第 59 卷 第 2 期 2010 年 2 月
1000-3290/2010/59(02)/0705-07

物 理 学 报
ACTA PHYSICA SINICA

Vol. 59, No. 2, February, 2010

节点抗攻击存在差异的无尺度网络恶意软件传播研究*

宋玉蓉[1)] 蒋国平[1)2)†]

1)(南京邮电大学控制与智能技术研究中心,南京 210003)

2)(南京邮电大学自动化学院,南京 210003)

(2009 年 4 月 1 日收到;2009 年 5 月 15 日收到修改稿)

在考虑节点抗攻击能力存在差异情形下,研究了恶意软件在无尺度网络中的传播行为. 基于元胞自动机理论,建立了节点具有攻击差异的恶意软件传播模型. 通过定义脆弱性函数,以描述不同度节点的抗攻击差异,使得模型更具普遍性. 研究了不同形式的脆弱性函数对恶意软件在无尺度网络中的传播临界值和时间演化的影响. 研究表明,节点抗攻击能力的差异对传播行为会产生重要影响,如导致传播临界值改变、传播速度减缓. 研究指出,脆弱性函数是网络选择适合的免疫策略的重要依据.

关键词: 无尺度网络, 恶意软件传播, 抗攻击能力, 脆弱性函数

PACC: 0250, 0565, 0570J

1. 引 言

复杂网络中,传染病、病毒、恶意软件等的传播作为网络传播动力学探究的问题之一,近年来已经吸引了大量研究者的兴趣,取得了许多重要的研究成果[1—6]. Pastor-Satorras 等[1—3,7,8]的研究表明,病毒在无尺度网络中,只要传播率大于零,病毒都能传播并最终维持在一个平衡状态. 通常度大的节点被称为 Hub 节点[9,10],其往往成为传播过程中的超级传播者[11]. 以上研究对于节点的抗攻击能力做了如下假设:任何一个健康节点不论度大小都具有相同的抗攻击能力. 在这种假设下,由于度大的节点有更多的机会和被感染节点接触,而使得受到感染的概率会大大增加,一旦被感染,会将病毒传染给更多的节点.

但是,在很多实际网络中,上述假定并不成立. 在一些实际网络中,节点度越大的节点往往有更高的安全意识,抵抗病毒入侵能力也会越强,从而这样的节点尽管有更多的机会和感染节点接触,但受到感染的概率随着其强的安全防范意识和措施而迅速降低. 例如,在 Internet 上,节点度大的节点往往是路由器或服务器等节点,路由器会设置严格的访问控制列表、防火墙、入侵检测、防御系统等安全机制[12,13]. 服务器大多使用 Linux, Sun 等操作系统,而当前大多安全攻击、病毒传播主要针对 Windows 操作系统. 这些因素都使得路由器或服务器这类节点度大的节点,由于其相应安全机制的应用和操作系统的选择,表现出较强的抗攻击能力,并不会被轻易感染,从而也降低了其成为超级传播者的可能性. 另外,尽管节点度大的节点可能和感染者接触的机会多,但由于其自身具有强的抗感染能力,其最终被感染的概率会低于甚至远低于系统平均感染率.

最近,针对上述情形的相关研究已有报道. Olinky 等[14]认为,病毒传播既依赖于网络结构,也依赖于病毒感染机制. 在他们建立的 SIS (susceptible-infected-susceptible) 模型中,定义一个度为 k 的健康节点和一个感染节点,接触后受到的感染概率 $A(k)$ 依赖于节点的度 k, k 越大的节点,受到感染的概率越低,即节点表现出更强的抗攻击能力. 这种基于连接依赖的感染方案能导致无尺度网

* 教育部新世纪优秀人才支持计划(批准号:NCET-06-0510)、国家自然科学基金(批准号:60874091)、江苏省"六大人才高峰"(批准号:SJ209006)和江苏省普通高校研究生科研创新计划(批准号:CX08B_081Z)资助的课题.

† 通讯联系人. E-mail: jianggp@njupt.edu.cn

络出现正的传播阈值. Wang 等[15]做了和 Olinky 等[14]相似的研究,基于 SIR 模型,将边的非均匀传输与网络结构相结合,研究边传输分布对传播阈值的影响.

上述研究[14,15]利用平均场方法,建立确定性模型,进行相关问题的研究. 而平均场方法只适合对传播过程做整体预测,难以反映传播过程的稀有概率事件和空时相关性等[16,17]. 近年来,元胞自动机(cellular automata,CA)模型对复杂系统的研究已经受到人们的广泛关注,并被成功用于研究多种网络中的病毒传播行为[16,18—23]. 例如,White 等[16]使用二维 CA,建立了考虑局域化效应的 SIR 传播模型;Song 等[23]使用一维元胞自动机,建立了随机传播模型,研究在多种网络拓扑下节点具有相同抗攻击能力的恶意软件传播概率行为.

本文将考虑网络节点存在抗攻击能力差异时,恶意软件在无尺度网络中的传播行为. 基于节点抗攻击差异,利用 CA 模型,建立无尺度复杂网络中恶意软件传播模型. 通过定义脆弱性函数,描述不同度节点的抗攻击差异,由抗攻击差异而表现出节点获得感染的概率差异,使提出的模型更具普遍性. 在此模型之上进行传播阈值和传播时间演化分析和讨论,结果表明,在节点脆弱性和度呈反比的情形下,即度大的节点具有更强的抗攻击能力时,网络中恶意软件的传播临界值增加,传播速度减缓. 具有相同度分布性质的不同网络,由于网络应用的不同,节点脆弱性函数可能不一致,不同的脆弱性函数对临界值和传播速度的影响也不同. 同时指出,反映网络抗攻击能力的脆弱性函数对于为网络选择适合的免疫策略提供了参考依据.

2. 节点存在抗攻击差异的元胞自动机传播模型

一个 CA 可以通过一个四元组 (C,Q,V,f) 定义,其中 C 表示元胞空间,Q 表示有限状态集,V 表示节点的邻域,f 代表状态转换规则函数[24].

元胞空间 C:建立包含 N 个元胞的一维元胞空间,一维元胞空间中的一个元胞即代表网络中的一个节点.

邻域 V:以网络的邻接矩阵 $\boldsymbol{A}$ 直接定义各元胞邻居关系,节点 i 的邻域 $\boldsymbol{V}_i$ 就被定义为 $\boldsymbol{A}$ 中的第 i 行向量,即 $\boldsymbol{V}_i=\{a_{ij}\mid a_{ij}\in\boldsymbol{A},j=1,2,\cdots,N\}$;若 $a_{ij}=1$,表示节点 i 和 j 之间存在连接.

状态集 Q:基于 SIS 模型,仅考虑节点的健康(S)、感染(I)两种状态,健康态用 0 表示,感染态以 1 表示,令 $Q=\{0,1\}$,节点 i 在 t 时刻的状态变量用 $s_i(t)$($s_i(t)\in Q$)表示,则有

$$s_i(t)=\begin{cases}1(\text{感染态}),\\0(\text{健康态}).\end{cases}\tag{1}$$

本地转换函数 f:任何节点仅能与其邻居接触而可能获得感染,节点 i 在离散时刻 t 的状态 $s_i(t)$ 依赖于节点在上一时刻的自身状态 $s_i(t-1)$ 和其邻居的状态 $s_{V_i}(t-1)$. 每个时间步内,一个感染节点试图以概率 p_i 接触处于健康状态的邻居节点,也即一个健康节点受到处于感染状态的一个邻居的接触概率为 p_i. 显然这个健康节点 i 获得感染节点接触的概率 $\hat{\beta}_i$ 必然随着其处于感染状态的邻居数目的增加而增加,这个接触概率定义为

$$\hat{\beta}_i=1-(1-p_i)^{m_i(t)},\tag{2}$$

这里,$m_i(t)$ 表示在 t 时刻,节点 i 的邻居中处于感染状态的邻居数目,且有 $m_i(t)=\sum_{j=1}^{N}a_{ij}s_j(t)$. 同时,在此时间步内,感染节点以概率 δ 恢复健康,由此建立节点状态转换函数

$$s_i(t+1)=\max(f_\delta(s_i(t)\times(1-\delta_i)),f_\beta(\overline{s_i(t)}\hat{\beta}_i)),\tag{3}$$

式中右侧的两项结果中的最大值即为节点经过一个时间 t 后的结果状态. 这里,$\bar{\cdot}$ 表示取反操作,(3)式中第一项 $f_\delta(s_i(t)(1-\delta_i))$ 表示治愈过程. 先前处于感染状态节点,经过一个离散时间 t 后,以 δ 概率治愈回到健康态,以 $1-\delta$ 概率维持原有的感染态,即 $f_\delta(x)$ 为治愈过程的状态转换子函数,具体定义如下:

$$f_\delta(x)=\begin{cases}1 & (x\geqslant\delta),\\0 & (x<\delta).\end{cases}\tag{4}$$

(3)式中第二项 $f_\beta(\overline{s_i(t)}\hat{\beta}_i))$ 表示感染过程. 处于健康状态的节点,经过一个离散时间 t 后的状态改变结果,即 $f_\beta(x)$ 为感染过程的状态转换子函数.

考虑到节点存在抗攻击差异,度大的节点更有可能因为安全机制相对完备,具有较强的抗攻击能力,并不易被感染,而度小的节点则可能疏于安全考虑,而显得比较脆弱易于受到感染. 那么每个节点从健康态到感染态的转换概率随其抗攻击能力的差异而不同. 这种差异我们用节点脆弱性来度

量. 为简单起见，考虑节点脆弱性仅和节点度有关. 因此，定义函数 $\alpha(k)$ 来表示一个度为 k 的节点的脆弱性，该函数是 k 的单调递减函数，函数值越大表示节点越脆弱，相应的抗攻击能力越低，反之节点越健壮，抗攻击能力越强.

在一个时间步里，显然一个节点抗攻击能力越弱，其可能的被感染率就越大. 一个度为 k 的节点 i，由 S 态变为 I 态的概率可以定义为

$$\beta_i = c \cdot \alpha(k), \tag{5}$$

这里 c 为一常数，按此定义，每一个节点可由其度的大小而拥有的不同的抗攻击能力而导致各个节点拥有不同的获得感染的概率.

经过以上分析，则感染函数可定义为

$$f_\beta(x_i) = \begin{cases} 1 & (x_i \leqslant \beta_i) \\ 0 & (x_i > \beta_i) \end{cases} \quad (i = 1,2,\cdots,N). \tag{6}$$

进一步说明(6)式，在一个时间步 t 中，节点 i 由健康态转为感染态的依据是其接触概率 $\hat{\beta}_i$ 与其被感染率 β_i 比较的结果. 特别注意的是，这里 β_i 正比于函数 $\alpha(k)$. 那么度大的节点，$\hat{\beta}_i$ 会随其感染邻居数目 $m_i(t)$ 的增加而增大，但 β_i 随抗攻击性的增强而降低，所以潜在地大度节点也并不易被感染.

假设网络中度为 k 的节点其概率服从分布 $P(k)$，网络中节点总数为 N，对(5)式左右两端分别取平均，则网络中所有节点的平均感染概率 $\overline{\beta}$ 为

$$\overline{\beta} = \frac{1}{N}\sum_i \beta_i = c\sum_k \alpha(k)P(k) = c\langle \alpha(k) \rangle. \tag{7}$$

由(7)式可以得到常数 c 的值为 $c = \overline{\beta}/\langle \alpha(k) \rangle$，代入(5)式得到

$$\beta_i = \overline{\beta}\alpha(k)/\langle \alpha(k) \rangle, \tag{8}$$

这里 $\alpha(k)$ 的具体形式可以依据研究需要和网络具体环境而确定.

特别地，若 $\alpha(k) = 1$，则表示各节点拥有相同的抗攻击能力，导致各节点的感染概率也是一致的，即为系统平均感染概率 $\overline{\beta}$. 那么显然度大的节点，$\hat{\beta}_i$ 会随其感染邻居数目 $m_i(t)$ 的增加而增大，而 $\overline{\beta}$ 是一定值，潜在地大度节点更容易被感染. 这种情况则与文献[23]中的模型完全等价.

最后令 $I(t)$ 表示 t 时刻网络中受感染节点的比例，$S(t)$ 表示处于健康状态节点比例；$I(0)$ 表示初始时刻的主机感染比例，则有下列统计结果：

$$I(t) = \frac{1}{N}\sum_{i=1}^{N} s_i(t),$$
$$I(t) + S(t) = 1. \tag{9}$$

模型中，恶意软件传播过程由两个主要因素决定：1)网络的拓扑结构，这反映在模型参数 $\hat{\beta}_i$ 中；2)网络节点的抗攻击差异性，通过定义节点脆弱性函数，这种差异最终体现在各节点的感染概率 β_i 中.

需要说明的是，以上模型考虑免疫过程后也同样适用于 SIR 模型. 在此不再赘述.

3. 仿真研究

我们考虑一个具有如下参数的 Barabasi-Albert (BA)无尺度网络[25]：$N = 2000$，$\langle k \rangle = 6$.

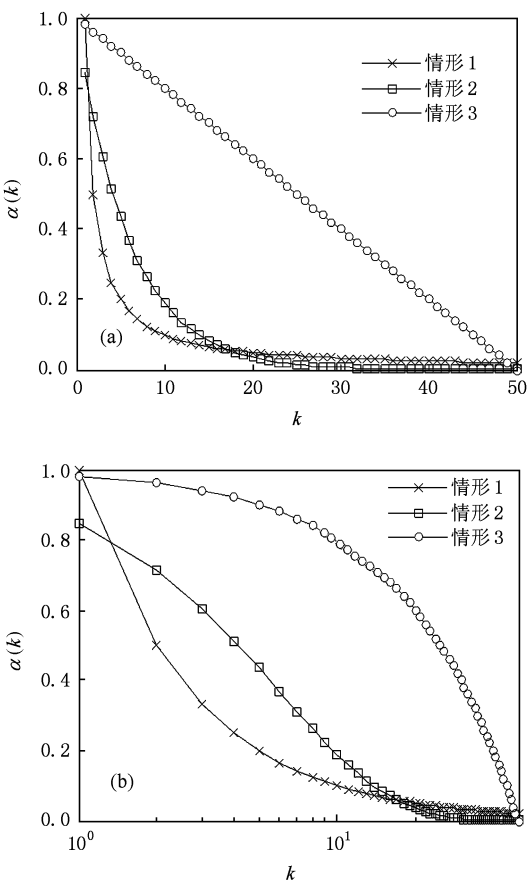

图 1　脆弱性函数与节点度的关系　(a)双线性坐标，(b)对数-线性坐标

定义节点脆弱性函数 $\alpha(k)$ 为以下几种形式，情形 1：$\alpha(k) = k^{-1}$；情形 2：$\alpha(k) = e^{-k/\langle k \rangle}$；情形 3：$\alpha(k) = 1 - k/\max(k)$；情形 4：$\alpha(k) = 1$. 特别地，情形 4 完全等价于节点抗攻击能力一致的情形，以便与前三种情形(考虑节点存在抗攻击差异)进行相互比较. 前三种情形下的脆弱性函数与自变量 k 的

关系如图 1 所示:图 1(a)为双线性坐标,图 1(b)的横坐标为对数坐标.

3.1. 传播阈值变化

基于上节所提出的传播模型,研究在上述四种脆弱性函数作用下的 BA 网络传播临界值问题.

仿真中,$N=2000$,初始受到感染的节点数目为 1,即 $I(0)=1/N$;$\overline{\beta}$ 从 0 以步长 0.01 线性增长到 1;不失一般性,取治愈率 $\delta=1$;已知传播值定义为 $\lambda=\overline{\beta}/\delta$. 在每个 λ 值下,分别运行模型 200 次后做统计平均.

CA 为随机数学模型,与确定性的微分方程最大不同就是 CA 能反映传播过程中的概率事件,那么每次的仿真实验中,当传染率在临界值附近时,病毒有可能会大规模流行,但也可能会在感染之初就趋于消亡. 这在我们先前的研究中已经有研究结论[23]. 例如,当取 $\lambda=0.16$,$\alpha(k)=k^{-1}$ 时,随机任选一个初始感染节点开始病毒传播时,在 200 次系统实现中,有 197 次病毒在感染之初就趋于消亡,仅有 3 次病毒大规模流行. 我们得到病毒爆发次数与传染率的关系曲线如图 2 所示. 四种脆弱性函数作用下,各 200 次的系统实现中,出现病毒爆发的最小传播值(记为传播阈值 λ_c)和病毒发作次数(记为 N_e)分别为

情形 1:$\lambda_c=0.14$,$N_e=1$;

情形 2:$\lambda_c=0.26$,$N_e=6$;

情形 3:$\lambda_c=0.07$,$N_e=5$;

情形 4:$\lambda_c=0.04$,$N_e=3$.

在 $\lambda<\lambda_c$ 时,病毒 100% 消亡. 当 $\lambda\geqslant\lambda_c$ 时,病毒传播可能爆发也可能消亡,且病毒爆发的比例随 λ 值的增加呈指数上升趋势. 显然在阈值附近,病毒爆发属于稀有事件.

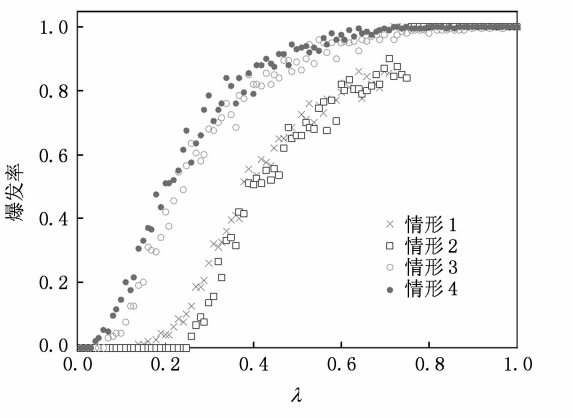

图 2 病毒爆发频度与传染率的关系

在传播值为 λ,N_1 次系统实现中,记病毒传播呈现消亡的实现次数为 N_0,显然 $N_1=N_0+N_e$,每次系统实现执行 T 个时间步. 如果在 N_1 次实现中不区分爆发还是消亡,直接做传播值 λ 下传播密度的混合统计平均 $I(\lambda)$,则有

$$I(\lambda)=\sum_{n=1}^{N_1}\sum_{t=1}^{T}I(t,n,\lambda)/(TN_1),\qquad(10)$$

这里,$I(t,n,\lambda)$ 表示在传播率为 λ,第 n 次系统实现,第 t 个时间步时的感染节点比例.

如果我们对区分爆发还是消亡做分类统计,则有

$$I(\lambda)=\begin{cases}\displaystyle\sum_{n=1}^{N_1}\sum_{t=1}^{T}I(t,n,\lambda)/(TN_1)\\ \qquad(N_0=N_1),\\ \displaystyle\sum_{I(T,n,\lambda)\neq 0}\sum_{t=1}^{T}I(t,n,\lambda)/\\ (T(N_1-N_0))\quad(N_0<N_1).\end{cases}\qquad(11)$$

图 3 为根据(10)式进行混合统计平均后,感染规模与传播值的关系;若区分爆发和消亡的情形,根据(11)式进行分类统计平均,得到图 4 感染规模与传播值的关系曲线,该曲线整体较图 3 中的曲线更为平滑. 但在靠近临界值附近我们看到波动较大,这是因为此时病毒爆发是稀有概率事件,统计样本数较少.

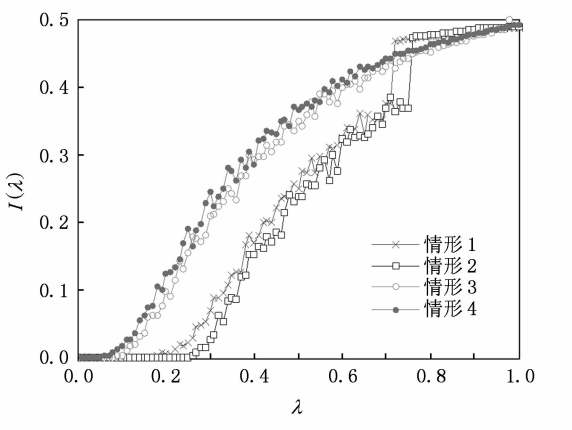

图 3 混合统计平均下的感染规模与传播值的关系

从图 3,4 中可看出前三种情形与情形 4 相比有效增大了传播阈值. 首先确保系统的全局平均感染率 $\overline{\beta}$ 在四种情形下均一致变化,前三种情形考虑网络中节点个体存在抗攻击差异性,由于个体的度差异而使得各个节点的脆弱性存在差异,继而其被感

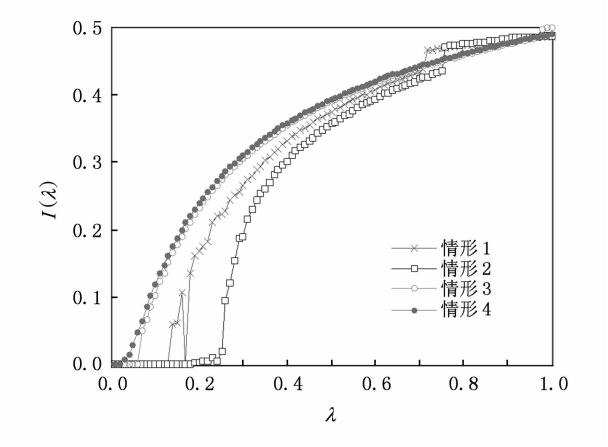

图 4　分类统计平均下的感染规模与传播值的关系

染率不同,从而表现出与节点被感染率一致情况下不同的阈值结论. 由于有效增大了传播阈值,从而也有效降低了病毒在 BA 无尺度网络大规模爆发和流行的可能性. 进一步分析发现,$\alpha(k)=e^{-k/\langle k\rangle}$ 时具有最大的传播临界值,$\alpha(k)=k^{-1}$ 时其次,$\alpha(k)=1-k/\max(k)$ 时再次之. 可见,传播阈值与 $\alpha(k)$ 有强的依赖关系.

接着,我们对网络规模对传播过程的影响做进一步仿真分析. 分别生成如下规模的 BA 网络:$N=200,500,1000,2000,5000$. 并取脆弱性函数为情形 1,对网络中节点数对阈值的影响进行了仿真比较,仿真结果如图 5 所示. 从图 5 中可以看到,在不同的网络规模下,表征感染规模 $I(\lambda)$ 与传播阈值 λ 的关系曲线在五种网络规模下几乎重合,网络规模对传播阈值有一定影响,但影响较小,且随着网络规模的增大,这种影响趋于消失.

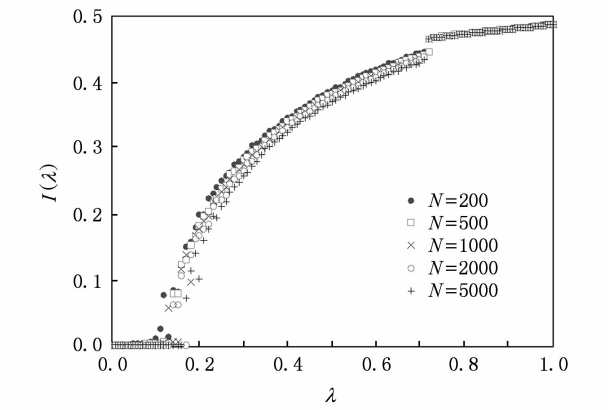

图 5　网络规模对传播的影响(分类统计结果)

3.2. 传播演化

进一步理解提出模型的时间演化特性,取仿真参数:$\overline{\beta}=0.2,\delta=0.5,I(0)=1/N$;此时 $\lambda=0.4$,同样考虑上节定义的脆弱性函数的四种情形. 基于这四种脆弱性函数对模型分别执行 100 次仿真实验,取这 100 次仿真结果的统计平均. 在不同抗攻击函数的作用下,仿真得到图 6 所示的恶意软件时间演化曲线.

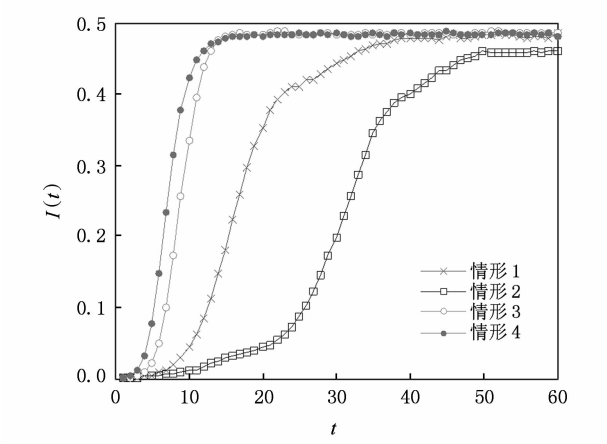

图 6　考虑抗攻击差异 SIS 模型的恶意软件传播时间演化　$N=2000,\overline{\beta}=0.2,\delta=0.5,I(0)=1/N$

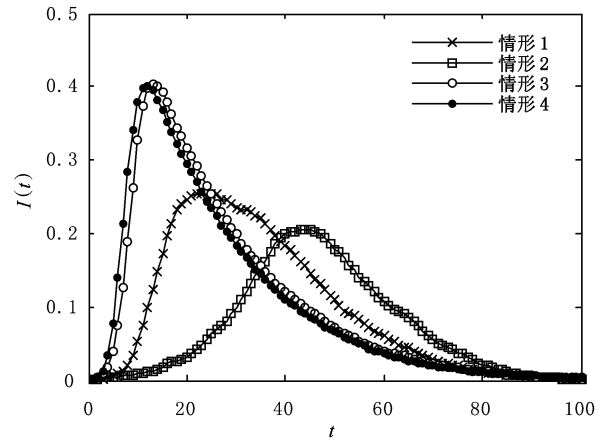

图 7　考虑抗攻击差异 SIR 模型的恶意软件传播时间演化　$N=2000,\overline{\beta}=0.2,\delta=0.5,I(0)=1/N$,随机免疫概率 $\gamma=0.1$

从图 6 中可看出,在考虑了节点脆弱性差异的前三种情形与不考虑节点脆弱性差异的情形 4 相比,传播速度有效减缓. 分析认为,低度节点虽然其感染率高于全局感染率,但它们和具有感染状态的节点的接触概率并不高,对恶意软件传播扩散的贡献是有限的;高度节点由于抗攻击能力强,获得感染的机会大大降低,也大大降低了其成为超级传播者的可能性,从而也降低了该类节点将病毒传播给

更多其他节点的风险,因而使得传播速度得以延缓.进一步分析发现,不同脆弱性函数对速度的影响是不同的.当 $\alpha(k)=e^{-k/\langle k\rangle}$ 时传播速度最为缓慢,$\alpha(k)=k^{-1}$ 时其次,$\alpha(k)=1-k/\max(k)$ 时再次之.

我们也对考虑节点抗攻击差异的 SIR 模型在时间演化特性方面进行了仿真研究,结果如图 7 所示.图 7 得到的结果与图 6 类似,考虑节点抗攻击差异以后,有效减缓了传播规模和传播速度,不同的脆弱性函数对传播速度和规模的影响是不同的.实施随机免疫后,前三种情形的病毒消亡速度也高于第四种情形.

这也再一次说明,反映网络抗攻击能力的网络脆弱性函数对于恶意软件在网络中的爆发和时间演化是密切相关的.

4. 结 论

本文研究了在考虑网络节点存在抗攻击能力差异时,恶意软件在无尺度网络中的传播行为.基于节点攻击差异,使用 CA 建立恶意软件传播模型.通过定义脆弱性函数,描述不同度节点的抗攻击差异,这种差异使得在传播过程中,不同度节点表现出不同的感染概率,模型更具普遍性.仿真中,定义四个度相关的脆弱性函数,在提出的模型之上进行了分析和比较研究.研究表明,在节点脆弱性和度呈反比的情形下,无尺度网络的传播临界被有效增加,病毒在网络中的传播速度变得缓慢.不同的脆弱性函数对临界值和传播速度的改变也不同.本文同时指出,反映网络抗攻击能力的脆弱性函数,对于网络选择适合的免疫策略提供了参考依据.在实际网络设计中,如何选择合适的脆弱性函数,使得网络具有大的传播临界值及较慢的传播速度,有效对抗网络病毒攻击,具有重要的意义,这也是我们下一步的研究重点.

[1] Pastor-Satorras R, Vespignani A 2001 *Phys. Rev.* E **63** 066117

[2] Moreno Y, Pastor-Satorras R, Vespignani A 2002 *Eur. Phys. J.* B **26** 521

[3] Boguna M, Pastor-Satorras R, Vespignani A 2003 *Phys. Rev. Lett.* **90** 028701

[4] Yang R, Zhou T, Xie Y B, Lai Y C, Wang B H 2008 *Phys. Rev.* E **78** 066109

[5] Li X, Wang X F, Xu D 2007 *Acta Phys. Sin.* **56** 1313 (in Chinese) [李 翔、汪小帆、许 丹 2007 物理学报 **56** 1313]

[6] Pei W D, Chen Z Q, Yuan Z Z 2008 *Chin. Phys.* B **17** 0373

[7] Pastor-Satorras R, Vespignani A 2002 *Phys. Rev.* E **65** 035108

[8] Pastor-Satorras R, Vespignani A 2001 *Phys. Rev. Lett.* **86** 3200

[9] Albert R, Barabasi A L 2002 *Rev. Mod. Phys.* **74** 47

[10] Newman M E J 2003 *SIAM Rev.* **45** 167

[11] Small M, Tse C K, Walker D M 2006 *Physica* D **215** 146

[12] Melnikov A 2005 *RFC* 4314—— *IMAP*4 *Access Control List*

[13] Desai N *http://securityfocus.com/printable/infocus/*1670

[14] Olinky R, Stone L 2004 *Phys. Rev.* E **70** 30902

[15] Wang J, Liu Z, Xu J 2007 *Physica* A **382** 715

[16] White S H, Rey A M D, Sanchez G R 2007 *Appl. Math. Comput.* **186** 193

[17] Nekovee M 2008 *Lecture Notes in Computer Science* **5151** 105

[18] Jin Z, Liu Q X, Mainul H 2007 *Chin. Phys.* **16** 1267

[19] Liu Q X, Jin Z 2005 *Chin. Phys.* **14** 1370

[20] Fuentes M A, Kuperman M N 1999 *Physica* A **267** 471

[21] Jin Z, Liu Q X 2006 *Chin. Phys.* **15** 1248

[22] Song Y, Jiang G P 2009 *The First International Conference on Complex Sciences: Theory and Application* (COMPLEX'2009), Shanghai, China, p487

[23] Song Y R, Jiang G P 2009 *Acta Phys. Sin.* **58** 5911 (in Chinese) [宋玉蓉、蒋国平 2009 物理学报 **58** 5911]

[24] Wolfram S 1986 *Theory and Applications of Cellular Automata* (Singapore: World Scientific Publication)

[25] Barabási A L, Albert R 1999 *Science* **286** 509

Malware propagation in scale-free networks for the nodes with different anti-attack abilities*

Song Yu-Rong[1)]　Jiang Guo-Ping[1)2)†]

1) (*Center for Control & Intelligence Technology, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*)

2) (*College of Automation, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*)

(Received 1 April 2009; revised manuscript received 15 May 2009)

Abstract

Considering the nodes with different anti-attack abilities in scale-free networks, we investigated the probabilistic behaviors of malware propagation in scale-free complex networks. Using the cellular automata, we proposed a model of malware propagation in complex networks with the nodes having different anti-attack abilities. In particular, a vulnerability function related to node's degree is firstly introduced into the model to describe the different anti-attack abilities of nodes. Then, the epidemic threshold and time evolution of malware propagation are investigated through analysis and simulation for the various vulnerability functions. The results show that different anti-attack abilities of nodes can produce significant effects on the behaviors of propagation. For example, different anti-attack abilities of nodes can change the value of epidemic propagation, and slow down the spreading speed of malware. Finally, it is pointed out that the vulnerability function is very important for adopting appropriate immunization strategies to control the malware propagation.

Keywords: scale-free network, malware propagation, anti-attack ability, vulnerability function

PACC: 0250, 0565, 0570J

* Project supported by the Program for New Century Excellent Talents in University of Ministry of Education of China (Grant No. NCET-06-0510), the National Natural Science Foundation of China (Grant No. 60874091), the "Six Sponsoring Talent Summits" of Jiangsu Province, China (Grant No. SJ209006), and the Scientific Innovation Program for University Research Students in Jiangsu Province, China (Grant No. CX08B_081Z).

† Corresponding author. E-mail: jianggp@njupt.edu.cn