

P2P 触发式主动型蠕虫传播建模

冯朝胜^{1,2}, 秦志光², 罗王平¹, 刘霞¹, 袁丁¹

(1. 四川师范大学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)

摘要: 对 P2P 触发式主动型蠕虫的攻击机制进行了研究, 发现该类蠕虫传播通常包括四个阶段: 信息收集, 攻击渗透、自我推进与干预激活. 基于对 P2P 触发式主动型蠕虫攻击机制的分析并运用流行病学理论提出了 P2P 触发式主动型蠕虫传播数学模型并基于该模型推导了蠕虫传播进入无蠕虫平衡状态的充分条件. 仿真实验验证了所提出传播模型的有效性.

关键词: P2P 网络; 触发激活; 主动型蠕虫; 建模; 仿真

中图分类号: TP393

文献标识码: A

文章编号: 0372-2112 (2016)07-1702-06

电子学报 URL: <http://www.ejournal.org.cn>

DOI: 10.3969/j.issn.0372-2112.2016.07.026

Modeling Artificial-Activation P2P Proactive Worm Propagation

FENG Chao-sheng^{1,2}, QIN Zhi-guang², LUO Wang-ping¹, LIU Xia¹, YUAN Ding¹

(1. Visual Computing & Virtual Reality Key Laboratory of Sichuan Province, 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)

Abstract: As a kind of proactive worms in the P2P network, the artificial-activation worm is studied in terms of attacking mechanism in this paper. The propagation procedure of this kind of worm consists of four stages: information collection, penetration, self propulsion and artificial activation. It is found that the worm is a kind of topology-awareness worms. Based on the analysis on the attacking mechanism of this kind of worms, the mathematical model of artificial-activation P2P proactive worm propagation is proposed. Further, the sufficient condition of worm propagation attaining the worm free equilibrium is deduced from the model in applying Epidemiology. Large scale simulation experiments validate this proposed model.

Key words: P2P networks; artificial activation; proactive worms; modeling; simulations

1 引言

P2P 网络中出现的蠕虫(简称为 P2P 蠕虫)对 P2P 网络的正常工作造成严重威胁,进而对整个 Internet 的安全构成威胁. 利用 P2P 网络的拓扑信息和正常的网络交互行为在 P2P 网络上传播的蠕虫就是 P2P 蠕虫. 根据攻击方式的不同, P2P 蠕虫可分成三类^[1]: 被动型蠕虫、激发型蠕虫和主动型蠕虫. 根据激活方式不同, P2P 主动型蠕虫可分为自启式和触发式两种. 自启式蠕虫将蠕虫代码传送到目标主机后立即就能将自己激活, 而触发式蠕虫在将蠕虫代码传送到目标主机后需要用户打开蠕虫文件才能将蠕虫激活. 该文对 P2P 触发式主动型蠕虫传播模型进行了研究.

2 相关研究

文献[2]指出, P2P 网络是同质网络, 该特点决定了它很适合蠕虫的传播. 文献[3]和文献[4]分别为“红色代码”蠕虫和电子邮件病毒构建了传播模型, 这两个模型较准确地预测了这些病毒的传播趋势和行为. 文献[5]利用流行病学理论分别构建 P2P 病毒模型和感染文件传播模型. 文献[1]认为 P2P 蠕虫为非扫描型蠕虫, 并对三类 P2P 蠕虫分别进行了仿真分析. 然而, 该文献并没有给出 P2P 蠕虫传播的数学模型. 文献[6]分别为 Chord、CAN、Pastry 这三种典型结构化对等网构建了 P2P 蠕虫传播模型, 揭示了覆盖网拓扑对蠕虫传播的影响. 2007 年, Li 等指出 P2P 系统会加快网络蠕虫在

收稿日期: 2014-12-09; 修回日期: 2015-08-28; 责任编辑: 李勇锋

基金项目: 国家自然科学基金(No. 61373163); 国家科技重大专项课题(No. 2011ZX03002-002-03); 国家科技支撑计划课题(No. 2014BAH11F01, No. 2014BAH11F02); 可视化计算与虚拟现实四川省重点实验室课题(No. PJ2012002); 四川省教育厅项目(No. 15ZB0042)

互联网上的传播^[7]. 2008 年, Yu 等研究了 P2P 网络对网络主动蠕虫传播的影响并构建了传播模型^[8], 分析表明 P2P 网络会大大加快主动蠕虫的传播速度, 其主要原因在于 P2P 网络的拓扑特性使得蠕虫无需扫描就能准确定位攻击目标. 文献[9]提出了被动型蠕虫在 Gnutella 网络上的传播模型. 文献[10]和文献[11]分别对 Contagion 蠕虫和拓扑蠕虫的传播情况进行了仿真分析. 2009 年, Toutonji 提出利用动态隔离策略和被动良性蠕虫来抑制网络蠕虫传播, 并给出了蠕虫的传播模型^[12], 研究针对的是攻击力很强的扫描型蠕虫. 2011 年, Yang 等提出了一种主动型 P2P 蠕虫的动态隔离策略并构建相应的传播模型^[13], 基于模型对蠕虫传播的稳定性进行了分析. 2013 年, Mojahedi 等在建模时考虑了网络拓扑、节点配置、反击措施、防御策略和感染时间这些因素, 提出了 P2P 主动拓扑蠕虫传播模型^[14]. Chen 等人基于三元逻辑矩阵提出了 P2P 主动蠕虫传播模型^[15]. 2014 年, Jafarabadi 等提出一个面向 P2P 主动式蠕虫的随机离散模型^[16], 该模型考虑了网络的动态性. Chen 等在提出被动型蠕虫传播模型^[17]时考虑了四个因素: 地址隐藏、配置差异、用户的上下线行为和下载持续时间. Yang 等提出了被动型蠕虫的静态传播模型和动态模型, 并提出抑制蠕虫传播的策略^[18]. 2015 年, 文献[19]提出了被动型蠕虫的传播模型, 该模型考虑了网络的动态性. 然而, 这些研究都针对的不是触发式主动型蠕虫.

3 P2P 触发式主动型蠕虫传播

P2P 触发式主动型蠕虫的传播步骤包括信息收集、攻击渗透、自我推进和触发激活四个阶段, 前三个步骤是主动型蠕虫攻击一般都会经历的步骤, 而最后一个步骤是触发式蠕虫才会经历的步骤. 一旦确定攻击目标, 蠕虫就会利用目标主机的漏洞发起攻击并在其上建立后门, 然后利用后门将蠕虫主体复制到目标主机. 这时, 目标主机进入到潜伏阶段. 当用户或其他进程打开伪装成正常文件的蠕虫代码文件时, 蠕虫就会被激活.

表 1 四种 P2P 蠕虫的比较

	漏洞	传播	激活	拓扑	伪装	攻击力	隐蔽性
①	要	渗透	人工	是	是	较强	较强
②	要	渗透	自动	是	否	强	弱
③	要	上传/下载	自动	否	否	较强	较强
④	不	下载	人工	否	是	弱	强

注: ①触发式主动型蠕虫 ②自启式主动型蠕虫
③激发型蠕虫 ④被动型蠕虫

触发式主动型蠕虫和自启式主动型蠕虫、激发型蠕虫以及被动型蠕虫看起来都有些相似, 但事实上有很大区别. 为了将这四种蠕虫区别开来, 从是否需要漏

洞、传播方式、激活方式、是否为拓扑蠕虫、是否会伪装为正常文件、攻击力和隐蔽性 7 个方面进行了对比, 如表 1 所示.

4 触发式主动型蠕虫传播建模

4.1 建模参数

在该文中, P2P 节点指安装有 P2P 客户端软件的主机. 根据节点是否连接到 P2P 网络中, 节点分为两种: 在线节点和离线节点. 在线节点指通过启动 P2P 客户端加入到 P2P 网络中的节点, 离线节点指没有启动 P2P 客户端软件(但操作系统已经启动)或没有连接到 P2P 网络中的节点. P2P 节点的状态根据感染情况分成三种: 健康的, 潜伏的和感染的.

- 健康节点: 尚未被感染但存在被感染可能的节点;
- 潜伏节点: 存在蠕虫但蠕虫尚未激活的节点;
- 感染节点: 存在蠕虫且蠕虫已被激活的节点.

表 2 列举了建模时要用到的参数和变量.

表 2 建模时用到的变量和参数

符号	说明	默认值
N	在线的和离线的 P2P 节点总数	2000
$S_{on}(t)$	t 时刻在线健康节点数	999
$S_{off}(t)$	t 时刻离线健康节点数	1000
$L_{on}(t)$	t 时刻在线潜伏节点数	0
$L_{off}(t)$	t 时刻离线潜伏节点数	0
$I_{on}(t)$	t 时刻在线感染节点数	1
$I_{off}(t)$	t 时刻离线感染节点数	0
s	蠕虫攻击力即单位时间蠕虫攻击节点的数量	1
p_r	恢复率	0.00001
p_{on}	上线率	0.003
p_{off}	下线率	0.003
p_h	潜伏节点激活率	0.001
p_s	攻击成功率	1

4.2 传播数学模型

建模基于平均场法. t 时刻在线感染节点有 $I_{on}(t)$ 个, 每个节点发起的有效攻击次数为 sp_s . 特别需要说明的是, 当攻击力大于节点的平均邻居数, 攻击力就等于平均邻居数. 所有的在线节点发起的总的有效攻击次数为 $sp_s I_{on}(t)$. 平均地看, 一次攻击击中任意一个节点的概率为 $\frac{1}{S_{on}(t) + L_{on}(t) + I_{on}(t)}$, 一个节点不被一次有效攻击击中的概率为 $1 - \frac{1}{S_{on}(t) + L_{on}(t) + I_{on}(t)}$. 对于任意一个健康节点, t 时刻发起的 $sp_s I_{on}(t)$ 次有效攻击中一次也不会击中该节点的概率为 $(1 - \frac{1}{S_{on}(t) + L_{on}(t) + I_{on}(t)})^{sp_s I_{on}(t)}$, 至少击中一次概率为 $(1 - (1 - \frac{1}{S_{on}(t) + L_{on}(t) + I_{on}(t)})^{sp_s I_{on}(t)})$. 因而, 由健康状

态转变为潜伏状态的节点数为 $S_{on}(t) \left(1 - \left(1 - \frac{1}{S_{on}(t) + L_{on}(t) + I_{on}(t)} \right)^{sp_s I_{on}(t)} \right)$. 与此同时, 有 $p_r I_{on}(t)$ 个节点由感染状态恢复为健康状态. 单位时间内上线节点数为 $p_{on} S_{off}(t)$, 而下线节点数为 $p_{off} S_{on}(t)$. 因此, 在线健康的 P2P 节点的变化率为:

$$\frac{dS_{on}(t)}{dt} = -S_{on}(t) \left(1 - \left(1 - \frac{1}{S_{on}(t) + L_{on}(t) + I_{on}(t)} \right)^{sp_s I_{on}(t)} \right) + p_r I_{on}(t) + p_{on} S_{off}(t) - p_{off} S_{on}(t)$$

类似地, 可得到离线健康节点、在线潜伏节点、离线潜伏节点、在线感染节点和离线感染节点的变化率. 故触发式主动型 P2P 蠕虫传播模型为:

$$\frac{dS_{on}(t)}{dt} = -S_{on}(t) \left(1 - \left(1 - \frac{1}{S_{on}(t) + L_{on}(t) + I_{on}(t)} \right)^{sp_s I_{on}(t)} \right) + p_r I_{on}(t) + p_{on} S_{off}(t) - p_{off} S_{on}(t) \quad (1)$$

$$\frac{dS_{off}(t)}{dt} = p_r I_{off}(t) - p_{on} S_{off}(t) + p_{off} S_{on}(t) \quad (2)$$

$$\frac{dL_{on}(t)}{dt} = S_{on}(t) \left(1 - \left(1 - \frac{1}{S_{on}(t) + L_{on}(t) + I_{on}(t)} \right)^{sp_s I_{on}(t)} \right) - p_h L_{on}(t) + p_{on} L_{off}(t) - p_{off} L_{on}(t) \quad (3)$$

$$\frac{dL_{off}(t)}{dt} = -p_h L_{off}(t) - p_{on} L_{off}(t) + p_{off} L_{on}(t) \quad (4)$$

$$\frac{dI_{on}(t)}{dt} = p_h L_{on}(t) - p_r I_{on}(t) + p_{on} I_{off}(t) - p_{off} I_{on}(t) \quad (5)$$

$$\frac{dI_{off}(t)}{dt} = p_h L_{off}(t) - p_r I_{off}(t) - p_{on} I_{off}(t) + p_{off} I_{on}(t) \quad (6)$$

$$N = S_{on}(t) + L_{on}(t) + I_{on}(t) + S_{off}(t) + L_{off}(t) + I_{off}(t) \quad (7)$$

5 无蠕虫平衡状态充分条件

定理 当条件

$$\frac{sp_s [(p_r + p_{on})(p_h + p_{on}) + p_{on} p_{off}]}{(p_h + p_{on} + p_{off}) [p_r^2 + (p_{on} + p_{off}) p_r]} < 1$$

成立时, 触发式蠕虫传播将进入无蠕虫平衡状态.

证明 蠕虫是否能够在网络中流行是由蠕虫的基本繁殖率 R_0 来决定的^[20], 而求基本繁殖率的一种较为简单的方法^[21,22]是: 将个体状态转移流分成新感染个体进入流 f 和其他流 v , 分别求这两个向量对各个状态变量的微分:

$$F = \left[\frac{\partial f_i}{\partial x_j}(x_0) \right], \quad V = \left[\frac{\partial v_i}{\partial x_j}(x_0) \right], \quad 1 \leq i, j \leq m$$

其中 f_i 和 v_i 分别是 f 和 v 的第 i 个分量, x_i 是第 i 个状态变量并且 $\dot{x}_i = f_i(x) - v_i(x)$, m 表示感染状态变量个数. 矩阵 FV^{-1} 的最大绝对特征值就是所要求的基本繁殖率. 触发式蠕虫传播状态分别为 L_{on} 、 L_{off} 、 I_{on} 和 I_{off} . 故 $m=4$, 于是

$$f = \left[S_{on}(t) \left(1 - \left(1 - \frac{1}{S_{on}(t) + L_{on}(t) + I_{on}(t)} \right)^{sp_s I_{on}(t)} \right) \right]$$

$$v = \begin{bmatrix} p_h L_{on}(t) - p_{on} L_{off}(t) + p_{off} L_{on}(t) \\ p_h L_{off}(t) + p_{on} L_{off}(t) - p_{off} L_{on}(t) \\ -p_h L_{on}(t) + p_r I_{on}(t) - p_{on} I_{off}(t) + p_{off} I_{on}(t) \\ -p_h L_{off}(t) + p_r I_{off}(t) + p_{on} I_{off}(t) - p_{off} I_{on}(t) \end{bmatrix}$$

在无蠕虫平衡状态有:

$$\frac{dS_{on}}{dt} = \frac{dL_{on}}{dt} = \frac{dI_{on}}{dt} = \frac{dS_{off}}{dt} = \frac{dL_{off}}{dt} = \frac{dI_{off}}{dt} = 0$$

$$L_{on} = L_{off} = I_{on} = I_{off} = 0$$

$$\tilde{S}_{on} = \frac{p_{on} N}{p_{on} + p_{off}}, \quad \tilde{S}_{off} = \frac{p_{off} N}{p_{on} + p_{off}}$$

$$\therefore \left(1 - \frac{1}{S_{on}(t) + L_{on}(t) + I_{on}(t)} \right)^{sp_s I_{on}(t)}$$

$$= 1 - \frac{sp_s I_{on}(t)}{S_{on}(t) + L_{on}(t) + I_{on}(t)} + \dots$$

$$\approx 1 - \frac{sp_s I_{on}(t)}{S_{on}(t) + L_{on}(t) + I_{on}(t)}$$

$$\therefore 1 - \left(1 - \frac{1}{S_{on}(t) + L_{on}(t) + I_{on}(t)} \right)^{sp_s I_{on}(t)}$$

$$\approx \frac{sp_s I_{on}(t)}{S_{on}(t) + L_{on}(t) + I_{on}(t)}$$

$$d \left(1 - \left(1 - \frac{1}{S_{on}(t) + L_{on}(t) + I_{on}(t)} \right)^{sp_s I_{on}(t)} \right) / d(I_{on}(t))$$

$$\approx - \frac{d \left(\frac{sp_s I_{on}(t)}{S_{on}(t) + L_{on}(t) + I_{on}(t)} \right)}{d(I_{on}(t))}$$

$$\approx \frac{sp_s (S_{on}(t) + L_{on}(t) + I_{on}(t)) - sp_s I_{on}(t)}{(S_{on}(t) + L_{on}(t) + I_{on}(t))^2}$$

$$\approx \frac{sp_s (S_{on}(t) + L_{on}(t))}{(S_{on}(t) + L_{on}(t) + I_{on}(t))^2}$$

用 L_{on} 、 L_{off} 、 $I_{on}(t)$ 和 $I_{off}(t)$ 分别微分 f 和 v , 在平衡点 $\{\tilde{S}_{on}, 0, 0, \tilde{S}_{off}, 0, 0\}$ 有

$$F = \begin{bmatrix} 0 & 0 & sp_s & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$V = \begin{bmatrix} p_h + p_{off} & -p_{on} & 0 & 0 \\ -p_{off} & p_h + p_{on} & 0 & 0 \\ -p_h & 0 & p_r + p_{off} & -p_{on} \\ 0 & -p_h & -p_{off} & p_r + p_{on} \end{bmatrix}$$

$$R_0 = \rho(FV^{-1})$$

$$= \frac{sp_s [(p_r + p_{on})(p_h + p_{on}) + p_{on} p_{off}]}{(p_h + p_{on} + p_{off}) [p_r^2 + (p_{on} + p_{off}) p_r]}$$

由文献[20]知,当 $R_0 < 1$ 时触发式主动型蠕虫传播进入无蠕虫平衡状态.

6 仿真实验

6.1 P2P 网络仿真

仿真实验包括初始化阶段和仿真阶段. 根据文献[5], 文件共享对等网中对等机和文件的流行度都服从 Zipf 分布,所以在初始化阶段先按照 Zipf 分布给所有的文件分配文件名,继而根据 Zipf 分布将文件分配到对等节点上. 仿真程序会定期的输出实验结果. 仿真实验的结果被称作仿真结果;相应地,由数学模型得到的结果被称作理论结果,使用数字分析工具 Matlab 求解理论结果. 如无特别说明,所有实验的变量和参数取表 2 给出的默认值.

6.2 实验结果与分析

图 1 ~ 10 中 T 代表理论值,而 S 代表仿真值. 图 1 ~ 4 表明,对触发式主动型蠕虫传播影响最大的是激活率,而不是攻击力,这一点和直觉并不一致. 已有研究和经验都表明,攻击力是影响蠕虫传播速度最重要因素之一,但这里的蠕虫是指自激活式主动型蠕虫,该类蠕虫传播并不需要人工触发. 对于需要人工触发的蠕虫而言,无论攻击力有多强,即使所有的邻居节点都变成了潜伏状态,如果没有人工触发,处于潜伏状态的节点永远都不具有攻击感染能力. 另外,当蠕虫攻击力接近或超过平均邻居节点数时,蠕虫攻击进入饱和状态. 此时,增加攻击力不会提高蠕虫的传播速度. 因此,激活率对该类蠕虫的传播有着举足轻重的影响. 在蠕虫传播进入平衡状态之前,激活率越高,蠕虫传播越快,图 1 ~ 2 充分说明了这一点. 蠕虫激活率通常由蠕虫文件的伪装性和用户的反病毒知识决定. 蠕虫文件伪装的越像正常文件,用户打开该文件的可能性越大,蠕虫被激活的概率越高. 用户的反病毒知识越多,反病毒意识越强,打开来路不明的蠕虫文件的可能性就越小,蠕虫被激活的概率就越低. 当然,用户反病毒知识越多,清除蠕虫能力越强,感染节点的恢复率就越大,蠕虫的传播就会受到一定抑制. 正如图 5 ~ 6 表明的那样,这种抑制力非常有限. 图 7 ~ 10 表明,上线率和下线率对蠕虫传播有

一定的影响. 上线率越高,下线率越高,蠕虫传播的越快. 这一点容易理解,在线的感染节点才具有攻击力,在线的健康节点才可能被在线的感染节点攻击. 上线率越高,下线率越低,健康节点暴露在感染环境的时间就越长,更容易被攻击和感染.

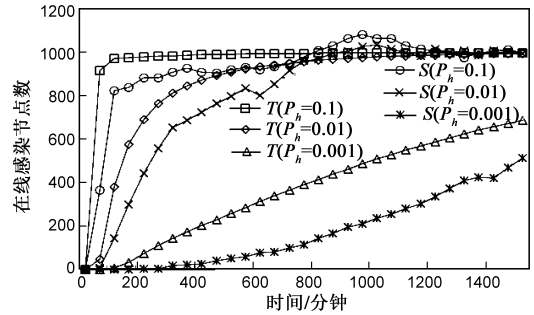


图2 蠕虫激活率对在线感染节点数的影响

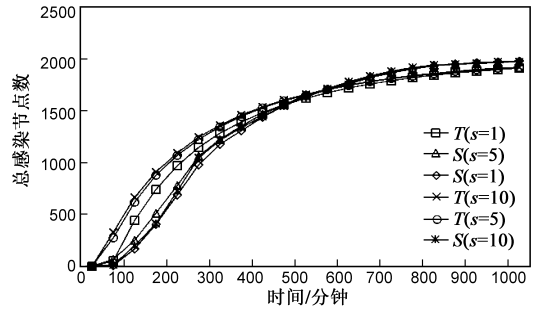


图3 攻击力对总感染节点数的影响

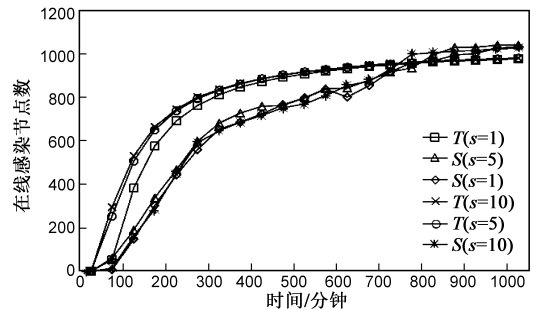


图4 攻击力对在线感染节点数的影响

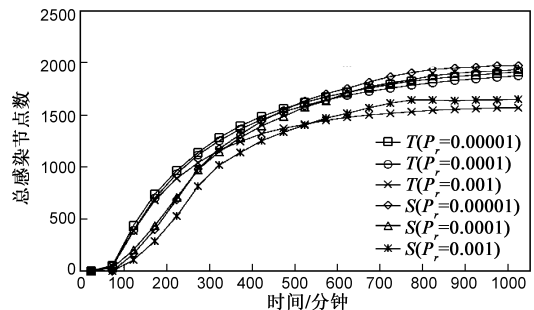


图5 恢复率对总感染节点数的影响

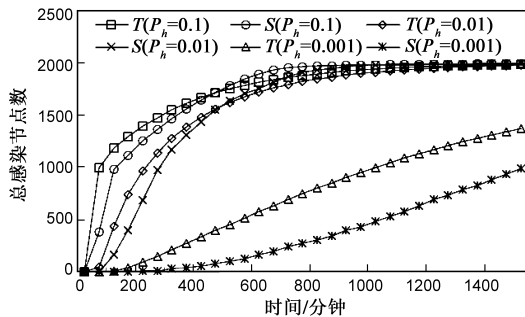


图1 蠕虫激活率对总感染节点数的影响

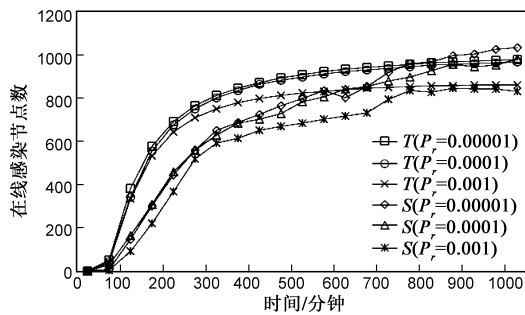


图6 恢复率对在线感染节点数的影响

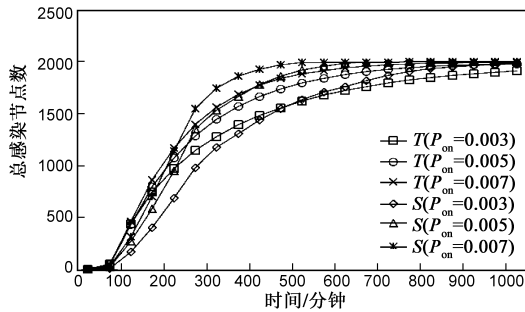


图7 上线率对总感染节点数的影响

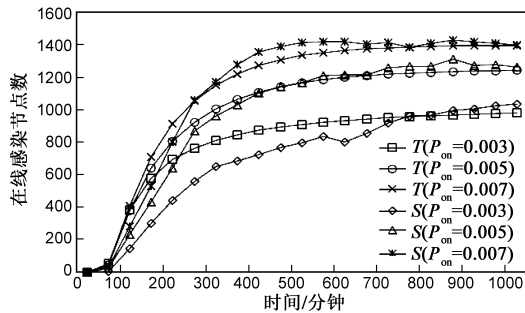


图8 上线率对在线感染节点数的影响

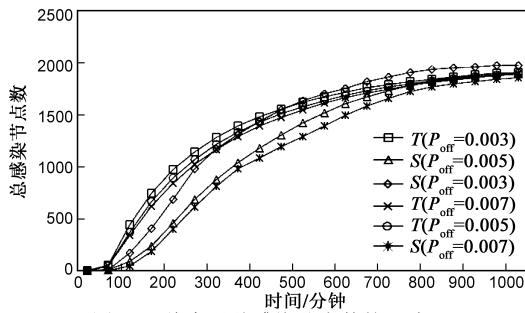


图9 下线率对总感染节点数的影响

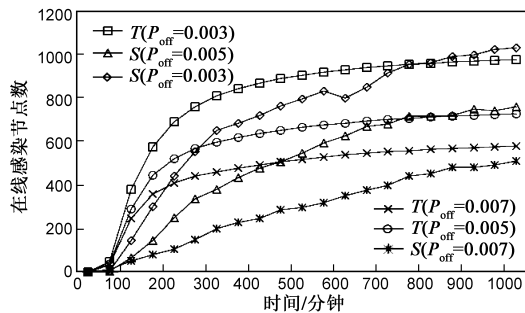


图10 下线率对在线感染节点数的影响

7 结束语

基于对触发式主动型蠕虫的攻击特点和传播机制的深入分析,运用流行病学理论,提出了 P2P 触发式主动型蠕虫传播的数学模型并基于该模型推导出蠕虫进入无蠕虫平衡状态的充分条件. 根据 P2P 蠕虫攻击机制,在 P2P 仿真网络中进行了蠕虫传播实验. 仿真实验验证了蠕虫传播模型的有效性. 未来工作的重点是提出 P2P 触发式主动型蠕虫的控制方法.

参考文献

- [1] Chen G, Gray R S. Simulating non-scanning worms on peer-to-peer networks [A]. Proceedings of the 1st International Conference on Scalable Information Systems [C]. Hong Kong: ACM, 2006. 29 - 41.
- [2] Staniford S, Paxson V, Weaver N. How to own the internet in your spare time [A]. Proceedings of the 11th USENIX Security Symposium [C]. San Francisco: ACM, 2002. 149 - 167.
- [3] Zou C C, Gong W, Towsley D. Code red worm propagation modeling and analysis [A]. Proceedings of ACM Conference on Computer and Communication Security (CCS'02) [C]. Washington: ACM, 2002. 138 - 147.
- [4] Zou C C, Towsley D, Gong W. Email worm modeling and defense [A]. Proceedings of the 13th International Conference on Computer Communications and Networks [C]. Chicago IL: IEEE, 2004. 409 - 414.
- [5] 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.
- [6] 夏春和, 石响平, 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 models of P2P worms in structured peer-to-peer networks [J]. Chinese Journal of Computers, 2006, 29(7): 952 - 959. (in Chinese)
- [7] Li T, Guan Z, Wu X. Modeling and analyzing the spread of active worms based on P2P systems [J]. Computer & Security, 2007, 26(3): 213 - 218.
- [8] Yu W, Chellappan S, Wan X, et al. Peer-to-peer system-based active worm attacks: Modeling, analysis and defense [J]. Computer Communications, 2008, 31(17): 4005 - 4017.
- [9] 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)
- [10] 王跃武,荆继武,向继,等. Contagion 蠕虫传播仿真分析[J]. 计算机研究与发展,2008,45(2):207-216.
Wang Yue-wu, Jing Ji-wu, Xiang Ji, et al. Contagion worm propagation simulation and analysis[J]. Journal of Computer Research and Development, 2008, 45(2):207-216. (in Chinese)
- [11] 王跃武,荆继武,向继,等. 拓扑相关蠕虫仿真分析[J]. 软件学报,2008,19(6):1508-1518.
Wang Yue-wu, Jing Ji-wu, Xiang Ji, et al. Topology aware worm simulation and analysis[J]. Journal of Software, 2008, 19(6):1508-1518. (in Chinese)
- [12] Toutonji O, Yoo S. Passive Benign worm propagation modeling with dynamic quarantine defense[J]. KSII Transactions On Internet and Information Systems, 2009, 3(1):96-107.
- [13] Yang W, Chang G, Yang Y, et al. Stability analysis of P2P Worm propagation model with dynamic quarantine defense[J]. Journal of Networks, 2011, 6(1):152-162.
- [14] Mojahedi E, Abdollahi Azgomi M. Modeling the propagation of topology-aware P2P worms considering temporal parameters[J]. Peer-to-Peer Networking and Applications, 2015, 8(1):171-180.
- [15] Chen T, Zhang X, Li H, et al. Propagation modeling of active P2P worms based on ternary matrix[J]. Journal of Network and Computer Applications, 2013, 36(5):1387-1394.
- [16] Jafarabadi A, Abdollahi Azgomi M. A stochastic epidemiological model for the propagation of active worms considering the dynamicity of network topology[J]. Peer-to-Peer Networking and Applications, 2015, 8(6):1008-1022.
- [17] Chen T, Zhang X, Wu Y. FPM: Four-factors propagation model for passive P2P worms[J]. Future Generation Computer Systems, 2014, 36(7):133-141.
- [18] Yang W, Gao Y, Zhu Z, et al. Modelling, analysis and containment of passive worms in P2P networks[J]. International Journal of Internet Protocol Technology, 2014, 8(2-3):130-142.
- [19] Feng C, Yang J, Qin Z, et al. Modeling and analysis of passive worm propagation in the P2P file-sharing network[J]. Simulation Modelling Practice and Theory, 2015, 51(2):87-99.
- [20] Diekmann O, Heesterbeek J A P. Mathematical Epidemiology of Infectious Diseases: Model Building, Analysis and Interpretation[M]. Wiley, 1999.
- [21] Driessche P, Watmough J. Reproduction numbers and sub-threshold endemic equilibria for compartmental models of disease transmission[J]. Mathematical Biosciences, 2002, 180:29-48.
- [22] Arnio J, Davis J, Hartley D, et al. A multi-species epidemic model with spatial dynamics[J]. Mathematical Medicine and Biology, 2005, 22(2):129-142.

作者简介



冯朝胜 男, 1971 年生于四川广元, 博士后, 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. 研究方向包括对等网络安全、恶意代码分析与防御、云计算安全等.
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.

罗王平 男, 1993 年生于四川南充, 本科生, 四川师范大学计算机科学学院学生. 研究方向为云计算与隐私保护.

刘霞 女, 1978 年生于四川都江堰, 硕士, 四川师范大学计算机科学学院讲师. 2004 年获得西南交通大学计算机应用专业硕士学位. 研究方向为网络安全.

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.