# 动态环境下的主动蠕虫攻击分析*

唐浩坤[1]，刘宴兵[2]，黄 俊[2]
(1. 电子科技大学 计算机科学与工程学院，成都 610054；2. 重庆邮电大学 通信与信息工程学院，重庆 400065)

**摘 要**：鉴于当前很少有传播模型充分考虑到 P2P 节点动态特征对主动蠕虫攻击的影响，提出两个动态环境下的主动蠕虫传播模型。分析了主动蠕虫两种常见的攻击方式，给出了相应攻击背景下的节点状态转换过程，在综合考虑 P2P 节点动态特征的基础上提出了两种主动蠕虫传播模型，并对所提出的模型进行了数值分析，探讨动态环境下影响主动蠕虫传播速度的关键因素。实验结果表明，通过提高 P2P 节点的离线率和免疫力可以有效地抑制主动蠕虫对 P2P 网络的攻击。

**关键词**：主动蠕虫；动态环境；传播模型；P2P 网络
**中图分类号**：TP393.08 **文献标志码**：A **文章编号**：1001-3695(2013)06-1831-04
doi:10.3969/j.issn.1001-3695.2013.06.060

# Analyze active worm attacks in dynamic environment

TANG Hao-kun[1], LIU Yan-bing[2], HUANG Jun[2]
(1. *School of Computer Science & Engineering, University of Electronic Science & Technology of China, Chengdu* 610054, *China*; 2. *School of Communication & Information Engineering, Chongqing University of Posts & Telecommunications, Chongqing* 400065, *China*)

**Abstract**: Given few works focused on the propagation model that fully considered the influence of the dynamic features of P2P nodes on active worm attack, this paper proposed two propagation models of active worms in dynamic environment. First, it studied two common attack strategies of active worms and provided states transition process of nodes when active worms spread in accordance with these attack strategies. Second, it presented two propagation models combined with the dynamic characteristic of P2P nodes. And finally, it conducted mathematical analysis on these presented models and explored the key factors affecting active worm propagation in dynamic P2P environment. The experimental result shows that it is able to effectively suppress the spread of active worm in P2P networks by increasing the off-line rate and immunity of P2P nodes.
**Key words**: active worm; dynamic environment; propagation model; P2P networks

## 0 引言

作为未来无线宽带网络的核心技术，P2P 传播模式已成为当前的一个研究热点，财富杂志更是将 P2P 网络定义为影响今后互联网发展的四项新技术之一。现在 P2P 应用流量占据了当前互联网流量的 37%，而这一比例在多媒体数据共享领域更是高达 90%[1]。虽然 P2P 网络在资源共享和快速路由方面具有极大的优势，但同时也为网络蠕虫的快速传播与大规模入侵提供了良好的平台。

根据美国计算机网络应急技术处理协调中心(CERT/CC)的统计数据，自 1998 年以来，网络安全事件每年以 50% 的速度呈指数级增长，其中网络恶意代码因其扩散速度快、受害面大、穿透能力强等特点一直高居网络安全事件之首。而在所有的恶意代码中，主动蠕虫因其可在无人干涉的情况下主动传播而成为危害性最大的病毒。

近年来，国内外学者针对主动蠕虫的传播模型及防御方法进行了大量的研究。Chen 等人[2]提出了基于离散时间的主动蠕虫传播模型；Yu 等人[3]按照 SEM 的思想，从静态网络拓扑的角度分析了 P2P 蠕虫的传播过程，并在文献[4]中比较了四种不同攻击策略下的蠕虫传播性能，指出基于目标列表的 P2P 蠕虫具有很好的攻击效率；Jia 等人[5]提出了利用良性蠕虫对抗恶性蠕虫以建立一个安全的 P2P 网络；Wang 等人[6]提出了在 Chord 网络中的主动蠕虫传播模型；Ravikumar 等人在文献[7]中为在类似 Gnutella 的分布式网络中的恶性代码的传播进行建模；Zhang 等人[8]提出非结构化 P2P 系统中的主动蠕虫静态模型；Yang 等人[9]提出了基于动态隔离的主动蠕虫模型；Feng 等人[10,11]参考节点间度数差异的情况下分别构建了主动蠕虫在非结构化 P2P 系统中的传播模型；Jafarabadi 等人[12]根据 P2P 节点的搅动特性，在 SIR 模型的基础上开发了一种主动蠕虫传播模型。

上述工作都在一定程度上对主动蠕虫的传播过程进行了描述，为主动蠕虫的防御机制提供了有益的参考，但这些工作中提及的传播模型或多或少地忽略了一些 P2P 节点在动态环境下的行为特征，没有充分考虑主动蠕虫在 P2P 节点这些动态特征综合作用下的传播效果，所以也不能够很准确地刻画出动态环境下主动蠕虫在 P2P 网络中的传播过程。本文力图解

**收稿日期**：2012-09-14；**修回日期**：2012-11-05 **基金项目**：国家科技重大专项基金资助项目(2011ZX03002-004-03)；重庆市高等教育成果转换基金资助项目(Kjzh10206)；公安部信息网络安全重点实验室项目(C11609)

**作者简介**：唐浩坤(1977-)，男，博士研究生，主要研究方向为网络安全、P2P 网络应用(tanghk@cqupt.edu.cn)；刘宴兵(1971-)，男，教授，博导，主要研究方向为网络安全、网格计算；黄俊(1982-)，男，博士，主要研究方向为网络优化、QoS.

决这个问题,并作了如下三点贡献:

a)分析了主动蠕虫在动态环境下的两种常用的攻击策略,给出了主动蠕虫按照这些攻击策略进行传播时,P2P 节点的动态转换过程。

b)在前面提到的攻击策略的基础上,构建了主动蠕虫的两种传播模型,同时也描述了主动蠕虫在多种 P2P 节点动态特征共同作用下的传播过程。

c)利用数学分析方法研究上述传播模型,推导出动态环境下影响主动蠕虫传播速度的关键参数,为今后的主动蠕虫防御提供指导。

## 1 主动蠕虫常用的攻击策略

在动态环境下,P2P 网络中存在两种常见的攻击策略。

### 1.1 基于随机扫描的攻击策略

按此种攻击策略,感染了主动蠕虫的节点在发起攻击前不会收集其他在线节点的路由信息,每次它只会随机地从 IPv4 的地址空间选择一个地址并尝试发起攻击,如果被选中的 IP 地址正好被分配给一个存在安全漏洞的 P2P 节点,则它会以 $\varphi$ 的概率被主动蠕虫感染,当此节点下载完所有蠕虫复本的分片后,它就变为一个新的蠕虫节点,再以同样的方式感染其他节点;否则本次尝试攻击失败。

### 1.2 基于列表扫描的攻击策略

在此种攻击策略下,主动蠕虫会事先收集 P2P 网络中在线节点的路由信息,自动生成一个扫描列表(hit-list),然后再按照此列表对目标节点发起攻击。一旦有新节点被蠕虫节点感染,蠕虫节点就会从扫描列表中将一部分未扫描的目标节点路由信息分发给这些新感染的节点,让这些新感染的节点继续按此信息对存在安全漏洞的列表节点发动攻击,这种攻击一直持续到列表中的所有节点都被扫描完为止。

### 1.3 主动蠕虫传播时的节点状态转换过程

当主动蠕虫在动态环境中传播时,节点存在以下六种状态,在任一时刻,每个节点只能属于其中一种状态:

a)易感染态($S$ 状态)。此类在线节点具有安全漏洞,容易受到蠕虫攻击,但没有被感染节点扫描到。

b)潜伏态($L$ 状态)。此状态的节点已经从一个蠕虫节点下载完所有的蠕虫分片,但整合后的蠕虫文件还未被本节点执行。在此阶段的节点既不会再被其他蠕虫节点感染,也不会感染其他易感染节点。

c)已感染态($I$ 状态)。一旦一个处于 $L$ 状态的节点执行了整合后的蠕虫文件,此节点的状态就由 $L$ 态转换为 $I$ 态,在此状态下的节点具有感染性,已经成为蠕虫节点。

d)隔离态($Q$ 状态)。如果一个已感染节点因传播蠕虫分片而被监控软件发现,它将被隔离并转换为隔离态,在此阶段,节点不再具有传染性。

e)免疫态($R$ 状态)。此类在线节点由于已经被安全软件打上漏洞补丁,不会再被蠕虫感染或感染其他在线节点。

f)离线态($O$ 状态)。节点离开 P2P 网络后的状态。

当一个存在安全漏洞的良性节点刚加入 P2P 网络时,它处于易感染态;打了漏洞补丁后就成为免疫态;一个具有感染性的恶性蠕虫刚加入 P2P 网络时,它处于已感染态;当一个处于 $I$ 状态的节点连接到一个处于 $S$ 状态的节点,它就会以 $\varphi$ 的概率向其注入蠕虫分片,当此 $S$ 状态的节点下载完所有的蠕虫分片,但并未执行整合后的蠕虫文件时,它处于潜伏态;当处于 $L$ 状态的节点以 $\eta$ 的概率执行了其上的蠕虫文件后,它就变为已感染态;当处于 $I$ 状态的节点因传播蠕虫分片而以 $\chi$ 的概率被监控软件发觉时,它会变为隔离状态;当安全软件在定期检测中发现处于 $S$、$L$、$I$、$Q$ 状态的在线节点存在安全漏洞时,这些漏洞节点会分别以 $r_1$、$r_2$、$r_3$ 和 $r_4$ 的概率转换到免疫态;所有在线节点会以 $\alpha$ 的概率选择离线并转换为 $O$ 状态;而离线节点又会以 $\beta$ 的概率选择上线,转换为离线前的状态;另外部分离线节点会以 $\delta$ 的概率重装系统,当它们重新上线时,它们会转换为 $S$ 状态。节点状态转换如图 1 所示

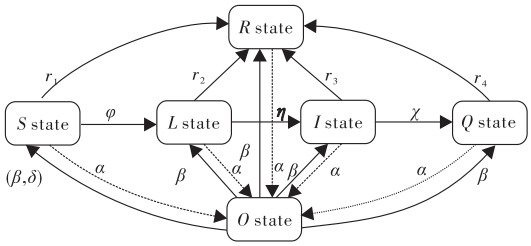


图1 节点状态转换图

## 2 动态环境下的两种传播模型

### 2.1 参数与假设

根据上面提到的两种攻击策略,本文开发了两种动态环境下的主动蠕虫传播模型,为了简化主动蠕虫的传播过程,假设基于列表扫描策略的蠕虫能事先收集到所有在线节点的路由信息;主动蠕虫不会对已感染节点进行重复攻击;蠕虫节点可以在一个单位时间向一个未感染节点注入所有的蠕虫分片;在整个测试阶段,P2P 节点的总量控制在 10 000 个。表 1 列出了所有模型中所用到的参数。

### 2.2 基于随机扫描的蠕虫传播模型(PRS model)

基于本策略的主动蠕虫传播模型应该满足以下定理。由于篇幅关系,省略了对以下定理的证明,感兴趣的读者可以关注笔者的后续文章。

**定理 1**

$$S_o(t)=\alpha\sum_{i=0}^{t-1}S_N(i)(1-\beta)^{t-i}$$

$$E_o(t)=\alpha\sum_{i=0}^{t-1}E_N(i)(1-\beta)^{t-i},I_o(t)=\alpha\sum_{i=0}^{t-1}I_N(i)(1-\beta)^{t-i}$$

$$Q_o(t)=\alpha\sum_{i=0}^{t-1}Q_N(i)(1-\beta)^{t-i}$$

$$R_o(t)=\alpha\sum_{i=0}^{t-1}R_N(i)(1-\beta)^{t-i} \tag{1}$$

**定理 2**

$$A_N(t+1)=\varphi\cdot S_N(t)\cdot\left[1-(1-1/T)^{I_N(t)\cdot\lambda\cdot(1-I_N(t)/S_N(0))}\right] \tag{2}$$

**定理 3**

$$S_N(t+1)=(1-\alpha-r_1)\cdot S_N(t)+\beta\cdot S_o(t)+\delta\cdot O(t)-A_N(t+1) \tag{3}$$

**定理 4**

$$L_N(t+1)=(1-\alpha-r_2-\eta)\cdot L_N(t)+\beta\cdot L_o(t)+A_N(t+1) \tag{4}$$

**定理 5**

$$I_N(t+1)=(1-\alpha-r_3-\chi)\cdot I_N(t)+\beta\cdot I_o(t)+\eta\cdot E_N(t) \tag{5}$$

**定理 6**

$$Q_N(t+1)=(1-\alpha-r_4)\cdot Q_N(t)+\beta\cdot Q_o(t)+\chi\cdot I_N(t) \tag{6}$$

**定理 7**

$$R_N(t+1)=(1-\alpha)\cdot R_N(t)+\beta\cdot R_o(t)+r_1\cdot S_N(t)+r_2\cdot L_N(t)+r_3\cdot I_N(t)+r_4\cdot Q_N(t) \tag{7}$$

**定理 8**

$$O(t+1)=(1-\beta)\cdot O(t)+\alpha\cdot[S_N(t)+E_N(t)+I_N(t)+Q_N(t)+R_N(t)] \quad (8)$$

表 1　模型中的参数

| 参数 | 描述 |
|---|---|
| $T$ | IPv4 网络中的节点数 |
| $\lambda$ | 已感染态节点的扫描率(蠕虫节点在一个单位时间内可以扫描到的节点数) |
| $\varphi$ | 被扫描到的易感染态节点能被已感染态节点感染的概率 |
| $\alpha$ | 在线节点的离线概率 |
| $\beta$ | 离线节点的上线概率 |
| $\delta$ | 重装系统后的离线节点重新上线的概率 |
| $a$ | P2P 网络的平均带宽 |
| $W$ | 蠕虫文件的平均大小 |
| $\eta$ | 蠕虫文件的下载率(潜伏节点在一个单位时间内可以下载到的蠕虫文件的个数,$\eta=a/W$) |
| $\chi$ | 已感染态节点因异常行为被监测软件发现并被隔离的概率 |
| $\gamma$ | P2P 中的有效地址占 IPv4 网络中的地址的比例,$\gamma<24\%$ [13] |
| $r_1$ | 易感染态节点被杀毒软件检测出安全漏洞,打上补丁转换为免疫态节点的概率 |
| $r_2$ | 潜伏态节点被杀毒软件检测出安全漏洞,清除蠕虫文件,打上补丁转换为免疫态节点的概率 |
| $r_3$ | 已感染态节点被杀毒软件检测出安全漏洞,清除蠕虫文件,打上补丁转换为免疫态节点的概率 |
| $r_4$ | 隔离态节点被杀毒软件检测出安全漏洞,清除蠕虫文件,打上补丁转换为免疫态节点的概率 |
| $S_N(t)$ | 在时刻 $t$,P2P 系统中处于易感染态的在线节点数。注 $S_N(0)$ 表示最初阶段 P2P 系统中脆弱节点的总数 |
| $S_O(t)$ | 在时刻 $t$,由易感染态转换而来的离线节点数 |
| $S(t)$ | 在时刻 $t$,P2P 系统中处于易感染态的所有节点数,显然有 $S(t)=S_N(t)+S_o(t)$ |
| $L_N(t)$ | 在时刻 $t$,P2P 系统中处于潜伏态的在线节点数 |
| $L_O(t)$ | 在时刻 $t$,由潜伏态转换而来的离线节点数 |
| $I_N(t)$ | 在时刻 $t$,P2P 系统中处于已感染态的在线节点数,其中 $I_N(0)$ 表示最初阶段 P2P 系统中的蠕虫节点数 |
| $I_O(t)$ | 在时刻 $t$,由已感染态转换而来的离线节点数 |
| $Q_N(t)$ | 在时刻 $t$,P2P 系统中处于隔离状态的在线节点数 |
| $Q_O(t)$ | 在时刻 $t$,由隔离态转换而来的离线节点数 |
| $R_N(t)$ | 在时刻 $t$,P2P 系统中处于免疫态的在线节点数 |
| $R_O(t)$ | 在时刻 $t$,由免疫态转换而来的离线节点数 |
| $A_N(t)$ | 在时刻 $t$,P2P 系统中从易感染态转换到潜伏态的新增在线节点数 |
| $O(t)$ | 在时刻 $t$,P2P 系统中处于离线态的节点总数 |

### 2.3　基于列表扫描的蠕虫传播模型(HLS model)

基于本策略的主动蠕虫传播模型满足的定理与上述模型基本一致,为了节省篇幅,本文只列出了其中有差异的一条定理。

**定理 9**

$$A_N(t+1)=\varphi\cdot S_N(t)\cdot\{1-[1-1/(S(t)-A_N(t))]^{I_N(t)\cdot\lambda}\}$$

其中:

$$S(0)=T\cdot\gamma, A_N(t)=0 \quad (9)$$

## 3　数值模拟与性能分析

本文利用 MATLAB 研究动态环境下,模型中的各种参数对主动蠕虫传播速度的影响,模拟平台运行在 Windows XP 专业版 SP3 下,CPU 主频 3.1 GHz,内存 4 GB,初始的 P2P 节点个数定为 10 000 个,通过调整模型中各个参数来观察蠕虫感染覆盖率(受感染节点数/P2P 节点总数)的变化,以此来推断影响主动蠕虫传播效率的关键因素。本文只列举出了部分实验结果,但推导出的结论很多也适用于其他一些蠕虫攻击模型。

### 3.1　PRS 模型的数值模拟结果

1)图 2 显示了 PRS 模型中蠕虫节点的扫描率对主动蠕虫传播的影响。如图 2 所示,在蠕虫传播初期阶段,蠕虫节点的扫描率越高,其达到感染覆盖率早期峰值的时间越早,最后的峰值数也越大;但到了蠕虫传播的中后期,蠕虫节点的扫描率越低,其达到的感染覆盖率反而越高,其数值会逐渐从早期峰值下降到一个平衡点。

分析原因在于蠕虫传播的初期,网络中存在着大量有安全漏洞的未感染节点,采用随机扫描方式的蠕虫节点的扫描率越高,在一轮扫描中发现有效的可攻击节点的数量也就越多,其蠕虫感染覆盖率增长得也越快;但随着 P2P 网络中蠕虫节点的不断增长,越来越多的节点由 $S$ 状态转换到 $L$ 状态或是 $I$ 状态,当蠕虫感染覆盖率达到峰值后,蠕虫节点每轮攻击能扫描到的有效可攻击节点的数量就越来越少,从而导致蠕虫传播中后期的蠕虫感染覆盖率逐步下降,当每轮中新增加的已感染状态的节点数与减少的感染状态的节点数相等时,蠕虫感染覆盖率就达到平衡点并持续保持;同时由于扫描率低的蠕虫节点在进行探测攻击时被监控软件发现并隔离的概率要比扫描率高的蠕虫节点低,从而导致扫描率低的蠕虫节点被发现并转换到 $Q$ 状态的节点数要比扫描率高的蠕虫节点少,因此在蠕虫传播的中后期,扫描率越低的蠕虫节点所保持的蠕虫感染覆盖率反而越大。

2)图 3 显示了 PRS 模型中在线节点的离线率对主动蠕虫传播的影响,如图 3 所示在蠕虫传播初期,在线节点的离线率越低,其达到的感染覆盖率越高;但到了蠕虫传播的中后期,在线节点的离线率越高,其达到的感染覆盖率也越高。

分析原因在于蠕虫传播的初期,网络中存在着大量有安全漏洞的未感染节点,这为采用随机扫描方式传播的主动蠕虫提供了大量的潜在攻击目标,此时在线节点的离线率越低,保持在线的易感染节点的数量越多,主动蠕虫可攻击的潜在目标也就越多,其蠕虫感染覆盖率上升得也越快;但当蠕虫感染覆盖率达到早期峰值后,越来越多的易感染节点转换为 $L$ 状态或 $I$ 状态,主动蠕虫可攻击的目标也逐步减少,另外越来越多的蠕虫节点因传播蠕虫分片而被隔离,使得其蠕虫感染覆盖率有所下降,紧接着,越来越多的各类离线节点因重装系统上线而重新变成易感染状态,而且这一趋势会随着在线节点的离线率提高而加强,从而为主动蠕虫的传播提供了更多新的可攻击对象,这就使得在蠕虫传播的中后期,节点的离线率越高,其后期感染覆盖率增长得也就越快。

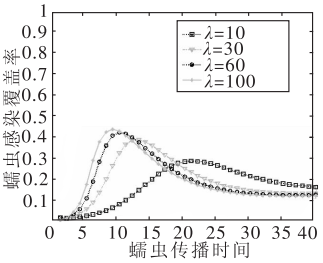

图2　PRS模型中蠕虫节点扫描率对蠕虫传播的影响

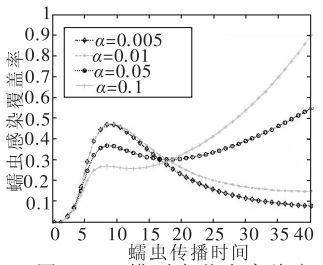

图3　PRS模型中节点离线率对蠕虫传播的影响

3)图 4 显示了 PRS 模型中,在线节点的免疫等级对主动蠕虫传播的影响。如图 4 所示,在线节点的免疫等级越高,其感染覆盖率的值越小;在蠕虫传播的中后期,由于蠕虫传播所引发的感染覆盖率会由早期的峰值下降到一个平衡点。

分析原因在于在线节点的免疫能力越高,各类存在安全漏洞的在线节点被监控软件发现并免疫的概率也越大,其蠕虫感染覆盖率也就越低。当一轮攻击中新增的已感染态节点与减

少的已感染节点的数目相同时,蠕虫感染覆盖率就达到平衡点并持续保持。从图中可以看出在线节点的免疫能力对蠕虫传播的影响很大。

### 3.2 HLS 模型的数值模拟结果

图 5 显示了无论是基于 PRS 还是 HLS 策略的蠕虫节点的扫描率都对主动蠕虫传播产生相同的影响,但是基于 HLS 策略的蠕虫节点扫描率对蠕虫传播速度的影响不如基于 PRS 策略的蠕虫节点扫描率明显。因为所有基于 HLS 策略的在线蠕虫节点都是从同一个扫描列表中寻找攻击目标,在蠕虫传播的中后期,列表中只剩下很少部分未扫描目标,因此这时基于 HLS 策略的蠕虫节点的扫描率对蠕虫感染覆盖率的影响不如基于 PRS 策略的蠕虫节点明显。

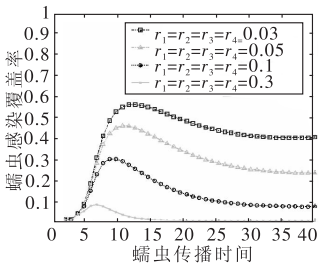


图4 PRS模型中节点的免疫等级对蠕虫传播的影响

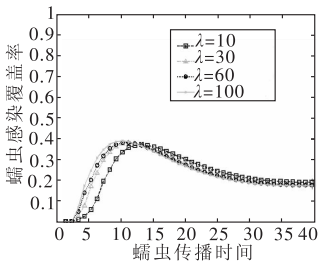


图5 HLS模型中蠕虫节点扫描率对蠕虫传播的影响

图 6 显示了 HLS 模型中在线节点的离线率对主动蠕虫传播的影响。如图 6 所示,在线节点的离线率越高,其达到的感染覆盖率越低;在蠕虫传播的中后期,由于蠕虫传播所引发的感染覆盖率会由早期的峰值下降到一个平衡点。

从图 3 和 6 中可以看出,PRS 模型中在线节点的离线率对主动蠕虫传播的影响比在 HLS 模型中的大得多,其根本原因在于 HLS 模型中,主动蠕虫是从 Hit-list 列表中选择攻击目标,在线节点的离线率越高,Hit-list 列表的有效期越短,主动蠕虫选中在线的有效攻击目标的可能性越小,所以在线节点的离线率越高,采用 HLS 策略的主动蠕虫传播所引发的蠕虫感染覆盖率越低。在蠕虫传播的初期,Hit-list 中大部分节点还没有离线,这为基于 HLS 策略的主动蠕虫提供了大量有效的攻击目标,蠕虫感染覆盖率也迅速上升,但当蠕虫感染覆盖率达到早期峰值后,Hit-list 中剩下的可供主动蠕虫选择的有效目标变得越来越少,使得蠕虫感染覆盖率也逐步降低,当一轮攻击中新增的已感染态节点与减少的已感染节点的数目相同时,蠕虫感染覆盖率就达到平衡点并持续保持。

图 7 显示了 HLS 模型中,在线节点的免疫等级对主动蠕虫传播的影响。其影响效果与 PRS 模型中的一致,在此不再赘述。

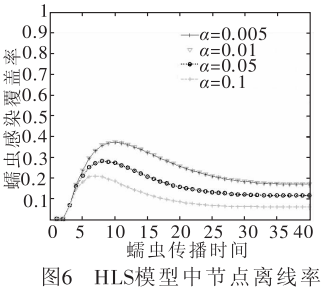


图6 HLS模型中节点离线率对蠕虫传播的影响

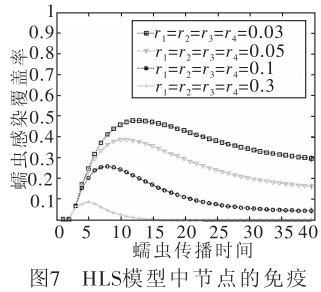


图7 HLS模型中节点的免疫等级对蠕虫传播的影响

综上所述,在动态环境下,通过限制 P2P 节点的扫描率,提高 P2P 节点的免疫等级以及在 HLS 模型中提高 P2P 节点的离线速度都能增强 P2P 网络对主动蠕虫的防御能力。

## 4 结束语

通过构造主动蠕虫传播模型,可以分析其在传播过程中的行为特征,找到影响主动蠕虫传播性能的关键因素,从而为主动蠕虫的检测与防御提供指导。本文结合真实的 P2P 网络中节点的众多动态特点,研究了动态环境下主动蠕虫常用的两种攻击策略,并根据上述策略建模了主动蠕虫的攻击模型,最后借助 MATLAB 软件对模型的参数进行数值分析,推导出影响主动蠕虫传播效率的关键参数。

在今后的工作中,将进一步研究如何提高动态环境下的蠕虫检测率,如何构建一个综合、有效的蠕虫防御体系。

**参考文献:**


[1] HONG Wei-ming. A novel method for P2P traffic identification[J]. Procedia Engineering,2011,23(1):204-209.

[2] CHEN Ze-sheng, GAO Li-xin, KWIAT K. Modeling the spread of active worms[C]//Proc of IEEE INFOCOM. San Francisco: IEEE Press,2003:1890-1900.

[3] YU Wei, BOYER C, CHELLAPPAN S, *et al*. Peer-to-peer system-based active worm attacks: modeling and analysis[C]//Proc of IEEE International Conference on Communications. Berlin: Springer-Verlag, 2005:295-300.

[4] YU Wei. Analyzing the performance of Internet worm attack approaches[C]//Proc of the 13th International Conference on Computer Communications and Networks. Chicago: IEEE Press,2004:501-506.

[5] JIA Chun-fu, LIU Xin, HU Zhi-chao, *et al*. Defending P2P networks against malicious worms based on benign worms[C]//Advances in Electric and Electronics. Berlin: Springer-Verlag,2012:653-660.

[6] WANG Xue-song, ZHU Jing-lin, LIN Huai-zhong, *et al*. Modeling propagation of active P2P worm in chord network[J]. Advances in Intelligent and Soft Computing,2012,133(2012):389-396.

[7] RAVIKUMAR V, RAJANI M. Peer-to-peer networks for modeling Malware propagation[J]. International Journal of Advanced Research in Computer Science and Software Engineering, 2012, 2(2): 1-4.

[8] ZHANG Ye-jiang, LI Zhi-tang, HU Zheng-bing, *et al*. Evolutionary proactive P2P worm: propagation modeling and simulation[C]//Proc of the 2nd International Conference on Genetic and Evolutionary Computing. [S.l.]: IEEE Computer Society,2008:261-264.

[9] YANG Wei, CHANG Gui-ran, YAO Yu, *et al*. Stability analysis of P2P worm propagation model with dynamic quarantine defense[J]. Journal of Networks,2011,6(1):153-162.

[10] FENG Chao-sheng, QIN Zhi-guang, CUTHBET L, *et al*. Propagation model of active worms in P2P networks[C]//Proc of the 9th International Conference for Young Computer Scientists. 2008:1908-1912.

[11] LI Hua, QIN Zheng, PAN Xiao-hui, *et al*. Propagation model of non-scanning active worm in unstructured P2P network[C]//Proc of International Conference on Multimedia Information Networking and Security. 2009:378-381.

[12] JAFARABADI A, AAGOMI M A. An SIR model for the propagation of topology-aware active worms considering the join and leave of hosts [C]//Proc of the 7th Information Assurance and Security. 2011:204-209.

[13] KEPHART J O, WHITE S R. Measuring and modeling computer virus prevalence[C]//Proc of IEEE Symposium on Security and Privacy. [S.l.]: IEEE Press,1993:2-15.