采用双异质群体演化博弈的网络安全防御决策方法

张恩宁[1]，王刚[1]，马润年[1]，伍维甲[1]，严丽娜[2]
（1. 空军工程大学信息与导航学院，710077，西安；2. 国防科技大学信息通信学院试验训练基地，710106，西安）

摘要：为提高网络安全防御决策的精准度，提出了采用双异质群体演化博弈的网络安全防御决策方法。针对网络攻防的竞争型决策特点，引入生物学种群异质概念，提出双异质群体演化博弈模型；将博弈群体对于博弈历史经验的反思机制模型化为泊松过程，改进经典复制动态方程，提出反思能力是提升模型决策速度的关键因素；结合网络安全防御单次决策的确定性需求和传统纳什均衡解的局限性，提出严格纳什均衡是双异质群体演化博弈稳定的充要条件，通过引入全局单调的势函数，给出了博弈模型存在严格纳什均衡的稳定性证明和仿真验证。理论分析和仿真结果表明，所提模型能够克服经典模型中 50%概率的最优策略事实偏差，且当博弈群体的反思能力为 1.5 时，防御群体决策趋于稳定的速率提升了 151%。

关键词：网络安全防御；决策方法；双异质群体演化博弈；复制动态方程；势函数
中图分类号：TP399 **文献标志码**：A
DOI：10.7652/xjtuxb202109020 **文章编号**：0253-987X(2021)09-0178-11

OSID 码

Network Security Defense Decision Making Method Based on Dual Heterogeneous Population Evolutionary Game Model

ZHANG Enning[1], WANG Gang[1], MA Runnian[1], WU Weijia[1], YAN Lina[2]
(1. Information and Navigation Institute, Air Force Engineering University, Xi'an 710077, China; 2. Information and Communication Institute Experimental Training Base, National University of Defense Technology, Xi'an 710106, China)

Abstract: To improve the accuracy of network security defense decision, according to the characteristics of competitive decision and the limitations of traditional Nash equilibrium (NE), the heterogeneous population evolutionary game model and decision method of network security defense are proposed. Analyzing the difference in decision behavior standards between the attackers and defenders, and introducing the biological population concept to distinguish the two sides as different game populations, a dual heterogeneous population evolutionary game model of network security defense is constructed. Then an improved replicator dynamic equation is proposed based on the reflection mechanism. Considering the deterministic demand of network defense decision-making and the limitations of NE, introducing the potential function and designing the stabilized pure strategy, the optimal defense pure strategy selection algorithm is proposed. It is concluded that a strict NE is just the necessary and sufficient condition for dual heterogeneous population evolutionary game stability, and the stability proof and simulation analysis are carried out for the strict NE combining with the global monotone property of potential function. The theoretical analysis and simulations show that the proposed game model

收稿日期：2021-03-09。 作者简介：张恩宁(1998—)，男，硕士生；王刚(通信作者)，男，教授。 基金项目：国家自然科学基金资助项目(61703420)。
网络出版时间：2021-06-02 网络出版地址：http://kns.cnki.net/kcms/detail/61.1069.T.20210601.1721.008.html

and decision-making method can ensure stable convergence of the defense strategy, and provide a practical and credible defense strategy for the precise decision-making of actual network attack and defense.

Keywords: network security defense; decision-making method; dual heterogeneous population evolutionary game; replicator dynamic equation; potential function

5G 和区块链等信息网络技术加速了信息化向智能化发展的步伐，与此同时，以高级可持续威胁为代表的隐蔽、高效和针对性网络攻击使得网络安全态势和防御决策日趋复杂[1]。网络安全防御决策是网络防御技战术运用的前提和关键环节，建立在对网络攻防行动特点和网络业务负载动态需求等要素的准确掌控上[1]。在现实环境中，网络态势信息的不完整性和决策者的有限理性使得网络攻防双方很难完全知悉对手的准确实时信息，在不完全信息条件下，攻防双方认知和决策模式的不同，导致攻防行为的差异性和攻防决策的异质群体演化博弈特征[2]。

演化博弈中的群体源于生物学中的种群概念。生物学中，同一物种的不同种群因为生存环境的不同而存在性状上的差异，在研究过程中需要将对象区分为异质种群。在学术领域，生物学中的种群映射为博弈理论中的群体，不同群体在博弈中代表的是属性类型相同但决策方式不同的博弈参与方。在一些网络攻防博弈情境中，博弈双方可设定为有限理性博弈参与者，但是其决策方式存在一定差异性。例如，在决策标准方面，防御方要权衡防护节点的资源重要程度，安防部署成本和防御操作代价，而攻击方则需要考虑攻击成本、攻击收益等因素[3]。因此，设定博弈参与方采用相同决策方式的传统演化博弈本质上属于同质群体演化博弈。相对而言，异质群体演化博弈能更好地体现出博弈参与方不同的决策方式对博弈均衡的影响，依据攻防双方收益函数不同的网络攻防博弈，属于双异质群体演化博弈。

决策差异性是网络攻防博弈中需重点关注的问题。对于具体决策，网络攻防双方很难完全知悉对手的准确实时信息，决策的可信度相对不足，攻防双方认知和决策模式的不同，同步导致攻防决策的差异性，这种差异性客观上使得基于防御方收益信息的预测分析很难实现精确性决策[3]。此外，对于决策者和执行单元，单次防御行为应是确定性的和基于纯策略的，经典纳什均衡解固有的多重性使得策略取舍成为网络攻防博弈决策的难题，基于智能算法的网络防御混合策略无法从根本上解决这一问题[2]。

博弈论和行为经济学中对于参与人目标对立、策略依存和非合作型关系的建模符合网络对抗的基本特征规律[4-5]。零和博弈、信号博弈、微分博弈、贝叶斯均衡博弈、马尔可夫博弈及演化博弈等模型被相继运用到网络攻防对抗的行为建模中[6-9]。其中，演化博弈模型可以在不完全信息条件下模拟网络攻防双方策略的互动演化过程，得到稳定的纳什均衡策略，为优选网络防御策略提供参考[10]。目前，相关研究主要集中在 3 个领域。一是演化博弈模型对决策的动态影响。在多阶段博弈中，有限理性的博弈双方会根据初始博弈信息改变策略选择倾向，最终达成混合策略的纳什均衡。文献[11]建立了物联网系统多级非对称信息攻防模型，分析了进攻型策略和防御型策略的收益变化；文献[12]结合现实生活中银行现金转运案例，建立多目标混合遗传算法，得到距离和风险最小化、利润最大化、车辆油耗最小化、时间最小化或最大化等多种目标下的演化博弈最优混合策略，对多目标网络安全防御决策具有很高的参考价值。二是环境对演化博弈模型中系统动力学方程的影响，结合实际环境改进复制动态方程，提升模型的精确性。文献[13-14]针对攻防博弈系统中存在各类随机干扰因素的问题，借鉴高斯白噪声的概念，建立随机复制动态微分方程，分析了系统环境、策略变化等各类随机干扰因素对攻防策略选取演化速率和倾向的影响；文献[15]考虑同一博弈方之间策略的相互影响，引入激励系数，改进传统复制动态方程，完善复制动态速率计算方法，分析了同一博弈方之间策略的促进和抑制作用；文献[16]引入学习机制和第三方惩罚机制，构建了网络攻防演化博弈系统动力学模型，发现通过第三方监管部门，采取对攻击者收益的动态惩罚策略，对攻防双方的恶化混合策略的偏移有重要影响。三是策略的可行性和决策方法。传统演化博弈模型得到的演化均衡解是混合策略，现实中以概率形式进行防御策略选取并不可取，以纯策略为基础进行决策更符合客观规律[17]。文献[18]结合动态目标防御理论，使用精炼贝叶斯均衡求解算法和先验信念修正，提出移动目标防御策略的跳变周期、差异性和先验知识是影响决策效果的 3 个关键因素；文献[19]将多阶段演

化博弈和马尔可夫决策方法相结合，提出多阶段多状态下最优防御策略选取方法；针对复杂网络中攻击方和防御方可用资源的差异性，文献[20]提出了复杂网络拓扑结构对策略选择的制约影响关系。

随着近年来网络攻防技战术的快速发展和实践应用，网络安全防御决策领域凸显了一些新的难题：①决策主体的差异性和基于主体差异性的防御行为模式突破了经典研究中对攻防博弈双方均为同质群体的假设，需要克服基于这种假设导致的最优防御策略事实偏差；②现实多阶段博弈中的防御决策，应充分考虑经验的参考价值和决策行为的智能化需求，在决策过程中引入反思机制和对应的可信支撑模型；③网络安全防御单次决策的确定性需求和传统纳什均衡解的局限性存在固有矛盾，传统纳什均衡解的多重性和混合纳什均衡的不确定性无法满足单次决策中防御行为的可行性要求，需要从模型求解等方面寻求新的突破。

针对这些问题，本文开展了基于异质群体演化博弈的决策方法研究。结合生物学中的种群概念，在博弈中将攻防双方区分为不同群体，提出双异质群体演化博弈模型，克服经典模型中最优防御策略的事实偏差。引入策略反思机制，将博弈主体对于博弈历史经验反馈模型化，改进复制动态方程以提升演化结果的精确性。在模型中引入势函数，突破传统纳什均衡解的局限性，使模型解稳定收敛于可行策略，满足网络安全防御决策的确定性需求。最后，通过理论分析和仿真，验证了所提模型和决策方法的有效性和先进性。

1 双异质群体演化博弈模型构建

1.1 双异质群体演化博弈模型

基于博弈双方决策行为标准的差异性分析，引入生物学种群概念，将攻防双方区分为不同博弈群体，参考经典演化博弈模型的定义[14-15]，提出了网络安全防御的双异质群体演化博弈模型。

定义 1 网络攻防博弈是对称博弈，所有博弈参与者根据其自身属性分为网络攻击方和网络防御方。

定义 2 网络攻防博弈是多阶段博弈，在后一阶段，每个博弈参与方对前一阶段的博弈策略进行模仿。在每一个阶段，博弈参与方的自然出生率为 $\beta(\beta\geqslant 0)$、自然死亡率为 $\delta(\delta\geqslant 0)$，以此代表博弈参与方对于该阶段环境的适应性，即网络攻防双方在阶段前和阶段中因断网掉线等不可抗因素退出博弈的概率。

定义 3 将生物学中的概念映射到博弈模型中。博弈模型中群体代表同一类别个体的集合，即种群。子群体代表具有同样特征的个体的集合，即具备同样性状的个体集合，子群体隶属于群体。

定义 4 每一阶段的博弈是从每个博弈方子群体中随机抽取一个人进行博弈。

定义 5 双异质群体演化博弈模型可表示为 4 元有序组 (N,S,P,U)，其中 $N=(N_1,N_2,\cdots,N_m)$ 为异质群体参与者空间。

结合定义 1，可设定 $N=(N_{\mathrm{A}},N_{\mathrm{D}})$。其中：$N_{\mathrm{A}}$ 是攻击方参与者总空间，$N_{\mathrm{A}}=(N_{\mathrm{A1}},N_{\mathrm{A2}},\cdots,N_{\mathrm{A}j})$，$N_{\mathrm{A1}},N_{\mathrm{A2}},\cdots,N_{\mathrm{A}j}$ 是攻击方参与者子群体；N_{D} 是防御方参与者总空间，$N_{\mathrm{D}}=(N_{\mathrm{D1}},N_{\mathrm{D2}},\cdots,N_{\mathrm{D}i})$，$N_{\mathrm{D1}},N_{\mathrm{D2}},\cdots,N_{\mathrm{D}i}$ 是防御方参与者子群体。

$S=(S_{\mathrm{A}},S_{\mathrm{B}})$ 为攻防博弈参与者群体的混合策略空间。其中：S_{A} 是攻击方参与者纯策略总空间，$S_{\mathrm{A}}=(S_{\mathrm{A1}},S_{\mathrm{A2}},\cdots,S_{\mathrm{A}j})$，$S_{\mathrm{A1}},S_{\mathrm{A2}},\cdots,S_{\mathrm{A}j}$ 是攻击方参与者子群体选择的纯策略；S_{D} 是防御方参与者纯策略总空间，$S_{\mathrm{D}}=(S_{\mathrm{D1}},S_{\mathrm{D2}},\cdots,S_{\mathrm{D}i})$，$S_{\mathrm{D1}},S_{\mathrm{D2}},\cdots,S_{\mathrm{D}i}$ 是防御方参与者子群体选择的纯策略。

$P=(P_{\mathrm{A}},P_{\mathrm{D}})$ 为博弈信念集合。其中：P_{A} 是攻击方博弈信念集合，$P_{\mathrm{A}}=(P_{\mathrm{A1}},P_{\mathrm{A2}},\cdots,P_{\mathrm{A}j})$，$P_{\mathrm{A}j}$ 是选择策略 $S_{\mathrm{A}i}$ 的概率；P_{D} 是攻击方博弈信念集合，$P_{\mathrm{D}}=(P_{\mathrm{D1}},P_{\mathrm{D2}},\cdots,P_{\mathrm{D}i})$，$P_{\mathrm{D}i}$ 是选择策略 $s_{\mathrm{D}i}$ 的概率。

$U=(U_{\mathrm{A}},U_{\mathrm{D}})$ 为博弈收益集合。其中：U_{A} 是攻击方博弈收益集合，$U_{\mathrm{A}}=(U_{\mathrm{A1}},U_{\mathrm{A2}},\cdots,U_{\mathrm{A}j})$，$U_{\mathrm{A}j}$ 是子群体 $N_{\mathrm{A}j}$ 采取纯策略 $S_{\mathrm{A}j}$ 在一个阶段博弈中所获得的期望收益，$\overline{U}_{\mathrm{A}}$ 是攻击方参与者群空间的平均收益，$\overline{U}_{\mathrm{A}}=\sum_{m=1}^{j}P_{\mathrm{A}m}U_{\mathrm{A}m}$；$U_{\mathrm{D}}$ 是防御方博弈收益集合，$U_{\mathrm{D}}=(U_{\mathrm{D1}},U_{\mathrm{D2}},\cdots,U_{\mathrm{D}i})$，$U_{\mathrm{D}i}$ 是子群体 $N_{\mathrm{D}i}$ 采取纯策略 $S_{\mathrm{D}i}$ 在一个阶段博弈中所获得的期望收益，$\overline{U}_{\mathrm{D}}$ 是防御方参与者群空间的平均收益，$\overline{U}_{\mathrm{D}}=\sum_{n=1}^{i}P_{\mathrm{D}n}U_{\mathrm{D}n}$。本文中的收益指博弈对博弈参与方适应性影响的增量效应。以防御方为例，$U_{\mathrm{D}i}=1$ 时博弈对博弈方策略选择不产生影响，$U_{\mathrm{D}i}>1$ 时对策略选择产生积极影响，$U_{\mathrm{D}i}<1$ 时对策略选择产生消极影响。

演化博弈是多阶段的动态博弈过程，每一个阶段的博弈结果都会对后一阶段的博弈产生影响。结合定义 2 和 4，t 时刻子群体 $N_{\mathrm{D}i}(t)$ 的时间导数为

$$N'_{\mathrm{D}i}(t)=(\beta+U_{\mathrm{D}i}(t)-\delta)N_{\mathrm{D}i}(t) \tag{1}$$

结合博弈信念集合定义，可得在任意时刻 t 有

$$P_{\mathrm{D}i}(t)N_{\mathrm{D}}(t)=N_{\mathrm{D}i}(t) \tag{2}$$

式(2)两边同时对 t 求导，整理可得

$$P'_{\mathrm{D}i}(t) = [(\beta+U_{\mathrm{D}i}(t)-\delta)-(\beta+\bar{U}_{\mathrm{D}}(t)-\delta]P_{\mathrm{D}i}(t) = (U_{\mathrm{D}i}(t)-\bar{U}_{\mathrm{D}}(t))P_{\mathrm{D}i}(t) \quad (3)$$

式中 $P'_{\mathrm{D}i}(t)$ 为 t 时刻的防御方博弈信念。式(3)为异质群体复制动态方程表达式。

1.2　关键参数与收益计算

参照文献[17-18]的攻防收益计算方法，定义本文中收益量化的关键参数和计算公式。

定义 6　资源重要程度 C_{r}，指在一次完整的攻防过程中，攻击方目标资源的重要程度。

定义 7　操作代价 O_{cost}，指防御方为使攻击方攻击无效做出针对性调整所需付出的代价。例如，系统开销增大、服务质量下降等。

定义 8　攻击成本 A_{cost}，攻击者进行攻击时所付出的代价。例如，攻击的时间成本、风险成本等。本文中攻击成本与漏洞的威胁级别有关，漏洞的威胁级别越高，攻击成本就越低。

定义 9　感染概率 λ，指攻击方成功利用漏洞感染防御方的概率。

定义 10　防御效果 γ，指防御方利用防御动作成功清除病毒的概率。

结合定义 6～10 可知，某一阶段博弈中，防御方的收益可表示为

$$U_{\mathrm{D}} = \gamma C_{\mathrm{r}} - O_{\mathrm{cost}} \quad (4)$$

攻击者收益源于感染平台后得到的收益，与感染概率有关。攻击收益可表示为

$$U_{\mathrm{A}} = \lambda C_{\mathrm{r}} - A_{\mathrm{cost}} \quad (5)$$

2　改进复制动态方程和决策方法

2.1　策略“反思-学习”机制

在多阶段博弈中，博弈双方通常不会满意当前阶段博弈策略的收益，认为存在更优策略。在这种假设下，博弈双方会寻求其他策略进行学习，在下一个阶段博弈中采用新的策略，这也就是策略“反思-学习”机制[2]。显然，现实网络攻防博弈决策本质上应是基于“反思-学习”机制的。在每一阶段博弈结束后，攻防双方的每一个子群体，都从群体中随机抽取一个其他子群体作为反思对象进行策略学习。这种“反思-学习”机制可结合建模分析，建立与之相一致的演化博弈模型和系统动力学方程。在有限理性条件下，网络攻防子群体基于“反思-学习”机制的策略调整行为，可视为独立的累计随机事件发生次数的增量过程，即泊松过程[2]。子群体的“反思-学习”时间可近似为泊松过程的到达时间，泊松过程到达率即为平均反思率 R_{s}。假设子群体的泊松分布在统计上是相互独立的，则采取防御策略 S_{D} 的子群体“反思-学习”时间之和是一个泊松过程，其到达率为

$$P_{\mathrm{arrive}} = P_{\mathrm{D}i}R_{\mathrm{s}}(N_{\mathrm{D}i}) \quad (6)$$

定义防御策略转变概率为 $T^j_{si}/(N_{\mathrm{D}i})$，即防御群体中除 $N_{\mathrm{D}i}$ 之外的其他子群体将防御策略转变为 $S_{\mathrm{D}i}$ 的概率。本文中，反思由子群体对自身策略的不满意驱动，而每次反思抽取的子群体是随机的，因此 $T^j_{si}(N_{\mathrm{D}i})=P_{\mathrm{D}i}$。如果防御策略的转变也是统计独立的，则群体中从其他策略转变为 $S_{\mathrm{D}i}$ 的总体泊松过程到达率 P_{arrive} 为

$$P_{\mathrm{arrive}} = P_{\mathrm{D}i}R_{\mathrm{s}}(x_i)T^j_{si}(x_i) \quad (7)$$

根据大数定律，设群体随机过程为确定性的流，则子群体 $N_{\mathrm{D}i}$ 来自选择防御策略 $S_{\mathrm{D}j}$ 的子群体 $N_{\mathrm{D}j}$ 的流入 P_{in} 为

$$P_{\mathrm{in}} = \sum_{j\neq i} P_{\mathrm{D}j}R_{\mathrm{s}}(N_{\mathrm{D}j})T^i_{sj}(N_{\mathrm{D}j}) \quad (8)$$

子群体 $N_{\mathrm{D}i}$ 的流出 P_{out} 为

$$P_{\mathrm{out}} = \sum_{j\neq i} P_{\mathrm{D}i}R_{\mathrm{s}}(N_{\mathrm{D}i})T^j_{si}(N_{\mathrm{D}i}) \quad (9)$$

防御策略的博弈信念 $P_{\mathrm{D}i}$ 变为

$$P'_{\mathrm{D}i} = \sum P_{\mathrm{D}j}R_{\mathrm{s}}(N_{\mathrm{D}j})T^i_{sj}(N_{\mathrm{D}j}) - P_{\mathrm{D}i}R_{\mathrm{s}}(N_{\mathrm{D}i}) \quad (10)$$

若群体中策略不成功的子群体的反思率高于策略更成功的子群体的反思率，就会出现收益严格单调递减的选择动态。引入 $\rho(x)$[2]，设势函数 $\rho(x)$ 在其自变量 x 上严格单调递减，则平均反思率表示为

$$R_{\mathrm{s}}(N_{\mathrm{D}i}) = \rho(U_{\mathrm{D}i}) \quad (11)$$

防御策略 $S_{\mathrm{D}i}$ 的选取概率 $P_{\mathrm{D}i}$ 可表示为

$$P'_{\mathrm{D}i} = \sum P_{\mathrm{D}j}\rho(U_{\mathrm{D}j})T^i_{sj}(N_{\mathrm{D}j}) - P_{\mathrm{D}i}\rho(U_{\mathrm{D}i}) \quad (12)$$

设子群体的反思率在其当前收益上是线性递减的，则

$$\rho(U_{\mathrm{D}i}) = a - bU_{\mathrm{D}i} \quad (a,b\in\mathbf{R}) \quad (13)$$

设反思率 $R_{\mathrm{s}}(N_{\mathrm{D}i})$ 非负，则

$$P'_{\mathrm{D}i} = b(U_{\mathrm{D}i}-\bar{U}_{\mathrm{D}})P_{\mathrm{D}i} \quad (14)$$

式中 b 为反思能力，对应策略调整到稳定状态的速率。此时，$P'_{\mathrm{D}i}$ 具有严格纳什均衡，若忽略时间自变量，则式(14)是式(3)的常数倍。

2.2　最优防御纯策略选取方法设计

按照 2.1 小节的防御决策理论，结合网络安全防御行为特点，设计最优防御纯策略选择方法，伪代码如下。

输入：双异质群体演化博弈模型

输出:最优防御纯策略 S_{Di}

BEGIN

1 初始化 P,U,S,b;

2 定义 T,function;

3 for ($k=1;k\leqslant T;k++$)

4 $\overline{U}_{D}=\sum_{i=1}^{N}P_{Di}U_{Di}$;

5 function=求解微分函数 $P'_{Di}=b(U_{Di}-\overline{U}_{D})P_{Di}$;

6 ode45(function,T,P);

7 When $P_{Di}=1$

8 Return S_{Di};

9 Else

10 Return 0;

11 end

END

本文方法对应的时间复杂度为 $O(k(m+n)^2)$。在实际网络攻防中,博弈参与方的数量增加只会导致相应的攻防策略数量也增加,该方法复杂度仍处于同一量级,理论上能够满足网络攻防的时敏需求[17]。

2.3 模型及方法对比

对照文献[11,15-17],从博弈类型、复制动态速率准确性和策略选取应用价值共 3 个方面分析本文模型和决策方法,结果如表 1 所示。

在博弈类型方面,文献[11,15-17]均以同质群体演化博弈理论为基础,不能体现出攻防双方差异性。在复制动态速率准确性方面,文献[11,16]考虑不完全信息条件,结合动态演化思想,突破传统演化博弈模型单阶段完全信息博弈的局限性,提出使用系统动力学方程来表示过程的动态演化特点,至于策略之间的相互影响还有待进一步挖掘。文献[15]引入激励系数刻画同一博弈方之间的策略激励与抑制作用,但并未能给出激励系数的求解过程。在策略选取应用价值方面,文献[11,15]并未区分纯策略和混合策略在实际应用中的价值高低,文献[16]考虑了第三方惩罚策略对防御策略选取的影响,但第三方惩罚策略有其自身局限性,一定程度上降低了模型求解的稳定性。文献[17]结合军事信息网络特点,给出了军事信息网络最优纯策略的选取办法,满足了网络安全防御确定性决策的需求,但是有待进一步研究可行策略的稳定性问题。

表 1 相关工作比较

Table 1 Comparison of related work

文献	群体演化博弈类型	复制动态速率准确性	防御策略类型	应用价值
文献[11]	同质	一般,未考虑策略间影响	未区分防御策略类型	一般
文献[15]	同质	高,定量分析策略间影响机制	未区分防御策略类型	一般
文献[16]	同质	一般,未考虑策略间影响	采用第三方惩罚策略	一般
文献[17]	同质	未涉及	采用纯策略	高
本文	异质	高,建模并定量分析策略间影响机制	采用纯策略	高

对比分析表明,所提模型和决策方法考虑攻防双方的差异性提出了双异质群体演化博弈模型,改进复制动态方程以提升模型求解的准确性,求解稳定可行的纯策略提升了策略的实际应用价值。

3 稳定性分析

3.1 数理证明

首先引入演化稳定和最优策略集合的定义。

定义 11 对于博弈参与方的不同混合策略 S_x、S_y,若存在 $\varepsilon_y\in(0,1)$ 满足不等式 $U(S_x,S_\omega)\geqslant u(S_y,S_\omega)$ 对所有的 $\varepsilon\in(0,\varepsilon_y)$ 都成立,那么 S_x 是演化稳定策略。其中,$S_\omega=\varepsilon S_y+(1-\varepsilon)S_x$ 是混合策略 S_y 入侵原有混合策略空间后形成的新混合策略,S_y 是入侵策略 S_y 在博弈中的被选取概率,$U(S_x,S_\omega)$ 是原策略空间被策略 S_y 入侵后的收益,$U(S_y,S_\omega)$ 是入侵策略的收益。

定义 12 最优策略集合 $\tilde{\beta}(S_i)$ 是所有博弈参与方 N_i 的演化稳定策略 S_i 的集合,$\tilde{\beta}(S_i)=\{S_i\in S:U_{si}\geqslant U_{sj},\forall S_j\in S\}$,集合 $\tilde{\beta}(S_i)$ 是博弈的严格纳什均衡。

定理 1 异质群体 N 演化稳定的充要条件是 N 存在严格纳什均衡。

证明 (1)充分性。设异质群体 N 是演化稳定的,且固定博弈参与者在博弈总空间中的位置为 N_i。令 $S_{yi}\in\tilde{\beta}_i$,并且对所有的 $j\neq i$,都有 $S_{yj}=S_{xj}$。混合策略 $S_\omega=\varepsilon S_y+(1-\varepsilon)S_x$,其中 $\varepsilon\in(0,\varepsilon_y)$,则对于任意 i 有 $U(S_{xi},S_{\omega i})=U(S_{yi},S_{\omega i})$,且对于所有的 $j\neq i$,有 $U(S_{xj},S_{-\omega j})=U(S_{yj},S_{-\omega j})$,其中 $S_{-\omega i}$ 是策略

空间对于博弈方 N_i 的混合策略 $S_{\omega i}$ 的补集。根据演化稳定性，$S_y=S_x$ 且 $S_{yi}\in\tilde{\beta}_i$，因此 $\tilde{\beta}_i=(S_{xi})$，所以 N 存在严格纳什均衡。

(2)必要性。设异质群体 N 存在严格纳什均衡，固定博弈参与者在博弈总空间中的位置为 N_i 且令 $S_y\neq S_x$。对于任意 i 有 $U(S_{xi},S_{-xi})=U(S_{xi})>U(S_{yi},S_{-xi})$，由于收益 $U(S_{xi})$ 是连续函数，必存在 $\varepsilon_y\in(0,1)$ 使得对任何 $\varepsilon\in(0,\varepsilon_y)$ 和 $S_\omega=\varepsilon S_y+(1-\varepsilon)S_x$ 都有 $U(S_{xi},S_{-\omega})>U(S_{yi},S_{-\omega})$，即异质群体 N 是演化稳定的。证毕。

由定理 1 的分析证明可知，R_s 的形式决定了方程是否有渐进稳定的演化均衡解。博弈模型中，不稳定的演化均衡解无法形成可行可信的优选策略。因此，引入势博弈和势函数概念[21]，即如果每个子群体的策略改变是单调的，并且能够映射到一个全局单调函数中，则这个全局单调函数就是势函数，此类博弈必存在严格纳什均衡。因此，将势函数引入式(12)可以使异质群体演化博弈模型得到演化稳定解，从而实现防御的有效精确决策。

引理 1　每个势博弈均有纯策略演化稳定解。

异质群体参与者空间 $N=(N_1,N_2,\cdots,N_m)$，函数 ρ 是异质群体博弈的势函数，因此 N_i 的演化稳定解可映射到 $N(\rho(i))$ 中，当且仅当 $U(\rho(i))\geqslant U(-\rho(i))$ 时成立。由于势函数单调，因此 $N(\rho(i))$ 存在纯策略演化稳定解，N_i 存在纯策略演化稳定解。

3.2　算例分析

以 2×2 攻防对称博弈为例，演绎演化均衡解求解过程。攻防双方各含有两个子群体 N_{A1}、N_{A2}，N_{D1}、N_{D2}，对应纯策略为 S_{A1}、S_{A2}，S_{D1}、S_{D2}。以博弈防御方为例，收益矩阵可以表示为

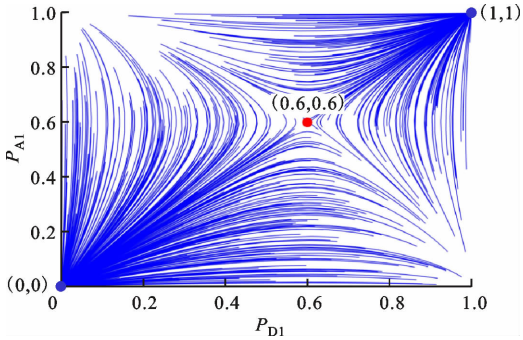
$$\boldsymbol{D}=\begin{bmatrix}u_1 & 0\\ 0 & u_2\end{bmatrix}\tag{15}$$

式中：$\boldsymbol{D}$ 是标准化矩阵，减少了需要观察的变量数；u_1 是攻击方采取纯策略 S_{A1} 时防御方采取纯策略 S_{D1} 获得的相对收益；u_2 是攻击方采取纯策略 S_{A2} 时防御方采取纯策略 S_{D2} 获得的相对收益。将 u_1、u_2 代入式(14)，可得对应防御方和攻击方的复制动态方程

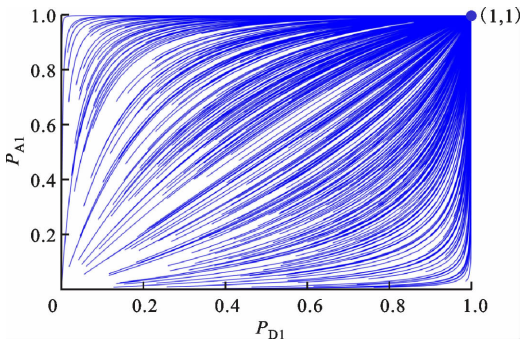
$$\left.\begin{aligned}P'_{A1}&=b[(u_1+u_2)P_{D1}-u_2]P_{A1}(1-P_{A1})\\ P'_{D1}&=b[(u_1+u_2)P_{A1}-u_2]P_{D1}(1-P_{D1})\\ P'_{A2}&=-P'_{A1};\ \ P'_{D2}=-P'_{D1}\end{aligned}\right\}\tag{16}$$

运用 MATLAB 分析博弈演化稳定解的稳定性。由式(15)可知：u_1、u_2 的正负会影响博弈的演化趋势，u_1、u_2 的数值不影响博弈的演化趋势；b 的数值会影响博弈的演化速率。实验中，对 u_1、u_2 及 b 的取值进行多次调整，发现并不影响演化稳定解的收敛结果。参考文献[10]，设定 $|u_1|=0.4$，$|u_2|=0.6$，$b=1$，初始博弈信念 P_{A1}、P_{D1} 为(0,1)间的随机数。图 1 为 500 次蒙特卡罗仿真实验得到的本文模型演化稳定解的收敛轨迹。图中，蓝色标记点是纯策略解收敛点，红色标记点是混合策略解收敛点。

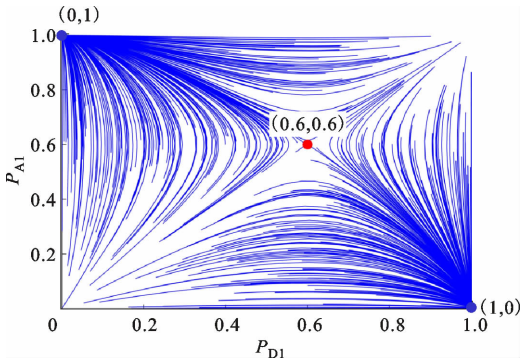
分析图 1b 和 1d 可知：当 $u_1u_2<0$ 时，博弈信念在状态空间内不改变符号，从状态空间内部任意初始位置开始，博弈双方的总体状态都会收敛到严格占优纯策略，即当 $u_1=0.4$、$u_2=-0.6$ 时，攻击方采取纯策略 S_{A1}，防御方采取纯策略 S_{D1}；当 $u_1=-0.4$、$u_2=0.6$ 时，攻击方采取纯策略 S_{A2}，防御方采取纯策略 S_{D2}。



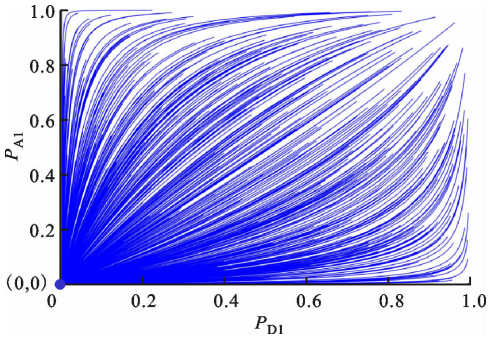
(a) $u_1=0.4$，$u_2=0.6$



(b) $u_1=0.4$，$u_2=-0.6$



(c) $u_1=-0.4$，$u_2=-0.6$



(d)$u_1=-0.4$,$u_2=0.6$

图 1 本文模型演化稳定解的收敛轨迹

Fig. 1 Converging tracks of evolutionary equilibrium of the proposed model

分析图 1a 和 1c 可知:当 $u_1u_2>0$ 时,博弈有两个严格纯策略纳什均衡和一个混合策略纳什均衡。结合式(16)可知,当博弈收敛到混合策略纳什均衡时,$P_{A1}=u_2/(u_1+u_2)$,$P_{D1}=u_2/(u_1+u_2)$。博弈的混合策略纳什均衡点不稳定,会随着 u_1u_2 的变化而发生改变。因此,当 $u_1u_2>0$ 时,博弈仅有两个稳定的严格纯策略纳什均衡。进一步分析图 1a 可知,混合策略纳什均衡是一个鞍点,除了通过鞍点的曲线外,其他的解轨迹都会收敛到两个稳定的纯策略纳什均衡,即当 $u_1=0.4$、$u_2=0.6$ 时,攻击方采取纯策略 S_{A1}、防御方采取纯策略 S_{D1},或者攻击方采取纯策略 S_{A2}、防御方采取纯策略 S_{D2}。进一步分析图 1c 可知,攻防博弈双方的博弈策略会收敛到更极端的情况,即当 $u_1=-0.4$、$u_2=0.6$ 时,攻击方采取纯策略 S_{A1}、防御方采取纯策略 S_{D2},或者攻击方采取纯策略 S_{A2}、防御方采取纯策略 S_{D1}。

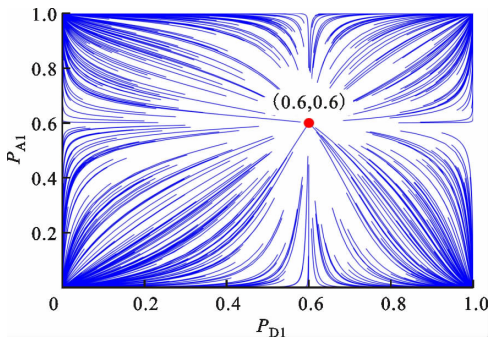
对比其他相关文献可知,双同质群体演化博弈模型中,2×2 对称博弈模型的混合策略演化稳定解是稳定的,可作为最优防御策略的参考[10,15],但在双异质群体博弈模型中,2×2 对称博弈模型的混合策略演化稳定解是鞍点,并不是严格稳定的。这也符合实际博弈过程的特点,即当博弈发生在两个有区别的群体中时,行为上会呈现极端化的趋势,决策会越来越偏向某一种单一策略[22]。

为体现模型及方法克服事实偏差的能力,设置对比实验。经典模型中复制动态方程[2,10]为

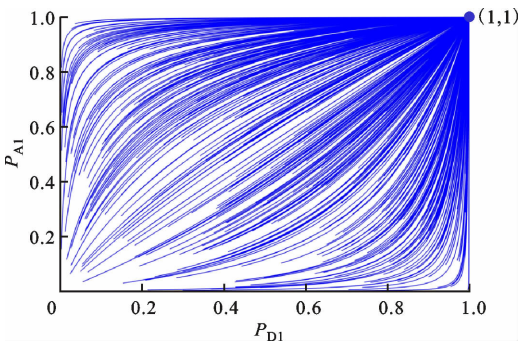
$$\left.\begin{aligned}P'_{A1}&=[(u_1+u_2)P_{A1}-u_2]P_{A1}(1-P_{A1})\\P'_{D1}&=[(u_1+u_2)P_{D1}-u_2]P_{D1}(1-P_{D1})\\P'_{A2}&=-P'_{A1};\ P'_{D2}=-P'_{D1}\end{aligned}\right\}\tag{17}$$

对比式(16)(17)可知,经典模型中攻防双方的策略调整并未考虑对方的博弈策略变化,而是通过自身收益变化调整策略选择。但是,现实网络攻防博弈是常和博弈,攻防双方收益的衡量方式并不相同。运用经典模型选择最优防御策略,可能会受到攻击方欺骗性策略的诱导,产生错误的策略参考结果。为证明这一点,保持$|u_1|=0.4$、$|u_2|=0.6$ 不变,初始博弈信念 P_{A1}、P_{D1} 为(0,1)间的随机数。图 2 为 500 次蒙特卡罗仿真得到的经典模型演化稳定解的收敛轨迹。

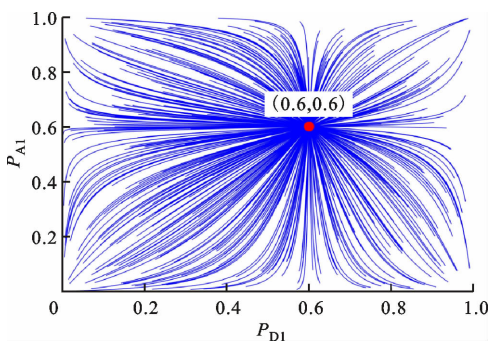
分析图 2a 可知,当 $u_1>0$、$u_2>0$ 时,博弈结果和初始博弈信念 P_{A1}、P_{D1} 的数值有关,无法实现策略的优选。分析图 2c 可知,当 $u_1<0$、$u_2<0$ 时,博弈收敛至混合策略纳什均衡点(0.6,0.6),此时博弈结果以概率形式出现,不利于现实中决策的确定性需求。对比分析图 1b、1d 和图 2b、2d 可知,当 $u_1u_2<0$ 时,经典模型和双异质演化博弈模型的演化稳



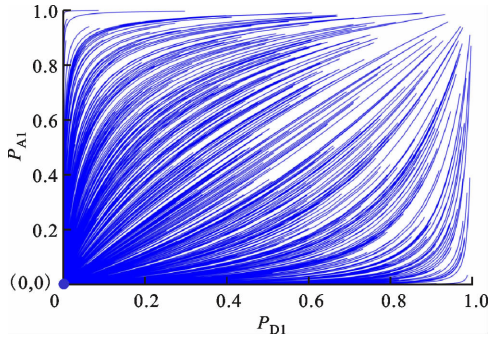
(a)$u_1=0.4$,$u_2=0.6$



(b)$u_1=0.4$,$u_2=-0.6$



(c)$u_1=-0.4$,$u_2=-0.6$



(d) $u_1=-0.4$，$u_2=0.6$

图 2　经典模型演化稳定解的收敛轨迹

Fig. 2　Traditonal converging tracks of evolutionary equilibrium

定解相同。需要说明的是，由于经典模型中防御策略演化并未考虑攻击方博弈信念的变化，攻击方完全可以利用这一漏洞设计欺骗策略来误导防御方。综合分析可知，经典模型有 50%的概率不能实现防御策略的确定性优选，相对而言，本文提出的模型及克服经典模型中同质群体假设带来的事实偏差，为网络安全防御提供可信的防御决策参考。

4　仿真分析

4.1　实验环境

借鉴经典网络信息系统设计理念和相关文献的实验设计[15,17,23]，部署一个简单的网络信息系统进行仿真实验。该网络信息系统的拓扑环境见图 3。

防火墙和网关将网络分为攻击方所在的外网区、实验进行的隔离区(DMZ)和防御方(用户)所在的内网区。防火墙的访问控制策略是非内网主机只能访问 DMZ 区的 FTP 服务器、Web 服务器、E-MAIL 服务器和堡垒主机 H，DMZ 区中的 3 个服务器都是思科服务器。使用 Nessus 工具扫描实验网络信息系统，结合国家信息安全漏洞库(CNNVD)提供的漏洞信息[24]及姜伟等关于网络防御策略及操作代价的定义[25]，本文实验使用原子攻击策略和原子防御策略，分别如表 2 和表 3 所示。

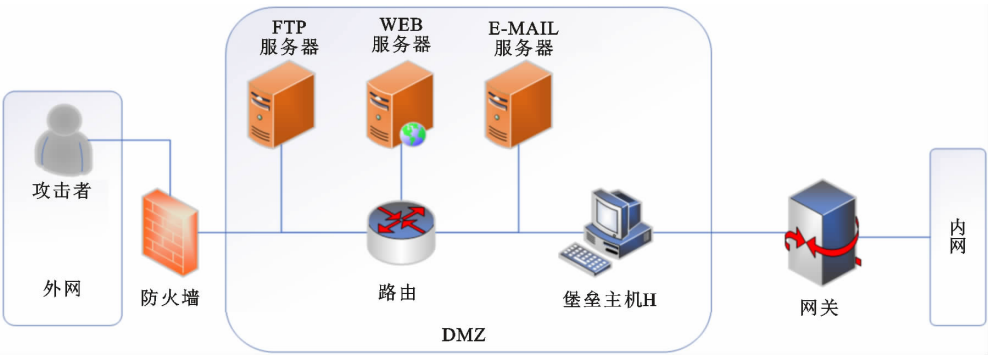


图 3　网络信息系统的拓扑结构

Fig. 3　Topological structure of network information system

表 2　原子攻击策略

Table 2　Atomic attack strategy

序号	原子攻击动作	所利用漏洞编号	漏洞评分	攻击成本	网络攻击策略
a_1	命令注入	CNNVD-202101-1623	0.95	0.1	S_{A1}
a_2	缓冲区错误	CNNVD-202101-1620	0.86	0.1	S_{A1}
a_3	数据伪造问题	CNNVD-202102-1301	0.88	0.1	S_{A1}
a_4	路径遍历	CNNVD-202101-1606	0.35	0.2	S_{A2}
a_5	资源管理错误	CNNVD-202102-1275	0.28	0.2	S_{A2}

攻击方利用高评分漏洞进行攻击，短期内收益见效快，但不利于长期持有后收益升值(典例为零日漏洞)。选择低评分漏洞为目标，攻击成本高，单次收益低[3]。本文将利用高评分漏洞设定为冒险型进攻策略 $S_{A1}=(a_1,a_2,a_3)$，利用低评分漏洞设定为保守型进攻策略 $S_{A2}=(a_4,a_5)$。

防御方的策略收益主要取决于操作代价，操作代价低的防御策略往往有效性较差。因此，本文将使用高操作代价策略设为冒险型防御策略 $S_{D1}=(b_4,b_5)$，使用低操作代价策略设为保守型防御策略 $S_{D2}=(b_1,b_2)$。结合收益计算式(4)(5)，设资源重要程度 $C_r=1$，可得攻防策略收益，如表 4 所示。

表 3 原子防御策略

Table 3 Atomic defense strategy

序号	原子防御动作	防御动作描述	操作代价	防御效果	网络防御策略
b_1	关闭进程	关闭可疑进程或所有进程	0.1	0.19	S_{D1}
b_2	删除文件	删除被修改或者感染的文件	0.2	0.33	S_{D1}
b_3	安装软件升级补丁	升级存在漏洞的软件到最新版本	0.5	0.85	
b_4	格式化硬盘	格式化硬盘去除所有恶意代码	0.7	0.99	S_{D2}
b_5	文件完整性检验	利用软件工具检验系统文件完整性	0.7	0.95	S_{D2}

表 4 攻防策略收益

Table 4 Benefits of attack and defense strategies

策略	攻防动作	收益	策略	攻防动作	收益
S_{A1}	a_1	0.85	S_{D1}	b_4	0.29
	a_2	0.76		b_5	0.25
	a_3	0.78			
S_{A2}	a_4	0.15	S_{D2}	b_1	0.09
	a_5	0.08		b_2	0.13

计算策略收益时，认为策略收益等于策略所包含的原子攻防动作的平均收益。结合式(15)，给出攻防双方的收益量化矩阵

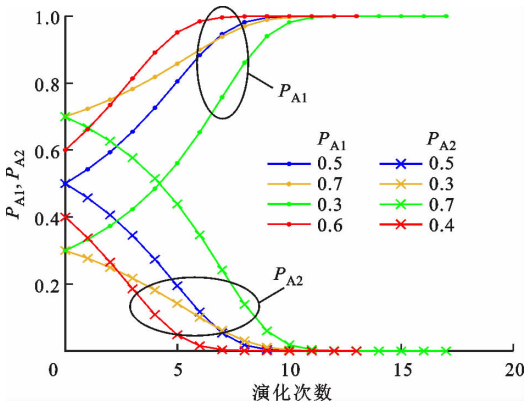
$$\boldsymbol{A}=\begin{bmatrix}0.797 & 0\\ 0 & 0.115\end{bmatrix} \tag{18}$$

$$\boldsymbol{D}=\begin{bmatrix}0.27 & 0\\ 0 & 0.11\end{bmatrix} \tag{19}$$

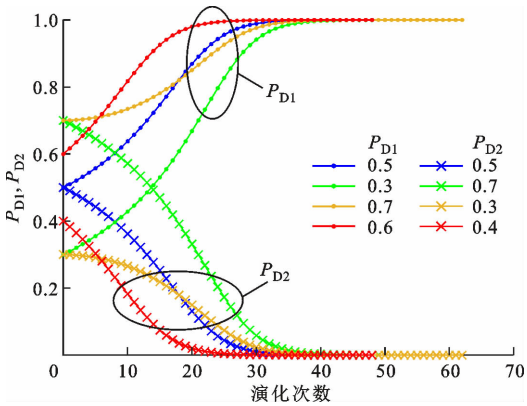
4.2 模型及算法仿真验证

4.2.1 攻防策略选取概率变化趋势 结合式(18)(19)，设置控制变量 $b=1$，研究实验条件下演化稳定策略的收敛情况。设置初始博弈信念$(P_{A1},P_{D1})=\{(0.5,0.5),(0.7,0.3),(0.3,0.7),(0.6,0.4)\}$分别代表攻防双方无策略选取倾向，攻击方倾向于选取策略 S_{A1}、御方倾向于选择策略 S_{D2}，攻击方倾向于选取策略 S_{A2}、防御方倾向于选择策略 S_{D1}，攻击方倾向于选取策略 S_{A1}、防御方倾向于选择策略 S_{D1} 共 4 种不同情况。图 4 给出了攻防双方策略选取概率变化趋势的仿真结果。

分析图 4a、4b 可知：对应不同的初始博弈信念$(P_{A1},P_{D1})=\{(0.5,0.5),(0.7,0.3),(0.3,0.7),(0.6,0.4)\}$，$P_{A1}$ 始终收敛至 1，P_{A2} 始终收敛至 0；P_{D1} 始终收敛至 1，P_{D2} 始终收敛至 0。结合实验条件 $\boldsymbol{A}$、$\boldsymbol{D}$ 的数值进一步分析可知，在冒险型策略的相对收益 u_1 远大于保守型策略的相对收益 u_2 的情况下，无论攻防双方在博弈开始前有无策略选取倾向，网络攻防双方最终都会选择冒险型策略。



(a)攻击策略选取概率



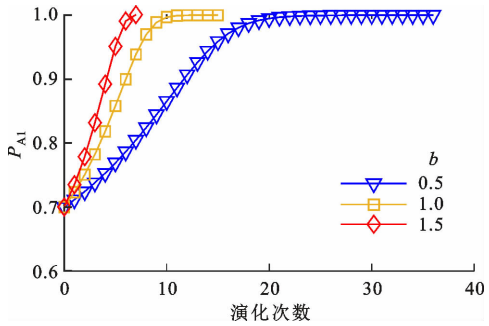
(b)防御策略选取概率

图 4 攻防双方策略选取概率变化趋势

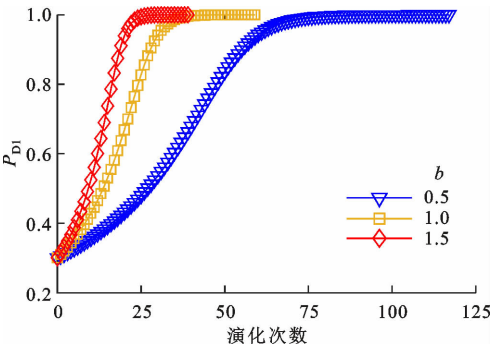
Fig. 4 Changing trend of strategy selection probability of attack and defense

4.2.2 反思能力 b 对攻防策略选取的影响 保持 u_1、u_2 不变，设定初始博弈信念$(P_{A1},P_{D1})=(0.7,0.3)$，分别取 $b=0.5,1,1.5$，研究参数 b 对于博弈结果的影响。图 5 给出了 b 不同取值下攻防双方策略选取概率变化趋势的仿真结果。

分析图 5 可知：当 $b=0.5,1,1.5$ 时，P_{A1} 达到演化稳定所需的演化次数分别为 36、15、7 次；P_{D1} 达到演化稳定所需的演化次数分别为 117、59、39 次。以 $b=1$ 为基准：当 $b=0.5$ 时，防御方博弈群体决策趋



(a)攻击策略选取概率



(b)防御策略选取概率

图 5　不同 b 取值下攻防双方策略选取概率变化趋势

Fig. 5　Changing trend of strategy selection probability of attack and defense for different b values

于稳定的速率减缓了 198%；当 $b=1.5$ 时，防御方博弈群体决策趋于稳定的速率提升了 151%。由此可见，反思能力 b 可以影响博弈结果的求解速度。现实意义在于，反思能力较弱的子群体($b<1$)需要更多时间适应环境才能做出决策；反思能力较强的子群体($b>1$)对环境适应性较强，决策反应较快。理论上合理调整参数 b，使其对应每次博弈的时间窗口，可提升博弈结果的时敏性。

5　结　论

本文根据网络攻防双方决策差异性特征，结合生物学种群概念，提出了双异质群体演化博弈模型。设计了基于策略反思机制的最优防御策略选取算法，结合模拟网络攻防实验环境，开展了仿真验证。本文主要结论如下。

(1)相比传统的演化博弈模型，所提双异质群体演化博弈模型可以突破对称博弈假设，凸显攻防双方的效用特征，得出的演化均衡策略更符合实际网络攻防的行为差异性特点。

(2)在非对称演化博弈中，引入恰当的势函数能够证明演化均衡稳定存在，确保博弈模型所得策略的稳定性和可信性。

(3)反思能力会影响模型和方法求解的速度，表明在不同信息交互机制的群体中最优策略的演化速率不同。由此，可设计网络拓扑结构中的信息交互机制，更好地对应攻防博弈的时间窗口，提升时敏性。

本文在模型求解和算例分析中，假设可选择策略数为 2，后期可考虑多维博弈策略空间的情况下双异质群体演化博弈模型的稳定性和适用性，以及当攻防双方认知信息错误时博弈模型的优化问题。

参考文献：

[1] FALCO G, ELING M, JABLANSKI D, et al. Cyber risk research impeded by disciplinary barriers [J]. Science, 2019, 366(6469): 1066-1069.

[2] SANDHOLM W H. Evolutionary game theory [M]// Complex Social and Behavioral Systems. Cham, Germany: Springer, 2020: 573-608.

[3] ALPCAN T, BASAR T. Network security: a decision and game-theoretic approach [M]. Cambridge, UK: Cambridge University Press, 2010: 20-34.

[4] CHOWDHURY S M. The attack and defense mechanisms: perspectives from behavioral economics and game theory [J]. The Behavioral and Brain Sciences, 2019, 42: e121.

[5] DO C T, TRAN N H, HONG C, et al. Game theory for cyber security and privacy [J]. ACM Computing Surveys, 2017, 50(2): 1-37.

[6] TOSH D, SENGUPTA S, KAMHOUA C A, et al. Establishing evolutionary game models for CYBer security information EXchange (CYBEX) [J]. Journal of Computer and System Sciences, 2018, 98: 27-52.

[7] 蒋侣，张恒巍，王晋东. 基于信号博弈的移动目标防御最优策略选取方法 [J]. 通信学报，2019，40(6)：128-137.
JIANG Lyu, ZHANG Hengwei, WANG Jindong. Optimal strategy selection method for moving target defense based on signaling game [J]. Journal on Communications, 2019, 40(6): 128-137.

[8] 谭晶磊，张恒巍，张红旗，等. 基于 Markov 时间博弈的移动目标防御最优策略选取方法 [J]. 通信学报，2020，41(1)：42-52.
TAN Jinglei, ZHANG Hengwei, ZHANG Hongqi, et al. Optimal strategy selection approach of moving target defense based on Markov time game [J]. Journal on Communications, 2020, 41(1): 42-52.

[9] 张恒巍，李涛，黄世锐. 基于攻防微分博弈的网络安全防御决策方法 [J]. 电子学报，2018，46(6)：1428-

1435.
ZHANG Hengwei, LI Tao, HUANG Shirui. Network defense decision-making method based on attack-defense differential game [J]. Acta Electronica Sinica, 2018, 46(6): 1428-1435.

[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.
HUANG Jianming, ZHANG Hengwei, WANG Jindong, et al. Defense strategies selection based on attack-defense evolutionary game model [J]. Journal on Communications, 2017, 38(1): 168-176.

[11] YANG Yu, CHE Bichen, ZENG Yang, et al. MA-IAD: a multistage asymmetric information attack and defense model based on evolutionary game theory [J]. Symmetry, 2019, 11(2): 215.

[12] GHANNADPOUR S F, ZANDIYEH F. A new game-theoretical multi-objective evolutionary approach for cash-in-transit vehicle routing problem with time windows (a real life case) [J]. Applied Soft Computing, 2020, 93: 106378.

[13] YUAN Huiqun, BI Ya, FU Hanchi, et al. Stability analysis of supply chain in evolutionary game based on stability theory of nonlinear differential equation [J]. Alexandria Engineering Journal, 2020, 59(4): 2331-2337.

[14] 黄健明，张恒巍. 基于随机演化博弈模型的网络防御策略选取方法 [J]. 电子学报，2018，46(9)：2222-2228.
HUANG Jianming, ZHANG Hengwei. A method for selecting defense strategies based on stochastic evolutionary game model [J]. Acta Electronica Sinica, 2018, 46(9): 2222-2228.

[15] 黄健明，张恒巍. 基于改进复制动态演化博弈模型的最优防御策略选取 [J]. 通信学报，2018，39(1)：170-182.
HUANG Jianming, ZHANG Hengwei. Improving replicator dynamic evolutionary game model for selecting optimal defense strategies [J]. Journal on Communications, 2018, 39(1): 170-182.

[16] 朱建明，宋彪，黄启发. 基于系统动力学的网络安全攻防演化博弈模型 [J]. 通信学报，2014，35(1)：54-61.
ZHU Jianming, SONG Biao, HUANG Qifa. Evolution game model of offense-defense for network security based on system dynamics [J]. Journal on Communications, 2014, 35(1): 54-61.

[17] 王增光，卢昱，李玺. 基于不完全信息博弈的军事信息网络主动防御策略选取 [J]. 兵工学报，2020，41(3)：608-617.
WANG Zengguang, LU Yu, LI Xi. Active defense strategy selection of military information network based on incomplete information game [J]. Acta Armamentarii, 2020, 41(3): 608-617.

[18] 刘江，张红旗，刘艺. 基于不完全信息动态博弈的动态目标防御最优策略选取研究 [J]. 电子学报，2018，46(1)：82-89.
LIU Jiang, ZHANG Hongqi, LIU Yi. Research on optimal selection of moving target defense policy based on dynamic game with incomplete information [J]. Acta Electronica Sinica, 2018, 46(1): 82-89.

[19] 张恒巍，黄健明. 基于 Markov 演化博弈的网络防御策略选取方法 [J]. 电子学报，2018，46(6)：1503-1509.
ZHANG Hengwei, HUANG Jianming. Network defense strategy selection method based on Markov evolutionary game [J]. Acta Electronica Sinica, 2018, 46(6): 1503-1509.

[20] LI Yapeng, DENG Ye, XIAO Yu, et al. Attack and defense strategies in complex networks based on game theory [J]. Journal of Systems Science and Complexity, 2019, 32(6): 1630-1640.

[21] LĀ Q D, CHEW Y H, SOONG B H. Potential game theory [M]. Cham, Germany: Springer, 2016: 1-12.

[22] 张峰，吴斌，王柏，等. 基于决策偏移的舆论演化动力学模型 [J]. 系统工程理论与实践，2014，34(S1)：172-178.
ZHANG Feng, WU Bin, WANG Bai, et al. Decision offset based dynamics opinion model [J]. Systems Engineering-Theory & Practice, 2014, 34(S1): 172-178.

[23] SHEYNER O, HAINES J, JHA S, et al. Automated generation and analysis of attack graphs [C] // Proceedings of the 2002 IEEE Symposium on Security and Privacy. Piscataway, NJ, USA: IEEE, 2002: 273-284.

[24] 中国信息安全测评中心. 国家信息安全漏洞库：漏洞信息 [EB/OL]. (2021-02-20)[2021-03-07]. http://www.cnnvd.org.cn/web/vulnerability/querylist.tag.

[25] 姜伟，方滨兴，田志宏，等. 基于攻防博弈模型的网络安全测评和最优主动防御 [J]. 计算机学报，2009，32(4)：817-827.
JIANG Wei, FANG Binxing, TIAN Zhihong, et al. Evaluating network security and optimal active defense based on attack-defense game model [J]. Chinese Journal of Computers, 2009, 32(4): 817-827.

（编辑 陶晴）