P2P网络中被动型蠕虫传播与免疫建模

冯朝胜[1,2,3],秦志光[2],袁 丁[1],卿 昱[3]
(1.四川师范大学计算机科学学院,可视化计算与虚拟现实四川省重点实验室,四川成都 610101;
2.电子科技大学计算机科学与工程学院,四川成都 610054;3.中国电子科技集团公司第30研究所,四川成都 610041)

摘 要: 鉴于被动型蠕虫的危害性,对被动型蠕虫进行了深入分析,进而基于平均场法建立了被动型蠕虫的传播模型和免疫模型.基于传播模型和流行病传播学理论推导出进入无蠕虫平衡状态的充分条件,仿真实验证明了该充分条件的正确性.另外,仿真实验还表明,下载率和恢复率是控制蠕虫传播的两个可控的关键参数.在免疫软件被编制出来前,降低下载率和提高恢复率能有效控制被动型蠕虫的传播.

关键词: 被动型蠕虫; P2P文件共享网; 传播; 免疫; 建模; 仿真
中图分类号: TP393 **文献标识码:** A **文章编号:** 0372-2112 (2013)05-0884-06
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2013.05.009

Modeling Propagation and Immunization of Passive Worms in Peer-to-Peer Networks

FENG Chao-sheng[1,2,3], QIN Zhi-guang[2], YUAN Ding[1], QING Yu[3]
(1. *School of Computer Science, Sichuan Normal University, Chengdu, Sichuan* 610101, *China*;
2. *School of Computer Science & Engineering, University of Electronic Science and Technology of China, Chengdu, Sichuan* 610054, *China*;
3. *The No.30 institute of China Electronic Technology Corporation, Chengdu, Sichuan* 610041, *China*)

Abstract: In this paper, we identified the features of passive worm. Further the models of propagation and immunization of passive worms are proposed in the mean-field methods. Based on the model of worm propagation and Epidemiology, the sufficient condition for the global stability of the worm free equilibrium is deduced. Simulations validate the condition. Both the sufficient condition and all the experiment results show that amongst all P2P-related factors having effect on passive wormpropagation, attack performance of passive worms is most sensitive to two P2P system parameters: the download rate and the recovery rate. Controlling the two parameters, i.e. decreasing the download rate and increasing the recovery rate, provides an effective means for throttling the spread of passive worms.

Key words: passive worms; P2P networks; propagation; immunization; modeling; Simulations

1 引言

威胁P2P网络安全的蠕虫根据传播策略可分为两种[1]:一种是基于社会工程学,将蠕虫代码伪装后提供下载传播,采用这种方式传播的蠕虫就是被动型蠕虫,目前这种蠕虫已有数十种之多;另一种是发掘P2P客户端软件漏洞,利用对等网拓扑及其交互性质自主传播,这就是所谓的P2P主动型蠕虫.

导致P2P网络易遭受蠕虫攻击的主要因素[2,3]有四个.第一,P2P网络用户通常运行同样的客户端软件,这意味着一旦客户端软件有漏洞,那么整个网络都有漏洞,黑客或蠕虫会在极短的时间内攻破网络甚至使整个网络瘫痪.第二,用户可能下载置入了被动型蠕虫的文件,如Gnutella上的Mandragore蠕虫就会随着所置入的文件被下载而传播.第三,防火墙不能有效地防止被动蠕虫进行传播,因为被动蠕虫利用正常连接(下载)进行传播.第四,许多置入了被动蠕虫的文件通常都被冠之以最受欢迎文件的文件名,这无疑大大增加了感染的概率.虽然在导致P2P网络容易遭受攻击的四个因素中,后三个都和被动型蠕虫紧密相关,但是人们对它的研究相对较少.考虑到P2P被动型蠕虫的危害性,本文主要关注P2P被动型蠕虫.

收稿日期:2011-01-27;修回日期:2013-03-13
基金项目:国家科技重大专项课题(No.2011ZX03002-002-03);国家自然科学基金(No.60873075);可视化计算与虚拟现实四川省重点实验室课题(No.PJ2012002);广东省产学研重点项目(No.2012B091000054)

2 P2P 被动型蠕虫

与传统的网络蠕虫不同,P2P 被动型蠕虫将自身置入到共享文件中,随着共享文件的下载和执行而传播.由于是利用下载进行传播,所以它们无须像主动蠕虫那样去主动寻找具有漏洞的被攻击对象.当一台易感主机成功下载并执行一个置入了被动型蠕虫的感染文件时,该主机被感染,蠕虫会在该主机的共享文件夹下建立多个感染文件以供其它用户下载.为了提高传播速度,这些新生成的感染文件通常会被命名成广受欢迎的共享文件的名称[2,4].从传播形式上看,被动型蠕虫和木马有些相似之处,实际上,二者差别很大,木马主要被用来控制受害主机和收集其上的有用信息,而被动型蠕虫的主要作用就是破坏 P2P 网络文件共享功能.与主动型蠕虫相比,被动型蠕虫传播速度要慢很多,但由于其利用的是用户下载文件的正常连接进行传播,因此不会产生异常的连接和流量,所以检测到它比检测到主动蠕虫要困难得多.

3 P2P 被动蠕虫传播和免疫模型

3.1 建模参数和假设

根据被动型蠕虫传播的实际情况,在传播模型中,主机的状态分成三种:易感的、暴露的和感染的;而在免疫模型中,主机的状态多了一种——免疫的.为了便于下面的蠕虫建模分析,将建模时要用到的参数和实验时使用的值列举在表 1 中.

表 1　模型中用到的符号

符号	说明
$N(t)$	t 个时间单元后网络中主机台数.在本文中这个值不随 t 变化.$N(0)=100000$.
$S(t)$	t 个时间单元后易感主机数.$S(0)=99800$.
$I(t)$	t 个时间单元后感染主机数.$I(0)=100$.
$E(t)$	t 个时间单元后暴露主机数.$E(0)=100$.
$R(t)$	t 个时间单元后免疫主机数.$R(0)=100$.
$K(t)$	t 个时间单元后感染文件数.$K(0)=1100$.
$M(t)$	t 个时间单元后未感染文件数.$M(0)=1000000$.
$h(t)$	t 个时间单元后下载感染文件的概率为 $h(t)=\frac{K(t)}{M(t)+K(t)}$.
r	正常文件(从共享文件夹)的移出率.
λ_d	每个时间单元内每个主机下载文件的平均个数.
λ_e	每个时间单元内执行感染文件的暴露主机数.
λ_r	每个时间单元内恢复为易感状态的感染主机比例.
p_{ei}	每个时间单元内暴露主机成功执行感染文件的概率.
p_d	下载成功率 $p_d=\frac{\eta_1}{1+e^{2-\beta_1 d}}$,其中 d 为种子数,$\eta_1=1,\beta_1=0.5$
c	执行了下载的感染文件后在共享文件中增加的感染文件数.

建模基于流行病学和平均场法[5],所以模型中的参数代表的是平均值.考虑到下载成功率 p_d 与下载种子数 d 紧密相关,一般说来,种子越多,下载越可能成功;然而还没有研究表明它们具体有什么关系,在本文中采取文献[2]中的处理方法,即下载成功率与 d 的关系为 $p_d=\frac{\eta}{1+e^{2-\beta d}}$.为了简化建模,作了如下假设.

(1)网络中在线的用户数量没有发生变化.

(2)主机状态转移在一个时间单元(Time Unit)内完成.

(3)一台主机一旦被感染,将在共享文件夹中生成 c 个文件.所有的感染主机共享同样 c 个感染文件名称.

(4)建模时考虑的文件都是可执行文件,包括被压缩的可执行文件,不能包含蠕虫的文件如媒体文件不被考虑.

3.2 主机状态转移分析

在 P2P 被动型蠕虫传播的情况下,根据蠕虫传播的特点容易得到主机的状态转移图(如图 1 所示),其中,线段旁标明了转移概率,实线部分代表没有考虑免疫情况下主机的状态转移,而整个图即包括实线部分和虚线部分代表考虑免疫情况下主机状态转移.

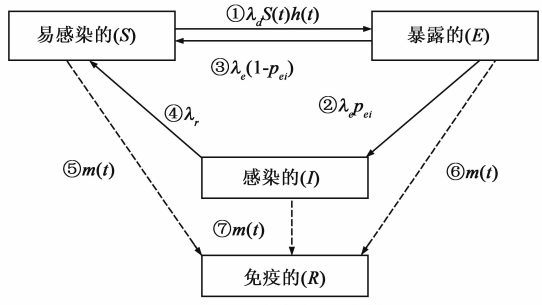


图1　P2P网络中主机状态转移图

(1)**主机所处状态说明:**①易感染的(S):当主机有因下载而被感染的风险时,该主机就处于易感染蠕虫状态.②暴露的(E):当主机上的 P2P 共享文件夹中至少拥有一个感染文件(下载而来,还没有执行)时,该主机就处于暴露状态.③感染的(I):当暴露主机执行了下载的感染文件后,感染文件的数量就会变成 c 个,此时主机处于感染状态.④免疫的(R):安装了免疫软件的主机就是免疫的.

(2)**主机状态转移说明:**① $S\rightarrow E$:当用户下载了感染文件,主机就由易感染状态转化到暴露状态.② $E\rightarrow I$:当暴露主机执行下载的感染文件时,如果下载的感染文件中被成功执行,那么主机就由暴露状态进入到已感染状态.③ $E\rightarrow S$:当暴露主机执行下载的感染文件时,如果下载的感染文件都被杀毒软件清除,那么主机就由暴露状态恢复到易感染状态.④ $I\rightarrow S$:当用户发现自己的主机已被感染并采取措施将共享文件夹中所有感染文件删除后,主机就由已感染状态回到易感染状态.⑤ $S\rightarrow R$, $E\rightarrow R$, $I\rightarrow R$:当在处于易感状态或暴露状态或感染状态的主机上安装上了蠕虫免疫软件后,该

主机就进入免疫状态.

3.3 蠕虫传播模型

根据蠕虫传播主机状态转移图(图 1 中的实线),不难得到如下蠕虫传播模型.

$$\frac{\mathrm{d}S(t)}{\mathrm{d}t} = -\lambda_d p_d h(t) S(t) + \lambda_r I(t) + \lambda_e (1-p_{ei}) E(t) \quad (1)$$

$$\frac{\mathrm{d}E(t)}{\mathrm{d}t} = \lambda_d p_d h(t) S(t) - \lambda_e E(t) \quad (2)$$

$$\frac{\mathrm{d}I(t)}{\mathrm{d}t} = \lambda_e p_{ei} E(t) - \lambda_r I(t) \quad (3)$$

$$N(t) = S(t) + E(t) + I(t) \quad (4)$$

其中, $p_d = \frac{\eta_1}{1+e^{2-\beta_1 d}}$, $h(t) = \frac{K(t)}{M(t)+K(t)}$.

$K(t)$是 t 个时间单元后感染文件的数量.在该时刻,$S(t)$台易感主机共成功下载了 $\lambda_d p_d h(t) S(t)$个感染文件;$E(t)$台暴露主机中有比例为 $\lambda_e p_{ei}$的主机执行了感染文件,有比例为 $\lambda_e(1-p_{ei})$的主机文件执行失败,感染文件相应增加 $\lambda_e p_{ei}(c-1)E(t)$个,减少 $\lambda_e(1-p_{ei})E(t)$个;感染主机中有 $\lambda_r I(t)$台主机恢复为易感主机,感染文件减少 $\lambda_r c I(t)$个.故 $K(t)$的变化率为:

$$\frac{\mathrm{d}K(t)}{\mathrm{d}t} = \lambda_d p_d h(t) S(t) + \lambda_e p_{ei}(c-1)E(t) - \lambda_e(1-p_{ei})E(t) - \lambda_r c I(t) \quad (5)$$

相应地,未感染文件的变化率为:

$$\frac{\mathrm{d}M(t)}{dt} = \lambda_d p_d N(t)(1-h(t)) - rM(t) \quad (6)$$

3.4 蠕虫免疫模型

随着感染主机的增多,用户的防范意识会不断增强,因而主机的免疫率不断增加.由于并不清楚免疫率与感染主机比例的具体关系,同样采用文献[2]的方法,即免疫率与感染主机比例的关系为

$$m(t) = \frac{\eta_2}{1+e^{2-\beta_2 \frac{I(t)}{N}}}$$

根据图 1,可以得到如下蠕虫免疫模型.

$$\frac{\mathrm{d}S(t)}{\mathrm{d}t} = -\lambda_d p_d h(t) S(t) + \lambda_r I(t) + \lambda_e (1-p_{ei}) E(t) - m(t) S(t) \quad (7)$$

$$\frac{\mathrm{d}E(t)}{\mathrm{d}t} = \lambda_d p_d h(t) S(t) - \lambda_e E(t) - m(t) E(t) \quad (8)$$

$$\frac{\mathrm{d}I(t)}{\mathrm{d}t} = \lambda_e p_{ei} E(t) - \lambda_r I(t) - m(t) I(t) \quad (9)$$

$$\frac{\mathrm{d}R(t)}{\mathrm{d}t} = m(t)(S(t)+E(t)+I(t)) \quad (10)$$

$$\frac{\mathrm{d}K(t)}{\mathrm{d}t} = \lambda_d p_d h(t) S(t) + \lambda_e p_{ei}(c-1)E(t) - \lambda_e(1-p_{ei})E(t) - \lambda_r c I(t) - m(t)(E(t)+cI(t)) \quad (11)$$

$$\frac{\mathrm{d}M(t)}{\mathrm{d}t} = \lambda_d (1-h(t)) N(t) - rM(t) \quad (12)$$

$$N(t) = S(t) + E(t) + I(t) + R(t) \quad (13)$$

其中, $h(t) = \frac{K(t)}{M(t)+K(t)}$, $p_d = \frac{\eta_1}{1+e^{2-\beta_1 d}}$.

4 无蠕虫平衡状态充分条件

定理 根据所提出模型和病毒学理论,被动型蠕虫传播进入无蠕虫平衡状态的充分条件是

$$\frac{N\lambda_d p_d}{\widetilde{M}\lambda_e} + \frac{NcP_{ei}\lambda_d p_d}{\widetilde{M}\lambda_r} < 1$$

证明:根据文献[6,7],传播模型状态变量为 E 和 I,由传播模型方程(2)和(3)可得:

$\boldsymbol{f} = \begin{bmatrix} \lambda_d p_d S(t) h(t) \\ 0 \end{bmatrix}$, $\boldsymbol{v} = \begin{bmatrix} \lambda_e E(t) \\ \lambda_r I(t) - \lambda_e E(t) P_{ei} \end{bmatrix}$,向量 $\boldsymbol{f}$ 和 $\boldsymbol{v}$ 分别代表输入流和输出流.其中,

$$h(t) = \frac{K(t)}{M(t)+K(t)} = 1 - \frac{M(t)}{M(t)+E(t)+cI(t)}$$

当网络处于无蠕虫平衡状态时,显然有

$$\frac{\mathrm{d}E(T)}{\mathrm{d}t} = \frac{\mathrm{d}I(T)}{\mathrm{d}t} = 0 \quad 和 \quad E(T) = I(T) = 0$$

分别求 $\boldsymbol{f}$ 和 $\boldsymbol{v}$ 对 E 和 I 的微分并将无蠕虫平衡状态值 $x_0 = \{\widetilde{S},0,0,0,\widetilde{M}\}$带入得

$$\boldsymbol{F} = \left[\frac{\partial f_i}{\partial x_j}(x_0)\right] = \begin{bmatrix} \frac{\lambda_d p_d N}{\widetilde{M}} & \frac{\lambda_d p_d cN}{\widetilde{M}} \\ 0 & 0 \end{bmatrix}$$

$$\boldsymbol{V} = \left[\frac{\partial v_i}{\partial x_j}(x_0)\right] = \begin{bmatrix} \lambda_e & 0 \\ -\lambda_e P_{ei} & \lambda_r \end{bmatrix} \Rightarrow \boldsymbol{V}^{-1} = \begin{bmatrix} \lambda_e^{-1} & 0 \\ \lambda_r^{-1} P_{ei} & \lambda_r^{-1} \end{bmatrix}$$

$$\boldsymbol{FV}^{-1} = \begin{bmatrix} \frac{\lambda_d p_d N}{\widetilde{M}} & \frac{\lambda_d p_d cN}{\widetilde{M}} \\ 0 & 0 \end{bmatrix} \begin{bmatrix} \lambda_e^{-1} & 0 \\ \lambda_r^{-1}\boldsymbol{P}_{ei} & \lambda_r^{-1} \end{bmatrix} = \begin{bmatrix} \frac{N\lambda_d p_d}{\widetilde{M}\lambda_e} + \frac{NcP_{ei}\lambda_d p_d}{\widetilde{M}\lambda_r} & \frac{Nc\lambda_d p_d}{\widetilde{M}\lambda_r} \\ 0 & 0 \end{bmatrix}$$

$$R_0 = \rho(\boldsymbol{FV}^{-1}) = \frac{N\lambda_d p_d}{\widetilde{M}\lambda_e} + \frac{NcP_{ei}\lambda_d p_d}{\widetilde{M}\lambda_r}$$

其中,$\rho()$表示求特征值.

根据文献[8]知,被动型蠕虫传播进入无蠕虫平衡状态的的充分条件是 $R_0 < 1$,即 $\frac{N\lambda_d p_d}{\widetilde{M}\lambda_e} + \frac{NcP_{ei}\lambda_d p_d}{\widetilde{M}\lambda_r} < 1$.

5 仿真及分析

5.1 实验说明

为了验证提出模型的有效性并检查 P2P 系统参数对蠕虫传播的影响,使用数值分析工具 Matlab 进行了

大规模仿真.为研究 P2P 参数的影响,将相关参数的仿真的结果放到同一个图中以便比较.表 1 给出了模型的参数和变量.在不作特别说明的情况下,参数的取值为表 2 给出的值,时间单位为分钟.

表 2　实验时参数的取值

参数	λ_d	λ_e	λ_r	p_{ei}	d	c
取值	0.02	0.02	0.001	0.8	6	10

5.2　仿真结果说明

从图 2 ~ 图 4 容易看出,下载率越大、暴露主机执行感染文件的概率和成功执行感染文件的概率越高,蠕虫传播得越快,进入稳定状态花费的时间越短,稳定时被感染的主机就越多.图 5 表明恢复率越高,蠕虫传播得就越慢,到达稳定状态需要的时间越多,稳定时被感染的主机越少.直观上讲,蠕虫能够生成的蠕虫文件越多,蠕虫文件使用的文件名越流行,那么蠕虫文件越可能被下载,主机感染的概率就越大.图 6 表明蠕虫能生成的文件越多,则蠕虫传播得越快,有更高感染峰值.在 Kazaa 网络中,蠕虫 Sanker 在共享文件夹中生成的恶意文件数是 20,其被著名的网络安全公司赛门铁克记录过的感染节点数不到 50 个,而能够生成 2000 个感染文件的蠕虫 Benjamin 去被记录感染了 1000 个节点.图 7 考查了下载种子数对蠕虫传播的影响,表明种子数越多,蠕虫传播得越快,进入稳定状态花费的时间越短,稳定时被感染的主机就越多.从直觉上看,初始感染主机数越多,蠕虫传播得越快,进入稳定状态花费的时间越短,稳定时被感染的主机就越多;图 8 表明初始感染主机数对蠕虫传播的影响不大,特别是对稳定状态时感染主机的数量没有影响.图 9 从实验上证明了被动型蠕虫传播进入无蠕虫平衡状态的充分条件.

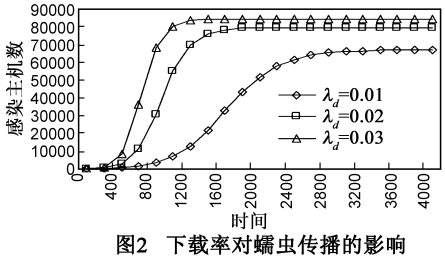


图2　下载率对蠕虫传播的影响

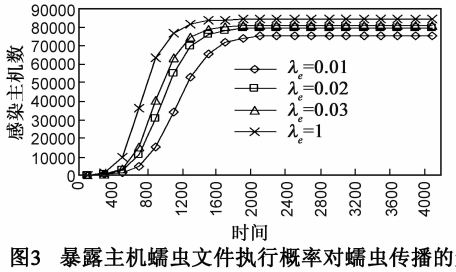


图3　暴露主机蠕虫文件执行概率对蠕虫传播的影响

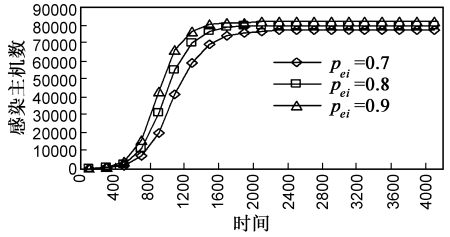


图4　成功执行蠕虫文件概率对蠕虫传播的影响

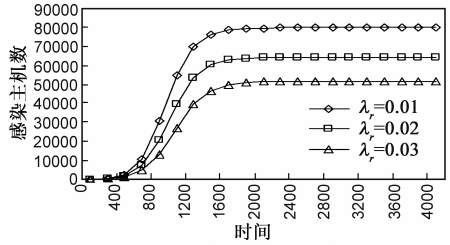


图5　恢复率对蠕虫传播的影响

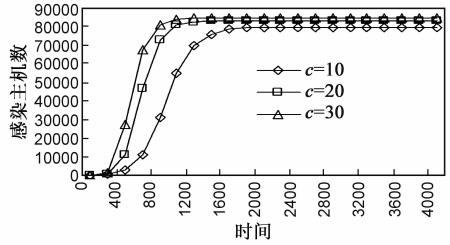


图6　*c*值对蠕虫传播的影响

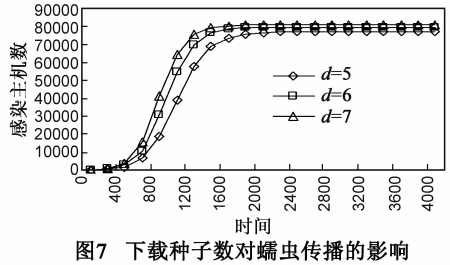


图7　下载种子数对蠕虫传播的影响

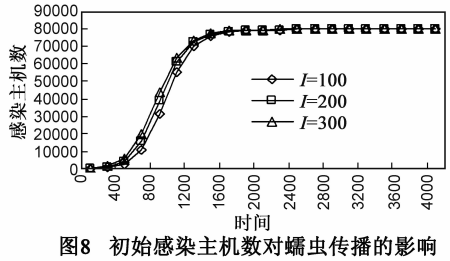


图8　初始感染主机数对蠕虫传播的影响

5.3　无蠕虫平衡状态充分条件的实验证明

为了从实验上证明基于所提出的传播数学模型推导出的蠕虫传播进入无蠕虫平衡状态充分条件的正确性,将图 9 相关实验对应的 R_0 值依次列举在表 3 中以便比较和分析.

表 3　图 9 相关实验对应的 R_0 值的比较

λ_r	0.012	0.013	λ_d	0.0018	0.0016	p_{ei}	0.07	0.06
R_0	1.06	0.94	R_0	1.05	0.97	R_0	1.10	0.95

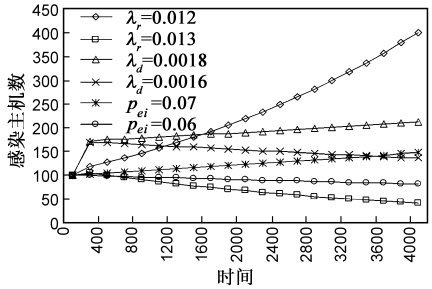


图9 蠕虫传播进入无蠕虫平衡状态充分条件的实验证明

当 $\lambda_r = 0.013$ 或 $\lambda_d = 0.0016$ 或 $p_{ei} = 0.06$(其它参数取默认值)时,网络中受感染的主机数量减少至消失,而对应的 R_0 值分别为 0.94,0.97 和 0.95,大量其它实验都有相似的结果,这就从实验上证明了无蠕虫平衡状态充分条件的正确性.

从表 3 和图 9 中可以发现,当 $R_0 < 1$ 时,蠕虫会逐渐消失;而当蠕虫始终存在时,一定有 $R_0 \geqslant 1$. 但当 $R_0 \geqslant 1$时,蠕虫是否一定会始终存在呢? 事实上,当 $\lambda_e = 0.0000002$ 时,蠕虫会迅速消失,而此时 $R_0 = 7322.283$,故 $R_0 \geqslant 1$ 为蠕虫始终存在的必要非充分条件.

5.4 蠕虫传播控制

实验表明,下载率 λ_d、恢复率 λ_r 和蠕虫生成文件数 c 是关键参数,其中前面两个是用户可控的,所以在没有找到免疫措施的情况下可以通过降低下载率和提高恢复率来控制蠕虫传播. 降低下载率有两条途径. 一条是提醒用户,让用户减少下载行为;另一条是通过服务器(如 BitTorrent 的 Tracker 服务器和 eDonkey2000 的全局服务器)来限制下载数量. 显然第二条更容易实施、更有效. 恢复率的提高可以通过在网上公布识别和删除 P2P 被动型蠕虫的方法来实现. 虽然用户无法控制蠕虫生成文件数,但其与恢复率关系紧密. 当蠕虫编写者想提高蠕虫感染能力而提高生成文件数数(如从 10 到 1000)时,蠕虫被用户识别的可能性也会增加,相应地恢复率也会增加.

在计算蠕虫繁殖率时,下载率可取 0.01 个文件/分钟[9],下载种子数可以通过实时下载文件测量获得,实时网络节点数可以从文件服务器上获取,干净文件数取最近一次没有检测出蠕虫时文件总数值,蠕虫文件生成数由蠕虫检测软件给出.

5.5 蠕虫的免疫

图 10 对两种免疫方法进行了比较($\eta_2 = 0.1$, $\beta_2 = 5$). 一种是常量免疫即每个时间单元的免疫率相同;另一种是动态免疫,这种情况下,免疫率和随感染主机占网络中所有主机的比率增加而增加. 图 10 表明,动态免疫能够更加有效地控制蠕虫传播. 这里,$m = 0.001257$ 和 $m = 0.001158$ 分别为动态免疫 $\lambda = 0.01$ 的 $\lambda = 0.009$ 的免疫率的均值(图 10 中 Gamma 对应的是动态免疫,而 m 是对应的是静态免疫).

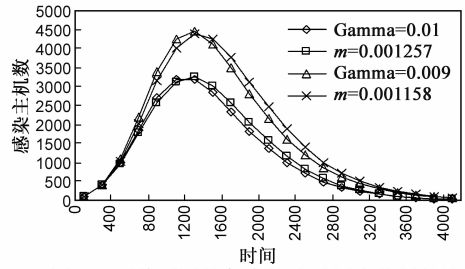


图10 两种不同的免疫策略对蠕虫传播的影响

6 相关研究

1988 年,Murray[10]率先利用数学流行病学对计算机病毒展开了研究. 1991 年,Kephart 和 White 将经典流行病模型引入计算机蠕虫传播建模中[11]. M. Ripeanu[12]、S. Sen[13]和 D. Stutzbach[26]等人分别在他们的论文指出,P2P 网络为无尺度网络,而 R. Pastor-Satorras 等人则在其 2001 年发表的论文中指出无尺度网络非常适合病毒(主动型蠕虫)的传播并给出了传播模型[14]. 2002 年,Staniford 等人撰文[15]指出 P2P 网络很适合 Contagion 蠕虫的传播,但没有给出任何模型. 2005 年 Dumitriu 等人[16]对感染文件在 P2P 网络上的传播进行了建模. R. W. Thommes 和 M. J. Coates 对 P2P 文件共享网上的病毒传播和感染文件传播分别进行了建模[9]. 2006 年,Chen 等人[17]对非扫描型 P2P 蠕虫进行了仿真分析,然而,他们并没有给出 P2P 蠕虫传播的数学模型. 2008 年,王方伟、马建峰等提出了被动型蠕虫在 P2P 网络上的传播模型[18],然而该模型主要是针对 Gnutella 这样的当前并不流行的 P2P 网络,并不适合 eDonkey2000 和 BitTorrent 这样的时下最流行的 P2P 网络. 2009 年,应凌云、冯登国等研究了 P2P 技术对僵尸网络的影响,提出了基于层次化 P2P 网络技术的新型僵尸网络结构[19].

7 总结与展望

本文对 P2P 被动型蠕虫的特点进行了说明和分析,深入分析了 P2P 网络中主机的状态转移过程并基于该分析利用平均场法提出了被动型蠕虫传播模型;在此基础上,基于流行病传播学理论推导出了蠕虫传播进入无蠕虫平衡状态的充分条件. 仿真实验结果不仅证明了该充分条件的正确性,还表明:不同的 P2P 参数对蠕虫传播的影响有很大不同,其中可控的关键参数是下载率和恢复率,因此在免疫软件开发出来前可以考虑通过降低下载率和提高恢复率来制定蠕虫抑制策略. 在未来研究中,重点是被动型蠕虫的预警、检测和扼制方法,并基于本文提出的模型来验证检测方法

和扼制方法的有效性.

参考文献

[1] 夏春和,石昀平,李肖坚.结构化对等网中的 P2P 蠕虫传播模型研究[J].计算机学报,2006,29(7):952 – 959.
Xia Chun-he, Shi Yun-ping, Li Xiao-jian. Research on epidemic modesl of P2P worms in structured peer-to-peer networks[J]. Chinese Journal of Computers, 2006, 29(7): 952 – 959. (in Chinese)

[2] Chen G, Gray R S. Simulating non-scanning worms on peer-to-peer networks[A]. Proc of the 1st Int Conf on Scalable Information Systems[C]. Hong Kong: ACM, 2006.

[3] Zhou L, Zhang L, McSherry F, et al. A first look at peer-to-peer worms: Threats and defenses[A]. Proc of the 4th Int Workshop on Peer-to-Peer Systems[C]. New York: Springer, 2005.24 – 35.

[4] Nassima K, Yannick C, Nazim A. The emerging threat of peer-to-peer worms [A]. Proc of IEEE / IST Workshop on Monitoring, Attack Detection and Mitigation[C]. Tuebingen, Germany: IEEE, 2006.18 – 20.

[5] Frauenthal J C. Mathematical Modeling in Epidemiology[M]. New York: Springer, 1980.

[6] Driessche P, Watmough J. Reproduction numbers and subthreshold endemic equilibria for compartmental models of disease transmission[J]. Mathematical Biosciences, 2002, 180: 29 – 48.

[7] Arnio J, Davis J, Hartley D, et al. A multi-species epidemic model with spatial dynamics[J]. Mathematical Medicine and Biology, 2005.

[8] Diekmann O, Heesterbeek J A P. Mathematical Epidemiology of Infectious Diseases: Model Builind, Analysis and Interpretation[M]. Wiley, 1999.

[9] Thommes R W, Coates M J. Modeling Virus Propagation in Peer-to-Peer Networks[R]. Montreal, Canada: Department of Electrical and Computer Engineering, McGill University, 2005.

[10] Murray W H. The application of epidemiology to computer viruses[J]. Computers and Security, 1988, 7: 130 – 150.

[11] Kephart J O, White S R. Directed-graph epidemiological models of computer viruses[A]. Proc of IEEE Symp. Security and Privacy[C]. Oakland : IEEE, 1991.343 – 359.

[12] Ripeanu M. Peer-to-peer architecture case study: Gnutella network[A]. Proc of the First International Conference on Peer-to-Peer Computing[C]. Linkoping, Sweden: IEEE, 2001.

[13] Sen S, Wang J. Analyzing peer-to-peer traffic across large networks[J]. IEEE/ACM Transactions on Networking, 2004, 12(2): 219 – 232.

[14] Stutzbach D, Rejaie R, Sen S. Characterizing unstructured overlay topologies in modern P2P file-sharing systems[A]. Proc of the Fifth ACM Internet Measurement Conference [C]. Berkeley: ACM, 2005.49 – 62.

[15] Pastor-Satorras R, Vespignani A. Epidemic spreading in scale-free networks[J]. Physical Review Letters, 2001, 86(14): 3200 – 3203.

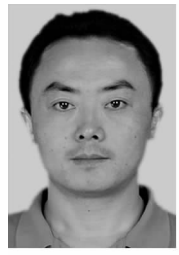
[16] Staniford S, Paxson V, Weaver N. How to Own the Internet in Your Spare Time[A]. Proc of the 11th USENIX Security Symposium[C]. San Francisco: ACM, 2002.149 – 167.

[17] Dumitriu D, Knightly E, Kuzmanovic A, et al. Denial-of-service resilience in peer-to-peer file-sharing systems[A]. Proc of ACM Sigmetrics[C]. Banff, Canada: ACM, 2005.

[18] 王方伟,张运凯,马剑峰.无结构 P2P 网络中被动型蠕虫传播建模和防治[J].天津大学学报,2008,14(1):66 – 72.
Wang Fang-wei, Zhang Yun-kai, Ma Jian-feng. Modeling and defending passive worms over unstructured peer-to-peer networks[J]. Transaction of Tianjin University, 2008, 14(1): 66 – 72. (in Chinese)

[19] 应凌云,冯登国,苏璞睿.基于 P2P 的僵尸网络及其防御[J].电子学报,2009,37(1):31 – 37.
Ying Ling-yun, Feng Deng-guo, Su Pu-rui. P2P-based super botnet: Threat s and defenses[J]. Acta Electronica Sinica, 2009, 37(1): 31 – 37. (in Chinese)

作者简介



冯朝胜　男,1971 年生于四川广元,博士后,副教授,硕士生导师,中国计算机协会高级会员.2010 年获得电子科技大学信息与通信工程博士学位.研究方向为分布式计算、网络与信息安全、恶意代码分析.
E-mail: csfenggy@126.com

秦志光　男,1956 年生于四川荣昌,博士,电子科技大学计算机科学与工程学院教授、博士生导师,IEEE 高级会员.研究方向为密码学、网络与信息安全.

袁　丁　男,1967 年生于四川宜宾,博士,四川师范大学计算机科学学院教授,硕士生导师.2003 年获得西南交通大学工学博士学位.研究方向为网络与信息安全.

卿　昱　女,1970 出生于四川,中国电子科技集团公司第三十研究所研究员,硕士生导师.研究方向为网络安全、软件设计.