基于节点差异性的无线传感网恶意软件传播模型研究 *

杨 雄[1,2], 朱宇光[1], 查志琴[1], 肖贤建[1,2]

(1. 常州工学院 计算机信息工程学院 通信工程系, 江苏 常州 213002; 2. 江苏省常州市软件技术研究与应用重点实验室, 江苏 常州 213002)

摘 要: 针对目前无线传感网络中恶意软件模型化工作的不足,在二维元胞自动机基础上提出了节点差异性的恶意软件传播模型。该模型引入了 MAC 无线信道争用机制和邻域通信距离因素,描述了节点差异度对恶意软件在无线传感网传播扩散的影响。分析仿真实验表明,大规模无线传感网络的节点差异度、无线信道争用机制都对传播行为产生了重要影响,降低了恶意软件的传播速度。与传统传播模型相比,该模型更能够准确描述恶意软件在无线传感网络环境下的传播行为,为无线传感网络安全防御研究提供基础。

关键词: 无线传感网络; 节点差异性; 恶意软件; 元胞自动机; 模型化

中图分类号: TP393.08 **文献标志码**: A **文章编号**: 1001-3695(2012)01-0316-03

doi:10.3969/j.issn.1001-3695.2012.01.087

Investigation of malware propagation model over wireless sensor network based on nodes' diversity

YANG Xiong[1,2], ZHU Yu-guang[1], ZHA Zhi-qin[1], XIAO Xian-jian[1,2]

(1. *Dept. of Communication Engineering, School of Computer & Information Engineering, Changzhou Institute of Technology, Changzhou Jiangsu* 213002, *China*; 2 *Key Laboratory of Changzhou Software Technology Research & Application, Changzhou Jiangsu* 213002, *China*)

Abstract: With the research on malware modeling in wireless sensor network is immature, this paper proposed the malware propagation model with the nodes' diversity based on the 2D cellular automata. It introduced the wireless channel MAC mechanism and the factor of the adjacent communication range into this model. Also depicted the impact of nodes' diversity on the malware spreading over the wireless sensor network. The analysis and simulation indicate that nodes' diversity of the large scale WSN and wireless channel MAC mechanism make the important influence on the spread of the malware and reduce the propagation speed. Compared with the traditional spreading model, this model can more accurately describe the dynamic behaviour of the malware propagation over the WSN, and produces the research foundation for security defense on WSN.

Key words: wireless sensor networks(WSN); nodes' diversity; malware; cellular automata; modeling

0 引言

无线传感网络已经成为 21 世纪的一个新兴研究领域,特别是现代通信技术领域对安全性的要求越来越高,无线传感网络中的安全问题也在近三年得到重视。由于无线通信的范围、节点能量有限、拓扑结构动态变化等特殊构成因素,该类网络非常容易受到各种攻击。当前针对无线传感网络的各种安全攻击行为包括了拒绝服务攻击、蠕虫攻击、中间人攻击及其他恶意程序代码等,本文主要将研究对象定位于网络蠕虫这种能自动快速传播并且引起严重疫情的恶意传播软件。

2002 年以来,Zou 等人对网络蠕虫在传统 Internet 上的传播行为进行了大量的研究,提出了 SI、SIS、SIR 为代表的一系列经典蠕虫传播模型[1~5]。这些研究工作为研究无线传感网环境下蠕虫、病毒等恶意程序的传播行为打下了一定的基础。但是需要注意的是无线传感网络与传统的 Internet 有着许多的不同:a)无线传感网络的通信范围往往具有一定的物理限制,传感节点能量受限的特性导致不同范围内节点的通信能力具有较大的差别;b)传感网络共享无线信道的链路层访问冲突及避免机制也为无线传感网的传播动力学引入了时空相关性;c)无线传感网络具有高度自组织特性,这也是区别于传统 Internet 的一大特征。因此,研究适用于无线传感网络环境的恶意软件传播模型就显得非常必要。

2006 年以来,国际上一些研究人员开始对无线传感网络环境中的蠕虫等恶意软件传播行为进行了研究。Khayam 等人[6]利用信号处理技术研究了蠕虫在无线传感网络中的传播模型。De 等人[7]利用流行疾病学理论研究了无线传感网络中的节点危害传播过程,指出基于随机图理论的无线传感网模型在描述恶意软件传播行为动力学上仍然有很大的不足之处。

收稿日期: 2011-06-27; **修回日期**: 2011-07-30 **基金项目**: 江苏省高校自然科学基础研究基金资助项目(10kjd520007);江苏省常州市社会发展科技计划资助项目(CS20100013)

作者简介:杨雄(1980-),男,江苏无锡人,讲师,硕士,主要研究方向为网络安全与无线传感网络(popobear801116@tom.com);朱宇光(1966-),男,江苏常州人,副教授,博士,主要研究方向为无线传感网络;查志琴(1968-),女,江苏溧阳人,副教授,硕士,主要研究方向为分布式网络;肖贤建(1974-),男,江西人,讲师,博士,主要研究方向为无线传感网.

2009 年,Tanachaiwiwat 等人[8] 开始研究在无线网络中的网络蠕虫传播行为,并且对蠕虫在无线网络环境下的防御策略进行了一定的阐述。上述的研究工作均利用平均场方法对蠕虫在无线传感网络中的扩散建立了确定性的宏观模型,但是这些方法只适用对传播过程进行整体的描述预测,对局部与微观的时空相关特性仍然无法进行有效的反映。针对这些特点,本文将采用当前已被广泛应用于研究复杂系统,同时可准确反映各种不确定行为的二维元胞自动机模型来描述恶意程序在无线传感网络中的传播行为。值得注意的是,虽然当前已有一些工作研究了蠕虫在无线传感网中的传播模型,但是这些研究均没有考虑节点差异性对蠕虫在无线传感网扩散传播的影响,简单地认为所有节点均具有相同的传播扩散效率。Olinky 等人[9] 的研究表明,病毒传播很大程度上依赖于网络结构,他在论文中定义了一个度为 k 的健康节点和一个感染节点,一个节点的感染概率 $P(k)$ 依赖于节点的度 k,k 越大受到的感染率越低,也即节点的连接度越大往往具有更高的安全防范意识,抵抗病毒的能力越强,这种假设符合目前的网络环境,因为节点连接度大的往往都是网络上的服务器或者骨干路由器,其相应的安全机制常常也较为完善。遗憾的是,Olinky 的理论对象是传统的 Internet,并没有考虑无线传感网中节点的差异性,也未将链路层访问冲突及避免 MAC 机制引入研究,建立的模型也是运用平均场方法,具有一定的局限性。2010 年,宋玉蓉等人[10] 利用一维元胞自动机建立了基于节点抗攻击差异性的复杂网络恶意软件传播模型,该模型能反映网络结构对蠕虫等恶意程序扩散的影响,但是该模型的提出依然是建立在对传统网络的研究基础之上,未对无线传感网络中节点的差异性进行研究。

1　无线传感网的节点差异度模型

无线传感网的节点主要分为两大类,一类位于网络的末梢及边界区域,负责数据的感应捕获与传递通信;另一类则主要为网关节点也即常说的 sink 节点。在大规模无线传感网络中,由于部署区域较大、节点通信距离受限,通常需要有若干个传感分网进行覆盖,每个传感分网负责完成本区域内感应数据的采集,然后由本区域的网关节点负责向上级的主干 sink 节点传递通信数据,如图 1 所示。这种网络结构在一定程度上造成了相关节点连接度的差异性,文献[9,10]的研究都表明该差异性将会显著影响恶意软件在网络中的传播速度和行为。本文基于此理论引入了无线传感网环境下相关节点的差异度模型,构建了无线传感网的二维元胞自动机恶意软件传播模型。

需要指出的是,大规模无线传感网络中连接度较大的节点往往都是一级、二级传感网关,这些节点由于担负着相应区域的数据汇总和外界通信的网关角色,因此在构建无线传感网络时管理人员常常会提高这些 sink 节点的强壮性以提高整个网络的通信质量,如管理人员会更关注于 sink 节点的电池能量,加强此类节点的安全性能和存活性能。因此可以认为无线传感网络中节点的脆弱性与节点的度有着很大的关系。节点连接度较大的代表着 sink 此类网关节点,其抗攻击能力往往较强;连接度较小的节点代表着终端传感节点,相应的抗攻击能力往往较弱。

2　无线传感网 MAC 机制

由于无线传感网的特殊性,恶意软件在无线传感网上的扩散传播与传统的 Internet 有很大的区别:a)传感节点在被恶意软件感染之后向周边健康节点扫描攻击时常常受到无线通信距离的限制;b)位于同一冲突区域内的节点在同一时刻只允许区域内一个节点进行数据的发送和接收,每个节点在进行数据传递前会检查自身状态和周边邻居节点信道空闲状态。为描述方便,应用二维布尔向量表解释上述机制,每个传感节点对应于二维表中的一个表元素,若一个节点正在进行数据通信,则与其相邻的节点在二维表中表项置“1”,代表该类节点处于阻塞状态不能进行数据传输。任何一个节点在进行数据通信前均需要检查该节点与邻居节点在二维向量表中的状态,信道如果空闲也即相应的表项为“0”,则允许传输,否则拒绝。一旦传感节点数据通信完毕,则其邻域内所有处于阻塞状态的节点表项重新恢复成“0”。二维向量布尔表如图 2 所示。

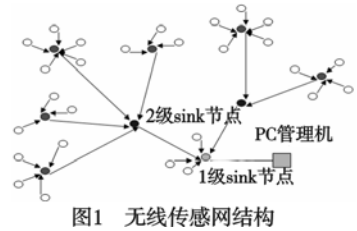

图1　无线传感网结构

0	0	0	0	0	0	0
0	0	0	0	0	0	0
0	0	1	1	1	0	0
0	0	1	0	1	0	0
0	0	1	1	1	0	0
0	0	0	0	0	0	0
0	0	0	0	0	0	0

图2　MAC二维向量表

3　节点差异度恶意软件传播模型

本文采用二维元胞自动机建立节点差异性无线传感网恶意软件的扩散传播模型,与以往采用一维元胞自动机的传播模型相比,二维元胞自动机能够更好地描述无线传感网平面中节点之间的时空交互特性,具有更好的微观局部描述效果。本文中用四元组 (C,V,Q,f) 定义元胞自动机模型,其中 C 表示元胞空间,V 表示节点的邻域,Q 表示有限状态集,f 代表状态转换规则函数。以下分四个部分逐步阐述基于二维元胞自动机的节点差异度恶意软件传播模型建立过程。

3.1　元胞空间

二维元胞空间采用平面二维坐标系来表示元胞空间中的任何一个元胞,一个传感节点相对应于该二维坐标系中的一个节点。任何传感节点的位置可以用二维坐标值 x、y 唯一标志,即 $C=\{(x,y);0\leqslant x\leqslant L,0\leqslant y\leqslant L\}$,$L$ 为二维空间的最大坐标值。

3.2　邻域空间

无线传感网络中节点之间的通信往往受到物理距离的限制,因此很有必要在元胞自动机模型中定义邻域节点空间,只有属于邻域空间内的节点才可以相互通信。假设每个节点都存在最大通信距离 R,定义任意传感节点 $C_{i,j}$ 的邻域空间

$$V_{i,j}=\{(x,y);\sqrt{(x-i)^2+(y-j)^2}\leqslant R,(x,y)\in C\}$$

3.3　状态集

在研究过程中只考虑恶意软件的 SIS 模型,无线传感网的恶意软件传播模型除了需要考虑节点的状态之外,还需要考虑信道访问的状态,因此给出两个状态集:Q_1 和 Q_2。其中:$Q_1=\{0,1\}$ 表示节点的状态,定义二维元胞空间坐标系中任意位置的一个节点 $C_{i,j}$ 的状态变量,$S_{i,j}(t)=0$ 代表 t 时刻该节点状态为健康,$S_{i,j}(t)=1$ 代表 t 时刻该节点状态为感染;$Q_2=\{0,1\}$ 表示无线信道的状态,同样定义任意节点 $C_{i,j}$ 的信道状态变量,$M_{i,j}(t)=0$ 表示 t 时刻该节点信道空闲,可以进行数据通信,$M_{i,j}(t)=1$ 表示 t 时刻该节点信道忙碌,需要等待信道空闲后再进行数据通信。值得注意的是,$C_{i,j}$ 进行数据传输时该节

点邻域空间 $V_{i,j}$ 内的所有节点的信道状态变量 $MV_{i,j}(t)$ 均设置为 1，这表示由于无线信道 MAC 机制的特殊性，邻域内的其他节点都需要等待信道空闲。

3.4 节点差异度状态转换函数

传感节点 $C_{i,j}$ 在 t 时刻的状态由 $t-1$ 时刻的自身状态 $S_{i,j}(t-1)$ 和其邻居 $V_{i,j}$ 状态 $SV_{i,j}(t-1)$ 共同决定。假设健康节点 $C_{i,j}$ 受到邻域内一个感染节点的感染概率为 β，则该节点与周围 u 个邻居进行通信受到感染的概率 $\beta_{i,j}^{*}=1-(1-\beta)^{u}$。其中 u 表示在一个离散时间间隔内，$C_{i,j}$ 邻域中节点处于感染状态 $SV_{i,j}(t-1)=1$ 且信道为空闲状态 $MV_{i,j}(t-1)=0$ 的邻居节点个数。即

$$u=\sum(Sxy(t-1)=1 \text{ and } Mxy(t-1)=0),(x,y)\in V_{i,j} \quad (1)$$

同时考虑在同一离散时间间隔内，一个感染节点以概率 δ 恢复健康，则节点的状态转换函数同时由节点自身状态与邻居状态共同决定，因此建立如下状态转换函数：

$$S_{i,j}(t)=\max(f_1(S_{i,j}(t-1)\times(1-\delta)),f_2(\overline{S_{i,j}(t-1)}\times\beta_{i,j}{}^{*})) \quad (2)$$

其中，右侧两项结果中最大值即为 t 时刻节点 $C_{i,j}$ 的状态变量；右侧第一项 $f_1(S_{i,j}(t-1)\times(1-\delta))$ 表示节点自身的治愈过程，先前处于感染状态的节点经过时间 t 后以 δ 概率恢复到健康状态，即 $f_1(x)$ 为治愈过程的状态转换函数，定义为

$$f_1(x)=\begin{cases}1 & x\geqslant\delta\\ 0 & x<\delta\end{cases} \quad (3)$$

式(3)表明当处于感染状态的节点继续保持感染状态的概率 $1-\delta$ 小于治愈概率 δ 时，节点状态恢复成健康，反之继续保持感染状态。式(2)右侧第二项表示感染过程，其中 $f_2(x)$ 为感染过程状态转换函数。如前文所述，定义一个单调递减的函数 $a(k)$ 来表示连接度为 k 的节点受到攻击被感染的概率，k 越大表示该节点连接度越大，相应的 $a(k)$ 函数值越小表示此类主干节点被感染的概率越小，因此可以将 $a(k)$ 定义成节点 $C_{i,j}$ 从健康节点变为感染节点的概率阈值。$f_2(x)$ 定义如下：

$$f_2(x)=\begin{cases}1 & x\leqslant a(k)\\ 0 & x>a(k)\end{cases} \quad (4)$$

式(4)表明节点 $C_{i,j}$ 由健康状态转为感染状态的依据就是其与周边邻居接触通信的感染概率 $\beta_{i,j}^{*}$ 与该节点被感染阈值 $a(k)$ 比较的结果，连接度大的节点，$\beta_{i,j}{}^{*}$ 往往会随着邻居数目 u 的增加而增加，但 $a(k)$ 随着连接度的增加而降低，所以度大的节点并不容易被感染。

3.5 传播模型

令 $I(t)$ 表示 t 时刻被感染的主机数，$S(t)$ 表示 t 时刻健康节点的主机数，$I(0)$ 表示初始时刻被感染的主机数，$I(t)/N$ 表示 t 时刻被感染的疫情百分率，$S(t)/N$ 表示 t 时刻健康节点的百分率，则可以得出以下二维元胞自动机的节点差异度恶意软件传播模型：

$$\begin{cases}S(t)/N+I(t)/N=1\\ I(t)/N=\dfrac{1}{N}\sum_{i,j}S_{i,j}(t)=1\\ S(t)/N=\dfrac{1}{N}\sum_{i,j}S_{i,j}(t)=0\end{cases} \quad (5)$$

4 仿真实验结果分析

实验环境为 200×200 的区域中随机布置 N 个传感器节点，实验从位于(60,60)到(120,120)的中心区域中任意选择一个感染节点开始。需要说明的是，与以往研究工作单纯地认为节点具有相同感染传播概率不同，笔者在仿真实验中首先考虑了节点差异度对恶意软件在无线传感网络中传播效果的影响；其次引入了 MAC 无线信道访问机制，对无线传感网环境下的恶意软件传播行为进行了分析；最后研究了感染概率对恶意软件传播速度的贡献。实验环境所设参数分别为：$N=1500$，$\beta=0.2$，$R=5$，$\delta=0.5$，$I(0)=1$，为获取精准的统计数据，本文实验了 100 次，以求取最终结果的平均值。

4.1 节点差异度函数对传播效果的影响

本文考虑了三种节点差异度函数，分别为：a) $a(k)=e^{-k/n}$，其中 n 表示节点的最大连接度，这里 $n=10$；b) $a(k)=k^{-1}$；c) $a(k)=1$，表示所有节点均没有差异性，受攻击感染的概率相同，这也是传统研究中普遍假设的一种情况。

图 3 表明考虑了节点差异度的函数 a)b) 与不考虑节点差异性的 c) 相比，恶意软件的传播速度较为缓慢。主要原因在于连接度大的节点虽然与周围节点接触的概率大，但是由于这些节点往往是骨干节点，安全保护措施较强，被感染的概率较小；而小连接度的节点虽然容易被攻击感染但是由于其与周边节点的接触机会不高，所以对整个疫情的传播影响也较小。因此可以得出在无线传感网络中，考虑类似于 sink 网关节点与普通节点连接度的差异性对描述恶意软件的传播行为具有重要的作用。

4.2 MAC 机制对传播效果的影响

在无线传感网络中，恶意软件的传播扩散模型必须考虑无线信道访问特有机制，只有信道空闲，具有感染特性的邻域内节点才可以竞争访问信道，恰恰是这种竞争信道的特性在一定程度上延缓了恶意软件的传播速度，降低了病毒快速流行的可能性。从图 4 可以看出，引入 MAC 机制的传播模型极大地抑制了病毒的传播，疫情到达饱和程度的时间延缓了 30% 左右。

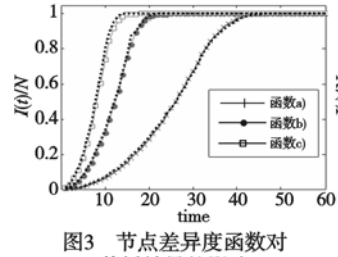

图3 节点差异度函数对传播效果的影响

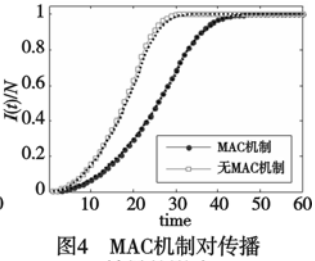

图4 MAC机制对传播效果的影响

4.3 感染率对传播过程的影响

在仿真实验中，本文与以往的研究一样分别对病毒的传播率进行分析，感染概率 β 分别为 0.2、0.5、0.8。从图 5 可以看到，恶意软件的传播感染率对恶意软件的扩散也有着较大的影响，当 $\beta=0.2$ 时在仿真实验的终止时刻病毒才刚刚达到饱和状态，而当 $\beta=0.5$ 和 0.8 时恶意软件的扩散速度非常惊人，两者的扩散效果较为一致，在病毒爆发的早期就迅速到达了疫情的饱和状态。因此在恶意软件的爆发早期采取抑制策略能够较好地减缓病毒的传播速度。

5 结束语

本文提出了一种基于节点差异度的恶意软件传播模型。该模型考虑了无线传感网特有的网络属性，将 MAC 无线信道争用机制与无线通信邻域距离考虑在内，同时 （下转第 321 页）

$$(zY)^{h(M\|r\|Y)} \bmod p$$

证毕。

2.2 安全性分析

1)可以抵抗各种伪造攻击

这里只对普通签名作分析,强制签名的分析类似。首先考虑外部敌手的伪造攻击,要伪造签名$(r,s,Y,h(x))$,必须伪造出r、s。而伪造r面临求解离散对数的数学难题;伪造s需要知道用户的秘密碎片,在系统安全的情况下秘密碎片不能获得。通过求解$z=g^x$获得群私钥$x=f(0)+\sum_{j=1}^{m}g_j(0) \bmod q$,以便伪造群签名在离散对数假设安全的前提下是不能成功的。接着考虑内部$t-1$个成员的伪造攻击,这里指出在离散对数假设和可证明安全理论的前提下是不能成功的,具体参见文献[2]给出的分析。最后考虑 KAC 的伪造攻击,假设 KAC 被敌手攻破实施伪造攻击,在已知δ_i、γ_{ij}的前提下还必须知道签名人的私钥x_i,而由$y_i=g^{x_i} \bmod p$求x_i在离散对数假设下是不可行的,故 KAC 不能伪造签名。

2)可以抵抗内部t个用户的合谋攻击

文献[9]指出 Chen Wei-dong 等人的方案安全隐患之一在于无法抵抗内部用户的合谋攻击。本文借鉴其设计方法加入随机控制参数d,克服了内部t个用户的合谋攻击带来的风险,具体分析参见文献[9]的安全性分析。

3)具有可追踪签名人真实身份的特性

在本方案中采用身份标志符来代替签名人的真实身份,隐藏了签名用户的真实身份有利于保护签名人的权益,实现了匿名性。另外追踪签名用户的真实身份也很容易,只需要将身份标志符代入追踪函数$h(x)$即可。若$h(U_i)=0$,则证明该用户参与了签名,最后可由 KAC 查出该用户的真实身份。另外文献[8]证明了对追踪函数的攻击是不可行的,所以追踪函数的安全性是有保证的。

4)具有门限特性

本方案既可实施普通签名又可实施强制签名,灵活易用。而且两种签名方案都必须达到特定的签名门限值,否则不能恢复群私钥,同时签名验证方程也将不能通过。

3 结束语

本文提出了一种新的门限签名方案,解决了一般存在特权集的门限签名方案中签名容易"难产"且安全性弱的问题,进一步完善了存在特权集的门限群签名方案。

参考文献:

[1] DESMEDT Y,FRANKEL Y . Shared generation of authenticators and signatures[C]//Proc of the 11th Annual International Compotology Conference on Advances in Cryptology. London: Springer-Verlag, 1992:457-469.

[2] CHEN Wei-dong,FENG Deng-guo. A group of threshold group signature schemes with privilege subsets [J]. Journal of Software,2005, 16(7):1289-1295.

[3] SHI Yi,FENG Deng-guo. he design and analysis of a new group of (t_j,t,n) threshold group-signature scheme[C]//Proc of the China-CRYP . Beijing: Science Press, 2000:156-159.

[4] 王天芹. 存在特权集的门限代理群签名方案[J]. 计算机应用研究,2008,25(7):2146-2147.

[5] XUE Ming-wang, YU Rong-dong. Threshold group signature scheme with privilege subjects based on ECC[C]//Proc of ICCIIS. 2010:84-87.

[6] 杨长海,唐西林. 具有多种特性的门限多代理多签名方案[J]. 计算机工程,2009,35(13):160-162.

[7] 贾晓芸. 面向群体的数字签名体制研究[D]. 北京:北京邮电大学,2008.

[8] 王泽成,斯桃枝,李志敏. 安全增强的存在特权集的门限群签名方案[J]. 计算机工程与应用,2007,43(9):151-153.

[9] 王勇兵,王际川. 对存在特权集的门限群签名方案的安全性分析[J]. 计算机工程与应用,2010,46(9):80-82.

(上接第 318 页)引入了节点连接度差异性导致感染率不同的恶意软件扩散模型。该模型能够较真实地反映实际环境中如骨干节点、sink 网关节点等连接度大的节点常常受管理人员关注而具有较强安全性的特点,提出了节点感染率并不与连接度简单成正比的观点。实验证明此二维元胞自动机模型能够更准确地描述恶意软件在无线传感网络环境下的传播行为,具有重要的研究价值。

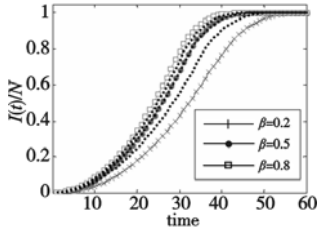

图5　感染率β对传播效果的影响

参考文献:

[1] STAN I S, PAXSON V, WEAVER N. How to own the Internet in your spare time[C]//Proc of the 11th USENIX Security Symposium. 2002:149-167.

[2] ZOU C C, OWSLEY D, GONG W B. Modeling and simulation study of the propagation and defense of Internet e-mail worms[J]. IEEE Trans on Dependable and Secure Computin , 2007, 4 (2):105-118.

[3] ZOU C C, GONG W, OWSLEY D. Code red worm propagation modeling and analysis[C]//Proc of the 9th ACM Conference on Computer and Communications Security. 2002:138-147.

[4] PASTOR-SA ORRAS R, VESP I I A. Epidemic spreading in scale free networks [J]. Physical Review Letters,2001,86(14):3200-3203.

[5] NEWMAN M E J, FORREST S, BAL HROP J. E-mail networks and the spread of computer viruses [J]. Physical Review E, 2002, 66 (3):35101.

[6] KHAYAM S A, RADHA H. Using signal processing techniques to model worm propagation over wireless sensor networks [J]. IEEE Si nal Processin Ma azine, 2006,23(2):164-169.

[7] DE P, LIU Y, DAS S K. Modeling node compromise spread in wireless sensor networks using epidemic theory[C]//Proc of International Symposium on World of Wireless, Mobile and Multimedia Networks. 2006:237-243.

[8] ANACHAIWIWAT S, HELMY A. Encounter-based worms: analysis and defense[J]. Ad hoc Networks,2009,7(7):1414-1430.

[9] OLINKY R, STONE L. Unexpected epidemic thresholds in heterogeneous networks [J]. Physical Review E,2004,70(3):30902.

[10] 宋玉蓉,蒋国平. 节点抗攻击存在差异的无尺度网络恶意软件传播研究[J]. 物理学报,2010,59(2):705-711.