doi:10.11959/j.issn.1000-436x.2017019

基于攻防演化博弈模型的防御策略选取方法

黄健明[1,2]，张恒巍[1,2]，王晋东[1,2]，黄世锐[1,2]
（1. 信息工程大学，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：当前运用博弈理论的网络安全研究方法大多采用完全理性假设，与实际情况并不相符。从网络攻防对抗的有限理性约束出发，基于非合作演化博弈理论，构建攻防演化博弈模型，提出演化稳定均衡的求解方法。在分析演化稳定策略的基础上，设计了最优防御策略选取算法。通过仿真实验验证了所提模型和方法的有效性，并且分析、总结了有限理性限制下攻防行为的演化规律。

关键词：网络攻防；有限理性；演化博弈；演化稳定策略；最优防御策略
中图分类号：TP390 **文献标识码**：A

Defense strategies selection based on attack-defense evolutionary game model

HUANG Jian-ming[1,2], ZHANG Heng-wei[1,2], WANG Jin-dong[1,2], HUANG Shi-rui[1,2]
(1. Information Engineering University, Zhengzhou 450001, China;
(2. State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China)

Abstract: Due to that the current network security researches based on game theory mostly use the completely rationality assumption, which is not consistent with the facts. Under the bounded rationality constraint of network attack-defense, attack-defense evolutionary game model and a method to solve evolutionary stable equilibrium based on the non-cooperative evolutionary game theory was proposed. The optimal defense strategy selection algorithm was designed based on the analysis of the evolutionary stable strategy. The effectiveness of the model and method proposed is verified by simulation results, through which some evolution conclusions of offensive behavior on the premise of limited rationality were drawn.

Key words: network attack-defense, bounded rationality, evolutionary game, evolutionary stable strategy, optimal defense strategy

1 引言

随着社会信息化程度的不断加强，网络规模日趋复杂，网络安全问题日益突出，亟需能够对网络攻防行为进行分析和预测，进而实施主动安全防御的新技术。网络安全状态在本质上由攻防双方的对抗行为及其结果决定，由于网络攻防对抗中所具有的目标对立性、策略依存性和关系非合作性正是博弈论的基本特征[1]，因此，博弈论在网络安全领域的研究和应用日渐兴起[2]。但是，目前的研究大都基于个体完全理性的假设前提，而这样的假设与实际情况并不相符。基于现实社会中人的有限理性约束，网络攻防双方的行为实际上不可能是一种完全理性的行为，而是一种有限理性行为。忽视有限理性的限制，对网络攻防行为的建模和分析将会出现与实际情况的偏差，削弱所得到的安全防御策略选取方法的准确性和指导价值。演化博弈具备分析有限理性攻防对抗行为的能力，因此，本文基于不完全信息条件，构建攻防演化博弈模

收稿日期：2016-06-03；**修回日期**：2016-09-10
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)

型，研究最优防御策略选取问题。

基于博弈论的网络安全研究已经成为近几年的一个热点，学者们将博弈论与网络安全相结合，构建了各种网络安全博弈模型，用于解决不同领域的问题[3]，但大多数的模型都是建立在完全理性的基础上。文献[4]基于博弈双方的对立以及双方策略选取的相互依存性，将博弈论应用于网络安全攻防对抗问题。文献[5]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。文献[6]建立重复的多阶段博弈模型，研究无线传感器网络中的安全防御问题。文献[7]提出了基于攻防信号博弈模型的防御策略选取方法。文献[8]提出了基于博弈论对信息安全技术进行评价的模型，侧重于对信息安全优化配置的研究。文献[9]提出了一种基于 Markov 博弈的网络安全态势感知方法。但是，上述文献均采用了完全理性假设，由于在现实网络攻防中很难满足，假设的局限性降低了研究成果的价值和实用性。

演化博弈以有限理性博弈方作为博弈分析的基础，采用不对称信息条件，基于生物动态进化的思想，通过学习机制刻画攻防双方，不断改进行为策略的内在驱动，符合网络攻防对抗动态演化的现实，能够有效增强博弈模型分析网络攻防行为的准确性和可信度。由于演化博弈模型在信息安全领域的应用起步较晚，目前研究成果较少。文献[10]提出基于演化博弈的网络性能最优控制方法，可以帮助网络代理根据策略信息和策略收益改变自身行为，达到整体网络性能最优的目的，但是未设计求解演化博弈均衡的方法。文献[11]基于演化博弈模型研究了攻防双方的复制动态及演化稳定策略，但是模型只对攻防双方拥有 2 种策略的简单情况进行了分析，模型的扩展性和适用范围有限，对安全防御的指导作用不强。文献[12]建立了基于系统动力学的攻防演化博弈模型，通过博弈模型和系统动力学方法对攻防双方的策略选取机制进行了分析，但是博弈模型比较简单，同时未给出具体的策略选取方法，难以指导安全防御决策。

针对网络攻防对抗中的安全防御策略选取问题，本文从现实中攻防双方的有限理性出发，构建攻防演化博弈模型，对攻防行为的对抗和演化趋势进行分析，在此基础上提出演化稳定策略求解方法，实现最优防御策略选取，并分析了不同情况下形成演化稳定均衡的规律。

2　网络攻防演化博弈模型及防御策略选取

在网络攻防中，不同的攻击者和防御者具有不同的安全知识和技能水平，因此，他们会形成不同的决策机制。由于博弈过程中参与者获得的收益具有差异，随着时间的推移，在收益差异的牵引和学习机制的驱动下，低收益参与者不断学习收益高的参与者的策略，改进自己的行为。在上述“学习—改进”机制的推动下，攻防对抗呈现动态进化趋势，形成不断演化的动态网络安全态势。

本文在攻防双方信息不对称的条件下构建攻防演化博弈模型，通过建模和研究低收益参与者学习高收益参与者的决策，并随时间动态演化到稳定状态的过程，分析攻防双方策略选择机制的变化规律，进而实现对最优防御策略的选取。

2.1　攻防演化博弈模型

传统博弈模型建立在完全理性的基础上，而实际网络攻防属于一种有限理性行为，因而降低了模型的现实可行性。本文以演化博弈为基础，在有限理性条件下，构建网络攻防演化博弈模型。

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

1) $N=(N_D,N_A)$ 是演化博弈的参与者空间，其中，N_D 为防御方，N_A 为攻击方。

2) $S=(DS,AS)$ 是博弈策略空间，其中，$DS=\{DS_1,DS_2,\cdots DS_n\}$ 表示防御者的可选策略集，$AS=\{AS_1,AS_2,\cdots,AS_m\}$ 表示攻击者的可选策略集。

3) $P=(p,q)$ 是博弈信念集合，其中，p_i 表示攻击者选择攻击策略 AS_i 的概率，q_j 表示防御者选防御策略 DS_j 的概率。

4) $U=(U_D,U_A)$ 是收益函数集合，表示参与者的博弈收益，由所有参与者的策略共同决定。

在网络攻防对抗中，攻击方 A 和防御方 D 的决策者均有多个策略可供选择，假设攻防双方决策者的可选策略集分别为 $\{AS_1,AS_2,\cdots,AS_m\}$、$\{DS_1,DS_2,\cdots,DS_n\}$，其中，$m,n\in \boldsymbol{N}$ 且 $m,n\geqslant 2$，在博弈过程的不同阶段，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，从而使攻防策略选取形成一个动态变化过程。形成的攻防博弈树如图 1 所示，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。

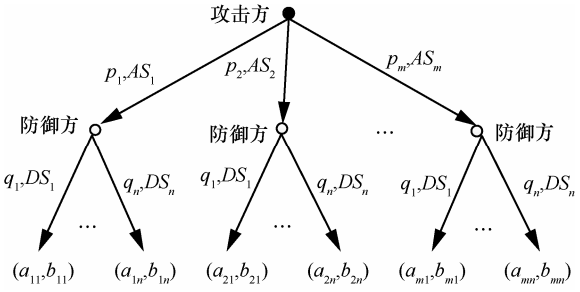


图 1 基本网络攻防博弈树

采用不同策略进行攻防对抗时，会产生相应的攻防收益值。具体数值用如下收益矩阵表示，其中，a_{ij} 和 b_{ij} 分别表示攻击者和防御者采取 AS_i、DS_j 时各自的收益。

$$\begin{Bmatrix} a_{11},b_{11} & a_{12},b_{12} & a_{13},b_{13} & \cdots & a_{1n},b_{1n} \\ a_{21},b_{21} & a_{22},b_{22} & a_{23},b_{23} & \cdots & a_{2n},b_{2n} \\ a_{31},b_{31} & a_{32},b_{32} & a_{33},b_{33} & \cdots & a_{3n},b_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m1},b_{m1} & a_{m2},b_{m2} & a_{m3},b_{m3} & \cdots & a_{mn},b_{mn} \end{Bmatrix}$$

对于防御方，策略的选取有 n 种可能，决策者以不同的概率 q_i 对各个防御策略 DS_i 进行选取，但对于整个策略集满足条件：$q_1+q_2+\cdots+q_n=1$。同样，攻击方针对自身 m 种可选策略，决策者以不同的概率 p_i 对各个攻击策略 AS_i 进行选取，对于整个策略集满足：$p_1+p_2+\cdots+p_m=1$。

基于以上条件，计算防御方不同防御策略的期望收益 U_{DS_i} 和平均收益 $\overline{U}_D$。

$$U_{DS_1}=p_1b_{11}+p_2b_{21}+p_3b_{31}+\cdots+p_mb_{m1} \quad (1)$$

$$U_{DS_2}=p_1b_{12}+p_2b_{22}+p_3b_{32}+\cdots+p_mb_{m2} \quad (2)$$

$$\vdots \qquad\qquad \vdots$$

$$U_{DS_n}=p_1b_{1n}+p_2b_{2n}+p_3b_{3n}+\cdots+p_mb_{mn} \quad (3)$$

$$\overline{U}_D=q_1U_{DS_1}+q_2U_{DS_2}+q_3U_{DS_3}+\cdots+q_nU_{DS_n} \quad (4)$$

由于防御收益较低者会学习模仿高收益者所选取的策略，针对防御策略集中的可选策略 $\{DS_1,DS_2,\cdots,DS_n\}$，选取不同策略的人数比例将随着时间的推移而发生变化，用 $q_i(t)$ 表示，其中，$q_i(t)$ 表示选择防御策略 DS_i 的人数比例，且满足 $\sum_{i=1}^{n}q_i(t)=1$。

对于某个特定防御策略 DS_i，选取该策略的人数比例是时间的函数，其动态变化速率可以用复制动态方程[13]进行表示。

$$D(q)=\frac{\mathrm{d}q_i(t)}{\mathrm{d}t}=q(U_{DS_i}-\overline{U}_D) \quad (5)$$

同理，针对攻击方策略集中的可选策略 $\{AS_1,AS_2,\cdots,AS_m\}$，选取不同策略的人数比例随时间动态变化，分别用 $p_i(t)$ 来进行表示，其中，$p_i(t)$ 满足 $\sum_{i=1}^{m}p_i(t)=1$。

针对攻击方的任意可选攻击策略 AS_i 可以得到相应的复制动态方程

$$A(p)=\frac{\mathrm{d}p_i(t)}{\mathrm{d}t}=p(U_{AS_i}-\overline{U}_A) \quad (6)$$

联立式(5)和式(6)，令 $Y=\begin{bmatrix}D(q)\\A(p)\end{bmatrix}=f(Y,t)=0$，通过求解，即可得到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。

2.2 演化稳定均衡求解

首先描述求解攻防演化博弈模型稳定均衡的过程和步骤，然后通过一个例子加以具体演示和说明。

算法过程描述如下。

1) 在攻防双方的可选策略集上建立概率推断 p_i、q_i。

2) 计算攻击方的复制动态方程

利用 p_i 及不同策略收益值，通过计算攻击方不同攻击策略的期望收益和平均收益。针对不同的攻击策略，通过计算

$$U_{AS_i}=\sum_{j=1}^{n}q_ja_{ij}$$

$$\overline{U}_A=\sum_{i=1}^{m}p_iU_{AS_i}$$

可进一步得到攻击方的复制动态方程为

$$A(p)=\frac{\mathrm{d}p_i(t)}{\mathrm{d}t}=p(U_{AS_i}-\overline{U}_A)$$

3) 计算防御方的复制动态方程

利用 q_i 及不同策略收益值，通过计算防御方不同防御策略的期望收益和平均收益。针对不同的防御策略，通过计算

$$U_{DS_j}=\sum_{i=1}^{m}p_ib_{ij}$$

$$\overline{U}_D = \sum_{i=1}^{n} q_i U_{DS_i}$$

可得到攻击方的复制动态方程为

$$D(q) = \frac{\mathrm{d}q_i(t)}{\mathrm{d}t} = q(U_{DS_i} - \overline{U}_D)$$

4) 计算演化稳定均衡解

联立步骤 2)和步骤 3)所得到的攻防双方的复制动态方程，建立演化复制动态方程组，$Y = \begin{bmatrix} D(q) \\ A(p) \end{bmatrix} = f(Y,t) = 0$，通过计算即可求得演化稳定均衡解。

分析上述计算过程可知，步骤 1)~步骤 3)的时间复杂度为 $O(m+n)$，步骤 4)的时间复杂度为 $O((m+n)^2)$。综上所述，求解演化稳定均衡解的时间复杂度不超过 $O((m+n)^2)$。存储空间消耗主要集中于策略收益和均衡求解中间值的存储上，其空间复杂度为 $O(nm)$。

针对上述建立的攻防演化博弈模型及算法描述，下面通过一个具体算例展示演化稳定均衡的求解方法。假定攻击方为 A，防御方为 D，$\{AS_1, AS_2\}$ 和 $\{DS_1, DS_2\}$ 分别是规范双方的策略集。攻防双方均以不同的概率对各自策略集中的策略进行选取，并产生不同的收益。其攻防博弈树如图 2 所示。

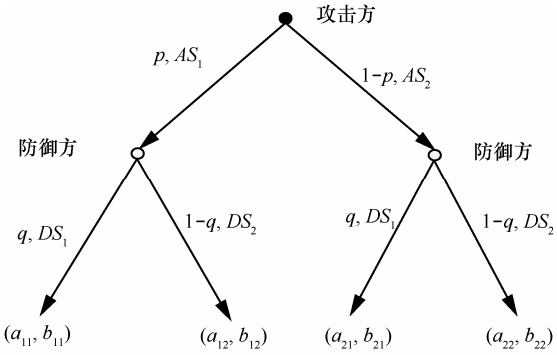


图 2　攻防博弈树

基于以上条件，针对防御方，计算防御方不同策略的期望收益以及平均收益。

$$U_{DS_1} = pb_{11} + (1-p)b_{21} \tag{7}$$

$$U_{DS_2} = pb_{12} + (1-p)b_{22} \tag{8}$$

$$\begin{aligned}\overline{U}_D &= qU_{DS_1} + (1-q)U_{DS_2} \\ &= q[pb_{11} + (1-p)b_{21}] + (1-q)[pb_{12} + (1-p)b_{22}]\end{aligned} \tag{9}$$

在实际的网络攻防过程中，防御方选取不同的防御策略会产生不同的收益效果，收益较低者会学习模仿收益较高者所选取的策略，在本文模型中，防御策略集中的 2 种可选策略 $\{DS_1, DS_2\}$，选取这 2 种策略的人数比例随着时间推移而产生变化，分别用 $q(t)$ 和 $1-q(t)$ 进行表示。

对于防御策略 DS_1，选取该策略的人数比例是时间的函数，其动态变化速率可以用以下复制动态方程进行表示。

$$\begin{aligned}D(q) &= \frac{\mathrm{d}q(t)}{\mathrm{d}t} = q(U_{DS_1} - \overline{U}_D) = q\{pb_{11} + (1-p)b_{21} - \\ &\quad q[pb_{11} + (1-p)b_{21}] - (1-q)[pb_{12} + (1-p)b_{22}]\} \\ &= q\{(1-q)[pb_{11} + (1-p)b_{21}] - (1-q)[pb_{12} + (1-p)b_{22}]\} \\ &= q(1-q)[p(b_{11} - b_{21} - b_{12} + b_{22}) + b_{21} - b_{22}]\end{aligned} \tag{10}$$

令 $D(q)=0$，则可以得到解：$q=0$，$q=1$，$p = \dfrac{b_{22} - b_{21}}{b_{11} - b_{21} - b_{12} + b_{22}}$。

同理，对于攻击方可以同样求解得到

$$U_{AS_1} = qa_{11} + (1-q)a_{12} \tag{11}$$

$$U_{AS_2} = qa_{21} + (1-q)a_{22} \tag{12}$$

$$\begin{aligned}\overline{U}_A &= pU_{AS_1} + (1-p)U_{AS_2} \\ &= p[qa_{11} + (1-q)a_{12}] + (1-p)[qa_{21} + (1-q)a_{22}]\end{aligned} \tag{13}$$

$$\begin{aligned}A(p) &= \frac{\mathrm{d}p(t)}{\mathrm{d}t} = p(U_{AS1} - \overline{U}_A) = p\{qa_{11} + (1-q)a_{12} - \\ &\quad p[qa_{11} + (1-q)a_{12}] + (1-p)[qa_{21} + (1-q)a_{22}]\} \\ &= p\{(1-p)[qa_{11} + (1-q)a_{21}] - (1-p)[qa_{12} + (1-q)a_{22}]\} \\ &= p(1-p)[q(a_{11} - a_{21} - a_{12} + a_{22}) + a_{21} - a_{22}]\end{aligned} \tag{14}$$

令 $A(p)=0$，则可以求解：$p=0$，$p=1$，$q = \dfrac{a_{22} - a_{21}}{a_{11} - a_{21} - a_{12} + a_{22}}$。

将攻防双方的策略选取复制动态方程相结合，构建攻防博弈演化方程组，对模型进行稳定性分析。令 $Y = \begin{bmatrix} D(q) \\ A(p) \end{bmatrix} = f(Y,t) = 0$，可以求出该博弈模型的平衡状态。最终求解为：$Y_1 = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$，$Y_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$，$Y_3 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$，$Y_4 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$，$Y_5 = \begin{bmatrix} \dfrac{a_{22} - a_{21}}{a_{11} - a_{21} - a_{12} + a_{22}} \\ \dfrac{b_{22} - b_{21}}{b_{11} - b_{21} - b_{12} + b_{22}} \end{bmatrix}$。其中，$Y_1 = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$ 表示攻击方选取纯策略 AS_2，防御方选取纯

策略 DS_2；$Y_2=\begin{bmatrix}0\\1\end{bmatrix}$ 表示攻击方选取纯策略 AS_1，防御方选取纯策略 DS_2；$Y_3=\begin{bmatrix}1\\0\end{bmatrix}$ 表示攻击方选取纯策略 AS_2，防御方选取纯策略 DS_1；$Y_4=\begin{bmatrix}1\\1\end{bmatrix}$ 表示攻击方选取纯策略 AS_1，防御方选取纯策略 DS_1；$Y_5=\begin{bmatrix}\dfrac{a_{22}-a_{21}}{a_{11}-a_{21}-a_{12}+a_{22}}\\ \dfrac{b_{22}-b_{21}}{b_{11}-b_{21}-b_{12}+b_{22}}\end{bmatrix}$ 表示攻击方以混合概率组合 $(\dfrac{b_{22}-b_{21}}{b_{11}-b_{21}-b_{12}+b_{22}},1-\dfrac{b_{22}-b_{21}}{b_{11}-b_{21}-b_{12}+b_{22}})$ 选取策略 $\{AS_1,AS_2\}$，防御方以混合概率组合 $(\dfrac{a_{22}-a_{21}}{a_{11}-a_{21}-a_{12}+a_{22}},1-\dfrac{a_{22}-a_{21}}{a_{11}-a_{21}-a_{12}+a_{22}})$ 选取策略 $\{DS_1,DS_2\}$。根据演化稳定均衡理论[14]可知，Y_1、Y_2、Y_3、Y_4 为鞍点，Y_5 为中心点，因此，本文系统存在演化稳定均衡。通过对博弈结果的分析可以得到演化稳定状态，并能够对策略选取机制的未来变化进行预测和评估，形成完整的安全防御策略选取模式，对防御决策提供指导。

2.3 演化稳定策略分析

演化稳定策略（ESS, evolutionary stable strategy）[15]作为一个能够抵抗侵犯的策略，是演化博弈中具有真正稳定性和较强预测能力的均衡策略。针对网络攻防演化博弈模型中双方各自存在的复制动态，以防御方为例，对其演化稳定策略进行详细分析。

由防御方的复制动态方程式(10)可知，防御方的复制动态相位有 3 种情况，如图 3~图 5 所示。

同理，由攻击方的复制动态方程式(14)可知，攻击方的复制动态相位有 3 种情况，如图 6~图 8 所示。

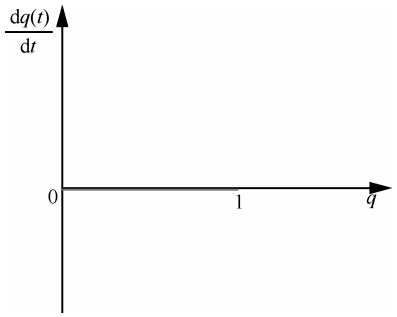


图 3 当 $p=\dfrac{b_{22}-b_{21}}{b_{11}-b_{21}-b_{12}+b_{22}}$ 时的相位

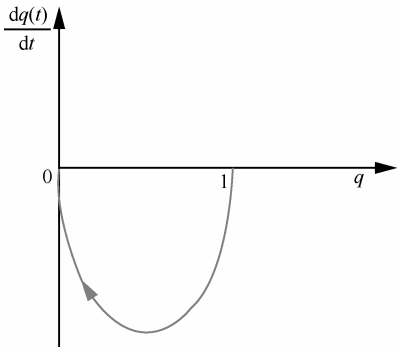


图 4 当 $p<\dfrac{b_{22}-b_{21}}{b_{11}-b_{21}-b_{12}+b_{22}}$ 时的相位

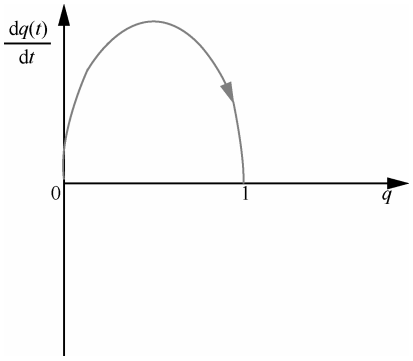


图 5 当 $p>\dfrac{b_{22}-b_{21}}{b_{11}-b_{21}-b_{12}+b_{22}}$ 时的相位

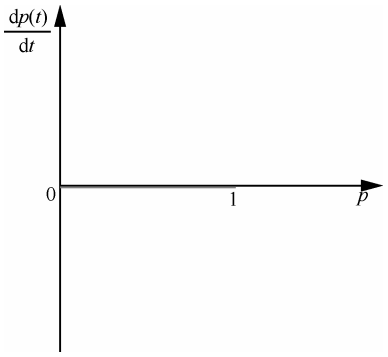


图 6 当 $q=\dfrac{a_{22}-a_{21}}{a_{11}-a_{21}-a_{12}+a_{22}}$ 时的相位

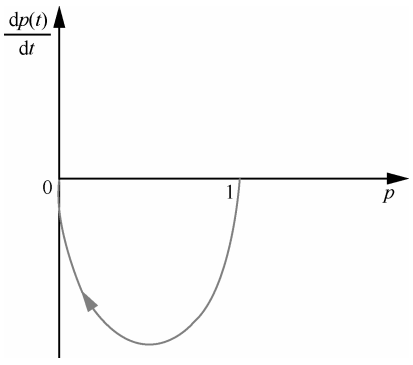


图 7 当 $q<\dfrac{a_{22}-a_{21}}{a_{11}-a_{21}-a_{12}+a_{22}}$ 时的相位

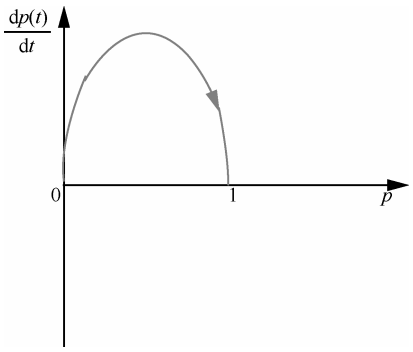


图 8　当 $q>\dfrac{a_{22}-a_{21}}{a_{11}-a_{21}-a_{12}+a_{22}}$ 时的相位

根据式(10)，并结合图 3 可知，当且仅当 $p=\dfrac{b_{22}-b_{21}}{b_{11}-b_{21}-b_{12}+b_{22}}$ 时，对于任意的防御策略选取概率 q，有 $\dfrac{\mathrm{d}q(t)}{\mathrm{d}t}=0$；但是，一旦 p 的取值发生偏移，则 $\dfrac{\mathrm{d}q(t)}{\mathrm{d}t}$ 将会剧烈变化，因此，图 3 代表的状态不具有稳定性。若 $p\neq\dfrac{b_{22}-b_{21}}{b_{11}-b_{21}-b_{12}+b_{22}}$，由图 4 和图 5 可知，$q=0$ 和 $q=1$ 是 2 个稳定状态。在这 2 个稳定状态中，当 $\dfrac{\mathrm{d}q(t)}{\mathrm{d}t}=0$ 且 $\dfrac{\mathrm{d}^2q(t)}{\mathrm{d}t^2}<0$ 时，则 q 为防御方的演化稳定策略。即复制动态曲线与水平坐标轴相交并且切线斜率为负的点就是防御方的演化稳定策略。基于此，当 $p<\dfrac{b_{22}-b_{21}}{b_{11}-b_{21}-b_{12}+b_{22}}$ 时，$q=0$ 为防御方演化稳定策略；当 $p>\dfrac{b_{22}-b_{21}}{b_{11}-b_{21}-b_{12}+b_{22}}$ 时，$q=1$ 为防御方演化稳定策略。

根据攻击方的复制动态方程式(14)，同理分析可得，当 $q=\dfrac{a_{22}-a_{21}}{a_{11}-a_{21}-a_{12}+a_{22}}$ 时，对于任意的攻击策略选取概率 p，有 $\dfrac{\mathrm{d}p(t)}{\mathrm{d}t}=0$；但是，图 6 代表的状态同样不具有稳定性；当 $q<\dfrac{a_{22}-a_{21}}{a_{11}-a_{21}-a_{12}+a_{22}}$ 时，$p=0$ 为攻击方的演化稳定策略；当 $q>\dfrac{a_{22}-a_{21}}{a_{11}-a_{21}-a_{12}+a_{22}}$ 时，$p=1$ 为攻击方演化稳定策略。

2.4　最优防御策略选取算法设计分析

获取最优网络防御策略的基本思想是，在建立网络攻防博弈树的基础上，攻防双方均有各自的可选策略集，双方以不同的概率进行策略选取，基于演化博弈理论，建立相应的复制动态方程，在计算演化稳定均衡解的基础上，选取最优防御策略。

基于上述研究，针对网络防御者，设计出一种基于演化博弈理论的最优防御策略选取算法，具体如下。

输入　网络攻防博弈树

输出　最优防御策略

1) 初始化；

2) 构建防御方的类型空间集合 $D=\{d_i,i\geqslant 1\}$；

3) 构建防御者可选策略空间集合 $DS=\{DS_j,1\leqslant j\leqslant m\}$；

4) 针对攻击方所选攻击策略，以概率 $q_i(1\leqslant i\leqslant m)$ 选取合理的防御策略 DS_i，其中，$\sum_{i=1}^{m}q_i=1$；

5) 针对攻防双方所选攻防策略对 $\{AS_i,DS_j\}$，得出其防御收益值 b_{ij}；

6) 计算各防御策略的期望收益 $U_{DS_i}=p_1b_{1i}+p_2b_{2i}+\cdots+p_nb_{ni}$，其中，$n$ 表示攻击方的策略个数；

7) 计算防御方的平均收益 $\overline{U}_D=\sum_{i=1}^{n}q_iU_{DS_i}$；

8) 建立防御复制动态方程 $D(q)=\dfrac{\mathrm{d}q(t)}{\mathrm{d}t}=q(U_{DS_i}-\overline{U}_D)$；

9) 令 $D(q)=0$，计算均衡解；

10) 输出均衡解中的安全防御策略；

该算法的时间复杂度主要集中于步骤 4)，由 2.2 节的分析可知，该算法的时间复杂度为 $O((m+n)^2)$；本算法的空间消耗主要集中于收益值和均衡求解中间结果的存储之上，其空间复杂度为 $O(nm)$。根据该算法，不仅可以获知各策略所对应的收益值，并能够通过复制动态方程，得到策略选取状态随时间的变化情况，从而实现网络演化稳定均衡的分析与预测。

通过与其他文献方法进行比较，可以得到比较结果如表 1 所示。对于传统博弈，如文献[1]和文献[3]中的模型方法是建立在参与者完全理性的假设基础之上，由于实现中参与者的非完全理性，降低了模型的现实可行性。而对于演化博弈，其参与者具有有限理性的特点，采用向他人学习的机制，随时间推移而不断演化最终达到演化均衡，与实际情况

比较吻合，增强了模型的现实基础。文献[12]和文献[13]均是演化博弈模型，但其模型求解过程过于简单，而本文给出了详细的求解过程。一个模型的通用性主要表现在该模型中的类型集合和策略集合是否很好地扩展至 n。如果模型中的集合可以扩展至 n，说明该模型的通用性较好；否则，说明该模型只能适用于特殊情况，模型通用性较差。本文模型通过对可选策略扩展至 n，使该模型具有良好的通用性，能够应用于一般的防御策略选取，而其他文献中的模型方法均未能完全将参数扩展至 n，从而降低了模型的通用性。

3 实验仿真与分析

3.1 仿真实验环境描述

为验证所提出的网络攻防演化博弈模型及相关均衡求解方法，通过部署如图 9 所示的网络信息系统进行仿真实验。该系统主要由安全防御设备、Web 服务器、应用服务器和数据库服务器组成。访问控制规则规定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。在实验中设计攻击策略为 AS_1(FTP rhost attack)和 AS_2 (oracle TNS listener) ，防御策略为 DS_1(patch SSH on FTP sever)和 DS_2(install oracle patch)。

3.2 实验分析

针对以上建立的模型，利用系统动力学进行仿真，分析演化博弈模型中最优防御策略的选取问题。由 2.2 节可知，本系统的演化稳定状态为 $Y_1=\begin{bmatrix}0\\0\end{bmatrix}$、$Y_2=\begin{bmatrix}0\\1\end{bmatrix}$、$Y_3=\begin{bmatrix}1\\0\end{bmatrix}$ 和 $Y_4=\begin{bmatrix}1\\1\end{bmatrix}$ 4 种情况。下面将针对 p 和 q 的不同初始状态，进行实验仿真。通过仿真，可以观察出 p 和 q 的演化趋势，得到最终的演化稳定状态，通过演化分析，实现对攻击策略的预测，从而选取出最优防御策略。

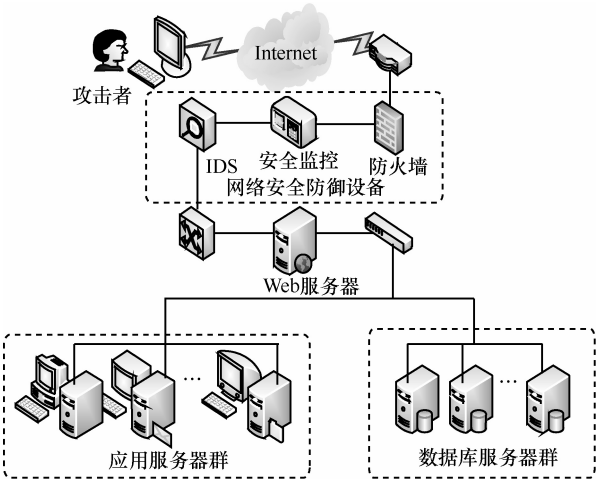


图 9 实验信息系统结构示意

1) 当初始状态为 $p=0$，$q=0$ 时，攻击方以概率 1 选取攻击策略 AS_2，防御方以概率 1 选取防御策略 DS_2，通过系统仿真，经过演化，攻防双方的策略选取将保持不变，即 DS_2 为最优防御策略。具体如图 10 所示。

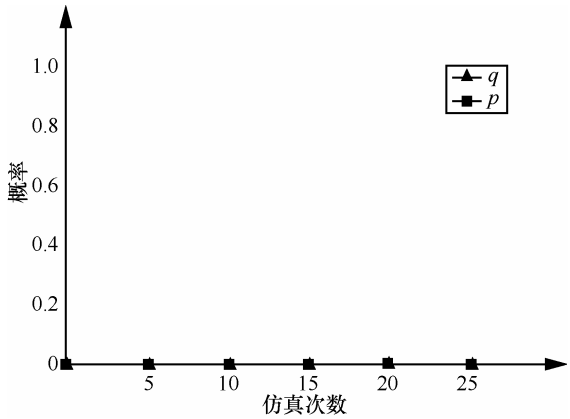


图 10 初始状态为 $p=0$，$q=0$ 时的演化曲线

2) 当初始状态为 $p=1$，$q=1$ 时，攻击方以概率

表 1 各方法结果比较

方法	博弈类型	行为理性	模型通用性	均衡求解	具体应用
文献[1]方法	随机博弈	完全理性	一般	简单	策略选取
文献[3]方法	动态博弈	完全理性	一般	详细	安全防御
文献[12]方法	演化博弈	不完全理性	差	简单	安全防御
文献[13]方法	演化博弈	不完全理性	一般	简单	群体行为分析
本文方法	演化博弈	不完全理性	较好	详细	策略选取

1 选取攻击策略 AS_1，防御方以概率 1 选取防御策略 DS_1，经过不断的演化，该系统的策略选取同样保持不变，DS_1 即为最优防御策略。具体如图 11 所示。

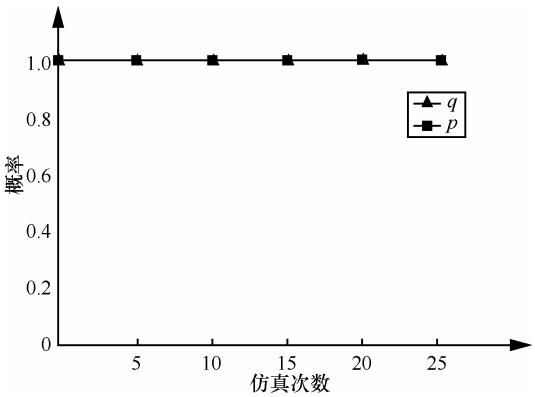


图 11　初始状态为 $p=1$，$q=1$ 时的演化曲线

3) 当初始状态为 $p=0.3$，$q=0.4$ 时，攻击方以 $\{0.3,0.7\}$ 的混合概率选取攻击策略 $\{AS_1,AS_2\}$，防御方以 $\{0.4,0.6\}$ 的混合概率对策略 $\{DS_1,DS_2\}$ 进行选取，通过演化，防御方最终以概率 0 选取策略 DS_1，以概率 1 选取策略 DS_2，达到均衡状态。则 $Y_1=\begin{bmatrix}0\\0\end{bmatrix}$ 为其中的一个演化均衡点，DS_2 为最优防御策略，如图 12 所示。

4) 当初始状态为 $p=0.6$，$q=0.4$ 时，攻击方以混合概率 $\{0.6,0.4\}$ 选取攻击策略 $\{AS_1,AS_2\}$，防御方以 $\{0.4,0.6\}$ 的混合概率对策略 $\{DS_1,DS_2\}$ 进行选取，经过不断的演化，q 的取值趋向于 0，p 的取值趋向于 1，防御方以概率 1 对策略 DS_2 进行选取。则 $Y_2=\begin{bmatrix}0\\1\end{bmatrix}$ 属于一个演化均衡点，DS_2 为最优防御策略，如图 13 所示。

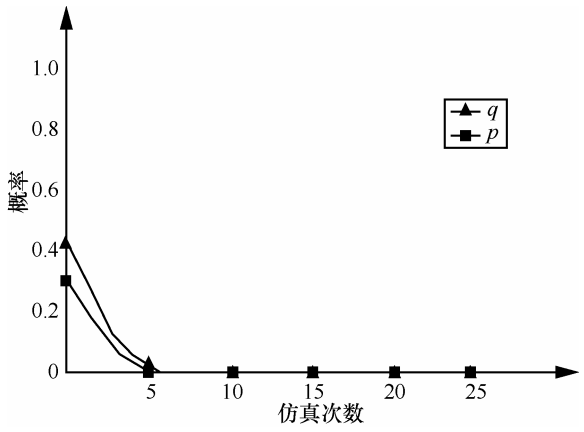


图 12　初始状态为 $p=0.3$，$q=0.4$ 时的演化曲线

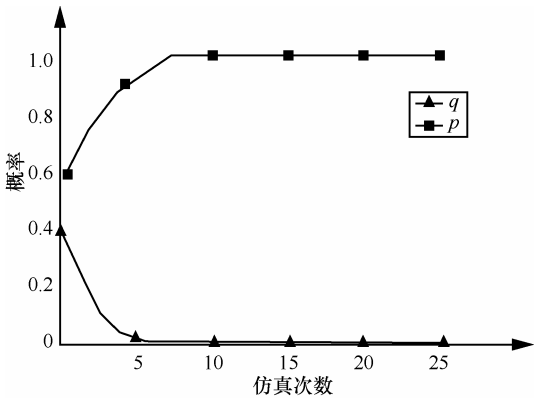


图 13　初始状态为 $p=0.6$，$q=0.4$ 时的演化曲线

5) 当初始状态为 $p=0.3$，$q=0.7$ 时，通过不断演化，攻击方以概率 1 选取攻击策略 AS_2，防御方以概率 1 对策略 DS_1 进行选取，达到稳定。则 $Y_3=\begin{bmatrix}1\\0\end{bmatrix}$ 属于该系统的一个演化稳定状态。DS_1 为最优防御策略，如图 14 所示。

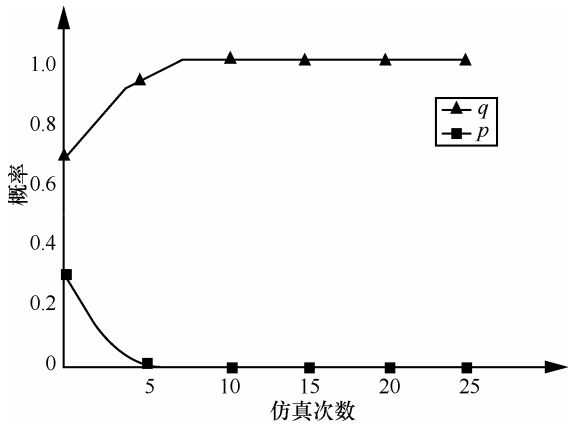


图 14　初始状态为 $p=0.3$，$q=0.7$ 时的演化曲线

6) 当初始状态为 $p=0.7$，$q=0.6$ 时，通过演化，p 和 q 的取值最终都趋向于 1，最终达到稳定。防御方以概率 1 选取防御策略 DS_1，DS_1 即为最优防御策略，如图 15 所示。

由以上仿真结果可知，给定不同的策略选取初始状态，经过演化，系统最终将会达到某个稳定状态。通过观察对比，不难发现本系统的模拟演化结果与模型中的理论分析保持一致，说明该演化博弈模型与现实系统中的演化规律相符，因此，本文中的攻防演化博弈模型具有有效性。将其应用于实际的网络攻防对抗中，通过对攻击方攻击策略的选取进行分析和预测，可以为自身最优防御策略的选取提供一定的依据。

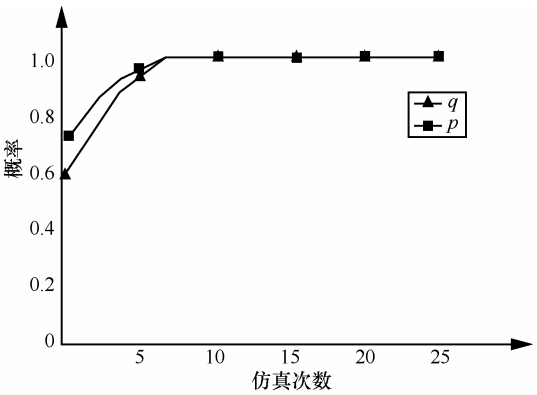


图 15　初始状态为 $p=0.7$，$q=0.6$ 时的演化曲线

4　结束语

安全防御决策问题一直是网络安全领域的研究重点和热点。本文基于攻防博弈参与者具备有限理性的假设，结合演化博弈理论与网络攻防实际，建立了攻防演化博弈模型，对双方的学习机制和决策模式的变化原因进行了研究。通过复制动态方程分析了攻防双方行为策略的变化过程以及演化稳定状态形成的机理，在此基础上，提出了演化稳定策略的求解方法，设计了最优安全防御策略选取算法。通过仿真实验对所提模型和方法的有效性进行了验证。研究成果能够为网络空间攻防对抗研究提供有效的模型方法，并为安全防御决策提供指导。

参考文献：

[1] 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.

[2] FALLAH M S. A puzzle-based defense strategy against flooding attacks using game theory[J]. Dependable and Secure Computing, 2016, 67(1): 5-19.

[3] 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.

[4] ANDERSON R. Why information security is hard: an economic perspective[C]//17th Annual Computer Security Application Conference. Washington, DC, USA: IEEE Computer Society, 2016: 39-40.

[5] BASUS S, WONG J. A taxonomy of intrusion response systems[J].International Journal of Information and Computer Security, 2015, 1(1/2): 169-184.

[6] SHEN S G, LI Y J, XU H Y. Signaling game based strategy of intrusion detection in wireless sensor networks[J]. Computers & Mathematics with Applications, 2016, 62(6): 2404-2416.

[7] 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.

[8] 朱建明. 基于博弈论的信息安全技术评价模型[J]. 计算机学报, 2015(4): 828-834.
ZHU J M. Evaluation model of information security technologies based on game theoretic[J]. Chinese Journal of Computers, 2015(4): 828-834.

[9] 张勇. 基于 Markov 博弈模型的网络安全态势感知方法[J]. 软件学报, 2016, 22(3): 495-508.
ZHANG Y. Network security situation awareness approach based on markov game model[J]. Journal of Software, 2016, 22(3): 495-508.

[10] CHENG D, HE F, QI H, et al. Modeling, analysis and control of networked evolutionary games[J]. IEEE Transactions on Automatic Control, 2015(99): 41-49.

[11] 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.

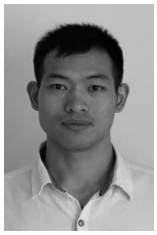
[12] 朱建明, 宋彪, 黄启发. 基于系统动力学的网络安全攻防演化博弈模型[J]. 通信学报, 2014, 35(1): 54-61.
ZHU J M, SONG B, HUANG Q F. Evolution game model of offense-defense for network security based on system dynamics[J]. Journal on Communications, 2014, 35(1): 54-61.

[13] 王元卓, 于建业, 邱雯. 网络群体行为的演化博弈模型与分析方法[J]. 计算机学报, 2015, 38(2): 282-300.
WANG Y Z, YU J Y, QIU W. Evolutionary game model and analysis methods for network group behavior[J]. Chinese Journal of Computers, 2015, 38(2): 282-300..

[14] BALKENBORG D, SCHLAG K. On the interpretation of evolutionary stable sets in symmetric and asymmetric games[D]. Mimeo: Bonn University Economics Department. 1994.

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

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，信息工程大学讲师，主要研究方向为网络安全行为分析、信息安全风险评估。

王晋东（1966-），男，山西洪桐人，信息工程大学教授，主要研究方向为网络与信息安全、云资源管理。

黄世锐（1994-），男，广东汕头人，信息工程大学硕士生，主要研究方向为网络安全预警与预测。