基于改进复制动态演化博弈模型的最优防御策略选取

黄健明[1,2]，张恒巍[1,2]
（1.信息工程大学三院，河南 郑州 450001；2. 数学工程与先进计算国家重点实验室，河南 郑州 450001）

摘 要：针对同一博弈群体之间存在策略依存性，通过引入激励系数，改进传统复制动态方程，完善复制动态速率计算方法，构建基于改进复制动态的网络攻防演化博弈模型。利用改进复制动态方程进行演化均衡求解，采用雅可比矩阵的局部稳定分析法对所求均衡点进行稳定性分析，得到不同条件下的最优防御策略。研究结果表明，同一群体的不同策略之间既存在促进作用，也存在抑制作用。通过实验仿真验证了所提模型和方法的准确性和有效性，为解决现实社会中的信息安全问题提供了新的理论支撑。

关键词：策略依赖性；激励系数；改进复制动态；复制动态速率；雅可比矩阵；最优防御策略
中图分类号：TP390
文献标识码：A
doi: 10.11959/j.issn.1000-436x.2018010

Improving replicator dynamic evolutionary game model for selecting optimal defense strategies

HUANG Jianming[1,2], ZHANG Hengwei[1,2]
1. The Third College, Information Engineering University, Zhengzhou 450001, China
2. State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China

Abstract: In terms of the existence of strategy dependency in the same game group, network attack-defense evolutionary game model based on the improved replicator dynamics was constricted by introducing the intensity coefficient, which completed the method of calculating replicator dynamic rate. The improved replicator dynamic equation was adopted to solve the evolutionary equilibrium for the situation that both attack and defense have two optional strategies. The stability of the equilibrium points was analyzed by the local stability analysis method of Jacobian matrix, and the optimal defense strategies were obtained under different conditions. The results show that the strategy dependency between the players in the same group has a certain influence on the evolution of the game, both the incentive and the inhibition. Finally, the accuracy and validity of the model and method are verified by the experimental simulation, which provides a new theoretical support for solving the information security problems in the real.

Key words: strategy dependency, strength coefficient, improving replicator dynamic, replicator dynamic rate, Jacobian matrix, optimal defense strategy

1 引言

“互联网+”时代[1]的到来，使互联网在给人类社会带来便利的同时，也带来了日益严峻的网络安全问题。由于网络规模日益扩大，网络攻击手段日益复杂化、智能化和多样化[2~4]，入侵检测、防火墙[5~7]等传统的静态防御措施已经无法满足当前网络安全的需要，如何确保网络空间安全成为一个亟

收稿日期：2017-05-31；**修回日期**：2017-10-12
通信作者：张恒巍，zhw11qd@163.com
基金项目：国家自然科学基金资助项目（No.61303074, No.61309013）；河南省科技计划基金资助项目（No.12210231003, No.13210231002）
Foundation Items: The National Natural Science Foundation of China (No.61303074, No.61309013), Henan Science and Technology Research Project (No.12210231003, No.13210231002)

待解决的问题。

网络攻防对抗过程具有目标对立性、关系非合作性以及策略依存性等特征，与博弈论的基本特征保持一致[8]，因此，将博弈论应用于网络信息安全已经成为该领域的研究热点。目前的研究成果大都基于传统博弈理论[9,10]，Lye 等[11]基于博弈双方的目标对立性和策略依存性，构建了静态网络攻防博弈模型，用于网络安全行为分析，但网络攻防具有动态变化特性，静态博弈模型无法分析其动态变化过程。基于此，林旺群等[12]基于非合作、非零和动态博弈理论提出了完全信息动态博弈主动防御模型，对网络安全主动防御技术问题进行了研究，对网络攻防动态对抗过程进行了分析，但完全信息条件在实际中无法满足，从而降低了模型的现实意义。姜伟等[13]通过建立不完全信息随机博弈模型，对入侵意图、入侵目标以及策略的选取进行推理。张恒巍等[14]针对具有不完全信息的动态攻防过程，提出了基于攻防信号博弈模型的防御策略选取方法。这些方法均停留在单阶段博弈分析的基础上，而实际网络攻防属于一个多阶段博弈过程，从而降低了模型和方法的适用性。基于此，王长春等[15]将网络攻防对抗过程与 Markov 随机过程相结合，构建多阶段 Markov 网络攻防对抗博弈模型，用于网络行动策略选取分析。但上述研究均以行为者完全理性为前提。由于现实社会中人的有限理性约束，网络攻防行为不可能达到完全理性，因此，完全理性假设与实际情况不符，从而降低了模型和方法的准确性。

演化博弈[16]是传统博弈理论与生物进化理论相结合的产物，建立在博弈者有限理性的前提条件下，以群体为研究对象，不仅继承了传统博弈模型的对抗性、非合作性以及策略依存性等特点，还具有动态演化的特征，强调博弈过程的动态演化[17]，与网络攻防实际更加契合。部分学者已经开始将演化博弈理论应用于网络信息安全领域，但目前相关研究还处于起步阶段。孙薇等[18]将演化博弈理论应用于网络信息安全，采用复制动态对网络攻防对抗的动态演化过程进行了研究，但仅对 2 种策略进行分析，模型的扩展性和适用范围有限。朱建明等[19]基于非合作演化博弈理论，提出了攻防双方信息不对称情况下具有学习机制的攻防演化博弈模型，并采用系统动力学进行过程分析，但仅对模型动力学进行分析，对安全防御指导作用不强。黄健明等[20]构建了基于非合作演化博弈理论的攻防演化博弈模型，采用复制动态对博弈均衡进行了求解分析，用于网络安全防御策略选取，但未对博弈演化过程进行具体分析，降低了模型的可信性。以上演化博弈模型均采用复制动态的学习机制，其思想是选取某一特定策略频率的变化等于该策略的适应度与群体平均适应之间的差值。然而，复制动态并未考虑同一群体下策略间的相互依赖关系。在实际网络攻防过程中，不仅攻防双方策略之间存在依存性，防御策略之间以及攻击策略之间均存在一定的依赖关系。

本文通过引入激励系数，用于表示同一博弈群体中的策略依存关系，改进传统复制动态方程，提高计算复制动态速率的准确性。然后，以实际网络攻防为背景，基于非合作演化博弈理论，构建基于改进复制动态的网络攻防演化博弈模型并对其进行均衡求解。最后，采用雅可比矩阵的局部稳定分析法[21]对所求均衡点进行稳定性分析，得到了不同条件下的博弈演化趋势和最优防御策略，可以用于网络攻击行为分析和预测，并为网络信息安全防御决策提供一定指导。

2　改进复制动态攻防演化博弈模型构建

演化博弈源于生物进化的思想[22]，学习机制是演化博弈的核心[23]，其中以复制动态[24]应用最为广泛。复制动态采用策略学习复制的思想，决策者通过模仿、学习的方法调整自身策略，该机制克服了最优反应动态[25]学习机制无法适用于学习能力较弱个体的问题，但是，并未考虑同一群体下策略之间的相互作用。基于此，通过引入激励系数，构建基于改进复制动态的网络攻防演化博弈模型，用于网络攻击行为预测和安全防御策略选取。

2.1　攻防演化博弈模型

定义 1　网络攻防演化博弈模型（attack-defense evolutionary game model）可以表示为 4 元组，$ADEGM=(N,S,P,U)$。

1) $N=(N_{\mathrm{D}},N_{\mathrm{A}})$ 是演化博弈的参与者空间。其中，N_{D} 表示防御方，N_{A} 表示攻击方，攻防双方均具有多个决策者。

2) $S=(DS,AS)$ 是博弈策略空间。其中，DS 表示防御者的可选策略集，AS 表示攻击者的可选策略集，攻防双方均具有多个可选策略。

3) $P=(q,p)$ 是博弈信念集合。其中，q 表示防御者选取不同防御策略的概率集合，p 表示攻击者选取不同攻击策略的概率集合。

4) $U=(U_{\mathrm{D}},U_{\mathrm{A}})$ 是博弈收益函数集合。其中，U_{D}

表示防御者的博弈收益，U_{A} 表示攻击者的博弈收益，攻防收益值由攻防决策者选取的策略共同决定。

在实际攻防过程中，攻防双方均有多个策略可供选择，假设 $DS=\{DS_1,DS_2,\cdots,DS_n\}$ 为防御方的可选策略集，$AS=\{AS_1,AS_2,\cdots,AS_m\}$ 为攻击方的可选策略集，其中，$m,n\in N$ 且 $m,n\geqslant 2$。在攻防演化过程中，攻防决策者在利益的驱动下通过模仿学习优势策略对自身策略进行调整和改进，使选取不同策略的决策者个数随着时间发生改变，攻防对抗过程呈现动态演化的特点。攻防过程中形成的博弈树如图 1 所示。

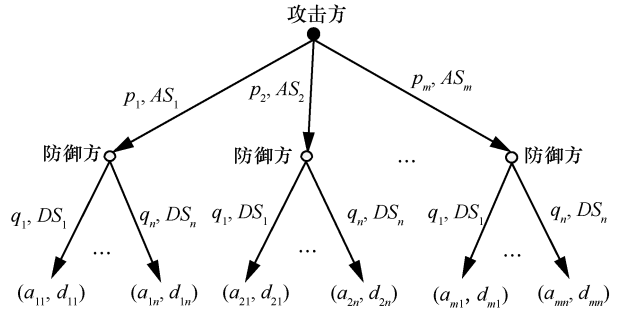

图 1 基本网络攻防博弈树

其中，p_i 表示选择攻击策略 AS_i 的概率，q_j 表示选防御策略 DS_j 的概率，a_{ij} 表示攻防策略对 (AS_i,DS_j) 在一次博弈过程中产生的攻击方收益，d_{ij} 表示攻防策略对 (AS_i,DS_j) 在一次博弈过程中产生的防御方收益。

基于以上条件，可以计算出防御方不同防御策略的期望收益 u_i^{D} 和平均收益 $\overline{u}^{\mathrm{D}}$。

$$u_i^{\mathrm{D}}=\sum_{j=1}^{m}p_j d_{ji} \tag{1}$$

$$\overline{u}^{\mathrm{D}}=\sum_{i=1}^{n}q_i u_i^{\mathrm{D}} \tag{2}$$

同理，可以计算出攻击方不同攻击策略的期望收益 u_i^{A} 和平均收益 $\overline{u}^{\mathrm{A}}$。

$$u_i^{\mathrm{A}}=\sum_{j=1}^{n}q_j a_{ij} \tag{3}$$

$$\overline{u}^{\mathrm{A}}=\sum_{i=1}^{m}p_i u_i^{\mathrm{A}} \tag{4}$$

2.2 改进复制动态构造

基于上述建立的攻防演化博弈模型，针对防御方的 n 种可选防御策略 $DS=\{DS_1,DS_2,\cdots,DS_n\}$，假设 t 时刻选取策略 DS_i 的防御者个数为 $x_i(t)$，其所占防御决策者总体个数比例为 $q_i(t)$，防御策略 DS_i 的适应能力[26]（期望收益）为 $u_i^{\mathrm{D}}(t)$，在 t 时刻的平均适应度[27]（平均收益）为 $\overline{u}^{\mathrm{D}}(t)$。

由此可知

$$\sum_{i=1}^{n}q_i(t)=1 \tag{5}$$

$$q_i(t)=\frac{x_i(t)}{\sum_{i=1}^{n}x_i(t)} \tag{6}$$

$$u_i^{\mathrm{D}}(t)=\sum_{j=1}^{m}p_j d_{ji} \tag{7}$$

$$\overline{u}^{\mathrm{D}}(t)=\sum_{i=1}^{n}q_i u_i^{\mathrm{D}}(t) \tag{8}$$

随着攻防过程的推进，选取策略 DS_i 的个体数目发生变化，其复制动态速率既正比于选取 DS_i 的个体数目，又与策略 DS_i 的适应能力正相关，即

$$x_i'(t)=\alpha_i x_i(t)u_i^{\mathrm{D}}(t) \tag{9}$$

其中，$\alpha_i(\alpha_i>0)$ 为策略影响因子，表示防御策略 DS_i 的影响力大小，正比于防御收益值，由防御策略 DS_i 自身性质决定，不同策略的影响因子不同。在实际网络攻防过程中，不同防御策略之间具有一定的影响关系，扩散速度较快的优势策略具有更强的策略影响力。α_i 越大，表示防御策略 DS_i 对其他防御策略的影响力越强；反之，表示防御策略 DS_i 对其他防御策略的影响力越弱。

通过对式(6)进行求导，可以得到选取防御策略 DS_i 的复制动态为

$$\begin{aligned}q_i'(t)&=\frac{x_i'(t)\sum_{i=1}^{n}x_i(t)-x_i(t)\sum_{i=1}^{n}x_i'(t)}{\left[\sum_{i=1}^{n}x_i(t)\right]^2}\\&=\frac{x_i(t)}{\sum_{i=1}^{n}x_i(t)}\left[\frac{x_i'(t)}{x_i(t)}-\frac{\sum_{i=1}^{n}x_i'(t)}{\sum_{i=1}^{n}x_i(t)}\right]\\&=q_i(t)\left[\frac{\alpha_i x_i(t)u_i^{\mathrm{D}}(t)}{x_i(t)}-\frac{\sum_{i=1}^{n}\alpha_i x_i(t)u_i^{\mathrm{D}}(t)}{\sum_{i=1}^{n}x_i(t)}\right]\\&=\alpha_i q_i(t)\left[u_i^{D}(t)-\overline{u}^{\mathrm{D}}(t)+\sum_{j=1}^{n}\left(1-\frac{\alpha_j}{\alpha_i}\right)x_j(t)u_j^{\mathrm{D}}(t)\right]\end{aligned} \tag{10}$$

对于攻击方的 m 种可选攻击策略 $AS=\{AS_1, AS_2,\cdots, AS_m\}$，假设 t 时刻选取策略 AS_i 的攻击者个数为 $y_i(t)$，其所占攻击决策者总体个数比例为 $p_i(t)$，攻击策略 AS_i 的适应能力（期望收益）为 $u_i^{\mathrm{A}}(t)$，在 t 时刻的平均适应度（平均收益）为 $\overline{u}^{\mathrm{A}}(t)$。

同理可知

$$\sum_{i=1}^{m} p_i(t)=1 \tag{11}$$

$$p_i(t)=\frac{y_i(t)}{\sum_{i=1}^{m} y_i(t)} \tag{12}$$

$$u_i^{\mathrm{A}}(t)=\sum_{j=1}^{n} q_j a_{ij} \tag{13}$$

$$\overline{u}^{\mathrm{A}}(t)=\sum_{i=1}^{m} p_i u_i^{\mathrm{A}}(t) \tag{14}$$

随着攻防过程的推进，选取策略 AS_i 的个体数目发生变化，其复制动态速率既正比于选取 AS_i 的个体数目，又与策略 AS_i 的适应能力正相关，即

$$y_i'(t)=\beta_i y_i(t) u_i^{\mathrm{A}}(t) \tag{15}$$

其中，$\beta_i(\beta_i>0)$ 为策略影响因子，表示攻击策略 AS_i 的影响力大小，正比于攻击收益值，由攻击策略 AS_i 自身性质决定。β_i 越大，表示攻击策略 AS_i 对其他攻击策略的影响力越强；反之，表示攻击策略 AS_i 对其他攻击策略的影响力越弱。

通过对式(12)进行求导，可以得到选取攻击策略 AS_i 的复制动态为

$$\begin{aligned} p_i'(t)&=\frac{y_i'(t)\sum_{i=1}^{m} y_i(t)-y_i(t)\sum_{i=1}^{m} y_i'(t)}{\left[\sum_{i=1}^{m} y_i(t)\right]^2}\\ &=\beta_i p_i(t)\left[u_i^{\mathrm{A}}(t)-\overline{u}^{\mathrm{A}}(t)+\sum_{j=1}^{m}\left(1-\frac{\beta_j}{\beta_i}\right) y_j(t) u_j^{\mathrm{A}}(t)\right] \end{aligned} \tag{16}$$

联立式(10)和式(16)，得到改进后的复制动态微分方程系统[28]为

$$\begin{cases} q_i'(t)=\alpha_i q_i(t)\left[u_i^{\mathrm{D}}(t)-\overline{u}^{\mathrm{D}}(t)+\sum_{j=1}^{n}\left(1-\frac{\alpha_j}{\alpha_i}\right) x_j(t) u_j^{\mathrm{D}}(t)\right] \\ p_i'(t)=\beta_i p_i(t)\left[u_i^{\mathrm{A}}(t)-\overline{u}^{\mathrm{A}}(t)+\sum_{j=1}^{m}\left(1-\frac{\beta_j}{\beta_i}\right) y_j(t) u_j^{\mathrm{A}}(t)\right] \end{cases} \tag{17}$$

通过观察可知，当 $\alpha_i=\alpha_j=1$、$\beta_i=\beta_j=1$ 时，即可得到 Taylor 和 Jonker[29]最早提出的复制动态方程

$$\begin{cases} q_i'(t)=q_i(t)\left[u_i^{\mathrm{D}}(t)-\overline{u}^{\mathrm{D}}(t)\right] \\ p_i'(t)=p_i(t)\left[u_i^{\mathrm{A}}(t)-\overline{u}^{\mathrm{A}}(t)\right] \end{cases} \tag{18}$$

令 $\lambda_{ij}=\frac{\alpha_i}{\alpha_j}$，将其定义为激励系数，在攻防过程中，表示防御策略 DS_i 和 DS_j 之间的激励关系，既包含正激励，也包含负激励。当 $\lambda_{ij}<1$ 时，表示防御策略 DS_i 对 DS_j 具有促进作用；当 $\lambda_{ij}>1$ 时，表示防御策略 DS_i 对 DS_j 具有抑制作用。

同理，令 $\gamma_{ij}=\frac{\beta_i}{\beta_j}$，用于表示攻击策略 AS_i 和 AS_j 之间的激励关系。将其分别代入式(17)可得

$$\begin{cases} q_i'(t)=\alpha_i q_i(t)\left[u_i^{\mathrm{D}}(t)-\overline{u}^{\mathrm{D}}(t)+\sum_{j=1}^{n}(1-\lambda_{ji}) x_j(t) u_j^{\mathrm{D}}(t)\right] \\ p_i'(t)=\beta_i p_i(t)\left[u_i^{\mathrm{A}}(t)-\overline{u}^{\mathrm{A}}(t)+\sum_{j=1}^{m}(1-\gamma_{ji}) y_j(t) u_j^{\mathrm{A}}(t)\right] \end{cases} \tag{19}$$

令 $\begin{cases} q_i'(t)=0 \\ p_i'(t)=0 \end{cases}$，通过求解改进复制动态方程式(19)，即可得到改进条件下的网络攻防演化博弈平衡状态点，从而可以实现安全防御策略选取的分析和预测。

3　攻防演化稳定分析

基于上述提出的改进复制动态攻防演化博弈模型，针对攻防双方均具有 2 种可选策略的案例，对相应的改进复制动态方程进行均衡求解，并对不同均衡解进行稳定性分析，得到不同条件下的最优防御策略。

3.1　攻防演化博弈描述

针对网络防御方，以防御者是否投资网络安全防御，构建防御方的可选策略集 $DS=\{DS_1, DS_2\}$，其中，DS_1 表示防御者投资安全防御，DS_2 表示防御者不投资安全防御。针对攻击方，以攻击者是否实施网络攻击，构建攻击方的可选策略集 $AS=\{AS_1, AS_2\}$，其中，AS_1 表示攻击者实施网络攻击，AS_2 表示攻击者不实施网络攻击。在攻防过程中，策略被攻防决策者采用的概率不同，且该概率随着时间的推移在学习机制的作用下不断变化，

使攻防策略选取形成一个动态变化过程。其对应的网络攻防博弈树如图 2 所示。

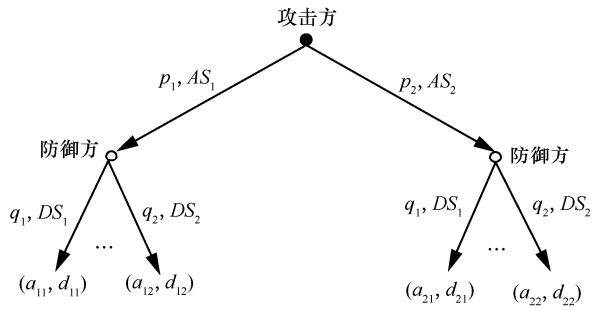

图 2 网络攻防博弈树

其中，p_1表示攻击者选取攻击策略 AS_1 的概率，p_2 表示选取攻击策略 AS_2 的概率，且满足 $p_1+p_2=1$；q_1 表示防御者选取防御策略 DS_1 的概率，q_2 表示选取防御策略 DS_2 的概率，且满足 $q_1+q_2=1$。a_{ij}、d_{ij} 分别表示攻防策略对 (AS_i, DS_j) 所产生的攻防收益值。

3.2 攻防演化博弈求解

基于上述条件，结合第 2.2 节可得

$$\begin{cases} u_1^{\mathrm{D}}(t)=p_1(t)d_{11}+p_2(t)d_{21} \\ u_2^{\mathrm{D}}(t)=p_1(t)d_{12}+p_2(t)d_{22} \\ \overline{u}^{\mathrm{D}}(t)=q_1(t)u_1^{\mathrm{D}}(t)+q_2(t)u_2^{\mathrm{D}}(t) \\ u_1^{\mathrm{A}}(t)=q_1(t)a_{11}+q_2(t)a_{12} \\ u_2^{\mathrm{A}}(t)=q_1(t)a_{21}+q_2(t)a_{22} \\ \overline{u}^{\mathrm{A}}(t)=p_1(t)u_1^{\mathrm{A}}(t)+p_2(t)u_2^{\mathrm{A}}(t) \end{cases} \tag{20}$$

由

$$q_1(t)+q_2(t)=1,\quad p_1(t)+p_2(t)=1$$

$$\boldsymbol{J}=\begin{bmatrix} \alpha_1(1-2q_1)\left[d_{21}-\lambda_{21}d_{22}+(d_{11}-d_{21}-\lambda_{21}d_{12}+\lambda_{21}d_{22})p_1\right] \\ \beta_1 p_1(1-p_1)(a_{11}-a_{12}-\gamma_{21}a_{21}+\gamma_{21}a_{22}) \end{bmatrix}$$

由此可知，该雅可比矩阵 $\boldsymbol{J}$ 的行列式和迹分别为

$$\begin{aligned} \det\boldsymbol{J}=&\alpha_1(1-2q_1)[d_{21}-\lambda_{21}d_{22}+ \\ &(d_{11}-d_{21}-\lambda_{21}d_{12}+\lambda_{21}d_{22})p_1]\beta_1(1-2p_1) \\ &[a_{12}-\gamma_{21}a_{22}+(a_{11}-a_{12}-\gamma_{21}a_{21}+\gamma_{21}a_{22})q_1]- \\ &\alpha_1 q_1(1-q_1)(d_{11}-d_{21}-\lambda_{21}d_{12}+\lambda_{21}d_{22})\cdot \\ &\beta_1 p_1(1-p_1)(a_{11}-a_{12}-\gamma_{21}a_{21}+\gamma_{21}a_{22}) \end{aligned} \tag{23}$$

$$\begin{aligned} \mathrm{tr}\boldsymbol{J}=&\alpha_1(1-2q_1)[d_{21}-\lambda_{21}d_{22}+(d_{11}-d_{21}-\lambda_{21}d_{12}+\lambda_{21}d_{22})p_1]+ \\ &\beta_1(1-2p_1)[a_{12}-\gamma_{21}a_{22}+(a_{11}-a_{12}-\gamma_{21}a_{21}+\gamma_{21}a_{22})q_1] \end{aligned} \tag{24}$$

可得 $q_1'(t)=-q_2'(t)$，$p_1'(t)=-p_2'(t)$。

因此，只需考虑 $q_1(t)$ 和 $p_1(t)$ 的演化状态，即可得到整个攻防博弈系统的策略选取演化情况。

结合式(19)，可以进一步得到防御策略 DS_1 和攻击策略 AS_1 的复制动态方程为

$$\begin{cases} \dfrac{\mathrm{d}q_1(t)}{\mathrm{d}t}=\alpha_1 q_1(1-q_1)[d_{21}-\lambda_{21}d_{22}+ \\ \qquad (d_{11}-d_{21}-\lambda_{21}d_{12}+\lambda_{21}d_{22})p_1] \\ \dfrac{\mathrm{d}p_1(t)}{\mathrm{d}t}=\beta_1 p_1(1-p_1)[a_{12}-\gamma_{21}a_{22}+ \\ \qquad (a_{11}-a_{12}-\gamma_{21}a_{21}+\gamma_{21}a_{22})q_1] \end{cases} \tag{21}$$

令 $\begin{cases} q_1'(t)=0 \\ p_1'(t)=0 \end{cases}$，通过求解可以得到以下 5 组解：

1) $\begin{cases} q_1=0 \\ p_1=0 \end{cases}$；2) $\begin{cases} q_1=0 \\ p_1=1 \end{cases}$；3) $\begin{cases} q_1=1 \\ p_1=0 \end{cases}$；4) $\begin{cases} q_1=1 \\ p_1=1 \end{cases}$；

5) $\begin{cases} p_1=\dfrac{-d_{21}+\lambda_{21}d_{22}}{d_{11}-d_{21}-\lambda_{21}d_{12}+\lambda_{21}d_{22}} \\ q_1=\dfrac{-a_{12}+\gamma_{21}a_{22}}{a_{11}-a_{12}-\gamma_{21}a_{21}+\gamma_{21}a_{22}} \end{cases}$。

3.3 攻防演化动力学分析

针对上述建立的改进复制动态网络攻防演化博弈模型，采用系统动力学方法[30,31]对复制动态演化博弈系统进行分析，能够有效探索博弈系统内在的演化特性。

基于上述 5 个演化平衡点，采用雅可比矩阵的局部稳定分析法对所有演化平衡点进行稳定性分析。复制动态方程式(21)的雅可比矩阵为

$$\begin{bmatrix} \alpha_1 q_1(1-q_1)(d_{11}-d_{21}-\lambda_{21}d_{12}+\lambda_{21}d_{22}) \\ \beta_1(1-2p_1)\left[a_{12}-\gamma_{21}a_{22}+(a_{11}-a_{12}-\gamma_{21}a_{21}+\gamma_{21}a_{22})q_1\right] \end{bmatrix} \tag{22}$$

针对该博弈复制动态系统中存在的演化平衡点，根据雅可比矩阵局部稳定分析法可知，当 $\det\boldsymbol{J}>0$，$\mathrm{tr}\boldsymbol{J}<0$ 时，平衡点是稳定的；当 $\det\boldsymbol{J}>0$，$\mathrm{tr}\boldsymbol{J}>0$ 时，平衡点是不稳定的；当 $\det\boldsymbol{J}<0$ 而 $\mathrm{tr}\boldsymbol{J}$ 为任意值时，平衡点为鞍点。下面将对所有结果进行列举分析。

1) 当 $d_{11}-d_{21}-\lambda_{21}d_{12}+\lambda_{21}d_{22}=0$，$a_{11}-a_{12}-\gamma_{21}a_{21}+\gamma_{21}a_{22}=0$ 时，攻防博弈系统式(21)具有 4 个平衡点：$A(0,0)$，$B(0,1)$，$C(1,0)$，$D(1,1)$。

将上述 4 个点分别代入式(22)和式(23)，可以得到表 1 的结果。

表 1　攻防博弈复制动态系统均衡点对应的雅可比行列式和迹计算式

均衡点 (q_1, p_1)	$\boldsymbol{J}$ 的行列式和迹的计算式
$A(0,0)$	$\det \boldsymbol{J} = \alpha_1\beta_1(d_{21}-\lambda_{21}d_{22})(a_{12}-\gamma_{21}a_{22})$ $\mathrm{tr}\boldsymbol{J} = \alpha_1(d_{21}-\lambda_{21}d_{22})+\beta_1(a_{12}-\gamma_{21}a_{22})$
$B(0,1)$	$\det \boldsymbol{J} = -\alpha_1\beta_1(d_{11}-\lambda_{21}d_{12})(a_{12}-\gamma_{21}a_{22})$ $\mathrm{tr}\boldsymbol{J} = \alpha_1(d_{11}-\lambda_{21}d_{12})-\beta_1(a_{12}-\gamma_{21}a_{22})$
$C(1,0)$	$\det \boldsymbol{J} = -\alpha_1\beta_1(d_{21}-\lambda_{21}d_{22})(a_{11}-\gamma_{21}a_{21})$ $\mathrm{tr}\boldsymbol{J} = -\alpha_1(d_{21}-\lambda_{21}d_{22})+\beta_1(a_{11}-\gamma_{21}a_{21})$
$D(1,1)$	$\det \boldsymbol{J} = \alpha_1\beta_1(d_{11}-\lambda_{21}d_{12})(a_{11}-\gamma_{21}a_{21})$ $\mathrm{tr}\boldsymbol{J} = -\alpha_1(d_{11}-\lambda_{21}d_{12})-\beta_1(a_{11}-\gamma_{21}a_{21})$

针对雅可比行列式和迹的计算式，可以分以下 4 种情况进行分析讨论。

情形 1　当 $d_{11}-\lambda_{21}d_{12}<0$，$a_{11}-\gamma_{21}a_{21}<0$ 时，$A(0,0)$ 为稳定点，$B(0,1)$ 和 $C(1,0)$ 为鞍点，$D(1,1)$ 为不稳定点。此时，（不投资防御，不实施攻击）为攻防演化稳定策略，不投资防御为防御方最优安全防御策略。

情形 2　当 $d_{11}-\lambda_{21}d_{12}<0$，$a_{11}-\gamma_{21}a_{21}>0$ 时，$B(0,1)$ 为稳定点，$A(0,0)$ 和 $D(1,1)$ 为鞍点，$C(1,0)$ 为不稳定点。此时，（不投资防御，实施攻击）为攻防演化稳定策略，不投资防御为防御方最优安全防御策略。

情形 3　当 $d_{11}-\lambda_{21}d_{12}>0$，$a_{11}-\gamma_{21}a_{21}<0$ 时，$C(1,0)$ 为稳定点，$A(0,0)$ 和 $D(1,1)$ 为鞍点，$B(0,1)$ 为不稳定点。此时，（投资防御，不实施攻击）为攻防演化稳定策略，投资防御为防御方最优安全防御策略。

情形 4　当 $d_{11}-\lambda_{21}d_{12}>0$，$a_{11}-\gamma_{21}a_{21}>0$ 时，$D(1,1)$ 为稳定点，$B(0,1)$ 和 $C(1,0)$ 为鞍点，$A(0,0)$ 为不稳定点。此时，（投资防御，实施攻击）为攻防演化稳定策略，投资防御为防御方最优安全防御策略。具体判别过程依据如表 2 所示。

2) 当 $d_{11}-d_{21}-\lambda_{21}d_{12}+\lambda_{21}d_{22}=0$，$a_{11}-a_{12}-\gamma_{21}a_{21}+\gamma_{21}a_{22}\neq 0$ 时，攻防博弈系统(21)具有 4 个平衡点：$A(0,0)$，$B(0,1)$，$C(1,0)$，$D(1,1)$。

针对表 1 中的雅可比行列式和迹的计算式，可以分以下 8 种情形进行分析讨论：①$d_{11}-\lambda_{21}d_{12}<0$，$a_{11}-\gamma_{21}a_{21}<0$，$a_{12}-\gamma_{21}a_{22}<0$；②$d_{11}-\lambda_{21}d_{12}<0$，$a_{11}-\gamma_{21}a_{21}>0$，$a_{12}-\gamma_{21}a_{22}<0$；③$d_{11}-\lambda_{21}d_{12}>0$，$a_{11}-\gamma_{21}a_{21}<0$，$a_{12}-\gamma_{21}a_{22}<0$；④$d_{11}-\lambda_{21}d_{12}>0$，$a_{11}-\gamma_{21}a_{21}>0$，$a_{12}-\gamma_{21}a_{22}<0$；⑤$d_{11}-\lambda_{21}d_{12}<0$，$a_{11}-\gamma_{21}a_{21}<0$，$a_{12}-\gamma_{21}a_{22}>0$；⑥$d_{11}-\lambda_{21}d_{12}<0$，$a_{11}-\gamma_{21}a_{21}>0$，$a_{12}-\gamma_{21}a_{22}>0$；⑦$d_{11}-\lambda_{21}d_{12}>0$，$a_{11}-\gamma_{21}a_{21}<0$，$a_{12}-\gamma_{21}a_{22}>0$；⑧$d_{11}-\lambda_{21}d_{12}>0$，$a_{11}-\gamma_{21}a_{21}>0$，$a_{12}-\gamma_{21}a_{22}>0$。具体判别过程依据如表 3 所示。

3) 当 $d_{11}-d_{21}-\lambda_{21}d_{12}+\lambda_{21}d_{22}\neq 0$，$a_{11}-a_{12}-\gamma_{21}a_{21}+\gamma_{21}a_{22}=0$ 时，攻防博弈系统(21)具有 4 个平衡点：$A(0,0)$，$B(0,1)$，$C(1,0)$，$D(1,1)$。

针对雅可比行列式和迹的计算式，可以分以下 8 种情况进行分析讨论：①$d_{11}-\lambda_{21}d_{12}<0$，$a_{11}-\gamma_{21}a_{21}<0$，$d_{21}-\lambda_{21}d_{22}<0$；②$d_{11}-\lambda_{21}d_{12}<0$，$a_{11}-\gamma_{21}a_{21}>0$，$d_{21}-\lambda_{21}d_{22}<0$；③$d_{11}-\lambda_{21}d_{12}>0$，

表 2　攻防博弈演化稳定判别依据（$d_{11}-d_{21}-\lambda_{21}d_{12}+\lambda_{21}d_{22}=0$，$a_{11}-a_{12}-\gamma_{21}a_{21}+\gamma_{21}a_{22}=0$）

情形	判别依据	$A(0,0)$	$B(0,1)$	$C(1,0)$	$D(1,1)$
情形 1	$\det \boldsymbol{J}$	+	–	–	+
	$\mathrm{tr}\boldsymbol{J}$	–	不定	不定	+
	稳定性	ESS	鞍点	鞍点	不稳定
情形 2	$\det \boldsymbol{J}$	–	+	+	–
	$\mathrm{tr}\boldsymbol{J}$	不定	–	+	不定
	稳定性	鞍点	ESS	不稳定	鞍点
情形 3	$\det \boldsymbol{J}$	–	+	+	–
	$\mathrm{tr}\boldsymbol{J}$	不定	+	–	不定
	稳定性	鞍点	不稳定	ESS	鞍点
情形 4	$\det \boldsymbol{J}$	+	–	–	+
	$\mathrm{tr}\boldsymbol{J}$	+	不定	不定	–
	稳定性	不稳定	鞍点	鞍点	ESS

表 3 攻防博弈演化稳定判别依据（$d_{11}-d_{21}-\lambda_{21}d_{12}+\lambda_{21}d_{22}=0$，$a_{11}-a_{12}-\gamma_{21}a_{21}+\gamma_{21}a_{22}\neq 0$）

情形	判别依据	$A(0,0)$	$B(0,1)$	$C(1,0)$	$D(1,1)$
情形 1	$\det \boldsymbol{J}$	+	–	–	+
	$\mathrm{tr}\boldsymbol{J}$	–	不定	不定	+
	稳定性	ESS	鞍点	鞍点	不稳定
情形 2	$\det \boldsymbol{J}$	+	–	–	–
	$\mathrm{tr}\boldsymbol{J}$	–	不定	+	不定
	稳定性	ESS	鞍点	鞍点	鞍点
情形 3	$\det \boldsymbol{J}$	–	+	+	–
	$\mathrm{tr}\boldsymbol{J}$	不定	+	–	不定
	稳定性	鞍点	不稳定	ESS	鞍点
情形 4	$\det \boldsymbol{J}$	–	+	–	+
	$\mathrm{tr}\boldsymbol{J}$	不定	+	不定	–
	稳定性	鞍点	不稳定	鞍点	ESS
情形 5	$\det \boldsymbol{J}$	+	+	–	+
	$\mathrm{tr}\boldsymbol{J}$	不定	–	不定	+
	稳定性	不定	ESS	鞍点	不稳定
情形 6	$\det \boldsymbol{J}$	–	+	+	–
	$\mathrm{tr}\boldsymbol{J}$	不定	–	+	不定
	稳定性	鞍点	ESS	不稳定	鞍点
情形 7	$\det \boldsymbol{J}$	+	–	+	–
	$\mathrm{tr}\boldsymbol{J}$	+	不定	–	不定
	稳定性	不稳定	鞍点	ESS	鞍点
情形 8	$\det \boldsymbol{J}$	+	–	–	+
	$\mathrm{tr}\boldsymbol{J}$	+	不定	不定	–
	稳定性	不稳定	鞍点	鞍点	ESS

$a_{11}-\gamma_{21}a_{21}<0$，$d_{21}-\lambda_{21}d_{22}<0$；④ $d_{11}-\lambda_{21}d_{12}>0$，$a_{11}-\gamma_{21}a_{21}>0$，$d_{21}-\lambda_{21}d_{22}<0$；⑤ $d_{11}-\lambda_{21}d_{12}<0$，$a_{11}-\gamma_{21}a_{21}<0$，$d_{21}-\lambda_{21}d_{22}>0$；⑥ $d_{11}-\lambda_{21}d_{12}<0$，$a_{11}-\gamma_{21}a_{21}>0$，$d_{21}-\lambda_{21}d_{22}>0$；⑦ $d_{11}-\lambda_{21}d_{12}>0$，$a_{11}-\gamma_{21}a_{21}<0$，$d_{21}-\lambda_{21}d_{22}>0$；⑧ $d_{11}-\lambda_{21}d_{12}>0$，$a_{11}-\gamma_{21}a_{21}>0$，$d_{21}-\lambda_{21}d_{22}>0$。具体判别过程依据如表 4 所示。

4) 当 $d_{11}-d_{21}-\lambda_{21}d_{12}+\lambda_{21}d_{22}\neq 0$，$a_{11}-a_{12}-\gamma_{21}a_{21}+\gamma_{21}a_{22}\neq 0$ 时，攻防博弈系统（式(21)）具有 5 个平衡点：$A(0,0)$，$B(0,1)$，$C(1,0)$，$D(1,1)$，$E(q^*,p^*)$。其中，$q^*=\dfrac{-a_{12}+\gamma_{21}a_{22}}{a_{11}-a_{12}-\gamma_{21}a_{21}+\gamma_{21}a_{22}}$，$p^*=\dfrac{-d_{21}+\lambda_{21}d_{22}}{d_{11}-d_{21}-\lambda_{21}d_{12}+\lambda_{21}d_{22}}$。

由于平衡点 $E(q^*,p^*)$ 的值不确定，无法采用雅可比矩阵的局部稳定分析法对其进行稳定性分析，因此，采用复制动态演化图对其进行博弈演化分析，下面，针对 q^*和p^* 取值的不同进行分类讨论。

情形 1 当满足条件 $0<q^*<1$，$0<p^*<1$ 时，攻防演化复制动态关系如图 3 所示，攻防双方均处于攻防循环的不良状态。在实际网络攻防过程中，攻防对抗过程会随着时间推移而不断升级，因此，该攻防循环过程很好地解释了现实攻防演化现象。

情形 2 当满足条件 $0<q^*<1$，$p^*<0$ 时，攻防演化复制动态关系如图 4 所示。该复制动态系统的演化稳定点为 $C(1,0)$，该点是攻防复制动态中唯一收敛和具有抗扰动的稳定状态。此时，（投资防御，不实施攻击）为攻防演化稳定策略，投资防御为防御方最优安全防御策略。

表 4　攻防博弈演化稳定判别依据（$d_{11}-d_{21}-\lambda_{21}d_{12}+\lambda_{21}d_{22}\neq 0$，$a_{11}-a_{12}-\gamma_{21}a_{21}+\gamma_{21}a_{22}=0$）

情形	判别依据	$A(0,0)$	$B(0,1)$	$C(1,0)$	$D(1,1)$
情形 1	det $\boldsymbol{J}$	+	–	–	+
	tr$\boldsymbol{J}$	–	不定	不定	+
	稳定性	ESS	鞍点	鞍点	不稳定
情形 2	det $\boldsymbol{J}$	–	+	+	–
	tr$\boldsymbol{J}$	不定	–	+	不定
	稳定性	鞍点	ESS	不稳定	鞍点
情形 3	det $\boldsymbol{J}$	+	+	–	–
	tr$\boldsymbol{J}$	–	+	不定	不定
	稳定性	ESS	不稳定	鞍点	鞍点
情形 4	det $\boldsymbol{J}$	–	–	+	+
	tr$\boldsymbol{J}$	不定	不定	+	–
	稳定性	鞍点	鞍点	不稳定	ESS
情形 5	det $\boldsymbol{J}$	–	–	+	+
	tr$\boldsymbol{J}$	不定	不定	–	+
	稳定性	鞍点	鞍点	ESS	不稳定
情形 6	det $\boldsymbol{J}$	+	+	–	–
	tr$\boldsymbol{J}$	+	–	不定	不定
	稳定性	不稳定	ESS	鞍点	鞍点
情形 7	det $\boldsymbol{J}$	–	+	+	–
	tr$\boldsymbol{J}$	不定	+	–	不定
	稳定性	鞍点	不稳定	ESS	鞍点
情形 8	det $\boldsymbol{J}$	+	–	–	+
	tr$\boldsymbol{J}$	+	不定	不定	–
	稳定性	不稳定	鞍点	鞍点	ESS

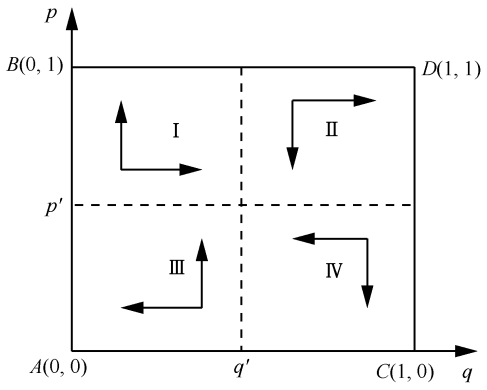

图 3　当 $0<q^*<1$，$0<p^*<1$ 时，攻防演化复制动态关系

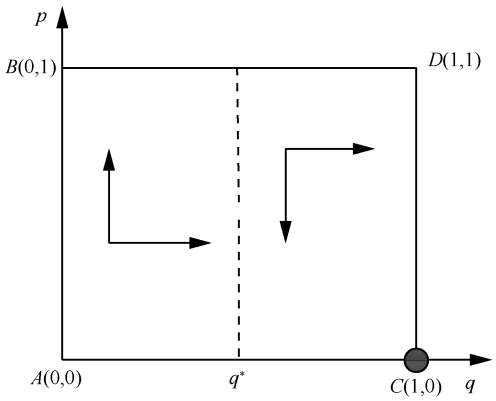

图 4　当 $0<q^*<1$，$p^*<0$ 时，攻防演化复制动态关系

同理，通过分析可以得出其他几种情形的演化关系，具体如图 5~图 11 所示。

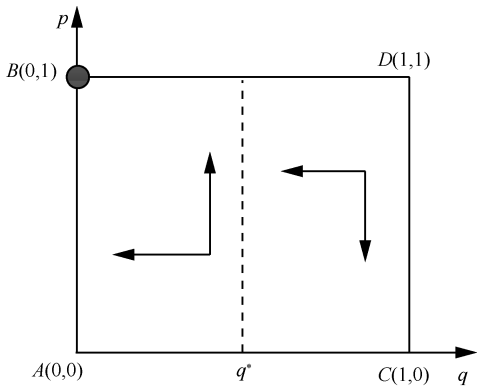

图 5　当 $0<q^*<1$，$p^*>1$ 时，不投资防御为防御方最优防御策略

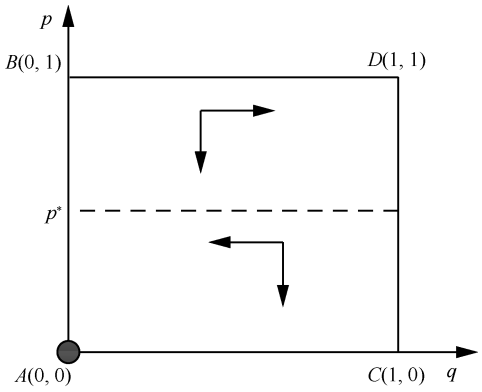

图 6　当 $q^*<0$，$0<p^*<1$ 时，不投资防御为防御方最优防御策略

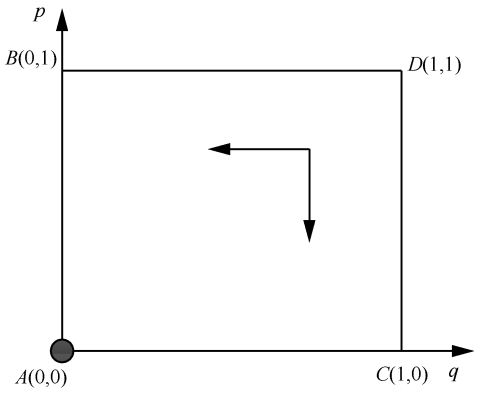

图 7　当 $q^*<0$，$p^*<0$ 时，投资防御为防御方最优防御策略

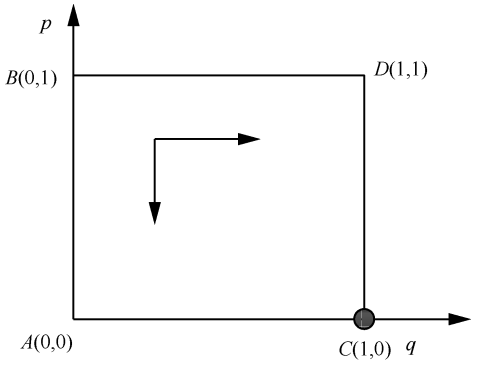

图 8　当 $q^*<0$，$p^*>1$ 时，不投资防御为防御方最优防御策略

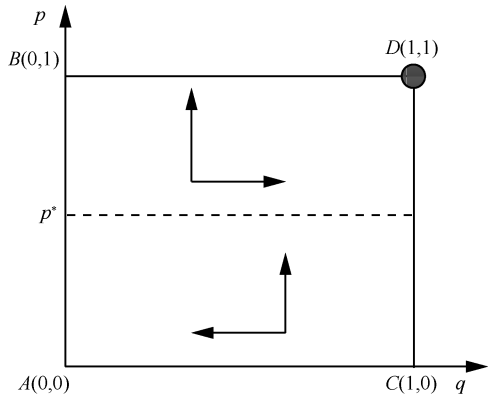

图 9　当 $q^*>1$，$0<p^*<1$ 时，投资防御为防御方最优防御策略

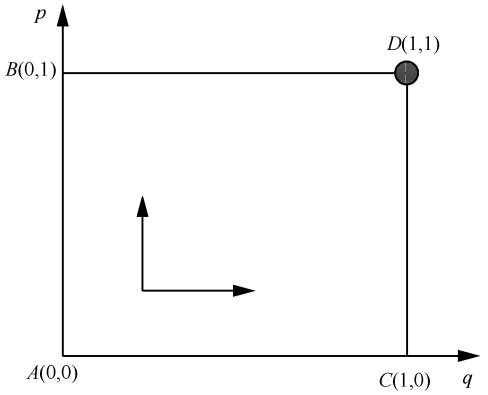

图 10　当 $q^*>1$，$p^*<0$ 时，投资防御为防御方最优防御策略

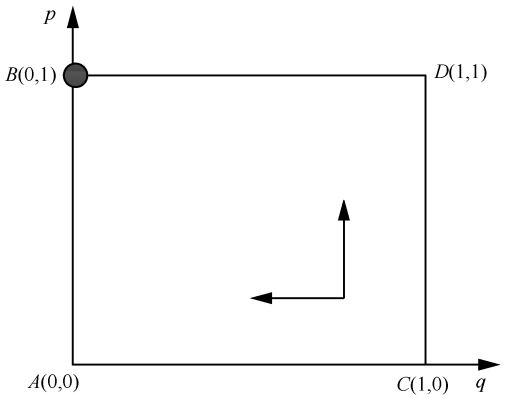

图 11　当 $q^*>1$，$p^*>1$ 时，不投资防御为防御方最优防御策略

综上可知，当攻防收益矩阵满足条件 1)~条件 3) 3 种条件时，系统式(21)具有 4 个平衡点：$A(0,0)$，$B(0,1)$，$C(1,0)$，$D(1,1)$。

博弈系统在不同条件下均存在唯一的演化稳定状态，该演化稳定状态的形成与激励系数 λ_{ij} 和 γ_{ij} 有关，且属于以上 4 个平衡点中的一个。当攻防收益矩阵满足条件 4)时，系统式(21)存在 5 个平衡点：$A(0,0)$，$B(0,1)$，$C(1,0)$，$D(1,1)$，$E(q^*,p^*)$。当且仅当满足条件 $0<q^*<1$，$0<p^*<1$ 时，博弈系

统式(21)会形成恶性循环，此时不存在最终的演化稳定状态；除此之外，系统在不同条件下均存在一个相应的演化稳定状态。

3.4　模型和方法对比

将本文模型与方法同其他文献方法进行比较，可以得到比较结果如表 5 所示。网络攻防主要由人来控制，由于实现中人的有限理性限制，以决策者完全理性为前提的传统博弈理论与网络攻防实际不符。如文献[13,14]中的模型方法是以传统博弈理论为基础，完全理性条件降低了模型和方法的现实可行性。演化博弈建立在决策者有限理性的条件下，采用复制学习的思想更新个体策略，具有过程动态演化的特点，增强了模型和方法的现实基础。如文献[18,19]均是演化博弈模型，采用传统复制动态学习机制，摆脱了行为者完全理性的限制，但其模型和方法并未考虑同类（同一群体）策略之间的相互影响。在实际攻防过程中，不仅攻防双方策略之间存在依存性，防御策略之间以及攻击策略之间均存在一定的依赖关系，而这种同类策略之间的相互作用会对博弈演化过程中的复制动态速率产生较大影响，从而降低了模型和方法的准确性。

本文以决策者非完全理性的传统演化博弈理论为基础，综合考虑并定量描述同类策略之间的影响，通过引入激励系数，用于描述攻防双方同一群体策略之间的相互作用，改进传统复制动态方程，构建基于改进复制动态的网络攻防演化博弈模型，并对模型进行了分析与求解，提高了模型和方法的准确性。相比表 5 中其他文献的方法，本文方法对网络防御策略选取具有更强的针对性，采用该方法选取的最优防御策略更准确，对网络防御具有更好的指导意义。

4　实验仿真与分析

4.1　实验环境描述

基于本文提出的基于改进复制动态网络攻防演化博弈模型，通过部署一个简单的网络信息系统进行仿真实验，用于验证本文模型和方法的有效性。该网络信息系统的拓扑环境如图 12 所示，主要由网络防御设备、Web 服务器、文件服务器、数据库服务器和客户终端机组成。通过防火墙将网络分为

表 5　　**模型与方法比较结果**

方法	博弈类型	行为理性	复制动态速率准确性	均衡求解	具体应用
文献[13]方法	随机博弈	完全理性	—	简单	策略选取
文献[14]方法	动态博弈	完全理性	—	一般	策略选取
文献[18]方法	演化博弈	不完全理性	低（未考虑同类策略间的影响）	一般	安全防御
文献[19]方法	演化博弈	不完全理性	低（未考虑同类策略间的影响）	简单	安全防御
本文方法	演化博弈	不完全理性	高（综合考虑并定量描述同类策略间的影响）	详细	策略选取

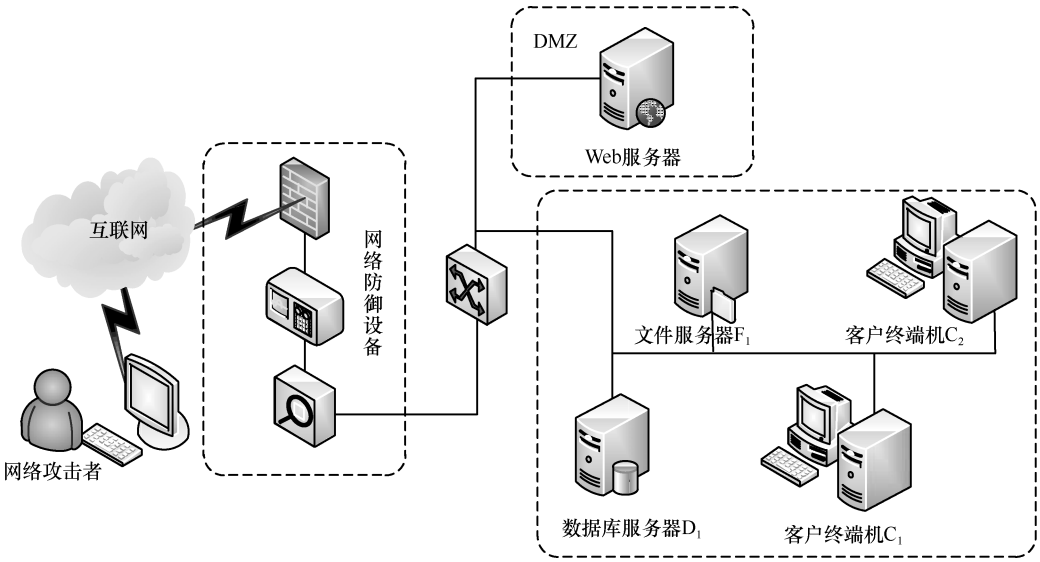

图 12　网络信息系统的拓扑环境

网络攻击者所在的外网区、DMZ 隔离区和内网安全区 3 部分。在 DMZ 区域的 Web 服务器为 Apache 服务器；内网中的数据库服务器为 Apache 服务器提供数据库服务；客户终端机可以运行邮件、FTP 和 SSH 程序。采用的访问控制规则是：非本网络的主机只能访问 Web 服务器，系统内 Web 服务器、应用服务器可以对数据库服务器进行访问。

在实验过程中，攻防策略均由多个原子攻防策略生成，即 $AS_i=\{a_1,a_2,\cdots,a_k\}$，$DS_j=\{d_1,d_2,\cdots,d_l\}$。在实验过程中，通过 Nessus 扫描实验信息系统，参考美国麻省理工学院的攻防行为数据库[28]，结合国家信息安全漏洞库（CNNVD）信息，该实验系统中所用到的原子攻击策略如表 6 所示，原子防御策略如表 7 所示。在实验中设计攻击策略为 $AS_1=\{a_1,a_2,a_5\}$ 和 $AS_2=\{a_3,a_6\}$，防御策略为 $DS_1=\{d_2,d_3,d_5,d_6\}$ 和 $DS_2=\{d_1,d_2,d_5\}$。

表 6　　原子攻击策略描述

序号	原子攻击动作名称	网络攻击策略	
		AS_1	AS_2
a_1	安装 Web 监听	√	
a_2	远程攻击	√	
a_3	盗取账户		√
a_4	SSH 攻击		
a_5	网页攻击	√	
a_6	数据库监听		√

表 7　　原子防御策略描述

序号	原子防御动作名称	网络防御策略	
		DS_1	DS_2
d_1	安装数据库补丁		√
d_2	重装监听程序	√	√
d_3	限制数据分组	√	
d_4	删除可疑账户		
d_5	重启数据服务器	√	√
d_6	主页修复	√	

4.2 应用验证与分析

针对本文提出的改进复制动态攻防演化博弈模型，通过对激励系数设置不同取值，验证同一群体中不同策略之间的依赖关系对博弈演化过程的影响，突出改进复制动态演化博弈模型的优越性。其中，激励系数越大，表示策略之间的影响度越大；否则，表示策略之间的影响度越小。

在网络攻防博弈系统中，攻防双方均存在 200 个决策者，分别设定 $a_{11}=10$，$a_{12}=10$，$a_{21}=10$，$a_{22}=10$，$d_{11}=10$，$d_{12}=10$，$d_{21}=10$，$d_{22}=10$，$\alpha_1=1$，$\beta_1=1$。在此基础上，针对激励系数的不同取值，对初始状态分别为 $(q_1,p_1)=(0.2,0.3)$ 和 $(q_1,p_1)=(0.6,0.7)$ 的状态演化趋势进行实验仿真，可以得到不同激励系数在博弈演化过程中起到的作用。

1) 当 $\lambda_{21}=1$，$\gamma_{21}=1$ 时，表示防御策略之间和攻击策略之间均不存在依赖关系。此时，改进复制动态与传统复制动态保持一致，即该演化过程属于传统复制动态的演化情形，该博弈系统的状态演化趋势如图 13 所示。当初始状态为 $(q_1,p_1)=(0.2,0.3)$ 时，策略 DS_1 在仿真 15 次时达到稳定，策略 AS_1 在仿真 30 次时达到稳定；当初始状态为 $(q_1,p_1)=(0.6,0.7)$ 时，策略 DS_1 在仿真 30 次时达到稳定，策略 AS_1 在仿真 25 次时达到稳定。

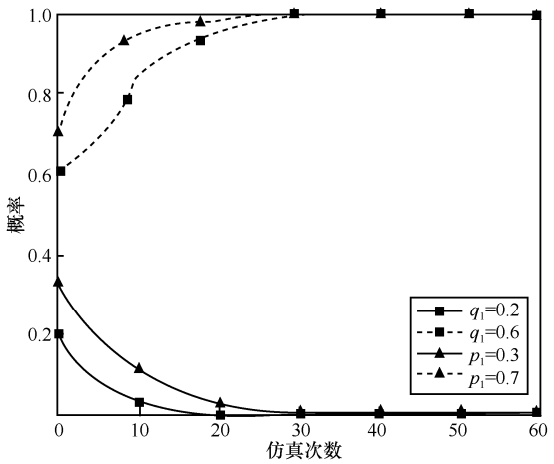

图 13　当 $\lambda_{21}=1$，$\gamma_{21}=1$ 时，不同初始状态下的攻防演化趋势

2) 当 $\lambda_{21}=0.5$，$\gamma_{21}=0.5$ 时，表示防御策略 DS_2 对 DS_1 具有促进作用，攻击策略 AS_2 对 AS_1 具有促进作用。通过仿真，该博弈系统的状态演化趋势具体如图 14 所示。当初始状态为 $(q_1,p_1)=(0.2,0.3)$ 时，策略 DS_1 在仿真 4 次时达到稳定，策略 AS_1 在仿真 10 次时达到稳定；当初始状态为 $(q_1,p_1)=(0.6,0.7)$ 时，策略 DS_1 在仿真 15 次时达到稳定，策略 AS_1 在仿真 10 次时达到稳定。显然，与情形 1)相比，当 $\lambda_{21}=0.5$，$\gamma_{21}=0.5$ 时，同一群体中的不同策略存在正激励作用，加快了博弈收敛的速度。

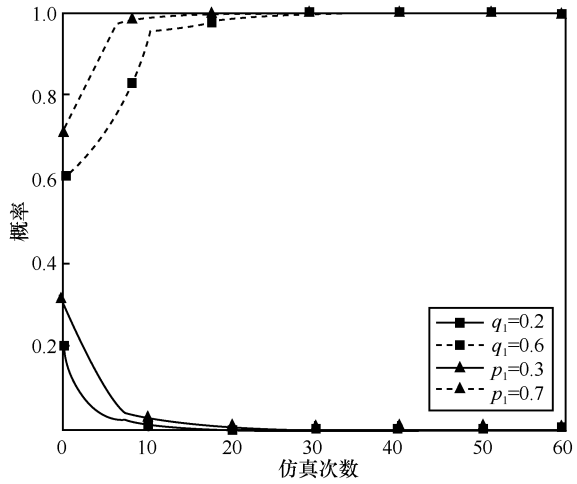

图 14　当 $\lambda_{21}=0.5$，$\gamma_{21}=0.5$ 时，不同初始状态的攻防演化趋势

3) 当 $\lambda_{21}=1.5$，$\gamma_{21}=1.5$ 时，表示防御策略 DS_2 对 DS_1 具有抑制作用，攻击策略 AS_2 对 AS_1 具有抑制作用。通过仿真，该博弈系统的状态演化趋势具体如图 15 所示。当初始状态为 $(q_1,p_1)=(0.2,0.3)$ 时，策略 DS_1 在仿真 28 次时达到稳定，策略 AS_1 在仿真 50 次时达到稳定；当初始状态为 $(q_1,p_1)=(0.6,0.7)$ 时，策略 DS_1 在仿真 50 次时达到稳定，策略 AS_1 在仿真 40 次时达到稳定。显然，与情形 1)相比，当 $\lambda_{21}=1.5$，$\gamma_{21}=1.5$ 时，同一群体中的不同策略存在抑制作用，降低了博弈收敛的速度。

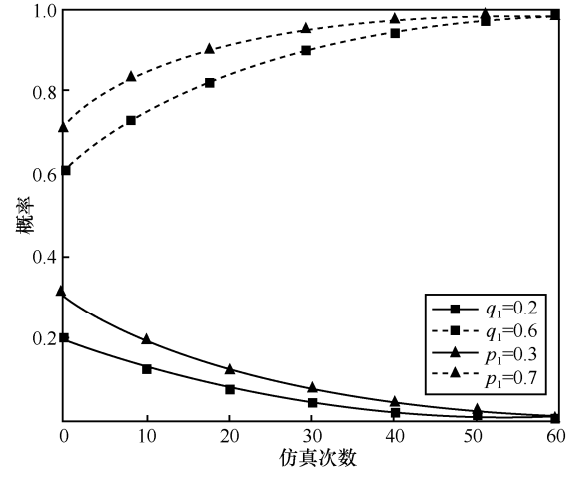

图 15　当 $\lambda_{21}=1.5$，$\gamma_{21}=1.5$ 时，不同初始状态的攻防演化趋势

4) 当 $\lambda_{21}=1.5$，$\gamma_{21}=0.5$ 时，表示防御策略 DS_2 对 DS_1 具有抑制作用，攻击策略 AS_2 对 AS_1 具有促进作用。通过仿真，该博弈系统的状态演化趋势如图 16 所示。当初始状态为 $(q_1,p_1)=(0.2,0.3)$ 时，策略 DS_1 在仿真 28 次时达到稳定，策略 AS_1 在仿真 12 次时达到稳定；当初始状态为 $(q_1,p_1)=(0.6,0.7)$ 时，策略 DS_1 在仿真 55 次时达到稳定，策略 AS_1 在仿真 10 次时达到稳定。显然，与情形 1)相比，当 $\lambda_{21}=1.5$ 时，防御方策略 DS_2 对 DS_1 具有抑制作用，降低了博弈收敛的速度；当 $\gamma_{21}=0.5$ 时，攻击策略 AS_2 对 AS_1 具有促进作用，加快了博弈收敛的速度。

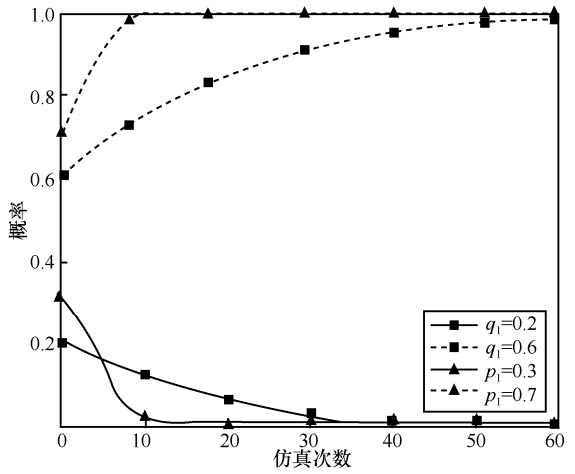

图 16　当 $\lambda_{21}=1.5$，$\gamma_{21}=0.5$ 时，不同初始状态的攻防演化趋势

由以上仿真结果可知，在给定各博弈参数取值的条件下，博弈系统在经过多次演化后，最终将收敛于某个稳定状态，得到相应的最优防御策略。通过观察对比发现，复制动态中激励系数的不同取值，对博弈系统演化的收敛速度具有不同的影响。由此可知，同一群体中的策略之间既存在促进作用，也存在抑制作用，实验仿真结果与本文所提模型中的理论分析保持一致，说明本文对传统复制动态方程的改进提高了模型和方法的准确性，可以用于指导网络安全防御决策。

5　结束语

本文针对同一群体中存在策略依存关系的问题，通过改进复制动态方程对网络攻防博弈过程中最优防御策略选取问题进行了研究。主要工作如下。

1) 从网络攻防实际出发，基于非合作演化博弈理论，通过引入激励系数，改进传统复制动态方程，构建基于改进复制动态的网络攻防演化博弈模型。

2) 利用改进复制动态方程进行均衡求解，采用雅可比矩阵的局部稳定分析法对所求均衡点进行稳定性分析，得到了不同条件下的最优防御策略。

3) 在给定各博弈参数取值的条件下，通过数值仿真，验证了激励系数在攻防博弈系统中对策略选取的激励作用。

研究结果表明，同一群体之间的策略存在相互依赖性，对博弈演化的收敛速度具有重要影响，这种依赖关系既包含促进作用，又包含抑制作用。研究成果拓展了演化博弈理论，对于在有限理性条件的动态攻防中实施网络防御决策具有指导意义，能够为开展网络空间攻防对抗研究提供模型和方法支持。但也还存在一些不足，如攻防策略集的确定以及激励系数的量化，这将成为下一步研究的重点。

参考文献：

[1] ROY S, ELLIS C, SHIVA S, et al. A survey of game theory as applied to network security[C]//43rd Hawaii International Conference on System Sciences, 2010: 1-10.

[2] LIANG X, XIAO Y. Game theory for network security[J]. IEEE Communications Surveys & Tutorials, 2013, 15(1): 472-486.

[3] VIDUTO V, HUANG W, MAPLE C. Toward optimal multi-objective models of network security: survey[C]//2011 17th International Conference on Automation & Computing. 2011: 6-11.

[4] GORDON L, LOEB M, LUCYSHYN W, et al. 2016 CSI/FBI computer crime and security survey[C]// 2016 Computer Security Institute. 2016: 48-64.

[5] SERRA E, JAJODIA S, PUGLIESE A, et al. Pareto-optimal adversarial defense of enterprise systems[J]. ACM Transaction on Information & System Security, 2015, 17(3): 11.

[6] RICHARD L, JOSHUA W. Analysis and results of the DARPA off-line intrusion detection evaluation[C]//17th International Workshop on Recent Advances in Intrusion Detection. 2015:162-182.

[7] EISENSTADT E, MOSHAIOV A, AVIGAD G. The competing travelling salespersons problem under multi-criteria[C]//2016 14th International Conference on Parallel Problem Solving from Nature. 2016: 463-472.

[8] GORDON L, LOEB M. Budgeting process for information security expenditures[J]. Communications of the ACM, 2016, 51(8): 395-406.

[9] WHITE J, PARK J S, KAMHOUA C A, et al. Game theoretic attack analysis in online social network (OSN) services[C]//2016 International Conference on Social Networks Technology. 2016: 1012-1019.

[10] OCEVICIC H, NENADIC K, SOLIC K. Game theory: active defense model and method[J]. IEEE Information and Network Security, 2016, 51(8):395-406.

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

[12] 林旺群, 王慧, 刘家红. 基于非合作动态博弈的网络安全主动防御技术研究[J]. 计算机研究与发展, 2013, 48(2): 306-316.
LIN W Q, WANG H, LIU J H. Research on active defense technology in network security based on non-cooperative dynamic game theory[J]. Journal of Computer Research and Development, 2013, 48(2): 306-316.

[13] 姜伟, 方滨兴, 田志宏. 基于攻防随机博弈模型的防御策略选取研究[J]. 计算机研究与发展, 2013, 47(10): 1714-1723.
JIANG W, FANG B X, TIAN Z H. Research on defense strategies selection based on attack-defense stochastic game model[J]. Journal of Computer Research and Development, 2013, 47(10): 1714-1723.

[14] 张恒巍, 余定坤, 韩继红, 等. 基于攻防信号博弈模型的防御策略选取方法[J]. 通信学报, 2016, 37(5): 39-49.
ZHANG H W, YU D K, HAN J H, et al. Defense policies selection method based on attack-defense signaling game model[J]. Journal on Communications, 2016, 37(5): 39-49.

[15] 王长春, 程晓航, 朱永文, 等. 计算机网络对抗行动策略的 Markov 博弈模型[J]. 系统工程理论与实践, 2014, 34(9): 2402-2410.
WANG C C, CHENG X H, ZHU Y W, et al. A Markov game model of computer network operation[J]. Systems Engineering -Theory & Practice, 2014, 34(9):2402-2410.

[16] MARTIN A N. Breaking the symmetry between interaction and replacement in evolutionary dynamics on graphs[J]. Physical Review Letters, 2016 (23):24-33.

[17] LI P, DUAN H B. Robustness of cooperation on scale-free networks in the evolutionary prisoner's dilemma game[J]. A Letters Journal Exploring the Frontiers of Physics, 2014 (105):12-19.

[18] 孙薇. 基于演化博弈论的信息安全攻防问题研究[J]. 情报科学, 2015 (9): 1408-1412.
SUN W. Research on attack and deference in information security based on evolutionary game[J]. Information Science, 2015 (9): 1408-1412.

[19] 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 J M, SONG B, HUANG Q F. Evolution game model of offense-defense for network security based on system dynamics[J]. Journal on Communications, 2014, 35(1): 54-61.

[20] 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 J M, ZHANG H W, WANG J D, et al. Defense strategies selection based on attack-defense evolutionary game model[J]. Journal on Communications, 2017, 38(1): 168-176.

[21] SHEN S G, HUANG L J, FAN E, et al. Trust dynamics in WSN: an evolutionary game-theoretic approach[J]. Journal of Sensors, 2016, 32(4): 34-43.

[22] LIU F M, DING Y S. Dynamics analysis of evolutionary game-based trust computing for P2P networks[J]. Application Research of Computers, 2016, 33(8): 2460-2463.

[23] FUDENBERG D, LEVINE D. Learning in games[J]. European Economic Review, 1998, 42(3-5): 631-639.

[24] GILBOA I, MATSUI A. Social stability and equilibrium[J]. Econometrica, 1991, 59(3):859-867.

[25] DREW F, JEAN T. Game theory[M]. Boston: Massachusettes Institute of Technology Press, 2012.

[26] BERGER U, HOFBAUER J. Irrational behavior in the Brown-von Neumann-Nash dynamics[J]. Games and Economic Behavior, 2006, 56(1): 1-6.

[27] SMITH M J. Stability of a dynamic model of traffic assignment-An application of a method of Lyapunov[J]. Transportation Science, 1984, 18(3):245-252.

[28] GUO H, WANG X W, CHENG H, et al. A routing defense mechanism using evolutionary game theory for delay tolerant networks[J]. Applied Soft Computing, 2016(38):469-476.

[29] TAYLOR P D, JONKER L B. Evolutionary stable strategies and game dynamics[J]. Mathematical Biosciences, 1978, 40(1/2):145-156.

[30] LEE W K, FAN W, MILLER M, et al. Toward cost-sensitive modeling for intrusion detection and response[J]. Journal of Computer Security, 2002, 10(1-2): 5-22.

[31] BORKOVSKY R N, DORASZELSKI U, KRYUKOV Y. A user' s guide to solving dynamic stochastic games using the homotopy method[J]. Operation Research, 2015, 58(4): 1116-1132.

[作者简介]

黄健明（1992-），男，湖南张家界人，信息工程大学硕士生，主要研究方向为网络安全主动防御。

张恒巍（1978-），男，河南洛阳人，博士，信息工程大学副教授，主要研究方向为网络安全与攻防对抗、信息安全风险评估。