基于微分博弈的异质无线传感器网络恶意程序传播研究与分析

汤梦晨[1] 吴国文[1] 张 红[1] 沈士根[2] 曹奇英[1*]

[1](东华大学计算机科学与技术学院 上海 201620)

[2](绍兴文理学院计算机科学与工程系 浙江 绍兴 312000)

摘 要 为抑制异质无线传感器网络(Heterogeneous Wireless Sensor Networks,HWSNs)恶意程序的传播,考虑节点能量和计算能力差异,提出一种 HWSNs 攻防博弈模型。通过计算得到攻防双方的混合纳什均衡,再结合微分博弈建立攻防双方节点转换微分方程,分析得到恶意节点比例动态演化规律。结合数值实验分析,验证有效抑制 HWSNs 恶意程序传播的方式。

关键词 异质无线传感器网络 微分博弈 恶意程序 入侵检测

中图分类号 TP393 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2024.07.016

RESEARCH AND ANALYSIS OF MALICIOUS PROGRAM PROPAGATION IN HETEROGENEOUS WIRELESS SENSOR NETWORKS BASED ON DIFFERENTIAL GAME

Tang Mengchen[1] Wu Guowen[1] Zhang Hong[1] Shen Shigen[2] Cao Qiying[1*]

[1](*College of Computer Science and Technology, Donghua University, Shanghai 201620, China*)

[2](*Department of Computer Science and Engineering, Shaoxing University, Shaoxing 321000, Zhejiang, China*)

Abstract In order to suppress the spread of malicious programs in heterogeneous wireless sensor networks (HWSNs), a HWSNs offensive and defensive game is proposed based on the differences in node energy and computing power. The mixed Nash equilibrium of the attacking and defending sides was obtained through calculation, and the differential equations of the node conversion of the attacking and defending sides were established by combining the differential game. The dynamic evolution law of the proportion of malicious nodes was analyzed. Combined with numerical experimental analysis, the method to effectively suppress the spread of HWSNs malicious programs was verified.

Keywords Heterogeneous wireless sensor networks Differential game Malicious program Intrusion detection

0 引 言

无线传感器网络 WSNs(Wireless Sensor Networks)具有良好的应用前景,在现阶段主要应用在军事、科研、森林系统、医疗、智能家居等方面[1-2]。WSNs 具有传感器节点分布的随机性和网络的自组织性的特点,同时这些特点也给 WSNs 的网络安全性能带来了极大的挑战[3]。WSNs 常见受到的攻击形式主要包括 Sybil 攻击、虫洞攻击、sinkhole 攻击、DoS 攻击和中间人攻击等。针对常见的攻击形式,国内外对此进行了大量的研究,也在这些问题上取得了很大的突破[4-8]。

对于无线传感器网络而言,要想有效地防御恶意程序的入侵,对于传感器节点的能量要求是非常大的。能量有限也正是传感器节点的缺陷,所以,如何在节点防御的能量消耗和节点防御的效益之间取得相对平衡是亟需解决的问题。博弈论[9]的对立性、策略依存性与网络中攻击方、防御方的攻防基本特征相似。因此,将博弈论与网络攻防相结合成为近几年的研究热点。文献[10]将网络攻防的实际情况与演化博弈的理论相结合,建立网络攻防演化博弈模型,并且设计了最优的安全策略的选取算法。文献[11]针对拟态防御系

收稿日期:2021-02-05。国家自然科学基金项目(61772018)。**汤梦晨**,硕士生,主研领域:无线传感器网络,博弈论。**吴国文**,副教授。**张红**,博士生。**沈士根**,教授。**曹奇英**,教授。

统的攻防博弈场景提出了改进模型 M-FlipIt,并对不同的拟态防御策略进行了评估,得出了维持防御方持续获取高收益的策略。文献[12]同时考虑了无线传感器网络中所可能遭受的内部攻击和外部攻击的情况,结合博弈论建立了攻防博弈模型,研究得出了攻防双方的最优策略。文献[13]依据异质无线传感器网络中的恶意程序的传播特性,提出了基于流行病学的恶意程序传播模型,并证明了该模型的稳定性。文献[14]在有限理性的前置条件下结合禁忌搜索法构建禁忌随机博弈模型,并得出了该模型的最优防御策略,使防御方付出最小的代价实现最好的防御效果。文献[15]提出一种基于扩展传染病理论的异质无线传感器网络恶意程序传播建模与分析方法。文献[16]结合元胞自动机理论和静态贝叶斯博弈理论,建立了无线传感器网络的恶意程序传染模型,揭示了恶意程序在无线传感器网络的传染行为。文献[17]考虑整个网络在"有限理性"的前提下,并结合最优反应均衡提出一种抑制无线传感网络恶意程序传播的方法。

文献[18 - 19]考虑无线传感器网络中合法节点和恶意节点之间的攻防情况,建立了基于微分博弈的恶意程序传播模型,研究得出了攻防双方的混合纳什均衡,得出了有效抑制无线传感器网络中恶意程序传播的方法。然而该文中的传感器节点都是一致的,在能量和检测恶意程序能力上是没有区别的,并且该文中假设防御方检测成功的概率为 1。实际情况中,无线传感器网络中节点的能量和计算能力是有差别的,簇头节点的能量和计算能力要大于普通节点,并且防御方在进行检测时检测成功率也不会达到 100%。

基于以上分析,首先本文提出一个基于异质无线传感器网络(HWSNs)的攻防模型,考虑了无线传感器网络中节点的异质性。其次,通过攻防双方的攻防策略分析,得到攻防双方收益的混合纳什均衡,并结合微分博弈来研究和分析在攻防过程中的节点的演化过程,从而得到如何抑制恶意程序的传播。最后,用数值模拟的方式,对恶意程序在异质无线传感器网络中的传播过程进行模拟仿真,并对仿真结果进行分析得到有效抑制恶意程序传播的方式。

1　HWSNs 中的攻防博弈概述

在 HWSNs 中,节点被分布在各个不同的区域,节点的能量来源一般是由电池提供,当节点的电池能量耗尽,该节点就无法正常工作。考虑到 HWSNs 中,节点间进行通信的能量损耗随着通信半径的增大而增大,为了节省每个节点在传输信息过程中的能量损耗,HWSNs 通常会把节点分为多个簇,每个簇中都有一个能量较大的簇头节点和多个普通节点。普通节点只和自己所在簇的簇头节点进行通信,再由簇头节点将信息传递给基站,如图 1 所示。

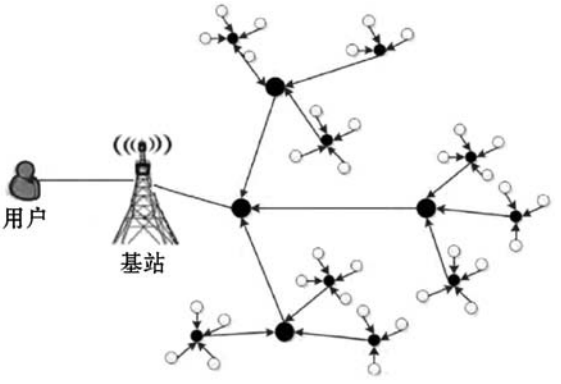

图 1　异质无线传感器网络的结构

在 HWSNs 中,合法节点(簇头节点,普通节点)为了不受恶意节点攻击的影响,会开启入侵检测系统 IDS(Intrusion Detection System)对节点接收到信息进行检测,但是由于节点又受到能量有限的限制,不能一直都开启检测状态,合法节点会采取一定的概率对接收到的信息进行检测。同时,对于恶意节点来说如果持续进行攻击会容易被合法节点检测到其攻击行为,所以恶意节点也是采取一定的概率进行攻击,在不攻击时,采取发送正常信息的方式来隐藏自己的身份。并且在整个的博弈过程中,攻击方节点和防御方节点都互相不知道对方的身份信息。根据以上的特点,本文采取不完全信息博弈的方法对攻击方和防御方的最优策略进行研究和分析。

定义 1　HWSNs 中的不完全信息博弈模型采用的是 $G\langle \phi, \{T_j\}, \varphi_i, \{\psi_j\}, \{U_j\}\rangle$,其中:

(1) ϕ 为博弈过程中的参与者,参与者 ϕ = {发送方,接收方}。

(2) $\{T_j\}$ 是传感器节点 j 的类型,在 HWSNs 中节点的类型分为防御方(簇头节点,普通节点)和攻击方(恶意节点),因此,$\{T_j\}$ = {簇头节点,普通节点,恶意节点},$j \in \phi$。

(3) φ_κ 为博弈双方在空间上的概率分布,这里表示为不同类型的节点在整个 HWSNs 中所占的比例,$\kappa \in T_j$。

(4) $\{\psi_j\}$ 是传感器节点 j 的行为策略集合。其中,信息的发送方可能是恶意节点也可能是合法节点,对于恶意节点来说有"攻击"和"不攻击"两种行为,对于合法节点来说只有不攻击一种行为,可分别表示为

$\psi_{发送方,恶意节点}=\{攻击,不攻击\}$，$\psi_{发送方,合法节点}=\{不攻击\}$。同时，信息的接收方也有不同类型的节点，分别是防御方（簇头节点，普通节点）和攻击方（恶意节点），对于恶意节点来说只有一种“不检测”行为，对于合法节点来说有“检测”和“不检测”两种行为，可分别表示 $\psi_{接收方,恶意节点}=\{不检测\}$ 和 $\psi_{接收方,合法节点}=\{检测,不检测\}$。此处有一点需要注意，对于恶意节点来说的不攻击行为并不是不做任何动作，而是发送正常的信息来伪装成合法节点。

（5）U_j为传感器节点 j 在选择某一策略之后的期望收益。

本文中的符号定义如表 1 所示。

表 1 符号定义

符号	含义
v	防御方检测成功的收益，攻击方被识别的损失
w_1	攻击簇头节点成功的收益，簇头节点被感染的损失
w_2	攻击普通节点成功的收益，普通节点被感染的损失
e_1	簇头节点检测信息所花费的能量代价
e_2	普通节点检测信息所花费的能量代价
e_M	传感器节点发送信息的能量代价
p_1	簇头节点检测成功的概率
p_2	普通节点检测成功的概率
x	攻击方进行攻击的概率
y	防御方进行防御检测的概率
E_{df}	防御方博弈过程中的期望收益
E_{at}	攻击方博弈过程中的期望收益

2 博弈模型的理论分析

在博弈模型中，发送方（合法节点，恶意节点）不论是发送正常信息还是攻击信息都需要消耗 e_M 的能量代价。合法节点分为簇头节点和普通节点，簇头节点的能量大于普通节点的能量，因此可以分配更多的能量去检测接收到的信息，并且簇头节点检测信息所消耗的能量大于普通节点检测信息所消耗的能量，即 $e_1>e_2$。由于簇头节点的计算能力和能量都要大于普通节点，因此，当攻击方进行攻击，并且防御方进行防御的时候，簇头节点防御成功的概率要大于普通节点，即 $p_1>p_2$。在 HWSNs 中，簇头节点相对于普通节点更加重要，因此，攻击方成功感染簇头节点的收益 w_1 大于成功感染普通节点的收益 w_2。当攻击方攻击的同时防御方也进行防御，并且防御方防御成功（检测出恶意节点）的收益为 v。需要说明的是，为了使整个的博弈过程有意义，需要满足 $v\geqslant e_1>e_2$，$w_1>w_2\geqslant e_M$。博弈双方的收益矩阵如表 2 所示。

表 2 防御方与攻击方博弈收益函数表

信息接收方		信息发送方		
		恶意节点		合法节点
		攻击	不攻击	不攻击
簇头节点	检测	$v-e_1,-v-e_M$	$-e_1-e_M,e_M$	$-e_1,e_M$
	不检测	$-w_1,w_1-e_M$	$0,-e_M$	$0,-e_M$
普通节点	检测	$v-e_2,-v-e_M$	$-e_2,-e_M$	$-e_2,e_M$
	不检测	$-w_2,w_2-e_M$	$0,-e_M$	$0,-e_M$
恶意节点	不检测	$0,-e_M$	$0,-e_M$	$0,-e_M$

定理 1 HWSNs 中防御方和攻击方之间存在混合纳什均衡策略。

证明：假设在 HWSNs 中，恶意节点所占的初始比例为 i，簇头节点所占的初始比例为 s_1，普通节点所占的初始比例为 s_2。根据实际网络环境情况，簇头节点占比要比普通节点少，故 $s_1<s_2$。本文中假设恶意节点发起攻击的概率是 x，发送正常信息（不发动攻击）的概率是 $1-x$，合法节点进行防御（对收到的信息进行检测）的概率是 y，不进行检测的概率是 $1-y$。则根据表 2 的矩阵，可以分别得到防御方的期望收益 E_{df} 和攻击方的期望收益 E_{at} 为：

$$\begin{aligned}E_{df}=&p_1ixy(v-e_1)+(1-p_1)ixy(-e_1-w_1)+i(1-x)\cdot y(-e_1)+ix(1-y)(-w_1)+i(1-x)(1-y)\cdot 0+p_2ixy\cdot(v-e_2)+(1-p_2)ixy(-e_2-w_2)+i(1-x)y(-e_2)+i\cdot x(1-y)(-w_2)+i(1-x)(1-y)\cdot 0-s_1ye_1-s_2ye_2+s_1\cdot(1-y)\cdot 0+s_2(1-y)\cdot 0\end{aligned}\tag{1}$$

$$\begin{aligned}E_{at}=&p_1s_1xy(-v-e_M)+(1-p_1)s_1xy(w_1-e_M)+s_1x\cdot(1-y)(w_1-e_M)-s_1(1-x)ye_M-s_1(1-x)(1-y)e_M+p_2s_2xy(-v-e_M)+(1-p_2)s_2xy(w_2-e_M)+s_2x\cdot(1-y)(w_2-e_M)-s_2(1-x)ye_M-s_2(1-x)(1-y)\cdot e_M+i(1-x)(-e_M)+ix(-e_M)\end{aligned}\tag{2}$$

令 $\dfrac{\partial E_{df}}{\partial y}=0$，得：

$$p_1ixv+p_1ixw_1+p_2ixv+p_2ixw_2=ie_1+ie_2+s_1e_1+s_2e_2\tag{3}$$

将 $s_1+s_2+i=1$ 代入式（3）中，整理得：

$$x=\frac{(e_1+e_2)i+s_1e_1+s_2e_2}{i(p_1v+p_1w_1+p_2v+p_2w_2)}\tag{4}$$

当 $x=\dfrac{(e_1+e_2)i+s_1e_1+s_2e_2}{i(p_1v+p_1w_1+p_2v+p_2w_2)}$ 时,$\dfrac{\partial E_{\mathrm{df}}}{\partial y}=0$,此时防御方无论是否采取防御检测,得到的期望收益不变;

当 $x>\dfrac{(e_1+e_2)i+s_1e_1+s_2e_2}{i(p_1v+p_1w_1+p_2v+p_2w_2)}$ 时,$\dfrac{\partial E_{\mathrm{df}}}{\partial y}>0$,此时防御方进行防御的期望收益要大于不进行防御的期望收益;

当 $x<\dfrac{(e_1+e_2)i+s_1e_1+s_2e_2}{i(p_1v+p_1w_1+p_2v+p_2w_2)}$ 时,$\dfrac{\partial E_{\mathrm{df}}}{\partial y}<0$,此时防御方不进行防御的期望收益大于进行防御的期望收益。

同理,令 $\dfrac{\partial E_{\mathrm{at}}}{\partial x}=0$,得:

$$\begin{aligned}&p_1i(v-e_1)+(1-p_1)i(-e_1-w_1)+ie_1+iw_1+\\&p_2i(v-e_2)+(1-p_2)i(-e_2-w_2)+ie_2+iw_2=0\\&\Rightarrow\\&y(p_1s_1v+p_1s_1w_1+p_2s_2v+p_2s_2w_2)=s_1w_1+s_2w_2\end{aligned}\tag{5}$$

将式(5)整理得:

$$y=\frac{s_1w_1+s_2w_2}{p_1s_1v+p_1s_1w_1+p_2s_2v+p_2s_2w_2}\tag{6}$$

当 $y=\dfrac{s_1w_1+s_2w_2}{p_1s_1v+p_1s_1w_1+p_2s_2v+p_2s_2w_2}$ 时,$\dfrac{\partial E_{\mathrm{at}}}{\partial x}=0$,此时攻击方无论是否进行攻击,得到的期望收益不变。

当 $y>\dfrac{s_1w_1+s_2w_2}{p_1s_1v+p_1s_1w_1+p_2s_2v+p_2s_2w_2}$ 时,$\dfrac{\partial E_{\mathrm{at}}}{\partial x}<0$,此时攻击方发动攻击的期望收益小于不发动攻击的期望收益。

当 $y<\dfrac{s_1w_1+s_2w_2}{p_1s_1v+p_1s_1w_1+p_2s_2v+p_2s_2w_2}$ 时,$\dfrac{\partial E_{\mathrm{at}}}{\partial x}>0$,此时攻击方发动攻击的期望收益大于不发动攻击的期望收益。

根据上述分析结果可知,攻击方进行攻击的概率和防御方进行防御的概率是互相影响的,攻击方会根据防御方采取的策略去选取最优策略,防御方也会根据攻击方采取的策略去选取自身的最优策略,$\begin{pmatrix}x^*=\dfrac{(e_1+e_2)i+s_1e_1+s_2e_2}{i(p_1v+p_1w_1+p_2v+p_2w_2)},\\ y^*=\dfrac{s_1w_1+s_2w_2}{p_1s_1v+p_1s_1w_1+p_2s_2v+p_2s_2w_2}\end{pmatrix}$ 便是防御方和攻击方进行博弈的混合纳什均衡策略。证毕。

3　微分博弈下 HWSNs 中恶意程序的演化过程

在 HWSNs 中,若合法节点防御成功,会将传感器节点中的恶意程序清除,使恶意节点转化为合法节点。反之,合法节点会被感染成为恶意节点,并可以继续感染其他合法的传感器节点。假设 HWSNs 中共有 N 个节点,其中簇头节点、普通节点、恶意节点的个数分别为 N_1、N_2 和 N_{I}。在单位时间内攻击方会以 x 的概率随机选择一个节点发送恶意程序,防御方会以 y 的概率对信息进行检测。从第 2 节的分析可知,防御方和攻击方最终会采取混合纳什均衡策略作为自己的最优策略,即 $x=x^*$,$y=y^*$。因此攻击方和防御方随时间的演化过程可用式(7)表示。

$$\begin{cases}\dfrac{\mathrm{d}N_{\mathrm{I}}}{\mathrm{d}t}=x^*(1-y^*)(s_1+s_2)N_{\mathrm{I}}+(1-p_1)x^*y^*s_1N_{\mathrm{I}}+\\(1-p_2)\cdot x^*y^*s_2N_{\mathrm{I}}-p_1x^*y^*s_1N_{\mathrm{I}}-p_2x^*y^*s_2N_{\mathrm{I}}\\\dfrac{\mathrm{d}N_1}{\mathrm{d}t}=p_1x^*y^*s_1N_{\mathrm{I}}-x^*(1-y^*)s_1N_{\mathrm{I}}-(1-p_1)x^*y^*s_1N_{\mathrm{I}}\\\dfrac{\mathrm{d}N_2}{\mathrm{d}t}=p_2x^*y^*s_2N_{\mathrm{I}}-x^*(1-y^*)s_2N_{\mathrm{I}}-(1-p_2)x^*y^*s_2N_{\mathrm{I}}\\N=N_1+N_2+N_{\mathrm{I}}\end{cases}\tag{7}$$

式(7)同时除以 N 整理得:

$$\frac{\mathrm{d}i}{\mathrm{d}t}=i[x^*(1-i)-2x^*y^*(-p_1s_1-p_2s_2)]\tag{8}$$

由式(8)可知,HWSNs 中恶意节点所占的比例与表 2 中的博弈模型参数有关,博弈模型中的参数决定了恶意节点在博弈过程中的演化过程。

4　数值模拟与仿真

4.1　博弈过程中攻防双方的收益数值模拟

令 $v=2$,$w_1=3$,$w_2=2.3$,$e_1=1$,$e_2=0.85$,$e_{\mathrm{M}}=0.5$,$i=0.3$,$s_1=0.1$,$s_2=0.6$,$p_1=0.85$,$p_2=0.75$,此时 $x^*=\dfrac{(e_1+e_2)i+s_1e_1+s_2e_2}{i(p_1v+p_1w_1+p_2v+p_2w_2)}=0.52$,$y^*=\dfrac{s_1w_1+s_2w_2}{p_1s_1v+p_1s_1w_1+p_2s_2v+p_2s_2w_2}=0.71$。分别对防御方和攻击方的收益进行数值模拟,结果如图 2 和图 3 所示。由图 2 可以得出,$x=0.52$ 时,防御方的收益和 y 的取值无关;当 $x>0.52$ 时,防御方的收益和 y 的取值成正相关,故防御方应采取检测策略增大自身的收益。当 $x<0.52$ 时,防御方的收益和 y 的取值成负相关,故防御方应采取不检测策略。由图 3 可以得出,当 $y=0.71$ 时,攻击方的收益和 x 的取值无关;当 $y>0.71$ 时,攻击方的收益和 x 的取值成负相关;当 $y<$

0.71 时,攻击方的收益和 x 的取值成正相关。实验模拟的结果与理论分析一致。

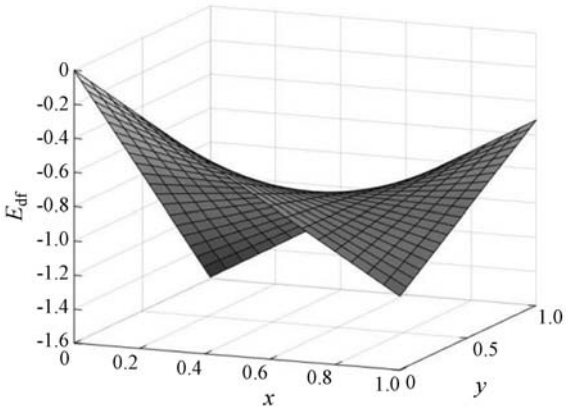

图 2 博弈过程中防御方期望收益随策略的变化

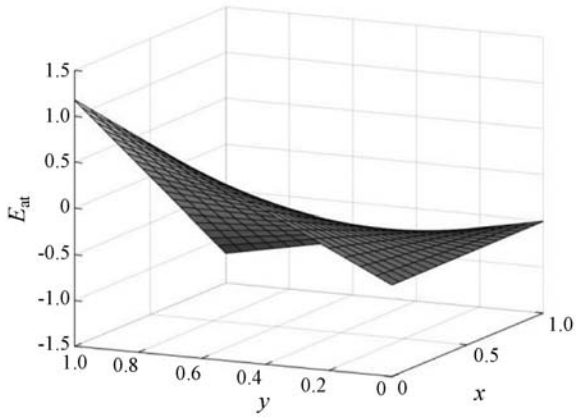

图 3 博弈过程中攻击方期望收益随策略的变化

4.2 博弈过程中恶意程序演化趋势数值模拟

在 HWSNs 中,防御方和攻击方节点状态随着博弈过程的演化趋势如式(7)所示,式(8)是该博弈系统的解析解。对式(8)进行模拟实验,实验结果如图 4 至图 7 所示。其中,图 4 – 图 6 分别描述了博弈参数 e_1 和 e_2 取不同的值时对 HWSNs 恶意程序传播的影响,图 7 描述了防御方的恶意程序检测率取不同的值时对 HWSNs 恶意程序传播的影响。

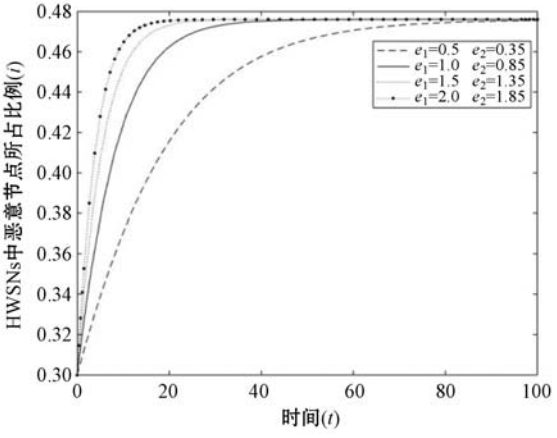

图 4 $v > w_1 > w_2$ 时恶意节点所占比例演化趋势

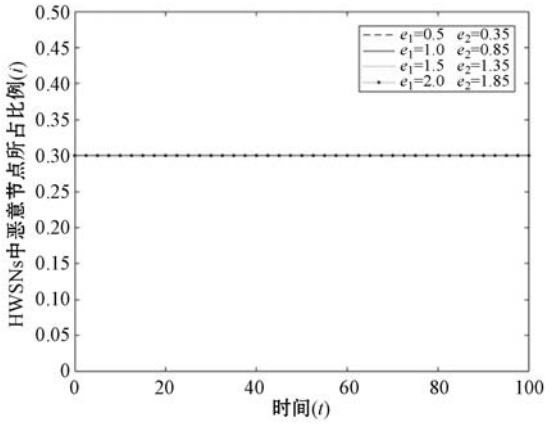

图 5 $v = w_1 = w_2$ 时恶意节点所占比例演化趋势

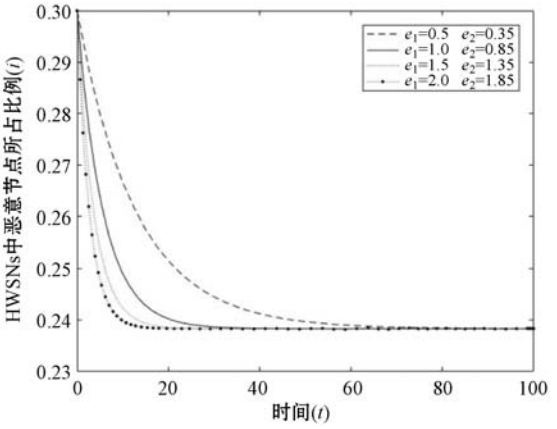

图 6 $w_1 > w_2 > v$ 时恶意节点所占比例演化趋势

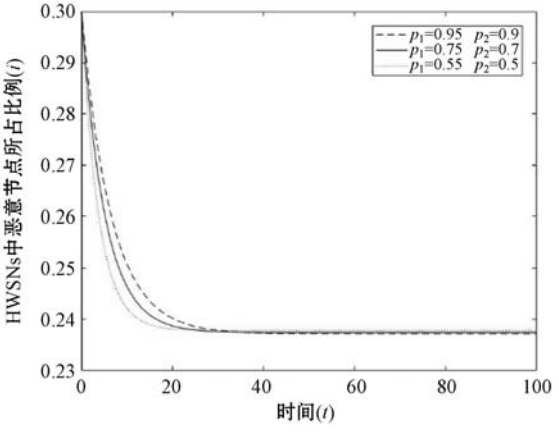

图 7 p_1、p_2 对恶意节点所占比例演化趋势的影响

由图 4 可知,当 $v > w_1 > w_2$ 时,有 $x^*(1-y^*)(s_1+s_2)N_I + (1-p_1)x^*y^*s_1N_I + x^*y^*s_2N_I \cdot (1-p_2) > p_1x^*y^*s_1N_I + p_2x^*y^*s_2N_I$,即在博弈初始阶段,正常节点被恶意程序感染的节点数要大于恶意节点恢复正常的节点数,故恶意节点在 HWSNs 中所占比例随着演化过程会逐渐增大直到博弈双方处于混合纳什均衡状态,最后趋于稳定。当防御方检测恶意程序所需的能量 e_1 和 e_2 增大时,由博弈双方混合纳什均衡可知,防御方选择检测的概率 y^* 不变,恶意程序选择攻击的概率 x^* 增大,故恶意程序传播的速率更快。

由图 5 可知,当 $v = w_1 = w_2$ 时,有 $x^*(1-y^*)(s_1+$

$s_2)N_I+(1-p_1)x^*y^*s_1N_I+x^*y^*s_2N_I\cdot(1-p_2)=p_1x^*y^*s_1N_I+p_2x^*y^*s_2N_I$,此时整个博弈系统中的恶意节点被修复的节点数和正常节点被恶意程序感染的节点数相同,故恶意节点在 HWSNs 中所占的比例始终保持初始值不变。当防御方检测恶意程序所需的能量 e_1 和 e_2 增大时,由防御方和攻击方的演化微分方程组可知,恶意节点增加的数量和被检测修复的数量始终相等,因此恶意节点在该状态下始终保持初始比例不变,不受 e_1 和 e_2 变化的影响。

由图 6 可知,当 $w_1>w_2>v$ 时,有 $x^*(1-y^*)(s_1+s_2)N_I+(1-p_1)x^*y^*s_1N_I+x^*y^*s_2N_I\cdot(1-p_2)<p_1x^*y^*s_1N_I+p_2x^*y^*s_2N_I$,即在博弈初始阶段,恶意节点恢复正常的节点数要大于正常节点被恶意程序感染的节点数,故恶意节点在 HWSNs 中所占比例随着演化过程会逐渐减小直到博弈双方处于混合纳什均衡状态,最后趋于稳定。当防御方检测恶意程序所需的能量 e_1 和 e_2 增大时,防御方选择检测的概率大于不检测的概率,即 $y^*>1-y^*$,导致恶意节点选择攻击的概率也会增大。此时恶意节点进行攻击时,被检测恢复成正常节点的概率要大于恶意节点不被检测的概率,因此恶意节点被检测恢复成正常节点的速度也会更快。

由图 7 可知,当 $w_1>w_2>v$ 并且 e_1 和 e_2 值相同时,恶意节点在 HWSNs 系统中所占比例减少的速率,随着防御方检测率的减少而增大。当 p_1 和 p_2 值增大时,y^* 减小,即防御方选择检测的概率减少,则在博弈的过程中,攻击方在选择攻击策略时,被防御方检测恢复成正常节点的速度会变慢。

5　结　语

本文采用微分博弈的方式对 HWSNs 中攻击方和防御方的最优策略进行分析与研究。通过本文的分析与研究可知:攻击方的攻击策略是动态变化的过程,与 HWSNs 中的攻击方恶意节点所占比例有关;攻击方传播恶意程序的演化过程受到博弈参数的影响,可以通过合理地改变博弈参数达到抑制攻击方传播恶意程序的目的。

参 考 文 献

[1] 曾建电,王田,贾维嘉,等. 传感云研究综述[J]. 计算机研究与发展,2017,54(5):925 – 939.

[2] 刘策,闵新力,薛君志,等. 基于无线传感器的环境监控系统[J]. 计算机应用与软件,2015,32(1):98 – 101.

[3] 王潮,胡广跃,张焕国. 无线传感器网络的轻量级安全体系研究[J]. 通信学报,2012,33(2):30 – 35.

[4] Han G, Li X, Jiang J, et al. Intrusion detection algorithm based on neighbor information against sinkhole attack in wireless sensor networks[J]. The Computer Journal, 2015, 58(6):1280 – 1292.

[5] 池玉辰,邓平. 一种移动无线传感器网络抵御虫洞攻击 MCL 算法[J]. 传感技术学报,2015,28(6):876 – 882.

[6] Lyu C, Zhang X, Liu Z, et al. Selective authentication based geographic opportunistic routing in wireless sensor networks for internet of things against dos attacks[J]. IEEE Access, 2019, 7:31068 – 31082.

[7] Zhang Z, Liu S, Bai Y, et al. M optimal routes hops strategy: Detecting sinkhole attacks in wireless sensor networks[J]. Cluster Computing, 2019, 22:7677 – 7685.

[8] Huang J, Ho D, Li F, et al. Secure remote state estimation against linear man-in-the-middle attacks using watermarking[J]. Automatica, 2020, 121:109182.

[9] 朱建明,王秦. 基于博弈论的网络空间安全若干问题分析[J]. 网络与信息安全学报,2015,1(1):43 – 49.

[10] 黄健明,张恒巍,王晋东,等. 基于攻防演化博弈模型的防御策略选取方法[J]. 通信学报,2017,38(1):168 – 176.

[11] 丁绍虎,齐宁,郭义伟. 基于 M-FlipIt 博弈模型的拟态防御策略评估[J]. 通信学报,2020,41(7):186 – 194.

[12] 刘妮,周海平,王波. 面向多种攻击的无线传感器网络攻防博弈模型[J]. 计算机应用研究,2020,37(8):2491 – 2495.

[13] Shen S, Zhou H, Feng S, et al. HSIRD: A model for characterizing dynamics of malware diffusion in heterogeneous WSNs[J]. Journal of Network and Computer Applications, 2019, 146:102420.

[14] 孙骞,薛雷琦,高岭,等. 基于随机博弈与禁忌搜索的网络防御策略选取[J]. 计算机研究与发展,2020,57(4):767 – 777.

[15] 沈士根,周海平,黄龙军,等. 基于扩展传染病模型的异质传感网恶意程序传播建模与分析[J]. 传感技术学报,2019,32(6):923 – 930.

[16] 张红,沈士根,吴小军,等. 基于元胞自动机和静态贝叶斯博弈的 WSN 恶意程序传染模型[J]. 电信科学,2019,35(6):60 – 69.

[17] 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.

[18] 周海平,沈士根,黄龙军,等. 攻防博弈驱动下的无线传感器网络病毒传播模型[J]. 计算机应用研究,2020,37(3):847 – 850.

[19] 周海平,沈士根,冯晟,等. 基于微分博弈的无线传感器网络恶意程序传播模型[J]. 传感技术学报,2019,32(6):931 – 939.