无线传感器网络中的病毒传播动力学研究

庄克琛 张 宏 张 琨 姜海涛
(南京理工大学计算机科学与技术学院 南京 210094)

摘 要 从无线传感器网络的基本特征出发,结合传感器病毒感染过程的具体特点,对无线传感器网络上的病毒传播动力学进行研究。分别使用均匀随机分布、簇分布、二维高斯分布、随机格状分布方法来建立平面无线传感器网络模型;结合传染病理论,考虑了无线传感器网络的传播特征以及不同的MAC机制对传感器网络中病毒传播的影响,建立了无线传感网中病毒传播模型。仿真实验表明,有局部聚集的节点散布方式会加快病毒的传播,而采用休眠唤醒机制的通信方式能够限制病毒传播的速度,降低病毒在传感器网络中快速扩散的风险。

关键词 无线传感器网络,病毒传播模型,休眠唤醒模式
中图法分类号 TP393 **文献标识码** A

Analysis of Spreading Dynamics of Virus in Wireless Sensor Networks

ZHUANG Ke-chen ZHANG Hong ZHANG Kun JIANG Hai-tao
(School of Computer Science and Technology, Nanjing University of Science and Technology, Nanjing 210094, China)

Abstract The spreading dynamics of wireless sensor networks (WSN) was analyzed by considering the basic characteristics of WSN and the characteristics of sensor virus infection process. The different WSN models were established by employing different sensor deployment patterns, which include uniform random deployment, clustered deployment, group Gaussian deployment and random grid deployment. A virus spreading model was established based on infectious disease theory by considering the propagation characteristics of WSN and the impact of different MAC mechanism on virus spreading in WSN. The simulations show that the local group node deployment pattern would speed up the spreading of virus in WSN, while the sleep/wake up communication mechanism would slow down the spreading of virus, reduce the risk of the virus rapidly spreading in WSN.

Keywords Wireless sensor networks(WSN), Virus spreading model, Sleep/wake-up mechanism

1 引言

无线传感器网络 WSN(Wireless Sensor Networks)是大量的静止或移动的传感器节点以自组织或者多跳的方式构成的无线网络,用于监测、处理网络覆盖范围内的感知对象的监测信息,并将信息传输到汇聚节点。它有着网络规模大、拓扑结构变化频繁、节点能量有限等特点,在民用和军用领域都有广阔的应用前景,如环境监测保护、医疗护理、目标跟踪等。由于大规模的传感器网络一般配置在恶劣环境、无人区域或者战场阵地中,网络的安全性能和可靠性是亟待解决的问题。

目前大多数针对 WSN 安全问题的研究主要集中于网络通信安全协议以及通信节点认证等方面。这些研究对抵御来自网络外部的入侵和破坏较为有效,但对于来自网络内部节点的攻击则往往捉襟见肘,例如拒绝服务攻击、虫洞攻击、蠕虫攻击等。

由于成本和资源的限制,为了大规模散布传感器节点,单个传感器节点的硬件结构和软件系统设计都比较简单,而且单个传感器节点的能量有限,没有较强的计算能力来保证自身的安全。因此,由缓冲区溢出等漏洞被利用导致的 Internet 病毒大规模传播同样可能发生在 WSN 中。

虽然传感器节点的 Harvard 架构不同于冯诺依曼架构,其程序的内存区和数据内存区被分离,普通的利用缓冲区溢出感染病毒已经无法对其进行感染,但 Yi Yang 等人在 Mica2 传感器上的病毒感染实验[1]仍然表明,这种架构下仍然存在缓冲区溢出的危险,从而导致恶意程序可以从数据内存区侵入程序内存区。而且一般的 WSN 的布局往往是大规模散布软硬件配置完全相同的传感器节点,这更会导致病毒一旦感染部分节点即可在 WSN 上大规模快速传播。

Internet 上的病毒传播已被广泛研究,尤其是近年来基于复杂网络理论的 Internet 中病毒传播的研究,并结合传染

到稿日期:2012-05-23 返修日期:2012-09-07 本文受国家自然科学基金(61003210),江苏省自然科学基金(BK2011023,BK2011370),江苏省"六大人才高峰项目"(11-C-028)资助。
庄克琛(1989-),男,博士生,主要研究方向为大规模网络动态性、网络安全,E-mail:zhuangkechen@gmail.com;张 宏(1956-),男,教授,博士生导师,主要研究方向为网络性能和信息安全;张 琨(1977-),女,博士后,副教授,主要研究方向为信息安全、网络通信等;姜海涛(1985-),男,博士生,主要研究方向为无线网络路由协议。

病理论进行分析，均有助于理解 WSN 上的病毒传播威胁。但 Internet 在拓扑结构、组织方式、通信机制等方面与 WSN 有很大的不同。WSN 需要的人工干预很少，具有高度自组织性。WSN 是一个空间网络，节点间的交互往往与空间距离有关，其拓扑结构因散布形式不同而不同，而且 WSN 的 MAC 机制也使得 WSN 中的信息传递具有时空相关性。这些特征都使得 Internet 中的病毒传播研究不适用于 WSN。

传统的 WSN 中病毒传播建模研究大都从传染病理论出发建立传播模型，或建立感染/免疫恢复模型，并进行数值分析，但对于 WSN 中不同的传感器节点分布情况，以及节点能量有限性等特征考虑较少。本文从 WSN 的不同空间布局的拓扑特征、考虑能量节约的休眠唤醒机制出发，研究 WSN 上的病毒传播动力学。首先构建 WSN 网络通信模型和 MAC 机制，建立 SID(Susceptible-Infected-Dead)病毒传播模型，并通过在接近真实环境的仿真环境进行模拟实验，研究 WSN 空间散布情况、不同 MAC 机制对 WSN 中的病毒传播的影响。

2 相关研究

较早的 WSN 病毒传播研究主要来自研究者对 WSN 中传感器节点操作系统和传输层漏洞的研究。Yi Yang 等人成功地在 Harvard 架构的 Mica2 传感器进行了恶意程序感染实验，验证了 WSN 中病毒大规模传播的威胁存在，提出了一种基于“着色”的利用软件版本差异性来减速或者遏制病毒传播的宏观控制方法[1]。Qijun Gu 等人研究恶意数据包在 WSN 中的传播[2]，验证了一个在 17bytes 内的恶意数据包可以利用传感器节点正常的数据传输功能在 WSN 中进行传播，从而造成大范围影响，提出恶意数据包对 WSN 中节点攻击的有效性直接取决于网络流量的规模。

近来的 WSN 中病毒传播的研究主要以基于传染病理论的建模为主。Khayam 和 Radha 研究了均匀分布节点的 WSN 中的拓扑感知病毒的传播动力学[3]，并应用信号处理技术建立了 WSN 中的病毒传播模型，他们将物理层、数据链路层、网络层以及传输层的各种特征整合在构建的病毒传播模型中，其中病毒的传播则因为节点通信半径的限制，采取临近节点传播策略。在文献[4]中，他们基于传染病理论，提出了一种 WSN 中的拓扑感知蠕虫病毒传播模型(TWPM)，其考虑了 WSN 实际的物理层、MAC 层以及网络层的通信机制，并模拟分析了蠕虫病毒在 WSN 中传播的时空动态性，但并没有考虑不同传感器节点分布情况对病毒传播的影响。

Pradip De 等人在分析 WSN 中的病毒传播特性时考虑了节点的二维高斯分布散布情况以及节点间的密钥分配情况对大规模传播的影响，并给出了一个同时考虑节点恢复情况的 WSN 中的病毒传播模型[5]。Sun Bo 等人基于渗透理论和随机图论研究了 WSN 中病毒传播的免疫机制[6]，分析了在网络拓扑的连通率、剩余边比例、连通子图规模不同的情况下的选择性免疫对 WSN 中病毒传播的遏制能力。Wang Xiaoming等人基于传染病理论的 SIR 模型，提出了一种 iSIR 病毒传播模型[7]，其结合传染病理论分析了在带有节点恢复功能的 WSN 中病毒传播的动态性。宋玉蓉等利用元胞自动机建立病毒传播模型[8]，分析了随机密钥预分布等因素对 WSN 中病毒传播的影响。

3 WSN 网络模型和通信机制

3.1 网络模型

本文主要建立传播模型，依靠大量的实验分析来研究不同 WSN 节点布局和 MAC 机制对其中病毒传播的影响。为了便于模拟分析，将 N 个传感器设备以不同的方法布局于一个面积为 S 的二维矩形平面中，将单个传感器设备抽象为一个平面中的节点，则 WSN 网络中节点之间的互相作用是其间距离的函数，节点 b 收到节点 a 的通信信号强度会随着它们之间距离的增加而衰减。简单起见，假设所有传感器节点均有全向型天线，不考虑方向性天线增益，假设节点 a 的发送功率为 P_a，节点 a 到节点 b 的路径损耗为 PLd，则 b 处的信号功率密度 P_b 应与 P_a 有如下关系：

$$P_b=\frac{P_a}{Gd_0^2}\left(\frac{d_0}{d}\right)^k \tag{1}$$

式中，d 为节点 a 与节点 b 间的欧式空间距离，$d_0=1\text{m}$ 为参考距离，G 为信道衰减因子。若有式(2)成立，则说明节点 a 能与节点 b 建立连接，节点 a 发出的数据能被节点 b 正确接收。

$$\frac{P_b}{v}=\frac{P_a}{vGd_0^2}\left(\frac{d_0}{d}\right)^k\geqslant\beta_0 \tag{2}$$

式中，β_0 是衰减临界值，v 是节点 b 的噪声电平。

为了模拟更加实际的无线传感网络传输，本文中采取的路径损耗 PLd 的 dB 表达式如下：

$$PLd=\begin{cases}0, & d<d_0/10\\ PLd_0+10*PE*\lg\left(\frac{d}{d_0}\right)+\delta, & d\geqslant d_0/10\end{cases} \tag{3}$$

式中，PLd_0 为参考距离 d_0 的路径损耗，PE 为路径损耗指数，δ 是随机损耗。设节点 b 的接收信号阈值为 P_{th}，则在使用的路径损耗计算方式下，若有式(4)成立，则可认为节点 b 能够正确接受节 a 发送的信号。

$$P_a-PLd\geqslant P_{th} \tag{4}$$

简单起见，所有 N 个节点散布在一个 S 区域($L*L$ 的矩形区域)中，所有节点使用相同的传输功率，在每次数据包传输时，分别根据计算节点间的传输距离确定连接能否正确建立。

本文考虑 4 种不同的节点分布方式。

(1) 均匀随机分布：使用均匀随机过程来创建节点的散布位置，使得所有节点处在 S 平面中任意点的概率相同，如图 1(a)所示。

(2) 簇分布：首先随机选取 S 区域中的一个点，然后以该点作为子区域的左下角坐标，构建一个 $v\times v(v<L)$ 的子区域，在该子区域中，使用参数为 λ 的泊松分布来产生该子区域中所需散布的节点个数 m，然后将 m 个节点均匀随机散布在该子区域中，重复上述过程，直到所有 N 个节点全部散布在 S 区域中，如图 1(b)所示。

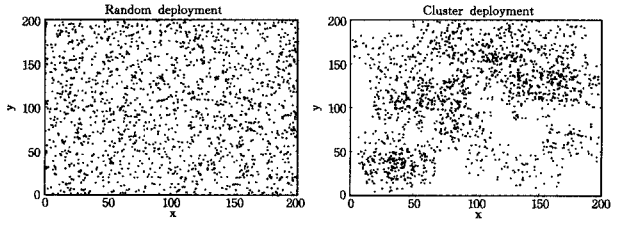
(3) 二维高斯随机分布：首先将传感器节点分为 t 个相同数目的组，同样将区域 S 分为 t 个面积形状相同的格状区

域，然后将每组的节点围绕格状区域的中心点按照二维高斯分布来确定相应的位置。设第 i 组 G_i 所投放的区域中心点坐标为(x_i, y_i)，则该组中任一节点 k 的坐标(x, y)的概率分布为：

$$f_k(x,y|k\in G_i)=\frac{1}{2\pi\sigma^2}e^{-[(x-x_i)^2+(y-y_i)^2]/2\sigma^2} \quad (5)$$

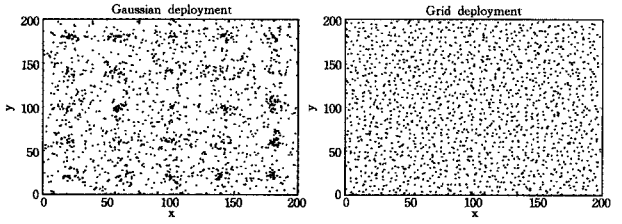
式中，σ 为标准差，分布情况如图 1(c)所示。

(4) 随机格状分布：普通的规则格状分布将节点规则地分布于 $n*n$ 的网格上，随机格状分布针对有 N 个节点的网络($N=n*n$)，则将 S 区域分为 N 个相等的格状区域，然后将每个节点随机散布在相应的格状区域内，如图 1(d)所示。



(a) 均匀随机分布，区域大小 200×200，平均最短邻居距离为 d_m = 2.5

(b) 簇分布，区域大小 200×200，子区域大小取 v=40，每簇的平均节点数目为 λ=40，平均最短邻居距离为 d_m=2.10



(c) 二维高斯随机分布，区域大小 200×200，分组个数 t=5*5=25，每组节点数目 n=64，二维高斯分布中标准差 σ=10，平均最短邻居距离为 d_m=2.49

(d) 随机格状分布，区域大小 200×200，平均最短邻居距离为 d_m=3.18

图 1　有 1600 个节点的 WSN 的 4 种不同分布方式

在考虑节点分布密度时，使用平均最短邻居间距离 d_m 来测量网络中节点的平均度数，平均最短邻居距离越小，表明网络中节点的平均度数越高。

3.2　通信机制

传感器节点能量有限，为了降低节点的能耗，一般均采用休眠唤醒工作模式。由于 IEEE802.15.4 标准的 MAC 机制不支持所有节点的广播数据传输，我们采用一种较为实用的基于 CSMA-CS 且支持广播数据传输的可调的 MAC 机制，其能够进行不同的休眠唤醒模式调节，也可以对退避机制进行调节。

本文中主要研究在信标使能通信方式(beacon-enabled)下采用常见的休眠唤醒方式工作的 WSN 中的病毒传播以及不考虑病毒数据包的多跳传播。网络建立好之后，节点需要周期性地广播信标帧，如果一个节点需要发送数据包，则其需要在收到信标帧后进行网络同步，定位各个时槽，然后采用基于时槽的 CSMA-CA 信道访问机制在竞争时段内进行信道竞争访问，即节点在发送数据包前先退避一个随机的 0 到 $2^{BE}-1$ 间的时间片(BE 默认为 3)，如果退避后信道依然被占用，则将退避系数加 1。重复该过程，直到 BE 达到最大值 aMaxBE(默认为 5)或一个固定最大值 macMaxCSMABackoffs 时发送失败。

每个节点在其工作周期内监听信道一段时间(如 10%的周期时间)，其余的时间(如 90%的周期时间)节点进入休眠状态，以节约能耗，节点的监听时间周期比例(duty cycle)为一个工作周期时间内监听时间与总时间的比例。

4　传播模型

在 WSN 中的部分节点被病毒感染后，为能够快速将病毒在网络中扩散，感染节点将会以 WSN 正常通信机制将病毒添加到正常数据包中向通信范围内的所有节点进行广播。当一个传感器节点接收到包含病毒的数据包后，该病毒会尝试利用系统漏洞来感染控制该节点，根据文献[1]的实验，此过程通常都需要重新启动该传感器节点，使得恶意程序能够写入程序内存区，以获得传感器的完全控制权。考虑到传感器节点的系统稳定性和散布地点环境情况的差异性，传感器节点在被病毒数据包感染后重启会出现故障，无法使用。

由于一般 WSN 应用往往部署在无人值守的环境，难以对节点进行及时免疫，因此不考虑节点的免疫恢复过程。考虑到节点在感染病毒时需要一定的重启时间，结合传染病建模理念，建立 WSN 中具有感染时延的病毒传播模型——SID(Susceptible-Infected-Dead)模型，网络中节点总数为 N，根据目前的 WSN 中各节点的状态，节点可以分为以下 3 种类型的集合：

(1)易感节点集合 S：未被病毒感染且具有系统漏洞的节点(Susceptible Nodes)集合。

(2)感染节点集合 I：被病毒成功感染，并能够向其他节点发送病毒数据包的节点(Infected Nodes)集合。

(3)死亡节点集合 D：在感染重启过程中出现故障而无法使用的节点(Dead Nodes)集合。

于是有：

$$S(t)+I(t)+D(t)=N \quad (6)$$

这里结合实际的 WSN 部署情况，做出下述的病毒传播假设：网络中共有 N 个传感器节点。首先网络中的少部分传感器节点 n_0 个被病毒感染，开始向其信号覆盖范围内的所有节点广播病毒数据包。收到病毒数据包的易感节点在处理数据包后，进行感染后重启，假设感染后重启所需时间为 Δt。该节点重启后有 ρ_I 的概率变为感染节点并加入感染节点集合 I，继续传播病毒；有 ρ_D 的概率出现重启故障，变为死亡节点并加入死亡节点集合 D，不再接收数据包也不再发送数据包；有 ρ_S 的概率在感染后重启之后没有被感染，仍然能够正常工作，留在易感节点集合 S。由于 WSN 中病毒传播速度一般较快，因此本文中不考虑因能量耗尽而造成的节点死亡。

从而有 SID 的理想传播模型如下：

$$\begin{cases}\dfrac{dI(t)}{dt}=\rho_I S(t-\Delta t)I(t-\Delta t)\\ \dfrac{dS(t)}{dt}=-(\rho_D+\rho_I)S(t-\Delta t)I(t-\Delta t)\\ \dfrac{dD(t)}{dt}=\rho_D S(t-\Delta t)I(t-\Delta t)\end{cases} \quad (7)$$

其中传感器节点的状态转换如图 2 所示。

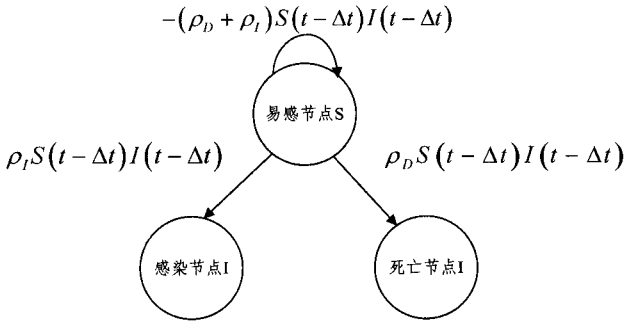


图 2　传感器节点的感染状态转换关系

5　仿真实验

采用上文提出的 SID 模型对病毒数据包在 WSN 中传播并感染传感器节点的情况进行了仿真实验分析。本文使用澳大利亚 NICTA 研究院开发的 Castalia 开源 WSN 模拟器，在一个平面的区域中散布传感器节点，每次仿真初始感染节点都选择网络中角落的传感器节点，将 SID 病毒传播模型在 Castalia 中予以实现，并仿真不同情况下病毒数据包在 WSN 中传播并感染传感器的节点过程。仿真实验中所需的主要仿真参数如表 1 所列，其中括号内为默认的参数值。

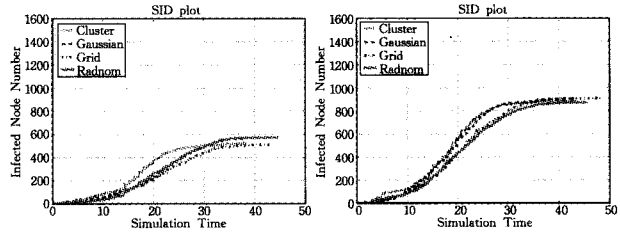
表 1　仿真实验主要参数设置

Parameter (unit)	Value
Number of nodes	1600
Area (m^2)	200×200
Simulation time (s)	50
Node restart time Δt (s)	1
Send interval (s)	0.1
Listen interval (s)	0.1
Beacon Interval Fraction	1
TxOutput Power (dBm)	−1,−5,(−10)
Duty cycle	(0.1),0.2,0.5
Infected probability ρ_I	0.3,0.5,(0.7)
Initial infected node	(1),2,4
Susceptible probability ρ_S	0.1
Death probability ρ_D	$1-0.1-\rho_I$

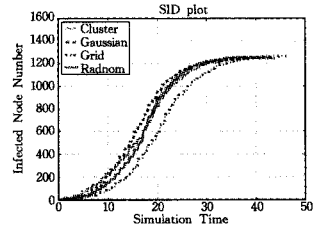
5.1　节点分布情况对病毒传播的影响

本部分中实验仿真暂时忽略通信机制的差异性，采用参数：节点一个周期内监听信道时间所占总时间的比例 duty cycle=0.1，节点发射功率 TxOutPower=−10dBm，初始的感染节点只有一个，即拓扑图中最左下角的节点为初始感染节点，选取方法为横纵坐标和最小：$\min(x+y)$。分别对 4 种散布情况的 WSN 进行模拟，散布方法如第 3 节中所述，拓扑参数如图 1 中设置。

图 3(a)－图 3(c)分别为病毒感染率 $\rho_I=0.3$、$\rho_I=0.5$、$\rho_I=0.7$ 时 3 种不同分布情况下感染节点数目的变化状况。在感染率相对较低($\rho_I=0.3$、$\rho_I=0.5$)时，簇分布的 WSN 中病毒传播较为迅速。而随着感染率的升高($\rho_I=0.5$、$\rho_I=0.7$)，高斯分布情况下的病毒传播更加迅速，这也是因为这两种散布方式都使得局部节点聚集，加快了中期的病毒传播速度，而在簇分布的情况下即使只有较低的感染率，病毒也能快速传播。说明这种散布方式面临的病毒快速扩散的风险很高，而实际环境中传感器节点很多都采用簇结构分布，这也相应加快了病毒的传播，有必要采取适当的措施来避免病毒瘫痪整个网络。而随机格状分布情况的病毒传播速度较慢，这与节点间的平均距离间隔较大有关，降低了传播速度。



(a)感染率 $\rho_I=0.3$，死亡率 $\rho_D=0.6$　(b) 感染率 $\rho_I=0.5$，死亡率 $\rho_D=0.4$



(c) 感染率 $\rho_I=0.7$，死亡率 $\rho_D=0.2$

图 3　节点散布情况对病毒传播的影响

5.2　初始感染节点对病毒传播的影响

本部分实验中 WSN 的节点分布选取均匀随机分布，来考察初始感染节点的位置和数目对病毒传播的影响，采用参数：duty cycle=0.1，TxOutPower=−10dBm，病毒感染率取 $\rho_I=0.7$。分别考察初始感染节点数目为 1 个(平面区域中左下角节点)、2 个(平面区域左下角和右上角节点)、4 个(平面区域 4 个角落节点)的情况。从图 4 中可以看出，随着初始节点的增多，病毒传播速度明显加快。

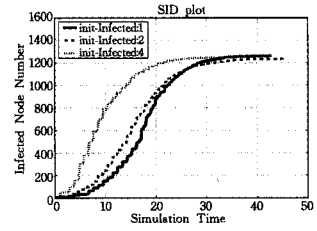


图 4　初始感染节点对病毒传播的影响

5.3　网络通信机制对病毒传播的影响

本部分实验中 WSN 的节点分布选取均匀随机分布来分别考察节点发射功率 TxOutPower 和监听时间周期比例 duty cycle 对病毒传播的影响，设定节点感染率为 $\rho_I=0.7$，初始感染节点选择区域左下角单个节点。

图 5 示出在 3 种不同的节点发射功率(TxOutPower=−1dBm，−5dBm，−10dBm)的情况下，WSN 中的感染节点数目的变化情况，其中 duty cycle=0.1。当节点的发射功率不同时，相应的节点通讯覆盖面积也有较大差别，当 TxOutPower=−1dBm 时，节点的通讯覆盖面积要远大于 TxOutPower=−10dBm 的情况，然而相应的节点能量消耗也会大幅增加。在图 5 中可以看到，在相同的感染率和初始节点情况下，节点的发射功率越高病毒感染速度越快，在仿真时间到

20s 时，TxOutPower=－1dBm 条件下感染的节点数目接近 TxOutPower=－10dBm 情况下的一倍。

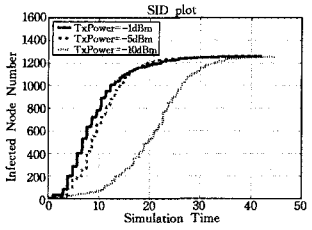


图 5　节点发射功率对病毒传播的影响

图 6 示出不同的节点监听时间周期比例(duty cycle=0.1,0.2,0.5)情况下，WSN 中的感染节点数目的变化情况，其中 TxOutPower=－10dBm。当 duty cycle 较大时，节点有更多的监听时间，能够减少数据包的延时，也同时加快了病毒数据包在 WSN 中的传播。当 duty cycle 取 0.1 时，病毒可以在 10s 左右扩散到整个 WSN 中，其余节点应为死亡节点，而且传播所消耗的时间大多为节点感染重启所用时间，可见 duty cycle 增大会极大地加快病毒传播速度。但一般的 WSN 应用中考虑到节约能量使用情况，会将 duty cycle 设置较小，这也会比较明显地降低病毒传播速度，对病毒传播可以起到一定的抑制作用。

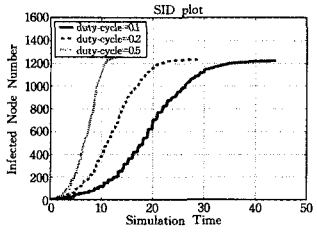


图 6　节点休眠时间比例对病毒传播的影响

结束语　通过分析 WSN 的基本特征，结合病毒的具体感染过程特点，建立了 WSN 中的病毒传播 SID 模型。重点研究了 WSN 的节点空间分布方式、无线通信机制等对病毒在 WSN 中传播的影响。仿真结果表明，本文中的 SID 模型能够较好地针对 WSN 特征描述病毒在 WSN 中传播的动态性。WSN 网络的散布情况会对病毒传播产生较大影响，休眠唤醒工作模式的采用能够相应抑制病毒的传播速度。文中 SID 对病毒在 WSN 中传播的模拟分析为病毒的防御机制研究提供了基础。WSN 中病毒的有效侦测以及对病毒的控制机制将是下一步研究的重点。

参 考 文 献

[1] Yang Yi, Zhu Sen-cun, Cao Guo-hong. Improving sensor network immunity under worm attacks: a software diversity approach [C]// Proceedings of the 9th ACM international symposium on Mobile ad hoc networking and computing. 2008: 149-158

[2] Gu Qi-jun, Noorani R. Towards self-propagate mal-packets in sensor networks[C]// Proceedings of the first ACM Conference on Wireless Network Security. 2008

[3] Khayam S A, Radha H. Using Signal Processing Techniques to Model Worm Propagation over Wireless Sensor Networks [J]. IEEE Signal Processing Magazine, 2006, 23(2): 164-169

[4] Khayam S A, Radha H. A topologically-aware worm propagation model for wireless sensor networks [C]// Distributed Computing Systems Workshops. 2005. 25th IEEE International Conference. 2005: 210-216

[5] De P, Liu Yong-he, Das S K. Deployment-aware modeling of node compromise spread in wireless sensor networks using epidemic theory [J]. ACM Transactions on Sensor Networks, 2009, 5(3): 413-425

[6] Bo Sun, Yan Guan-hua, Yang Xiao. Self-propagating mal-packets in wireless sensor network: Dynamics and Defense Implications [J]. Ad Hoc Networks, 2009, 7(8): 1489-1500

[7] Wang Xia9o-ming, Li Ying-shu. An Improved SIR Model for Analyzing the Dynamics of Worm Propagation in Wireless Sensor Networks [J]. Chinese Journal of Electronics, 2009, 18(1): 8-12

[8] 宋玉蓉，蒋国平. 无线传感器网络中恶意软件传播研究[J]. 南京邮电大学学报：自然科学版，2009，4：1-7

(上接第 182 页)

网络，完成数据模型的建立，保证入侵检测的准确性。仿真实验表明，这种无监督入侵检测模型方法，克服了高校网络外网访问数据的识别特性不明显，提高了高校网络入侵检测的准确率，具有一定的使用价值。

参 考 文 献

[1] 徐子豪，张腾飞. 基于语音识别和无线传感网络的智能家居系统设计[J]. 计算机测量与控制，2012(01)

[2] Deng H, Zeng P-A, Agrawal D P. An Unsupervised Network Anomaly Detection System Using Random Projection Technique [C]// Proceedings of the 2003 International Workshop on Cryptology and Network Security. 2003: 593-598

[3] 李辉，等. 基于支撑向量机的网络入侵检测[J]. 计算机研究与发展，2003，40(6)：799-807

[4] Du H, Jiao L, Wang S. Clonal Operator and Antibody Clone Algorithms[J]. Proceedings of the Firs! International Conference on Machine Learning and Cybernetics, 2002, 4(11): 506-510

[5] 杨杰，李中文. 神经网络在高校科研能力中的评价研究[J]. 计算机仿真，2011(5)：384-387

[6] 田俊峰，张晶，毕志明. 基于改进 RBF 神经网络的入侵检测研究[J]. 计算机工程与应用，2008，44(31)：135-138

[7] 孙晓艳，郑淑丽，沈洪伟. 优化的 RBF 神经网络在入侵检测中的应用[J]. 合肥工业大学学报：自然科学版，2008，31(11)：1794-1797

[8] 康世瑜. 基于数据挖掘和特征选择的入侵检测模型[J]. 微电子学与计算机，2011(8)

[9] 唐鑫，高博. 高校校园网安全性研究与对策[J]. 重庆理工大学学报：自然科学版，2011，25(2)：91-95