导数部分, 可得

$$\begin{aligned} \operatorname{sgn} \left[\frac{d\operatorname{Re}\lambda}{d\tau} \right]_{\tau=\tau_k} &= \operatorname{sgn} \left[\operatorname{Re} \left(\frac{d\lambda}{d\tau} \right) \right]_{\lambda=i\omega_0}^{-1} = \\ &= \operatorname{sgn} \frac{\omega_0^2}{\Gamma} (4\omega_0^6 + 3D_3\omega_0^4 + 2D_2\omega_0^2 + D_1) = \end{aligned}$$

$$\operatorname{sgn} \frac{\omega_0^2}{\Gamma} \{h'(\omega_0^2)\} = \operatorname{sgn} \{h'(\omega_0^2)\}, \quad (22)$$

式中, $\Gamma = (b_0\omega_0)^2 + (b_1\omega_0^2)^2$ 。

遵循假设 A(2) 和假设 $h'(\omega_0^2) \neq 0$, 可得

$$\left. \frac{d(\operatorname{Re}\lambda)}{d\tau} \right|_{\tau=\tau_k} > 0. \quad (23)$$

根据 Routh-Hurwitz 准则, 式 (11) 的根在虚轴上从左向右交叉。当一个参数连续变化, 从小于某值到大于某值时, 系统变得不稳定。因此, 根据泛函微分方程的 Hopf 分岔定理, 横向条件成立, 满足 Hopf 分岔的条件。证毕。

定理 5 假设满足条件 A(1) 和 A(2):

① 当 $\tau < \tau_0$, 系统是稳定的, 当 $\tau > \tau_0$, 系统是不稳定的; ② 当式 (3) 满足 A(2) 时, 在 $\tau = \tau_0$ 时发生 Hopf 分岔。

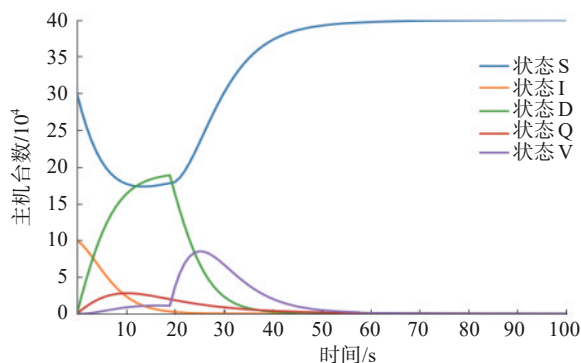
由此可得: 当 $\tau < \tau_0$ 时, 系统稳定, 可以通过实施相关的方法和策略来抑制恶意软件的传播; 当 $\tau > \tau_0$ 时, 系统不稳定, 恶意软件的传播将难以得到有效的控制。

3 数值模拟与实验

为验证模型的有效性和理论分析的准确性, 针对 $R_0 < 1$ 和 $R_0 > 1$ 两种情形开展数值仿真实验, 分析模型的动态行为。从定性与定量两个维度对理论推导结果进行验证, 探讨各参数对恶意软件传播过程的影响, 同时对比分析理论预期与实际仿真结果。

3.1 $R_0 < 1$ 时的实验分析

当 $R_0 < 1$ 时, 设主机总数为 4×10^5 台。感染率 β



(a) $\tau < \tau_0$

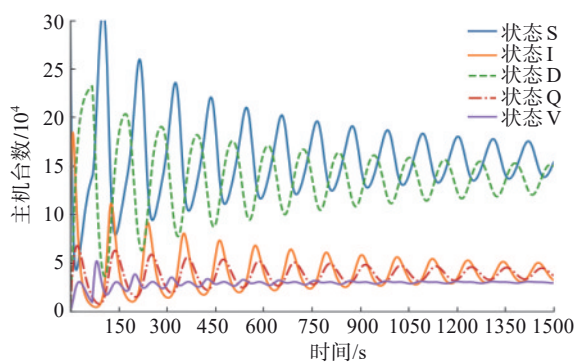
为 0.83×10^{-6} , 传染宿主的恢复率 γ 为 0.25, 被隔离主机的免疫率 θ 为 0.08, 接受补丁的主机以 δ 为 0.17 的速率丧失免疫力, 感染主机的隔离率 α 为 0.1。受隔离策略影响的模型中, 隔离率随实际感染主机数的变化函数为

$$f(I(t)) = I(t)/(1 + aI(t)),$$

式中, a 代表隔离率对受感染主机数量的敏感性。当 $a=0$ 时, 隔离率为常数。设初始感染主机为 10^5 台, 其他状态均为易感状态。为验证第二部分中推导的关于时延结论的正确性, 进行如下数值实验。

当 $\tau=20 < \tau_0$ 、 $a=10^{-5}$ 时, 5 种主机数量的变化情况见图 2 (a)。由图 2 (a) 可知, 感染主机的数量持续降低, 当 $t=60$ s 时, 感染主机的数量为 0。可知, 在时延较短时, 防御策略可迅速响应感染情况并快速实施隔离策略, 从而在传染过程中形成正反馈的控制效应, 使系统具有良好的稳定性。表明当 $R_0 < 1$ 时, 工业互联网中恶意软件的传播可通过及时动态的隔离机制得到遏制。

当 $\tau=70 > \tau_0$ 、 $a=10^{-5}$ 时, 5 种主机数量的变化情况见图 2 (b)。由图 2 (b) 可见, 5 种主机数量变化波动较大, 当时延较大时, 防御措施的响应滞后, 难以在感染初期及时隔离被感染的主机, 导致恶意软件在工业互联网的局部区域反复传播。在实际工业互联网环境中, 防御系统的时延若超出阈值范围时, 防护措施不能及时覆盖所有受感染节点, 出现局部感染暴发的风险, 此时就需要引入更加智能化和自适应的防护策略, 补偿时延所带来的不利影响。



(b) $\tau > \tau_0$

图 2 5 种主机的恶意软件传播结果

Fig.2 simulation results of malware spread in five host categories

通过仿真实验来验证理论分析和数值结果的一致性和正确性。其中, 在 $\tau=20 < \tau_0$ 时, 易感主机、感染主机、隔离主机和恢复主机数量的理论

值与模拟值的对比结果见图 3。由图 3 可见, 4 种主机的模拟值与理论值总体趋势一致, 其中感染主机和恢复主机的数量曲线几乎完全重合, 表明

这2种主机在传播过程中的转换速率及比例符合理论预期。易感主机的数量在最低点处存在微小偏差,但随时间的增加逐渐减小为0,这表明模型参数在动态调控下能够准确捕捉易感主机状态变化的细节。此外,隔离主机的数量在峰值处略

有偏差,但随着时间的推移逐渐减小为0。仿真实验结果验证了理论计算的准确性,表明该模型能够准确描述不同类型主机在感染过程中的状态转换规律,有效预测恶意软件在工业网络中的传播趋势。

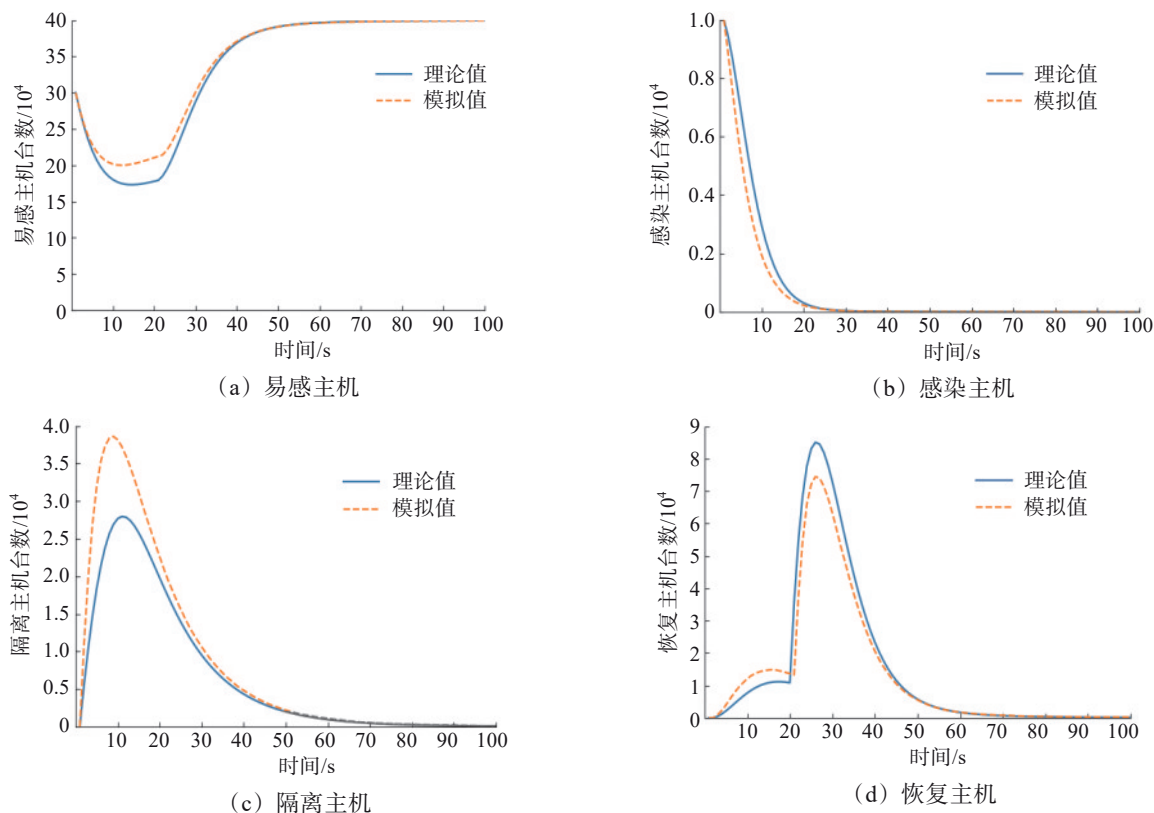


图3 $\tau < \tau_0$ 时4种主机台数的理论值与模拟值对比曲线

Fig.3 comparison of theoretical and simulated values for the number of four host types under $\tau < \tau_0$

3.2 $R_0 > 1$ 时的实验分析

当 $R_0 > 1$ 时,初始感染主机是5台,其他主机状态均为易感状态。为验证第二部分关于时延结论的正确性,进行如下数值实验,其他参数设置与 $R_0 < 1$ 时相同。

(1) τ 对系统稳定性影响

τ 对5种主机数量的影响见图4,由图4(a)可见,当 $\tau = 20 < \tau_0$, $a = 10^{-5}$ 时,在 $t = 250$ s处,各类主机都趋近于理论值,此时防御措施能迅速响应感染动态,系统中各状态变量的调整过程呈现平滑收敛的趋势,系统在平衡点 E^* 处为局部渐近稳定。此时,系统表现为线性稳定状态,易感主机、感染主机、隔离主机和恢复主机之间的转换遵循预期的动态规律,各状态之间的相互作用达到平衡。

由图4(b)可见,当 $\tau = 70 > \tau_0$, $a = 10^{-5}$ 时,曲线波动较大,此时防御措施响应滞后,系统中恶意软件的传播过程呈周期性振荡。这种周期性振荡现象正是Hopf分岔所预测的动态不稳定状态的特征,说明系统由于延迟反馈效应在局部失去了稳定。此外,这种动态不稳定现象在实际工业互联网中意味着防护系统可能无法及时、有效地抑制恶意软件的传播,易引发大规模安全事件。

基于第2部分的理论推导和Hopf分岔理论分析,得到 $a = 10^{-5}$ 时的系统分岔图,见图5。通过计算雅可比矩阵的特征值,在 τ 为58附近发现一对共轭纯虚根,此时系统的实部正好穿过0值点,出现Hopf分岔。当系统时延参数 τ 大于58时,系统将从稳定状态转变为周期性振荡状态,说明工业互联网

中防御措施的时延效应对系统稳定性有显著影响。在实际应用中,如果防御系统的响应时延超过该临界值,恶意软件可能会以周期性爆发的方式扩散,

从而增加预测和防御的难度。基于此,在实际网络中可以进一步预测工业互联网中的稳定性边界,为制定有效的网络安全抑制策略提供理论依据。

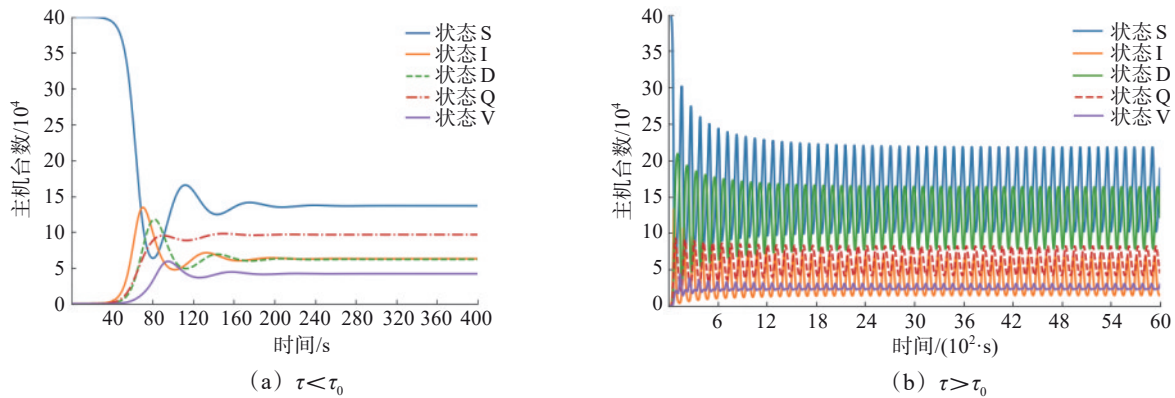


图 4 τ 值对 5 种主机台数的影响

Fig.4 impact of τ values on the number of five types of hosts

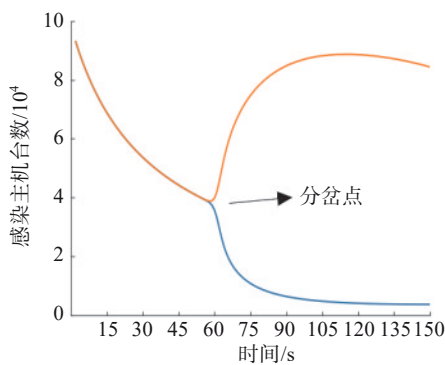


图 5 $a=10^{-5}$ 时的系统分岔

Fig.5 system bifurcation with $a=10^{-5}$

为进一步验证时延对工业互联网的影响,探讨不同时延下,同一坐标内感染主机台数的变化情况(见图 6), τ 分别取 20、30、50、70。

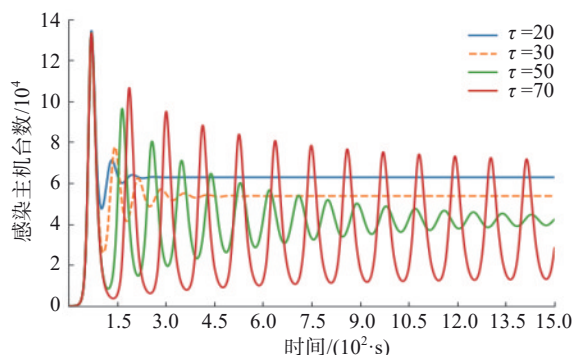


图 6 不同时延下感染主机的数量变化

Fig.6 number of infected hosts changes under different delay

由图 6 可知,当时延较小时,系统相对稳定。当时延达到阈值后,系统稳定性逐渐降低,开始出现振荡现象。这表明时延的增加可延长系统的响应

时间,导致隔离策略难以快速实施,使恶意软件的持续传播。在实际应用中,当工业互联网中的时延较长时,防御系统必须具备较高的应急响应能力,例如快速调整隔离策略、增加系统的防护力度,以应对恶意软件的传播。

(2) 参数 a 对系统稳定性影响

不同参数 a 对被感染主机的数量的影响见图 7,由图 7 (a) 可知, a 从 10^{-7} 增至 10^{-4} 时,感染主机的峰值数量由 8×10^4 台上升至 2.15×10^5 台。由图 7 (b) 可知, a 越大,感染主机数量变化曲线的振幅越大。这表明,较大的 a 值会使隔离措施过于激进,影响网络的正常运行和系统效率。但较小的 a 值会使系统对感染主机的响应不足。因此,在工业互联网的实际应用中,防御系统应根据实时的网络状况和感染态势,动态调整 a 值,以实现既能有效控制恶意软件传播,又能保证系统高效运行的需求。

(3) 感染率对系统稳定性影响

当 $\tau < \tau_0$ 和 $\tau > \tau_0$ 时,不同感染率对被感染主机台数的影响情况见图 8。由图 8 可见,感染率越大,感染主机台数的峰值也随之增大,表明感染率直接影响了恶意软件的传播范围和扩散速度。当感染率较高时,恶意软件能够迅速传播至更多主机,从而使感染主机的数量迅速增加,且台数的峰值明显更高。

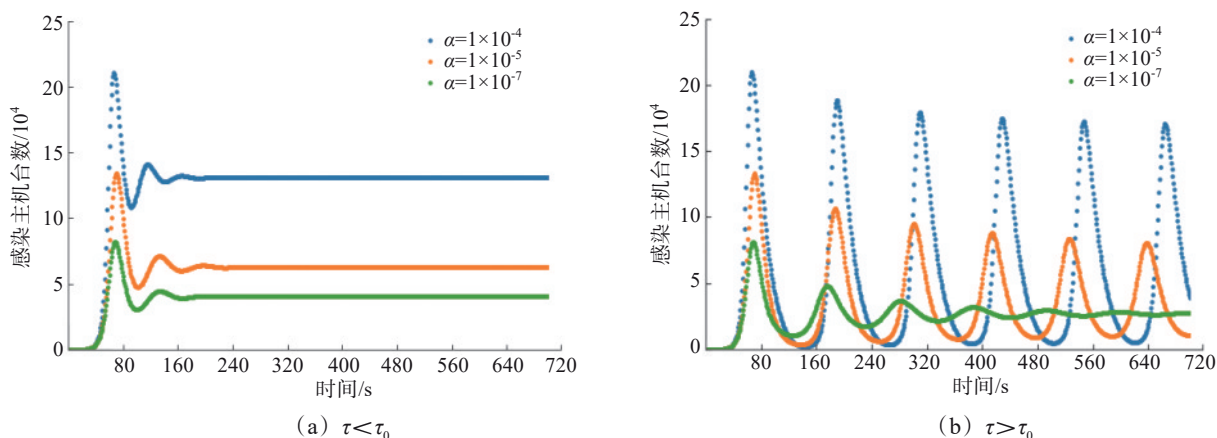
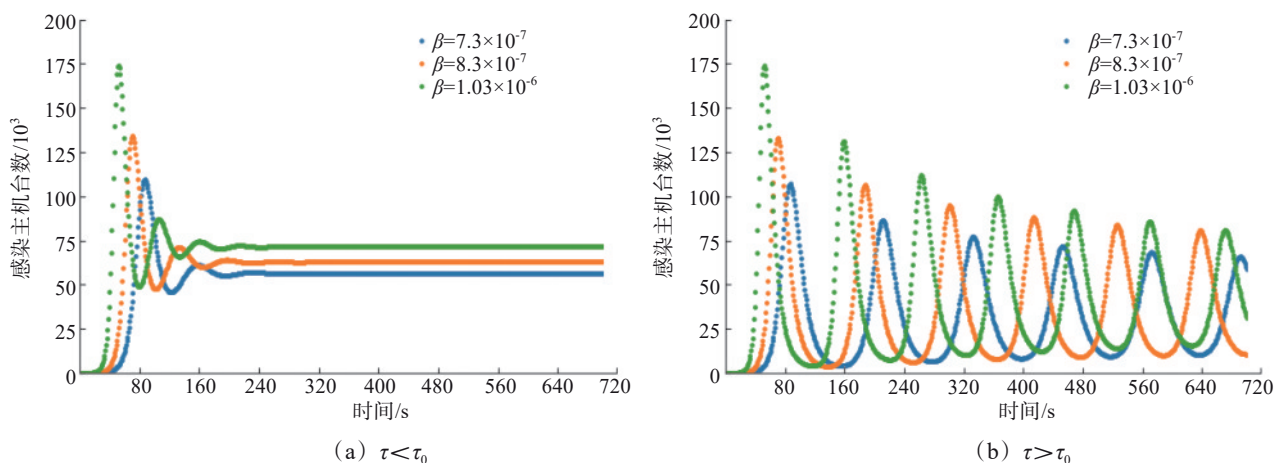
图7 参数 α 对被感染主机的数量的影响Fig.7 impact of parameter α values on the number of infected hosts.

图8 感染率与被感染主机台数关系

Fig.8 relationship between infection rates and the number of infected hosts

对比图8(a)和图8(b)可见,时延对恶意软件传播影响更显著。在时延较小时,系统能够有效抑制高感染率下的恶意软件传播,保持系统的稳定性。而在时延较大时,即使降低感染率,恶意软件的扩散仍不可控,导致系统不稳定。因此,综合考虑感染率和时延以及系统的响应能力,是确保工业互联网安全的核心逻辑。在实际应用中,应通过优化网络架构和提高防御系统响应能力,减少时延的影响,确保恶意软件的传播能够在初期得到有效控制。

(4) α 对系统稳定性影响

当 $\tau < \tau_0$ 和 $\tau > \tau_0$ 时,不同 α 对被感染主机的数量的影响情况见图9。由图9(a)可见, α 较大时,恶意软件传播受到有效抑制,工业互联网能够快速恢复安全状态;而当 α 较小时,感染范

围扩大,感染主机数量增速加快且峰值显著提高。由图9(b)可见,在 α 较小时,恶意软件会持续存在并长期传播;随着隔离率提高,感染主机数量迅速减少,证明提高隔离率能有效遏制恶意软件扩散,但由于时延较大,系统仍不稳定。综合分析图9可知,隔离率与感染主机台数的峰值呈负相关关系, α 越小,恶意软件传播越难控制,感染规模也越大。因此,在实际应用中,为防止恶意软件的蔓延,必须根据传播阶段的不同动态调整隔离率。在感染初期,系统需要保证一定的运行效率,可以维持较低的隔离率,以减少过早的资源消耗和对系统性能的影响;而当感染扩散加速时,必须及时提高隔离率,以控制感染范围,确保系统不陷入失控状态。

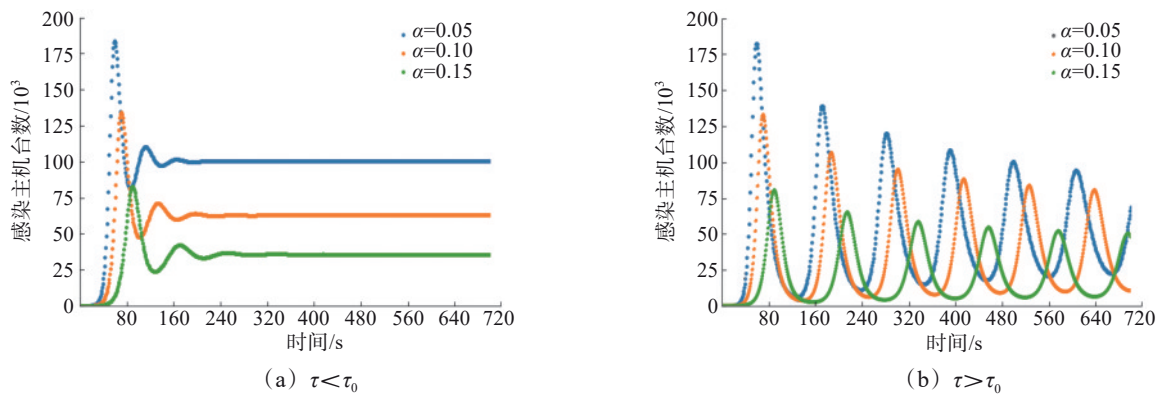


图9 隔离率与被感染主机数量关系

Fig.9 relationship between isolation rates and the number of infected hosts.

(5) γ 对系统稳定性影响

不同 γ 对感染主机数量的影响见图 10。由图 10 可见, 当 γ 较高时, 感染主机能快速转变为恢复状态, 有效减缓恶意软件传播速度, 促使系统趋于稳定; 反之, 当恢复率较低时, 主

机恢复速率显著降低, 恶意软件传播周期延长, 扩散风险加剧。低恢复率会延长感染主机的恢复时间, 增加恶意软件的持续传播时间。这种现象不仅会增加恶意软件威胁的消除难度, 还会显著加剧工业互联网的安全风险。

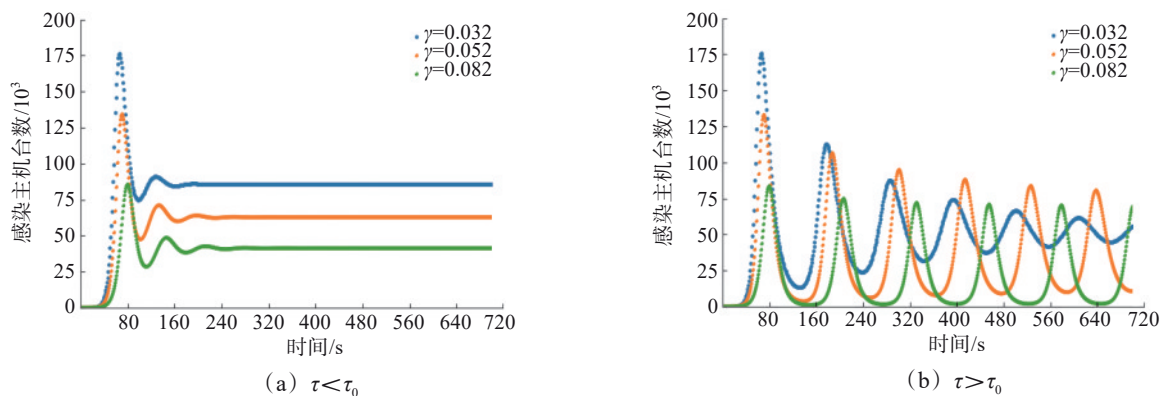


图10 恢复率与被感染主机数量关系

Fig.10 relationship between recovery rates and the number of infected hosts

由图 10 (a) 可知, 时延小于阈值时, 恢复率的优化能够更为有效地控制恶意软件的传播, 减少潜在的安全威胁。而由图 10 (b) 可知, 时延过大时, 防御系统对恶意软件的响应变得迟缓, 恢复措施无法及时有效地隔离和清除感染主机, 导致恶意软件的传播失控。在这种情况下, 提高恢复率的效果被时延的影响所削弱, 系统的稳定性无法得到有效保障。

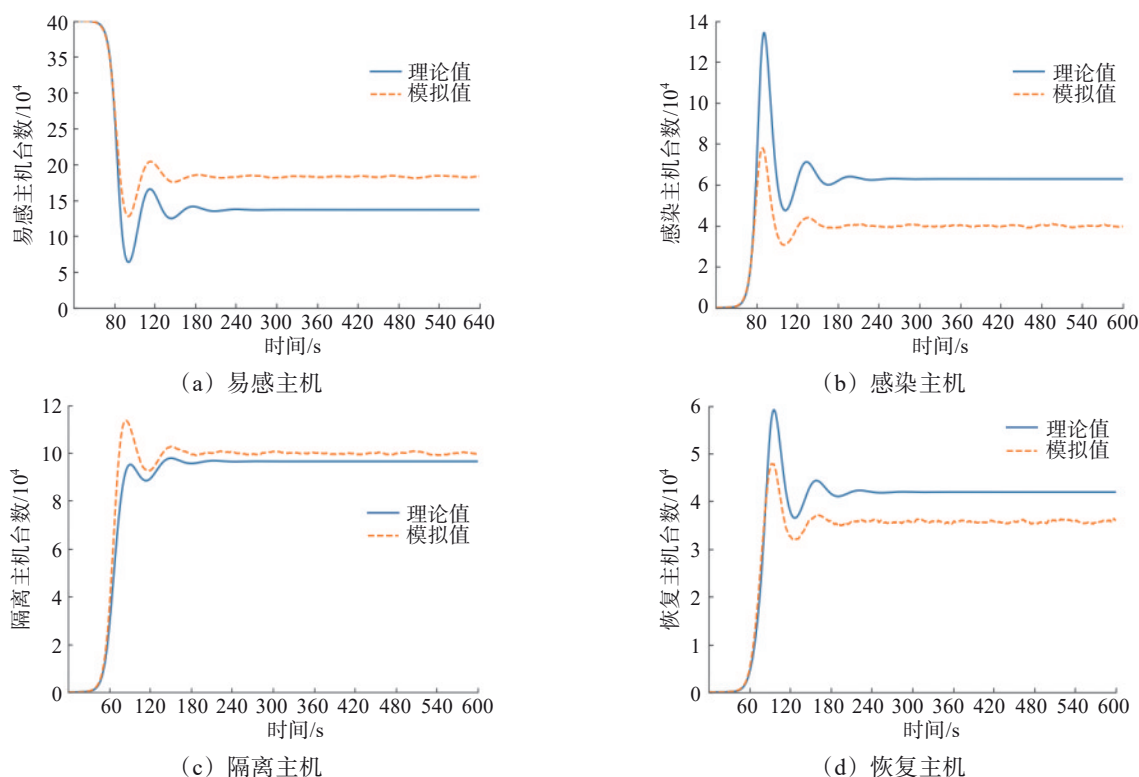
因此, 在实际应用中, 除了提高恢复率外, 还应优化网络的时延特性, 减少时延对系统恢复的负面影响, 从而构建更为高效和稳定的防御体系。

综上, 在工业互联网中, 通过合理选择参数值可有效控制恶意软件传播, 进而制定更优化的防御策略。在实际应用中, 可以根据网络的实际情况和攻击的不同阶段, 合理调整这些参数, 灵活应对恶意软件的传播趋势, 避免系统陷入失控状态。

(6) 理论值与模拟值对比

为了更加准确地描述恶意软件的传播行为, 本部分设计了仿真实验来验证理论分析和数值模拟结果的一致性和正确性:

4 种主机在 $\tau=20<\tau_0$ 时的理论值与模拟值的对比情况见图 11, 由图 11 可知, 4 种主机的模拟值与理论值的总体趋势变化一致。证明数值实验可以准确反映恶意软件传播的动态过程, 模型在不同阶段的表现与实际系统的运行情况相符。易感主机的数量在初期迅速下降, 而感染主机数量在短时间内急剧攀升至峰值后持续衰减。这表明, 防护机制未完全介入之前的传播初期, 恶意软件快速传播并迅速感染大量主机。随着隔离机制的介入, 传播范围得到抑制, 最终促使工业互联网系统恢复稳定状态。这一规律验证了模型对恶意软件传播动力学特征的准确描述。

图 11 4 种主机在 $\tau=20 < \tau_0$ 时的理论值与模拟值对比Fig.11 comparison of theoretical and simulated values for four types of hosts at $\tau=20 < \tau_0$

(7) 对比实验

为验证模型的有效性, 通过数值仿真实验, 在相同参数设置下对比 SIDQV 模型与经典 SIRD 模型 (不考虑隔离率的变化), 结果见图 12, 由图 12 可知, 本文提出的 SIDQV 模型的感染峰值明显低于 SIRD 模型。说明在相同的隔离资源下, 动态调整隔离率可以有效降低感染峰值和感染总量, 控制恶意软件的传播。SIDQV 模型通过实时调整隔离率应对网络中的感染主机数量, 使得系统能够灵活响应感染的变化。在传播初期, 系统可采用

较低的隔离率, 以保证网络的流畅性和资源的有效利用。随着感染主机数量的增加, 系统则会自动提高隔离率, 限制更多主机的感染。相比之下, SIRD 模型始终依赖固定的隔离策略, 导致感染主机的数量在较长时间内维持较高水平, 无法如 SIDQV 模型那样快速有效地遏制恶意软件的扩散。因此, 引入可变隔离率和时延因素, 可使 SIDQV 模型能够提供比传统静态模型更精确的传播预测与更高效的防控措施。

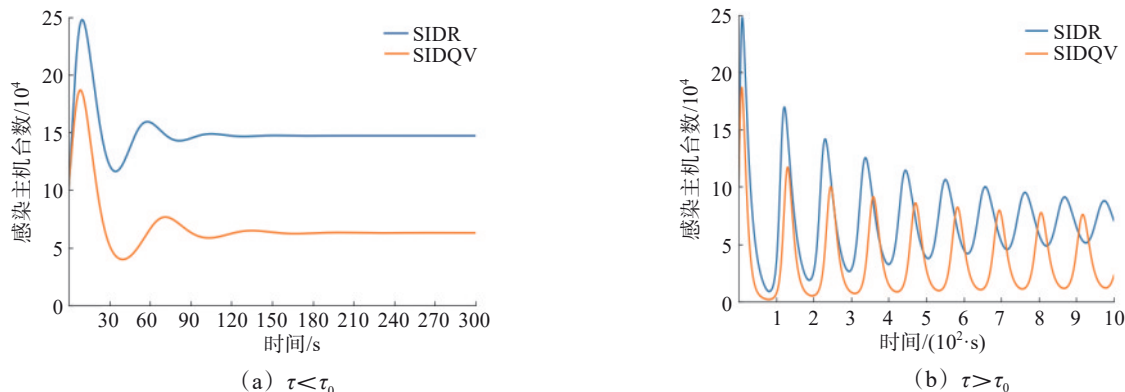


图 12 相同参数下 SIRD 与 SIDQV 模型感染主机数量对比

Fig.12 comparison of the number of infected hosts between the SIRD and SIDQV models under the same parameters.

4 结论

(1) 可变隔离率的SIDQV模型在特定条件下具有一个正平衡点,且当时延超过阈值时,系统会失去稳定并出现Hopf分岔现象。

(2) 在参数合理调控下,采用动态隔离策略可降低恶意软件的感染峰值,并减小其恶意软件的传播速度和范围,增强工业互联网的防护能力。因此,本文提出的模型和抑制策略能够为工业互联网的防护提供明确的参数指导,提高其对恶意软件传播的应对能力与稳定性。

(3) 模型仍存在一定的局限性。首先,在处理超大规模网络时,模型可能会面临计算资源和时间方面的挑战。其次,模型参数调整的过程较为复杂,需要针对不同的网络环境进行细致调整。在未来的工作中,可以考虑更复杂的网络拓扑结构并引入更多的实际约束,以进一步提高模型的逼真度和工程实用性。

参考文献(References):

- [1] WANG C, JIANG C X, WANG J J, et al. Blockchain-aided network resource orchestration in intelligent Internet of Things[J]. IEEE Internet of Things Journal, 2023, 10(7): 6151-6163.
- [2] KUN X, WANG Z L, ZHOU Z A, et al. Design of industrial Internet of Things system based on machine learning and artificial intelligence technology[J]. Journal of Intelligent & Fuzzy Systems, 2021, 40(2): 2601-2611.
- [3] MENDONÇA R V, SILVA J C, ROSA R L, et al. A lightweight intelligent intrusion detection system for industrial Internet of Things using deep learning algorithms[J]. Expert Systems, 2022, 39(5): e12917.
- [4] KHAN I A, KESHK M, PI D C, et al. Enhancing IIoT networks protection: a robust security model for attack detection in Internet Industrial Control Systems[J]. Ad Hoc Networks, 2022, 134: 102930.
- [5] TRAUTMAN L J. Industrial cyber vulnerabilities: lessons from stuxnet and the Internet of Things[J]. SSRN Electronic Journal, 2017, 72: 761-826.
- [6] BINDRA A. Securing the power grid: protecting smart grids and connected power systems from cyberattacks[J]. IEEE Power Electronics Magazine, 2017, 4(3): 20-27.
- [7] MAKRAKIS G M, KOLIAS C, KAMBOURAKIS G, et al. Industrial and critical infrastructure security: technical analysis of real-life security incidents[J]. IEEE Access, 2021, 9: 165295-165325.
- [8] AKBARZADEH A. Dependency based risk analysis in Cyber-Physical Systems[D]. Trondheim: Norwegian University of Science and Technology, 2023: 5-8.
- [9] FLÓREZ J, MONTOYA G A, LOZANO-GARZÓN C. An epidemiological SIS malware spreading model based on Markov chains for IoT networks[C]//Proceedings of Eighth International Congress on Information and Communication Technology. Singapore: Springer Nature Singapore, 2023: 663-672.
- [10] JHUN B, JO M, KAHNG B. Simplicial SIS model in scale-free uniform hypergraph[J]. Journal of Statistical Mechanics: Theory and Experiment, 2019, 12(12): 123207.
- [11] DADLANI A, KUMAR M S, KIM K, et al. Stability and immunization analysis of a malware spread model over scale-free networks[J]. IEEE Communications Letters, 2014, 18(11): 1907-1910.
- [12] DEL REY A M, VARA R C, GONZÁLEZ S R. A computational propagation model for malware based on the SIR classic model[J]. Neurocomputing, 2022, 484: 161-171.
- [13] TAGHVAEI A, GEORGIOU T T, NORTON L, et al. Fractional SIR epidemiological models[J]. Scientific Reports, 2020, 10: 20882.
- [14] TAYNITSKIY V, GUBAR E, ZHU Q Y. Optimal impulse control of bi-virus SIR epidemics with application to heterogeneous Internet of Things[C]//2017 Constructive Nonsmooth Analysis and Related Topics (Dedicated to the Memory of V.F. Demyanov). May 22-27, 2017, St. Petersburg, Russia. IEEE, 2017: 1-4.
- [15] XIAO M, CHEN S, ZHENG W X, et al. Tipping point prediction and mechanism analysis of malware spreading in cyber-physical systems[J]. Communications in Nonlinear Science and Numerical Simulation, 2023, 122: 107247.
- [16] DEL REY A M, ENCINAS A H, VAQUERO J M, et al. A method for malware propagation in industrial critical infrastructures[J]. Integrated Computer-Aided Engineering, 2016, 23(3): 255-268.
- [17] MAHBOUBI A, CAMTEPE S, MORARJI H. A study on formal methods to generalize heterogeneous mobile malware propagation and their impacts[J]. IEEE Access, 2017, 5: 27740-27756.
- [18] YAO Y, FU Q, YANG W, et al. An epidemic model of computer worms with time delay and variable infection rate[J]. Security and Communication Networks, 2018, 2018: 9756982.
- [19] YU Z H, GAO H X, WANG D, et al. SEI²RS malware propagation model considering two infection rates in cyber-physical systems[J]. Physica A: Statistical Mechanics and its Applications, 2022, 597: 127207.
- [20] YANG W, FU Q, YAO Y. A malware propagation model with dual delay in the industrial control network[J]. Complexity, 2023, 2023: 8823080.