基于随机演化博弈模型的网络防御策略选取方法

黄健明[1],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: 针对攻防博弈系统中存在攻防策略集和系统运行环境改变等各类随机干扰因素的问题,传统确定性博弈模型无法准确描述攻防博弈过程. 利用非线性 Itó 随机微分方程构建随机演化博弈模型,用于分析攻防随机动态演化过程. 通过求解,并根据随机微分方程稳定性判别定理对攻防双方的策略选取状态进行稳定性分析,设计出基于随机攻防演化博弈模型的安全防御策略选取算法. 最后,通过仿真验证了不同强度的随机干扰对攻防决策演化速率的影响,且干扰强度越大,防御者更倾向于选择强防御策略,攻击者更倾向于选择强攻击策略. 本文模型和方法能够用于网络攻击行为预测和安全防御决策.

关键词: 网络安全;网络攻防;博弈论;有限理性;演化博弈;网络防御;Itó 随机微分方程;策略选取
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2018)09-2222-07
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2018.09.025

A Method for Selecting Defense Strategies Based on Stochastic Evolutionary Game Model

HUANG Jian-ming[1], ZHANG Heng-wei[1,2]
(1. *The Third Institute, Information Engineering University, Zhengzhou, Henan* 450001, *China*;
2. *State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou, Henan* 450001, *China*)

Abstract: In the network attack-defense game systems, there are many stochastic factors, such as changes of attack-defense strategy sets and system operating environment. The traditional deterministic game model can not describe the game process of network attack and defense accurately. This paper constructed an attack-defense stochastic evolutionary game model by adapting the nonlinear Itó stochastic differential equations. The model can be applied to analyze the stochastic evolutionary process of network attack and defense. In addition, the stability of the strategy selection of attack and defense was analyzed according to the discriminant theorem of stochastic differential equations. Besides, an algorithm to select the security defense strategies based on stochastic attack-defense evolutionary game model was designed. Finally, the simulations demonstrate that the different intensity influences of stochastic interference on the speed of decision-making evolution of attack and defense. The attackers and defenders are more inclined to choose strong strategies when the game system has great intensity of interference. The model and the method proposed in this paper can provide guidance for attack behavior prediction and defense strategy selection.

Key words: network security; network attack-defense; game theory; bounded rationality; evolutionary game; network defense; Itó stochastic differential equation; strategy selection

1 引言

针对网络攻击手段日益复杂化、智能化和多样化,直面网络空间安全领域的诸多挑战[1],增强网络安全防御能力,确保网络空间安全已成为亟待解决的迫切问题[2,3]. 博弈论[4,5]具有目标对立性、关系非合作性、策略依存性等特点均与网络攻防的基本特征吻合[6]. 因此,将博弈理论应用于网络攻防过程的建模与分析成为近几年的研究热点.

传统博弈[7,8]建立在决策者完全理性前提下,与攻防实际不符,降低了模型和方法的有效性. 考虑到现实社会中的有限理性,将演化博弈理论应用于攻

收稿日期:2017-07-06;修回日期:2017-10-16;责任编辑:覃怀银
基金项目:国家自然科学基金(No. 61303074, No. 61309013);河南省科技计划基金(No. 12210231003, No. 13210231002)

防过程研究[9-12],分析攻防双方的复制动态及演化稳定策略,得出攻防对抗的规律和长期稳定趋势,但相关模型和方法均建立在确定性攻防条件下. 在实际攻防过程中,攻击手段的选择、系统运行环境的改变及其他外来因素的干扰等均具有一定的随机性,因此,对随机因素进行考虑能够提高模型和方法的准确性. 基于此,部分学者将攻防过程看作多个状态之间的随机跳变,采用传统博弈构建攻防随机博弈模型[13,14],但完全理性成为最大束缚. 为提高模型的有效性和准确性,本文借鉴高斯白噪声的概念,构建非对称条件下的随机攻防演化博弈模型,用于描述网络攻防对抗的实时随机动态演化过程. 对攻防双方的 Itó 随机微分方程进行数值求解,并根据随机微分方程稳定性判别定理对攻防双方的策略选取状态进行稳定性分析.

2　网络攻防随机演化博弈模型

2.1　攻防随机演化博弈模型构建

定义 1　攻防随机演化博弈模型 ADSEGM(Attack-Defense Stochastic Evolutionary Game Model)可以表示为 5 元组,ADSEGM = (N,S,P,Δ,U).

(1) $N=(N_D,N_A)$ 是博弈参与者空间. N_D 为防御方,N_A 为攻击方.

(2) $S=(\mathrm{DS},\mathrm{AS})$ 是博弈策略空间. 其中 DS 为防御策略集,AS 为攻击策略集.

(3) $P=(q,p)$ 是博弈信念集合. 其中 q 为选取防御策略的概率集合,p 为选取攻击策略的概率集合.

(4) $\Delta=\{\delta_1,\delta_2\}$ 是随机干扰强度系数集合. 其中 δ_1 为防御方随机干扰强度系数,δ_2 为攻击方随机干扰强度系数,且 $\delta_1>0,\delta_2>0$.

(5) $U=(U_D,U_A)$ 是博弈收益函数集合. 其中 U_D 为防御者收益,U_A 为攻击者收益.

构建防御方的可选策略集 DS = $\{\mathrm{DS}_1,\mathrm{DS}_2\}$. 同理,构建攻击方的可选策略集 AS = $\{\mathrm{AS}_1,\mathrm{AS}_2\}$. 对应的攻防博弈树如图 1 所示.

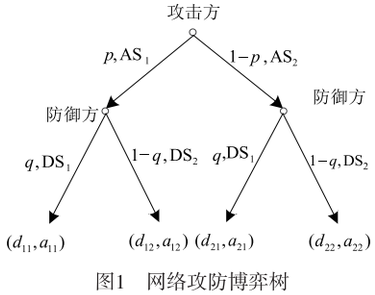

图1　网络攻防博弈树

注:图 1 中,a_{ij}、d_{ij} 分别为攻防收益值,该博弈的收益矩阵如表 1 所示.

表 1　网络攻防博弈收益矩阵

	强攻击策略(AS_1)	弱攻击策略(AS_2)
强防御策略(DS_1)	$V_n-C_d-V_{ad},-C_a+V_{ad}$	$V_n-C_d,0$
弱防御策略(DS_2)	$V_n-V_a,-C_a+V_a$	$V_n,0$

其中,V_n 表示防御方本身所拥有的信息资产能够带来的固定收益;

C_d 表示防御方选取 DS_1 时所需的防御成本;

C_a 表示攻击方选取 AS_1 时所需的攻击成本;

V_a 表示防御方选取 DS_2 时,攻击方选取 AS_1 能够获得的攻击回报;

V_{ad}表示防御方选取 DS_1 时,攻击方选取 AS_1 能够获得的攻击回报,且 $V_a>V_{ad}$.

在博弈过程中,假设 AS_2 的成本相对 AS_1 为 0.

基于此,分别计算出防御方的期望收益 U_{DS_i}和平均收益 $\overline{U}_D$.

$$U_{\mathrm{DS}_1}=p(t)(V_n-C_d-V_{ad})+(1-p(t))(V_n-C_d) \tag{1}$$

$$U_{\mathrm{DS}_2}=p(t)(V_n-V_a)+(1-p(t))V_n \tag{2}$$

$$\overline{U}_D=q(t)U_{\mathrm{DS}_1}+(1-q(t))U_{\mathrm{DS}_2} \tag{3}$$

针对 DS_1,可以采用如下复制动态方程描述其动态演化过程.

$$\begin{aligned}\mathrm{d}q(t)&=q(t)(U_{\mathrm{DS}_1}-\overline{U}_D)\mathrm{d}t\\&=q(t)(1-q(t))(U_{\mathrm{DS}_1}-U_{\mathrm{DS}_2})\mathrm{d}t\end{aligned} \tag{4}$$

由于 $1-q(t)\in[0,1]$,因此,式(4)可转化为

$$\begin{aligned}\mathrm{d}q(t)&=q(t)(U_{\mathrm{DS}_1}-U_{\mathrm{DS}_2})\mathrm{d}t\\&=q(t)[(V_a-V_{ad})p(t)-C_d]\mathrm{d}t\end{aligned} \tag{5}$$

通过分析可知,防御决策者选取策略 DS_1 的比例随时间的变化率$\dfrac{\mathrm{d}q(t)}{\mathrm{d}t}$与选取 DS_1 的期望收益和选取 DS_2 的期望收益差值幅度($U_{\mathrm{DS}_1}-U_{\mathrm{DS}_2}$)成正相关关系.

在此基础上,借鉴高斯白噪声的概念,采用随机微分方程[15]描述博弈系统中防御方存在的各类随机干扰,即可得到防御方的随机复制动态微分方程

$$\begin{aligned}\mathrm{d}q(t)&=q(t)[(V_a-V_{ad})p(t)-C_d]\mathrm{d}t\\&\quad+\delta_1\sqrt{(1-q(t))q(t)}\,\mathrm{d}\omega(t)\end{aligned} \tag{6}$$

同理可得,攻击方的随机复制动态微分方程

$$\begin{aligned}\mathrm{d}p(t)&=p(t)[q(t)(V_{ad}-V_a)+(V_a-C_a)]\mathrm{d}t\\&\quad+\delta_2\sqrt{(1-p(t))p(t)}\,\mathrm{d}\omega(t)\end{aligned} \tag{7}$$

其中,$\omega(t)$ 属于一维的标准 Brown 运动,可以很好地描述网络攻防过程中博弈演化是如何受到随机干扰因素的影响. $\omega(t)$ 服从正态分布 $N(0,t)$;$\mathrm{d}\omega(t)$ 表示随机干扰,当 $t>0$ 且 $h>0$ 时,其增量 $\Delta\omega(t)=\omega(t+h)-\omega(t)$ 服从正态分布 $N(0,\sqrt{h})$. 因此,$p(t)$ 和 $q(t)$ 的演化也成为一种随机过程,使其构成了随机攻防演化系统.

联立式(6)和(7),可得

$$\begin{cases} \mathrm{d}q(t) = q(t)[(V_a - V_{ad})p(t) - C_d]\mathrm{d}t \\ \qquad + \delta_1 \sqrt{(1-q(t))q(t)}\mathrm{d}\omega(t) \\ \mathrm{d}p(t) = p(t)[q(t)(V_{ad} - V_a) + (V_a - C_a)]\mathrm{d}t \\ \qquad + \delta_2 \sqrt{(1-p(t))p(t)}\mathrm{d}\omega(t) \end{cases} \tag{8}$$

2.2 演化均衡求解

结合随机泰勒展开式[17]和 Itó 随机公式,对随机微分方程进行展开求解.

针对以下 Itó 随机微分方程[18]

$$\mathrm{d}x(t) = f(t,x(t))\mathrm{d}t + g(t,x(t))\mathrm{d}\omega(t) \tag{9}$$

其中,$t \in [t_0, T]$,$x(t_0) = x_0$,$x_0 \in R$,$\omega(t)$一维的标准 Brown 运动,服从正态分布 $N(0,t)$,而 $\mathrm{d}\omega(t)$服从正态分布 $N(0,\Delta t)$.

令 $h = (T - t_0)/N$,$t_n = t_0 + nh$,将式(9)进行随机泰勒展开,可得

$$\begin{aligned} x(t_{n+1}) &= x(t_n) + K_0 f(x(t_n))\mathrm{d}t + K_1 g(x(t_n)) \\ &\quad + K_{11} M^1 g(x(t_n)) + K_{00} M^0 f(x(t_n)) + R \end{aligned} \tag{10}$$

其中,R 表示展开式的余项,且满足:

$$M^0 = f(x)\frac{\partial}{\partial x} + \frac{1}{2}g^2(x)\frac{\partial^2}{\partial x^2}; M^1 = g(x)\frac{\partial}{\partial x};$$

$$K_0 = h; K_1 = \Delta\omega_n; K_{00} = \frac{1}{2}h^2;$$

$$K_{11} = \frac{1}{2}[(\Delta\omega_n)^2 - h].$$

根据式(10),对式(6)进行泰勒展开,可得

$$\begin{aligned} q(t_{n+1}) &= q(t_n) + hq(t_n)[(V_a - V_{ad})p(t_n) - C_d] \\ &\quad + \Delta\omega_n\delta_1\sqrt{(1-q(t_n))q(t_n)} \\ &\quad + \frac{1}{4}[(\Delta\omega_n)^2 - h]\delta_1^2\sqrt{(1-q(t_n))q(t_n)} \\ &\quad \cdot \frac{1-2q(t_n)}{\sqrt{(1-q(t_n))q(t_n)}} \\ &\quad + \frac{1}{2}h^2 q(t_n)[((V_a - V_{ad})p(t_n) - C_d)^2] + R_1 \end{aligned}$$

同理,将式(7)泰勒展开可得

$$\begin{aligned} p(t_{n+1}) &= p(t_n) + hp(t_n)[(V_{ad} - V_a)q(t_n) + V_a - C_a] \\ &\quad + \Delta\omega_n\delta_2\sqrt{(1-p(t_n))p(t_n)} \\ &\quad + \frac{1}{4}[(\Delta\omega_n)^2 - h]\delta_2^2\sqrt{(1-p(t_n))p(t_n)} \\ &\quad \cdot \frac{1-2p(t_n)}{\sqrt{(1-p(t_n))p(t_n)}} \\ &\quad + \frac{1}{2}h^2 p(t_n)[(V_{ad} - V_a)q(t_n) + V_a - C_a)^2] + R_2 \end{aligned}$$

基于此,采用 Milstein 方法[19]对攻防随机微分方程进行数值求解,可得

$$\begin{aligned} x(t_{n+1}) &= x(t_n) + hf(x(t_n)) + \Delta\omega_n g(x(t_n)) \\ &\quad + \frac{1}{2}[(\Delta\omega_n)^2 - h]g(x(t_n))g'(x(t_n)) \end{aligned} \tag{11}$$

根据式(11)可以实现对微分方程式(6)和(7)的数值求解,得到相应的攻防演化均衡解.

2.3 演化稳定性分析

针对存在的均衡解,根据随机微分方程稳定性判别定理[16]对攻防双方的策略选取进行稳定性分析.

定理 1 针对式(6),令 $V(t,q(t)) = q(t)$,$q(t) \in [0,1]$,$c_1 = c_2 = 1$,$p = 1$,$\gamma = 1$,则 $\mathrm{LV}(t,q(t)) = f(t,q(t))$,于是满足:

(1)当 $p(t) \leqslant \dfrac{C_d - 1}{V_a - V_{ad}}$且 $C_d \geqslant 1$ 时,式(6)的零解期望矩指数稳定;

(2)当 $p(t) \geqslant \dfrac{C_d + 1}{V_a - V_{ad}}$且 $C_d - V_a + V_{ad} + 1 \leqslant 0$ 时,式(6)的零解期望矩指数不稳定.

证明 (1)针对式(6),已知 $c_1 = c_2 = 1$,$p = 1$,$\gamma = 1$,$V(t,q(t)) = q(t)$,$q(t) \in [0,1]$,$\mathrm{LV}(t,q(t)) = f(t,q(t)) = q(t)[(V_a - V_{ad})p(t) - C_d]$,要使式(6)满足零解期望矩指数稳定,则需满足

$$\mathrm{LV}(t,q(t)) \leqslant -\gamma V(t,q(t))$$

由 $q(t) \in [0,1]$可知,

$$(V_a - V_{ad})p(t) - (C_d - 1) \leqslant 0$$

又因为 $V_a > V_{ad}$,可得

$$p(t) \leqslant \frac{C_d - 1}{V_a - V_{ad}} \text{且 } C_d \geqslant 1.$$

证毕.

(2)要使式(6)满足零解期望矩指数不稳定,则

$$\mathrm{LV}(t,q(t)) \geqslant \gamma V(t,q(t))$$

由 $q(t) \in [0,1]$可得

$$(V_a - V_{ad})p(t) - (C_d + 1) \geqslant 0$$

根据 $V_a > V_{ad}$可得

$$p(t) \geqslant \frac{C_d + 1}{V_a - V_{ad}} \text{且 } C_d - V_a + V_{ad} + 1 \leqslant 0.$$

证毕.

由定理 1 可知:当 $p(t) \leqslant \dfrac{C_d - 1}{V_a - V_{ad}}$且 $C_d \geqslant 1$ 时,防御者最终将选择弱防御策略;相反,当 $p(t) \geqslant \dfrac{C_d + 1}{V_a - V_{ad}}$且 $C_d - V_a + V_{ad} + 1 \leqslant 0$ 时,防御者更倾向于选取强防御策略.

定理 2 针对式(7),令 $V(t,p(t)) = p(t)$,$p(t) \in [0,1]$,$c_1 = c_2 = 1$,$p = 1$,$\gamma = 1$,$\mathrm{LV}(t,p(t)) = f(t,p(t))$则满足

(1)当 $q(t) \geqslant \dfrac{C_a - V_a - 1}{V_{ad} - V_a}$且 $C_a - V_{ad} \geqslant 1$ 时,式(7)

的零解期望矩指数稳定;

(2)当 $q(t)\leqslant\frac{C_a-V_a+1}{V_{ad}-V_a}$且 $C_a-V_a+1\leqslant 0$ 时,式(7)的零解期望矩指数不稳定.

证明　根据定理1,同理可进行证明.

由定理2可知:当 $q(t)\geqslant\frac{C_a-V_a-1}{V_{ad}-V_a}$且 $C_a-V_{ad}\geqslant 1$ 时,攻击者最终将选取弱攻击策略;当 $q(t)\leqslant\frac{C_a-V_a+1}{V_{ad}-V_a}$且 $C_a-V_a+1\leqslant 0$ 时,攻击者更倾向于强攻击策略.

由定理1和定理2可知,当 $p(t)\leqslant\frac{C_d-1}{V_a-V_{ad}}$且 $C_d\geqslant 1$,$q(t)\geqslant\frac{C_a-V_a-1}{V_{ad}-V_a}$且 $C_a-V_{ad}\geqslant 1$ 时,攻防博弈系统存在唯一的演化稳定策略 ESS(0,0),即攻击方实施弱攻击策略,防御方选取弱防御策略;当 $p(t)\geqslant\frac{C_d+1}{V_a-V_{ad}}$且 $C_d-V_a+V_{ad}+1\leqslant 0$,$q(t)\leqslant\frac{C_a-V_a+1}{V_{ad}-V_a}$且 $C_a-V_a+1\leqslant 0$ 时,系统存在唯一的演化稳定策略 ESS(1,1),即攻击方实施强攻击策略,防御方选取强防御策略,这与实际网络攻防对抗不断演化升级保持一致.

2.4　安全防御策略选取算法设计分析

在建立攻防随机演化博弈模型的基础上,对博弈模型进行演化均衡求解,基于此,设计出一种基于随机演化博弈理论的安全防御策略选取算法,具体如算法1.

算法1　基于随机演化博弈模型的安全防御策略选取算法

输入:网络攻防博弈树
输出:安全防御策略
BEGIN
1. 初始化 ADEGM = (N,S,P,Δ,U);
2. 构建防御方的类型空间 $D=\{d_i,i\geqslant 1\}$;
3. 构建防御者可选策略空间 DS = $\{\mathrm{DS}_j,1\leqslant j\leqslant m\}$;
4. 针对所选攻击策略,以概率 $q_i(1\leqslant i\leqslant m)$ 选取合理的防御策略 DS_i,且 $\sum_{i=1}^{m}q_i=1$;
5. 针对所选攻防策略对 $\{\mathrm{AS}_i,\mathrm{DS}_j\}$,得出其防御收益值 b_{ij};
6. 计算各防御策略的期望收益 $U_{\mathrm{DS}_i}=p_1b_{1i}+p_2b_{2i}+\cdots+p_nb_{ni}$;
7. 计算防御方平均收益 $\overline{U}_D=\sum_{i=1}^{n}q_iU_{\mathrm{DS}_i}$;
8. 构建攻防随机干扰强度系数集合 $\Delta=\{\delta_1,\delta_2\}$,且 $\delta_1>0$,$\delta_2>0$;
9. 建立防御方随机复制动态演化方程 $\mathrm{d}q(t)=q(t)[(V_a-V_{ad})p(t)-C_d]\mathrm{d}t+\delta_1\sqrt{(1-q(t))q(t)}\mathrm{d}\omega(t)$;
10. 将防御方演化微分方程进行泰勒展开;
11. 采用 Milstein 方法对攻防随机微分方程进行数值求解;
12. Return(DS_k^*);
END

通过与已有研究成果进行比较,如表2所示. 文献[7]构建的静态博弈模型无法准确描述动态的攻防博弈过程. 文献[8]构建了动态博弈模型,但完全理性假设在现实中无法满足. 文献[9,11,12]采用有限理性条件下的演化博弈,但模型中均未考虑博弈系统中随机干扰的影响. 文献[13,14]将攻防博弈视为一个状态随机跳变的过程,但模型仅考虑了博弈状态的瞬时随机跳变. 本文将有限理性条件下的演化博弈理论与随机微分理论相结合,构建攻防随机演化博弈模型,提高了模型和方法的准确性和有效性.

表2　方法比较结果

文献	博弈类型	行为理性	模型通用性	均衡求解	模型准确性	具体应用
文献[7]	静态博弈	完全理性	一般	简单	较差	策略选取
文献[8]	动态博弈	完全理性	一般	详细	一般	安全防御
文献[9,11,12]	演化博弈	有限理性	差	简单	一般	安全防御
文献[13,14]	随机博弈	完全理性	一般	简单	一般	安全防御
本文	随机演化博弈	有限理性	较好	一般	较好	策略选取

3　实验仿真与分析

针对本文提出的随机攻防演化博弈模型及求解分析过程,采用 Matlab 2014 进行仿真. 构建攻防策略集,AS = {强攻击策略,弱攻击策略},DS = {强防御策略,弱防御策略},且攻防策略均由不同的原子策略所组成,即 $\mathrm{AS}_i=\{a_1,a_2\cdots a_k\}$,$\mathrm{DS}_j=\{d_1,d_2\cdots d_l\}$. 在实验过程中,参考美国 MIT 的攻防行为数据库[20],结合国家信息安全漏洞库(CNNVD)信息[21],构建攻防策略集,具体如表3和表4所示.

表3　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	remote buffer overflow	√	√
a_2	install Web Listener program	√	
a_3	attack SSH on Ftp sever		
a_4	homepage attack	√	
a_5	Oracle TNS Listener		√
a_6	install SQL Listener program	√	

表 4 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	install oracle patches	√	√
d_2	uninstall delete Trojan		
d_3	limit packets from ports	√	
d_4	restart Database server	√	
d_5	correct homepage	√	
d_6	add physical resource		√

在仿真过程中,取模拟步长 $h=0.01$,模拟攻防双方在不同条件下的策略演化过程. 假定策略选取初始状态为 $q(0)=0.5$,$p(0)=0.5$. 给定攻防博弈收益,通过改变攻防随机扰动强度系数 δ_i,观察随机扰动强度 δ_i 对攻防双方博弈演化的影响.

(1)参考文献[8,9,13]中的成本量化方法,取 $C_a=10$,$C_d=10$,$V_n=20$,当选取 DS_2 时,$V_a=10$,当选取 DS_1 时,$V_{ad}=5$. 此时,$\frac{C_d-1}{V_a-V_{ad}}=1.8$,满足式(6)的零解矩指数稳定条件 $p(0)\leqslant\frac{C_d-1}{V_a-V_{ad}}$且 $C_d\geqslant 1$,防御者倾向于选取 DS_2,防御方最终将稳定在 $q(t)=0$ 的状态,即所有防御者选择弱防御策略.

采用 Milstein 方法进行数值模拟,对随机扰动强度系数分别取值 $\delta_1=0.5$,$\delta_1=2$,$\delta_1=5$,用于分析不同随机干扰下防御策略的演化规律. 图 2 为防御方的零解稳定策略演化趋势图,其中横坐标 N 表示采样次数,纵坐标 $q(t)$ 表示选取 DS_1 的比例. 由图可知,防御方 DS_1 的选取在演化过程中呈现出一定的波动性,表明系统演化受随机因素的干扰. 随着 δ_1 减小,防御策略演化达到稳定状态所需的仿真次数越少,说明 δ_1 越小,防御方更倾向于选取 DS_2.

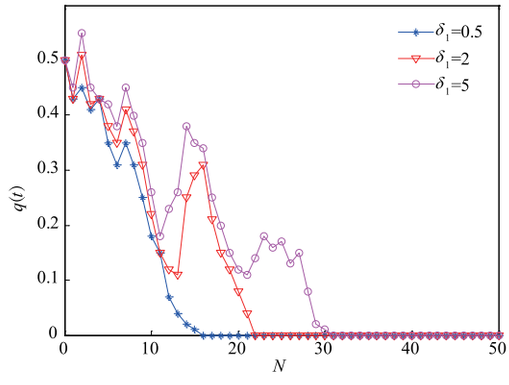

图2 防御方的零解稳定策略演化趋势

同理,针对攻击方的随机演化过程,$\frac{C_a-V_a-1}{V_{ad}-V_a}=0.2$ 且 $C_a-V_{ad}=5$,满足式(7)的零解矩指数稳定条件 $q(0)\geqslant\frac{C_a-V_a-1}{V_{ad}-V_a}$且 $C_a-V_{ad}\geqslant 1$,攻击者倾向于选取 AS_2,攻击方最终将稳定在 $p(t)=0$ 状态. 针对攻击方,分别取 $\delta_2=0.5$,$\delta_2=2$,$\delta_2=5$,用于分析不同随机干扰下的攻击策略演化规律. 如图 3 所示. 随着 δ_2 减小,AS_1 演化达到稳定状态的次数越少,说明随机因素干扰强度越小,攻击方更倾向于选取 AS_2.

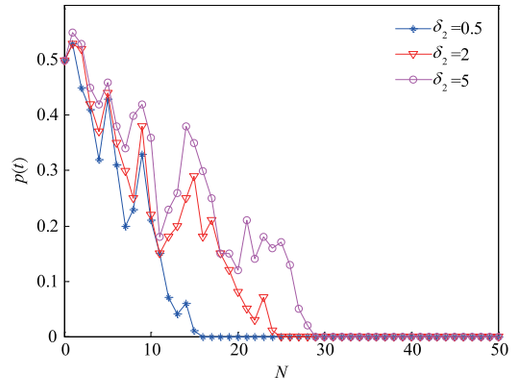

图3 攻击方的零解稳定策略演化趋势

(2)同样,取 $C_a=4$,$C_d=5$,$V_n=20$,当防御方选取 DS_2 时,$V_a=15$,当防御方选取 DS_1 时,$V_{ad}=2$. 此时,$\frac{C_d+1}{V_a-V_{ad}}=\frac{6}{13}$且 $C_d-V_a+V_{ad}+1=-7$,满足式(6)的零解矩指数不稳定条件 $p(0)\geqslant\frac{C_d+1}{V_a-V_{ad}}$且 $C_d-V_a+V_{ad}+1\leqslant 0$,防御者将倾向于选取 DS_1,最终将稳定在 $q(t)=1$ 的状态.

采用 Milstein 方法对防御方的演化进行数值模拟,分别取 $\delta_1=0.5$,$\delta_1=2$,$\delta_1=5$,用于分析不同随机干扰强度下的防御策略演化规律,如图 4 所示. 随着干扰强度 δ_1 减小,防御策略演化达到稳定状态所需的仿真次数越多,说明随机因素干扰强度越小,防御方更倾向于选取 DS_2.

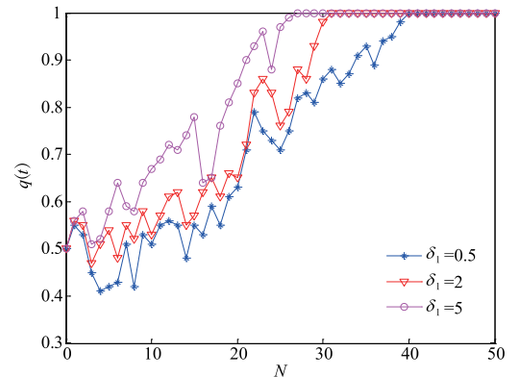

图4 防御方的零解非稳定策略演化趋势

同理,$\frac{C_a - V_a + 1}{V_{ad} - V_a} = \frac{10}{13}$且 $C_a - V_a + 1 = -10$,针对攻击方的演化过程,满足式(7)的零解矩指数不稳定条件 $q(0) \leqslant \frac{C_a - V_a + 1}{V_{ad} - V_a}$且 $C_a - V_a + 1 < 0$,攻击者倾向于选取 AS_1,攻击方最终将稳定在 $p(t) = 1$ 的演化状态.

针对攻击方的策略演化,取 $\delta_2 = 0.5$,$\delta_2 = 2$,$\delta_2 = 5$,用于分析不同随机干扰下攻击策略的演化规律,如图 5 所示. 随着干扰强度 δ_2 减小,AS_1 演化达到稳定状态的次数越多,说明随机因素干扰强度越小,攻击方更倾向于选取 AS_2.

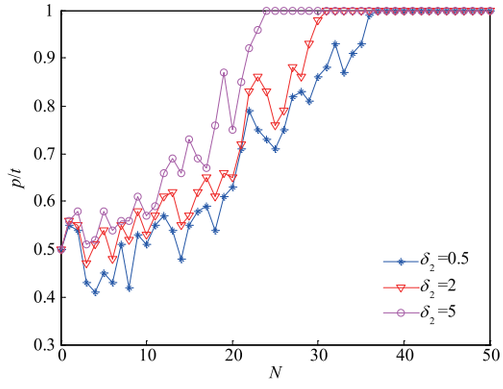

图5　攻击方的零解非稳定策略演化趋势

综上可知,不同随机干扰强度对攻防博弈系统的演化速率具有不同的影响,且干扰强度越大,防御者更倾向于选择强防御策略,攻击者更倾向于选择强攻击策略,该实验结果与随机控制理论中的系统追求稳定性保持一致. 当存在随机干扰时,系统通过加强攻防强度来防止扰动对系统稳定性的破坏,说明该随机演化博弈模型符合现实网络攻防系统中的演化规律.

4　结束语

本文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,采用 Itó 随机微分方程建立随机攻防演化博弈模型,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的影响. 根据随机微分方程稳定性判别定理对攻防策略选取状态的稳定性进行了分析. 此外,设计了基于随机攻防演化博弈模型的安全防御策略选取算法. 研究表明:在不同的条件下,攻防博弈系统存在唯一的演化稳定策略 ESS(0,0)或 ESS(1,1);攻防博弈系统中存在各类随机因素对攻防博弈系统的演化速率具有一定的影响,且干扰强度越大,防御者更倾向于选择强防御策略,攻击者更倾向于选择攻击策略. 在实际攻防博弈过程中,可根据随机干扰的强度大小来选取相应强度的防御策略. 但由于现实攻防过程复杂且受到的干扰因素众多,文中对攻防对抗中实际随机因素的阐述和分析不够,这将成为下一步研究的重点.

参考文献

[1] Gordon L, Loeb M, Lucyshyn W, Richardson R. 2016 CSI/FBI computer crime and security survey[A]. Proceedings of the 2016 Computer Security Institute[C]. San Francisco:IEEE, 2016. 48 – 64.

[2] Lye K W, Jeannette W. Markov game strategies in network security[J]. International Journal of Information Security, 2015, 4(1):71 – 86.

[3] Gordon L, Loeb M. Budgeting process for information security expenditures[J]. Communications of the ACM, 2016, 51(8):395 – 406.

[4] 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.

[5] 朱建明,王秦. 基于博弈论的网络空间安全若干问题分析[J]. 网络与信息安全学报,2015,1(1):43 – 49.
ZHU Jian-ming, WANG Qin. Analysis of cyberspace security based on game theory[J]. Chinese Journal of Network and Information Security, 2015, 1(1):43 – 49. (in Chinese)

[6] Nilim A, Ghaoui L E. Robust control of Markov decision processes with uncertain transition matrices[J]. Operations Research, 2016, 53(5):780 – 798.

[7] 张恒巍,余定坤,韩继红. 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):51 – 61.
ZHANG Heng-wei, YU Ding-kun, HAN Ji-hong. Defense policies selection method based on attack-defense signaling game model[J]. Journal on Communications, 2016, 37(5):51 – 61. (in Chinese)

[8] 张恒巍,李涛. 基于多阶段攻防信号博弈的最优主动防御[J],电子学报,2017,45(2):431 – 439.
ZHANG Heng-wei, Li Tao. Optimal active defense based on multi-stage attack-defense signaling game[J]. Acta Electronica Sinica, 2017, 45(2):431 – 439. (in Chinese)

[9] 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 Wei. Research on attack and deference in information security based on evolutionary game[J]. Information Science, 2015, (9):1408 – 1412. (in Chinese)

[10] Herbert Gintis. Game Theory Evolving[M]. Boston: Priceton University Press, 2015. 10.

[11] 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 Jian-ming, SONG Biao, HUANG Qi-fa. Evolution game model of offense-defense for network security based

on system dynamics[J]. Information Science, 2014, 35(1):54 – 61. (in Chinese)

[12] 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 Jian-ming, ZHANG Heng-wei, WANG Jin-dong, et al. Defense strategies selection based on attack-defense evolutionary game model[J]. Information Science, 2017, 38(1):168 – 176. (in Chinese)

[13] 王元卓,林闯,程学旗,等. 基于随机博弈模型的网络攻防量化分析方法[J]. 计算机学报,2015,33(9):1748 – 1764.
WANG Yuan-zhuo, LIN Chuang, CHENG Xue-qi, et al. Analysis for network attack-defense based on stochastic game model[J]. Chinese Journal of Computers, 2015, 33(9):1748 – 1764. (in Chinese)

[14] 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,2016,47(10):1714 – 1723.
JIANG Wei, FANG Bing-xing, TIAN Zhi-hong. Research on defense strategies selection based on attack-defense stochastic game model[J]. Journal of Computer Research and Development, 2016, 47(10):1714 – 1723. (in Chinese)

[15] D Cheng, F He, H Qi. Modeling, analysis and control of networked evolutionary games[J]. IEEE Transactions on Automatic Control, 2017, (99):41 – 49.

[16] 胡适耕,黄乘明,吴付科. 随机微分方程[M]. 北京:科学出版社,2008. 66 – 67.
Hu Shi-gen, Huang Cheng-ming, Wu Fu-ke. Stochastic Differential Equation[M]. Beijing: Science Press, 2008. 66 – 67. (in Chinese)

[17] Erwin A, Alex P. On the stability of evolutionary dynamics in games with incomplete information[J]. Mathematical Social Sciences, 2016, (58):310 – 321.

[18] White J, Park J S, Kamhoua C A, Kwiat K A. Game theoretic attack analysis in online social network services[A]. Proceedings of the 2017 International Conference on Social Networks Technology[C]. Los Angeles: IEEE, 2017. 1012 – 1019.

[19] Richard Lippmann, Joshua W. Haines. Analysis and results of the DARPA off-line intrusion detection evaluation[A]. Proceedings of the 17' th International Workshop on Recent Advances in Intrusion Detection[C]. New York: ACM, 2016. 162 – 182.

[20] Maleki H, Valizadeh M H, Koch W, et al. Markov modeling of moving target defense games[J]. Journal of Cryptology, 2017, (23):47 – 83.

[21] ZHANG Yong. Network security situation awareness approach based on Markov game model[J]. Journal of Software, 2016, 22(3):495 – 508.

作者简介

黄健明 男,1992 年出生于湖南张家界,硕士研究生,主要研究方向为网络安全主动防御.
E-mail:hjm-i-jbb@126.com

张恒巍(通信作者) 男,1978 年出生于河南洛阳,博士,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.
E-mail:zhw11qd@126.com