有向天线的无线传感器网络病毒传播模型

胡金涛[1] 宋玉蓉[1] 苏晓萍[2]
(南京邮电大学自动化学院 南京 210046)[1] (南京工业职业技术学院计算机与软件学院 南京 210046)[2]

摘 要 采用定向感知天线模型建立基于有向天线的无线传感器网络中的病毒传播模型,通过智能监视节点广播的切换天线消息触发无线传感器网络节点使用有向天线,以研究无线传感器网络中的病毒传播。研究结果表明:使用有向天线不仅能够节约传感器节点能量,延长网络生命周期,还能够有效抑制病毒传播,减小无线传感器网络中病毒大规模爆发的风险,而且该模型适用于不同的病毒传播模型和不同结构的无线传感器网络。

关键词 无线传感器网络,有向天线,病毒,传播模型
中图法分类号 N94,TP391 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.5.024

Model of Virus Propagation in Wireless Sensor Network Based on Directional Antenna

HU Jin-tao[1] SONG Yu-rong[1] SU Xiao-ping[2]
(College of Automation, Nanjing University of Posts and Telecommunications, Nanjing 210046, China)[1]
(School of Computer & Software Engineering, Nanjing Institute of Industry Technology, Nanjing 210046, China)[2]

Abstract In this paper, the model of virus propagation in the wireless sensor networks was established based on the model of directional antenna. The nodes in the wireless sensor networks were triggered by the message of switching antenna broadcasted by the intelligent monitoring nodes to use directional antenna, which was used to study the virus propagation in the wireless sensor networks. The results of research show that using directional antenna not only saves the sensor energy and prolongs the life cycle of networks, but also effectively inhibits the virus propagation, reduces the risk of virus outbreaks in the wireless sensor networks, and the proposed model is suitable for different model of virus propagation and wireless sensor networks with different structure.

Keywords Wireless sensor network, Directional antenna, Virus, Propagation model

1 引言

无线传感器网络(Wireless Sensor Network, WSN)是由无线传感器节点通过自组织方式构成的无线网络,具有网络规模大、节点数量多和计算资源受限等特征,因此解决无线传感器网络的安全问题面临着巨大挑战[1]。随着红外、超声波等技术的发展,现代传感器的天线被设计成有向天线[2,3]。节点使用有向感知模型进行数据采集和链路通信,以此来减少节点能量消耗,延长网络生命周期。近年来,研究者对有向无线传感器网络的研究局限于网络的覆盖度和连通度[4-6],忽略了网络安全问题。然而,无线传感器通常部署在偏远或交通不便的环境中,节点能量有限、拓扑结构动态变化等因素使无线传感器网络极易受到各种攻击,从而导致网络无法正常工作。

自2000年以来,Pastor R等人研究了流行病在人群中的传播行为和特征,提出了以SI(Susceptible-Infected)、SIR(Susceptible-Infected-Recovered)、SIS(Susceptible-Infected-Susceptible)为代表的一系列病毒传播模型[7-9]。近年来,诸多学者对无线传感器网络中的病毒传播行为进行大量研究。Khayam S A等建立具有拓扑意识的蠕虫传播模型(TWPM),该模型描述蠕虫时空动态传播特性[10]。Song Y等人利用二维元胞自动机建立恶意软件动态传播模型[11],提出恶意软件传播过程会呈现邻居饱和现象,而且这种现象最终会限制恶意软件传播,这也使传播速度逐渐减缓。Guo W利用空间相关度建立蠕虫传播的数学模型[12],通过实验仿真分析了网络中传感器节点的分布、网络中蠕虫的传播速度以及感染节点的位置。Tang S等人利用传感器节点的睡眠调度机制建立SIS模型[13],模型中在每个传感器节点上安装病毒查杀程序,当传感器即将进入睡眠状态时启动杀毒程序,以此来抑制网络中的病毒传播;同时还指出该模型适用于各种网络,如社交网络、Internet网络和无线网络。Peng S等人利用元胞自动机建立蠕虫传播模型[14],在该模型中提出评价感染节点感染强度的感染因子和易感节点抵抗强度的抵抗因子。Mishra B K等人提出SEIQRS-V(Susceptible-Exposed-Infectious-Quarantine-Recovered with a Vaccination)模型[15],讨论了病毒爆发的阈值、平衡点和传播的稳定性,同时数值仿真结果表明检疫能够孤立感染节点,免疫能够暂时减缓蠕虫的传播速度。上述都是基于全向天线的无线网络中的病毒传播进

到稿日期:2015-03-18 返修日期:2015-07-29 本文受国家自然科学基金(61373136,61374180),教育部人文社科规划基金(12YJAZH120),江苏省"六大人才高峰"高层次人才项目(RLD201212),南京工业职业技术学院重大项目(YK13-02-03)资助。
胡金涛(1988-),男,硕士生,主要研究方向为无线传感器网络中恶意软件传播及免疫控制策略,E-mail:hujintao88@163.com;宋玉蓉(1971-),女,博士,教授,主要研究方向为复杂网络病毒传播和信息安全;苏晓萍(1971-),女,博士,教授,主要研究方向为复杂网络信息传播。

行研究，Hu L 等人提出使用有向天线抑制虫洞攻击[16]，还提出一种合作协议用来识别健康的邻居节点，实验结果表明此方法能够有效抑制虫洞攻击。Panyim K 等人基于密钥预分布机制使用有向天线建立安全链路[17]，实验表明该方法能够抑制 WSN 中的人工攻击。

目前，大多数关于无线传感器网络中病毒传播的研究主要在具有全向天线的无线传感器网络中展开，针对具有有向天线的无线传感器网络中病毒传播的研究甚少。考虑到在一些附加硬件设备（如云平台）的支持下，传感器可以将全向天线切换到不同的感知方向。本文通过触发使用有向天线分析无线传感器网络中的病毒传播，建立 SI 病毒传播模型，研究无线传感器网络中的病毒传播，通过实验仿真分析触发使用有向天线对网络中病毒传播的影响。

2 具有有向天线的无线传感器网络模型

2.1 无线传感器网络模型

考虑到在一个无线传感器网络中，N 个配有全向天线的无线传感器节点随机均匀分布在一个 $L\times L$ 的平面网格内。从复杂网络理论的角度来看，无线传感器网络是一个时空相关网络，网络中节点之间的相互作用是它们的空间距离的函数[18]，节点 n 接收到来自节点 m 的信号强度在空间中会随着它们之间距离的增加而衰减。表示如下：

$$P_{mn}=\frac{P_m}{Cd_{mn}^{\alpha}} \tag{1}$$

其中，P_m 为节点 m 的发射功率，d_{mn} 为节点 m 与节点 n 之间的欧几里得距离，C 为节点间通信信道的衰减因子（是一个受传输频率等其他多个因素影响的常数），P_{mn} 为节点 n 接收来自节点 m 信号的接收功率。通常对自由空间传播而言，α 取 2，根据不同的传输环境，其取值范围为 2～5[19]。当式(2)成立时，节点 m 与节点 n 能建立一条通信链路，即节点 n 能正确接收来自节点 m 发送的数据。其中，l 为节点 n 处的噪声电平，β_0 为衰减临界值。

$$\frac{P_{mn}}{l}=\frac{P_m}{Cd_{mn}^{\alpha}l}\geqslant\beta_0 \tag{2}$$

由式(2)可得到节点 m 的最大传输距离 d_{mn}：

$$d_{mn}=\left(\frac{P_m}{C\beta_0 l}\right)^{\frac{1}{\alpha}} \tag{3}$$

2.2 有向天线模型

无线传感器的感知通信模式分为全向感知全向通信、有向感知全向通信、有向感知有向通信、全向感知有向通信[2]。本文选取全向感知有向通信模式，将传感器有向天线抽象为如图 1 所示的天线模型[20]，利用扇形区域描述有向传感器节点的天线方向。

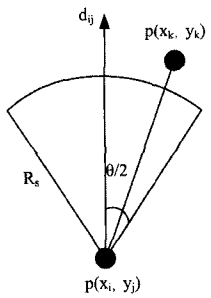


图 1 传感器天线模型

传感器节点 W_i 可以用一个四元组来表示，如式(4)所示，其中 $P(x_i,y_i)$ 表示传感器节点在二维空间的坐标位置，R_s 表示传感器节点的最大通信半径，θ 表示传感器节点的方向角，d_{ij} 表示有向天线的方向向量。当满足(5)时节点 k 为节点 i 的邻居节点。

$$W_i=\{p(x_i,y_i),d_{ij},R_s,\theta\} \tag{4}$$

$$\begin{cases}\vec{v_{ik}}=\vec{t_k}-\vec{l_i}\\ \vec{d_{ij}^{T}}\cdot\vec{v_{ik}}\geqslant\|\vec{v_{ik}}\|_2\cos\left(\frac{\theta}{2}\right)\\ \|\vec{v_{ik}}\|_2\leqslant R_s\end{cases} \tag{5}$$

无传感器节点使用有向天线时，其通信距离、方向角以及信号增益之间的关系如表 1 所列[17]。

表 1 不同方向角对应的通信范围

方向角 θ	增益(G/dBi)	通信距离(m)
360°	0	40
120°	1.2	43
90°	6	57.84
60°	10.8	77.70
30°	17.5	117.31

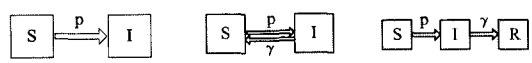
2.3 介质访问控制方法

当无线信道作为无线传感器网络的传输介质时难免会出现数据信号发生碰撞，因此必须要解决传感器节点争用信道的问题以保证数据正确发送。无线网络介质访问控制(MAC)方法具体为：当某传感器节点监听到信道空闲时，随机退避一段时间后再次发送数据，当一个节点发送数据时其邻居节点均不能发送数据，只能在监听到信道空闲时才进行数据发送。无线传感器网络中的恶意软件传播也必须遵循介质访问控制方法，因此本文采用冲突避免方式进行介质访问控制。

3 无线传感器网络中的病毒传播模型

3.1 病毒传播模型

本文主要研究触发使用有向天线对无线传感器网络中病毒传播的影响，采用 SI、SIS、SIR 病毒传播模型描述病毒在无线传感器网络中的传播。SI 模型如图 2(a)所示，初始网络中传感器节点处于健康状态(S)，当传感器节点受到病毒感染处于感染状态(I)时，感染节点以概率 p 感染其邻居节点，病毒通过这种方式在网络中传播。SIS 模型如图 2(b)所示，当节点受到病毒攻击时会以概率 p 被感染处于感染状态，其中概率 p 的大小与病毒攻击能力和传感器自身安全防御能力有关。一般传感器节点内部装有简单查杀病毒程序，或者当传感器节点受到病毒入侵时会自动重新启动以删除病毒程序，在此情况下被感染的节点会以概率 γ 恢复到健康状态，且恢复到健康状态的节点能继续被感染，其中恢复概率 γ 与传感器自身病毒查杀能力有关。SIR 模型如图 2(c)所示，当节点受到病毒攻击时会以概率 p 被感染处于感染状态。当传感器节点内部的杀毒程序对该病毒有免疫作用时，被感染的节点会以概率 γ 恢复到免疫状态(R)。处于此状态的节点对病毒有免疫作用，不会再被同种病毒感染。



(a)SI 病毒传播模型 (b)SIS 病毒传播模型 (c)SIR 病毒传播模型

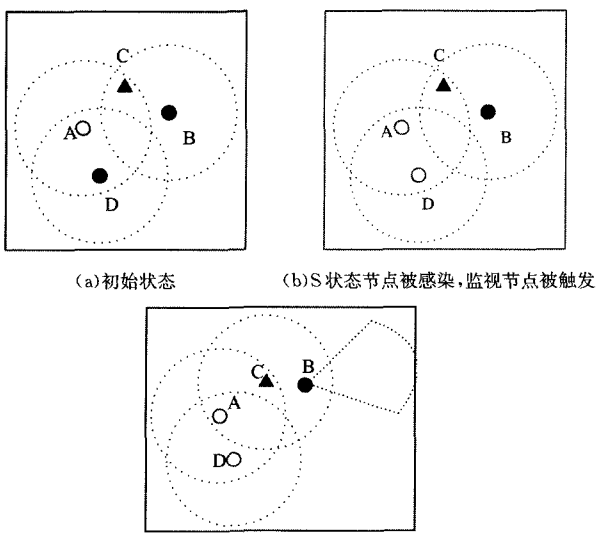
图 2 病毒传播模型

3.2 触发使用有向天线的 WSN 中病毒传播模型

(1)初始时,配有全向天线的无线传感器节点通过人工随机散布在监测区域(此部分只为描述传播模型,取少许节点以作说明),其中包含一个或多个传感器监视节点,该监视节点能够检测到接收的数据包是否带有病毒。初始时期所有节点处于S状态,当节点受到病毒攻击被感染时将处于I状态,如图3(a)所示,节点 A 为处于I状态的节点,节点 B 和 D 初始处于S状态,节点 C 为监视节点,处于I状态的节点 A 会向自己所有的邻居节点广播带病毒的数据包。

(2)接收到带病毒数据包的邻居节点一般会以概率 p 被感染成I状态,当带病毒数据包抵达邻居范围内的监视节点时触发该监视节点向邻居节点广播切换天线的消息。如图3(b)所示,节点 D 以概率 p 被感染,节点 C 接收到带病毒数据包,被触发向其邻居节点广播切换天线消息。

(3)监视节点被触发向其邻居节点广播切换天线消息,接收到该消息并且处于S状态的邻居节点会将切换天线的消息广播给自己的邻居,然后将自身的全向天线切换为有向天线(此时该有向天线的方向是随机选择的)。接收到切换天线消息并处于I状态的节点将保持原有的全向天线状态,并继续向其邻居节点传播带病毒的数据包。此时网络中的病毒和切换天线消息可以通过全向天线和有向天线两种方式进行传播。如图3(c)所示,处于S状态的节点 B 接收到监视节点 C 广播的切换天线消息,向其邻居发送该消息之后将自己的全向天线切换为有向天线。有向天线方向的选取机制有3种:随机选取、选取度最大的方向、选取度最小的方向。下文中若不加说明,有向天线方向的选取机制为随机选择。



(a)初始状态　(b)S状态节点被感染,监视节点被触发

(c)触发节点进行天线切换

图3　触发使用有向天线的 WSN 中病毒传播过程

4 算法描述

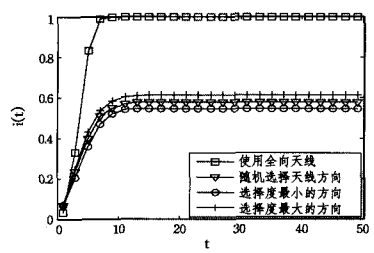
在 $L\times L$ 的区域中随机均匀布散 N 个传感器节点,整个实验中 L 为1000,密度 $\rho=N/L^2$ 为0.005,节点的最大通信半径为 R_s。在实验中假设监视节点不会被感染,且有向天线方向集合中每个方向覆盖范围不重叠。首先构建网络,初始化传感器节点属性值,即用二维数组 *coState*[N][5]存储传感器的坐标位置、感染状态、监视状态和是否收到切换天线消息状态。初始化传感器的天线为全向天线,使用有向天线时用 *derectionFlag*[N]存储每个传感器的天线方向集合。当在分簇结构网络中进行实验时,还要选取初始化簇头节点,用 *cuTout*[i]存储簇头节点。之后随机取若干感染节点进行病毒传播演化,在一定时间步后停止传播。对100次仿真结果取平均值得到最终的仿真结果。基于有向天线的无线传感器网络病毒传播算法描述如下。

1. while round do
2. {coState[i][j] | i=0,1,…,N−1;j=0,1,2,3,4;}//构建并初始化网络。
3. {derectionFlag[i] | i=0,1,…,N−1}//初始化网络中节点的天线为全向天线。
4. {cuTout[i] | i=0,1,…,N−1}//选举并标识簇头节点,此步骤在分簇网络中执行。
5. while t do
6. cuTout[i]=selectCutou(cuTout[i]) //以 Ta 为周期选举簇头节点,此步骤在分簇网络中执行。
7. {coState[i][j],derectionFlag[i]}=changeDerction(coState[i][j],derectionFlag[i]);//天线的切换和切换天线消息的传播,即更新 coState[i][4]和 derectionFlag[i]的值。
8. coState[i][j]=infecting(coState[i][j],derectionFlag[i])//病毒的传播演化,即更新 coState[i][2]的值。
9. coState[i][j]=recovering(coState[i][j])//感染病毒的节点恢复成S态或R态,在SI模型中不执行。
10. c=couter(coState[i][j])// 统计 t 时刻网络中感染消息的传感器所占比例。
11. t−−
12. end while
13. round−−
14. end while

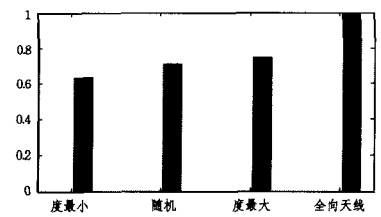
5 仿真分析

5.1 选择触发使用有向天线

本文首先基于SI病毒传播模型,通过仿真分析网络中所有节点在初始时使用有向天线对正常数据包收发的影响,从而选择触发使用有向天线。



(a)病毒演化情况



(b)正常数据包成功发送比例

图4　全部节点使用有向天线和使用全向天线对网络中病毒传播和正常数据包发送的影响

图4(a)是在 L 为20、方向角 θ 为90°、最大通信半径 R_s 为3、密度 ρ 为0.5、感染概率 p 为0.5时病毒的传播演化情

况，传感器天线的方向选取方式分为随机选取、选取度最大和度最小的方向。如图 4(a)所示，全部节点使用有向天线的网络中感染病毒的节点比例比使用全向天线的网络中感染病毒的节点比例低。图 4(b)显示在上述参数下正常数据包成功抵达汇聚节点所占比例。如图 4(b)所示，全部节点使用有向天线的网络中成功发送的数据包比例比使用全向天线的网络低。由图 4 可以看出，当网络中所有节点使用有向天线时，在一定程度上能够很好地抑制病毒的传播，但是同时也使正常数据包的发送受到很大影响。原因是当网络节点全部使用有向天线时，网络的连通度很差，从而导致数据包的收发受到阻碍。因此本文在网络中增添监视节点，触发部分节点切换为有向天线。为简便起见，后文中有向天线皆为触发使用有向天线。

5.2 平面无线传感器网络病毒传播

5.2.1 触发使用有向天线对传播过程的影响

取参数 L 为 1000，考虑病毒的感染能力和传感器自身的抵御能力取 p 为 0.3，节点个数 N 为 5000，全向天线的最大通信半径 R_o 为 40，方向角 θ 为 90°，网络中有一个初始感染节点和一个监视节点。同时与相同参数下基于全向天线的平面传感器网络中病毒传播过程进行比较。仿真结果如图 5 所示，圆圈连线表示有向天线网络中处于感染状态的节点所占比例随时间的变化趋势，三角连线表示全向天线网络中处于感染状态的节点所占比例随时间的变化趋势。由图可知在有向天线网络中病毒传播速度减慢，而且最终被感染的节点数量较全向天线网络的少。由此可知有向天线能够抑制网络中的病毒传播。由图 5 中的内嵌图可知在 10 时间步监视节点受到触发，并且向网络广播切换天线的消息，所以在 10 时间步时病毒传播开始受到抑制。由于消息传播的速度比病毒传播速度快，接收到消息的节点切换为有向天线，若该节点被感染，其感染的邻居节点数将减少，因此最终被感染的节点数目较低。

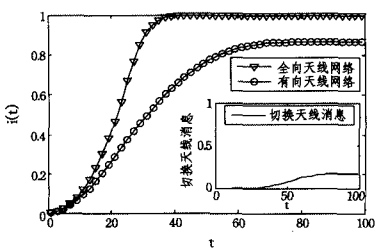


图 5 两种网络中 $i(t)$的变化情况

5.2.2 监视节点个数对传播过程的影响

图 6 为初始监视节点个数分别为 1、2、3 且其他参数不变时，网络中感染病毒节点所占比例随时间的变化情况。

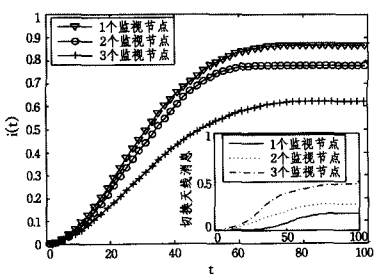


图 6 监视个数不同时 $i(t)$的变化情况

如图 6 所示，三角连线、圆圈连线和十字连线分别表示网络中有 1 个监视节点、2 个监视节点和 3 个监视节点时病毒的传播情况。由图可知，当监视节点个数越多时，文中提出的模型对病毒的抑制效果更好。由图 6 中的内嵌图可知，当监视节点增多，触发监视节点广播切换天线消息的可能性越大，网络中使用有向天线的节点就越多，由于使用有向天线节点的邻居节点较少，单个时间步被感染的节点数就越少，因此病毒传播的速度就越慢，最终感染节点所占比例也就越低。

5.2.3 方向角大小对传播过程的影响

取参数 L 为 1000，传感器节点个数 N 为 5000，全向天线的最大通信半径 R_o 为 40。仿真结果如图 7 所示，三角连线、圆圈连线和星形连线分别表示方向角 θ 分别为 360°、120°、90°时网络中感染病毒节点所占比例随时间的变化情况。由图 7 可知，方向角越小病毒传播的速度越慢。当方向角为 360°时对应网络中所有节点使用全向天线，此时网络中病毒传播速度最快。

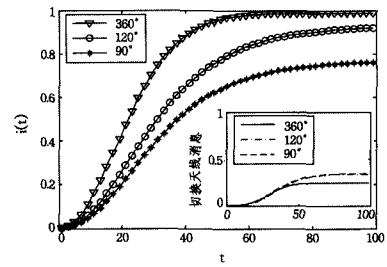


图 7 方向角不同时 $i(t)$的变化情况

5.2.4 有向天线方向的选取机制对病毒传播的影响

本节分析触发使用有向天线时天线方向的选择机制对病毒传播的影响，方向角 θ 为 90°，感染概率 p 为 0.3，其他参数同上。仿真结果如图 8 所示，星形连线、圆圈连线和三角连线分别表示当触发使用有向天线分别选取度最大的方向、度最小的方向和随机选择方向时网络中病毒的传播情况。选择度最大的方向网络中病毒传播速度最快，同时网络中通知邻居节点切换天线的消息传播最快；选择度最小的方向时网络中病毒传播速度最慢，同时网络中通知邻居节点切换天线的消息传播最慢。当选择度最小的方向时，虽然每个时间步接收到切换天线消息的邻居节点数量小，但是在此情况下每个时间步感染病毒的邻居节点数量同样也很小，从而达到了抑制网络中病毒传播的目的。随机选择方向时网络中病毒传播速度介于两者之间，这是因为此时网络节点的度大小接近平均度。

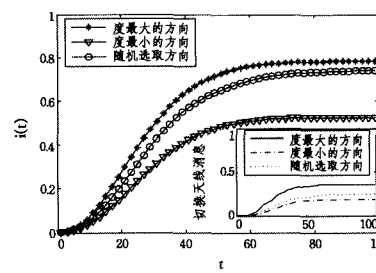


图 8 方向选择机制不同时 $i(t)$的变化情况

5.3 不同病毒传播模型下病毒的传播过程

本节分析在平面传感器网络中采用不同的病毒传播模型时，触发使用有向天线对网络中病毒传播的影响。由上节分析，触发使用有向天线选择度最小的方向时病毒抑制效果最佳，因此在本节触发使用有向天线时选择度最小的方向。方

向角 θ 为 90°，感染概率 p 为 0.3，分别分析采用 SI、SIS、SIR 模型时网络中病毒传播的特性，仿真结果如图 9 所示。图 9 为采用 SI 模型时 $i(t)$ 的变化情况，十字连线和星形连线分别表示触发使用有向天线网络和全向天线网络中病毒传播特性。由图可知触发使用有向天线的网络中处于感染状态的节点数目增加的速度较慢，说明采用 SI 病毒模型时触发使用有向天线能够抑制网络中病毒传播。

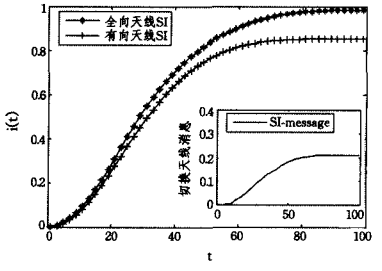


图 9　采用 SI 病毒传播模型时 $i(t)$ 的变化情况

图 10 为采用 SIS 模型时 $i(t)$ 的变化情况，星形连线和方形连线分别表示触发使用有向天线和使用全向天线的网络中病毒传播特性。由图可知触发使用有向天线的网络中处于感染状态的节点数目较少，传播速度慢，表明采用 SIS 病毒传播模型时触发使用有向天线同样能够抑制网络中病毒传播，但此时网络中切换为有向天线的节点数目增多，原因是在病毒传播过程中有部分节点恢复为健康节点，当健康节点接收到切换天线消息时会将自己的全向天线切换为有向天线。

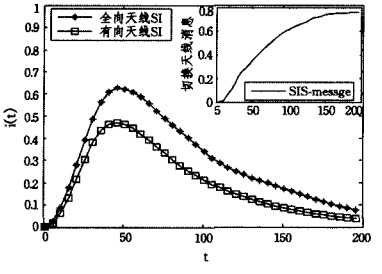


图 10　采用 SIS 病毒传播模型时 $i(t)$ 的变化情况

图 11 为采用 SIR 模型时 $i(t)$ 的变化情况，圆圈连线和星形连线分别表示触发使用有向天线和使用全向天线的网络中病毒传播特性，三角连线和方形连线分别表示触发使用有向天线和使用全向天线的网络中恢复节点的变化曲线。由图可知触发使用有向天线的网络中处于感染状态的节点数目增加的速度较慢，因此恢复节点数目增加的速度较慢。这表明采用 SIR 病毒传播模型时触发使用有向天线的网络中被病毒感染的节点数量较小。由此可知，触发使用有向天线在不同的病毒传播模型中都能很好地抑制病毒传播。

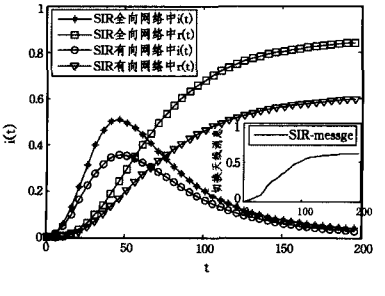


图 11　采用 SIR 病毒传播模型时 $i(t)$ 和 $r(t)$ 的变化情况

5.4　基于有向天线的 GAF 分簇网络中病毒传播

本节通过数值仿真，分析在分簇网络结构中触发使用有向天线对病毒传播的影响，有向天线的方向选取机制为随机选取。取方向角 θ 为 120°，其他参数不变。图 12 中，星形连线、三角连线和圆圈连线分别表示使用全向天线（即监视节点个数为 0）、使用有向天线时有 1 个监视节点和 2 个监视节点的 GAF 分簇网络病毒传播过程。由图 10 可知使用有向天线同样能够抑制 GAF 分簇网络中的病毒传播，而且当监视节点个数增加时网络中病毒传播的速度会减慢；同时也说明本文提出的模型适用于不同结构的网络。

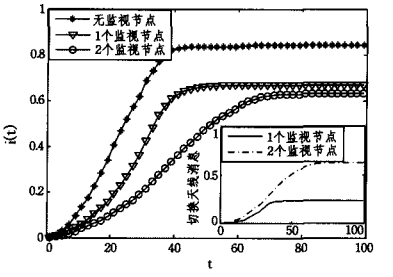


图 12　基于有向天线的 GAF 分簇网络中 $i(t)$ 的变化情况

结束语　本文提出触发使用有向天线研究无线传感器网络中的病毒传播，建立无线传感器网络中病毒传播的 SI 模型，分析在该模型下病毒传播的特性，并且与使用全向天线的无线传感器网络中的病毒传播进行比较。仿真结果表明：触发使用有向天线能够有效抑制网络中的病毒传播，减小无线传感器网络中病毒大规模爆发的风险。本文还将此模型应用于 GAF 分簇网络，仿真结果表明在分簇网络中触发使用有向天线同样能够抑制病毒传播；而且该模型适用于不同结构的网络，在不同的病毒传播模型下都能达到抑制病毒传播的效果。研究结果还指出增加监视节点的个数、减小方向角的角度、触发使用有向天线时选取度最小的方向也能够有效抑制无线传感器网络中的病毒传播。

参 考 文 献

[1] Perrig A, Stankovic J, Wagner D. Security in Wireless Sensor Networks[J]. Communications of the ACM, 2004, 47(6): 53-57

[2] Liang J, Liu M, Kui X. A Survey of Coverage Problems in Wireless Sensor Networks[J]. Sensors & Transducers Journal, 2014, 76(7): 326-334

[3] Tao D, Ma H D. The Controlling Algorithm of Coverage in Wireless Sensor Networks[J]. Journal of Software, 2011, 22(10): 2317-2334(in Chinese)
陶丹，马华东. 有向传感器网络覆盖控制算法[J]. 软件学报，2011，22(10)：2317-2334

[4] Amac Guvensan M, Gokhan Yavuz A. On Coverage issues in Directional Sensor Networks: A survey[J]. Ad Hoc Networks, 2011, 9(7): 1238-1255

[5] Kranakis E, MacQuarrie F, Maffra I K T, et al. Strong Connectivity of Wireless Sensor Networks with Double Directional Antennae in 3D[M]// Ad-hoc, Mobile, and Wireless Network. Springer Berlin Heidelberg, 2013: 257-268

[6] Wu M C, Lu W F. On Target Coverage Problem of Angle Rotatable Directional Sensor Networks[C]// 2013 Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing(IMIS). IEEE, 2013: 605-610

（下转第 145 页）

gorithm for Reputation Managementin P2P Networks[C]//Proceedings of the International Conference on WWW. Budapest, Hungary, 2003

[3] Wang Jin-dong, Wei Bo, Zhang Heng-wei, et al. Research on Service Trust Evaluation Approach under Cloud Computing Environment[J]. Computer Science, 2014, 41(12): 38-42(in Chinese)
王晋东,卫波,张恒巍,等. 云计算环境下服务信任评估方法研究[J]. 计算机科学,2014,41(12):38-42

[4] Tian Chun-qi, Yang Bai-jian. R^2 Trust, a Reputation and Risk Based Trust Management Framework For Large-Scale, Fully Decentralized Overlay Networks[J]. Future Generation Computer Systems, 2011, 27(8): 1135-1141

[5] Zhang Ming-qing, Fan Tao, Tang Jun, et al. Agent-based simulation of trust model in distributed system[J]. Computer Engineering & Design, 2014, 35(9): 3202-3206(in Chinese)
张明清,范涛,唐俊,等. 基于 Agent 的分布式系统信任模型仿真[J]. 计算机工程与设计,2014,35(9):3202-3206

[6] Tian Jun-feng, Cai Hong-yun. Actuality and Development of Trust Model[J]. Journal of Hebei University(Natural Science Edition), 2011, 31(5): 555-560(in Chinese)
田俊峰,蔡红云. 信任模型现状及进展[J]. 河北大学学报(自然科学版),2011,31(5):555-560

[7] Chang E, Thomson P, Dilion, et al. The Fuzzy and Dynamic Nature of Trust[M]//Trust, Privacy, and Security in Digital Business(LNCS 3592). Berlin: Springer-Verlag, 2005: 161-174

[8] Li Xiao-yong, Gui Xiao-lin. Trust Quantitative Model with Multiple Decision Factors in Trusted Network[J]. Chinese Journal of Computers, 2009, 32(3): 405-416(in Chinese)
李小勇,桂小林. 可信网络中基于多维决策属性的信任量化模型[J]. 计算机学报,2009,32(3):405-416

[9] Vu L H, Hauswirth M, Aberer K. QoS-Based service selection and ranking with trust and reputation management[C]//Meersman R, Tari Z, eds. Proc. of the OTM 2005(LNCS 3760). 2005: 466-483

[10] Ali A S, Ludwig S A, Rana O F. A cognitive trust-based approach for Web service discovery and selection[C]//Proc. of the 3rd European Conf. on Web Services. 2005: 38-49

[11] Day J, Deters R. Selecting the best Web service[C]//Proc. of the 14th Annual IBM Centers for Advanced Studies Conf.. 2004: 293-307

[12] Billhardt H, Hermoso R, Ossowski S, et al. Trust-Based service provider selection in open environments[C]//Proc. of the 22nd Annual ACM Symp. on Applied Computing. New York: ACM Press, 2007: 1375-1380

[13] Page L, Brin S, Motwani R, et al. The PageRank citation ranking: Bringing order to the Web[R/OL]. Stanford Digital Library Technologies Project, 1998. http://ilpubs.stanford.edu:8090/422/

[14] Wang Y, Vassileva J. Trust and reputation model in peer-to-peer networks[C]//Proc. of the 3rd Int'l Conf. on Peer-to-Peer Computing. IEEE Computer Society Press, 2003: 150-157

(上接第 131 页)

[7] Moreno Y, Nekovee M, Vespignani A. Efficiency and Reliability of Epidemic Data Dissemination in Complex Networks[J]. American Physical Sciety, 2004, 69(5): 343-358

[8] Newman M E J. Spread of Epidemic Disease on Networks[J]. Physical Review E Statistical Nonlinear & Soft, Matter Physics, 2002, 66(1): 016128

[9] Pastor-Satorras R, Vespignani A. Epidemic Spreading in Scale-Free Networks[J]. Physical Review Letters, 2001, 86(14): 3200-3203

[10] Khayam S A, Radha H. A Topologically-Aware Worm Propagation Model for Wireless Sensor Networks[C]//25th IEEE International Conference on Distributed Computing Systems Workshops, 2005. IEEE, 2005: 210-216

[11] Song Y, Jiang G P. Model and Dynamic Behavior of Malware Propagation over Wireless Sensor Networks[M]//Complex Sciences. Springer Berlin Heidelberg, 2009: 487-502

[12] Guo W, Zhai L, Guo L, et al. Worm Propagation Control based on Spatial Correlation in Wireless Sensor Network[M]//Web Technologies and Applications. Springer Berlin Heidelberg, 2012: 68-77

[13] Tang S, Myers D, Yuan J. Modified SIS Epidemic Model for Analysis of Virus Spread in Wireless Sensor Networks[J]. International Journal of Wireless and Mobile Computing, 2013, 6(2): 99-108

[14] Peng S, Wang G, Yu S. Modeling the Dynamics of Worm Propagation Using Two-Dimensional Cellular Automata in Smartphones[J]. Journal of Computer and System Sciences, 2013, 79(5): 586-595

[15] Mishra B K, Tyagi I. Defending against Malicious Threats in Wireless Sensor Network: A Mathematical Model[J]. International Journal of Information Technology and Computer Science (IJITCS), 2014, 6(3): 12-19

[16] Hu L, Evans D. Using Directional Antennas to Prevent Wormhole Attacks[C]//NDSS. 2004: 241-245

[17] Panyim K, Krishnamurthy P, Le A. Secure Connectivity through Key Predistribution with Directional Antennas to Cope with Jamming in Sensor Networks[C]//2013 International Symposium on Intelligent Signal Processing and Communications Systems (ISPACS). IEEE, 2013: 471-475

[18] Mickens J W, Noble B D. Modeling Epidemic Spreading in Mobile Environments[C]//Proceedings of the 4th ACM Workshop on Wireless Security. ACM, 2005: 77-86

[19] Pantazis N A, Vergados D J, Vergados D D, et al. Energy efficiency in wireless sensor networks using sleep mode TDMA scheduling[J]. Ad Hoc Networks, 2009, 7(2): 322-343

[20] Ai J, Abouzeid A A. Coverage by Directional Sensors in Randomly Deployed Wireless Sensor Networks[J]. Journal of Combinatorial Optimization, 2006, 11(1): 21-41