操作系统病毒传播模型及混合防御策略

李 娟[1,2],王 刚[1],冯 云[3]
(1.空军工程大学信息与导航学院,西安,710077;2.国防科技大学信息通信学院,武汉,430030;
3.95577部队,云南曲靖,655601)

摘要 针对现实网络中用户业务需求偏好和单一防御策略的局限性,研究提出操作系统病毒传播模型及混合防御策略。首先,将网络按照采取的防御策略拆分成子网,综合考虑子网间的交叉感染和网络中病毒传播的关联性,构建多防御策略下的操作系统病毒传播模型,给出了系统的平衡点求解和稳定性分析。其次,引入网络业务评估指数及负面成本定义,提出了抑制操作系统病毒传播的混合防御策略,设计了策略最优配置计算方法、执行流程和参数辨识算法。理论和实验结果表明,所提出的操作系统病毒传播模型及混合防御策略能有效补充传统防御手段的空档期。

关键词 操作系统病毒;病毒传播模型;链路中断;操作系统迁移;混合防御策略
DOI 10.3969/j.issn.2097-1915.2024.04.015
中图分类号 TP393.1 **文献标志码** A **文章编号** 2097-1915(2024)04-0107-11

An Operating System Virus Propagation Model and Hybrid Defense Strategy

LI Juan[1,2], WANG Gang[1], FENG Yun[3]
(1. Information and Navigation School, Air Force Engineering University, Xi'an 710077, China;
2. Information Communication Institute, National University of Defense Technology, Wuhan 430030, China;
3. Unit 95577, Qujing 655601, Yunnan, China)

Abstract Aimed at the problems that user's business is different in demand for partiality and single defense strategy is limited in real network services, a virus propagation model and mixed defense strategy is proposed in operating system. First of all, the network is split into different subnets by adopting link interrupt and operating system migration strategies. In synthetic consideration of the correlation of the virus infection between subnets and virus propagation, an operating system virus propagation model is constructed, and the equilibrium solution and the stability analysis of the system are given. Secondly, by introducing the network service evaluation index and the definition of negative cost, a hybrid defense strategy is proposed to suppress the spread of operating system virus. The calculation method of optimal policy configuration, execution process and parameter identification algorithm are designed. The theoretical and experimental results show that the proposed virus propagation model and the hybrid defense strategy can effectively supplement the gap period of the traditional defense means in short supply.

Key words operating system virus; virus propagation model; link break; operating system migration; hy-

收稿日期:2024-02-27
基金项目:国家自然科学基金(62271500)
作者简介:李 娟(1984—),女,陕西富平人,博士生,讲师,研究方向为复杂网络建模与决策优化方法。E-mail:17792704193@163.com
通信作者:王 刚(1976—),男,湖北浠水人,教授,博士生导师,研究方向为体系设计与复杂网络。E-mail:wglxl@nudt.edu.cn

引用格式:李娟,王刚,冯云.操作系统病毒传播模型及混合防御策略[J].空军工程大学学报,2024,25(4):107-117. LI Juan, WANG Gang, FENG Yun. An Operating System Virus Propagation Model and Hybrid Defense Strategy[J]. Journal of Air Force Engineering University, 2024, 25(4): 107-117.

brid defense strategy

利用操作系统漏洞对用户及网络发起攻击的病毒(简称为操作系统病毒)是当前网络安全的主要威胁之一。对于操作系统病毒,目前防御思路主要有2种:一是防火墙、入侵检测等病毒查杀堵漏方法。由于攻击方漏洞利用和攻击设计总是先于防御方,客观上存在病毒扩散的空档期,防御方需要投入的成本和精力远大于攻击方,通常处于攻防博弈的弱势地位[1-3]。另一种是结合病毒传播规律和影响传播的共性因素分析,通过调整网络拓朴结构抑制病毒传播。这类方法将网络看作一个系统,运用动力学方法分析节点状态转化关系和系统稳定性[4-6],根据稳定性影响因素分析设计抑制病毒传播的方法。

在一般网络拓扑中,为方便局域网内部通信,通常是同一类操作系统,这也为针对操作系统的蓄意攻击提供了便利[7-8]。相对于被动防御,动态目标防御(moving target defense, MTD)是解决这类高持续威胁难题的新途径。文献[9]提出通过多样的、不断变化的评价和部署机制及策略来增加攻击者的攻击难度和代价,从而有效限制脆弱性暴露及被攻击的机会。基于动态防御思路,文献[10]运用系统动力学方法研究了操作系统病毒传播规律,提出了基于操作系统动态迁移的病毒传播抑制策略和算法。对于操作系统病毒防御而言,需要结合病毒传播特点和现实需求进一步深化。

1)现有研究主要局限于单一防御策略,默认不同网络节点对业务的需求一致,但实际网络中不同用户节点对业务需求存在偏好,单一策略难以适应这种差异性。

2)现有病毒传播模型通常将网络看成一个大系统,节点行为、传播规则和防御策略是相同的。执行采取多防御策略的不同子网在节点行为、传播规则和防御策略方面存在差异性,子网之间仍然存在逻辑关联、信息流通和病毒交叉感染可能。

3)从防御角度分析,需要综合考虑攻防收益和用户需求偏好,建立适用于多防御策略的评估指数、损失函数和收益指标,结合网络中用户业务需求差异,设计抑制操作系统病毒传播的混合策略,以及相应的最优配置计算方法、执行流程和参数辨识算法等。

基于以上考虑,分析了信息扩散/病毒传播模型和基于网络结构调整的病毒防御方法,构建了多防御策略下的操作系统病毒传播模型,给出了系统的平衡点求解和稳定性分析。在此基础上,提出了网络业务评估指数和抑制操作系统病毒传播的混合防御策略,设计了相应的最优配置计算方法、执行流程和参数辨识算法。

1 传播模型与防御策略

1.1 信息扩散/病毒传播模型

针对病毒/信息的特征差异,增减/修改网络中节点状态、状态转化关系或增添时延因素,是当前病毒传播/信息扩散研究的重要方向。为提高网络安全防御决策的精准度,文献[11]提出了采用双异质群体演化博弈的网络安全防御决策方法。针对病毒潜伏及隔离行为,文献[12]建立了具有感染潜伏期的病毒和补丁传播的确定性非线性数学模型,并探讨了补丁的影响。时延问题也是信息扩散/病毒传播需要考虑的因素[13-15]。

目前,病毒传播/信息扩散研究中病毒传播模式和关键参数在网络所有节点上保持一致。在现实网络中,不同的用户子网通常会根据自身特点采取不同的防御策略,病毒在不同的节点之间的传播模式和参数存在差异,现有模型难以兼容这种差异性。

1.2 病毒防御策略

近年来网络安全专家提出了动态目标防御、拟态防御、区块链等网络防御新理念和技术[16-18]。对操作系统病毒而言,可借鉴网络层动态目标防御,通过动态改变网络拓扑结构来抑制操作系统病毒的传播[19-21]。

除了链路中断、节点免疫等手段外,改变节点属性(如操作系统类型)和操作系统迁移频率同样能抑制操作系统病毒传播[10,22],这些调整可通过平台动态目标防御技术来实现[23-25]。

在抑制病毒传播方面,改变网络拓扑结构比传统封堵查杀方法更具普遍性[26]。尽管存在承载业务能力损失,但这类方法主要依赖网络安全状态统计信息,相对传统防御方法,技术难度和代价低,既可填补系统补丁和反病毒软件部署前的病毒防御空档,减小损失,也可作为传统防御手段的补充。

1.3 参数设置

由于本文设计参数较多,为便于理解,将贯穿全文的部分参数的含义作简要说明,如表1所示。

表 1　部分参数说明

参数	含义
k^*	表示采取策略*的节点的子网的平均度
k	链路总数
N^*	采取策略*的节点数
N	节点总数
d_O^*	采取策略*的节点从其他操作系统切换到 OS-A 的概率
d_A^*	采取策略*的节点从 OS-A 切换到其他操作系统的概率
φ	易感节点获取免疫能力的概率
ω	感染节点获得暂时免疫的概率
δ	免疫节点失去其免疫能力的概率
β	单位时间内易感节点在与感染节点通信过程中感染操作系统病毒的概率
R_0	基本再生数
R_0^*	采取策略*的节点的子网的基本再生数
v_i	节点 i

2　多防御策略下操作系统病毒传播模型

以链路中断和操作系统迁移 2 种典型防御策略为例开展研究，相关结论将拓展到多防御策略和其他复杂情况。假设：①网络中存在且仅存在 2 种操作系统；②感染节点在网络中均匀分布；③仅有 1 种针对主流操作系统（OS-A）的操作系统病毒。存在多种防御策略时，采取不同防御策略的节点之间感染免疫行为显然不同，感染概率也需要调整。

根据采取防御策略的差异，将网络分割为 2 个子网。若用户业务依赖于某特定操作平台但对通信的需求较低，则可选择链路中断策略；若主要业务对平台的依赖程度较低，但有大量文件、信息传输及共享需求，则可选择操作系统迁移策略。每个子网将来自其他子网的感染视为外部感染。

将网络节点划分为易感状态（susceptible，S）、感染状态（infected，I）、免疫状态（recovery，R）以及其他操作系统（others，O）。先忽略采取不同策略节点之间的感染，分析处于不同状态下节点的变化趋势可得病毒传播规律[26]，对应的动力学方程为：

$$\begin{cases}\dfrac{\mathrm{d}S^*(t)}{\mathrm{d}t}=-(\varphi+d_A^*)S^*(t)-\dfrac{\beta k^* S^*(t)I^*(t)}{N}+\\ \delta R^*(t)+d_O^* O^*(t)\\ \dfrac{\mathrm{d}I^*(t)}{\mathrm{d}t}=\dfrac{\beta k^* S^*(t)I^*(t)}{N}-(\omega+d_A^*)I^*(t)\\ \dfrac{\mathrm{d}R^*(t)}{\mathrm{d}t}=\varphi S^*(t)+\omega I^*(t)-(\delta+d_A^*)R^*(t)\\ \dfrac{\mathrm{d}O^*(t)}{\mathrm{d}t}=d_A^* S^*(t)+d_A^* I^*(t)+d_A^* R^*(t)-d_O^* O^*(t)\end{cases} \tag{1}$$

式中：$S^*(t)$、$I^*(t)$、$R^*(t)$和$O^*(t)$分别为 t 时刻处于不同状态下的节点数量。对应基本再生数[12]为：

$$R_0^*=\frac{d_O^*(d_A^*+\delta)\beta k_1^*}{(d_A^*+d_O^*)(d_A^*+\omega)(d_A^*+\delta+\varphi)} \tag{2}$$

2.1　链路中断策略和操作系统迁移策略

链路中断通过影响节点度来改变基本再生数，操作系统迁移通过调整网络中不同操作系统的比例和迁移频率来改变基本再生数。当 $R_0^*<1$ 时，网络在无病毒状态稳定[6]，链路中断策略和操作系统迁移策略（仅考虑调整 d_A）使网络达到无病毒状态的条件如表 2 所示，γ 为式(3)的正根。

表 2　不同策略下网络消除病毒的条件

策略	调整参数	条件
链路中断	k^*	$k<\dfrac{(d_A^*+d_O^*)(d_A^*+\omega)(d_A^*+\delta+\varphi)}{d_O^*(d_A^*+\delta)\beta}$
操作系统迁移	d_A^*	$d_A^*>\gamma$

$$\begin{cases}x^3+bx^2+cx+d=0\\ x=d_A^*\\ b=d_O^*+\omega+\varphi+\delta\\ c=d_O^*\omega+d_O^*(\delta+\varphi)+\omega(\delta+\varphi)-d_O^*\delta\beta k\\ d=d_O^*\omega(\delta+\varphi)-d_O^*\delta\beta k\end{cases} \tag{3}$$

2.2　操作系统病毒传播模型

将不同防御策略记为“$*$”，对应状态分别为 S^*、I^*、R^* 和 O^* 节点的状态转化关系如图 1 所示。

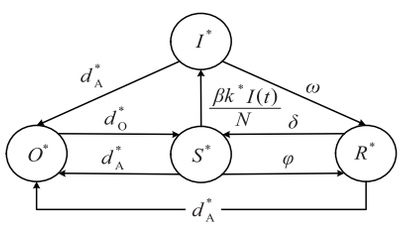


图 1　不同防御策略节点状态转化关系

由于不同子网的区别仅在于防御策略，其物理连接关系并未改变。因此，子网中的任意节点可能受到整个网络中的任意节点病毒感染。根据平均场理论，$*$ 类节点的感染概率可表示为 $\beta k^{*} I(t)/N$，对应的动力学方程为：

$$\begin{cases}\dfrac{\mathrm{d}S^{*}(t)}{\mathrm{d}t}=-(\varphi+d_{\mathrm{A}}^{*})S^{*}(t)-\dfrac{\beta k^{*}S^{*}(t)I(t)}{N}+\\ \delta R^{*}(t)+d_{\mathrm{O}}^{*}O^{*}(t)\\ \dfrac{\mathrm{d}I^{*}(t)}{\mathrm{d}t}=\dfrac{\beta k^{*}S^{*}(t)I(t)}{N}-(\omega+d_{\mathrm{A}}^{*})I^{*}(t)\\ \dfrac{\mathrm{d}R^{*}(t)}{\mathrm{d}t}=\varphi S^{*}(t)+\omega I^{*}(t)-(\delta+d_{\mathrm{A}}^{*})R^{*}(t)\\ \dfrac{\mathrm{d}O^{*}(t)}{\mathrm{d}t}=d_{\mathrm{A}}^{*}S^{*}(t)+d_{\mathrm{A}}^{*}I^{*}(t)+d_{\mathrm{A}}^{*}R^{*}(t)-\\ d_{\mathrm{O}}^{*}O^{*}(t)\end{cases} \tag{4}$$

分析式(4)可知，式(5)始终存在无病毒平衡点：

$$\boldsymbol{P}_{0}(S_{0}^{*},I_{0}^{*},R_{0}^{*},O_{0}^{*})=\left(\frac{d_{\mathrm{O}}^{*}(d_{\mathrm{A}}^{*}+\delta)N^{*}}{(d_{\mathrm{A}}^{*}+d_{\mathrm{O}}^{*})(d_{\mathrm{A}}^{*}+\delta+\varphi)},0,\frac{d_{\mathrm{O}}^{*}\varphi N^{*}}{(d_{\mathrm{A}}^{*}+d_{\mathrm{O}}^{*})(d_{\mathrm{A}}^{*}+\delta+\varphi)},\frac{d_{\mathrm{A}}^{*}N^{*}}{d_{\mathrm{A}}^{*}+d_{\mathrm{O}}^{*}}\right) \tag{5}$$

式中：N^{*} 为网络中节点的数量。

设 I_{ex} 为网络中另一类节点中感染节点数量。当 $I_{\mathrm{ex}}>0$ 时，式(6)对应的系统不存在无病毒平衡点；2 类节点相互影响，当一类节点无法消除操作系统病毒时，另一类节点也无法根除。由式(1)可得任意一类子网对应的动力学方程为：

$$\begin{cases}\dfrac{\mathrm{d}S^{*}(t)}{\mathrm{d}t}=-(\varphi+d_{\mathrm{A}}^{*})S^{*}(t)-\dfrac{\beta k^{*}S^{*}(t)(I^{*}(t)+I_{\mathrm{ex}})}{N}+\\ \delta R^{*}(t)+d_{\mathrm{O}}^{*}O^{*}(t)\\ \dfrac{\mathrm{d}I^{*}(t)}{\mathrm{d}t}=\dfrac{\beta k S^{*}(t)(I^{*}(t)+I_{\mathrm{ex}})}{N}-(\omega+d_{\mathrm{A}}^{*})I^{*}(t)\\ \dfrac{\mathrm{d}R^{*}(t)}{\mathrm{d}t}=\varphi S^{*}(t)+\omega I^{*}(t)-(\delta+d_{\mathrm{A}}^{*})R^{*}(t)\\ \dfrac{\mathrm{d}O^{*}(t)}{\mathrm{d}t}=d_{\mathrm{A}}^{*}S^{*}(t)+d_{\mathrm{A}}^{*}I^{*}(t)+d_{\mathrm{A}}^{*}R^{*}(t)-d_{\mathrm{O}}^{*}O^{*}(t)\end{cases} \tag{6}$$

设 $I_{1}^{\mathrm{B}}=\psi I_{1}^{\mathrm{M}}$，可得式(6)的有病毒平衡点：

$$\boldsymbol{P}_{1}(S_{1}^{\mathrm{B}},I_{1}^{\mathrm{B}},R_{1}^{\mathrm{B}},O_{1}^{\mathrm{B}},S_{1}^{\mathrm{M}},I_{1}^{\mathrm{M}},R_{1}^{\mathrm{M}},O_{1}^{\mathrm{M}})=\left[\frac{(\omega+d_{\mathrm{A}}^{\mathrm{B}})N}{\beta k^{\mathrm{B}}(1+1/\psi)},I_{1}^{\mathrm{B}},\frac{\varphi S_{1}^{\mathrm{B}}+\omega I_{1}^{\mathrm{B}}}{\delta+d_{\mathrm{A}}^{\mathrm{B}}},\frac{d_{\mathrm{A}}^{\mathrm{B}}N^{\mathrm{B}}}{d_{\mathrm{A}}^{\mathrm{B}}+d_{\mathrm{O}}^{\mathrm{B}}},\frac{(\omega+d_{\mathrm{A}}^{\mathrm{M}})N}{\beta k^{\mathrm{M}}(1+\psi)},I_{1}^{M},\frac{\varphi S_{1}^{\mathrm{M}}+\omega I_{1}^{\mathrm{M}}}{\delta+d_{\mathrm{A}}^{\mathrm{M}}},\frac{d_{\mathrm{A}}^{\mathrm{M}}N^{\mathrm{M}}}{d_{\mathrm{A}}^{\mathrm{M}}+d_{\mathrm{O}}^{\mathrm{M}}}\right] \tag{7}$$

式中：

$$I_{1}^{\mathrm{B}}=\frac{\begin{bmatrix}d_{\mathrm{A}}^{\mathrm{B}}d_{\mathrm{O}}^{\mathrm{B}}\beta k^{\mathrm{B}}(1-\mathrm{clu})(\delta+d_{\mathrm{A}}^{\mathrm{B}})(1+1/\psi)N^{\mathrm{B}}-\\ d_{\mathrm{A}}^{\mathrm{B}}(d_{\mathrm{A}}^{\mathrm{B}}+d_{\mathrm{O}}^{\mathrm{B}})(\delta+\varphi+d_{\mathrm{A}}^{\mathrm{B}})(\omega+d_{\mathrm{A}}^{\mathrm{B}})N\end{bmatrix}}{\beta k^{\mathrm{B}}(1+1/\psi)(d_{\mathrm{A}}^{\mathrm{B}}+d_{\mathrm{O}}^{\mathrm{B}})\left[(\omega+d_{\mathrm{A}}^{\mathrm{B}})(\delta+d_{\mathrm{A}}^{\mathrm{B}})-\delta\omega\right]};$$

$$I_{1}^{\mathrm{M}}=\frac{\begin{bmatrix}d_{\mathrm{A}}^{\mathrm{M}}d_{\mathrm{O}}^{\mathrm{M}}\beta k^{\mathrm{M}}(1-clu)(\delta+d_{\mathrm{A}}^{\mathrm{M}})(1+\psi)N^{\mathrm{B}}-\\ d_{\mathrm{A}}^{\mathrm{M}}(d_{\mathrm{A}}^{\mathrm{M}}+d_{\mathrm{O}}^{\mathrm{M}})(\delta+\varphi+d_{\mathrm{A}}^{\mathrm{M}})(\omega+d_{\mathrm{A}}^{\mathrm{M}})N\end{bmatrix}}{\beta k^{\mathrm{M}}(1+\psi)(d_{\mathrm{A}}^{\mathrm{M}}+d_{\mathrm{O}}^{\mathrm{M}})\left[(\omega+d_{\mathrm{A}}^{\mathrm{M}})(\delta+d_{\mathrm{A}}^{\mathrm{M}})-\delta\omega\right]}。$$

对应 2 类策略的基本再生数 R_{0}^{B} 和 R_{0}^{M} 分别为：

$$\begin{cases}R_{0}^{\mathrm{B}}=\dfrac{d_{\mathrm{O}}^{\mathrm{B}}(d_{\mathrm{A}}^{\mathrm{B}}+\delta)\beta k_{1}^{\mathrm{B}}}{(d_{\mathrm{A}}^{\mathrm{B}}+d_{\mathrm{O}}^{\mathrm{B}})(d_{\mathrm{A}}^{\mathrm{B}}+\omega)(d_{\mathrm{A}}^{\mathrm{B}}+\delta+\varphi)},\ k_{1}^{\mathrm{B}}=\dfrac{N^{\mathrm{B}}}{N}\\ R_{0}^{\mathrm{M}}=\dfrac{d_{\mathrm{O}}^{\mathrm{M}}(d_{\mathrm{A}}^{\mathrm{M}}+\delta)\beta k_{1}^{\mathrm{M}}}{(d_{\mathrm{A}}^{\mathrm{M}}+d_{\mathrm{O}}^{\mathrm{M}})(d_{\mathrm{A}}^{\mathrm{M}}+\omega)(d_{\mathrm{A}}^{\mathrm{M}}+\delta+\varphi)},\ k_{1}^{\mathrm{M}}=\dfrac{N^{\mathrm{M}}}{N}\end{cases} \tag{8}$$

若想使网络在无病毒状态稳定，则网络整体的基本再生数 $R_{0}^{\mathrm{M}}+R_{0}^{\mathrm{B}}<1$，此时可设定 $R_{0}^{\mathrm{B}}\leqslant\psi/(1+\psi)$，$R_{0}^{\mathrm{M}}\leqslant 1/(1+\psi)$，对照表 1 中的相应条件调整参数 k_{1}^{B}、k_{1}^{M}、$d_{\mathrm{A}}^{\mathrm{B}}$、$d_{\mathrm{A}}^{\mathrm{M}}$。

2.3 系统稳定性分析

由以上分析可知，对操作系统病毒传播而言，当网络在无病毒平衡点处稳定时，即便网络受到操作系统病毒的入侵且存在感染节点，网络依然能在动态演化中消除病毒，重回无病毒状态。当网络在有病毒平衡点处稳定时，一旦被操作系统病毒入侵，网络将无法依靠自身能力完全消除病毒，操作系统病毒将持续存在。通过系统稳定性分析，可找出病毒持续存在的条件，为抑制操作系统病毒传播提供理论依据。经分析，存在如下结论：

定理 1 $R_{0}^{\mathrm{B}}+R_{0}^{\mathrm{M}}<1$ 时，网络在无病毒平衡点 $\boldsymbol{P}_{0}$ 附近局部稳定(证明过程见附录)。

定理 2 $R_{0}^{\mathrm{B}}+R_{0}^{\mathrm{M}}>1$ 时，网络在有病毒平衡点 $\boldsymbol{P}_{1}$ 附近局部稳定(证明过程见附录)。

定理 1 和定理 2 表明，当网络采取 2 种策略时，网络彻底消除操作系统病毒的条件为 $R_{0}^{\mathrm{B}}+R_{0}^{\mathrm{M}}<1$，相应参数阈值可根据网络实际和用户需求合理配置。

3 操作系统病毒混合防御策略

3.1 网络业务评估指数及负面成本

通过改变网络拓扑结构抑制病毒，是牺牲部分业务承载能力以提升网络安全性能的一种折中办法[27]。不同策略对网络业务的影响侧重点也不相同。如链路中断策略会影响通信效率，加大剩余链

路的业务承载量；操作系统迁移策略则体现在用户使用习惯和业务处理的持续性。为方便衡量策略引起的业务承载能力损失，以下首先定义网络业务评估指数。

用有向图 $G=\{V,E\}$ 表示网络，其中 $V=\{v_i \mid i=1,2,\cdots,N\}$ 和 $E=\{(v_i,v_j) \mid i\neq j, v_i,v_j\in V\}$ 分别为顶点集合和边集合，(v_i,v_j) 为从 v_i 到 v_j 的连接有序数对。按照承担载体不同，网络业务分为节点业务和链路业务两大类，分别定义节点业务指数 $f(I_{\text{link}}^{i,j})$ 和链路业务指数 $g(I_{\text{node}}^{i})$：

$$\begin{cases} f(I_{\text{link}}^{i,j})=c_l I_{\text{link}}^{i,j} \\ g(I_{\text{node}}^{i})=c_n I_{\text{node}}^{i} \end{cases} \tag{9}$$

式中：$I_{\text{link}}^{i,j}$ 为 v_i 到 v_j 的链路承载业务；I_{node}^{i} 为节点 v_i 承载的业务；c_l 为调整网络结构过程中链路业务保留程度；c_n 为调整网络结构过程中的节点业务保留量。定义 2 类业务的加权为网络业务评估指数 I：

$$I=\sum_{m=1}^{N}\left[a_{\text{node}}^{m} g(I_{\text{node}}^{m})+a_{\text{link}}^{m}\sum_{(v_m,v_n)\in E} f(I_{\text{link}}^{m,n})\right] \tag{10}$$

式中：a_{node}^{m} 为节点 v_m 对节点业务的依赖程度；a_{link}^{m} 为节点 v_m 对链路业务的依赖程度；$a_{\text{node}}^{m}+a_{\text{link}}^{m}=1$。

用攻击收益指标量化病毒传播过程中对网络造成的危害[27]，计算式为：

$$\text{AF}=c\int_0^{T_{\text{sec}}} I(t)\,\text{d}t \tag{11}$$

式中：c 为操作系统病毒感染节点后造成的损失因子；T_{sec} 为相应防病毒软件开发成功并完成系统升级的时间。攻击收益越低，对应的防御也就越有效。

3.2　混合防御策略

设网络中的节点需求分为 2 类：一类是平台依赖型业务，链路中断更加适合有这类业务需求的节点；另一类是链路依赖型业务，更加适合操作系统迁移策略。

以下提出一种混合防御策略，网络节点根据自身需求选择策略，网络管理员则根据节点价值等因素确定具体参数条件。

$$c_l=\begin{cases} 1, & \text{case1} \\ e^{-\text{clb}p^{\text{BL}}}, & \text{case2} \\ e^{-\text{clm}p^{\text{ML}}}, & \text{case3} \end{cases} \qquad c_n=\begin{cases} 0, & \text{case1} \\ e^{-\text{cnb}p^{\text{BN}}}, & \text{case4} \\ e^{-\text{cnm}p^{\text{MN}}}, & \text{case5} \end{cases} \tag{12}$$

式中：p^{BL} 为以 B 类节点为起点的链路中断比例；p^{BN} 为某个节点周围链路中断比例；p^{ML} 表示以 M 类节点为起点的链路中，起点操作系统类型与其需求不符的链路所占比例；p^{MN} 为操作系统类型与其需求不符合的节点在 M 类节点中的比例；clb、cnb、clm 和 cnm 分别为对应的衰减因子，其对应的值越大表示衰减程度越高；case1 指正常状态；case2 指相应链路被单向断开（特指不接受主动发送的文件类型数据，但仍接受双方建立连接的基础数据包）；case3 表示其起点操作系统类型不符合其需求；case4 表示该节点周边有链路被断开；case5 表示该节点的操作系统类型不符合其自身需求。

设 p^{B} 为执行网络中 B 类节点中断链路的比例，k_0^{B} 为初始状态下 B 类节点的平均度，$k^{\text{B}}=(1-p^{\text{B}})k_0^{\text{B}}$，$p^{\text{B}}\leqslant 1$。$d_{\text{A}0}^{\text{M}}$ 表示初始状态下 OS-A 迁移到其他操作系统的频率，当网络中节点均匀分布时，可得如表 3 所示参数。

表 3　链路中断和操作系统迁移后网络结构参数变化

节点数量	网络结构参数	B 类节点	M 类节点
n_{osd}	n_{lb}	$p^{\text{B}}k_0^{\text{B}}N^{\text{B}}$	0
	$d_{\text{A}}^{\text{M}}>d_{\text{A}0}^{\text{M}}$	0	$\dfrac{(d_{\text{A}}^{\text{M}}-d_{\text{A}0}^{\text{M}})N^{\text{M}}}{d_{\text{A}}^{\text{M}}+d_{O}^{\text{M}}}$
	$d_{\text{A}}^{\text{M}}<d_{\text{A}0}^{\text{M}}$	0	$\dfrac{(d_{\text{A}0}^{\text{M}}-d_{\text{A}}^{\text{M}})d_{O}^{\text{M}}N^{\text{M}}}{d_{\text{A}0}^{\text{M}}(d_{\text{A}}^{\text{M}}+d_{O}^{\text{M}})}$
	p^{BL}	p^{B}	0
	p^{BN}	p^{B}	0
	p^{ML}	0	$\dfrac{n_{\text{osd}}}{N^{\text{M}}}$
	p^{MN}	0	$\dfrac{n_{\text{osd}}}{N^{\text{M}}}$

表 3 中，n_{lb} 为断开的链路的数量，n_{osd} 为操作系统不符合自身需求的节点数量。结合式(9)、式(10)和表 3，定义网络业务损失函数 L 为：

$$L=\sum_{m=1}^{N}\left[a_{\text{node}}^{m}I_{\text{node}}^{m}+a_{\text{link}}^{m}\sum_{(v_m,v_n)\in E} I_{\text{link}}^{m,n}\right]-\sum_{m=1}^{N}\left[a_{\text{node}}^{m}g(I_{\text{node}}^{m})+a_{\text{link}}^{m}\sum_{(v_m,v_n)\in E} f(I_{\text{link}}^{m,n})\right] \tag{13}$$

$R_0^{\text{B}}+R_0^{\text{M}}<1$ 时，网络在无病毒平衡点 $\boldsymbol{P}_0$ 附近局部稳定。设 $R_0^{\text{B}}=q$，$R_0^{\text{M}}=1-q$，则：

$$\begin{cases} k^{\text{B}}=q\dfrac{(d_{\text{A}}^{\text{B}}+d_{\text{O}}^{\text{B}})(d_{\text{A}}^{\text{B}}+\omega)(d_{\text{A}}+\delta+\varphi)}{d_{\text{O}}^{\text{B}}(d_{\text{A}}^{\text{B}}+\delta)\beta} \\ d_{\text{A}}^{\text{M}}=(1-q)\gamma \\ q^{*}=\underset{q}{\text{argmin}}\ \text{loss} \end{cases} \tag{14}$$

式中：$q=q^{*}$ 时，网络损失最小，γ 对应方程正根。

$$\begin{cases} x^3+bx^2+cx+d=0 \\ b=d_{\mathrm{O}}^{\mathrm{M}}+\omega+\varphi+\delta \\ c=d_{\mathrm{O}}^{\mathrm{M}}\omega+d_{\mathrm{O}}^{\mathrm{M}}(\delta+\varphi)+\omega(\delta+\varphi)-d_{\mathrm{O}}\delta\beta k^{\mathrm{M}} \\ d=d_{\mathrm{O}}^{\mathrm{M}}\omega(\delta+\varphi)-d_{\mathrm{O}}^{\mathrm{M}}\delta\beta k^{\mathrm{M}} \end{cases} \tag{15}$$

当操作系统病毒入侵网络后，网络管理员检测到操作系统病毒的入侵，然后通知全网并收集用户相关参数，包括 a_{node}^{m} 和 I_{node}^{m} 以及以其自身为起点的所有链路的参数 a_{link}^{m} 和 I_{link}^{m}。网络管理员根据这些参数，计算使网络达到安全状态的前提下，网络业务承载能力损失最小的各策略所调整的参数的阈值并下发至用户；用户根据这些阈值执行相应策略，直到相应的反病毒软件被研发或病毒彻底消失。

3.3 模型参数辨识

在历史感染信息（感染节点数）和部分已知信息（节点度、网络节点总数等）基础上，利用模拟退火算法估计模型参数。采用模型演化结果的感染节点数和实际感染节点数的均方差作为参数估计过程中的损失函数，计算方法如下：

$$\mathrm{loss}(I_{\mathrm{model}},I_{\mathrm{actual}})=\sum_{t}\{[I_{\mathrm{model}}(t)-I_{\mathrm{actual}}(t)]^2\} \tag{16}$$

未采取防御策略时，病毒在不同节点之间的传播规则相同，I_{model} 由式（1）求得，I_{actual} 通过对网络感染情况的统计获取。参数辨识算法如下：

算法 1 混合防御策略参数辨识算法

输入：初始值 $(S(0),L(0),I(0),R(0))$，已知参数 N、k、d_{A}、d_{O}。需要估计的初始参数值 $(\omega^0,\beta^0,\delta^0,\varphi^0)$，初始温度 Tem，温度衰减因子 η，终止温度 E_p，每一轮迭代次数 iter

输出：最终估计的参数值 $(\omega,\beta,\delta,\varphi)$

1. $\omega\leftarrow\omega^0,\beta\leftarrow\beta^0,\delta\leftarrow\delta^0,\varphi\leftarrow\varphi^0$
2. loss1$\leftarrow$MEP$(\omega,\beta,\delta,\varphi)$
3. **While** Tem$<E_p$ **Do**
4. **For** $i\leftarrow1$:iter **Do**
5. $(\omega^1,\beta^1,\delta^1,\varphi^1)\leftarrow$randomDisturb$(\omega,\beta,\delta,\varphi)$
6. loss2$\leftarrow$MEP$(\omega^1,\beta^1,\delta^1,\varphi^1)$
7. **If** loss1$>$loss2 or exp(abs(loss2$-$loss1)/Tem)$>$rand()
8. **Then**
9. $\omega,\beta,\delta,\varphi\leftarrow\omega^1,\beta^1,\delta^1,\varphi^1$
10. loss1$\leftarrow$loss2
11. **End**
12. Tem$\leftarrow$Temη
13. **End**
14. **Return** $\omega,\beta,\delta,\varphi$

其中，MEP$(\omega,\beta,\delta,\varphi)$用于计算损失函数，先将当前参数值代入式（1）求解感染节点数的理论值，再按照式（15）计算损失函数；randomDisturb$(\omega,\beta,\delta,\varphi)$用于给当前参数添加随机扰动。算法的时间复杂度为 $O(T\cdot\mathrm{iter}\cdot\log_{\eta}\frac{E_p}{\mathrm{Tem}})$，$T$ 为数据集的数据组数。

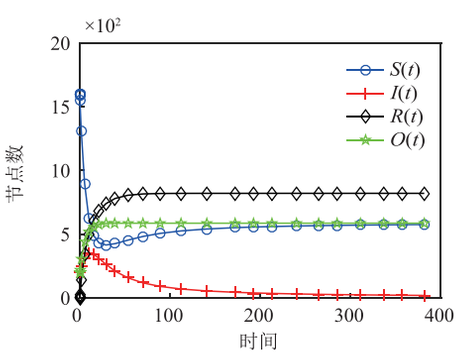
4 仿真分析

为验证模型的有效性，利用编程工具（Python、Matlab）随机生成网络，每一个单位时间发生一次通信，网络中的节点按照预设概率发生感染、免疫等行为，以此模拟病毒传播和防御过程，并实时记录各类节点数量变化，并同数学模型生成的去演对比，验证防御策略有效性。

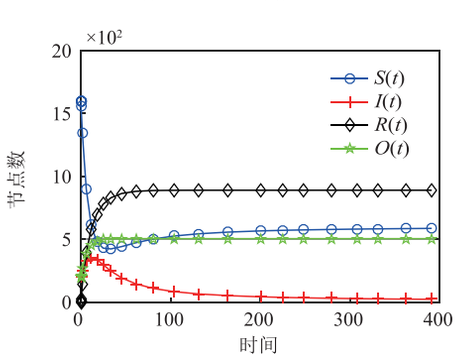
4.1 混合防御策略-单防御策略对比

设包含平台依赖型业务和链路依赖型业务 2 种主要需求的均匀网络，对应初始状态参数，$d_{\mathrm{A}}^{\mathrm{B}}=d_{\mathrm{A}0}^{\mathrm{M}}=0.01$，$d_{\mathrm{O}}^{\mathrm{B}}=d_{\mathrm{O}}^{\mathrm{M}}=0.09$，$\omega=0.05$，$\delta=0.01$，$\varphi=0.05$，$N=20\ 000$，$N^{\mathrm{B}}=N^{\mathrm{M}}=10\ 000$。当 $\beta k^*=0.116\ 7$ 时，$R_0^{\mathrm{B}}=R_0^{\mathrm{M}}=0.5$。

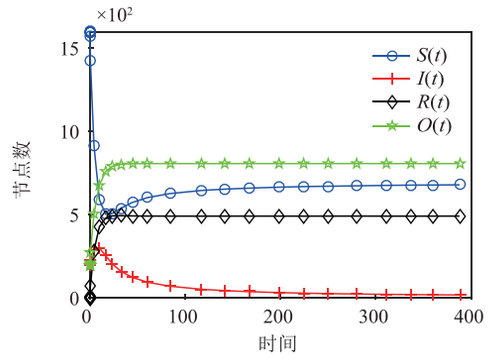
令 $k=16$，$\beta=0.02$，图 2 为链路中断策略、操作系统迁移策略、多防御策略以及混合防御策略下操作系统病毒的传播情况。



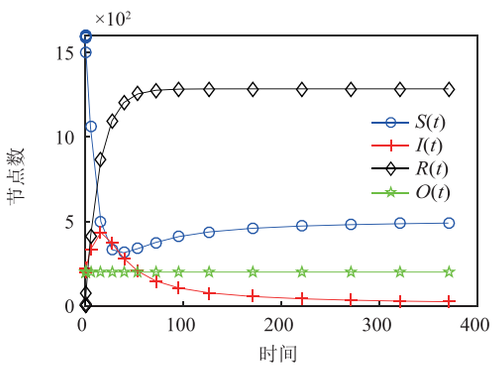
（a）混合防御策略（参数优化后）



（b）混合防御策略（参数优化前）



(c)操作系统迁移策略



(d)链路中断策略

图 2　不同策略下的操作系统病毒传播情况

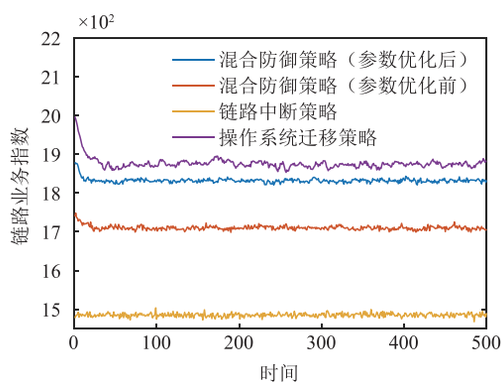
由表 3 分析可知，链路中断消除操作系统病毒的条件为 $p \geqslant 0.271$，操作系统迁移消除操作系统病毒的条件为 $d_A \geqslant 0.061$。分别取链路中断策略、操作系统迁移策略、多防御策略的相应参数为 $p=0.271$，$d_A=0.061$，$p^B=0.271$，$d_A^M=0.061$。根据混合防御策略，$p^B=0.124$，$d_A^M=0.085$ 时，网络损失达到最小。在不同策略下网络中感染节点数量均趋向于 0，表明链路中断、操作系统迁移、多防御策略和混合防御策略都能有效抑制操作系统病毒的传播。

随机生成小世界网络，按照相应策略参数对网络进行相应的调整，重复实验 500 次，记录网络结构变化，不同防御策略对 B 类节点和 M 类节点的影响统计结果如表 4 所示。由统计结果分析可知，混合防御策略下 2 类不同节点采取了不同的策略，参数未优化前，不同节点受到相应影响的节点和链路比例与相应的单一策略基本一致，这表明，相比单一策略，参数优化前的混合防御策略仅是对网络中不同需求的节点采取了不同的防御策略，因此 M 类节点子网的结构变化与操作系统迁移基本一致，B 类节点子网的结构变化与链路中断策略基本一致。参数优化后，混合防御策略则是根据网络节点需求及价值，在不同策略中采用不同的参数值，结果表现出 2 种节点子网结构变化的差异。

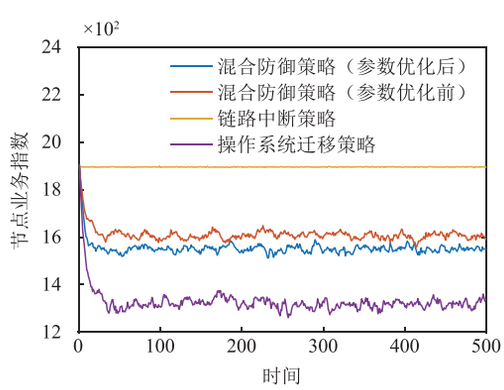
表 4　不同网络结构调整策略下的网络结构变化

节点	策略	链路中断	操作系统迁移	混合防御策略	
				未优化参数	优化参数
M 类	p_{lb}	0.271 1	0.000 0	0.000 0	0.000 0
	p_{osd}	0.000 0	0.335 7	0.336 7	0.425 9
B 类	p_{lb}	0.271 0	0.000 0	0.271 0	0.124 0
	p_{osd}	0.000 0	0.336 7	0.000 0	0.000 0

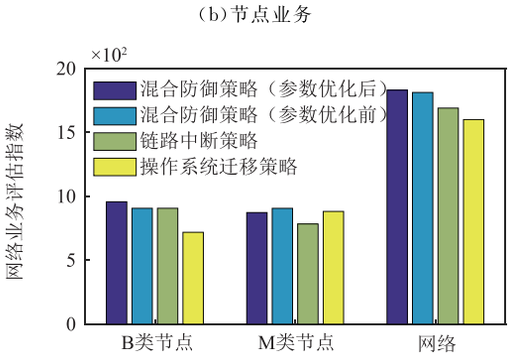
分析不同策略执行过程中链路业务、节点业务和网络业务情况。设 clb＝0.8，cmb＝0.2，cmn＝0.6，cml＝0.4，$a_{node}^M=0.2$，$a_{link}^M=0.8$，$a_{node}^B=0.8$，$a_{link}^B=0.2$。$I_{node}^B=kI_{link}^B=I_{node}^M=kI_{link}^M=1$。



(a)链路业务



(b)节点业务



(c)网络业务

图 3　不同策略执行过程中网络业务评估指数

图 3 分别给出了不同策略执行过程中 3 类业务的评估指数。分析表明，链路中断策略能保留更多的节点业务量，而操作系统迁移策略则保留更多的链路业务量；混合防御策略的节点业务指数和链路业务指数均处于 2 种单一策略之间，参数优化后的

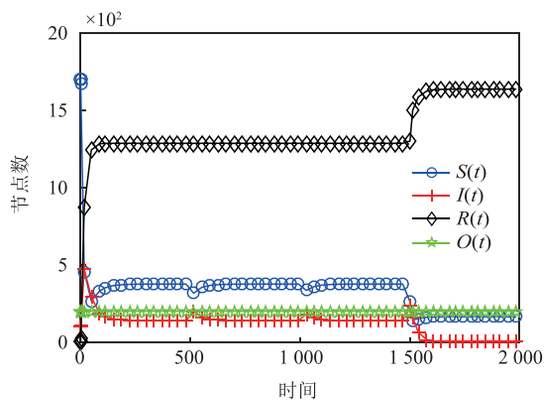
混合策略倾向于保留链路业务。图 3(c)显示,由于需求不同,不同类型节点对节点业务和链路业务的依赖程度也不同,链路中断策略在 M 类节点上表现相对较差,而操作系统迁移策略在 B 类节点上表现相对较差;混合防御策略允许节点选取适合自身需求的防御策略,可通过参数优化调整防御策略的参数配置,共同作用提升网络业务承载能力。在参数优化前,混合防御策略的网络业务承载能力,较链路中断策略提高了 7.22%,较操作系统迁移策略提高了 13.25%;参数优化后,分别提升了 8.28% 和 14.37%。

4.2 防御过程攻击收益对比

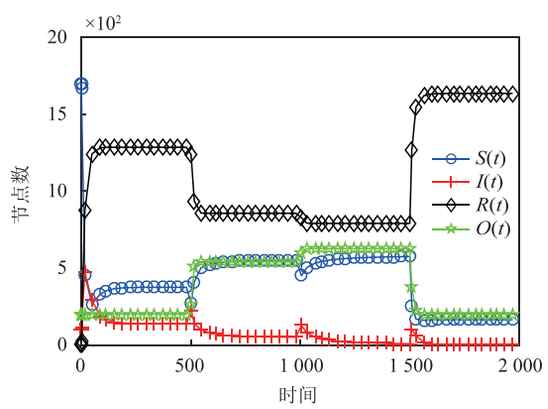
结合以上分析,将病毒传播和防御过程划分为 4 个阶段:①初期阶段,病毒入侵网络并在网络中传播;②前期阶段,根据网络中感染节点数变化和感染主机大致粗略估计参数(ω、δ、φ、β 均未知),并按照估计的参数初步计算策略参数进行防御;③中期阶段,以完成对病毒样本的捕获及初步解析工作,部分参数得以明确如(ω、δ、φ 或 δ、φ 已知),重新估计参数,并调整策略,同步开发系统补丁和反病毒工具;④后期阶段,补丁和防病毒软件开发成功,全网部署和系统升级,该病毒威胁基本解除。4 个阶段均有一定时耗,所提策略主要针对前期和中期的空档期,目标是尽可能降低攻击收益。以下仿真给出了不同空档期时长下所提策略与传统防御方法的攻击收益对比。

令 $N=2\ 000$,$N^{\mathrm{B}}=N^{\mathrm{M}}=1\ 000$,$k=16$,$\beta=0.02$,$c=1$,初期阶段时间 T_1 为 500 个单位时长,前期阶段采用 $\beta=0.012$,$\omega=0.049\ 1$,$\delta=0.007\ 2$,$\varphi=0.018\ 8$ 的参数估计结果配置所提策略参数,$p^{\mathrm{B}}=0.084\ 1$,$d_{\mathrm{A}}^{\mathrm{M}}=0.071$;中期阶段采用 δ、φ 已知,$\beta=0.019\ 8$,$\omega=0.049$ 的参数估计结果配置所提策略参数,$p^{\mathrm{B}}=0.128\ 4$,$d_{\mathrm{A}}^{\mathrm{M}}=0.085$;后期阶段,设定时长 T_4 为 500 个单位时长,考虑相应补丁和反病毒软件已开发成功,调整参数为 $\beta=0.02$,$\omega=0.5$,$\delta=0.01$,$\varphi=0.2$,$p^{\mathrm{B}}=0$,$d_{\mathrm{A}}^{\mathrm{M}}=0.01$。仿真实验中,中前期的时长 T_2 和 T_3 为变量;病毒传播过程中每间隔 500 个单位时长,新增 100 个感染节点,模拟网络攻击。网络分别执行混合防御策略和仅执行传统防御方法,$T_2=500$ 和 $T_3=500$ 时的病毒传播情况如图 4 所示。仿真结果表明,混合防御策略能在完成补丁开发之前的空档期内有效抑制操作系统病毒传播,控制感染规模。

T_2 为捕获病毒样本和初步分析的时耗,T_3 为补丁和反病毒软件开发的时耗,分别令 T_2 和 T_3 在区间[500,3 000]内变化,按照式(11)计算相应攻击收益,相应攻击收益曲线如图 5 所示。分析可知,较之传统防御方法,混合防御策略能有效降低攻击收益,减小网络因受操作系统病毒攻击而造成的损失;随着 T_2 和 T_3 增加,混合防御策略和传统防御方法的攻击收益差值越来越大,这表明系统补丁和反病毒软件开发周期越长,操作系统病毒造成的持续危害时间越长,越有需要在空档期内抑制病毒传播,控制感染节点规模和降低损失,为系统补丁和反病毒软件的开发争取时间。在执行混合防御策略时,在 T_2 和 T_3 变化幅度相同情况下,T_2 发生变化对应的攻击收益增加更多,对网络造成的损失越大,这表明,前期相比中期阶段拥有的信息较少,对参数估计不够准确,一定程度上影响了混合防御策略的实施效果;在不同防御阶段,传统防御手段和所提混合防御策略可互为补充。



(a)仅传统方法时网络中病毒传播情况



(b)混合防御策略下网络中病毒传播情况

图 4 病毒传播和防御过程中不同状态节点数变化曲线

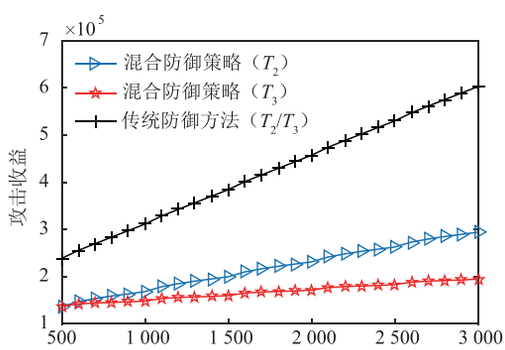


图 5 不同混合策略下攻击收益变化曲线

5　结语

以链路中断和操作系统迁移 2 种防御策略为候选，研究了多防御策略条件下网络中操作系统病毒的传播规律，提出了抑制操作系统病毒传播的混合防御策略。研究表明，执行不同策略的子网的基本再生数之和是决定网络安全性的关键因素；混合防御策略能针对传统病毒防御的空档期和网络中多种业务需求，通过灵活采取策略和设计参数，以小的代价抑制操作系统病毒扩散。尽管完全消除病毒威胁仍然依赖于针对性补丁和反病毒软件，但在打补丁和软件部署之前，链路中断和操作系统迁移等手段能有效降低攻击收益。此外，单一防御策略往往适用于业务需求单一的网络，混合防御策略则适应现实网络业务需求的多样化发展趋势。

本文以均匀网络为背景研究操作系统病毒的传播问题，当网络中不同节点采取不同策略时，均匀网络就会表现一定程度的异质特性，所提的操作系统病毒传播模型也可为异质网络中病毒传播研究提供思路和方法基础，混合防御策略对一般性病毒传播抑制也具有推广价值，如存在多种操作系统病毒、多防御策略的情况。现实网络往往更加复杂，网络结构复杂性更高，这种高度异质的网络如采用子网划分的办法研究，子网数量将达到一个较高的级别，后续将进一步改进病毒传播模型，针对网络结构和节点差异性对病毒传播的影响进一步研究，提升模型对网络结构和节点差异的包容性，进而减少复杂网络划分出子网的数量，增加研究成果的可用性。

参考文献

[1] 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.

[2] SHARMA A, GUPTA B B, SINGH A K, et al. Orchestration of APT Malware Evasive Manoeuvers Employed for Eluding Anti-Virus and Sandbox Defense [J]. Computers & Security, 2022, 115: 102627.

[3] SULTANA N, CHILAMKURTI N, PENG W, 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.

[4] HOANG M T, NGO T K Q, TRAN D H. Dynamically Consistent Nonstandard Numerical Schemes for Solving Some Computer Virus and Malware Propagation Models [J]. Mathematical Foundations of Computing, 2023, 6(4): 704-727.

[5] XUE X F, SHEN Y M. Large and Moderate Deviation Principles for Susceptible-Infected-Removed Epidemic in a Random Environment [J]. Frontiers of Mathematics in China, 2021, 16(4): 1117-1161.

[6] ZHU L H, GUAN G, LI Y M. Nonlinear Dynamical Analysis and Control Strategies of a Network-Based SIS Epidemic Model with Time Delay [J]. Applied Mathematical Modelling, 2019, 70: 512-531.

[7] YANG L X, YANG X F, WU Y B. The Impact of Patch Forwarding on the Prevalence of Computer Virus: A Theoretical Assessment Approach [J]. Applied Mathematical Modelling, 2017, 43: 110-125.

[8] SHAHREAR P, CHAKRABORTY A K, ISLAM M A, et al. Analysis of Computer Virus Propagation Based on Compartmental Model [J]. Applied and Computational Mathematics, 2017, 7(1): 12-21.

[9] ZHENG J J, NAMIN A S. A Survey on the Moving Target Defense Strategies: An Architectural Perspective [J]. Journal of Computer Science and Technology, 2019, 34(1): 207-233.

[10] 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.

[11] 张恩宁，王刚，马润年，等. 采用双异质群体演化博弈的网络安全防御决策方法 [J]. 西安交通大学学报，2021，55(9)：178-188.

[12] BEHAL K S, GAKKHAR S, SRIVASTAVA T. Dynamics of Virus-Patch Model with Latent Effect [J]. International Journal of Computer Mathematics, 2022, 99(9): 1754-1769.

[13] SONG H T, LIU S Q, JIANG W H. Global Dynamics of a Multistage SIR Model with Distributed Delays and Nonlinear Incidence Rate [J]. Mathematical Methods in the Applied Sciences, 2017, 40(6): 2153-2164.

[14] ZHU L H, ZHOU M T, ZHANG Z D. Dynamical Analysis and Control Strategies of Rumor Spreading Models in both Homogeneous and Heterogeneous Networks [J]. Journal of Nonlinear Science, 2020, 30(6): 2545-2576.

[15] 李黎，张瑞芳，杜娜娜，等. 基于有限临时删边的病毒传播控制策略 [J]. 南京大学学报(自然科学)，2019，55(4)：651-659.

[16] 潘传幸，张铮，马博林，等. 面向进程控制流劫持攻击的拟态防御方法 [J]. 通信学报，2021，42(1)：37-47.

[17] 张恒巍，黄世锐. Markov 微分博弈模型及其在网络安全中的应用[J]. 电子学报，2019，47(3)：606-612.

[18] 宋克，刘勤让，魏帅，等. 基于拟态防御的以太网交换机内生安全体系结构[J]. 通信学报，2020，41(5)：18-26.

[19] LEI C，ZHANG H Q，TAN J L，et al. Moving Target Defense Techniques：A Survey[J]. Security and Communication Networks，2018，2018：3759626.

[20] CAI J，LUO J Z，LIU Y，et al. A Network Community Restructuring Mechanism for Transport Efficiency Improvement in Scale-Free Complex Networks[J]. Concurrency and Computation：Practice and Experience，2018，30(5)：e4273.

[21] CAI J，WANG Y，LIU Y，et al. Enhancing Network Capacity by Weakening Community Structure in Scale-Free Network[J]. Future Generation Computer Systems，2018，87：765-771.

[22] 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.

[23] 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.

[24] VÉSTIAS M P. A Survey of Convolutional Neural Networks on Edge with Reconfigurable Computing[J]. Algorithms，2019，12(8)：154.

[25] POTTEIGER B，DUBEY A，CAI F Y，et al. Moving Target Defense for the Security and Resilience of Mixed Time and Event Triggered Cyber-Physical Systems[J]. Journal of Systems Architecture，2022，125：102420.

[26] 陈子涵，程光. 基于 Stackelberg-Markov 非对等三方博弈模型的移动目标防御技术[J]. 计算机学报，2020，43(3)：512-525.

[27] 谭晶磊，张恒巍，张红旗，等. 基于 Markov 时间博弈的移动目标防御最优策略选取方法[J]. 通信学报，2020，41(1)：42-52.

（编辑：徐楠楠）

附录

定理 1 $R_0^{\mathrm{B}}+R_0^{\mathrm{M}}<1$ 时，网络在无病毒平衡点 $\boldsymbol{P}_0$ 附近局部稳定。

证明 式(3)在无病毒平衡点 $\boldsymbol{P}_0$ 处的雅可比矩阵为：

$$\boldsymbol{J}(\boldsymbol{P}_0)=\begin{bmatrix}
-(\varphi+d_{\mathrm{A}}^{\mathrm{B}}) & -\mu_1 & \delta & d_{\mathrm{O}}^{\mathrm{B}} & 0 & -\mu_1 & 0 & 0\\
0 & \nu_1 & 0 & 0 & 0 & \mu_1 & 0 & 0\\
\varphi & \omega & -(\delta+d_{\mathrm{A}}^{\mathrm{B}}) & 0 & 0 & 0 & 0 & 0\\
d_{\mathrm{A}}^{\mathrm{B}} & d_{\mathrm{A}}^{\mathrm{B}} & d_{\mathrm{A}}^{\mathrm{B}} & -d_{\mathrm{O}}^{\mathrm{B}} & 0 & 0 & 0 & 0\\
0 & -\mu_2 & 0 & 0 & -(\varphi+d_{\mathrm{A}}^{\mathrm{M}}) & -\mu_2 & \delta & d_{\mathrm{O}}^{\mathrm{M}}\\
0 & \mu_2 & 0 & 0 & 0 & \nu_2 & 0 & 0\\
0 & 0 & 0 & 0 & \varphi & \omega & -(\delta+d_{\mathrm{A}}^{\mathrm{M}}) & 0\\
0 & 0 & 0 & 0 & d_{\mathrm{A}}^{\mathrm{M}} & d_{\mathrm{A}}^{\mathrm{M}} & d_{\mathrm{A}}^{\mathrm{M}} & -d_{\mathrm{O}}^{\mathrm{M}}
\end{bmatrix} \tag{A1}$$

令 $\boldsymbol{J}(\boldsymbol{P}_0)$ 的特征多项式 $|\lambda\boldsymbol{E}-\boldsymbol{J}(\boldsymbol{P}_0)|=0$，得：

$$\lambda^2(\lambda+\varphi+\delta+d_{\mathrm{A}}^{\mathrm{B}})(\lambda+d_{\mathrm{A}}^{\mathrm{B}}+d_{\mathrm{O}}^{\mathrm{B}})(\lambda+\varphi+\delta+d_{\mathrm{A}}^{\mathrm{M}})(\lambda+d_{\mathrm{A}}^{\mathrm{M}}+d_{\mathrm{O}}^{\mathrm{M}})(\lambda^2+b\lambda+c)=0 \tag{A2}$$

式中：

$$b=-(\omega+d_{\mathrm{A}}^{\mathrm{M}})(R_0^M-1)-(\omega+d_{\mathrm{A}}^{\mathrm{B}})(R_0^B-1),\ c=(\omega+d_{\mathrm{A}}^{\mathrm{B}})(\omega+d_B)(1-R_0^M-R_0^B) \tag{A3}$$

当 $R_0^{\mathrm{B}}+R_0^{\mathrm{M}}<1$ 时，$b>0$ 且 $c>0$，设方程 $(\lambda^2+b\lambda+c)=0$ 的根为 λ_0^1 和 λ_0^2，根据韦达定理，若 λ_0^1 和 λ_0^2 为实根，则均为负，否则，则其实部为负。式(A1)的其他根为：

$$\lambda_0^3=\lambda_0^4=0,\lambda_0^5=-(\varphi+\delta+d_{\mathrm{A}}^{\mathrm{B}}),\lambda_0^6=-(d_{\mathrm{A}}^{\mathrm{B}}+d_{\mathrm{O}}^{\mathrm{B}}),\lambda_0^7=-(\varphi+\delta+d_{\mathrm{A}}^{\mathrm{M}}),\lambda_0^6=-(d_{\mathrm{A}}^{\mathrm{M}}+d_{\mathrm{O}}^{\mathrm{M}}) \tag{A4}$$

因此，式(A1)的所有特征根均位于坐标轴的左半平面，由 Routh-Hurwitz 稳定判据，此时网络系统稳定在无病毒平衡点 $\boldsymbol{P}_0$ 处。当 $R_0^B+R_0^M>1$ 时，λ_0^1 和 λ_0^2 至少有一个为正，则网络系统在无病毒平衡点处不稳定。证毕。

定理 2 $R_0^B+R_0^M>1$ 时，网络在有病毒平衡点 $\boldsymbol{P}_1$ 附近局部稳定。

证明 式(3)在无病毒平衡点 $\boldsymbol{P}_1$ 处的雅可比矩阵为：

$$\boldsymbol{J}(\boldsymbol{P}_1)=\begin{bmatrix} \mu_3 & -\frac{\beta k^{\mathrm{B}} S_1^{\mathrm{B}}}{\chi N} & \delta & d_{\mathrm{O}}^{\mathrm{B}} & 0 & -\frac{\beta k^{\mathrm{B}} S_1^{\mathrm{B}}}{\chi N} & 0 & 0 \\ \frac{\beta k^{\mathrm{B}} I_1}{\chi N} & \nu_3 & 0 & 0 & 0 & \frac{\beta k^{\mathrm{B}} S_1^{\mathrm{B}}}{\chi N} & 0 & 0 \\ \varphi & \omega & -\delta-d_A & 0 & 0 & 0 & 0 & 0 \\ d_{\mathrm{A}}^{\mathrm{B}} & d_{\mathrm{A}}^{\mathrm{B}} & d_{\mathrm{A}}^{\mathrm{B}} & -d_{\mathrm{O}}^{\mathrm{B}} & 0 & 0 & 0 & 0 \\ 0 & -\frac{\beta k^{\mathrm{M}} S_1^{\mathrm{M}}}{\chi N} & 0 & 0 & \mu_4 & -\frac{\beta k^{\mathrm{M}} S_1^{\mathrm{M}}}{\chi N} & \delta & d_{\mathrm{O}}^{\mathrm{M}} \\ 0 & \frac{\beta k^{\mathrm{M}} S_1^{\mathrm{M}}}{\chi N} & 0 & 0 & \frac{\beta k^{\mathrm{M}} I_1}{\chi N} & \nu_4 & 0 & 0 \\ 0 & 0 & 0 & 0 & \varphi & \omega & -\delta-d_{\mathrm{A}}^{\mathrm{M}} & 0 \\ 0 & 0 & 0 & 0 & d_{\mathrm{A}}^{\mathrm{M}} & d_{\mathrm{A}}^{\mathrm{M}} & d_{\mathrm{A}}^{\mathrm{M}} & -d_{\mathrm{O}}^{\mathrm{M}} \end{bmatrix} \tag{A5}$$

令 $\boldsymbol{J}(\boldsymbol{P}_1)$ 的特征多项式 $|\lambda\boldsymbol{E}-\boldsymbol{J}(\boldsymbol{P}_1)|=0$ 得：

$$\lambda^2(\lambda+d_{\mathrm{A}}^{\mathrm{B}}+d_{\mathrm{O}}^{\mathrm{B}})(\lambda^2+b_1\lambda+c_1)(\lambda+d_{\mathrm{A}}^{\mathrm{M}}+d_{\mathrm{O}}^{\mathrm{M}})(\lambda^2+b_2\lambda+c_2)=0 \tag{A6}$$

其中：

$$\begin{aligned} &b_1=\varphi+\delta+d_{\mathrm{A}}^{\mathrm{B}}+\frac{\omega+d_{\mathrm{A}}^{\mathrm{B}}}{1+\psi}+\frac{\beta k^{B} I_1}{\chi N},c=(\varphi+\delta+d_{\mathrm{A}}^{\mathrm{B}})\frac{\omega+d_{\mathrm{A}}^{\mathrm{B}}}{1+\psi}+(\delta+\omega+d_{\mathrm{A}}^{\mathrm{B}})\frac{\beta k^{\mathrm{B}} I_1}{\chi N}, \\ &b_1=\varphi+\delta+d_{\mathrm{A}}^{\mathrm{M}}+\frac{(\omega+d_{\mathrm{A}}^{\mathrm{M}})\psi}{1+\psi}+\frac{\beta k^{\mathrm{M}} I_1}{\chi N},c=(\varphi+\delta+d_{\mathrm{A}}^{\mathrm{B}})\frac{(\omega+d_{\mathrm{A}}^{\mathrm{M}})\psi}{1+\psi}+(\delta+\omega+d_{\mathrm{A}}^{\mathrm{M}})\frac{\beta k^{\mathrm{M}} I_1}{\chi N} \end{aligned} \tag{A7}$$

当 $R_0^{\mathrm{B}}+R_0^{\mathrm{M}}>1$ 时，$b_1>0$，$b_2>0$，$c_1>0$，$c_2>0$，根据韦达定理，方程 $\lambda^2+b_1\lambda+c_1=0$ 和 $\lambda^2+b_2\lambda+c_2=0$ 的根均为负根或实部为负的复根，式(A6)的其他根显然非正，因此，式(12)的所有特征根均位于坐标轴的左半平面，由 Routh-Hurwitz 稳定判据，此时网络系统稳定在有病毒平衡点 $\boldsymbol{P}_1$ 处。证毕。