DOI: 10.13382/j.jemi.B2306568

基于演化博弈的无线传感器网络入侵检测研究*

王心怡 行鸿彦 侯天浩 郑锦程
(南京信息工程大学电子与信息工程学院 南京 210044)

摘 要:针对无线传感器网络易遭受内部节点攻击的问题,本文提出了一种基于演化博弈的无线传感器网络入侵检测方法。将传感器网络的攻防对抗映射到博弈过程中,建立恶意节点和簇头节点之间的攻防博弈模型,改进传统复制动态方程,使得簇头节点在演化博弈过程中考虑到其他节点的历史策略,预测恶意节点的攻击策略;同时将改进复制动态方程应用于入侵检测算法,提高算法响应时间。实验表明,与传统方法的复制动态方程相比,采用该算法使得演化博弈能够快速达到均衡,收敛速度相比传统方法提高了 80%,保障了网络安全性的同时避免了传感器网络检测能量的消耗。

关键词: 无线传感器网络;入侵检测;演化博弈;改进的复制动态方程
中图分类号: TP393; TN911.7 **文献标识码**:A **国家标准学科分类代码**: 510.40

Research on wireless sensor network intrusion detection based on evolutionary game

Wang Xinyi Xing Hongyan Hou Tianhao Zheng Jincheng
(School of Electronics and Information Engineering, Nanjing University of Information Science & Technology, Nanjing 210044, China)

Abstract: In the context of wireless sensor networks (WSNs), prone to internal node attacks, this study advances an intrusion detection approach underpinned by evolutionary game theory. The attack-defense confrontation of sensor networks is mapped into the game process, and the attack-defense game model between malicious nodes and cluster head nodes is established. The traditional replication dynamic equation is improved, so that the cluster head node takes the historical strategies of other nodes in the evolutionary game process to predict the attack strategy of malicious nodes. At the same time, the improved replication dynamic equation is applied to the intrusion detection algorithm to improve the response time of the algorithm. Experiments show that compared with the replication dynamic equation of the traditional method, the evolutionary game can quickly reach equilibrium by using this algorithm, and the convergence speed is 80% higher than that of the traditional method, which ensures the network security and avoids the consumption of sensor network detection energy.

Keywords: wireless sensor network; intrusion detection; evolutionary game; improved replication dynamic equation

0 引 言

无线传感器网络(wireless sensor networks, WSNs)是由分散在监测区域内的微型智能传感器节点通过无线通信方式互相连接组成的[1],能够实时监测、感知和采集节点区域内的环境和各类信息,并对这些信息进行加工处理后以无线的方式发送给基站。但 WSNs 具有监测环境复杂、无线传输信道带宽有限且易受外界干扰等特点[2-3],使得 WSNs 易遭受来自网络外部和内部的攻击,尤其是内部节点的攻击难以被预测发现。常见的 WSNs 节点攻击类型有:欺骗攻击,攻击节点伪装成正常节点;拒绝服务攻击,攻击节点发送虚假信息消耗网络资源;篡改攻击,攻击节点在传输中修改数据内容;隐私泄露攻击,攻击节点通过监听得到基站敏感信息等。

入侵检测系统(intrusion detection system, IDS)是一种可以快速检测到内部节点攻击并主动采取反应措施的网络安全设备,能够有效维护网络安全[4],将入侵检测系

收稿日期:2023-05-29 Received Date: 2023-05-29
*基金项目:国家重点研发计划(2021YFE0105500)、国家自然科学基金(62171228)项目资助

统最优化利用在无线传感器网络中具有重大的研究意义。

随着 WSNs 的不断普及和应用,IDS 作为保障网络信息安全的一种有效手段,迅速成为这一领域的研究热点[5]。传统的网络入侵检测算法通常基于统计模型、网络节点分类、神经网络等方法。Denning[6] 利用数学统计相关理论对节点采集的信息进行网络特征分析,提出了基于统计模型的入侵检测算法;Loannis 等[7] 提出一种适用于传感器网络的分布式入侵检测方法,通过划分网络实现节点监控邻居,使得邻近节点协同工作;Jin 等[8] 提出一种基于多智能体和节点信任值的入侵检测方案,在节点上建立多智能体模型框架并定义典型节点信任输信,并用马氏距离理论判断节点是否正常,实现较高的检测率;Hu 等[9] 引入改进的神经网络算法,建立用于发现恶意节点的入侵检测模型,通过规则库实时采集和分析反补偿数据,提高入侵检测率。

近年来,基于博弈论的入侵检测方法也引起了广泛的关注和应用。Lye 等[10] 构建了攻击者和防御者之间的静态博弈模型,但是忽略了攻防双方的动态变化;Han 等[11] 提出了一种基于博弈论和自回归模型的入侵检测算法,将传统自回归模型改进成非合作完全信息的博弈模型,提出最优决策算法求解检测算法的混合纳什均衡解,降低了系统检测能耗;陈行等[12] 将贝叶斯博弈理论引入到无线网络入侵检测,根据博弈中的完美均衡设计入侵检测时间间隔调整算法 TSMA-BG 和参数修正算法 DPMA,有效地检测出发生变化的攻击行为。陈赵懿等[13] 利用博弈论原理,分析 Ad Hoc 网络入侵防御系统与攻击者之间的攻防过程,建立了多阶段动态博弈下的网络风险预测模型,量化攻防效用矩阵,得到攻防双方最优混合策略。孙薇等[14] 利用演化博弈建立攻防模型,根据攻击方与防守方的群体复制动态关系推演信息安全攻防对抗的规律,为解决信息安全问题提供新思路。上述方法都在一定程度上改善了检测效果,但面对日益复杂的网络环境和难以检测的内部节点攻击,现有的许多方法不能有效检测和抑制节点攻击。

演化博弈建立在有限理性条件下,具有动态过程演化的特征,能更好地描述和分析网络攻防过程。因此,本文从网络攻防实际出发,引入演化博弈理论,建立恶意节点和簇头节点的博弈模型,改进传统复制动态方程,预测节点短期策略并及时调整簇头节点检测概率抑制攻击,使得演化博弈能够快速达到稳定均衡,在节约检测能量的同时抑制入侵攻击。

1 无线传感器网络演化博弈模型

博弈论是一种用来研究具有竞争性质的数学理论和方法,可以为研究 WSNs 入侵检测技术提供新思路,将 WSNs 内部节点的攻防过程看作博弈过程,攻防节点双方会根据当前的网络环境状态、自身收益信息不断调整策略,达到最优状态。

演化博弈不同于传统的博弈论,结合了生物进化的思想[15],是一种把博弈理论与动态演化过程相融合的理论。演化博弈认为博弈参与者是在不断试错的过程中来学习其他策略,从而不断反复最终达到最优策略。该方法既保留了传统对博弈论中的有限理性,又充分考虑了博弈过程的动态性,更符合现实中的网络对抗问题。

1.1 网络节点分簇

为了节约节点的能量和提高处理数据的效率,对网络节点进行分类[16]。如图 1 所示,网络被划分为不同的簇,每个簇由一个簇头节点和多个成员节点组成,成员节点负责收集和发送网络中的各类信息,簇头节点对接收到的信息进行融合处理后再转发给基站。然而,成员节点中可能存在恶意节点,对 WSNs 发起内部攻击,例如内部节点选择性转发或者拒绝转发有效信息,甚至成为伪装节点伺机对网络发起攻击,破坏 WSNs 稳定状态。

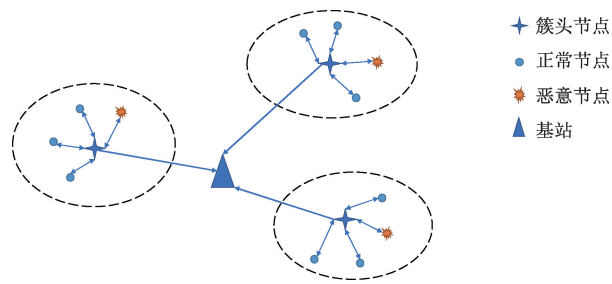


图 1 WSNs 分簇模型

Fig. 1 WSNs clustering model

簇头节点对于成员节点发送的信息可以选择检测或者不检测,若检测到恶意节点的攻击,则对其进行入侵检测;而恶意节点为了避免被检测,会选择伪装成正常节点发送有效信息,寻找合适的机会再进行攻击。研究发现,当 IDS 检测到恶意节点时,直接隔离恶意节点不能为 WSNs 节省能耗,相反,利用恶意节点在伪装时发送的有效数据假意合作能带来更大的收益[17]。

1.2 演化博弈模型

基于恶意节点和簇头节点的网络分簇,建立关于 WSNs 的演化博弈模型[18],表示为一个五元组 $(N,S,X,U,\dot{P})$:

1) $N=(N_A,N_D)$ 是博弈参与者空间。群体博弈发生在一个所有群体共同存在的空间中,在无线传感器网络中,存在两个参与博弈的群体,即攻击方和检测方。$N_A=N_{A1},N_{A2},N_{A3},\cdots,N_{Aj}$ 表示恶意节点的参与者集合;$N_D=N_{D1},N_{D2},N_{D3},\cdots,N_{Di}$ 表示簇头节点的参与者集合。

2) $S=(S_A,S_D)$ 是博弈参与者策略集合空间。恶意节点 $S_A=\{$攻击,合作$\}$,簇头节点 $S_D=\{$检测,不检测$\}$。

3) $X=(X_A,X_D)$ 是博弈双方的策略概率分布。$X_A=\alpha,1-\alpha,\alpha$ 表示恶意节点攻击的概率,$1-\alpha$ 表示恶意节点选择假意合作的概率;$X_D=\beta,1-\beta,\beta$ 表示簇头节点检测的概率,$1-\beta$ 表示簇头节点不检测的概率。

每个群体中的个体从属于自己群体的策略集中选择策略,设一个群体中选择某个策略的个体状态为 x_j^A 或 x_i^D。

4) $U=(U_A,U_D)$ 表示博弈双方的收益。

恶意节点的平均收益:

$$\bar{U}_A=\sum_{i\in S^A}x_j^A\cdot U_{Aj}((1\leqslant m\leqslant j) \tag{1}$$

簇头节点的平均收益:

$$\bar{U}_D=\sum_{i\in S^D}x_i^D\cdot U_{Di}((1\leqslant n\leqslant i) \tag{2}$$

5) $\dot{P}=(\dot{P}_A,\dot{P}_D)$ 表示对博弈双方下一阶段策略的短期预测。

在演化博弈的过程中,收益低的参与者会向高收益者进行学习,不断优化改进自身策略,这就导致不同策略的比例会随时间推移发生变化。策略变化可以表示为一个与时间相关的函数,其动态变化速率通过复制动态方程表示,以试错的方式不断寻优。

假设节点通过模仿其他节点的策略来调整自己的策略:每个节点随机从传感器网络中选择一个模仿对象,每个节点策略被选择作为模仿对象的概率正比于这个策略在传感器网络中所占的比例,如果模仿对象策略的收益大于这个节点本身策略的收益,则该节点以正比于两者收益差的概率采用模仿对象的策略;否则,该节点保持其原来策略不变。

基于上述规则,得到复制动态方程定义如下:

$$\dot{x}_i=\frac{\mathrm{d}x}{\mathrm{d}t}=x_i(U_i-\bar{U}) \tag{3}$$

式(3)描述了博弈中节点选择策略比例的变化率,即节点在博弈过程中如何调整自己的策略。在复制动态方程的思想下,簇头节点检测时考虑了其他节点的历史策略,不断调整策略逼近期望收益最大值,使得节点具有学习和动态调整的能力。

1.3　演化稳定均衡

在演化博弈过程中,博弈双方不再将纳什均衡作为最后的策略选择,而是在不断竞争、学习和模仿中,逐步寻求演化稳定均衡解。

根据 WSNs 攻防的实际情况,给出如表 1 所示定义求解演化稳定均衡解。

为使簇头节点的检测和恶意节点的攻击有意义,满足:$A_1>W>D,B_1>C_1,A_2>Q,B_2>C_2$。

表 1　收益符号定义

Table 1　Benefit symbol definition

符号表示	符号含义
A_1	恶意节点数据转发成功的收益
B_1	恶意节点攻击成功的收益
C_1	恶意节点攻击被检测到的损失
D	恶意节点攻击未被检测到的收益
W	恶意节点假意合作成功发送有效信息的收益
A_2	簇头节点将数据转发给基站的收益
B_2	簇头节点检测到攻击的收益
C_2	簇头节点没有检测到攻击的损失
Q	簇头节点使用 IDS 检测数据的能耗

基于此得到演化博弈模型的收益矩阵如表 2 所示。

表 2　演化博弈双方收益矩阵

Table 2　Evolutionary game payoff matrix

恶意节点/簇头节点	检测(β)	不检测($1-\beta$)
攻击(α)	A_1-C_1+D,A_2+B_2-Q	A_1+B_1,A_2-C_2
合作($1-\alpha$)	A_1+W,A_2-Q	A_1,A_2

恶意节点和簇头节点的平均收益可表示为:

$$\bar{U}_A=\alpha\beta(A_1-C_1+D)+\alpha(1-\beta)(A_1+B_1)+(1-\alpha)\beta(A_1+W)+(1-\alpha)(1-\beta)A_1 \tag{4}$$

$$\bar{U}_D=\beta\alpha(A_2+B_2-Q)+\beta(1-\alpha)(A_2-Q)+(1-\beta)\alpha(A_2-C_2)+(1-\beta)(1-\alpha)A_2 \tag{5}$$

根据复制动态方程原理,博弈模型中恶意节点、簇头节点的收益函数 $\bar{U}_A$、$\bar{U}_D$ 对攻击率 α、检测率 β 的偏导:

$$\partial_\alpha U_A(\alpha,\beta)=\frac{\partial U_A(\alpha,\beta)}{\partial\alpha}=\beta(D-B_1-C_1-W)+B_1 \tag{6}$$

$$\partial_\beta U_D(\alpha,\beta)=\frac{\partial U_D(\alpha,\beta)}{\partial\beta}=\alpha(B_2+C_2)-Q \tag{7}$$

令:

$$f(X,t)=\begin{pmatrix}\partial_\alpha U_A(\alpha,\beta)\\ \partial_\beta U_D(\alpha,\beta)\end{pmatrix}=0 \tag{8}$$

得到系统唯一的平衡态:

$$X_1=\begin{pmatrix}\alpha^*\\ \beta^*\end{pmatrix}=\begin{pmatrix}\dfrac{Q}{B_2+C_2}\\ \dfrac{B_1}{B_1+C_1+W-D}\end{pmatrix} \tag{9}$$

建立雅可比矩阵:

$$\boldsymbol{J}(X)=\begin{pmatrix}\dfrac{\partial U_A(\alpha,\beta)}{\partial\alpha} & \dfrac{\partial U_A(\alpha,\beta)}{\partial\beta}\\ \dfrac{\partial U_D(\alpha,\beta)}{\partial\alpha} & \dfrac{\partial U_D(\alpha,\beta)}{\partial\beta}\end{pmatrix} \tag{10}$$

将求解出的均衡点代入雅可比矩阵,会得到对角矩

阵 $\begin{pmatrix} 0 & \Delta_1 \\ \Delta_2 & 0 \end{pmatrix}$，其中：

$$\Delta_1 = \frac{Q(D - B_1 - C_1 - W) + W(B_2 + C_2)}{(B_2 + C_2)} < 0,$$

$$\Delta_2 = \frac{B_1(B_2 + C_2) - Q(B_1 + C_1 + W - D)}{(B_1 + C_1 + W - D)} < 0$$

由于矩阵特征值中不存在负实部特征值，由李雅普诺夫(Lyapunov)稳定性理论[19]可知，基于演化博弈的入侵检测算法不具有渐进稳定性，求得的唯一平衡点 X_1 为 Lyapunov 意义下的临界稳定状态。

1.4 复制动态方程

在动态演化的过程中，如果某一策略的收益大于 WSNs 整体的平均收益，那么这个策略在网络中所占的比例就会增长；相反，如果某一策略的收益小于 WSNs 整体的平均收益，那么这个策略在网络中所占的比例就会下降。同时，一个策略所占比例的平均增长率或下降率正比于这个策略的收益与整个网络平均收益的差。

本文中，恶意节点和簇头节点的传统复制动态方程分别表示为：

$$\dot{x}_{Aj} = U_{Aj}(t) - \bar{U}_A(t) \tag{11}$$

$$\dot{x}_{Di} = U_{Di}(t) - \bar{U}_D(t) \tag{12}$$

其中，$U_{Aj}(t)$ 表示恶意节点 N_{Aj} 在 t 时刻采取策略 S_{Aj} 的收益，$\bar{U}_A(t)$ 表示恶意节点在 t 时刻的平均收益；$U_{Di}(t)$ 表示簇头节点 N_{Di} 在 t 时刻采取策略 S_{Di} 的收益，$\bar{U}_D(t)$ 表示簇头节点在 t 时刻的平均收益。

除了上述传统的策略调整方法，复制动态方程还可由其他状态调整协议生成，如 BNN 动力学方程、Logit 动力学方程等。

1) BNN 动力学方程

BNN(brown-von neumann-nash dynamics)动力学[20]假设：每个个体从所有策略中随机选择一个新策略，如果这个新策略的收益大于整个群体的平均收益，那么该个体以正比两者收益差的概率采用新策略，否则保持不变。

在这种方式下，整个群体状态的复制动态方程如下：

$$\dot{x}_i = \sum_{j \in S} x_j [U_i - \bar{U}]_+ - x_i \sum_{j \in S} [U_j - \bar{U}]_+, \forall i,j \in S \tag{13}$$

2) Logit 动力学方程

Logit 动力学[21]假设：每个个体从所有策略中随机选择一个新策略，并以与新策略成比例的概率改变策略。Logit 动力学引入理性选择强度参数 η，用来衡量博弈者自身的理性程度，得到复制动态方程如下：

$$\dot{x}_i = \frac{\exp(\eta^{-1} U_i)}{\sum_{j \in S} \exp(\eta^{-1} U_j)} - x_i, \eta > 0, \forall i,j \in S \tag{14}$$

1.5 复制动态方程的优化与改进

传统的复制动态方程虽然可以衡量演化博弈的动态变化、对博弈过程进行稳定性分析，但是收敛速度慢，达到演化均衡不够稳定，因此提出改进复制动态方程，优化基于演化博弈的入侵检测模型的响应决策。

实际上，簇头节点的收益是对恶意节点攻击策略的逻辑映射[22]，定义响应系数 γ，则：

$$U_{Di}(t) = \gamma \cdot [X_{Aj}(t)] \tag{15}$$

在演化博弈模型的定义中，与传统博弈论不同，增加 $\dot{P} = (\dot{P}_A, \dot{P}_D)$ 表示为对博弈双方下一阶段策略的短期预测。在非合作不完全信息的博弈条件下，簇头节点可以利用 IDS 获取 t 时刻历史博弈信息，并根据该数据对恶意节点下一步采取的策略作一个短期的预测，簇头节点的收益可以表示为对恶意节点攻击策略和对攻击策略变化率短期预测的联合响应：

$$U_{Di}(t) = \gamma \cdot [X_{Aj}(t) + \hat{P}_{Aj}(t)] \tag{16}$$

结合 Logit 动力学，将理性选择强度参数引入传统复制动态方程，得到改进后的簇头节点复制动态方程，在理论上具有更快的响应能力：

$$\dot{x}_{Di}(t) = U_{Di}(t) - \bar{U}_D(t) = \frac{\exp\{\eta^{-1} \cdot \gamma \cdot [X_{Aj}(t) + \dot{P}_{Aj}(t)]\}}{\sum_{j \in S} \exp(\eta^{-1} U_{Aj})} - \bar{U}_D(t) \tag{17}$$

2 演化博弈实验与分析

演化博弈论摒弃经典博弈论中完全信息和完全理性两种假设，利用自然选择、突变等机制，分析和预测参与个体的策略演化过程和动态平衡。其核心特征在于群体博弈中的群体状态随时间变化的动态过程，并通过群体状态的演化特性说明群体在博弈中的决策行为。演化博弈模型如图 2 所示。

2.1 演化博弈仿真

对基于演化博弈的 WSNs 入侵检测过程进行模拟仿真，借助 ode45 函数求解微分方程。在实验中，设置演化博弈有两个种群，每个种群有两个策略(簇头节点检测/不检测、恶意节点攻击/合作)，相同条件下所提改进复制动态方程与传统复制动态方程、BNN 动力学方程、Logit 动力学方程进行比较。

基于改进复制动态方程的演化博弈参数设置如下：种群 $P = 2$；每个种群纯策略数 $n = 2$；迭代时间 $t = 30$ s；Logit 复制方程理性选择强度参数 $\eta = 0.08$。

假设簇头节点和恶意节点各参数收益如表 3 所示。

2.2 实验结果与分析

1) 传统复制动态方程

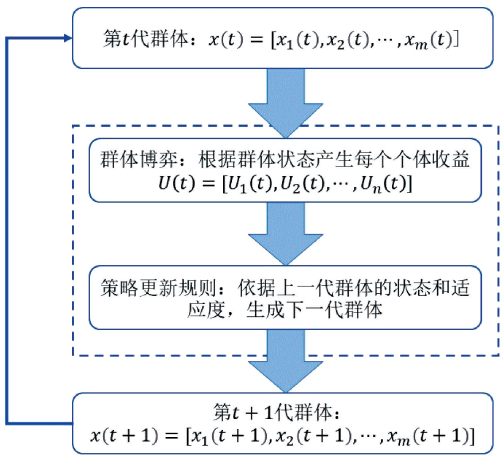


图 2　演化博弈模型

Fig. 2　Evolutionary game model diagram

表 3　演化博弈收益矩阵参数设置

Table 3　Evolutionary game payoff matrix parameter setting

符号表示	符号含义	假设值
A_1	恶意节点数据转发成功的收益	1
B_1	恶意节点攻击成功的收益	2
C_1	恶意节点攻击被检测到的损失	1
D	恶意节点攻击未被检测到的收益	1
W	恶意节点假意合作成功发送有效信息的收益	1
A_2	簇头节点将数据转发给基站的收益	3
B_2	簇头节点检测到攻击的收益	1
C_2	簇头节点没有检测到攻击的损失	2
Q	簇头节点使用 IDS 检测数据的能耗	2

图 3 表示博弈双方采用传统复制动态方程的演化博弈过程。如图 3(a)所示，当恶意节点的初始攻击概率大于簇头节点初始检测概率时，簇头节点检测到攻击后快速提高 IDS 的检测概率，抑制了恶意节点的攻击，使得博弈达到演化均衡；当恶意节点的初始攻击概率小于簇头节点初始检测概率时，簇头节点能及时调整自身策略，抑制恶意节点攻击的同时减少检测能量的损耗，如图 3(b)所示；图 3(c)说明，簇头节点初始检测概率略大于恶意节点攻击概率时，簇头节点为节省检测能耗会主动降低检测概率，但当恶意节点攻击时，簇头节点也能快速提高检测策略，演化博弈收敛到稳定均衡状态。

2) BNN 动力学方程

图 4 表示博弈双方采用 BNN 动力学方程的演化博弈过程。当恶意节点、簇头节点之间的初始概率相差较大时，簇头节点都能及时调整策略，对恶意节点的攻击做出回应，提高或适当降低检测概率，一定程度上减少 IDS 检测能耗，如图 4(a)和(b)所示；当两者初始概率相近时，如果恶意节点保持攻击概率不变，很大可能会被检测

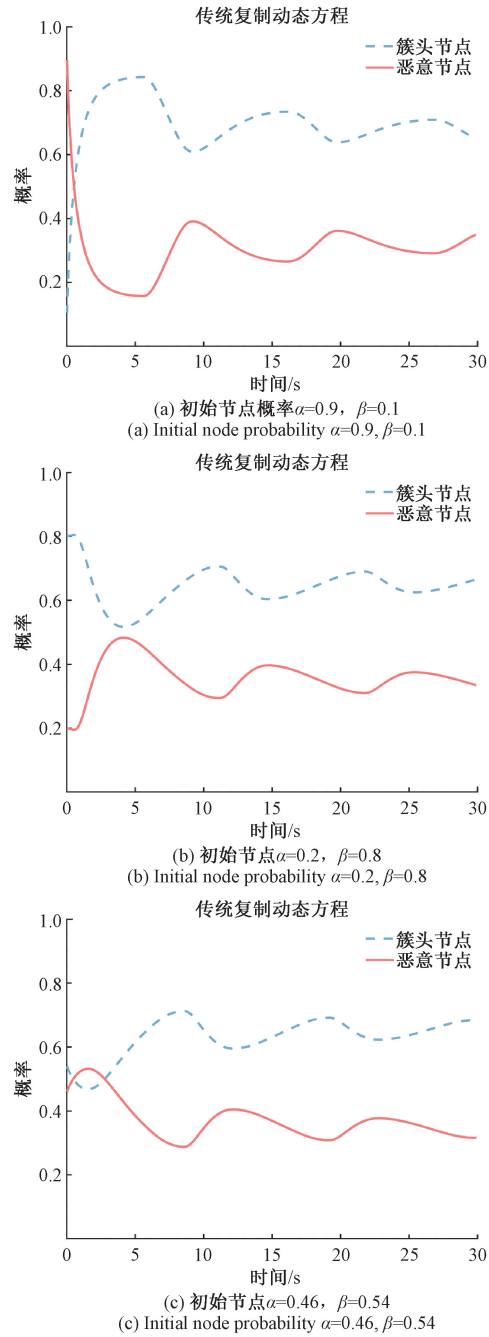


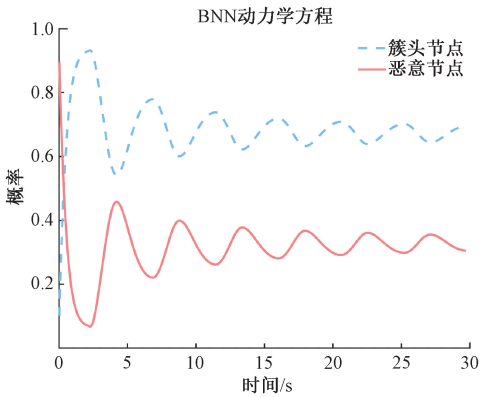
图 3　基于传统复制动态方程的演化博弈过程

Fig. 3　Evolutionary game process based on traditional replication dynamic equation

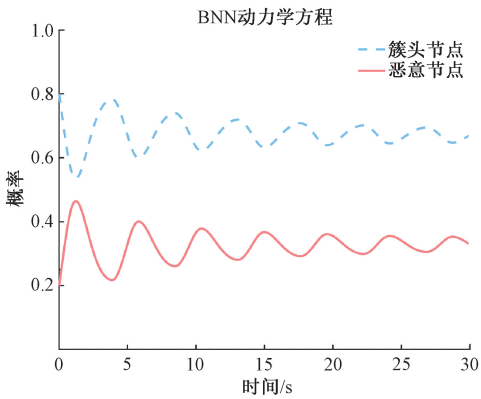
到从而导致收益降低，因此恶意节点选择降低攻击概率，此时簇头节点也不用大幅提高检测概率，整个博弈逐步达到演化均衡，如图 4(c)所示。

3) Logit 动力学方程

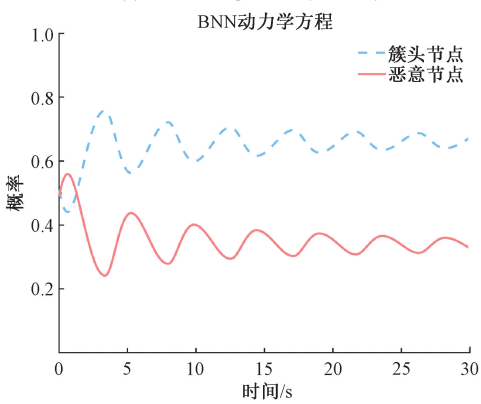
图 5 表示博弈双方采用 Logit 动力学方程的演化博弈过程。如图 5(a)所示，当恶意节点概率大于簇头节点概率时，簇头节点能快速做出反应调整策略，有效抑制恶



(a) 初始节点α=0.9，β=0.1
(a) Initial node probability α=0.9, β=0.1



(b) 初始节点α=0.2，β=0.8
(b) Initial node probability α=0.2, β=0.8

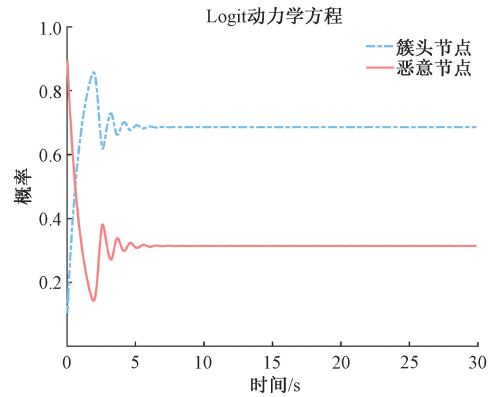


(c) 初始节点α=0.49，β=0.51
(c) Initial node probability α=0.49, β=0.51

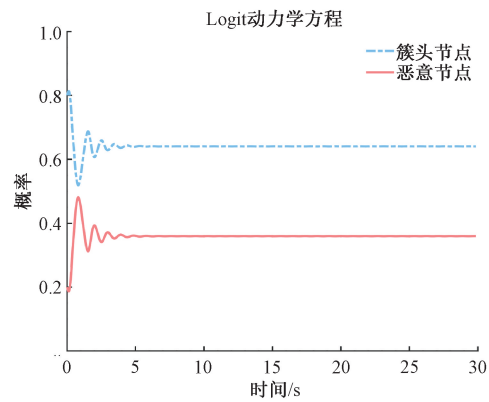
图 4　基于 BNN 动力学方程的演化博弈过程

Fig. 4　Evolutionary game process based on BNN dynamic equation

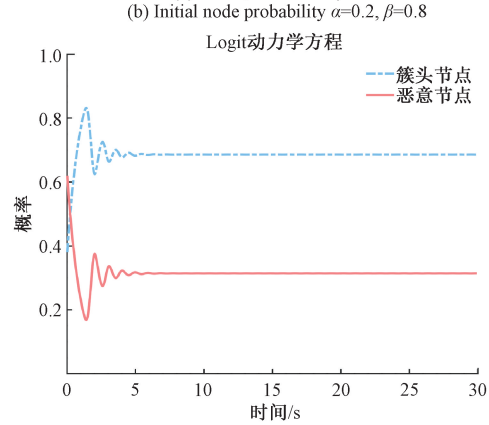
意节点的攻击，达到演化均衡的速度相较于 BNN 动力学方程又有了进一步的提升；如图 5(b)所示，恶意节点为了更高的攻击收益选择提高攻击概率，而簇头节点为了减少检测能耗降低检测概率但其检测概率始终高于恶意节点攻击概率；如图 5(c)所示，两者初始概率适中的情况下，达到博弈平衡后，节点的概率不再有大幅度变化，这是因为簇头节点和恶意节点是通过对方策略变化来进行策略选择的，因此在博弈平衡后，博弈双方根据对方情况做出理性选择，概率不再变化。



(a) 初始节点α=0.9，β=0.1
(a) Initial node probability α=0.9, β=0.1



(b) 初始节点α=0.2，β=0.8
(b) Initial node probability α=0.2, β=0.8



(c) 初始节点α=0.62，β=0.38
(c) Initial node probability α=0.62, β=0.38

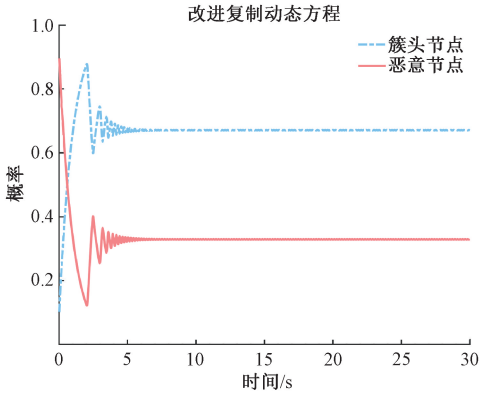
图 5　基于 Logit 动力学方程的演化博弈过程

Fig. 5　Evolutionary game process based on Logit dynamic equation

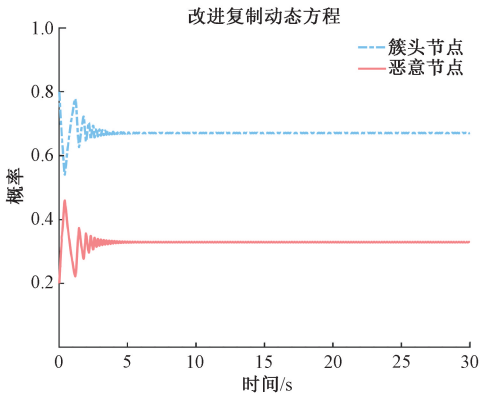
4)改进复制动态方程

图 6 表示博弈双方采用改进复制动态方程的演化博弈过程。从图 6(a)、(b)可以看出，博弈双方在初始概率极端时，相较于上述演化博弈方法，改进后的复制动态方程拥有更快的收敛速度。簇头节点的检测概率根据博弈

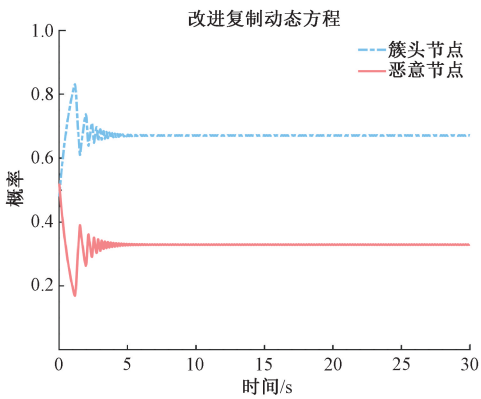
实际情况不断变换，恶意节点攻击也在利益最大化的前提下变换策略，避免被 IDS 发现。该法降低 WSNs 检测成本消耗的同时有效抑制恶意节点攻击；当双方节点初始概率相近时，如图 6(c)所示，达到平衡后的簇头节点检测概率始终大于恶意节点攻击概率，演化稳定后双方策略不再大幅度变化；图 6(d)表示在初始概率适中的情况下，此时恶意节点的攻击概率略高选择降低攻击概率避免被 IDS 检测到，簇头节点检测概率在快速提高后逐渐放缓，博弈达到平衡。



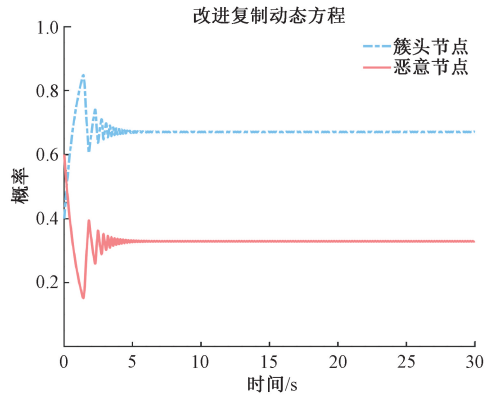
(a) 初始节点概率α=0.9，β=0.1
(a) Initial node probability α=0.9, β=0.1



(b) 初始节点α=0.2，β=0.8
(b) Initial node probability α=0.2, β=0.8



(c) 初始节点α=0.52，β=0.48
(c) Initial node probability α=0.52, β=0.48



(d) 初始节点α=0.6，β=0.4
(d) Initial node probability α=0.6, β=0.4

图 6　基于改进复制动态方程的演化博弈过程

Fig. 6　Evolutionary game process based on improved replication dynamic equation

实验结果表明，初始概率条件不同的情况下，簇头节点在上述 4 种复制动态方程中都能根据博弈过程中的概率变化调整自身策略，控制博弈达到演化均衡，但是传统方法下的攻防博弈达到平衡的时间较长，且演化均衡不够稳定。本文提出的改进后的复制动态方程在传统方法的基础上引入节点短期预测，在一定程度上优化了传统方法，簇头节点追求利益最大化的同时做到了对恶意节点策略的短期预测，提前预防了 WSNs 可能遭受的攻击，抑制恶意节点攻击概率的增大，避免网络大量检测能量的消耗。并且提出的改进复制动态方程使得簇头节点具有更快的响应能力，缩短了演化博弈达到均衡时间，从传统方法下的 20 s 缩短至 4 s。如表 4 所示。

表 4　演化仿真实验对比

Table 4　Comparison of evolutionary simulation experiments

方程	初始概率	达到演化均衡时间/s
传统复制动态方程	$\alpha=0.9,\beta=0.1$	21.40
	$\alpha=0.2,\beta=0.8$	22.00
	$\alpha=0.46,\beta=0.54$	20.32
BNN 动力学方程	$\alpha=0.9,\beta=0.1$	13.76
	$\alpha=0.2,\beta=0.8$	15.10
	$\alpha=0.49,\beta=0.51$	14.05
Logit 动力学方程	$\alpha=0.9,\beta=0.1$	7.44
	$\alpha=0.2,\beta=0.8$	6.12
	$\alpha=0.62,\beta=0.38$	6.36
本文所提动态方程	$\alpha=0.9,\beta=0.1$	5.05
	$\alpha=0.2,\beta=0.8$	3.94
	$\alpha=0.52,\beta=0.48$	4.03
	$\alpha=0.6,\beta=0.4$	4.57

将所提方法与其他基于博弈论的入侵检测方法对比,如图7所示。从图中可以看出,使用本文算法的入侵检测的准确率在65%左右,高于其他3种方法,说明本文方法存在一定优势;文献[10]采用静态博弈模型进行入侵检测,而WSNs的节点博弈是一个动态过程,因此该方法得到的检测率较低且不稳定,只有20%左右;文献[12]将贝叶斯理论引入博弈论模型,贝叶斯决策能对节点收集信息做量化判断,而非单一的绝对判断,检测率稳定在30%左右;文献[13]建立了一种动态的多阶段网络风险预测博弈模型,相比于前两者,它可以根据攻击策略动态调整,因此检测率较高,稳定在40~50%。

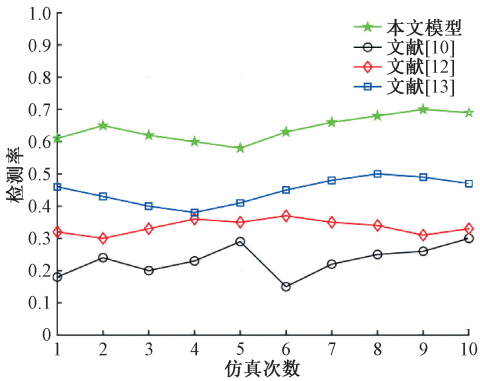


图7　本文模型与其他博弈论模型方法对比

Fig. 7　Comparison of this model with other game theory model methods

3　结　论

本文从WSNs内部节点攻防问题出发,提出了一种基于演化博弈的WSNs入侵检测算法,利用博弈论的方法建立了恶意节点和簇头节点之间的攻防博弈模型,模拟双方节点在博弈中的策略选择,通过改进传统复制动态方程,使得簇头节点具有主动调整策略的能力和较好的短期预测能力,预测博弈过程中恶意节点可能选择的攻击行为。仿真实验说明基于改进复制动态方程的入侵检测算法有效抑制了恶意节点的攻击,提高了博弈收敛速度,减少了WSNs检测能量的消耗。但是目前建立的攻防博弈模型与实际的WSNs攻防场景仍有差异存在,不能完全模拟构建,实际的网络对抗模型更为复杂,双方节点的策略更为多变,因此建立更具有普适性的改进复制动态方程,还原真实的网络攻防场景是下一步研究的方向与挑战。

参考文献

[1] 孙宇嘉, 于纪言, 王晓鸣. 自适应温度补偿无线传感器网络时间同步方法[J]. 仪器仪表学报, 2019, 40(1): 132-141.
SUN Y J, YU J Y, WANG X M. Adaptive temperature compensation time synchronization method for wireless sensor network [J]. Chinese Journal of Scientific Instrument, 2019, 40(1): 132-141.

[2] 朱庆豹, 施伟斌. 基于TDMA技术的无线传感器网络时间同步新方法[J]. 电子测量技术, 2019, 42(3): 135-139.
ZHU Q B, SHI W B. New method of time synchronization for wireless sensor network using TDMA technology [J]. Electronic Measurement Technology, 2019, 42(3): 135-139.

[3] 钱钢, 王黎明, 毕帅帅, 等. 水下无线传感器网络路由协议节能算法研究[J]. 国外电子测量技术, 2019, 38(11): 29-33.
QIAN G, WANG L M, BI SH SH, et al. Research on energy saving algorithm of underwater wireless sensor network routing protocol [J]. Foreign Electronic Measurement Technology, 2019, 38(11): 29-33.

[4] LOPEZ DELGADO M. On the effectiveness of intrusion detection strategies for wireless sensor networks: An evolutionary game approach [J]. Adhoc & Sensor Wireless Networks, 2017, 35(1-2): 25-40.

[5] 张志华. 无线传感器网络入侵检测关键技术研究[D]. 北京:北京邮电大学, 2018.
ZHANG ZH H. Research on key technologies of intrusion detection in wireless sensor networks [D]. Beijing: Beijing University of Posts and Telecommunications, 2018.

[6] DENNING D E. An intrusion-detection model[J]. IEEE Transactions on Software Engineering, 1987, 13(2): 222-232.

[7] LOANNIS K, DIMITRRIOU T, FREILING F C. Towards intrusion detection in wireless sensor networks [C]. Proceedings of the 13th European Wireless Conference. IEEE, 2007: 150-161.

[8] JIN X J, LIANG J Q, TONG W M, et al. Multi-agent trust-based intrusion detection scheme for wireless sensor networks [J]. Computers & Electrical Engineering, 2017, 59: 262-273.

[9] HU X, BAI R. Research on intrusion detection model of wireless sensor network[C]. International Conference on Computer Science and Service System (CSSS), Nanjing, 2011.

[10] LYE K W, WING J. Game strategies in network security[J]. International Journal of Information Security, 2005, 4(1-2): 71-86.

[11] HAN L, ZHOU M, JIA W, et al. Intrusion detection model of wireless sensor networks based on game theory and an autoregressive model[J]. Information Sciences,

2019, 476: 491-504.

[12] 陈行, 陶军. 无线网络中基于贝叶斯博弈模型的入侵检测算法研究[J]. 通信学报, 2010, 31(2): 107-112,119.
CHEN X, TAO J. Research on intrusion detection algorithm in wireless network based on Bayes game model [J]. Journal on Communications, 2010, 31(2): 107-112,119.

[13] 陈赵懿, 高秀峰, 王帅. 攻防博弈下的 Ad Hoc 网络风险预测[J]. 火力与指挥控制, 2020, 45(8): 16-21.
CHEN ZH Y, GAO X F, WANG SH. Risk prediction of Ad Hoc network based on game [J]. Fire Control & Command Control, 2020, 45(8): 16-21.

[14] 孙薇, 孔祥维, 何德全, 等. 基于演化博弈论的信息安全攻防问题研究[J]. 情报科学, 2008, 26(9): 1408-1412.
SUN W, KONG X W, HE D Q, et al. Research on attack and deference in information security based on evolutionary game [J]. Information Science, 2008, 26(9): 1408-1412.

[15] KOLIAS C, KOLIAS V, KAMBOURAKIS G. A distributed swarm intelligence-based approach for wireless intrusion detection [J]. International Journal of Information Security, 2016, 21(6): 1-16.

[16] 赵亮, 兰智高, 熊志利. 基于 LEACH 的无线传感器网络簇首选取改进算法[J]. 电子测量与仪器学报, 2019, 33(12): 86-93.
ZHAO L, LAN ZH G, XIONG ZH L. Modified cluster-head selection algorithm for WSNs based on LEACH[J]. Journal of Electronic Measurement and Instrumentation, 2019, 33(12): 86-93.

[17] WANG W, CHATTERJEE M, KWIAT K, et al. A game theoretic approach to detect and co-exist with malicious nodes in wireless networks [J]. Computer Networks, 2014, 71: 63-83.

[18] 巩俊辉, 胡晓辉, 杜永文. 基于演化博弈的最优防御策略选取研究[J]. 计算机工程与应用, 2021, 57(13): 116-123.
GONG J H, HU X H, DU Y W. Research on selection of optimal defense strategy based on evolutionary game [J]. Computer Engineering and Applications, 2021, 57(13): 116-123.

[19] 朱美玉, 尤晓琳. 李雅普诺夫稳定性理论应用研究[J]. 河南师范大学学报(自然科学版), 2009, 37(4): 148-149.
ZHU M Y, YOU X L. The research of applications in Lyapunov stability theory [J]. Journal of Henan Normal University (Natural Science), 2009, 37(4): 148-149.

[20] HOFBAUER J, OECHSSLER J, RIEDEL F. Brown-von neumann-nash dynamics: The continuous strategy case[J]. Games and Economic Behavior, 2009, 65(2): 406-429.

[21] HOMMES C H, OCHEA M I. Multiple equilibria and limit cycles in evolutionary games with logit dynamics [J]. Games and Economic Behavior, 2012, 74(1): 434-441.

[22] 张恩宁, 王刚, 马润年, 等. 采用双异质群体演化博弈的网络安全防御决策方法[J]. 西安交通大学学报, 2021, 55(9): 178-188.
ZHANG EN N, WANG G, MA R N, et al. Network security defense decision making method based on dual heterogeneous population evolutionary game model [J]. Journal of Xi'an Jiaotong University, 2021, 55(9): 178-188.

作者简介

王心怡, 2022 年于南京信息工程大学获得学士学位, 现为南京信息工程大学硕士研究生, 主要研究方向为信号处理。
E-mail: 1169089489@qq.com

Wang Xinyi received her B. Sc. degree from Nanjing University of Information Science & Technology in 2022. Now she is a M. Sc. candidate at Nanjing University of Information Science & Technology. Her main research interest includes signal processing.

行鸿彦(通信作者), 1983 年于太原理工大学获得学士学位, 1990 年于吉林大学获得硕士学位, 2003 年于西安交通大学获得博士学位, 现为南京信息工程大学教授、博士生导师, 主要研究方向为微弱信号检测与处理、生物医学信号采集与处理、智能化电子测量技术与仪器。
E-mail: xinghy@nuist.edu.cn

Xing Hongyan (Corresponding author), received his B. Sc. degree from Taiyuan University of Technology in 1983, M. Sc. degree from Jilin University in 1990, and Ph. D. degree from Xi'an Jiaotong University in 2003. Now he is a professor and supervisor for Ph. D. student in Nanjing University of Information Science & Technology. His main research interests include weak signal detection, bio-medical signal collection and processing, and design of intelligent electronic measurement technology and instrument.