BitTorrent网络中的P2P蠕虫传播仿真分析

吴春江，周世杰，肖春静，吴 跃

(电子科技大学计算机科学与工程学院 成都 610054)

【摘要】对等网络蠕虫(简称P2P蠕虫)是目前P2P网络面临的重大安全威胁之一。由于具有极强的隐蔽性和破坏性，P2P蠕虫能够控制访问感染节点的路由表，获取该节点的邻居信息，构建攻击列表，以实现精确的目标攻击。该文通过仿真的方法，分析了P2P蠕虫在BitTorrent网络中的传播特性，验证了相关参数对P2P蠕虫传播的影响。实验结果表明，P2P蠕虫的传播与BT网络的状态、蠕虫的攻击能力、初始感染蠕虫节点比例以及单位时间内免疫节点比例有着非常紧密的联系。

关 键 词 BitTorrent; 对等网络; 仿真; 蠕虫
中图分类号 TP393.08 文献标识码 A

Simulation of Epidemic of P2P Worms in BitTorrent Networks

WU Chun-jiang，ZHOU Shi-jie，XIAO Chun-jing，WU Yue

(School of Computer Science and Engineering, University of Eletronic Science and Technology of China Chengdu 610054)

Abstract Peer-to-Peer (P2P) worms have become one of some major threats to peer-to-peer network security nowadays. With its strong hidden feature and destructivity, the P2P worms can attack the goal nodes accurately by manipulating the router table of infected nodes, getting information of their neighbors and constructing a target list. Through some simulation experiments, this paper analyzes the characteristic of P2P worms spreading through BitTorrent network, and tests the effect of some parameters. The performances of simulation experiments show that the spread of P2P worms is related to the state of BT network, the attack capacity of worms, the rate of initial infected node, and immune node per unit time.

Key words BitTorrent; peer-to-peer; simulation; worm

对等计算(Peer-to-Peer，P2P)是信息技术领域的热点问题。P2P网络是基于互联网而发展起来的，互联网的最大安全威胁来自于恶意代码的传播。而在恶意代码中，又以网络蠕虫对计算机系统安全和网络安全的威胁为最。因此，随着P2P技术的发展，P2P网络的安全问题也越来越受到重视。

2005年P2P蠕虫[1]概念被正式提出。根据P2P蠕虫的传播策略，可以将P2P蠕虫分为两类：第一类是基于社会工程学，将蠕虫代码伪装后提供下载传播，最早出现的是VBS. Gnutella蠕虫[2]。目前，这一类蠕虫已有不下数十种，但由于该类蠕虫在伪装时很难保证将文件名更名为近期比较热门的资源，因此在P2P网络上的传播并不是很广。第二类是基于P2P软件的漏洞，利用对等网络拓扑及其交互性质自主传播。该类蠕虫可以利用P2P节点主机缓存列表(Host Cache)中的邻居节点来构建攻击列表，以实现准确的目标定位，因此，它具有更强的隐蔽性和破坏性，是P2P网络安全问题的重点研究对象。

目前，P2P网络的应用已经涉及到资源搜索、文件传输、IP电话、流媒体等领域，成为互联网中的主要流量之一。而在文件传输应用中，又以BitTorront协议(简称BT协议)[3]应用最为广泛。因此，研究分析P2P蠕虫在BT网络中的传播特性，构建BT网络中P2P蠕虫的传播模型，对于BT网络中P2P蠕虫的检测和抑制有着非常重要的意义。本文对BitTorrent网络中的P2P蠕虫传播进行了仿真分析。

1 相关研究工作

文献[4]指出P2P网络具有非常适合蠕虫传播的特性；文献[5]进行了利用漏洞感染P2P网络中逻辑邻居的蠕虫传播仿真实验，揭示了P2P蠕虫的主动攻击性和强大的感染能力。

对于P2P蠕虫传播模型的建立与分析，文献[6]提出了利用传统计算机病毒传播模型来研究P2P蠕虫传播的方法；文献[7]对非扫描型P2P蠕虫进行了仿真分析；文献[8]又对各种扫描策略下P2P蠕虫的

收稿日期：2005 – 09 – 07
基金项目：国家自然科学基金(60473090)；国家242信息安全专题计划(2006B19)
作者简介：吴春江(1982 –)，男，硕士生，主要从事P2P仿真方面的研究.

传播性能进行了仿真分析；文献[9]利用数字模拟的方法分析了P2P系统参数对被动式P2P蠕虫传播的影响；文献[10]提出了主动式P2P蠕虫的传播模型及Matlab仿真分析的方法；文献[11]基于结构化对等网路由表构造方法，建立了P2P蠕虫在Chord、CAN、Pastry三种典型结构化对等网中的传播模型，给出刻画P2P蠕虫传播能力的函数，并揭示了覆盖网拓扑对蠕虫传播的负面影响。

对于P2P蠕虫的检测与抑制，文献[12-14]提出了利用P2P网络的特性来防治P2P蠕虫的方法；文献[15]提出了利用P2P软件多样性进行P2P蠕虫防治的模型和方法；文献[16]利用流量分类和应用识别的方法来检测和防治P2P蠕虫的方法，改进了干扰流量的识别和过滤规则，提出了P2P蠕虫检测规则，并引进博弈论的研究方法讨论了检测周期的选取问题；文献[17]提出了一种用于恶意代码防治的激励机制，可以激励网络中的用户提高自身节点对恶意代码的防范能力；文献[18]也提出了一种基于恶意代码行为特征的恶意代码识别方法，并利用这种识别方法制定了一个适合P2P文件共享系统的恶意代码防治策略来减缓、遏制恶意代码的传播；文献[19]运用图论的方法研究在网络节点具有相同度约束的情况下优化直径网络的构造方法以及路由问题，提出了一种简单有效的启发式路由算法，分析了其计算复杂度，设计了一个基于该算法的P2P蠕虫防御系统。

2　BT网络中P2P蠕虫传播仿真实验

2.1　仿真环境及实验假设

由于BT网络规模大、动态性强，在真实的BT网络环境中进行P2P蠕虫传播研究具有很大的困难，必须借助一定的仿真工具。本文采用peersim仿真工具进行BitTorrent网络中P2P蠕虫传播仿真实验，peersim中的cycle作为P2P蠕虫传播的时间片。

为简化设计，充分体现各参数对BT网络中P2P蠕虫传播的影响，假设：(1) 蠕虫攻击某节点成功后，具有对该节点路由表的访问权力。(2) 蠕虫完成从一个节点到另一个节点的感染过程所需的平均时间为 Δt。(3) 在蠕虫传播的短时间内对BT网络中的节点没有搅动行为。(4) 被感染节点对邻居节点的传播几乎是同时的。(5) BT网络中在线的节点充分多。

2.2　实验参数

BT网络中P2P蠕虫传播仿真实验所涉及到的参数及含义如表1所示。

表1　仿真参数及含义

参　数	含　义
N	网络规模
neighbor_max	最大邻居节点数
neighbor_min	最小邻居节点数
connect_max	最大TCP连接数
connect_min	最小TCP连接数
numwant	节点向tracker服务器请求邻居节点数
N_t	第t个单位时间时节点总数
N_{new}^t	第t个单位时间内新加入的节点数
K_{w}	感染蠕虫节点比例
N_{w}	感染蠕虫节点数
K_{i}	免疫节点比例
N_i	免疫节点数
K_{w}^t	第t个单位时间内感染蠕虫节点比例
N_{w}^t	第t个单位时间内感染蠕虫节点数
K_i^t	第t个单位时间内免疫节点比例
N_i^t	第t个单位时间内免疫节点数
C_{w}	蠕虫攻击能力

2.3　P2P蠕虫随BT网络构建传播实验

在P2P蠕虫随BT网络构建传播实验中，令 $N=1000$、$K_{\text{w}}^0=1\%$、$C_{\text{w}}=5$，同时定义单位时间内新增节点函数为 $f(t)$。改变 $f(t)$，观察P2P蠕虫随BT网络构建传播的变化规律。

2.3.1　单位时间内新增节点函数为常数

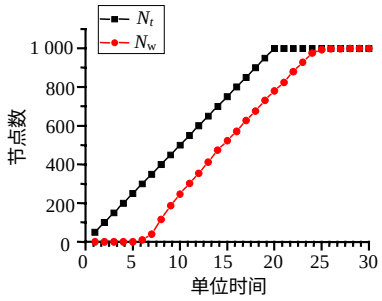

图1　网络节点数和感染蠕虫节点数变化图

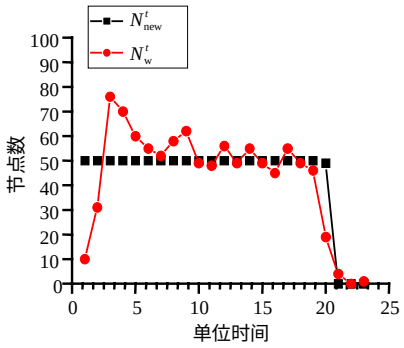

图2　单位时间内新增节点数和感染蠕虫节点数变化图

令 $f(t)=a$，$a=N\times 5\%$。图1是网络节点数 N_t 和感染蠕虫节点数 N_{w} 的变化图，图2是单位时间内新增节点数 N_{new}^t 和新增感染蠕虫节点数 N_{w}^t 的变化图。

2.3.2　单位时间内新增节点函数为线性函数

令 $f(t)=at$，$a=N\times 0.4\%$。N_t 和 N_{w} 的变化如

图3所示，N_{new}^{t} 和 N_{w}^{t} 的变化如图4所示。

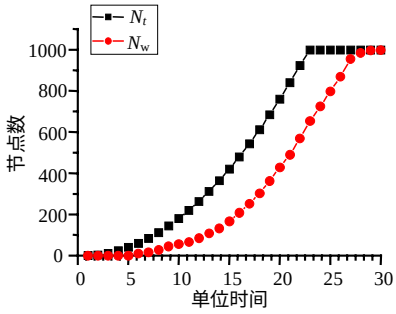

图3 网络节点数和感染蠕虫节点数变化图

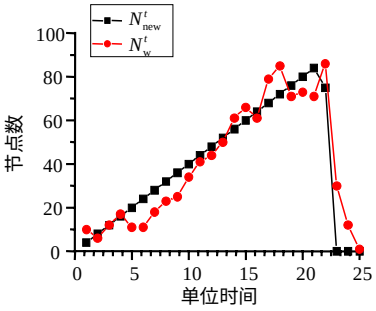

图4 单位时间内新增节点数和感染蠕虫节点数变化图

2.2.3 单位时间内新增节点函数为分段函数

令：

$$f(t)=\begin{cases} a+t\times a/10 & 1\le t\le 10 \\ 2a+(t-10)\times a/10 & 10<t\le 20 \\ a+(t-20)\times a/10 & t>20 \end{cases}$$

式中 $a=N\times 2\%$。N_t 和 N_{w} 的变化如图5所示，N_{new}^{t} 和 N_{w}^{t} 的变化如图6所示。

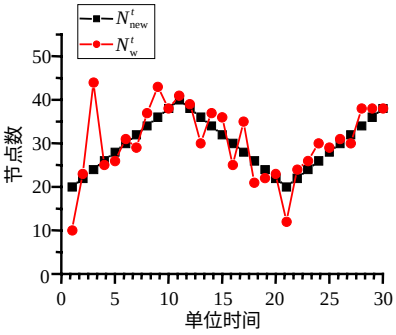

图5 网络节点数和感染蠕虫节点数变化图

从图1、图3和图5可以看出，感染蠕虫节点数的增长曲线与BT网络规模的增长曲线是一致的。并且，从图2、图4和图6可以看出，单位时间内新增节点数和新增感染蠕虫节点数的变化曲线也是一致的。其原因在于P2P蠕虫在BT网络中的传播速度是相当快的，会在短时间内感染BT网络中已有的节点。当有新节点加入时，新节点也会在短时间内被感染。因此，单位时间内新增感染蠕虫节点数的变趋势同新增节点数的变化趋势是一致的，从而感染蠕虫节点数的变化趋势与BT网络规模增长的趋势也是一致的。

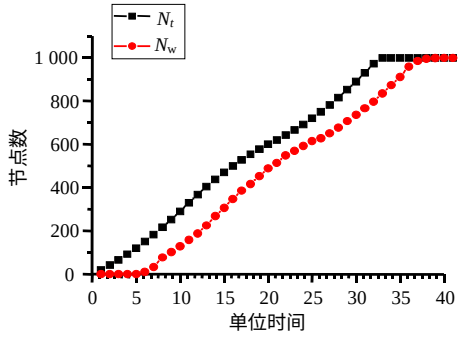

图6 单位时间内新增节点数和感染蠕虫节点数变化图

2.4 P2P蠕虫在稳定BT网络传播

同样采用2.3节中的参数设置以及三种不同的 $f(t)$ 函数表达式，进行P2P蠕虫在稳定BT网络中传播实验，观察 N_t 和 N_{w} 的变化趋势，其实验结果如表2所示。

表 2 P2P 蠕虫在稳定 BT 网络中传播实验

时间	$f(t)$为常数		$f(t)$为线性函数		$f(t)$为分段函数	
	N_{w}	K_{w}/(%)	N_{w}	K_{w}/(%)	N_{w}	K_{w}/(%)
1	10	1.00	10	1.00	10	1.00
2	56	5.61	57	5.71	57	5.71
3	260	26.03	257	25.73	265	26.53
4	611	61.16	611	61.16	605	60.56
5	855	85.59	869	86.99	871	87.19
6	968	96.90	968	96.90	965	96.60
7	995	99.60	989	99.00	991	99.20
8	998	99.90	997	99.80	998	99.90
9	999	100.00	999	100.00	999	100.00

从表2中可以看出，P2P蠕虫在稳定BT网络中的传播并不受节点增长方式的影响。同时，P2P蠕虫强大的攻击性使得短时间内就可以感染BT网络中的所有节点。

2.5 攻击能力对P2P蠕虫传播的影响

P2P蠕虫的攻击能力是指单位时间内攻击的邻居节点数。在本文实验中，令 $N=2\,000$、$K_{\text{w}}^{0}=1\%$，N_{new}^{t} 为0.05 N ～0.1 N 之间的一个随机数，修改 C_{w} 的值，观察 N_t 和 N_{w} 的变化趋势，实验结果如图7和图8所示。

从图7可以看出，在P2P蠕虫随BT网络构建传播的过程中，蠕虫的攻击能力对P2P蠕虫传播的影响并不大。这是因为P2P蠕虫强大的攻击性使得新增节点在短时间内被感染，网络中感染蠕虫节点数的变化受新增节点数变化的影响。

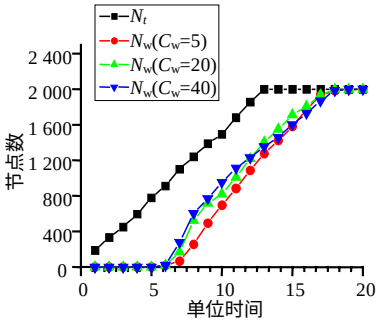

图 7　攻击能力对 P2P 蠕虫传播的影响(随 BT 网络构建)

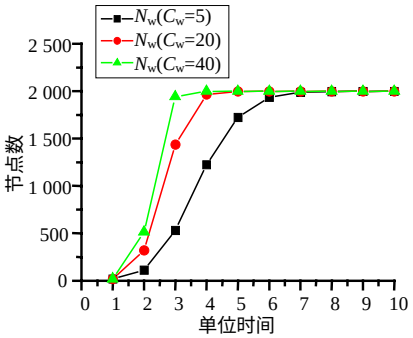

图8　攻击能力对P2P蠕虫传播影响(稳定BT网络)

从图8可以看出，在稳定的BT网络中，攻击能力强的P2P蠕虫明显比攻击能力弱的蠕虫具有更大的传染性，其原因在于攻击能力越强的P2P蠕虫在单位时间内攻击的邻居节点数越多。

2.6　初始感染蠕虫节点比例对**P2P**蠕虫传播的影响

实验中，令 $N=2\,000$、$C_w=5$、N_{new}^t 为0.05 N ～0.1 N 之间的一个随机数，修改 K_w^0 的值，观察 N_t 和 N_w 的变化趋势，实验结果如图9和图10所示。

从图 9 可以看出，在 P2P 蠕虫随 BT 网络构建传播的过程中，初始感染蠕虫节点比例对 P2P 蠕虫传播的影响并不大，原因同 2.5 节中分析的一样。

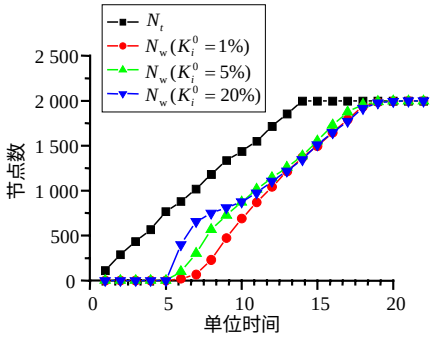

图 9　初始感染蠕虫节点对 P2P 蠕虫传播的影响
(随 BT 网络构建)

从图10可以看出，在稳定的BT网络中，初始感染蠕虫节点比例越高，其P2P蠕虫传播的速度越快，传染性越强。其原因在于初始感染蠕虫节点比例越高，其基数就越大，在相同的蠕虫攻击能力 C_w 下，单位时间内感染的节点数就越多。

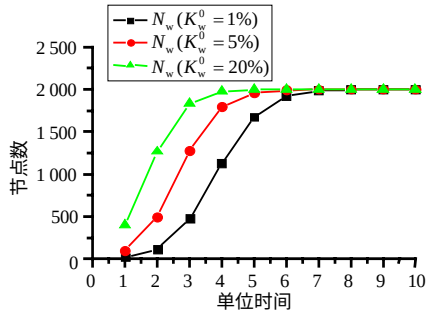

图10　初始感染蠕虫节点对P2P蠕虫传播的影响
(稳定BT网络)

2.7　初始免疫节点比例对**P2P**蠕虫传播影响

实验中，令 $N=2\,000$、$C_w=5$、$K_w^0=1\%$，N_{new}^t 为0.05 N ～0.1 N 间的随机数，修改 K_i^0 的值，观察 N_t 和 N_w 的变化趋势，实验结果如图11和图12所示。

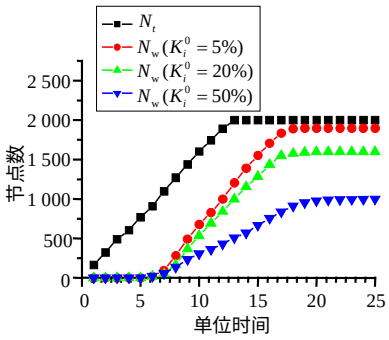

图11　初始免疫节点比例对P2P蠕虫传播的影响
(随BT网络构建)

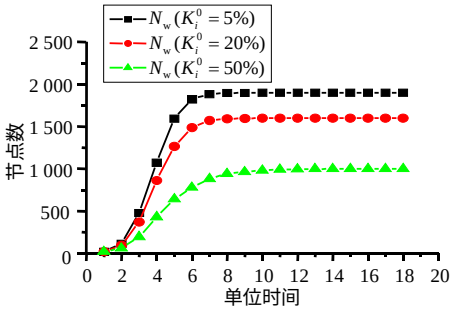

图12　初始免疫节点比例对P2P蠕虫传播的影响
(稳定BT网络)

从图11和图12可以看出，不管是P2P蠕虫随BT网络构建传播还是P2P蠕虫在稳定BT网络中传播，最终蠕虫都会感染所有未免疫的节点。虽然初始免疫节点比例越大，会对P2P蠕虫的传播有一定的延迟作用，但延迟时间并不长，所以初始免疫节点比例对P2P蠕虫的传播影响并不大。

2.8　单位时间内免疫节点比例对**P2P**蠕虫传播的影响

在实验中，令 $N=2\,000$、$C_w=5$、$K_w^0=1\%$，N_{new}^t 为0.05 N ～0.1 N 之间的一个随机数，修改 K_i^t 的值，观察 N_t 和 N_w 的变化趋势，实验结果如图13和图14所示。

从图13和图14可以看出，不管是P2P蠕虫随BT网络构建传播还是P2P蠕虫在稳定BT网络中传播，单位时间内免疫节点比例越大，对P2P蠕虫传播的抑制效果就越好。随着时间的推移，最终网络中将不再有P2P蠕虫的传播。

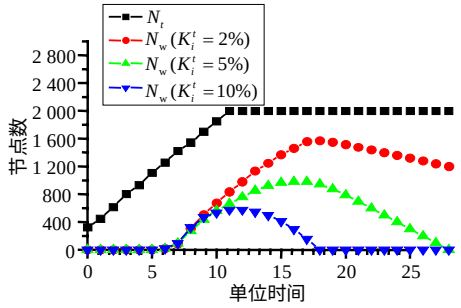

图13 单位时间内免疫节点对P2P蠕虫传播的影响
(随BT网络构建)

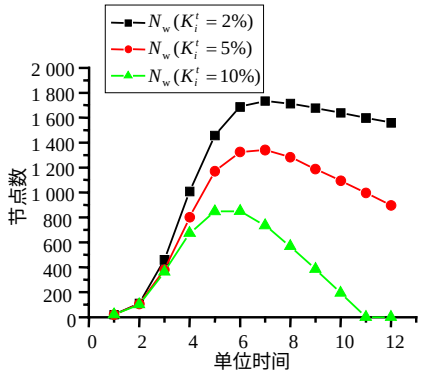

图14 单位时间内免疫节点对P2P蠕虫传播的影响
(稳定BT网络)

3 总 结

本文通过仿真实验的方法，分析研究了P2P蠕虫在BitTorrent网络中的传播特性，以及相关参数对P2P蠕虫传播的影响。实验结果表明，P2P蠕虫的传播与BT网络的状态、蠕虫的攻击能力、初始感染蠕虫节点比例以及单位时间内免疫节点比例有着非常紧密的联系。

参 考 文 献

[1] ZHOU Li-dong, ZHANG Lin-tao, MCSHEERY Frank. A first look at peer-to-peer worms threats and defenses[C]// IPTPS. New York: [s. n.], 2005.

[2] Symantec Inc. VBS Gnutella[EB/OL]. http:// securityresponse. Symantec.com/avcener/venc/data/vbs. gnutella.html, 2007-06-08.

[3] COHEN B. Bittorrent Protocol Specification v1.0[EB/OL]. http://www. bitconjurer.org/BitTorrent/protocol. html, 2007-03-10.

[4] STUART S, VERN P, NICHOLAS W. How to own the Internet in your spare time[C]//In proceedings of the 11th USENIX Security Symposium. San Francisco, CA: [s.n.], 2002.

[5] KANNAN J, LAKSHMINARAYANAN. K. Implications of peer-to-peer networks on worm attacks and defense. [C]// CS294-4-F03, California: EECS, 2003.

[6] YU Wei. Analyze the worm-based attack in large scale P2P networks[C]//Proceedings of the 8th IEEE International Symposium on High Assurance Systems Engineering. Tampa, Florida: IEEE, 2004: 308-309.

[7] CHEN Guan-ling, GRAY R S. Simulating non-scanning worms on peer-to-peer networks[C]//In Proceedings of the 1st International Conference on Scalable Information systems. Hong Kong, China: [s.n.], 2006.

[8] YU Wei. Analyzing the performance of internet worm attack approaches[C]//13th International Conference on Computer Communications and Networks. [S.l.]: [s.n.], 2004: 1095-2055.

[9] MA Jie, CHEN Xin-meng, XIANG Guang-li. Modeling passive worm propagation in peer-to-peer system[C]//In Proceedings of Computational Intelligence and Security : [S.l.]: IEEE, 2006: 1129-1132.

[10] GAO Chang-xi, ZHANG Fu-yuan, XIN Yang, et al. Research on worm's propagation and defense model in different P2P networks[J]. Journal of Beijing University of Posts and Telecommunications, 2006, (supple2): 49-53.

[11] XIA Chun-he, SHI Yun-ping, LI Xiao-jian. Research on epidemic models of P2P worm in structured peer-to-peer networks[J]. Chinese Journal of Computers, 2006, 29(6): 952-959.

[12] YU Wei, BOYER C, CHELLAPPAN S, et al. Peer-to-peer system-based active worm attacks: Modeling and analysis[C]//In Proc. of IEEE International Conference on Communications (ICC 2005). Seoul, Korea: IEEE, 2005: 295-300.

[13] YU Wei, CHELLAPPAN S, WANG Xun, et al. On defending peer-to-peer system-based active worm attacks[C]//In Proceedings of IEEE GLOBECOM 2005. [S.l.]: IEEE, 2005: 1757-1761.

[14] SHAKKOTTAI S, SRIKANT R. Peer to peer networks for defense against internet worms[C]//Proceedings From the 2006 Workshop on Interdisciplinary Systems Approach in Performance Evaluation and Design of Computer & Communications Systems. Pisa, Italy: [s.n.], 2006.

[15] ZHOU Ying, WU Zhong-fu, WANG Hao, et al. Breaking monocultures in P2P networks for worm prevetion[C]//In Proceedings of the Fifth International Conference on Machine Learning and Cybernetics. Dalian, China: [s.n.], 2006: 2793-2798.

[16] XIA Chun-he, SHI Yun-ping, LI Xiao-jian. P2P worm detection based on traffic classification and application identification[J]. Journal of Beijing University of Aeronautics and Astronautics, 2006, 32(8): 998-1002.

[17] 董健全, 谢承灏, 李 超. P2P文件共享系统中恶意代码防治的激励机制[J]. 计算机工程与应用, 2006, 42(34): 152-156.

[18] 谢承灏, 董健全. P2P文件共享系统中的恶意代码防治策略[J]. 计算机工程与应用, 2006, 42(34): 152-156.

[19] 丁 强, 徐 恪, 刘惠山. 优化直径网络构造与d分路由算法[J]. 小型微型计算机系统, 2006, 27(6): 1059-1063.

编 辑 漆 蓉