



研究与开发

基于博弈论的无线传感器网络恶意程序传播模型

周海平, 沈士根, 黄龙军, 冯晟

(绍兴文理学院计算机科学与工程系, 浙江 绍兴 312000)

摘要: 恶意程序传播是无线传感器网络 (wireless sensor network, WSN) 面临的一类重要安全问题。从博弈论的角度对 WSN 恶意程序传播的微观机理进行分析, 建立了 WSN 的攻防博弈模型, 求出了博弈模型的混合纳什均衡解, 并根据博弈双方的混合纳什均衡策略确定恶意程序的传染概率, 从而建立了 WSN 的恶意程序传播模型。通过使用元胞自动机方法对 WSN 的恶意程序传播过程进行模拟, 揭示了恶意程序的传播速度与博弈参数之间的关系, 研究结果对抑制 WSN 恶意程序传播具有理论指导意义。

关键词: 无线传感器网络; 恶意程序传播; 攻防博弈; 元胞自动机

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2018252

Game theory-based malware propagation model for wireless sensor network

ZHOU Haiping, SHEN Shigen, HUANG Longjun, FENG Sheng

Department of Computer Science and Engineering, Shaoxing University, Shaoxing 312000, China

Abstract: Malware propagation is an important security problem faced by wireless sensor network (WSN). From the perspective of game theory, the microscopic mechanism of malware propagation in WSN was analyzed. The attack-defense game model of WSN was built, and the mixed Nash equilibrium solution of the model was obtained. With the solution, the infection probability of malware was determined and the theoretical model for the malware propagation in WSN was established. Meanwhile, a cellular automata model was proposed to simulate malware propagation process in WSN. Simulation experiments reveal the relationship between the propagation speed and the game parameters. The results of this study are of significance for people to formulate measures to reduce the propagation speed of malware.

Key words: wireless sensor network, malware propagation, attack-defense game, cellular automation

1 引言

无线传感器网络 (wireless sensor network,

WSN) 是由大量分布在不同位置的传感器节点以无线通信的方式组成的信息传输网络。由于 WSN 节点具有布设方便、组网灵活等特点, 目

收稿日期: 2018-04-17; 修回日期: 2018-09-09

基金项目: 国家自然科学基金资助项目 (No.61772018)

Foundation Item: The National Natural Science Foundation of China (No.61772018)



前已经在环境监测、智能交通、森林防火等领域中得到了广泛应用。然而, WSN 很容易受到恶意攻击, 常见的攻击方式有虫洞攻击、女巫攻击、泛洪攻击、选择性转发、恶意程序传播等多种形式^[1-4]。相比其他攻击方式, 恶意程序传播是一种影响范围更大、破坏力更强的攻击方式, 因为传感器节点一旦被恶意程序感染又会向其他节点发送恶意程序, 导致整个网络迅速被恶意程序攻陷^[5-7]。

目前, 恶意程序传播已成为 WSN 安全中的重要研究内容^[8-10]。要控制 WSN 中恶意程序的传播, 一方面要对恶意程序入侵的检测方法和策略进行研究, 另一方面要对恶意程序传播的机理和规律进行研究。目前人们已经在这两个方面分别做了大量研究。在入侵检测方面, 熊自立等人^[11]针对 WSN 面临多种不同攻击方式的特点提出了基于不完全信息博弈的入侵检测模型, 该模型可以使 WSN 在抵御多种攻击的同时降低能耗。周伟伟等人^[12]针对 WSN 资源受限的特性提出了一种多阶段动态入侵检测博弈模型, 该模型通过贝叶斯法则修正每一阶段簇头的信念值, 提高了入侵检测的成功率。参考文献[13]针对 WSN 攻防双方的策略会随时间变化的特点提出了一个基于微分博弈的入侵检测模型, 通过求解博弈模型得到了最优检测策略。参考文献[14]针对入侵检测系统 (intrusion detection system, IDS) 存在误检率的问题提出了一个基于贝叶斯博弈的检测模型, 该模型能够在网络资源受限的情况下提高检测成功率。在恶意程序传播的研究方面, 王小明等人^[15]利用元胞自动机方法对移动无线传感器网络中的恶意数据分组传播行为进行模拟, 揭示了不确定环境下恶意数据分组传播的时空特征。曹玉林等人^[16]将传染病模型应用于 WSN 的病毒传播研究, 他们将易感节点的免疫比例和感染节点的恢复比例作为最优控制变量, 实现了最小成

本开销下最大程度遏制病毒传播的目标。参考文献[17]提出了一个 WSN 的蠕虫病毒传播模型, 研究了通信半径和节点分布密度对病毒传播效果的影响。参考文献[18]对 WSN 中的移动代理被攻击时恶意程序的传播过程进行了研究, 发现在移动代理被攻击的情况下恶意程序更容易扩散。

至今为止, 人们在入侵检测和恶意程序传播这两个方面的研究都是独立开展的, 没有考虑它们之间的关联性。事实上, 这两类问题之间有着不可分割的内在联系。例如, IDS 所采用的检测策略会影响恶意程序对合法节点的攻击成功率, 从而进一步影响恶意程序在 WSN 中的传播速度^[19]。恶意节点与合法节点作为两种智能主体, 两者在攻防过程中会采取理性的策略使自身利益最大化^[20]。基于此, 本文从博弈论的角度对合法节点与恶意节点之间的攻防博弈行为进行分析, 并进一步对博弈策略驱动下的 WSN 恶意程序传播过程进行研究与探讨, 揭示博弈参数与 WSN 恶意程序传播速度之间的关系。

2 WSN 的攻防博弈模型

WSN 由恶意节点与合法节点组成, 其中恶意节点的目的是向合法节点传播恶意程序, 合法节点可以利用 IDS 对接收的信息进行检测。恶意节点为了掩饰自己的攻击行为也会给合法节点发送正常信息。合法节点对收到的信息进行检测需要消耗一定的能量, 由于无线传感器节点由电池供电, 如果合法节点对收到的所有信息都进行检测, 则很快会因能量耗尽而无法工作。因此, 合法节点在决定是否进行检测时需要综合考虑其付出的能耗代价及被攻击的可能性。由此可见, 恶意节点和合法节点的攻防行为其实就是一个博弈过程, 攻防双方会在分析博弈局势的基础上采取对自己最有利的策略。因此, 本文用博弈论的方法对攻防双方的策略进行分析。

定义 1 WSN 中恶意节点与合法节点之间的攻防博弈模型可以表示为一个三元组 $\Xi = [N, \{S_i\}, \{u_i\}]$, 其中:

- N 为博弈的参与者集合, 对于本文来说, $N = \{\text{合法节点}, \text{恶意节点}\}$;
- S_i 为参与者可采取的策略集合, 当 i 为合法节点时, $S_{\text{合法节点}} = \{\text{检测}, \text{不检测}\}$, 当 i 为恶意节点时, $S_{\text{恶意节点}} = \{\text{攻击}, \text{不攻击}\}$, 需要特别指出的是, 这里的不攻击策略并不是指恶意节点不发送任何信息, 而是指其发送正常信息;
- u_i 为参与者 i 在博弈过程中获得的收益, u_i 的值由博弈双方所采取的策略决定。表 1 给出了本文用到的一些符号的定义, 表 2 给出了博弈双方的收益矩阵。

表 1 符号定义

符号	含义
a	合法节点检测到恶意程序获得的收益, 恶意节点被识别造成的损失
b	恶意节点攻击成功带来的收益, 合法节点感染恶意程序造成的损失
e_s	合法节点对收到的信息进行检测所需的能量代价
e_l	恶意节点发送恶意程序或正常信息所消耗的能量代价
x	恶意节点进行攻击的概率
y	合法节点进行检测的概率
Eu_s	合法节点在攻防博弈中的期望收益
Eu_l	恶意节点在攻防博弈中的期望收益

表 2 合法节点与恶意节点的博弈收益函数

合法节点	恶意节点	
	攻击	不攻击
检测	$a - e_s, -a - e_l$	$-e_s, -e_l$
不检测	$-b, b - e_l$	$0, -e_l$

在攻防对抗过程中, 恶意节点向其他节点发送信息(恶意程序或正常信息)需要消耗代价为 e_l 的能量, 合法节点对收到的信息进行检测需要消耗代价为 e_s 的能量, 当恶意节点向合法节点发起

攻击, 合法节点又正好进行检测时, 合法节点会因成功检测出恶意程序而获得价值为 a 的收益, 恶意节点则会因暴露身份而造成代价为 a 的损失。当恶意节点发起攻击, 而合法节点不进行检测时, 恶意节点会因成功传播恶意程序获得价值为 b 的收益, 而合法节点则会因感染恶意程序造成代价为 b 的损失。另外, 为了使博弈有意义, 模型须满足 $a \geq e_s$ 及 $b \geq e_l$ 这两个条件。

由表 2 可知, 若恶意节点发起攻击, 合法节点就应该进行检测, 反之, 合法节点就不应该检测; 而对恶意节点来说, 若合法节点进行开启检测, 它就不应该进行攻击, 反之, 就应该发起攻击。由此可见, 上述博弈模型不存在纯策略纳什均衡解, 下面从混合均衡策略的角度分析博弈双方的攻防行为。

定理 1 由定义 1 建立的 WSN 攻防博弈模型存在混合纳什均衡策略。

证明: 假设恶意节点以概率 x 进行攻击(传播恶意程序), 以概率 $1-x$ 不进行攻击(传播正常信息), 合法节点以概率 y 进行检测, 以概率 $1-y$ 不进行检测, 则根据收益矩阵, 合法节点的期望收益 Eu_s 为:

$$Eu_s = xy(a - e_s) + (1-x)y(-e_s) + x(1-y)(-b) \quad (1)$$

恶意节点的期望收益 Eu_l 为:

$$Eu_l = xy(-a - e_l) + (1-x)y(-e_l) + x(1-y)(b - e_l) + (1-x)(1-y)(-e_l) \quad (2)$$

令 $\frac{\partial Eu_s}{\partial y} = 0$, 得:

$$x(a - e_s) + (1-x)(-e_s) - x(-b) = 0 \quad (3)$$

整理式 (3) 得:

$$x = \frac{e_s}{a + b} \quad (4)$$

当 $x = \frac{e_s}{a + b}$ 时, $\frac{\partial Eu_s}{\partial y} = 0$, 合法节点进行检测的期望收益等于不进行检测的期望收益;

当 $x > \frac{e_s}{a + b}$ 时, $\frac{\partial Eu_s}{\partial y} > 0$, 合法节点进行检



测的期望收益大于不进行检测的期望收益:

$$\text{当 } x < \frac{e_s}{a+b} \text{ 时, } \frac{\partial Eu_s}{\partial y} < 0, \text{ 合法进行检测的}$$

期望收益低于不进行检测的期望收益。

$$\text{同理, 令 } \frac{\partial Eu_l}{\partial x} = 0, \text{ 得:}$$

$$y(-a - e_l) - y(-e_l) + (1-y)(b - e_l) - (1-y)(-e_l) = 0 \quad (5)$$

整理式 (5) 得:

$$y = \frac{b}{a+b} \quad (6)$$

当 $y = \frac{b}{a+b}$ 时, $\frac{\partial Eu_l}{\partial x} = 0$, 恶意节点发起攻击的期望收益等于不攻击的期望收益;

当 $y > \frac{b}{a+b}$ 时, $\frac{\partial Eu_l}{\partial x} < 0$, 恶意节点发起攻击的期望收益低于不攻击的期望收益;

当 $y < \frac{b}{a+b}$ 时, $\frac{\partial Eu_l}{\partial x} > 0$, 恶意节点发起攻击的期望收益高于不攻击的期望收益。

由以上分析可知, 合法节点会根据恶意节点的攻击概率决定是否进行检测, 而恶意节点也应该根据合法节点进行检测的概率决定是否发起攻击, $\left(x^* = \frac{e_s}{a+b}, y^* = \frac{b}{a+b}\right)$ 便是恶意节点与合法节点进行攻防博弈的混合纳什均衡策略。证毕。

定理 1 表明, 当恶意节点的攻击概率大于 x^* 时, 合法节点就会采取检测策略, 这会使合法节点的检测概率增加。当检测概率大于 y^* 时, 恶意节点就会采取不攻击策略, 这又会使恶意节点的攻击概率降低。当攻击概率小于 x^* 时, 合法节点就会采取不检测策略, 从而使检测概率降低。当检测概率小于 y^* 时, 恶意节点又会采取攻击策略, 因此恶意节点与合法节点的策略会在均衡策略附近作小幅交替波动, 但平均来看, 合法节点的检测概率是 $y^* = \frac{b}{a+b}$, 而恶意节点的攻击概率是

$$x^* = \frac{e_s}{a+b}。$$

3 博弈驱动下的 WSN 恶意程序传播模型

由 WSN 的攻防博弈模型可知, 如果恶意节点向合法节点发起攻击, 合法节点在不进行检测的情况下就会被恶意节点感染, 被感染的节点会进一步向其他节点发起攻击并造成更多节点被感染。假设 WSN 中总共有 N 个节点, 其中恶意节点个数为 N_l , 占总节点数的比例为 i , 合法节点个数为 N_s , 占总节点数的比例为 s 。每个恶意节点在单位时间内会随机选择一个其他节点发送信息, 其中发送恶意程序的概率为 x , 发送正常信息的概率为 $1-x$, 合法节点会以概率 y 对收到的信息进行检测。根据第 2 节的分析, 恶意节点与合法节点作为理性的智能体, 会采用混合纳什均衡策略作为各自的攻防策略, 即 $x = x^*$, $y = y^*$, 因此, 单位时间内网络中新增的恶意节点数为 $x^*(1-y^*)sN_l$, 相应减少的合法节点数也为 $x^*(1-y^*)sN_l$, 这时 WSN 中两种节点的数目随时间的演化过程用微分方程组表示为:

$$\begin{cases} \frac{dN_l}{dt} = x^*(1-y^*)sN_l \\ \frac{dN_s}{dt} = -x^*(1-y^*)sN_l \\ N_l + N_s = N \end{cases} \quad (7)$$

方程组两边同时除以 N 得:

$$\begin{cases} \frac{di}{dt} = x^*(1-y^*)si \\ \frac{ds}{dt} = -x^*(1-y^*)si \\ i + s = 1 \end{cases} \quad (8)$$

其中, s 代表网络中合法节点所占比例, i 代表网络中恶意节点所占比例。于是有:

$$\frac{di}{dt} = x^*(1-y^*)i(1-i) \quad (9)$$

即:

$$\frac{di}{i(1-i)} = x^*(1-y^*)dt \quad (10)$$

令 $t_0 = 0$ ，并假设初始时刻的感染比例为 i_0 ，对式 (10) 从 t_0 到 t 进行积分得：

$$\ln \frac{i_t}{1-i_t} - \ln \frac{i_0}{1-i_0} = x^*(1-y^*)t \quad (11)$$

对式 (11) 进一步求解可得到 t 时刻恶意节点占总节点数的比例 i_t ：

$$i_t = \frac{i_0}{i_0 + (1-i_0)e^{-x^*(1-y^*)t}} \quad (12)$$

将 $x^* = \frac{e_s}{a+b}$ ， $y^* = \frac{b}{a+b}$ 代入式 (12) 得：

$$i_t = \frac{i_0}{i_0 + (1-i_0)e^{-\frac{ae_s}{(a+b)^2}t}} \quad (13)$$

由式 (13) 可知，恶意程序的传播速度与合法节点被感染的概率有关，感染概率由博弈双方所采取的策略决定，而该策略又是由收益矩阵中的参数决定的，因此网络中恶意程序的传播速度最终由博弈的收益参数决定。

4 数值模拟与仿真

4.1 攻防博弈策略数值模拟

令 $a=2$ ， $b=3$ ， $e_s=1$ ， $e_t=0.5$ ，此时，

$\frac{e_s}{a+b}=0.2$ ， $\frac{b}{a+b}=0.6$ 。分别对式 (1) 和式 (2)

进行数值模拟，结果如图 1 和图 2 所示。从图 1 可以看出，当 $x=0.2$ 时，合法节点的期望收益不随 y 的变化而改变，此时合法节点的期望收益与其采取哪种策略无关；当 $x>0.2$ 时，合法节点的期望收益随着 y 的增大而增加，此时合法节点应该采取检测策略；而当 $x<0.2$ 时，合法节点的期望收益随着 y 的增大而减少，此时合法节点应该采取不检测策略。从图 2 可以看出，当 $y=0.6$ 时，恶意节点的期望收益不随 x 的变化而改变，此时恶意节点的收益与其采取哪种策略无关；当 $y>0.6$ 时，恶意节点的期望收益随着 x 的增加而减少，此时恶意节点应该采取不攻击策略；而当

$y<0.6$ 时，恶意节点的期望收益随着 x 的增加而增大，此时恶意节点应该采取攻击策略，这与前面的理论分析一致。

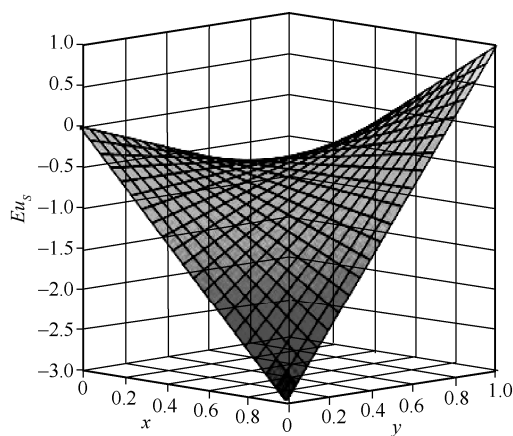


图 1 博弈双方策略的变化对合法节点期望收益的影响

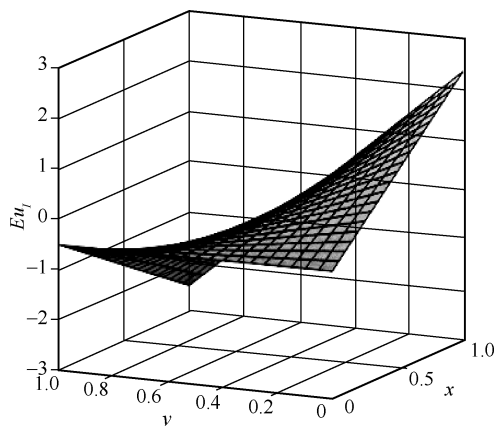


图 2 博弈双方策略的变化对恶意节点期望收益的影响

4.2 恶意程序传播数值模拟

根据前面建立的 WSN 恶意程序传播模型，对式 (8) 进行数值模拟，便可得到收益参数与恶意程序传播速度之间的关系，模拟结果如图 3~图 5 所示。

从图 3 可以看出，合法节点对信息进行检测时的能耗对恶意程序传播速度具有较大影响，合法节点的检测能耗越大，恶意程序的传播速度迅速增大。可解释为：当检测能耗 e_s 增大时，合法节点为了节约能量理应降低检测的概率，但这会促使恶意节点提高攻击概率，从而造成合法节点

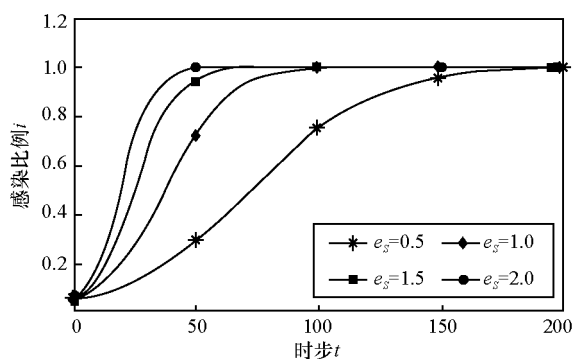


图3 合法节点检测过程的能耗对传播速度的影响
($a=2.0, b=3.0$)

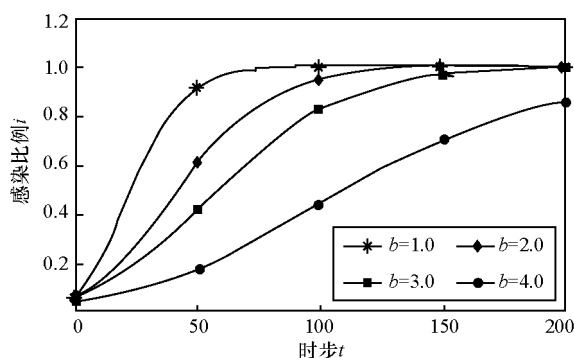


图4 合法节点被感染恶意程序的损失对传播速度的影响
($e_s=1.0, a=2.0$)

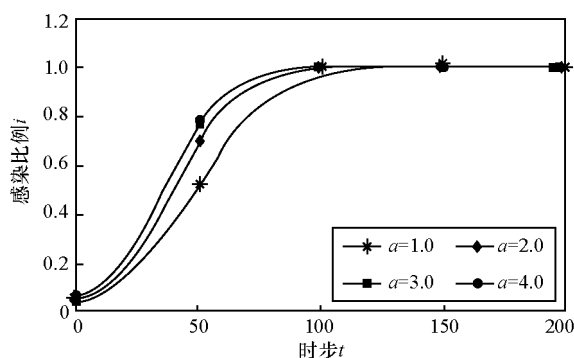


图5 成功检测出恶意程序的收益对传播速度的影响
($e_s=1.0, b=3.0$)

更大的损失,由混合纳什均衡策略可知,双方最终的博弈结果是合法节点保持检测概率不变,而恶意节点提高了攻击概率,从而使恶意程序的传播速度变快。

从图4可以看出,随着合法节点被感染时损失(恶意节点攻击成功的收益)的增大,恶意程序的传播速度会降低。可解释为:当恶意节点攻

击成功的收益 b 增加时,表面看其应该增大攻击概率,但由于此时合法节点的损失也增大了,促使合法节点提高检测概率,从而造成恶意节点的损失增大,最终双方的博弈结果是合法节点提高了检测概率,恶意节点降低了攻击概率,因此恶意程序的传播速度变慢了。

从图5可以看出,合法节点成功检出恶意程序的收益(恶意节点被检出的损失)的大小对恶意程序的传播速度没有太大影响。可解释为:当恶意节点被检出的损失 a 增大时,恶意节点理应降低攻击概率,但这会促使合法节点也降低检测概率,最终双方的博弈结果是恶意节点降低攻击概率,合法节点也降低检测概率,因此恶意程序的传播速度变化不大。

4.3 恶意程序传播元胞自动机仿真

前面用微分方程组建立的恶意程序传播模型依赖一个假设条件——网络是全连接的,即网络中的任意两个节点之间都可以直接通信。然而,对于真实的WSN来说,由于节点的发射功率与传输距离的平方成正比,传感器为了节约能量,只会与其附近的部分节点进行直接通信。因此,前面的理论模型是在理想条件下建立的,与真实情况存在差异,为了更精确地研究WSN中恶意程序的传播规律,同时也为了对前面的理论研究结果进行验证,本节用元胞自动机方法对WSN中的恶意程序传播过程进行仿真。

4.3.1 仿真算法

仿真算法步骤如下。

步骤1 生成一个如图6所示的规格为 100×100 格的网格,随机选择比例为 p_w 的格子布设传感器节点。

步骤2 每个传感器节点与距离自己半径不超过 r 的节点产生连边(组网),由此生成传感器网络。

步骤3 在初始时刻 $t_0=0$,随机选取比例为 i_0 的节点设置为恶意节点。

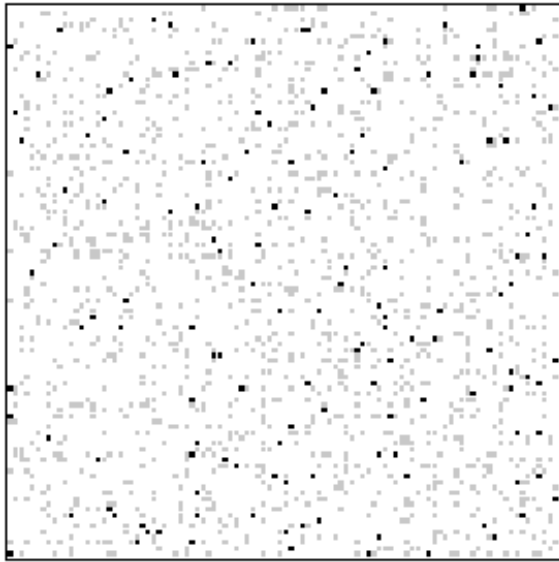


图6 无线传感器节点分布图(灰色为正常节点, 黑色为恶意节点)

步骤4 每个恶意节点在自己的邻居节点(可以与其直接通信的节点)中随机选择一个节点发送信息, 其中发送恶意信息的概率为 x^* , 发送正常信息的概率为 $1-x^*$ 。

步骤5 若恶意节点选中的节点也是恶意节点, 则信息会被直接丢弃。反之, 若恶意节点选中的是合法节点, 则合法节点会以概率 y^* 对收到的信息进行检测, 以概率 $1-y^*$ 不对信息进行检测。当合法节点接收的是恶意程序且正好没有启动检测时则会被感染, 感染后的节点就变成恶意节点, 并能继续向其他节点传播恶意程序。

步骤6 若 t 小于预设的模拟步数, 则 t 的值增加 1, 并转入步骤 4 继续执行, 否则, 结束运行。

4.3.2 仿真结果

设定参数 $p_w=0.1$, $i_0=0.05$, 执行上述模拟步骤, 考查不同博弈参数下 WSN 恶意程序的传播速度。模拟结果如图 7~图 10 所示。图 7 显示, 随着合法节点检测能耗的增大, 恶意程序的传播速度也相应变大; 图 8 显示, 随着合法节点被感染时损失(恶意节点攻击成功的收益)的增大, 恶意程序的传播速度变慢; 图 9 显示合法节点成功检测出恶意程序的收益(恶意节点被检出的损失)

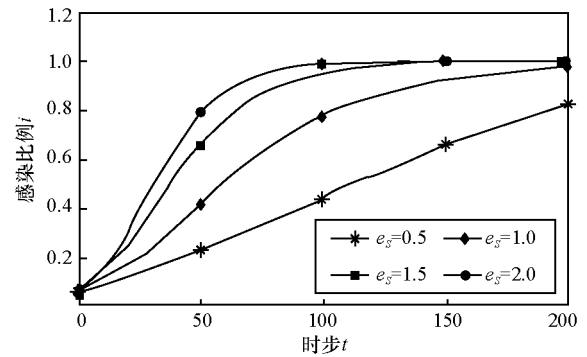


图7 合法节点检测过程的能耗对传播速度的影响 ($a=2.0$, $b=3.0$)

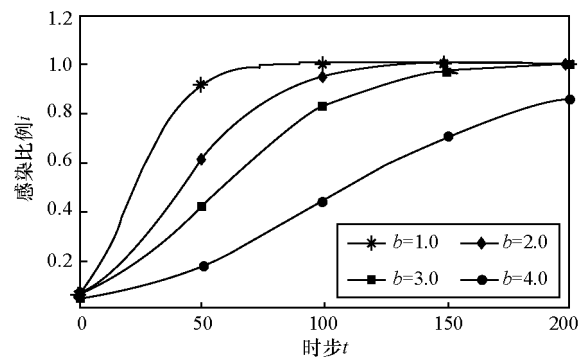


图8 合法节点感染恶意程序的损失对传播速度的影响 ($e_s=1.0$, $a=2.0$)

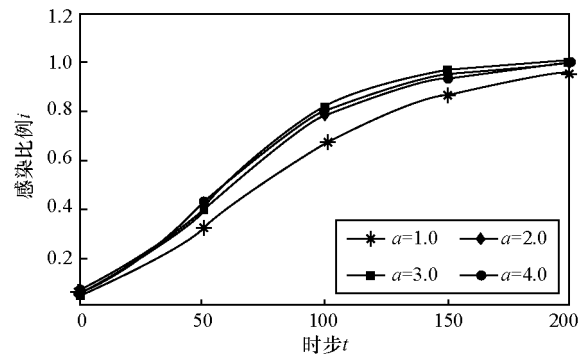


图9 成功检测出恶意程序的收益对传播速度的影响 ($e_s=1.0$, $b=3.0$)

对恶意程序传播速度的影响不大。这些结论与理论解析结果一致。此外, 由于 WSN 中恶意程序的传播过程与通信半径有关, 因此, 进一步研究了传感器节点的通信半径对恶意程序传播速度的影响, 在模拟过程中通过修改通信半径的值, 得到了不同通信半径下恶意程序的传播曲线, 图 10 显示, 在其他参数固定的情况下, 恶意程序的传播速度随着通信半径的增加而增大。

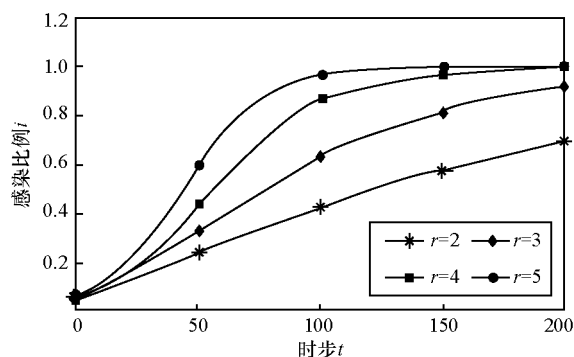


图 10 通信半径对恶意程序传播速度的影响
($e_s=1.0, a=2.0, b=3.0$)

在某些应用领域中(如军事侦察领域),传感器节点在工作时会不断移动位置,为了考察节点的移动行为对恶意程序传播速度的影响,进一步对移动环境下 WSN 的恶意程序传播过程进行了仿真,仿真步骤与静态传播的步骤基本一致,只需在步骤 5 后面增加一个步骤,使每个传感器节点在每个时步随机地选择一个方向移动一格(前提是目标位置没有被其他节点占据)。仿真结果如图 11 所示,从图 11 可以看出,在同等参数条件下,移动无线传感器网络中恶意程序的传播速度要高于静态无线传感器网络。

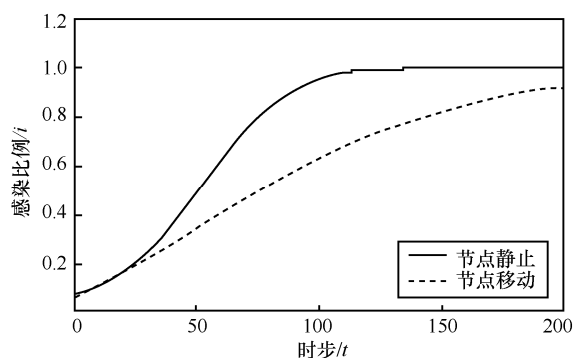


图 11 节点的移动行为对恶意程序传播速度的影响
($r=3, e_s=1.0, a=2.0, b=3.0$)

5 讨论与分析

5.1 理论模型与元胞自动机模型的比较

尽管本文的理论模型和元胞自动机模拟得到的研究结论是一致的,但两者之间仍然存在一些差异,其中最明显的一点是:在同等参数条件下,

理论模型中恶意程序的传播速度要大于元胞自动机模拟的传播速度。这一点从图 3 与图 7、图 4 与图 8、图 5 与图 9 的比较中可以反映出来。下面对这种差异进行解释。

(1) 理论模型的建立依赖一种假设——网络中任意两个节点都是直接相连的,然而,在元胞自动机模型中,每个节点只与其附近的节点(距离不超过 r) 进行通信,当某个恶意节点附近没有未被感染的邻居节点时就不能传播恶意程序,这就会降低恶意程序的传播速度。

(2) 在元胞自动机模型中,每个恶意节点都只能选择其附近的节点进行传播,随着时间的推移,就会导致大量恶意节点聚集成簇,而处于簇中心的节点由于其附近没有合法节点就不能传播恶意程序,这是导致传播速度变慢的另一个重要原因。图 12 显示了元胞自动机模拟至第 150 步时恶意节点与合法节点的时空分布图,从图 12 中可以很清楚地看到恶意节点的簇形分布形状。

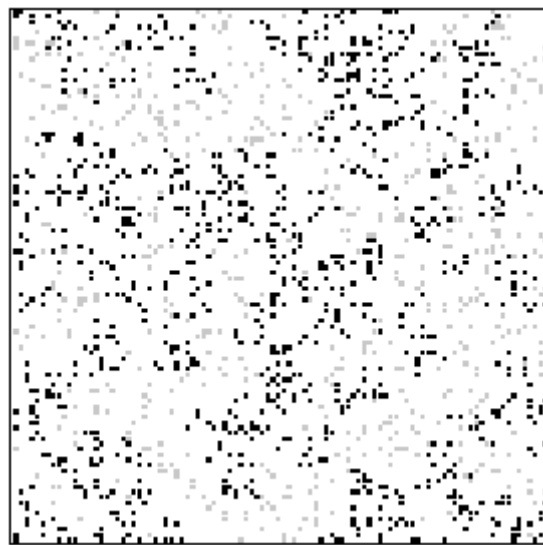


图 12 恶意程序传播过程中两种节点的时空分布图
(灰色为正常节点,黑色为恶意节点)

从节点是否运动的角度看,对于理论模型来说,恶意程序的传播速度与节点是否运动无关,而对于元胞自动机模型来说,节点的运动提高恶意程序的传播速度。原因如下:理论传播模型

是在全局耦合网络上建立的, 该网络中任意两节点都是直接相连的, 节点的运动并不会改变网络的连接关系, 所以节点运动与否不会影响传播速度。而对于元胞自动机模型来说, 由于每个节点只与其附近的节点相连, 节点的运动能够促使恶意节点与合法节点充分混合, 降低成簇效应, 从而提高传播速度。

从研究方法上看, 元胞自动机方法能够更加真实地反映 WSN 中恶意程序的传播过程, 但是该方法会受到网络规模的限制, 当网络规模增大时模拟的复杂性也随之增加; 而对于理论模型来说, 该方法具有一定的普适性, 研究过程与网络规模无关, 但是该模型只是一种近似模型, 无法反映 WSN 的真实结构及通信特点。这两种方法的配合使用可以让人们更全面地了解 WSN 的恶意程序传播过程。

5.2 关于研究结果的讨论

本文的理论模型及元胞自动机模拟揭示了博弈驱动下的 WSN 恶意程序的传播特点: 恶意程序的传播速度随合法节点的检测能耗的增加而变快, 随恶意节点攻击成功时的收益(合法节点被感染时的损失)的增加而变慢, 随节点通信半径的增大而变快, 而合法节点检出恶意程序的收益(恶意节点被检测的损失)对传播速度的影响不大。值得指出的是, 在判断某个博弈参数的变化对传播速度的影响时, 不能只根据某一方可能采取的行动进行推断, 而必须综合考虑双方的行动。例如, 当合法节点检出恶意程序的收益增加时, 表面看其应该通过提高检测概率来提高其收益, 但是, 此时恶意节点为了减少损失会降低攻击概率, 这又会促使合法节点降低检测概率, 因此, 整体上看恶意程序的传播速度变化不大, 这说明恶意程序的传播速度本质上是由攻防双方最终的博弈结果决定的。

另外, 基于本文的研究结果, 可以制定相关的措施来减缓恶意程序的传播速度, 为开发清除

恶意程序的补丁赢取时间。具体措施可以如下: 优化合法节点的检测算法, 节约其在信息检测过程中消耗的能量; 适当减小传感器节点的通信半径, 一方面可以降低恶意程序的传播速度, 另一方面也可以节约传感器节点的能耗, 延长其使用寿命。

6 结束语

本文从博弈论的角度对 WSN 中恶意节点与合法节点的攻防博弈策略进行了分析, 求出了博弈模型的混合纳什均衡策略, 并对该均衡策略驱动下的 WSN 恶意程序的传播过程进行了研究。从理论建模和元胞自动机模拟两个角度对恶意程序的传播过程进行研究, 得到了恶意程序的传播速度与博弈参数之间的关系, 揭示了博弈驱动下 WSN 的恶意程序传播机制, 这对制定延缓 WSN 恶意程序传播的措施具有理论指导作用。在 WSN 中, 恶意程序一旦被发现后, 人们会立即开发相关的补丁程序来修复感染节点, 这种带有修复机制的恶意程序传播模型将是笔者下一步研究的内容。

参考文献:

- [1] 张焕国, 韩文报, 来学嘉, 等. 网络空间安全综述[J]. 中国科学: 信息科学, 2016, 46(2): 125-164.
ZHANG H G, HAN W B, LAI X J, et al. Surveyon cyberspace security[J]. Scientia Sinica: Informationis, 2016, 46(2): 125-164.
- [2] SHI H, WANG W, KWOK N, et al. Game theory for wireless sensor network: a survey[J]. Sensors, 2012, 12(7): 113-122.
- [3] 沈士根, 刘建华, 曹奇英. 博弈论与无线传感器网络安全[M]. 北京: 清华大学出版社, 2016.
SHEN S G, LIU J H, CAO Q Y. Game theory meets wireless sensor network security [M]. Beijing: Tsinghua University Press, 2016.
- [4] ABDALZAHERM, SEDDIK K, ELSABROUTY M, et al. Game theory meets wireless sensor network security requirements and threats mitigation: a survey[J]. Sensors, 2016, 16(7): 1-27.
- [5] 沈士根, 黄龙军, 胡珂立, 等. 基于微分博弈的在线社交网络恶意程序传播优化控制方法[J]. 电信科学, 2015, 31(10): 66-73.



- SHEN S G, HUANG L J, HU K L, et al. Differential game-based optimal control method for preventing malware propagation in online social network[J]. Telecommunications Science, 2015, 31(10): 66-73.
- [6] 沈士根, 冯晟, 周海平, 等. 基于云计算和动态贝叶斯博弈的WSN恶意程序传播优化抑制方法[J]. 电信科学, 2018, 34(9).
SHEN S G, FENG S, ZHOU H P, et al. Optimal approach to suppressing WSN malware propagation based on cloud computing and dynamic Bayesian game [J]. Telecommunications Science, 2018, 34(9).
- [7] 沈士根, 周海平, 黄龙军, 等. 基于最优反应均衡的传感网恶意程序传播抑制方法[J]. 传感技术学报, 2017, 30(10): 1589-1595.
SHEN S G, ZHOU H P, HUANG L J, et al. Quanta response equilibrium-based method for preventing WSN malware infection[J]. Chinese Journal of Sensors and Actuators, 2017, 30(10): 1589-1595.
- [8] 沈士根, 黄龙军, 周海平, 等. 面向恶意程序传播的异质WSN 稳态可用度评估[J]. 传感技术学报, 2017, 30(7): 1100-1105.
SHEN S G, HUANG L J, ZHOU H P, et al. Steady-state availability evaluation for heterogeneous WSN under malware infection[J]. Chinese Journal of Sensors and Actuators, 2017, 30(7): 1100-1105.
- [9] 沈士根, 范恩, 胡珂立, 等. 面向恶意程序传播的传感网可靠度评估[J]. 电子学报, 2018, 46(1): 75-81.
SHEN S G, FAN E, HU K L, et al. Reliability evaluation for WSN with malware spread[J]. Acta Electronica Sinica, 2018, 46(1): 75-81.
- [10] 庄克琛, 张宏, 张琨, 等. 无线传感器网络中的病毒传播动力学研究[J]. 计算机科学, 2013, 40(3): 187-191.
ZHANG K C, ZHANG H, ZHANG K, et al. Analysis of spreading dynamics of virus in wireless sensor network [J]. Computer Science, 2013, 40(3): 187-191.
- [11] 熊自立, 韩兰胜, 徐行波, 等. 基于博弈的无线传感器网络入侵检测模型[J]. 计算机科学, 2017, 44(S1): 326-332.
XIONG Z L, HAN L S, XU H B, et al. Research on intrusion detection of wireless sensor network based on game theory[J]. Computer Science, 2017, 44(S1): 326-332.
- [12] 周伟伟, 郁滨. WSN 多阶段入侵检测博弈最优策略研究[J]. 电子与信息学报, 2018, 40(1): 63-71.
ZHOU W W, YU B. Optimal defense strategy in WSN based on the game of multi-stage intrusion detection[J]. Journal of Electronics & Information Technology, 2018, 40(1): 63-71.
- [13] CHENG Z. A differential game model between intrusion detection system and attackers for wireless sensor network[J]. Wireless Personal Communications, 2016, 90(3): 1211-1219.
- [14] SEDJELMACI H, SENOUCI S, ANSARI N. Intrusion detection and ejection framework against lethal attacks in UAV-aided network: a Bayesian game-theoretic methodology [J]. IEEE Transactions on Intelligent Transportation Systems, 2017, 18(5): 1143-1153.
- [15] 王小明, 李成博, 李英姝. 移动无线传感网恶意数据包传播随机模型[J]. 电子与信息学报, 2013, 35(6): 1290-1297.
WANG X M, LI C B, LI Y Z. A stochastic model of malicious data packet propagation in mobile wireless sensor network[J]. Journal of Electronics & Information Technology, 2013, 35(6): 1290-1297.
- [16] 曹玉林, 王小明, 何早波. 移动无线传感网中恶意软件传播的最优安全策略[J]. 电子学报, 2016, 44(8): 1851-1857.
CAO Y L, WANG X M, HE Z B. Optimal security strategy for malware propagation mobile wireless sensor network[J]. Acta Electronica Sinica, 2016, 44(8): 1851-1857.
- [17] SINGH A, AWASTHI A, SINGH K, et al. Modeling and analysis of worm propagation in wireless sensor network [J]. Wireless Personal Communications, 2018, 98(3): 2535-2551.
- [18] WANG T, WU Q, WEN S, et al. Propagation modeling and defending of a mobile sensor worm in wireless sensor and actuator network[J]. Sensors, 2017, 17(12): 139-155.
- [19] LIU W, LIU, C, YANG Z, et al. Modeling the propagation of mobile malware on complex network [J]. Communications in Nonlinear Science and Numerical Simulation, 2016(37): 249-264.
- [20] CHRISTOPHE B, LIZA C, CORINNE T. Optimal design and defense of network under link attacks [J]. Journal of Mathematical Economics, 2017(68): 62-79.

[作者简介]



周海平 (1977-), 男, 博士, 绍兴文理学院计算机科学与工程系教授, 主要研究方向为复杂网络、推荐算法、博弈论。



沈士根 (1974-), 男, 博士, 绍兴文理学院计算机科学与工程系教授, 主要研究方向为无线传感器网络、物联网、博弈论。

黄龙军 (1976-), 男, 博士, 绍兴文理学院计算机科学与工程系讲师, 主要研究方向为无线传感器网络、博弈论。

冯晟 (1979-), 男, 博士, 绍兴文理学院计算机科学与工程系讲师, 主要研究方向为无线传感器网络、物联网、计算机视觉、智能机器人。