具有多区域选择性的网络蠕虫传播分析

张建峰 陈够喜 杨秋翔
(中北大学计算机与控制工程学院 太原 030051)

摘 要 当今蠕虫不仅注重快速传播,而且根据不同区域的特征能够实施选择性感染。首先,围绕这一特点,在AAWP离散模型的基础上,基于不同区域的漏洞分布概率,量化影响平均扫描率的若干因素,提出了一种多区域选择性蠕虫离散模型Areas-AAWP;其次,在该模型下,解析了多个子区域扫描策略之间的相关性,评判了整体区域中协同感染行为的相关度,并分析了该相关度对整体感染效率的影响;最后,通过实验证明,蠕虫的区域整体感染速率随多区域间扫描相关度的增大而上升,并随之形成明显的感染差异。

关键词 离散模型,Areas-AAWP模型,多区域选择性,扫描策略,相关性
中图法分类号 TP393.08 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.3.026

Understanding Spread of Worms with Multi-area and Selectivity

ZHANG Jian-feng CHEN Gou-xi YANG Qiu-xiang
(School of Computer and Control Engineering, North University of China, Taiyuan 030051, China)

Abstract Today worm not only spread more quicklying, but also can implement selective infection based on the different characteristics of the regions. Firstly, on the characteristic, quantifying certain factors of the average scan rate based on AAWP model by the probability distribution of the vulnerability of different regions, we raised a multi-area and selective worm propagation model named Areas-AAWP with discrete time. Then, under this model, we analyzed the correlation between the scanning strategies adopted by each subarea, judged the degree of relevance to the whole infectious process between subareas, and analyzed the important impact on the overall efficiency of infection by this degree of relevance. Finally, the experiments testify that the whole worm infection rate increases with the degree of correlation among multi-zone scanning increases, and forms the obvious regional differences in infection.

Keywords Discrete model, Areas-AAWP, Multi-area and selective, Scanning strategy, Correlation

1 引言

蠕虫传播注重攻击的快速性,还具有攻击的区域针对性。知名的Code-Red蠕虫[1]是一种在全球范围内迅速泛滥的网络蠕虫。而Conficker蠕虫[2]利用DNS及人为控制的方式实行了区域针对的选择性攻击。

蠕虫传播模型主要包括连续数学模型和离散数学模型。Kermack等人[3]提出的流行病三态模型(Kermack-Mckendrick,KM模型)广泛应用于蠕虫传播的研究。现实中蠕虫传播是不连续的,Chen等人[4]提出离散时间下的蠕虫传播模型(Analytical Active Worm Propagation,AAWP模型)。

Cliff C Zou等人[5]提出的路由蠕虫通过减小扫描范围来增加传播速率,并提出了利用IP分配地理信息进行区域针对性攻击的思想。Yubin Li等人[6]通过将一块区域进行随时间均分为2^t块小区域来深度解析蠕虫分治扫描过程,具有一定的区域划分思想。然而此类模型的本质都是对一个/n子网内外传播进行研究的,并不是从多个区域自身脆弱主机的分布特性来研究其传播特性。

Zesheng Chen等人[7]利用信号理论深度刻画了网络不均匀分布的特征及其对感染率的影响,并基于此解析了一种具有网络察觉并做出扫描优化的智能蠕虫传播模型。Bose A等人[8]针对新型蠕虫利用网络的幂率连通性来发起攻击的特点,主要考虑了子网合作性和用户在地理上的移动性对该恶意蠕虫传播的影响。Wagdarikar等人[9]针对脆弱节点分布,提出了一种优先扫描策略的传播模型。佟晓筠等人[10]分析了免疫率对蠕虫非线性传播的影响。上述模型仅注重考虑网络的不均匀性、免疫率和扫描策略优化对蠕虫在多个子网区域传播的影响,但是没有考虑蠕虫多区域传播的差异性,更没有从相关性角度解析扫描协同性对其传播的影响。

本文针对不同区域的脆弱节点分布特性,提出了一种具有区域选择性的蠕虫传播模型,利用相似矩阵理论对区域之间扫描策略协同性进行相关度判定,论证多个子区域间相关度与整体感染效率存在的关系。最后实验验证了:①扫描率的大小是导致选择性蠕虫形成区域感染差异性的重要因素;②扫描率相同时,一定数量的子区域间扫描相关度对整体的传播速率与危害程度有着重要影响。

2 Areas-AAWP模型的建立

蠕虫存在于网络节点之间,而全球网络根据IP分配与地

到稿日期:2014-04-16 返修日期:2014-07-18 本文受山西省科技攻关项目(20090322004),中北大学科学研究基金(2014)资助。
张建峰(1989-),男,硕士生,CCF会员,主要研究方向为信息安全、网络安全,E-mail:zjf49797@163.com;陈够喜(1966-),男,博士,副教授,主要研究方向为信息安全、信息隐藏;杨秋翔(1969-),男,硕士,教授,主要研究方向为信息安全、网络拓扑。

理信息等特征划分为多个区域。多区域蠕虫根据漏洞分布决定的脆弱主机分布特性来调节各区域的扫描率，得到所需的感染率，达到区域危害程度差别的感染针对性。其中，蠕虫的扫描率不仅影响其传播速率，也导致不同区域被同类蠕虫感染后危害程度存在差异性。

2.1 扫描率的分析

文献[11]指出蠕虫扫描率与带宽、DNS域名解析时间以及成功建立连接所需时间有关。扫描率主要与3个要素有关，分别是蠕虫自身扫描进程数 S_0、扫描间隔时间 $\tau(t)$、脆弱主机的分布 F。蠕虫自身的传播机制对 S_0 有决定性影响。$\tau(t)$决定单位时间内的每个扫描进程所发出的扫描数。$\tau(t)$的大小与扫描方式、网络拓扑和网络阻塞程度有关。文献[8]针对80(HTTP)，135(DCE/RPC)与445(Net-BIOS/SMB)等漏洞端口采集的数据，显示其具有正态分布性，故而假设 $F\sim N(f,\sigma^2)$，其中 f 为脆弱性主机分布比例。则扫描率为：

$$s(t)=KS_0\frac{1}{\tau(t)}F \tag{1}$$

平均扫描率为：

$$s=KS_0\frac{1}{\tau(t)}f \tag{2}$$

其中，K 为其他相关影响参数。

2.2 AAWP模型

该模型下蠕虫对整个IPv4地址空间(即 2^{32} 个IP地址)进行随机扫描来传播。在 $t+1$ 时刻，感染的节点数为：

$$n(t+1)=(1-d-\delta)n(t)+[(1-\delta)^tN-n(t)][1-(1-\frac{1}{2^{32}})^{sm(t)}] \tag{3}$$

其中，δ 为修复率，d 为移除率，N 为起始脆弱节点数，s 为平均扫描率。对于任意的均匀分布目标区域 Ω，在 $t+1$ 时刻，感染的节点数为：

$$n(t+1)=(1-d-\delta)n(t)+[(1-\delta)^tN-n(t)][1-(1-\frac{1}{\Omega})^{sm(t)}] \tag{4}$$

2.3 建立区域针对性Areas-AAWP传播模型

多区域蠕虫制造者首先聚合所攻击地理区域的IP地址，划定扫描范围。随后该蠕虫需扫描网络中主机漏洞的分布状况，并基于此，针对各区域平均分布的脆弱节点差异性实行不同感染程度的区域选择性攻击。为解析该类蠕虫的传播行为，以上述AAWP模型为基础并针对区域选择性特点来构建Areas-AAWP模型。

建模常用参数与注释见表1。

表1 模型参数与注释

参数	参数注释
N_i	任意区域i中的初始脆弱节点数(包括易感与感染性节点)
$m(t)$	在时刻t所有区域中脆弱节点总数
$m_i(t)$	在时刻t任意区域i的脆弱节点数
$n(t)$	在时刻t所有区域中感染性节点总数
$n_i(t)$	在时刻t任意区域i中的感染性节点数
s_i	任意区域i中内蠕虫的平均扫描率
Ω	所有区域的总扫描空间
w_i	任意区域i中的扫描空间
δ	脆弱性节点的修复率
d	脆弱性节点的移除率
$\triangle n(t)$	在时刻t所有区域中新增的感染性节点数
P_{ij}	任意区域j中感染节点对区域i中脆弱节点的扫描概率
P_{jj}	任意区域j中感染节点对本区域中脆弱节点的扫描概率

假设：

以本地优先扫描即 $p_{jj}\geq p_{ij}$ 为例，蠕虫在 m 个区域中实施不同程度传播时，第 j 区域 n_j 个蠕虫对第 i 区域内脆弱节点的感染率为 $\alpha_{ij}=1-(1-\frac{1}{w_i})^{p_{ij}s_in_j}\approx p_{ij}\frac{s_in_j}{w_i}$，则平均感染率为 $\beta_{ij}=\frac{\alpha_{ij}}{n_j}\approx p_{ij}\frac{s_i}{w_i}$，其中 $p_{ij}=\frac{w_i}{\Omega_i-w_j}(1-p_{jj})$。

具体传播模型为：

仅有两个区域1、2，状态 $t+1$ 时，其感染节点数为：

$$\begin{cases}n_1(t+1)=(\alpha_{11}+\alpha_{12})(m_1(t)-n_1(t))+(1-d-\delta)n_1(t)\\ n_2(t+1)=(\alpha_{21}+\alpha_{22})(m_2(t)-n_2(t))+(1-d-\delta)n_2(t)\end{cases} \tag{5}$$

当有 m 个区域1,2,…,m 时，构建 m 阶矩阵：

$$n(t+1)=\alpha[m(t)-n(t)]+(1-d-\delta)n(t) \tag{6}$$

即为：

$$n(t+1)=\beta n(t)[m(t)-n(t)]+(1-\gamma)n(t) \tag{7}$$

其中，$\alpha=(\alpha_{ij})_{m\times m}$，$\beta=(\beta_{ij})_{m\times m}$，$m(t)$ 为 m 阶方阵，对角元素为 $m_i(t)=(1-\delta)^tN_i$，其余元素为0。$n(t)$ 亦为同类 m 阶方阵，对角元素为 $n_i(t)$，免疫率 $\gamma=d+\delta$。

3 区域感染率的相关性分析与判定

3.1 基于各区域扫描策略的相关性分析

为讨论子区域间的扫描策略协同性对不同区域整体感染效率的影响，现将一个大区域划分为 k 块小区域。其中有效攻击区域为 $m(m\leqslant k)$ 块。假设各区域感染率 β_i 为子样本，所有区域感染率的联合分布函数 $\beta(\beta_1,\beta_2,\cdots,\beta_m)^T$ 为多维正态分布。由于 $F\sim N(f,\sigma^2)$，因此 $\beta\sim N(\mu,\sigma^2)$。为考虑其中感染率 β_i 与 β_j 之间的协同性，引入相似矩阵 $\boldsymbol{R}=(r_{ij})_{m\times m}$，其中 i 区域平均感染率为 $\beta_i=(\beta_{ij})_{1\times m}$，第 i 与 j 区域之间相关系数 $r_{ij}=\frac{E\{[\beta_i-E(\beta_i)][\beta_j-E(\beta_j)]\}}{\sqrt{D(\beta_i)}\sqrt{D(\beta_j)}}$。具体定义为：

定义1 $r_{ij}=0$，此时该类蠕虫采用相互独立的重复随机扫描，区域 i 与区域 j 中进行的感染行为无线性相关性。

证明：任意第 i 个/n 子网区域，其实际IP地址空间为 $w_i\leqslant 2^{32-n}$，网络中总地址空间 $\Omega=\sum_{i=1}^{k}w_i\leqslant 2^{32}$；当蠕虫进行随机扫描时，则有 $p_{ii}=\frac{w_i}{\Omega}$，$p_{jj}=\frac{w_j}{\Omega}$，则 $p_{ij}=\frac{w_i}{\Omega-w_j}(1-\frac{w_j}{\Omega})=\frac{w_i}{\Omega}$，故而 $\beta_{ij}=\beta_{ii}\approx\frac{s_i}{\Omega}$，则 $\beta_i(\beta_{i1},\beta_{i2},\cdots,\beta_{im})$ 中各个元素均相等，存在 $E[\beta_i-E\beta_i]=0$，即 $r_{ij}=0$，定义1成立。

则 $t+1$ 时刻：

$$\Delta n_i(t+1)=\frac{1}{m}\sum_{i=1}^{m}\frac{s_i}{\Omega}[m_i(t)-n_i(t)]n_i(t)-\gamma n_i(t)$$

若所有 $r_{ij}=0$，则 m 个区域的新增感染节点总数为：

$$\Delta n(t+1)\approx\frac{1}{m}\sum_{i=1}^{m}\frac{s_i}{\Omega}[m(t)-n(t)]n(t)-\gamma n(t)$$

所有区域的平均感染率为：

$$\beta=\frac{1}{m}\sum_{i=1}^{m}\frac{s_i}{\Omega} \tag{8}$$

定义2 $r_{ij}=1$，此时该类蠕虫采用合作的分治扫描策略，区域 i 与区域 j 中进行的感染行为线性相关。

假设：

①蠕虫在区域 i 与区域 j 中进行协同感染，它们的总扫

描区域为 $\Omega_s=\sum_{i=1,2}w_i\leqslant 2^{32}$；

②由整体脆弱主机分布 f 可知，$n_s(t)$ 个蠕虫消耗的扫描空间为 $n_s(t)/f$，其扫描空间为 $\Omega_s-n_s(t)/f$；对于第 i 区域，已感节点 $n_i(t)$ 扫描空间为 $w_i=\frac{\Omega_s-n_s(t)/f}{n_s(t)}$；

③t 时刻，有 $n_i(t)=\frac{w_i-n_i(t-1)/f_i}{\Omega_s-n_s(t-1)/f}n_s(t-1)$，即已感染主机按各个区域的大小进行均匀分配，其中 $\frac{1}{f}=\frac{w_i}{\Omega_s f_i}+\frac{w_j}{\Omega_s f_j}$；区域 i 被扫描的概率为 $p_i=\frac{w_i-n_i(t-1)/f_i}{\Omega_s-n_s(t-1)/f}\approx\frac{w_i}{\Omega_s}$。

证明：任意感染性蠕虫节点命中 i 区域内节点的概率为

$$\beta_i=\beta_{ii}+\sum_{v\neq i,v\neq j}^{m}\beta_{iv}=p_{ii}\frac{p_i s_i}{w_i/n_i-1/f_i}+\frac{(1-p_{vv})s_i}{\Omega-w_v} \tag{9}$$

该策略下 $p_{ii}\approx 1$，$p_{vv}=\frac{w_k}{\Omega}$。

由 $\frac{p_{ii}}{w_i/n_i-1/f_i}\gg\frac{(1-p_{ii})}{\Omega-w_i}$ 可知 $\beta_i\approx\frac{p_i s_i}{w_i/n_i-1/f_i}$。

故而 $\frac{\beta_i}{\beta_j}\approx\frac{p_i s_i}{w_i/n_i-1/f_i}/\frac{p_j s_j}{w_j/n_j-1/f_j}$。

由假设③可知 $\frac{1}{w_i/n_i-1/f_i}/\frac{1}{w_j/n_j-1/f_j}=1$ 可得 $\frac{\beta_i}{\beta_j}\approx\frac{s_i p_i}{s_j p_j}=\frac{s_i w_i}{s_j w_j}=k$，即 β_i 与 β_j 线性相关，定义 2 成立。

此时，第 i 与 j 两区域的联合扫描率 $s=\frac{w_i s_i+w_j s_j}{\Omega_s}$，其整体平均感染率 $\beta_s\approx\frac{n_s(t)s}{\Omega_s-n_s(t)/f}$。

在 $t+1$ 时刻，两区域整体的新增感染节点总数为：

$$\Delta n_s(t+1)=\frac{sn_s(t)}{\Omega_s-n_s(t)/f}[m_s(t)-n_s(t)]-\gamma n_s(t) \tag{10}$$

其中，$m_s(t)=(1-\delta)^t(N_i+N_j)$，$n_s(t)<N_i+N_j$。该模型下，两区域整体平均感染率表示为：

$$\beta_s'=\frac{s}{\Omega_s-n_s(t)/f} \tag{11}$$

若其中 n 个区域具有关系 $r_{ij}=1$ 时，所有区域整体平均感染率为：

$$\beta'=\frac{n}{m}\frac{s}{\Omega-n(t)/f}+\frac{1}{m}\sum_{m-n}\frac{s_i}{\Omega} \tag{12}$$

3.2 相关性的判断

由式(9)可知，子式 $\frac{(1-p_{vv})s_i}{\Omega-w_v}$ 正是其非线性影响因素，严格意义讲，在非所有区域完全线性相关的情况下，不存在独立的两个或几个完全线性相关的区域。

此时为考虑其相关度可设置相关度参数 ξ，通过其 ξ 截矩阵分析各区域之间的大致相关性。

$$存在\begin{cases}r_{ij}=1, r_{ij}\geqslant\xi\\ r_{ij}=0, r_{ij}<\xi\end{cases} \tag{13}$$

假设 m 阶相似矩阵 $\boldsymbol{R}$ 在相互的完全线性关系，即具有关系：当 $r_{ij}=1$，$r_{jv}=1$ 时，必有 $r_{iv}=1$(见图 1(a))。

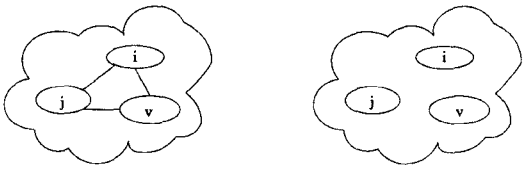
相似矩阵 $\boldsymbol{R}$ 及其特征矩阵值的秩 r 用来判断其是否存在相关性。具体为：

定理 1 当 $r=m$ 时，各区域间进行的传播行为无线性相关性。此时各区域进行互不相干的随机感染(见图 1(b))。

定理 2 当 $r<m$ 时，各区域进行的传播行为必然存在至少 $m-r+1$ 个区域两两完全线性相关。此时相关区域之间进行合作的分治感染。

证明：将 $\boldsymbol{R}$ 对角化得其特征矩阵即 $\boldsymbol{P}^{-1}\boldsymbol{R}\boldsymbol{P}=\boldsymbol{\lambda}$，且 $\boldsymbol{\lambda}$ 的秩为 r，若秩 $r=m$，则 $|\boldsymbol{\lambda}|=1$，无线性相关性。结合定义 1 可知，定理 1 成立。

若秩 $r<m$，则 $|\boldsymbol{R}|$ 必有 $r+1$ 阶子式为 0，存在 $k_1,k_2,\cdots,k_r,k_{r+1}$ 不恒等于 0 时，$k_1\beta_1+k_2\beta_2+\cdots+k_r\beta_r+k_{r+1}\beta_{r+1}=0$ 恒成立，必存在至少一对两两线性关系的元素；同理，m 阶矩阵 $\boldsymbol{R}$ 必有 $m-r+1$ 个元素之间存在着相互完全线性关系。结合定义 2 可知，定理 2 成立。



(a)完全线性相关　　(b)非线性相关

图 1　多区域的扫描行为关联图

3.3 相关性度量

为了进行相关性度量，进而由协同程度判断其传播的快慢程度，本文引入相关性度量指标 ρ。

$$\rho=\frac{m-r}{m-1} \tag{14}$$

其中，r 为矩阵 $\boldsymbol{R}$ 的秩，m 为矩阵 $\boldsymbol{R}$ 的阶数。讨论如下：

①只有两个变量 β_1 与 β_2 时，$m=2$，相关矩阵为 $\begin{bmatrix}1 & r_{12}\\ r_{21} & 1\end{bmatrix}$。由对称性可知 $r_{12}=r_{21}$，存在两种状况，非线性相关时，$r_{12}=0$，秩 $r=2$，则 $\rho=0$；线性相关时，$r_{12}=1$，秩 $r=1$，则 $\rho=1$。

②当存在 m 个变量，其中 n 个变量之间两两线性相关时，秩 r 为 $m-n+1$，则 $\rho=\frac{m-(m-n+1)}{m-1}=\frac{n-1}{m-1}$。

结论 1 对于一定数量的子区域中进行的蠕虫感染，扫描率一定时，域间相关度越大则整体的传播效率越高。

证明：首先 $s_i=s_j=\cdots=s$，为便于分析亦可令 $w_i=w_j=\cdots=w$，则有：以两区域即 $m=2$ 为例，由式(8)与式(11)可知：$\beta_s'=\frac{s}{\Omega_s-n_s(t)/f}>\frac{s}{\Omega_s}=\beta$，得证。当 $\rho=1$ 时的整体感染率较大。

同理，$m\geqslant 3$ 时，所有区域的整体感染相关度为 $\rho=\frac{n-1}{m-1}$，由式(12)可知 m 一定时，$\beta'\geqslant\beta$ 恒成立；并且对于某时刻 t 而言，视 $n(t)$ 为定值，则 β' 随 ρ 的增大而线性增大，得证。

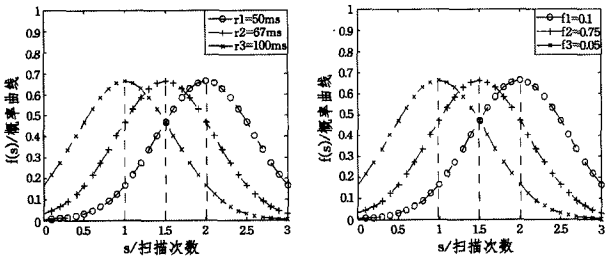
4 实验过程与分析

为了分析扫描率在相关参数下的影响，验证本多区域选择性蠕虫模型，并对比不同相关度对整体区域蠕虫传播的影响，利用 Matlab 软件的仿真功能来实现，运行平台为 widows 7，cpu 3.10GHz，4GB 内存。实验包括：①扫描时间间隔与漏洞分布影响因素下的扫描率仿真；②仿真该 Areas-AAWP 模型下区域危害程度可选择的感染效果；③对比不同相关度下的多区域整体的传播效率。

4.1 对扫描率的仿真

设定扫描线程数 S_0 为 1，其他影响因子 $K=1$。图 2(a)中漏洞节点分布概率 $f=0.1$，分别取扫描间隔 τ 为 50ms、

67ms 与 100ms，则平均扫描率 s_1、s_2 与 s_3 分布在 2/s、1.5/s 与 1/s 次周边；图 2(b)设定 τ=50ms，分别取 f 为 0.1、0.75 与0.05，则平均扫描率 s_1、s_2 与 s_3 分布在 2/s、1.5/s 与 1/s 次周边，可知扫描进程数 S_0 与其他因素 K 一定时，漏洞节点分布越稀疏，时间间隔越长，则扫描率越小，反之亦成立。



(a)时间间隔　　(b)脆弱主机分布

图 2　扫描间隔与时间间隔对扫描率的可能影响

4.2　区域选择性传播的仿真

图 3 中区域数量 m=3；各区域起始脆弱节点数 $N_1=N_2=N_3$=500000；扫描空间 w 均为 1000000；扫描率分别为2/s、1.5/s、1/s；时间步长为 1 秒；本地扫描概率 p 为 98%；补丁率 δ=0.001，移除率 d=0.0001。由图可见，其他条件一定时，从 area3 到 area1，随着扫描率的上升，3 个区域中的感染速率逐渐增大，危害程度逐渐增高，则该类蠕虫对 3 个区域实现了不同感染程度的选择性传播。结果表明：其他条件一定时，扫描率的差异是导致蠕虫进行选择性传播的重要原因，其值越大，则对应的区域感染越迅速，危害越大。

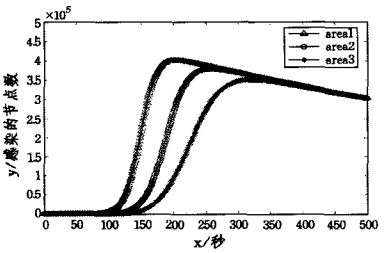


图 3　Areas-AAWP 模型下 3 区域不同危害程度对比图

4.3　不同级别相关度下的感染效果对比

图 4 中子区域数 m=4，扫描率均为 1/s，区域整体起始脆弱节点总数 N=2000000；扫描空间 w 为 4000000；补丁率δ=0.001，移除率 d=0.0001；时间步长为 10 秒。曲线 1、曲线 2、曲线 3、曲线 4 与曲线 5 分别为相关度 ρ 为 1、0.67、0.33 与 0(曲线 4 与曲线 5)下的传播曲线。当 ρ=1 时，曲线 1 具有最快的传播速率和最大的危害程度；曲线 2、曲线 3 与曲线 4 传播速率与危害随着相关度 ρ 的减小逐级减低；曲线 5 为独立扫描，其传播速率最慢，危害最轻。最终，各曲线之间形成了层次分明的感染效率差距。

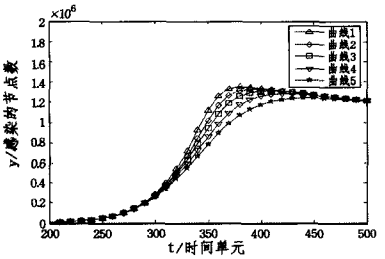


图 4　不同级别相关度下的整体感染效果曲线图

曲线 4 与曲线 5 均为线性相关度 ρ 为 0 的蠕虫传播曲线，二者的不同之处在于，曲线 4 有且只有一个独立区域进行自我协同的分治扫描；而曲线 5 为各区域均进行随机扫描。二者为同一级别(域间完全非线性相关)下的特殊情形，基于域间感染线性相关级别不同所得结论不受其影响。

图 4 验证了结论 1，理想状态下，扫描率一定时，蠕虫在确定的 m 块区域传播时，其扫描策略的相关度越大，则整体的传播速率越高，危害越大。实验现象亦表明，正是不同等级的相关度形成了明显的区域整体感染程度差异。

结束语　本文的主要贡献在于提出了基于不同扫描率的区域选择性蠕虫传播模型，并借助矩阵相关度来评定蠕虫扫描行为间的协同性，最终得出感染速率以及危害程度同该相关度间的关系。这有助于预测与分析现实中该类蠕虫传播表现出的区域针对性。本文未考虑在具体网络拓扑与网络阻塞的情况下的时间延迟影响与网络特性，这些都是后续工作的重点。

参 考 文 献

[1] Moore D, Shannon C. Code-Red: a case study on the spread and victims of an Internet worm[C]// Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurment. Marseille, France: ACM, 2002: 273-284

[2] Nazario J. The conficker cabal announced [EB/OL]. http://www.asert.arbornetworks.com/2009/02/the-conficker-cabal-announced/, 2009

[3] Kermack W O, McKendrick A G. Contributions to the mathematical theory of epidemics. II. The problem of endemicity[J]. Proceedings of the Royal society of London, 1932, 138(834): 55-83

[4] Chen Z, Gao L, Kwiat K. Modeling the spread of active worms [C]// Twenty-Second Annual Joint Conference of the IEEE Computer and Communications(INFOCOM 2003). IEEE Societies, 2003: 1890-1900

[5] Zou C C, Towsley D, Gong W, et al. Routing worm: A fast, selective attack worm based on ip address information[C]// Proceedings of the 19th Workshop on Principles of Advanced and Distributed Simulation. Washington, DC, USA: IEEE Computer Society, 2005: 199-206

[6] Li Y, Chen Z, Chen C. Understanding divide-conquer-scanning worm-s[C] // Performance, Computing and Communications Conference, 2008 (IPCCC 2008). IEEE International, Austin, Texas: IEEE, 2008: 51-58

[7] Chen Z, Ji C. An information-theoretic view of network-aware malware attacks[J]. IEEE Transactions on Information Forensics and Security, 2009, 4(3): 530-541

[8] Bose A, Shin K G. Agent-based modeling of malware dynamics in heterogeneous environments[J]. Security and Communication Networks, 2011, 6(12): 1576-1589

[9] Wagdarikar R R, C Maheshwar R, Raichurakar M A. Securing a Network by Modeling and Containment of Worms Using Preference Scanning[J]. International Journal of Research in Computer and Communication Technology, 2013, 2(10): 959-963

[10] 佟晓筠，李巧军. 基于免疫主机的蠕虫非线性传播新模型优化[J]. 计算机科学，2013，39(5)：99-101

[11] 苏飞，林昭文，马严，等. IPv6 网络环境下的蠕虫传播模型研[J]. 通信学报，2011，32(9)：51-60