



文章编号:1001-9081(2018)10-2899-04

DOI:10.11772/j.issn.1001-9081.2018040850

## 考虑社交网络用户行为的网络病毒传播建模

冯丽萍<sup>1,2,3\*</sup>, 韩燮<sup>1</sup>, 韩琦<sup>4</sup>, 郑芳<sup>2</sup>

(1. 中北大学 信息与通信工程学院, 太原 030051; 2. 山西财经大学 信息管理学院, 太原 030006;  
3. 忻州师范学院 计算机系, 忻州 034000; 4. 重庆科技学院 电气与信息工程学院, 重庆 401331)  
(\* 通信作者电子邮箱 fenglip@yeah.net)

**摘要:**针对已有病毒传播模型都没有考虑不同社交网络间的用户交互行为对网络病毒传播规律的影响,建立了考虑不同社交网络用户交互行为的微分方程动力学模型。利用稳定性理论分析了模型反映的网络病毒传播动力学性态,得到了控制网络病毒传播的基本再生数的精确数学表达式。进一步,采用龙格-库塔数值方法,通过仿真实验,验证了理论分析的正确性。研究结果表明,基本再生数是网络病毒扩散基本态势的直接决定因素,当基本再生数的值小于等于1时,随着时间演化,网络病毒的扩散会被彻底控制。另外还发现,分散用户到不同社交网络更有利缓解网络病毒的扩散。

**关键词:**病毒模型;社交网络;用户行为;动力学性态;网络病毒

中图分类号:TP309.5 文献标志码:A

### Network virus propagation modeling considering social network user behaviors

FENG Liping<sup>1,2,3\*</sup>, HAN Xie<sup>1</sup>, HAN Qi<sup>4</sup>, ZHENG Fang<sup>2</sup>

(1. School of Information and Communication Engineering, North University of China, Taiyuan Shanxi 030051, China;  
2. School of Information Management, Shanxi University of Finance & Economics, Taiyuan Shanxi 030006, China;  
3. Computer Department, Xinzhou Teachers University, Xinzhou Shanxi 034000, China;  
4. School of Electrical and Information Engineering, Chongqing University of Science & Technology, Chongqing 401331, China)

**Abstract:** Concerning that the existing networks virus propagation models do not consider the influence of interactive behaviors among the users in different social networks on network virus propagation, a dynamic model of differential equations was established. The stability theory was used to analyze the dynamical behaviors of the network virus propagation, and the accurate expression of the basic reproduction number was obtained, which is the threshold of controlling the network virus propagation. Furthermore, using Runge-Kutta numerical method, the correctness of theoretic analysis was verified by simulations. The results show that the basic reproduction number is the direct decisive factor of network virus prevalence situations. When the value of the basic reproduction number is less than or equal to one, the propagation of the network viruses will be controlled with the evolution of time. Additionally, the research reveals that it is helpful for distributing the users to different social networks to slow the prevalence of network viruses.

**Key words:** virus model; social network; user behavior; dynamical behavior; network virus

### 0 引言

在信息化建设高度发达的今天,互联网应用已经渗透到各个领域,给人们的生活和工作带来了极大的方便。然而,网络安全给人们带来方便的同时,网络安全已成为一个非常严重的全球化问题。2010年6月爆发的震网病毒(Stuxnet),是一次极具破坏性的、针对现实世界基础设施的蠕虫病毒,在短时间内感染了全球超过45 000个网络,伊朗核电站因此受到严重损失<sup>[1]</sup>。2017年5月12日爆发的勒索病毒(WannaCry)感染了全球100多个国家和地区,超过10万台电脑,涉及到金融、能源、教育以及医疗等多个行业<sup>[2]</sup>。可见,建设安全、可靠的网络空间环境是推动信息化社会不断发展的基本保障。

社交网络作为眼下最具影响力的网络社交平台,已拥有大量用户。以我国最流行的微信、QQ为例,2016年,网民使用率分别达到85.8%、67.5%<sup>[3]</sup>。这些用户,以自己在现实世界中的关系网为基础,建立联系人列表、微信群或QQ群。这些用户之间存在着错综复杂的关系,很容易引起交互感染。比如,用户A的联系人列表里有用户B,但是A和B所处的微信或QQ群不一定完全一样,假如用户A受到了感染,那么A就会感染B,从而产生了不同用户群之间的相互感染。本文的目的旨在研究不同社交网络间用户相互感染的网络病毒传播动力学行为。

针对网络病毒传播建模和用户行为的研究已有许多,自从1991年Kephart等<sup>[4-5]</sup>将人类病毒传播建模机理引入计算机病毒传播研究,许多学者在此基础上做了大量网络病毒建

收稿日期:2018-04-25;修回日期:2018-06-11;录用日期:2018-07-13。

基金项目:国家自然科学基金资助项目(61503050);忻州师范学院重点学科建设项目(XK201403)。

作者简介:冯丽萍(1976—),女,山西宁武人,教授,博士,CCF会员,主要研究方向:网络安全、动力系统;韩燮(1964—),女,山西文水人,教授,博士生导师,博士,主要研究方向:虚拟现实、网络安全;韩琦(1981—),男,山西榆社人,副教授,博士,主要研究方向:网络安全、优化控制、细胞神经网络;郑芳(1982—),女,山西石楼人,讲师,硕士,主要研究方向:信息安全、隐私保护。



模的工作。Zou 等<sup>[6]</sup>通过建立 SIR ( Susceptible-Infected-Recovered) 模型,分析了“红色蠕虫”传播的动力学特性,并且通过与实际红色蠕虫传播数据比较,表明微分方程动力学模型可以有效地反映真实网络病毒传播规律。Han 等<sup>[7]</sup>建立了带时滞的 SIRS ( SIR-Susceptible) 模型,刻画了具有延迟感染的计算机病毒传播过程,通过详细的数学分析,得出了控制计算机病毒大规模扩散的阈值,最后,通过数值仿真验证了理论分析的正确性。冯丽萍等<sup>[8]</sup>考虑到现实网络中节点数量是可变的,在已有工作基础上建立了改进的 SIR 模型,并且分析了模型的动力学性质,通过与 2001 年红色蠕虫爆发时实际观察值的比较发现,根据模型得到的仿真结果和实际观察值基本相符。紧接着,冯丽萍等<sup>[9-11]</sup>又通过考虑网络病毒扩散依赖的不同因素,建立了一系列不同的病毒传播模型,进一步研究了网络病毒传播的动力学性质,以及控制病毒扩散的有效措施。还有许多研究者做了大量类似的工作<sup>[12-15]</sup>。这些已有的研究从不同侧重点揭示了网络病毒传播规律,为网络管理员采取合理的网络安全防御措施提供了良好的理论指导,而且这些模型从不同角度考虑了用户的反病毒行为对网络病毒传播速度以及规模的影响。但是,针对不同社交网络间用户行为的相互作用而引起的网络病毒传播规律还没有相应研究。为此,本文通过考虑不同社交网络中用户相互联系的行为,建立相应的网络病毒传播动力学模型,进一步揭示由于不同社交网络间用户交互行为引起的网络病毒传播规律,从而提出对应的防御策略。

## 1 模型建立

本章采用经典的 SI ( Susceptible-Infected) 模型来建模不同社交网络用户行为相互感染的网络病毒传播过程。在 SI 模型中,网络中节点的状态分为两种:1) 易感染状态  $S$ ,表示节点用户对网络病毒没有免疫功能,一旦和已感染节点接触就会被感染。2) 已感染状态  $I$ ,表示节点用户已经被网络病毒感染,而且具有感染其他用户的能力。在任意时刻  $t$ ,网络中的节点处于这两种状态中的其中一种。

现实世界中,不同用户群会根据不同用途与关系形成相应的社交网络群,比如:微信群、QQ 群等。据此,本文把处于  $S$  状态的节点用户分为不同的群,用  $S_k (k = 1, 2, \dots, n)$  表示,其中,  $n$  表示网络中用户群的个数。相应地,处于  $I$  状态的节点用户也分为不同的群,用  $I_k (k = 1, 2, \dots, n)$  表示。假设  $I_j (j = 1, 2, \dots, n)$  表示第  $j$  个用户群的已感染用户,  $S_k$  表示第  $k$  个用户群的易感染用户,如果  $I_j$  用户同时也在第  $k$  个用户群,那么,  $I_j$  就会感染用户  $S_k$ ,用  $\beta_{kj}$  表示  $I_j$  对  $S_k$  的感染率。因此,易感染用户群被感染的概率为:  $S_k \left( \sum_{j=1}^n \beta_{kj} I_j \right)$ 。节点的状态变化图 1 所示。

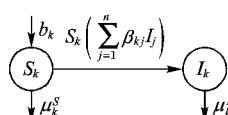


图 1 节点状态转化图

Fig. 1 Transition among states of nodes

在图 1 中,  $b_k$  表示新加入社交网络中的节点用户,  $\mu_k^S$  和  $\mu_k^I$  分别表示从社交网中退出的易感染和已感染节点用户。

图 1 可用微分方程模型表示为:

$$\begin{cases} \frac{dS_k}{dt} = b_k - \mu_k^S S_k - S_k \left( \sum_{j=1}^n \beta_{kj} I_j \right) \\ \frac{dI_k}{dt} = S_k \left( \sum_{j=1}^n \beta_{kj} I_j \right) - \mu_k^I I_k \end{cases} \quad (1)$$

根据实际物理意义,式(1) 中参数  $b_k$ 、 $\mu_k^S$  和  $\mu_k^I$  均为正数,  $\beta_{kj}$  为非负数。设置式(1) 的初始条件为:

$$\begin{cases} S_k(0) = \varphi_1^k \geq 0, k = 1, 2, \dots, n \\ I_k(0) = \varphi_2^k \geq 0 \\ (\varphi_1^1, \varphi_2^1, \varphi_1^2, \varphi_2^2, \dots, \varphi_1^n, \varphi_2^n) \in \mathbf{R}_+^{2n}, \end{cases} \quad (2)$$

其中:

$$\mathbf{R}_+^{2n} = \{(x_1, y_1, x_2, y_2, \dots, x_n, y_n) | x_k, y_k \geq 0, k = 1, 2, \dots, n\}$$

假设,  $n$  阶矩阵  $\mathbf{B} = (\beta_{kj})_{n \times n}$  是不可约的。式(1) 的可行区域为:

$$C = \{(S_1, I_1, S_2, I_2, \dots, S_n, I_n) \in \mathbf{R}_+^{2n} | S_k \leq S_k^0, S_k + I_k \leq b_k / \mu_k^S, k = 1, 2, \dots, n\}$$

## 2 模型分析

本章通过求式(1) 的平衡点,确定模型中  $S$  和  $I$  的取值,进一步确定由模型(1) 反映的控制网络病毒传播的临界值。从而为有效控制网络病毒传播提供理论指导。

根据平衡点的定义,令

$$\frac{dS_k}{dt} = \frac{dI_k}{dt} = 0$$

可求得式(1) 的免疫平衡点:

$$\mathbf{E}^0 = (S^0, 0)$$

其中:

$$S^0 := (S_1^0, S_2^0, \dots, S_n^0)^T = \left( \frac{b_1}{\mu_1^S}, \frac{b_2}{\mu_2^S}, \dots, \frac{b_n}{\mu_n^S} \right)^T$$

令  $R_0 = \rho(\tilde{\mathbf{M}}(S^0))$ , 其中:

$$\tilde{\mathbf{M}}(S^0) = \left( \frac{\beta_{kj} S_k^0}{\mu_k^I} \right)_{n \times n}$$

$\rho(\tilde{\mathbf{M}}(S^0))$  表示矩阵  $\tilde{\mathbf{M}}(S^0)$  的谱半径,生物学上称  $R_0$  为基本再生数<sup>[16]</sup>。

**定理 1** 如果  $R_0 \leq 1$ , 那么免疫平衡点  $\mathbf{E}^0$  在可行区域  $C$  内全局渐近稳定。

**证明** 令  $\tilde{\mathbf{M}}(S) := \left( \frac{\beta_{kj} S_k}{\mu_k^I} \right)_{n \times n}$ 。由方程(1) 有:  $0 \leq S_k \leq S_k^0 (k = 1, 2, \dots, n)$  并且  $0 \leq \tilde{\mathbf{M}}(S) \leq \tilde{\mathbf{M}}(S^0)$  成立。由于矩阵  $\mathbf{B}$  是不可约的,所以  $\tilde{\mathbf{M}}(S)$  和  $\tilde{\mathbf{M}}(S^0)$  也是不可约的,所以,当  $S \neq S^0$  时,有:  $\rho(\tilde{\mathbf{M}}(S)) < \rho(\tilde{\mathbf{M}}(S^0)) = R_0 \leq 1$ 。

$\tilde{\mathbf{M}}(S)I = I$  有唯一平凡解  $I = 0$ , 所以,  $\mathbf{E}^0$  是原公式(1) 在区域  $C$  中的平衡点。令

$$(\omega_1, \omega_2, \dots, \omega_n) \rho(\tilde{\mathbf{M}}(S^0)) = (\omega_1, \omega_2, \dots, \omega_n) \tilde{\mathbf{M}}(S^0)$$

因为矩阵  $\tilde{\mathbf{M}}(S^0)$  是不可约的,所以有  $\omega_k > 0 (k = 1, 2, \dots, n)$ 。令

$$L = (\omega_1, \omega_2, \dots, \omega_n) \times \begin{bmatrix} \mu_1^I & 0 & \cdots & 0 \\ 0 & \mu_2^I & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \mu_n^I \end{bmatrix}^{-1} \begin{bmatrix} I_1 \\ I_2 \\ \vdots \\ I_n \end{bmatrix}$$



对  $L$  求导, 得

$$\begin{aligned} L' &= (\omega_1, \omega_2, \dots, \omega_n) [\tilde{\mathbf{M}}(\mathbf{S})I - I] \leqslant \\ &(\omega_1, \omega_2, \dots, \omega_n) [\tilde{\mathbf{M}}(\mathbf{S}^0)I - I] = \\ &[\rho\tilde{\mathbf{M}}(\mathbf{S}^0) - 1](\omega_1, \omega_2, \dots, \omega_n) \leqslant 0 \\ \text{如果 } R_0 &= \rho(\tilde{\mathbf{M}}(\mathbf{S}^0)) < 1, \text{那么 } L' = 0 \Leftrightarrow I = 0. \\ \text{如果 } R_0 &= 1, \text{那么 } L' = 0 \text{ 表明:} \\ (\omega_1, \omega_2, \dots, \omega_n)\tilde{\mathbf{M}}(\mathbf{S}) &< (\omega_1, \omega_2, \dots, \omega_n)\tilde{\mathbf{M}}(\mathbf{S}^0) = \\ (\omega_1, \omega_2, \dots, \omega_n) \end{aligned} \quad (3)$$

式(3)有唯一的平衡解  $I = 0$ , 所以, 当  $R_0 \leqslant 1$  时,  $L' = 0$  等价于  $I = 0$  或  $\mathbf{S} = \mathbf{S}^0$ 。根据 LaSalle's 不变集原理, 可得, 当  $R_0 \leqslant 1$  时, 免疫平衡点  $\mathbf{E}^0$  是全局渐近稳定的。证毕。

考虑到网络安全防御者关心的是如何控制网络病毒的快速扩散, 保证网络正常运行, 本文在理论分析部分只研究免疫平衡点的性态。

### 3 仿真验证

为了观察微分方程(1)刻画的网络病毒的传播过程, 本章采用龙格-库塔(Runge-Kutta)法对微分方程(1)进行数值求解, 在 Matlab2016R 环境下进行仿真验证。模型(1)中的参数分为两种类型: 系统参数( $b_k$  和  $\mu_k$ )和状态转换参数(除  $b_k$  和  $\mu_k$  之外的其余参数), 其中系统参数反映网络空间要素的运行状态, 状态转换参数反映社交网络中用户行为以及反病毒措施对网络病毒扩散的影响程度。另外, 系统的初始状态, 即  $S(0)$  和  $I(0)$  对网络病毒的扩散也会产生很大影响。不失一般性, 实验时假设  $I(0)$  的取值较小。仿真实验主要是: 1) 验证针对模型(1)的理论分析的正确性; 2) 在确定系统参数值的情况下, 通过改变状态转换参数的值来观察模型(1)反映的网络病毒传播过程; 3) 比较用户活跃的社交网络数量对网络病毒传播的影响; 4) 本文模型和传统模型之间的比较。

1) 首先, 进行数值模拟来验证理论分析的正确性。取  $n = 3$  ( $k = 1, 2, 3$ ), 即, 假设用户经常活跃的社交网络群依次为: 家庭、工作、朋友三个群。为了模拟网络病毒扩散的长期行为, 设置单位时间为“月”。根据参数的实际物理意义, 设  $b_1^s = 1/480, b_2^s = 1/12, b_3^s = 1/6, \mu_1^s = \mu_1^l = 1/540, \mu_2^s = \mu_2^l = 1/12, \mu_3^s = \mu_3^l = 1/6$ 。感染率  $\beta_{kj}$  的值取  $10^{-4}$  数量级, 即:  $\beta_{11} = 0.0009, \beta_{12} = 0.0008, \beta_{13} = 0.0006, \beta_{21} = 0.0007, \beta_{22} = 0.0008, \beta_{23} = 0.0005, \beta_{31} = 0.0006, \beta_{32} = 0.0004, \beta_{33} = 0.0003$ ;  $S_k$  的初值分别取 20, 40, 80;  $I_k$  的初值分别取 2, 4, 6 ( $k = 1, 2, 3$ )。计算得  $R_0 = 0.5475 < 1$ 。仿真结果如图2所示。

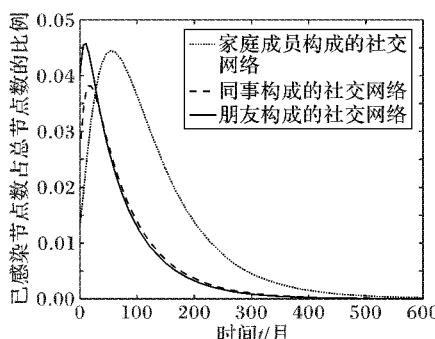


图 2  $R_0 = 0.5475 < 1$  时已感染节点比例随时间变化  
Fig. 2 Infected nodes' ratio versus time when  $R_0 = 0.5475 < 1$

从图2可以看出, 随着时间的演化, 最终每个社交网络中被感染节点数都趋于0, 也就是网络病毒的扩散被完全控制, 与理论分析结果相符。同时, 图中三条曲线的变化趋势都是在开始 0~100 的时间段内被感染节点数迅速增大, 随后逐渐减小直至趋于0, 这是因为, 开始时, 社交网络中易感染节点较多, 被感染的风险就会较大, 转换为已感染节点的速度也会快一些, 随着易感染节点数的减少, 转化为已感染节点的数量也会随着减少, 直到0, 成为一个稳定状态。

2) 然后, 通过实验观察感染率  $\beta_{kj}$  的变化对网络病毒扩散规模的影响。

取  $\beta_{kj}$  为  $10^{-2}$  数量级, 即:  $\beta_{11} = 0.008, \beta_{12} = 0.003, \beta_{13} = 0.003, \beta_{21} = 0.003, \beta_{22} = 0.002, \beta_{23} = 0.002, \beta_{31} = 0.003, \beta_{32} = 0.004, \beta_{33} = 0.002$ , 其他参数值和初始值都不变(同图2), 计算得  $R_0 = 2.3849 > 1$ 。仿真结果如图3所示。从图3可看出, 当基本再生数  $R_0$  的值大于1时, 网络病毒不会被完全控制, 而是稳定于一个正数。这个结论在已有工作中已得到证实<sup>[13]</sup>, 说明这一定律在交叉感染模型中仍然成立。而且, 与图2相比, 发现增大感染率后, 病毒感染的速度大幅提升, 在最初 0~50 的时间段内, 迅速达到最高值, 随后逐步下降到一个稳定的正数。这一结论与实际经验相符。

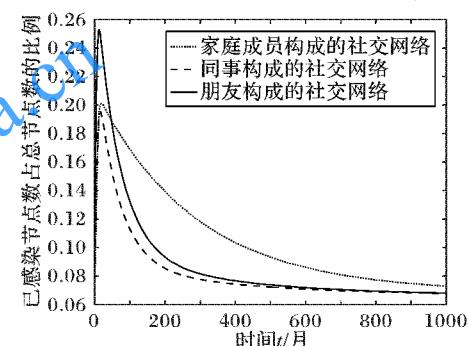


图 3  $R_0 = 2.3849 > 1$  时已感染节点比例随时间变化  
Fig. 3 Infected nodes' ratio versus time when  $R_0 = 2.3849 > 1$

3) 为了观察用户活跃的社交网络个数对网络病毒扩散的影响, 取参数  $n = 2$  ( $k = 1, 2$ ), 考虑到家庭群成员相对较固定, 而且人员数量也相对较少, 所以保留工作与朋友群为活跃群, 即去掉反映家庭群的所有参数, 其他参数值与图2的参数取值相同。为了保持和图2的网络总节点数相同, 设置  $S_k$  的初始值分别为 42 和 100;  $I_k$  的初始值分别为 4 和 6, 其中:  $k = 1$  代表由同事构成的社交网络;  $k = 2$  代表由朋友构成的社交网络。仿真结果如图4所示。

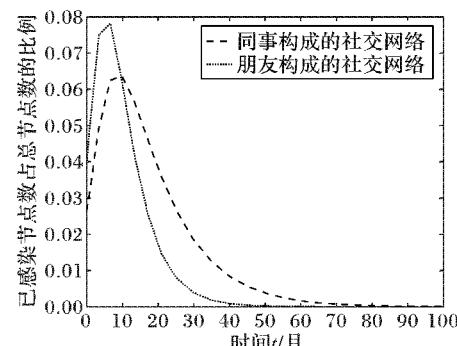


图 4 只考虑两个社交网络时已感染节点比例随时间变化  
Fig. 4 Infected nodes' ratio versus time when considering two social networks



图 4 表明,当用户活跃的社交网络数为 2 时,网络病毒的扩散在短时间内会达到最大值,随后快速降低,直到趋于 0。与图 2 相比,病毒爆发得快,控制得也快。而且在图 4 中被感染节点最大值的比例超过了图 2,也就是说在病毒爆发初期,用户所在的社交网络数越多,越不利于病毒传播,但是,在病毒衰减期,社交网络数越少,越容易被控制。

4) 最后,将本文模型与传统模型进行比较,仿真结果如图 5 所示。传统模型曲线  $n$  的取值为 1, 本文模型曲线  $n$  的取值为 2, 其余参数的取值如表 1 所示。观察图 5 发现, 在病毒传播初期, 本文模型反映的网络病毒扩散态势要比传统模型弱一些, 这说明用户分布于不同的社交网络要比集中于一个网络更有利于缓解网络病毒的扩散, 而在病毒衰减期, 呈现出的是相反的态势。图 5 和图 4 呈现出了相同的规律。这一现象与文献[4]中提出的把大网络分割为不同小网络有利于控制网络病毒扩散的结论一致。

表 1 图 5 中模型各参数取值表

Tab. 1 Parameters values of Fig. 5

本文模型		传统模型	
参数	值	参数	值
$\beta_{kj}$	0.003	$\beta$	0.003
$b_k$	1/12, 1/6	$b$	1/12
$\mu_k^S$	1/12, 1/6	$\mu_S$	1/12
$\mu_k^I$	1/12, 1/6	$\mu_I$	1/12
$(S_k(0), I_k(0))$	(20, 40, 2, 4)	$(S(0), I(0))$	(60, 6)

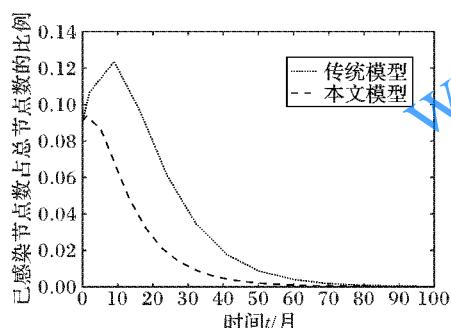


图 5 本文模型与传统模型的比较

Fig. 5 Comparison between proposed model and traditional model

#### 4 结语

社交网络已经成为人们利用互联网进行工作、交流和生活的活跃平台,由不同社交网络间用户交互行为引起的网络安全问题也日益明显。本文构建了不同社交网络间用户交互行为引起的网络病毒传播动力学模型。该模型与已有病毒传播模型<sup>[7-8]</sup>的不同之处在于考虑了社交网络间的交叉感染。利用微分方程稳定性理论分析了模型反映的网络病毒传播的动力学性态,得到了控制网络病毒扩散的基本再生数  $R_0$  的阈值,当  $R_0$  的值小于等于 1 时,网络病毒会被完全控制,这与不考虑交叉感染的已有模型结论一致。最后,数值仿真实验证了理论分析的正确性。同时,通过取不同参数值进行模拟,发现网络病毒传播的态势是由基本再生数直接决定的,只要基本再生数  $R_0$  的值小于 1, 病毒扩散最终就会被控制;相反,当基本再生数  $R_0$  的值大于 1 时, 病毒在网络中会一直存在。另

外,仿真结果表明,在网络节点总数相同的情况下,用户在社交网络中越分散,越有利于缓解网络病毒的爆发。

今后,将对不同活跃用户参与的社交网络数,以及对敏感信息处理的态度进行调研和统计分析,进一步检验模型的实际应用价值。

#### 参考文献(References)

- [1] FALLIERE N, MURCHU L O, CHIEN E. W32. Stuxnet dossier [EB/OL]. [2018-01-10]. [http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/w32\\_stuxnet\\_dossier.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf).
- [2] 国家计算机病毒应急处理中心. 关于“Petya”勒索病毒攻击事件的预警 [EB/OL]. [2018-02-10]. [http://www.cverc.org.cn/yubao/yubao\\_730.htm](http://www.cverc.org.cn/yubao/yubao_730.htm). (National Computer Virus Emergency Response Center. Early warning about the “Petya” ransomware attack [EB/OL]. [2018-02-10]. [http://www.cverc.org.cn/yubao/yubao\\_730.htm](http://www.cverc.org.cn/yubao/yubao_730.htm).)
- [3] 中国互联网络信息中心. 2016 年中国社交应用用户行为研究报告 [R/OL]. [2018-02-10]. <http://www.cnnic.net.cn/hlwfzyj/hlwzxbg/sqbg/201712/P02018010348597597840.pdf>. (China Internet Network Information Center. 2016 China social application user behavior research report [R/OL]. [2018-02-10]. <http://www.cnnic.net.cn/hlwfzyj/hlwzxbg/sqbg/201712/P02018010348597597840.pdf>.)
- [4] KEPHART J O, WHITE S R. Directed-graph epidemiological models of computer viruses [EB/OL]. [2018-02-10]. [https://www.worldscientific.com/doi/abs/10.1142/9789812812438\\_0004](https://www.worldscientific.com/doi/abs/10.1142/9789812812438_0004).
- [5] KEPHART J O, WHITE S R. Measuring and modeling computer virus prevalence [C]// Proceedings 1993 IEEE Computer Society Symposium on Research in Security and Privacy. Washington, DC: IEEE Computer Society, 1993: 2–15.
- [6] ZOU C C, GONG W B, TOWSLEY D. Code red worm propagation modeling and analysis [C]// CCS 2002: Proceedings of the 9th ACM Conference on Computer and Communications Security. New York: ACM, 2002: 138–147.
- [7] HAN X, TAN Q L. Dynamical behavior of computer virus on Internet [J]. Applied Mathematics and Computation, 2010, 64(7): 1–7.
- [8] 冯丽萍, 王鸿斌, 冯素琴. 改进的 SIR 计算机病毒传播模型 [J]. 计算机应用, 2011, 31(7): 1891–1893. (FENG L P, WANG H B, FENG S Q. Improved SIR model of computer virus propagation in the network [J]. Journal of Computer Applications, 2011, 31(7): 1891–1893.)
- [9] 冯丽萍, 韩琦, 王鸿斌. 具有变化感染率的僵尸网络传播模型 [J]. 计算机科学, 2012, 39(11): 51–53. (FENG L P, HAN Q, WANG H B. Botnet propagation model with variable infection rate [J]. Computer Science, 2012, 39(11): 51–53.)
- [10] 冯丽萍, 宋礼鹏, 王鸿斌, 等. P2P 僵尸网络的传播建模与分析 [J]. 计算机应用, 2015, 35(1): 68–71. (FENG L P, SONG L P, WANG H B, et al. Propagation modelling and analyzing of peer-to-peer botnet [J]. Journal of Computer Applications, 2015, 35(1): 68–71.)

(下转第 2922 页)



- Journal of Computers, 2014, 37(4): 927–949.)
- [5] OLIVEIRA S R M, ZAIANE O R. Achieving privacy preservation when sharing data for clustering [M]// JONKER W, PETKOVIC M. Secure Data Management. Berlin: Springer, 2004: 67–82.
- [6] MUKHERJEE S, CHEN Z, GANGOPADHYAY A. A privacy-preserving technique for Euclidean distance-based mining algorithms using Fourier-related transforms [J]. VLDB Journal, 2006, 15(4): 293–315.
- [7] BLUM A, DWORK C, McSHERRY F, et al. Practical privacy: the SuLQ framework [C]// Proceedings of the Twenty-Fourth ACM Sigmod-Sigact-Sigart Symposium on Principles of Database Systems. New York: ACM, 2005: 128–138.
- [8] DWORK C, NAOR M, PITASSI T, et al. Pan-private streaming algorithms [EB/OL]. [2018-01-10]. <http://nebula.wsimg.com/e2c5b9c40e7ca5ee436f9cb470b3ea7b?AccessKeyId=0EF19C92671ED94CE585&disposition=0&alloworigin=1>.
- [9] 李杨, 郝志峰, 温雯, 等. 差分隐私保护  $k$ -means 聚类方法研究 [J]. 计算机科学, 2013, 40(3): 287–290. (LI Y, HAO Z F, WEN W, et al. Research on differential privacy preserving  $k$ -means clustering [J]. Computer Science, 2013, 40(3): 287–290.)
- [10] 李洪成, 吴晓平, 陈燕. MapReduce 框架下支持差分隐私保护的  $k$ -means 聚类方法 [J]. 通信学报, 2016, 37(2): 124–130. (LI H C, WU X P, CHEN Y.  $k$ -means clustering method preserving differential privacy in MapReduce framework [J]. Journal on Communications, 2016, 37(2): 124–130.)
- [11] 吴伟民, 黄焕坤. 基于差分隐私保护的 DP-DBScan 聚类算法研究 [J]. 计算机工程与科学, 2015, 37(4): 830–834. (WU W M, HUANG H K. A DP-DBScan clustering algorithm based on differential privacy preserving [J]. Computer Engineering and Science, 2015, 37(4): 830–834.)
- [12] 刘晓迁, 李千目. 基于聚类匿名化的差分隐私保护数据发布方法 [J]. 通信学报, 2016, 37(5): 125–129. (LIU X Q, LI Q M. Differentially private data release based on clustering anonymization [J]. Journal on Communications, 2016, 37(5): 125–129.)
- [13] MATKOVIC Y, MATKOVIC Y. Robust spectral clustering for noisy data: modeling sparse corruptions improves latent embeddings [C]// Proceedings of the 2017 ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. New York: ACM, 2017: 737–746.
- [14] 熊平, 朱天清, 王晓峰. 差分隐私保护及其应用 [J]. 计算机学报, 2014, 37(1): 101–122. (XIONG P, ZHU T Q, WANG X F. A Survey on differential privacy and applications [J]. Chinese Journal of Computers, 2014, 37(1): 101–122.)
- [15] DWORK C. Differential privacy: a survey of results [C]// Proceedings of the 2008 International Conference on Theory and Applications of Models of Computation. Berlin: Springer, 2008: 1–19.
- [16] McSHERRY F, TALWAR K. Mechanism design via differential privacy [C]// Proceedings of the 2007 IEEE Symposium on Foundations of Computer Science. Piscataway, NJ: IEEE, 2007: 94–103.

This work is partially supported by the National Natural Science Foundation of China (61772034, 61602009), the Natural Science Foundation of Anhui Province (1808085MF172).

**ZHENG Xiaoyao**, born in 1981, Ph. D. candidate, associate professor. His research interests include information security, personalized recommendation.

**CHEN Dongmei**, born in 1994, M. S. candidate. Her research interests include information security, intelligent computing.

**LIU Yuqing**, born in 1994, M. S. candidate. Her research interests include information security, data mining.

**YOU Hao**, born in 1997. His research interests include information security, personalized recommendation.

**WANG Xiangshun**, born in 1992, M. S. candidate. His research interests include personalized recommendation.

**SUN Liping**, born in 1980, Ph. D., professor. Her research interests include spatial data processing, intelligent computing.

## (上接第 2902 页)

- [11] FENG L P, SONG L P, ZHAO Q S, et al. Modelling and stability analysis of worm propagation in wireless sensor networks [J]. Mathematical Problems in Engineering, 2015, 2015: Article ID 129598.
- [12] ZHU Q Y, CEN C. A novel computer virus propagation model under security classification [J]. Discrete Dynamics in Nature and Society, 2017, 2017: Article ID 8609082.
- [13] 孙文君, 苏旸, 曹镇. 一种非对称信息条件下的 APT 攻防博弈模型 [J]. 计算机应用, 2017, 37(9): 2557–2562. (SONG W J, SU Y, CAO Z. Attack-defense game model for advanced persistent threats with asymmetric information [J]. Journal of Computer Applications, 2017, 37(9): 2557–2562.)
- [14] 唐赞玉, 刘虹. 多阶段大规模网络攻击下的网络安全态势评估方法研究 [J]. 计算机科学, 2018, 45(1): 245–248. (TANG Z Y, LIU H. Study on evolution method of network security situation under multi-stage large-scale network attack [J]. Computer Science, 2018, 45(1): 245–248.)
- [15] LIU W P, ZHONG S M. Web malware spread modelling and optimal control strategies [J]. Scientific Report, 2017, 7: Article ID

42308.

- [16] 马知恩, 周义仓. 传染病动力学的数学建模与研究 [M]. 北京: 科学出版社, 2004. (MA Z E, ZHOU Y C. Mathematical Modelling and Study on Infectious Disease Dynamics [M]. Beijing: Sceince Press, 2004.)

This work is partially supported by the National Natural Science Foundation of China (61503050), the Key Disciplines Construction Project of Xinzhou Teachers University (XK201403).

**FENG Liping**, born in 1976, Ph. D., professor. Her research interests include network security, dynamical system.

**HAN Xie**, born in 1964, Ph. D., professor. Her research interests include virtual reality, network security.

**HAN Qi**, born in 1981, Ph. D., associate professor. His research interests include network security, optimistic control, cellular neural network.

**ZHENG Fang**, born in 1982, M. S. lecturer. Her research interests include information security, privacy protection.