零日病毒传播模型及稳定性分析

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

摘 要：针对零日病毒特点和传播规律，该文研究了零日病毒传播模型及稳定性。首先，分析了零日病毒传播机理，在易感-感染-移除-易感(SIRS)病毒传播模型基础上，重新定义了感染状态节点，引入执行状态节点和毁损状态节点，建立了零日病毒传播的易感-初始感染-零日-毁损-移除(SIZDR)病毒传播动力学模型；其次，运用劳斯稳定性判据，分析了系统平衡点的局部稳定性，基本再生数R_0及其对病毒传播规模的影响。最后，仿真验证了模型局部稳定性，分析了节点感染率、节点度和节点毁损率等因素对零日病毒传播的影响。理论分析与仿真结果表明，该模型能客观反映零日病毒传播规律，零日病毒扩散规模与节点度、节点感染率正相关，与节点毁损率负相关，对已知病毒的针对性防控可有效提升对零日病毒的防御效果。

关键词：零日病毒；病毒传播模型；稳定性
中图分类号：TP393; TP309.5 **文献标识码**：A **文章编号**：1009-5896(2021)07-1849-07
DOI: 10.11999/JEIT200519

Zero-day Virus Transmission Model and Stability Analysis

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

Abstract: According to the characteristics and propagation law of zero-day virus, the propagation model and stability of zero-day virus are studied. Firstly, the mechanism of zero-day virus transmission is analyzed. Based on the Susceptible-Infected-Removed-Susceptible(SIRS) virus transmission model, the node of infection state is redefined, the node of execution state and the node of damage state are introduced, and the zero-day virus transmission Susceptible - Initial-state-of infection- Zero-day - Damaged – Recovery (SIZDR) dynamic model is established. Secondly, the local stability of the system equilibrium point, the basic regeneration number and its influence on the scale of virus transmission are analyzed by using Rous stability criterion. Finally, the local stability of the model is verified by simulation, and the influence of node infection rate, node degree and node damage rate on zero-day virus transmission is analyzed. Theoretical analysis and simulation results show that the proposed model can objectively reflect the law of zero-day virus transmission, and the magnitude of zero-day virus spread is positively correlated with node degree and node infection rate, and negatively correlated with node damage rate. Targeted prevention and control of known viruses can effectively improve the defense effect against zero-day viruses.

Key words: Zero-day attack; Virus propagation model; Stability

1 引言

零日漏洞是指被发现后立即被恶意利用的安全漏洞，又称为零时差攻击，主要存在于软件和操作系统中。黑客和非法组织通常利用目标用户存在的零日漏洞，编写恶意代码并实施针对性攻击，这类基于零日漏洞的恶意代码称为零日病毒。与传统病毒相比，零日病毒传播机理相对复杂，具有隐蔽突发性强、破坏性大和防御难度大等特点。从零日病毒的攻防两端分析，防御方的被动弱势地位更明显。攻击者具有零日漏洞信息的优先权和掌握优势，防御者对这种漏洞一无所知，或者即使知道暂时也无能为力；开发零日漏洞的补丁较已知漏洞而言，工作量明显更大，开发时间也明显更长。2010年伊朗“震网”病毒事件[1]，让人们对零日漏洞有了深刻的认识。研究表明，该病毒是先通过木马和蠕虫等恶意程序与rootkit相结合，将rootkit这一恶

收稿日期：2020-06-23；改回日期：2020-11-26；网络出版：2020-12-01
*通信作者： 王刚 wglxl@nudt.edu.cn
基金项目：国家自然科学基金(61573017)
Foundation Item: The National Nature Science Foundation of China (61573017)

意软件及恶意代码注入并隐藏在目标主机上[1]，并利用恶意代码中具有提升权限功能的零日病毒，获得目标主机的内核级权限。接着，该恶意代码在分析核设施的相关数据后，利用其余的零日漏洞以及已知漏洞，在核心部件中分别进行了自我复制、传播、破坏等非法活动，最终导致伊朗核物理设施全面瘫痪。据报道与Windows10系统有关的零日攻击事件对用户造成了严重影响[2]。此外，WannaCry勒索病毒也是典型的零日攻击事件，该事件造成全世界大约99个国家金融、能源、医疗等行业出现危机管理问题[3]。

零日病毒的攻防博弈特点使得防御方始终处于被动地位，客观上加大了防御难度和复杂度，零日病毒防御已经成为目前网络安全领域亟待解决的现实问题。当前比较成熟的病毒防御手段都致力于微观上研究病毒自身作用机理，重在查漏补缺。而“零日”是一相对概念，防御方对零日漏洞的掌握必然晚于攻击方，难以及时修复。因此，当前对零日病毒防御方面的研究重点在于攻击行为的发现和病毒样本的捕捉[4–10]。如Sun等人[4]考虑到利用先验知识库中信息会造成信息爆炸的情况，提出一种基于计算机系统调用生成数据图的方法并利用贝叶斯网络对可能的零日攻击路径进行概率认证。通过该方法，提高了零日攻击认证正确率同时减少了数据分析量；考虑到传统的机器学习技术很难检测出零日攻击而深度学习技术具有极强的特征提取能力这一情况，Diro等人[6]针对社会物联网中的零日攻击提出利用深度学习方法来进行检测并比较了传统机器学习与深度学习在发掘零日攻击行为方面的性能差异。这些防御技术理论上能检测到利用零日病毒发起的攻击并采集样本，对零日病毒的防御有着积极的意义。但是，零日病毒的彻底清除依然依赖于相应补丁和查杀手段，而病毒入侵前期往往缺乏这些手段，需要投入时间和精力进行开发工作。为了避免零日病毒在入侵初期大范围传播，造成负面影响甚至瘫痪网络，可考虑病毒在感染与传播过程中存在的共性因素，从相对宏观的角度研究零日病毒在网络中的传播问题，进而采取针对性措施对病毒传播的速度与规模加以控制。当前病毒传播研究主要通过动力学建模方法，研究病毒的传播机理并提出相应的控制手段。相关研究最初借鉴了生物学病毒传播理论，将易感-感染-移除(Susceptible-Infected-Removed, SIR)模型[11]和易感-感染-移除-易感(Susceptible–Infected–Removed–Susceptible, SIRS)模型[12]等经典病毒传播模型应用于计算机病毒传播领域。近年来，相关研究主要是结合具体应用背景，有针对性地引入新的节点状态或调整节点状态转化机制对病毒传播机理进行研究[13-17]。如针对高级持续性威胁(Advanced Persistent Threat, APT)攻击和病毒潜伏特性，王刚等人[13]引入了潜伏状态，提出了易感-潜伏-感染-隔离-移除-易感(Susceptible–Escape-Infected–Quarantine-Removed–Susceptible, SEIQRS)模型，研究了基于潜伏隔离机制下的病毒传播规律。文献[11]通过研究一类新型混合攻击病毒，将该类病毒命名为“去二存一”病毒并在SEIQRS模型的基础上根据该类病毒的扩散机理，构建了相应的病毒传播模型。Wang等人[14]考虑到现有的病毒传播模型由于简化近似，对大型网络中病毒传播分析造成准确性损失这一情况，构造了离散时间吸收马尔可夫过程来精确地描述病毒的传播，并通过仿真分析论证了该方法的准确性。为了更加精准地刻画病毒在智能校园网上的传播过程，Wang等人[15]考虑感染病毒个体间的差异性，将病毒感染个体的进化过程扩展到整个网络中，建立了智能校园网的病毒传播差分模型从而大大提高了智能校园网的安全性与鲁棒性。文献[16]在考虑级联故障普遍存在于复杂网络中的这一情况，提出了基于局部负荷重分配原则的新型级联失效模型，建立了SIR病毒传播与级联失效的交互模型：SIR- c模型，为网络拓扑和路由策略的管理和优化提供了理论参考。文献[17]考虑实际网络中节点可以随机移动的情况，基于平均场理论提出了一个移动环境下网络病毒传播的数学模型，并验证了这一模型的合理性。这些研究揭示了病毒传播的一般规律，为病毒的有效防控提供了理论基础。然而不同病毒传播模型有其适用范围，零日病毒传播机理相对复杂、隐蔽性强、防御难度大且破坏性大，需要具体问题具体分析，在现有研究成果的基础上，结合零日病毒特点研究零日病毒的传播规律及防控手段。

本文基于对零日病毒传播机理的认知，建立与零日病毒传播过程相适应的易感-初始感染-零日-毁损-移除(Susceptible - Initial-state-of infection-Zero-day - Damaged - Removed, SIZDR)网络病毒传播模型，本模型在传统SIRS病毒扩散模型基础上定义了初始感染状态、零日病毒执行状态以及毁损状态，并以模型为基础研究零日病毒传播过程的机理和稳定性，给出了不同病毒传播影响因素对网络系统存活率的影响结果。通过研究掌握零日病毒传播的规律，为零日病毒防御策略和技术实现提供理论参考。

2　零日病毒传播模型

按照网络病毒作用机理，零日病毒传播过程可划分为初始感染、病毒传播、病毒发作和毁损等4个阶段。(1)在初始感染阶段，攻击者利用木马或者蠕虫等常见的已知病毒将以隐藏非法活动为目的的恶意代码植入目标主机当中。同时，被已知病毒攻击的目标主机与已经感染零日病毒的目标主机接触后以一定的概率被植入零日病毒。在这一阶段，防御方可以通过反病毒软件将木马或者蠕虫等已知病毒拦截。如果拦截成功，节点将处于免疫状态。处于免疫状态的目标主机有可能因为系统重装等使得其再次处于易感状态。(2)在病毒传播阶段，已经感染零日病毒的目标主机中，零日病毒利用零日漏洞将自己复制并传播至其他目标主机当中。在这一过程中，针对零日漏洞的恶意代码随着大量复制的恶意文件流入其他目标主机而在整个网络中传播。(3)病毒发作阶段，当已经感染零日病毒的目标主机满足一定条件时将会激活零日病毒(例如：在震网病毒摧毁核设施的过程中，当恶意代码分析出其所感染的物理设施是核心部件时，零日病毒才会进行攻击)，零日病毒对相应的目标实施攻击。本文将病毒传播和病毒发作两个阶段统称为零日病毒执行阶段，简称零日阶段。(4)在毁损阶段。由于零日漏洞的未知性，防御方难以及时地发现并阻止零日病毒实施非法活动，最终目标主机被零日病毒所摧毁。防御方为了确保网络的正常运转，会将被毁损的目标主机进行修复或者更新。

经典SIRS模型是分析流行病传播的常用模型。该模型相对成熟且更适用于现阶段计算机病毒传播，因此，在对零日病毒传播过程的分析基础上，对传统的病毒传播SIRS模型进行了改进。本文重新定义了一个节点状态并引入了两个新的节点状态，分别是：初始感染状态I(Initial-state-of-infection)、零日病毒执行状态(简称零日状态)Z(Zero-day)和毁损状态D(Damaged)。提出了SIZDR模型，其状态转移关系如图1所示。

(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，节点由易感状态转化为初始感染状态。其中，$\eta{=}\beta K\cdot Z(t)/N$, β代表节点接触概率，K代表节点度值，$Z(t)$表示在t时刻零日状态节点数量。

(2) 初始感染状态I→免疫状态R。目标主机中的反病毒软件等安全系统对已知漏洞病毒的捕获，使得感染已知漏洞病毒的节点及时被查杀，并利用补丁修复了相关漏洞从而使得感染已知漏洞病毒状态的节点向免疫状态转化。α代表了感染已知漏洞病毒的免疫率。

(3) 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。

(4) 初始感染状态I→零日状态Z。防御系统的失误使得初始感染状态的目标并没有被查杀，从而使得恶意代码有机会执行针对零日漏洞的恶意代码。当满足一定条件时，零日病毒实施非法活动，造成初始感染状态向零日状态转化。γ代表零日病毒发起攻击的概率。

(5) 零日状态Z→毁损状态D。零日病毒的隐蔽性使得该病毒无法被防御系统识别并阻止其非法活动，从而导致感染零日病毒的目标主机被毁损。σ代表感染零日病毒后的毁损率。

(6) 毁损状态D→易感状态S。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，因此目标主机在被毁损后，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代表由毁损状态恢复为易感状态的恢复率。

设网络相对稳定且节点总数N为各状态节点数量和，$S(t)$, $I(t)$, $Z(t)$, $D(t)$分别表示t时刻易感状态节点，初始感染状态节点，零日状态节点以及毁损状态节点的数量，则对应免疫节点数量可表示为$R(t)=N-S(t)-I(t)-Z(t)-D(t)$。根据微分动力学原理，可得模型对应的动力学方程

$$\left.\begin{aligned}
&\frac{\mathrm{d}S(t)}{\mathrm{d}t}=\frac{-\beta KS(t)\cdot Z(t)}{N}+\upsilon\cdot R(t)+\omega\cdot D(t)\\
&\frac{\mathrm{d}I(t)}{\mathrm{d}t}=\frac{\beta KS(t)\cdot Z(t)}{N}-\alpha\cdot I(t)-\gamma\cdot I(t)\\
&\frac{\mathrm{d}Z(t)}{\mathrm{d}t}=\gamma\cdot I(t)-\sigma\cdot Z(t)\\
&\frac{\mathrm{d}D(t)}{\mathrm{d}t}=\sigma\cdot Z(t)-\omega\cdot D(t)\\
&R(t)=N-S(t)-I(t)-Z(t)-D(t)
\end{aligned}\right\}\quad(1)$$

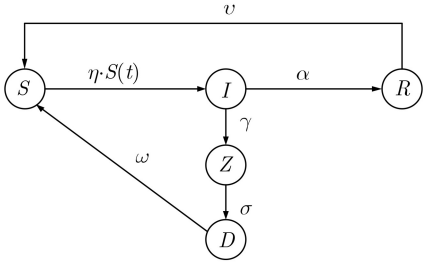


图 1 SIZDR病毒传播模型

3 稳定性分析

网络病毒传播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，且在受到干扰后能够回到平衡点的位置。令式(1)中$\frac{\mathrm{d}S}{\mathrm{d}t}=0$, $\frac{\mathrm{d}I}{\mathrm{d}t}=0$, $\frac{\mathrm{d}Z}{\mathrm{d}t}=0$, $\frac{\mathrm{d}D}{\mathrm{d}t}=0$，网络始终存在平衡点$\boldsymbol{P}^0(S^0,I^0,D^0,Z^0)=(N,0,0,0)$。此外，式(1)中存在另一个平衡点$\boldsymbol{P}^1(S^1,I^1,D^1,Z^1)=\left(\frac{(\alpha+\gamma)\sigma}{\beta K\gamma}\cdot N,I^1,\frac{\gamma}{\sigma}I^1,\frac{\gamma}{\omega}I^1\right)$，其中$I^1=\frac{[\beta K\gamma-(\alpha+\gamma)\sigma]\upsilon N}{\beta K\gamma[\omega\sigma(\alpha+\upsilon)+\upsilon\gamma(\omega+\sigma)]}$，基本再生数为$R_0=\frac{\beta K\gamma}{(\alpha+\gamma)\sigma}$。当$R_0>1$时，即$I^1>0$时，存在有病毒平衡点；当$R_0=1$时，即$I^1=0$时，存在无病毒平衡点；当$R_0<1$时，即$I^1<0$时，根据实际情况节点个数不为负，因此存在无病毒平衡点。

设$\boldsymbol{P}^*(S^*,I^*,Z^*,D^*)$为式(1)的任意平衡点，则式(1)的雅可比矩阵$\boldsymbol{J}(\boldsymbol{P}^*)$为

$$\boldsymbol{J}(\boldsymbol{P}^*)=\begin{pmatrix}\frac{-\beta kZ}{N}-\upsilon & -\upsilon & \frac{-\beta kS}{N}-\upsilon & \omega-\upsilon\\ \frac{\beta kZ}{N} & -(\alpha+\gamma) & \frac{\beta kS}{N} & 0\\ 0 & \gamma & -\sigma & 0\\ 0 & 0 & \sigma & -\omega\end{pmatrix} \tag{2}$$

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

证明： 由式(2)可得平衡点P^0处的雅可比矩阵$\boldsymbol{J}(\boldsymbol{P}^0)$为

$$\boldsymbol{J}(\boldsymbol{P}^0)=\begin{pmatrix}-\upsilon & -\upsilon & -\beta K-\upsilon & \omega-\upsilon\\ 0 & -(\alpha+\gamma) & \beta K & 0\\ 0 & \gamma & -\sigma & 0\\ 0 & 0 & \sigma & -\omega\end{pmatrix} \tag{3}$$

矩阵$\boldsymbol{J}(\boldsymbol{P}^0)$对应的特征多项式为

$$(\lambda+\upsilon)(\lambda+\sigma)(\lambda+\omega)[(\lambda+\alpha+\gamma)(\lambda+\sigma)-\beta K\gamma]=0 \tag{4}$$

解得特征根$\lambda_1=-\upsilon$, $\lambda_2=-\sigma$, 经计算得$\lambda_3<0,\lambda_4<0$。当$R_0\le 1$时，$\lambda_1,\lambda_2,\lambda_3,\lambda_4<0$，$\boldsymbol{P}^0$处局部稳定；当$R_0>1$时$\lambda_4$这一特征根为正，平衡点$\boldsymbol{P}^0$处局部不稳定。 证毕

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

证明： 由式(2)可得平衡点$\boldsymbol{P}^1$处的雅可比矩阵$\boldsymbol{J}(\boldsymbol{P}^1)$为

$$\begin{pmatrix}-\frac{\beta kI^1}{N}-\upsilon & -\upsilon & -\frac{\beta kS^1}{N}-\upsilon & \omega-\upsilon\\ \frac{\beta kI^1}{N} & -(\alpha+\gamma) & \frac{\beta kS^1}{N} & 0\\ 0 & \gamma & -\sigma & 0\\ 0 & 0 & \sigma & -\omega\end{pmatrix} \tag{5}$$

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

$$\lambda^4+\mu_1\lambda^3+\mu_2\lambda^2+\mu_3\lambda+\mu_4=0 \tag{6}$$

其中

$$\left.\begin{aligned}\mu_1&=\frac{\beta KI^1}{N}+\sigma+\upsilon+\omega+\alpha+\gamma\\ \mu_2&=(\alpha+\gamma)\sigma-\frac{\beta KS^1\gamma}{N}+(\alpha+\gamma+\sigma)(\upsilon+\omega)\\ &\quad+\upsilon\omega+\frac{\beta KI^1}{N}(\sigma+\upsilon+\omega+\alpha+\gamma)\\ \mu_3&=\left[(\alpha+\gamma)\sigma-\frac{\beta KS^1\gamma}{N}\right](\upsilon+\omega)+\upsilon\omega(\alpha+\gamma+\sigma)\\ &\quad+\frac{\beta KI^1}{N}[\omega\sigma+(\upsilon+\alpha+\gamma)(\sigma+\omega)+\upsilon\gamma]\\ \mu_4&=\left[(\alpha+\gamma)\sigma-\frac{\beta KS^1\gamma}{N}\right]\upsilon\omega\\ &\quad+\frac{\beta KI^1}{N}[(\alpha+\gamma)\omega\sigma+(\upsilon-\omega)\gamma\sigma+\upsilon\gamma\omega]\end{aligned}\right\} \tag{7}$$

当$R_0>1$时，$\mu_1,\mu_2>0$, $\mu_1\mu_2-\mu_3>0$且$\mu_1\mu_2\mu_3-{\mu_3}^2-\mu_1\mu_4>0$。根据劳斯-赫尔维茨稳定判据，在平衡点$\boldsymbol{P}^1(S^1,I^1,D^1,Z^1)$处局部稳定。 证毕

上述结论表明，当$R_0\le 1$时，系统在无病毒平衡点$\boldsymbol{P}^0$处局部渐近稳定，即网络系统中没有感染病毒的节点，初始感染节点和零日状态节点全部被清除；当$R_0>1$时，系统在感染源平衡点$\boldsymbol{P}^1(S^1,I^1,Z^1,D^1)$处局部渐近稳定，即网络系统中既有初始感染状态节点又有零日状态的节点，同时还有部分节点处于毁损状态。

分析基本再生数$R_0=\beta K\gamma/[(\alpha+\gamma)\sigma]$可知，$\beta$, K和基本再生数R_0正相关，R_0越大；α, σ与网络基本再生数负相关，R_0越小。如果零日病毒传播过程中病毒的攻击强度不超过防御门限值，则网络系统可通过检杀-免疫机制修复感染节点，使网络系统最终恢复到没有病毒的正常状态，并趋于稳定；反之，如果攻击强度超过防御门限值，网络系统无法完全清除系统内感染节点，可以通过调整零日病毒传播过程中的相关参数有效控制零日病毒的传播。

4 仿真分析

在实际防控过程中，病毒实施非法活动的概率γ不易被调节，但可通过断开网络连接、提高操作

人员安全意识、人为移除感染节点等方法人为调整β,K,σ来抑制病毒扩散规模。因此，本文重点围绕节点感染系数、节点度值和毁损率等3个影响因素开展仿真验证。参照文献[13]中的仿真实验，设$\beta=0.5,\ K=4,\ \alpha=0.2,\upsilon=0.8$。设初始感染状态节点若不能被防御系统免疫，则转化为零日状态节点，即$\alpha+\gamma=1,\ \gamma=0.8$。鉴于零日漏洞的隐蔽性，设毁损率$\sigma=0.9$；被毁损主机恢复为正常主机的概率为$\omega=0.6$。设置节点总数$N=1000$，初始状态下，不同状态节点数为$(S(0),I(0),Z(0),D(0),R(0))=(970,20,10,0,0)$。在达到稳定状态的网络系统中，毁损节点的数量不能直观反映零日病毒对目标主机的毁损程度，而毁损节点的数量与网络系统中全部节点数量的比值可直观反映零日病毒对整个网络系统造成的影响。因此，定义毁损节点数量与网络系统中全部节点数量的比值为网络破坏率。

4.1 节点感染系数β

调整节点感染系数，来验证其对病毒传播的影响。通过理论分析可得节点感染系数阈值$\beta_{\lim}=0.28$，即当$\beta<\beta_{\lim}$时，系统将在$\boldsymbol{P}^0$处局部渐近稳定；反之，当$\beta>\beta_{\lim}$时，系统将会在$\boldsymbol{P}^1$处局部渐近稳定。分别取$\beta=0.2,\ 0.5,\ 0.8$进行研究分析。图2所示为不同β时对应的系统状态。

图2(a)—图2(c)分别对应$\beta=0.2,\ 0.5,\ 0.8$的系统状态。仿真结果表明，当$\beta=0.2$ $(\beta<\beta_{\lim})$时，系统在平衡点$\boldsymbol{P}^0(1000,0,0,0,0)$处局部渐近稳定；当$\beta=0.5(\beta>\beta_{\lim})$时，系统在$\boldsymbol{P}^1(562,126,112,168,32)$处局部渐近稳定；当$\beta=0.8$ $(\beta>\beta_{\lim})$时，系统在$\boldsymbol{P}^1(351,187,166,249,47)$处局部渐近稳定；当系统在局部渐近稳定平衡点$\boldsymbol{P}^1$处时，初始感染状态$I$的节点数随着$\beta$的增大而增大，零日状态节点数随着$\beta$的增大而增大。可见，节点感染率越大，零日病毒传播过程中病毒成功入侵目标主机的概率也越大，通过调节节点感染率β，可有效抑制零日病毒传播。

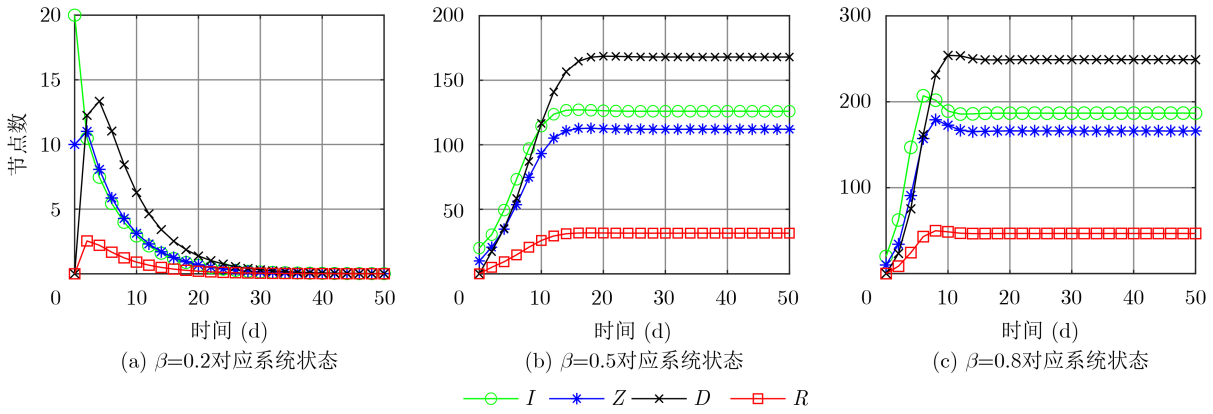
通过对不同β下节点毁损个数的统计可知，当节点感染率$\beta=0.2$时，网络破坏率为0；当节点感染率$\beta=0.5$时，网络破坏率为16.8%；当节点感染率$\beta=0.7$时，网络破坏率为24.9%。由统计数据可知，随着感染系数的提高，网络破坏率也越高。在实际情况中，防御方可通过调整感染率降低网络破坏率。

4.2 节点度K

通过调整节点度值来验证其对病毒传播的影响。通过理论分析可得节点度值的阈值$K_{\lim}=2.2$，即当$K<K_{\lim}$时，系统将在$\boldsymbol{P}^0$处局部渐近稳定；反之，当$K>K_{\lim}$时，系统将会在$\boldsymbol{P}^1$处局部渐近稳定。分别取$K=2,4,6$进行研究分析。图3分别表示不同K时对应的系统状态。

图3(a)—图3(c)分别对应$K=2,4,6$时的系统状态。仿真结果表明，当$K=2$ $(K<K_{\lim})$时，系统在平衡点$\boldsymbol{P}^0(1000,0,0,0,0)$处局部渐近稳定；当$K=4$ $(K>K_{\lim})$时，系统在$\boldsymbol{P}^1(562,126,112,168,32)$处局部渐近稳定；当$K=6$ $(K>K_{\lim})$时，系统在$\boldsymbol{P}^1(375,180,160,240,45)$处局部渐近稳定。当系统在局部渐近稳定平衡点$\boldsymbol{P}^1$处时，初始感染状态$I$的节点数随着$K$的增大而增大，零日状态节点数随着$K$的增大而增大。可见，节点度越大，零日病毒传播过程中的病毒成功入侵目标主机的概率也越大。通过调节节点度值K，可以有效地控制零日病毒实施非法活动。

通过对不同K时节点毁损个数的统计可知，当节点度$K=2$时，网络破坏率为0；当节点度$K=4$时，网络破坏率为16.8%；当节点度$K=6$时，网络破坏率为24.0%。由统计数据可知，随着节点度值的提高，网络破坏率也相应提高。在实际情况中，防御方应当调整网络拓扑结构降低节点度值从而使得网络破坏率尽可能低，但是降低网络破坏率势必通过降低节点度值来实现，一味降低节点度值将会影响到网络的性能。因此，防御方应当综合考



(a) β=0.2对应系统状态　(b) β=0.5对应系统状态　(c) β=0.8对应系统状态

图 2 不同β对应的系统状态

虑网络性能与网络破坏率的关系从而对零日病毒进行布防。

4.3 毁损率σ

通过调整毁损率来验证其对病毒传播的影响。根据实际情况，毁损率阈值应满足$\sigma_{\lim}<1$，可分别设$\sigma=0.5,0.7,0.9$。图4分别表示不同σ对应的系统状态。

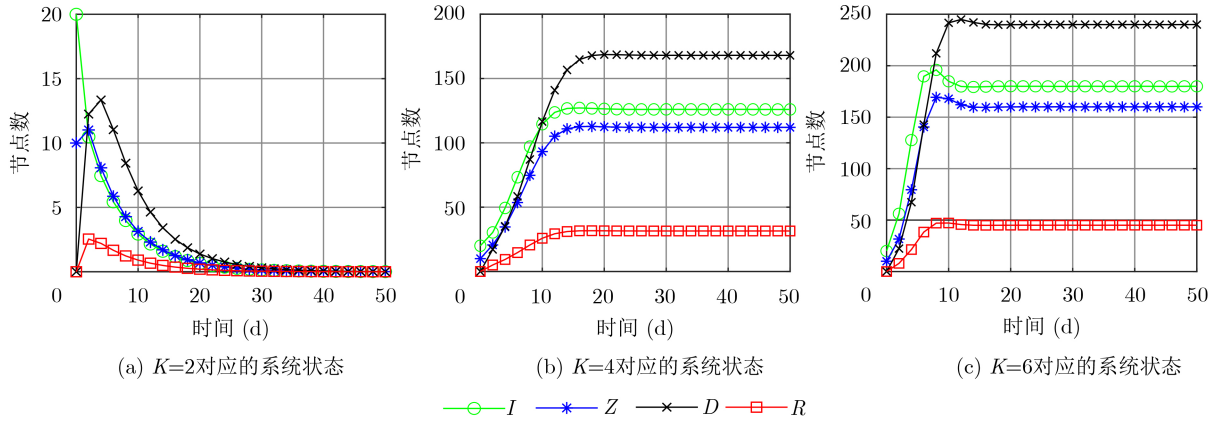
图4(a)—图4(c)分别对应$\sigma=0.5,0.7,0.9$时的系统状态。仿真结果表明，当$\sigma=0.5$时，系统在$\boldsymbol{P}^1(310,165,263,220,42)$处局部渐近稳定，当$\sigma=0.7$时，系统在$\boldsymbol{P}^1(436,151,173,202,38)$处局部渐近稳定；当$\sigma=0.9$时，系统在$\boldsymbol{P}^1(562,126,112,168,32)$处局部渐近稳定。当系统在局部渐近稳定平衡点$\boldsymbol{P}^1$处时，初始感染状态的节点数随着$\sigma$的增大而减小，零日状态节点数随着$\sigma$的增大而减小。可见，毁损率越大，网络系统中零日病毒的传播性能将会受到限制从而导致系统中未感染病毒节点的数量增加。

通过调节毁损率σ，可有效控制零日病毒传播。基于σ的统计表明，毁损率$\sigma=0.5$时，网络破坏率为21.9%；毁损率$\sigma=0.7$时，网络破坏率为20.0%；毁损率$\sigma=0.9$时，网络破坏率为16.8%。随着毁损率的升高，网络破坏率则越低，防御方恢复网络性能的代价也就越大。出现这种情况的原因是：当毁损率提高后，恢复率不变的情况下，网络中易感节点数量上升，初始感染节点和零日节点的数量都会下降，从而导致毁损节点的数量也相应下降。在实际情况中，防御方可适度调整毁损率与网络破坏率，使得恢复性能代价与网络破坏率在可接受范围内。

根据仿真分析结果，针对零日病毒的实际防控过程中，防御方可通过提高操作人员安全意识，减少操作人员具有安全风险的操作，从而降低节点感染系数；同时，根据网络拓扑结构以及网络功能，断开部分网络连接，从而在不严重影响网络业务承载能力的情况下，降低网络节点度K。防御方针对零日病毒进行的防御手段并不仅仅局限于以上两种方法，这些方法的核心思想就是通过调控基本再生数达到控制病毒传播的规模。

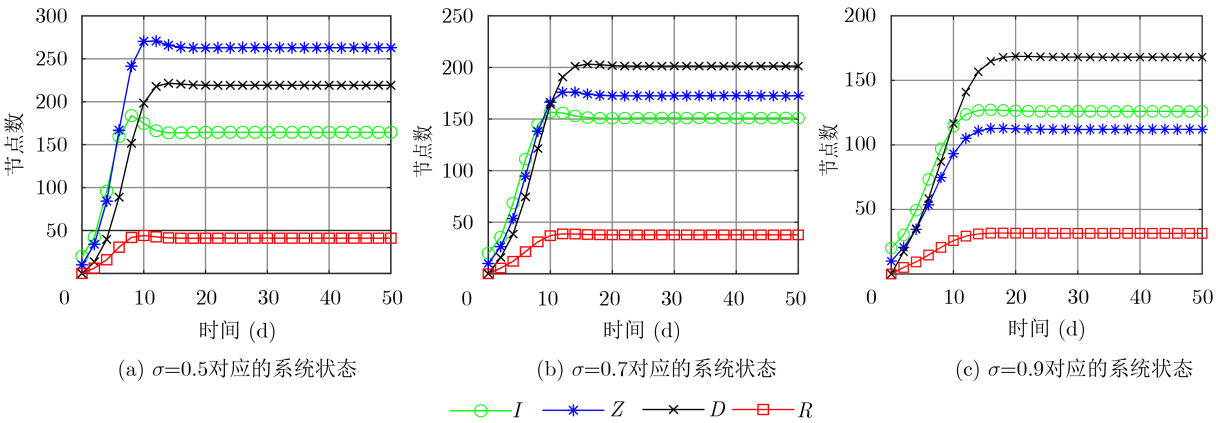
5 结束语

本文在SIRS模型基础上，结合零日病毒特点提出了SIZDR传播模型，通过稳定性分析，讨论了相关因素对病毒传播的影响，就节点度、感染率和毁损率3个参数开展了仿真实验。理论分析和仿真



(a) K=2对应的系统状态 (b) K=4对应的系统状态 (c) K=6对应的系统状态

图 3 不同K对应的系统状态



(a) σ=0.5对应的系统状态 (b) σ=0.7对应的系统状态 (c) σ=0.9对应的系统状态

图 4 不同σ对应的系统状态

结果表明，改变网络度、节点感染系数等参数，可以使得网络系统稳定在无病毒状态。在网络受到零日病毒的威胁时，通过对已知漏洞的合理防控和网络结构的调整，能一定程度上抑制零日病毒的传播甚至彻底消除病毒。论文中还存在一定的不足之处，后期的工作将进一步完善零日病毒传播模型并在零日病毒传播机理的基础上提出相应的免疫措施。

参 考 文 献

[1] ZETTER K. Countdown to Zero Day[M]. ZETTER K. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Broadway Books, 2015.

[2] Cnbeta. 卡巴斯基透露有黑客同时利用Windows 10和Chrome零日漏洞发动攻击[EB/OL]. http://cnnvd.org.cn/web/xxk/yjxwById.tag?id=11,170, 2019.

[3] Cnbeta. 网络安全研究人员发现新漏洞: 或成另一个WannaCry[EB/OL]. http://cnnvd.org.cn/web/xxk/yjxwById.tag?id=8,486, 2017.

[4] SUN Xiaoyan, DAI Jun, LIU Peng, *et al*. Using Bayesian networks for probabilistic identification of zero-day attack paths[J]. *IEEE Transactions on Information Forensics and Security*, 2018, 13(10): 2506–2521. doi: 10.1109/TIFS.2018.2821095.

[5] SUN Xiaoyan, DAI Jun, LIU Peng, *et al*. Using Bayesian Networks to Fuse Intrusion Evidences and Detect Zero-day Attack Paths[M]. WANG Lingyu, JAJODIA S, and SINGHAL A. Network Security Metrics. Cham: Springer, 2017.

[6] DIRO A A and CHILAMKURTI N. Distributed attack detection scheme using deep learning approach for internet of things[J]. *Future Generation Computer Systems*, 2018, 82: 761–768. doi: 10.1016/j.future.2017.08.043.

[7] KIM J Y, BU S J, and CHO S B. Zero-day malware detection using transferred generative adversarial networks based on deep Autoencoders[J]. *Information Sciences*, 2018, 460/461: 83–102. doi: 10.1016/j.ins.2018.04.092.

[8] 张瑜, 潘小明, LIU Qingzhong, 等. APT攻击与防御[J]. 清华大学学报: 自然科学版, 2017, 57(11): 1127–1133. doi: 10.16511/j.cnki.qhdxxb.2017.21.024.
ZHANG Yu, PAN Xiaoming, LIU Qingzhong, *et al*. APT attacks and defenses[J]. *Journal of Tsinghua University: Science & Technology*, 2017, 57(11): 1127–1133. doi: 10.16511/j.cnki.qhdxxb.2017.21.024.

[9] ZHANG Mengyuan, WANG Lingyu, JAJODIA S, *et al*. Network diversity: A security metric for evaluating the resilience of networks against zero-day attacks[J]. *IEEE Transactions on Information Forensics and Security*, 2016, 11(5): 1071–1086. doi: 10.1109/TIFS.2016.2516916.

[10] VALDEZ J S, GUEVARA P, AUDELO J, *et al*. 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.

[11] 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(S1): 64–67.
GU Haijun, JIANG Guoping, and XIA Lingling. SIRS epidemic model and its Threshold based on state transition probability[J]. *Computer Science*, 2016, 43(S1): 64–67.

[12] 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. doi: 10.11918/j.issn.0367-6234.201805136.
WANG Gang, LU Shiwei, HU Xin, *et al*. Network virus spreading SEIQRS model and its stability under escape mechanism[J]. *Journal of Harbin Institute of Technology*, 2019, 51(5): 131–137. doi: 10.11918/j.issn.0367-6234.201805136.

[13] 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. doi: 10.11999/JEIT180381.
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. doi: 10.11999/JEIT180381.

[14] 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.

[15] WANG Lei, YAO Changhua, YANG Yuqi, *et al*. Research on a dynamic virus propagation model to improve smart campus security[J]. *IEEE Access*, 2018, 6: 20663–20672. doi: 10.1109/ACCESS.2018.2817508.

[16] 秦李, 黄曙光, 陈骁. 病毒传播下的因特网级联故障模型构建与仿真[J]. 计算机应用研究, 2016, 33(4): 1228–1231, 1235. doi: 10.3969/j.issn.1001-3695.2016.04.059.
QIN Li, HUANG Shuguang, and CHEN Xiao. Model and simulation for cascading failure on internet based on virus propagation[J]. *Application Research of Computers*, 2016, 33(4): 1228–1231, 1235. doi: 10.3969/j.issn.1001-3695.2016.04.059.

[17] 巩永旺, 宋玉蓉, 蒋国平. 移动环境下网络病毒传播模型及其稳定性研究[J]. 物理学报, 2012, 61(11): 110205. doi: 10.7498/aps.61.110205.
GONG Yongwang, SONG Yurong, and JIANG Guoping. Epidemic spreading model and stability of the networks in mobile environment[J]. *Acta Physica Sinica*, 2012, 61(11): 110205. doi: 10.7498/aps.61.110205.

孟庆微：男，1980年生，博士后，副教授，研究方向为网络空间安全、通信信号处理.

仇铭阳：男，1997年生，硕士生，研究方向为网络空间安全.

王　刚：男，1977年生，博士，副教授，研究方向为信息网络系统建设与规划.

马润年：男，1963年生，博士后，教授，研究方向为生物计算、神经网络.

责任编辑：余　蓉