DOI: 10.13382/j.jemi.B2407440

基于复杂网络演化博弈的无线传感器网络入侵检测方法*

王心怡[1] 行鸿彦[1] 史 怡[2] 侯天浩[1] 郑锦程[1]
(1 南京信息工程大学电子与信息工程学院 南京 210044;
2. 中国铁道科学研究院集团有限公司通信信号研究所 北京 100081)

摘 要:针对无线传感器网络资源受限和入侵检测系统策略优化问题,本文提出一种基于复杂网络演化博弈的无线传感器网络入侵检测方法。结合小世界模型理论,模拟网络节点之间的连接关系,在不改变节点原有关系的前提下增强网络连通性并降低传输能耗;构建关于簇头节点和恶意节点的无线传感器网络攻防博弈模型,通过收益矩阵计算节点收益,利用奖惩机制描述节点在博弈过程中选择不同策略的收益变化;引入经验加权吸引力学习算法改进传统博弈的策略更新规则并将该算法应用于入侵检测系统,使得簇头节点能够动态更新策略选择,得到不同条件下的入侵检测最优策略。实验结果表明,与传统方法相比,所提算法的簇头节点检测策略扩散深度可以达到 79%,该算法下簇头节点在保障自身检测收益的同时尽可能选择检测传感器网络中出现的攻击,保证网络检测率并减少网络各类资源的消耗。

关键词: 无线传感器网络;入侵检测;演化博弈;复杂网络;小世界模型理论
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

Intrusion detection method for wireless sensor networks based on complex network evolutionary game

Wang Xinyi[1] Xing Hongyan[1] Shi Yi[2] Hou Tianhao[1] Zheng Jincheng[1]
(1. School of Electronics and Information Engineering, Nanjing University of Information Science & Technology, Nanjing 210044, China; 2. Signal & Communication Research Institute, China Academy of Railway Sciences Corporation Limited, Beijing 100081, China)

Abstract: Aiming at the problem of limited wireless sensor network resources and intrusion detection system strategy optimization, this paper proposes a wireless sensor network intrusion detection method based on complex network evolutionary game. Combined with the small world model theory, the connection relationship between network nodes is simulated, and the network connectivity is enhanced and the transmission energy consumption is reduced without changing the original relationship of nodes. Then, the attack and defense game model of wireless sensor network about cluster head nodes and malicious nodes is constructed. The node income is calculated by the income matrix, and the reward and punishment mechanism are used to describe the income change of nodes choosing different strategies in the game process. At the same time, the empirical weighted attraction learning algorithm is introduced to improve the strategy update rules of the traditional game and the algorithm is applied to the intrusion detection system, so that the cluster head nodes can dynamically update the strategy selection and obtain the optimal strategy of intrusion detection under different conditions. The experimental results show that compared with the traditional method, the diffusion depth of the cluster head node detection strategy of the proposed algorithm can reach 79%. Under this algorithm, the cluster head nodes choose to detect the attacks in the sensor network as much as possible while ensuring its own detection income, so as to ensure the network detection rate and reduce the consumption of various resources in the network.

Keywords: wireless sensor network; intrusion detection; evolutionary game; complex network; small world model theory

收稿日期: 2024-04-16 Received Date: 2024-04-16
*基金项目:国家自然科学基金(62171228)、国家重点研发计划(2021YFE0105500)项目资助

0 引 言

无线传感器网络(wireless sensor networks, WSNs)是一种由大量低成本、低功耗传感器节点构成的自组织协作网络,因其网络部署简单、环境适应性强等特点,能够实现对周围环境的实时监测,在军事、医疗、交通等领域有着广泛的应用[1-2],同时这也对 WSNs 的安全防御性有了更高的要求。

入侵检测系统(intrusion detection system, IDS)是一种重要的网络安全防护技术,能够有效感知网络攻击[3],经过多年的研究已被熟练运用于 WSNs,但网络攻击手段日渐多样化和智能化,单一的入侵检测技术难以满足网络安全需求,需要结合新的网络防御技术弥补这一缺陷。

基于博弈论的网络入侵检测方法不需要额外数据建立模型,相比其他方法复杂度较低,引起了广泛的关注和应用。王增光等[4]提出了一种基于静态贝叶斯博弈的网络入侵检测防御方法,以防御效能为标准进行防御策略选取,但静态博弈模型无法模拟网络攻击的动态变化。Shen 等[5]建立了关于恶意攻击的微分博弈模型,IDS 可以动态选择策略以达到最小化网络检测成本,抑制恶意攻击行为。Zhang 等[6]将演化博弈与马尔可夫决策过程结合,构建了多阶段 Markov 攻防博弈模型,但是该方法采用传统演化博弈防御方法,难以准确预测攻击行为。Han 等[7]结合自回归理论,提出了一种基于博弈论和自回归模型的网络入侵检测方法,通过求解纳什均衡解来预测攻击行为,但是该方法在检测过程中会消耗大量网络能量。Liu 等[8]提出了一种基于 WoLF-PHC 学习算法的网络攻防随机博弈模型,使防御者在有限理性下面对不同攻击者能做出最优选择,提高了防御及时性。上述方法都在一定程度上加强了网络的防御性能,提高了网络入侵检测效率,但是没有针对 WSNs 节点的连接关系做进一步的研究。

复杂网络[9]用于研究大规模复杂系统,可以将网络中不同个体之间的联系描绘成图中点到点的链接[10],刻画博弈个体间的关系。WSNs 在结构上由大量节点组成,具有一定的复杂性;在行为上网络的拓扑结构会随着节点死亡或加入产生复杂变化,具有一定的动态特性。因此,借助复杂网络理论构建合适的 WSNs 演化博弈模型是近年来的研究热点。

Lin 等[11]根据复杂网络理论的网络拓扑优化解决 WSNs 的能源效率问题,利用网络节点的聚类特征,提出了基于小世界网络的 WSNs 节能模型。Bo 等[12]利用多信道技术和小世界网络特性,缩短了无线网络的平均路径长度,提高了网络性能。张静莲等[13]优化网络拓扑结构,提出了一种新的具有小世界特性的 WSNs 构造方法,通过 Sink 节点建立捷径降低平均路径长度,使网络在低冗余的条件下具有较好的防御性能。上述方法通过不同方法构建了 WSNs 模型,在一定程度上增强了传感器网络的防御能力,但随着网络攻击技术的不断更新升级已无法满足现阶段的网络安全需求。

基于复杂网络小世界模型理论,建立基于簇头节点与恶意节点的 WSNs 攻防演化博弈模型,通过奖惩机制描述簇头节点博弈收益的动态变化,提出一种注重经验加权和适应能力的学习算法(experience weighted attraction, EWA),使得簇头节点具有动态更新网络博弈策略选择的能力,得到不同条件下的博弈最优策略,降低节点能量消耗的同时延长网络生存周期。

1 无线传感器网络攻防模型

1.1 网络分簇

为减少节点能耗、保障数据稳定传输,根据网络路由协议[14]将 WSNs 划分为多个相互连接的簇。其中,每个簇由一个簇头节点和若干普通节点组成,普通节点负责处理监测环境内收集到的各类信息;簇头节点定期随机产生,会将这些信息整合汇总发送到基站。考虑到 WSNs 本身存在多种制约性,并且运行 IDS 会增加节点能耗,存在簇头节点能量耗尽,普通节点升级成为簇头节点的可能。本章使用 IDS 混合部署模式[15]均衡能量消耗和检测效率,即在网络中的每个传感器节点都安装 IDS,但是只开启位于簇头节点上的 IDS 用于识别网络攻击行为。

1.2 攻防模型

WSNs 的攻击类型按照来源可以分为外部攻击和内部攻击,外部攻击指的是攻击者使用 WSNs 外部设备进行攻击,如物理捕获节点破坏网络结构等[16];内部攻击指的是攻击者利用 WSNs 内部隐藏的恶意节点进行攻击,如控制内部恶意节点拒绝或选择性转发有效信息,甚至发送虚假信息。建立的 WSNs 攻防模型如图 1 所示。

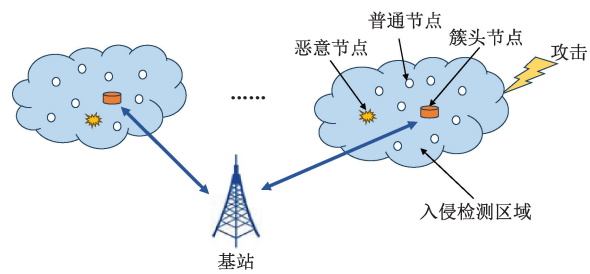


图 1 无线传感器网络攻防模型

Fig. 1 Attack-defense model for WSNs

2　基于复杂网络的无线传感器网络演化博弈模型

复杂网络和演化博弈结合形成了复杂网络上的演化博弈这一新型交叉领域[17]，为分析和预测 WSNs 环境下的节点决策行为提供了一种新的研究框架，设定研究的基本框架如图 2 所示。首先，建立关于 WSNs 的演化博弈模型，提出博弈基本假设，利用奖惩机制计算簇头节点收益；然后，构建 NW（newman-watts，NW）小世界网络模型模拟 WSNs 中各节点之间的博弈关系；最后，改进传统博弈策略更新规则，引入 EWA 加权学习算法更新节点策略。

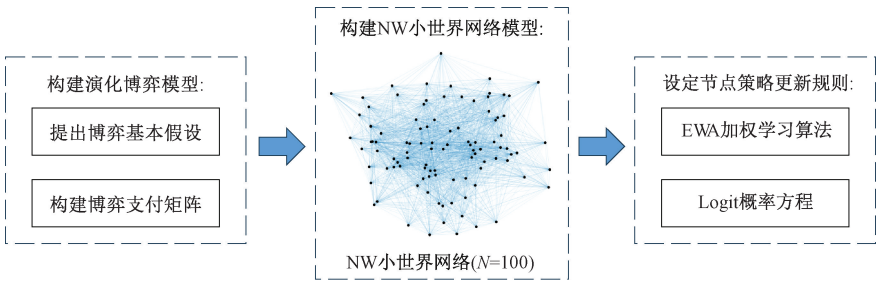


图 2　模型框架

Fig. 2　Model framework

2.1　演化博弈模型

不同于经典博弈论[18-19]，演化博弈不要求每次博弈的策略选择都是最优选择，而是考虑一个较长的时间周期内，个体对自身策略进行学习和优化。基于簇头节点和恶意节点的网络攻防模型，给出以下演化博弈基本假设：

假设 1：如果簇头节点选择检测网络是否受到攻击，会产生启动 IDS 的检测成本 C。簇头节点安装 IDS 系统需要耗费一定的时间、成本，并且启动 IDS 进行攻击检测会消耗大量的网络能量。

假设 2：如果簇头节点检测成功，会获得检测奖励收益 E，此时，被检测到攻击的恶意节点会得到攻击损失 P。由于簇头节点开始检测就会产生检测成本，为提高簇头节点选择检测攻击的积极性，假定对成功检测到攻击的簇头节点给予一定的奖励，并可根据检测结果调整奖励价值。同时，被检测到攻击的恶意节点会得到一定的损失。

假设 3：如果恶意节点发动攻击并且簇头节点没有检测到，那么簇头节点要承担网络受到的攻击损失 W，此时恶意节点会获得攻击收益 A。在 WSNs 中，簇头节点为了自身收益的最大化，会选择合理的博弈策略避免网络损失，适当的惩罚措施可以促进簇头节点发起检测攻击行为。

假设 4：如果某一簇头节点在某次博弈中没有启动 IDS，则会从其他簇头节点获得交互检测信息收益 D。WSNs 是一种自组织、开放的系统，节点通过无线通信的方式实现彼此间的信息交互，因此，簇头节点能够共享检测信息。

根据上述假设，构建簇头节点与恶意节点的演化博弈支付矩阵，如表 1 所示。

表 1　WSNs 演化博弈支付矩阵

Table 1　WSNs evolutionary game payoff matrix

簇头节点	恶意节点	
	攻击	不攻击
检测	$E-C, A-P$	$E-C, -P$
不检测	$D-W, A$	0,0

2.2　NW 小世界网络

在规则网络中，每个节点都与固定数量的邻居节点相连，具有高度的规律性和稳定性，但其平均路径长度较长，不利于信息的快速传输。完全随机的网络虽然节点的平均路径长度可能会缩短，但节点聚集相对分散，难以形成联系紧密的局部群体。NW 小世界网络[20]介于这两种网络结构之间，可以通过一条很短的链路将分散的、关系不紧密的个体联系在一起。并且 NW 小世界网络可以在不改变网络节点原有关系的前提下，通过随机加边的方法增强网络的连通性。

在 WSNs 中，节点之间的数据传输是能量消耗的主要来源，降低能耗可以通过降低节点的平均路径长度来实现。小世界网络具有聚集系数较大和平均路径长度较短的特点，簇头节点具有较强的数据处理能力可以作为聚集中心节点连接部分普通节点，形成聚簇群组，同时节点之间的路径长度得到缩短，有利于提高 WSNs 性能。因此，利用 NW 小世界网络模型可以更加贴切模拟 WSNs 节点入侵检测行为决策的演化博弈关系。

假定每个传感器节点都与相邻的 x 个邻居节点存在信息交互关系，根据 NW 小世界网络特性，每次博弈之后

节点都会以随机加边概率 ω 与任一非邻居节点重新建立新的网络连接关系,概率 ω 越高,节点间的连接关系越多,更加符合现实的 WSNs 节点连接结构。

基于此,构建 WSNs 入侵检测扩散网络 $\boldsymbol{G}=(\boldsymbol{V},\boldsymbol{R})$, $\boldsymbol{V}=\{v_1,v_2,\cdots,v_N\}$ 表示所有节点的集合, $\boldsymbol{R}$ 表示所有节点之间边的集合,代表节点间的连接关系,网络表达式为:

$$\boldsymbol{R}=\begin{bmatrix} r_{11} & \cdots & r_{1N} \\ \vdots & \ddots & \vdots \\ r_{N1} & \cdots & r_{NN} \end{bmatrix} \tag{1}$$

其中, $r_{ij}=1$ 表示节点 v_i 与 v_j 之间存在连接关系, $r_{ij}=0$ 则表示两者不存在关系,任何节点都不能与自身相连[21]。

2.3 基于经验加权吸引力学习算法的博弈模型

传感器节点内部嵌有微型操作系统,将经验加权吸引力学习算法写入系统内可以使其具有一定的智能性,簇头节点作为一种智能体能够不断检测攻击、执行收益最大化策略。

1) EWA 学习算法

传统博弈理论采用复制动态方程的思想进行策略更新,在此基础上,提出一种注重经验加权和适应能力的吸引力(experience weighted attraction, EWA)学习算法作为簇头节点的策略更新规则,定义一个衡量策略吸引力的中间结构用于更新簇头节点的策略选择。

首先,定义第 t 次博弈簇头节点 i 选择策略 k 的收益 $U_i[s_i^k,s_{-i}(t)]$ 为:

$$U_i[s_i^k,s_{-i}(t)]=\alpha_i^k+u[e_i^k(t)] \tag{2}$$

其中, $\boldsymbol{S}=\{s_1,\cdots,s_n\}$ 表示博弈参与者的策略空间, s_{-i} 表示除了簇头节点 i 外所有参与节点的策略组合; α_i^k 表示簇头节点 i 与其相邻节点博弈获得的历史累积收益; $u[e_i^k(t)]$ 表示网络中同样选择策略 k 的节点带来的信息交互收益。

根据复杂网络理论,网络中的博弈主体具有适应预期行为的能力,即 WSNs 演化博弈具有显著的网络效应,网络中的信息交互收益表示为:

$$u[e_i^k(t)]=\sum_{k=1}^{m}\delta_k e_i^k(t)^{\frac{1}{\beta}},\ m\geqslant 1,\beta>1 \tag{3}$$

其中, m 表示簇头节点 i 可以选择的策略个数; δ_k 表示网络效应参数,指策略 k 的价值取决于选择该策略的其他节点的数量; β 表示网络效应指数,需要满足大于 1 以保证 $u[e_i^k(t)]$ 的二阶导数小于零; $e_i^k(t)$ 表示第 t 次博弈时,簇头节点 i 对同样选择策略 k 的节点数量的预测:

$$e_i^k(t)=(1-\varepsilon)\cdot e_i^k(t-1)+\varepsilon\cdot q_i^k(t-1) \tag{4}$$

其中, ε 表示预测因子,取值越小说明上一次博弈选择策略 k 的节点预测数量在本次博弈中占比越大; $q_i^k(t-1)$, $t>1$ 表示上一次博弈中选择策略 k 的节点的实际数量。

EWA 学习算法中,每个博弈策略根据吸引力指数所决定的概率大小被随机选择,吸引力指数越大的策略被选择的概率更高,其更新规则是将 $A_i^k(t)$ 设置为 t 时刻与上一时刻吸引力 $A_i^k(t-1)$ 的加权平均收益,则第 t 次博弈簇头节点 i 选择策略 k 的吸引力指数 A 表示为:

$$A_i^k(t)=\frac{\varphi\cdot N(t-1)\cdot A_i^k(t-1)+U_i[s_i^k,s_{-i}(t)]}{\varphi\cdot N(t-1)+1} \tag{5}$$

其中, φ 表示吸引力指数的折扣因子,取值越大说明簇头节点对该策略的预期越高,选择该策略的可能性也就越大; $N(t)$ 表示经验权重,通常用来衡量过去经验在本次博弈过程中的影响, $N(0)$ 和 $A(0)$ 取值范围是 [1,2] 和 [1,3] 中的随机数。

2) Logit 概率方程

传统博弈利用收益矩阵建立簇头节点的复制动态方程对网络攻防状态进行分析,在给定初始选择概率的情况下,EWA 学习算法使得簇头节点可以通过历史博弈信息计算出选择任一防御策略所带来的吸引力,在入侵检测时根据回报经验实时更新策略,并通过 Logit 方程决定在 $t+1$ 时刻的最优策略选择。

利用 Logit 概率方程[22]将吸引力指数 A_i^k 转化为策略选择概率,即 $t+1$ 时刻簇头节点 i 选择策略 k 的概率 P 为:

$$P_i^k(t+1)=\frac{\exp[\sigma\cdot A_i^k(t)]}{\sum_{k=1}^{m}\exp[\sigma\cdot A_i^k(t)]} \tag{6}$$

其中, σ 表示吸引力指数 A_i^k 的敏感系数,用于判断博弈决策者策略选择是否理性,取值越高说明决策者的理性程度越高,能够在充分考虑实际情况下选择合适的 WSNs 入侵检测防御策略。

3 演化博弈仿真与分析

构建基于复杂网络的 WSNs 演化博弈入侵检测过程如下:

步骤 1)随机生成具有 100 个传感器节点的网络模型,每个节点的初始化能量设为 2.5 J;

步骤 2)利用分簇协议对网络结构进行划分,假定节点被随机选为簇头节点的概率为 0.1,即网络中包含 10 个簇头节点和 90 个普通节点,其中存在若干恶意节点隐藏在普通节点中;

步骤 3)根据小世界网络理论,进一步完善 WSNs 模型,每个节点都与相邻 $x=5$ 个节点建立连接;

步骤 4)建立簇头节点与恶意节点的 WSNs 博弈模型,利用奖惩机制计算节点博弈收益;

步骤 5) $t = 1$ 开始博弈,簇头节点开启 IDS;

步骤 6)簇头节点以概率 ω 与任意非相邻的节点建立新的连接关系,并依据 EWA 学习算法调整下一时刻博弈策略;

步骤 7)簇头节点断开上次连接,以概率 ω 与非相邻节点建立新链接,再次利用 EWA 学习算法调整策略达到演化稳定;

步骤 8)对上述步骤进行多次重复模拟仿真,减少随机过程带来的误差,直到 $t = 10$。

3.1　演化博弈仿真参数初始值设置

仿真实验主要考虑演化博弈过程中,不同奖惩机制及参数对于簇头节点检测策略扩散深度的影响,扩散程度越深说明选择检测的概率越大,网络中的簇头节点在面对攻击时更倾向选择检测策略,网络安全防御得到保障。结合相关文献[23],设置初始参数如表 2 所示。

表 2　演化博弈参数设置

Table 2　Parameter setting of evolutionary game

符号表示	符号含义	假设初始值
N	无线传感器网络节点个数	100
p	节点随机选为簇头节点的概率	0.1
x	相邻节点个数	5
ω	随机加边概率	0.3
P	簇头节点初始检测概率	0.3
β	网络效应指数	2
δ_k	网络效应参数	6
ε	预测因子	0.5
φ	吸引力指数的折扣因子	0.5
σ	吸引力指数的敏感系数	5

3.2　奖惩机制对入侵检测的影响

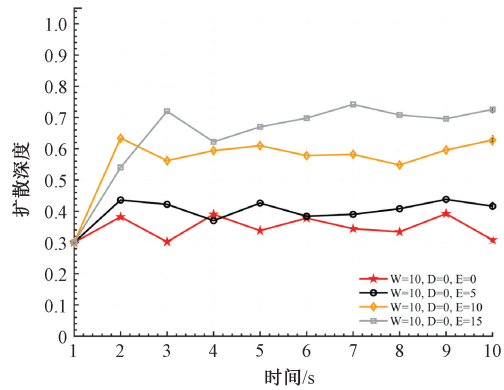
在 WSNs 入侵检测博弈中,节点更倾向于选择收益最大化策略,而节点策略收益大小受奖惩机制的影响,确定合适的奖惩取值激励簇头节点选择检测策略是 WSNs 入侵检测算法的研究重点。

根据 WSNs 通常情况下的经验值及各参数意义,假设簇头节点使用 IDS 的检测成本 $C = 5$、恶意节点攻击成功的收益 $A = 10$、攻击被检测到的损失 $P = 5$,通过改变 E、W 取值,观察奖惩机制如何影响簇头节点决策。

1)簇头节点检测到攻击的收益 E

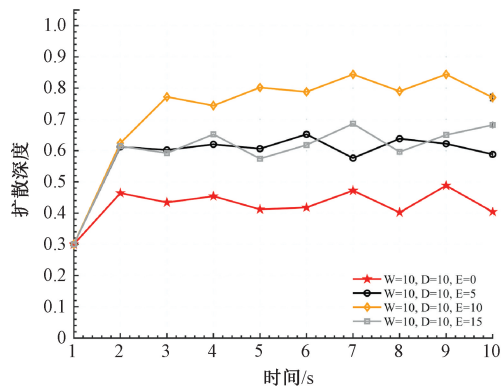
图 3 表示 $P = 0.3$、$W = 10$、$D = 0$ 时,簇头节点在不同奖励措施下的检测策略扩散深度。从图 3(a)中可以看出,随着奖励 E 的不断增大,簇头节点在入侵检测博弈过程中选择检测攻击的概率也在逐渐变大;当 $E = 0$ 或 5 时,节点策略的扩散深度在 0.3~0.4 变化,说明没有检测奖励或者奖励过小对节点策略选择影响不大;当 $E = 10$ 时,相较之前两种情形,检测策略的扩散深度有了大幅提高,快速达到 0.62 后稳定波动;当 $E = 15$ 时,簇头节点选择检测的概率最高,达到了 0.73。

图 3(b)在图 3(a)的基础上,将 D 的取值增加到 10,通过改变奖励 E,观察不同 E 值下的检测策略扩散深度。如图 3(b)所示,簇头节点获得交互检测信息收益 D 后,策略扩散深度整体相比图 3(a)有了一定的提升,涨幅在 10%左右;$E = 0$ 依旧是策略扩散最低的,经过博弈后略高于初始检测概率,在 0.4 左右;当 $E = 5$ 和 15 时,其策略扩散深度变化趋势相近,在 0.6~0.7 波动;$E = 10$ 时,簇头节点选择检测策略的概率最大,达到平衡后趋近于 0.8,说明当奖励 E 强度超过簇头节点自身承受极限后,节点会选择降低策略扩散深度保证网络 IDS 正常运行。



(a) 簇头节点没有获得节点交互检测信息收益D

(a) The cluster head node does not obtain the node interaction detection information benefit D



(b) 簇头节点获得交互检测信息收益，假设D=10

(b) The cluster head node obtains the benefit of interactive detect information, assuming D=10

图 3　不同奖励措施下的簇头节点检测策略扩散趋势

Fig. 3　The diffusion trend of cluster head node detection strategy under different reward measures

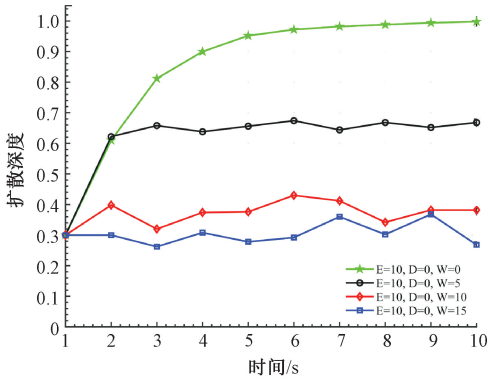
图 3 表明,一般情况下检测到攻击的奖励 E 越大,簇头节点选择检测策略的概率越高,但要根据实际选择合适的奖励措施,当检测奖励增加到一定值时策略概率选择反而减小。综上,选择 $E = 10$ 作为奖励措施,该措施下的检测策略扩散深度能快速升至 0.8,进一步鼓励簇头

节点启用 IDS 对网络中的攻击行为进行检测。

2)簇头节点没有检测到攻击的损失 W

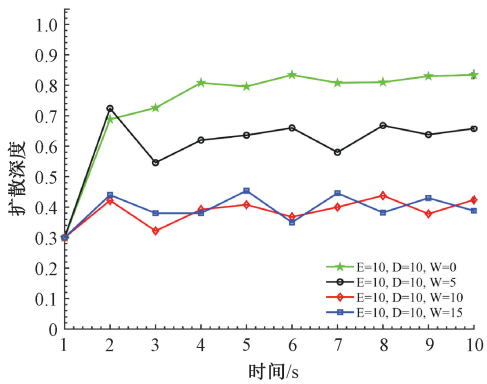
图 4 展示了当 $P=0.3$、$E=10$、$D=0$ 时,不同惩罚力度对于簇头节点检测策略选择的影响。由图 4(a)可知,损失 W 越小,入侵检测策略扩散越深;当 $W=0$ 时,簇头节点开启 IDS 实行检测策略的扩散深度接近 1,并且随着惩罚力度加大,簇头节点会逐渐降低检测策略的选择以减少检测失败带来的网络能量损失,当 $W=15$ 时,簇头节点检测概率甚至低于初始概率 0.3,下降至 2.8。

与图 4(a)不同,图 4(b)在其他条件不变的情况下,将 D 由 0 增加到 10。从图 4(b)可以看出,加入交互信息收益 D 后,不同惩罚力度下的节点检测概率都有所提高,均大于初始检测概率 0.3;$W=0$ 时的扩散深度虽然相较于图 4(a)下降到 0.8,但是幅度变化更加符合实际场景。



(a) 簇头节点没有获得节点交互检测信息收益D

(a) The cluster head node does not obtain the node interaction detection information benefit D



(b) 簇头节点获得交互检测信息收益，假设D=10

(b) The cluster head node obtains the benefit of interactive detection information, assuming D=10

图 4 不同惩罚措施下的簇头节点检测策略扩散趋势

Fig. 4 The diffusion trend of cluster head node detection strategy under different punishment measures

总体来看,当 $W=0$ 时,簇头节点选择检测策略的概率最大,但实际 WSNs 攻防场景中,必然存在检测失败后网络受到攻击造成一定损失;$W=5$ 时,无论有无节点间的信息共享,检测策略的扩散深度都较高且保持在 0.6~0.7 之间;当 $W=10$ 或 15 时,图 4 中的策略扩散深度趋势相近,说明继续加大惩罚对于簇头节点策略选择影响不大且检测策略扩散深度较低。因此,取 $W=5$ 作为惩罚,既能激励簇头节点实行攻击检测,又能减少能量损耗,维护网络安全。

3.3 演化博弈模型的参数敏感性分析

通过奖惩机制对簇头节点策略选择的影响分析,确定 $E=10$、$W=5$、$D=10$ 为奖惩机制取值,促使簇头节点在博弈时尽可能选择检测策略。

在假定的模型场景下,通过改变博弈参数的取值,观察 WSNs 簇头节点检测策略演化曲线的变化情况,比较簇头节点检测策略扩散深度对不同参数的敏感程度。

1)改变初始检测概率

图 5 表示不同初始概率 P 条件下的簇头节点检测策略扩散深度。当 P 相同时,簇头节点从其他相邻节点获得的交互信息收益 D 越多,策略扩散越深;当 P 不同时,交互信息收益对节点策略选择影响不大,初始选择概率越高,其对应的策略扩散效果越好,簇头节点启用 IDS 检测攻击的可能性就越大。

当 $P=0.3$ 时,簇头节点会快速提高 IDS 检测概率抑制恶意节点攻击,此时网络处于激烈的攻防博弈状态,恶意节点攻击被抑制后,簇头节点也会相应减少 IDS 的开启,曲线呈现波动状态,经过一段时间博弈达到平衡,簇头节点选择检测策略的扩散深度在 0.5~0.6 之间;当 P 较大为 0.6 时,节点进一步提高了检测概率,但由于策略初始扩散深度较高,因此策略扩散幅度较为平缓。

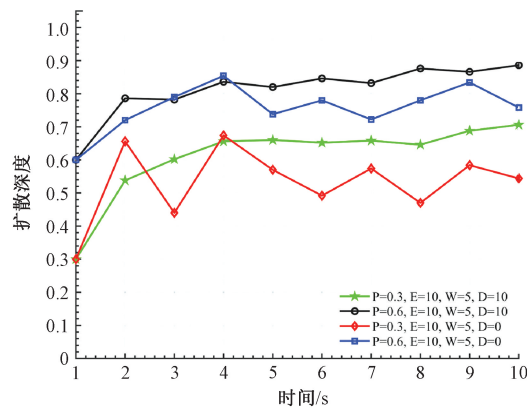


图 5 不同初始检测概率的敏感性分析

Fig. 5 Sensitivity analysis of the different initial detection probabilities

2)改变传感器网络节点数量

如图 6 所示,表示簇头节点检测策略在不同网络节点数量情况下的扩散深度,分别对 N 取 100、200、300、400、500 进行仿真。簇头节点检测策略扩散深度整体波动趋势相似,经历一系列攻防对抗后策略扩散趋于平缓。

网络节点数量在 100、300 和 400 时，达到烟花稳定均衡后节点扩散深度在 0.65 左右；N = 200 时节点选择检测策略的概率反而最低；网络节点规模达到 500 时，簇头节点检测概率提高至 0.82，簇头节点检测到攻击后加大检测规模抑制攻击行为。由图 6 可知，不同的 WSNs 节点数量会对博弈策略的选择产生一定的影响，在构建模型时要考虑这一因素，选择合适的节点数量，以达到博弈收益最大化。

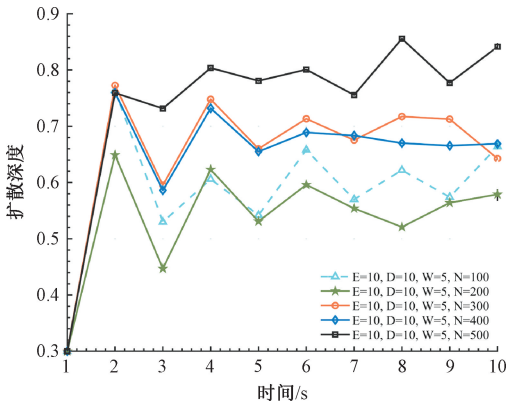


图 6　不同节点数量的敏感性分析

Fig. 6　Sensitivity analysis of the different number of nodes

3) 改变 EWA 学习算法关键参数

为进一步分析簇头节点策略选择是否受其他参数影响，改变 EWA 学习算法中的部分关键参数，如表 3 所示。情形 1 使用初始仿真数值作为对照组，每种情形基于情形 1 改变某一参数的初始值。

表 3　EWA 学习算法的参数设置

Table 3　Parameter settings for the EWA learning algorithm

仿真实验	β	δ_k	ε	φ
情形 1：对照组	2	6	0.5	0.5
情形 2：增大网络效应指数	**3**	6	0.5	0.5
情形 3：减小网络效应参数	2	**2**	0.5	0.5
情形 4：减小收益预测因子	2	6	**0.1**	0.5
情形 5：增大吸引力指数折扣因子	2	6	0.5	**0.9**

如图 7 所示，情形 1~5 的节点策略扩散深度变化趋势类似。情形 1 作为对照组，其结果符合上述结论，检测策略最终扩散至 0.71；情形 2 增大网络效应指数后，检测策略扩散深度呈现先大幅度增大至 0.82，经过波动变化，最终减小至 0.58 的变化过程，说明增大网络效应指数会降低网络启动 IDS 的概率；情形 3~5，分别通过减小网络效应参数、减小收益预测因子和增大吸引力指数折扣因子来判断策略选择的影响因素，情形 3~5 均在情形 1 的附近波动，说明改变这 3 种参数对节点策略选择的影响不明显。

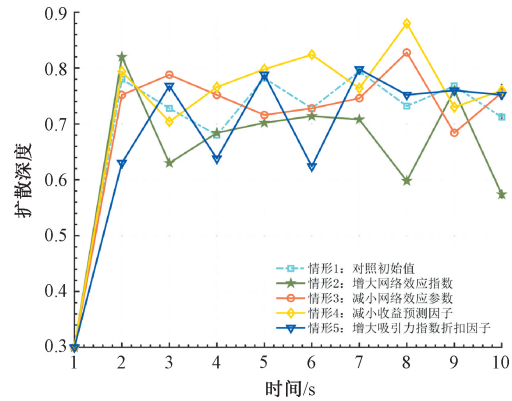


图 7　EWA 学习算法关键参数的敏感性分析

Fig. 7　Sensitivity analysis of the key parameters in EWA learning algorithm

3.4　不同策略更新规则对比

博弈参与者学习和策略调整方式是复杂网络演化博弈的核心，采用 EWA 加权学习算法改进传统的 Logit 策略更新规则，与费米更新规则[24]、马尔可夫更新规则[25]进行对比。根据上述对 WSNs 入侵检测过程中奖惩机制和参数敏感性分析，取初始检测概率为 0.1，仿真结果如图 8 所示。

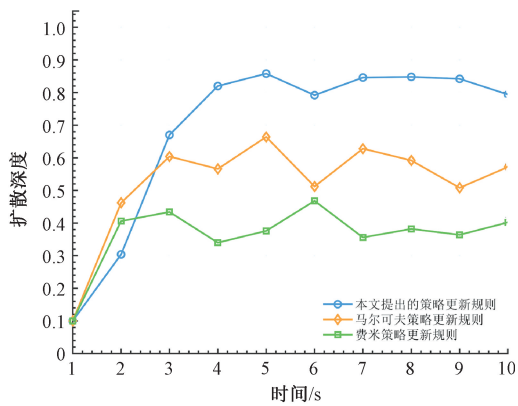


图 8　不同策略更新规则对比

Fig. 8　Comparison of the different strategy update rules

3 种方法经过一段时间均能达到演化稳定，费米策略更新规则以每一次的博弈收益为重点，忽略过去的历史博弈收益，策略的扩散深度在 40%；马尔可夫策略更新规则本质是随机学习，博弈参与者采用混合策略随机学习的方式更新目标函数，相比费米规则扩散深度提高了 18%；而提出的改进后的策略更新算法的策略扩散深度最高在 79%左右，高于其他两种算法，说明 EWA 学习算法有利于帮助簇头节点尽可能选择检测策略，增强网络防御。

3.5 节点平均剩余能量

图 9 展示了随着博弈进程未启动 IDS 防御、只开启位于簇头节点的 IDS、全面启动 IDS 3 种情况下的网络节点平均剩余能量。网络未开启 IDS 防御时,节点仅需要维持 WSNs 正常运行,没有额外的检测能量消耗,剩余能量最多;若是开启所有节点的 IDS,节点能量会被大量消耗,加重网络运行负担;当选择只开启位于簇头节点的 IDS 时,不仅保证了 WSNs 的防御能力,还减少了网络资源开销。

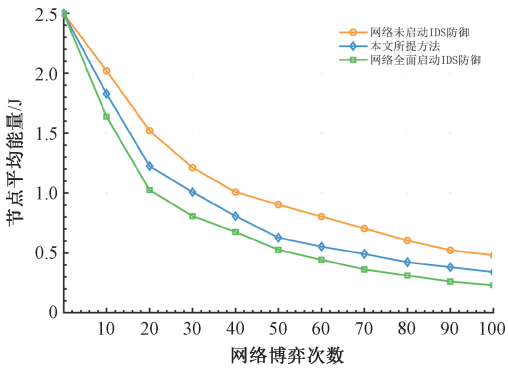


图 9 节点平均剩余能量

Fig. 9 Average residual energy of nodes

4 结 论

在已有的基于博弈论的入侵检测算法基础上,通过引入复杂网络中的 NW 小世界模型理论,进一步描述 WSNs 节点的连接关系和行为决策,构建了基于复杂网络演化博弈的 WSNs 入侵检测模型,缩短了节点之间的平均路径长度,减少 WSNs 在传输过程的能量损耗;并且改进传统博弈的策略更新规则,提出了一种基于 EWA 加权学习算法的网络入侵检测方法,通过定义一个衡量策略吸引力的中间结构判断簇头节点下一步的策略更新,通过改变节点在不同策略的奖惩收益寻找合适的奖惩机制使得簇头节点选择检测攻击时的策略吸引力最大,保证自身收益的同时做到了对网络攻击的检测。仿真实验表明,选取合适的博弈参数能够激励簇头节点开启 IDS 检测攻击,基于复杂网络演化博弈的入侵检测方法使得簇头节点及时调整检测策略来实现有效的入侵防御,保证了 IDS 检测效率,检测策略的扩散深度最高可达 79%。但是目前建立的模型与实际 WSNs 场景存在一定差异,没有考虑传感器网络外部环境因素干扰带来的影响,在未来的研究中,会考虑引入节点的生成与消亡机制,采集真实网络数据进行实验,更加准确地描绘网络攻防情况。

参考文献

[1] 黄艺, 赵春华, 汤宝平,等. 冗余策略下的机械振动 WSN 高效可靠传输方法[J]. 仪器仪表学报, 2022, 43(3): 146-152.
HUANG Y, ZHAO CH H, TANG B P, et al. Efficient and reliable transmission method for mechanical vibration of WSN based on redundancy strategy [J]. Chinese Journal of Scientific Instrument, 2022, 43(3): 146-152.

[2] 高海燕, 高晋阳. 一种实现 WSNs 中 QoS 保证和高能效的路由协议[J]. 国外电子测量技术, 2022, 41(3): 26-32.
GAO H Y, GAO J Y. Routing protocol to achieve QoS guarantee and high energy efficiency in WSNs [J]. Foreign Electronic Measurement Technology, 2022, 41(3): 26-32.

[3] 梁欣怡, 行鸿彦, 侯天浩. 基于自监督特征增强的 CNN-BiLSTM 网络入侵检测方法[J]. 电子测量与仪器学报, 2022, 36(10): 65-73.
LIANG X Y, XING H Y, HOU T H. CNN-BiLSTM network intrusion detection method based on self-supervised feature enhancement [J]. Journal of Electronic Measurement and Instrumentation, 2022, 36(10): 65-73.

[4] 王增光, 卢昱, 李玺,等. 静态贝叶斯博弈最优防御策略选取方法[J]. 西安电子科技大学学报, 2019, 46(5): 55-61.
WANG Z G, LU Y, LI X, et al. Optimal defense strategy selection based on the static Bayesian game[J]. Journal of Xidian University, 2019, 46(5): 55-61.

[5] SHEN S G, LI H J, HAN R S, et al. Differential game-based strategies for preventing malware propagation in wireless sensor networks[J]. IEEE Trans on Information Forensics and Security, 2014, 9(11): 1962-1973.

[6] ZHANG H, HUANG J. Network defense strategy selection method based on Markov evolutionary Game [J]. Acta Electronica Sinica, 2018, 46(6): 1503-1509.

[7] HAN L S, ZHOU M, JIA W J, et al. Intrusion detection model of wireless sensor networks based on game theory and an autoregressive model[J]. Information Sciences, 2019, 476(1): 491-504.

[8] LIU J, ZHANG Y C. Optimal decision-making approach for cyber security defense using game theory and intelligent learning [J]. Security and Communication Networks, 2019, 2019(2): 1-16.

[9] CHEN J W, LIU B, MUBARAK U. Evolutionary dynamics games based on edge diversity in complex networks[C]. International Conference on Networking and Network Applications, 2020.

[10] JIA C, ZHANG R X, WANG D. Evolutionary game of

cooperative behavior among social capitals in PPP projects: A complex network perspective[J]. Ain Shams Engineering Journal, 2023, 14(7):102006.

[11] LIN X, WU F H, YANG D C, et al. Energy efficient wireless sensor network modelling based on complex networks[J]. Journal of Sensors, 2016(1): 1-8.

[12] BO L, MUQING W, JINGRONG W, et al. Small worlds in multi-channel wireless networks: An analytical approach [C]. IEEE International Conference on Communications, 2013.

[13] 张静莲, 刘三阳, 张朝辉. 具有小世界现象的无线传感器网络构造方法[J]. 信号处理, 2017, 33(3): 417-421.
ZHANG J L, LIU S Y, ZHANG CH H. Approach to construct wireless networks with small world phenomenon[J]. Journal of Signal Processing, 2017, 33(3): 417-421.

[14] 冯程鹏, 何汇成, 邹杰, 等. 簇首优选改进算法设计及其网络能耗影响研究[J]. 电子测量技术, 2022, 45(18): 173-178.
FENG CH P, HE H CH, ZOU J, et al. Research on improved algorithm design of cluster heads optimization and influence of network's energy consumption [J]. Electronic Measurement Technology, 2022, 45(18): 173-178.

[15] 夏金棕. 无线传感器网络的入侵检测及防御响应研究[D]. 兰州: 兰州交通大学, 2021.
XIA J Z. Research on intrusion detection and defense response of wireless sensor networks [D]. Lanzhou: Lanzhou Jiaotong University, 2021.

[16] 陆浩维, 姜文淇, 李中伟, 等. 无线传感器网络攻击技术分析[J]. 自动化与仪表, 2022, 37(10): 19-23.
LU H W, JIANG W Q, LI ZH W, et al. Analysis of wireless sensor networks attack technique [J]. Automation & Instrumentation, 2022, 37(10): 19-23.

[17] 谭少林, 吕金虎. 复杂网络上的演化博弈动力学——一个计算视角的综述[J]. 复杂系统与复杂性科学, 2017, 14(4): 1-13.
TAN SH L, LYU J H. A computational survey of evolutionary game dynamics on complex networks [J]. Complex Systems and Complexity Science, 2017, 14(4): 1-13.

[18] MABROUK A, NAJA A. Intrusion detection game for ubiquitous security in vehicular networks: A signaling game based approach[J]. Computer Networks, 2023, 255(2): 1-7.

[19] FANG Y, WEI W, LIU F, et al. Improving solar power usage with electric vehicles: Analyzing a public-private partnership cooperation scheme based on evolutionary game theory[J]. Journal of Cleaner Production, 2019, 233(1): 1284-1297.

[20] SAIF M A, SHUKRI M A. SIR model on one dimensional small world networks [J]. Physica A: Statistical Mechanics and Its Applications, 2024, 633(1): 1-14.

[21] 魏夕凯, 马本. 农村生活垃圾分类治理的奖惩激励机制——基于复杂网络演化博弈模型[J]. 中国环境科学, 2022, 42(8): 3822-3831.
WEI X K, MA B. Reward and punishment incentive mechanism of domestic waste classification in rural China: based on complex network evolutionary game model[J]. China Environmental Science, 2022, 42(8): 3822-3831.

[22] HWANG S H, BELLET L R. Positive feedback in coordination games: stochastic evolutionary dynamics and the Logit choice rule [J]. Games and Economic Behavior, 2021, 126(3): 355-373.

[23] XIAN Y B, MEI L. Adaptive expectation, complex network and the dynamic of standard diffusion——research based on computational economics[J]. Journal of Management Sciences, 2007, 20(4): 62-72.

[24] LIU J Z, MENG H R, WANG W, et al. Evolution of cooperation on independent networks: The influence of asymmetric information sharing updating mechanism[J]. Applied Mathematics and Computation, 2019, 340(1): 234-241.

[25] HAO X C, WANG L Y, YAO N, et al. Topology control game algorithm based on Markov lifetime prediction model for wireless sensor network [J]. Ad Hoc Networks, 2018, 78(1): 13-23.

作者简介

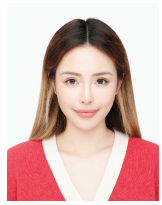
王心怡, 2022 年于南京信息工程大学获得学士学位, 现为南京信息工程大学硕士研究生, 主要研究方向为信号处理。
E-mail: 1169089489@qq.com

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.



史怡，2019 年于南加利福尼亚大学获得理学硕士学位，现工作于中国铁道科学研究院集团有限公司通信信号研究所，主要研究方向为信号监控、复杂网络建模技术。
E-mail：shiyi6226@ sina. com

Shi Yi received her master degree from University of Southern California in 2019. Currently, she is a research trainee at the Communication Signal Research Institute of China Academy of Railway Sciences Group Co., LTD. Her main research interests are signal monitoring and complex network modeling technology.