(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 107483486 A
(43)申请公布日 2017.12.15

(21)申请号 201710827946.9

(22)申请日 2017.09.14

(71)申请人 中国人民解放军信息工程大学
地址 450000 河南省郑州市高新区科学大道62号

(72)发明人 黄健明 张恒巍 王衡军 王晋东 王娜 寇广

(74)专利代理机构 郑州大通专利商标代理有限公司 41111
代理人 周艳巧

(51)Int.Cl.
H04L 29/06(2006.01)

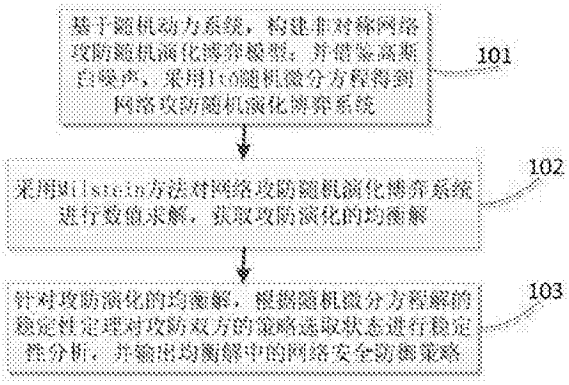
权利要求书2页 说明书15页 附图5页

(54)发明名称

基于随机演化博弈模型的网络防御策略选取方法

(57)摘要

本发明属于网络安全技术领域，特别涉及一种基于随机演化博弈模型的网络防御策略选取方法，包含：基于随机动力系统，构建非对称网络攻防随机演化博弈模型；并借鉴高斯白噪声，采用Itô随机微分方程得到网络攻防随机演化博弈系统；采用Milstein方法对网络攻防随机演化博弈系统进行数值求解，获取攻防演化的均衡解；针对攻防演化的均衡解，根据随机微分方程解的稳定性定理对攻防双方的策略选取状态进行稳定性分析，并输出均衡解中的网络安全防御策略。本发明解决传统确定博弈模型应用于网络防御策略选取不够准确等问题，能够更加准确地分析有限理性的攻防决策者之间的随机动态演化过程，增强安全防御策略选取的实用性，对网络安全防御技术具有重要指导意义。



CN 107483486 A

1.一种基于随机演化博弈模型的网络防御策略选取方法,其特征在于,包含:

基于随机动力系统,构建非对称网络攻防随机演化博弈模型;并借鉴高斯白噪声,采用Itô随机微分方程得到网络攻防随机演化博弈系统;

采用Milstein方法对网络攻防随机演化博弈系统进行数值求解,获取攻防演化的均衡解;

针对攻防演化的均衡解,根据随机微分方程解的稳定性定理对攻防双方的策略选取状态进行稳定性分析,并输出均衡解中的网络安全防御策略。

2.根据权利要求1所述的基于随机演化博弈模型的网络防御策略选取方法,其特征在于,所述的网络攻防随机演化博弈模型采用五元组表示。

3.根据权利要求2所述的基于随机演化博弈模型的网络防御策略选取方法,其特征在于,网络攻防随机演化模型ADEGM=(N,S,P,Δ,U),其中,N=(N_D,N_A)是演化博弈的参与者空间,N_D表示防御方,N_A表示攻击方;S=(DS,AS)是博弈策略空间,DS表示防御者的可选策略集,AS表示攻击者的可选策略集;P=(q,p)是博弈信念集合,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;$\Delta=\{\delta_1,\delta_2\}$是随机干扰强度系数集合,$\delta_1$表示随机干扰对防御方的影响强度系数,$\delta_2$表示随机干扰对攻击方的影响强度系数,且满足$\delta_1>0$,$\delta_2>0$;U=($U_D$,$U_A$)是博弈收益函数集合,$U_D$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。

4.根据权利要求3所述的基于随机演化博弈模型的网络防御策略选取方法,其特征在于,防御方的可选策略集$DS=\{DS_1,DS_2\}$,其中,DS_1表示防御者采取强防御策略,DS_2表示防御者采取弱防御策略;攻击方的可选策略集$AS=\{AS_1,AS_2\}$,其中,AS_1表示攻击者实施强攻击策略,AS_2表示攻击者实施弱攻击策略。

5.根据权利要求4所述的基于随机演化博弈模型的网络防御策略选取方法,其特征在于,网络攻防随机演化博弈系统的获取,包含如下内容:

A1)、构建防御方的类型空间集合$D=\{d_i,i\geq 1\}$;构建防御者可选策略空间集合$DS=\{DS_j,1\leqslant j\leqslant m\}$,其中,m为攻击方决策者可选策略数目;

A2)、针对攻击方所选攻击策略,以概率q_i选取防御策略DS_i,其中,$\sum_{i=1}^{m}q_i=1,\ 1\leq i\leq m$;

A3)、计算防御方的平均收益$\overline{U}_D$;构建攻防随机干扰强度系数集合$\Delta=\{\delta_1,\delta_2\}$,其中$\delta_1>0$,$\delta_2>0$;

A4)、借鉴高斯白噪声并采用随机微分方程描述攻防双方演化博弈的随机干扰,得到防御方和攻击方的随机复制动态微分方程;

A5)、联立防御方和攻击方的随机复制动态微分方程,得到网络攻防随机演化博弈系统。

6.根据权利要求5所述的基于随机演化博弈模型的网络防御策略选取方法,其特征在于,A3)中计算防御方的平均收益$\overline{U}_D$,包含:结合网络攻防博弈树,获取博弈收益矩阵;根据博弈收益矩阵,计算攻防双方的平均收益,其中,防御方的平均收益$\overline{U}_D=\sum_{i=1}^{n}q_iU_{DS_i}$,$U_{DS_i}$为防御方的期望收益。

7.根据权利要求5所述的基于随机演化博弈模型的网络防御策略选取方法，其特征在于，A5)中，网络攻防随机演化博弈系统表示为：

$$dq(t)=q(t)[(V_a-V_{ad})p(t)-C_d]dt+\delta_1\sqrt{(1-q(t))q(t)}d\omega(t)$$

$$dp(t)=p(t)[q(t)(V_{ad}-V_a)+(V_a-C_a)]dt+\delta_2\sqrt{(1-p(t))p(t)}d\omega(t),$$

其中，C_d表示防御方选择强防御策略时所需的防御成本；C_a表示攻击方选择强攻击策略时所需的攻击成本；V_a表示防御方选取弱防御策略时，攻击方选择强攻击策略能够获得的攻击回报；V_{ad}表示防御方选取强防御策略时，攻击方选择强攻击策略能够获得的攻击回报，且满足$V_a>V_{ad}$；q(t)和1-q(t)分别表示选取不同防御策略的防御者数量和选取不同防御策略的人数比例关于时间的函数；ω(t)属于一维的标准Brown运动，描述网络攻防过程中博弈演化受随机干扰因素的影响。

8.根据权利要求1所述的基于随机演化博弈模型的网络防御策略选取方法，其特征在于，获取攻防演化的均衡解，具体包含：

B1)、根据Itó随机微分方程对网络攻防随机演化博弈系统中防御方和攻击方两者的随机演化微分方程进行随机泰勒展开；

B2)、采用Milstein方法对网络攻防随机演化博弈系统中微分方程进行数值求解，得到相应的攻防演化均衡解。

9.根据权利要求8所述的基于随机演化博弈模型的网络防御策略选取方法，其特征在于，B1)中，Itó随机微分方程表示为dx(t)＝f(t,x(t))dt+g(t,x(t))dω(t)，其中，$t\in[t_0,T]$，$x(t_0)=x_0$，$x_0\in R$，ω(t)属于一维的标准Brown运动，服从正态分布N(0,t)，dω(t)服从正态分布N(0,Δt)，其中，T表示时间维度的延续，R为实数。

10.根据权利要求7所述的基于随机演化博弈模型的网络防御策略选取方法，其特征在于，攻防双方的策略选取状态进行稳定性分析，验证网络攻防随机演化博弈系统的演化稳定策略，包含：当满足$p(t)\le\frac{C_d-1}{V_a-V_{ad}}$且$C_d\ge1$，$q(t)\ge\frac{C_a-V_a-1}{V_{ad}-V_a}$且$C_a-V_{ad}\ge1$时，网络攻防随机演化博弈系统存在唯一演化稳定策略ESS(0,0)；当满足$p(t)\ge\frac{C_d+1}{V_a-V_{ad}}$且$C_d-V_a+V_{ad}+1\le0$，$q(t)\le\frac{C_a-V_a+1}{V_{ad}-V_a}$且$C_a-V_a+1\le0$时，网络攻防随机演化博弈系统存在唯一演化稳定策略ESS(1,1)。

基于随机演化博弈模型的网络防御策略选取方法

技术领域

[0001] 本发明属于网络安全技术领域，特别涉及一种基于随机演化博弈模型的网络防御策略选取方法。

背景技术

[0002] 目前，网络攻击手段日益复杂化、智能化和多样化，攻击者的攻击目的也不断转向经济利益驱动。直面网络空间安全领域的诸多挑战，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。博弈论是研究决策主体之间行为直接相互作用的决策理论，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。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。但已有研究成果具有一个共同特征，即所有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有效性和准确性。

[0003] 网络安全的本质在于攻防对抗，因此从攻防对抗的角度出发，研究探索网络安全分析方法和防御技术体系，具有重要现实意义。博弈论是研究决策主体之间行为直接相互作用的决策理论，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。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。由于传统博弈模型大都建立在行为者完全理性的前提下，与实际情况不符，基于非完全理性的演化博弈理论更加符合攻防对抗的实际，但目前使用最多的复制动态学习机制并未考虑攻防过程中存在的各类随机干扰因素的影响，确定型博弈模型降低了其实际的应用价值。网络攻防演化博弈模型ADEGM(Attack-Defense Evolutionary Game Model)表示为4元组，ADEGM＝(N,S,P,U)，其中，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。S＝(DS,AS)是博弈策略空间。其中DS＝{DS_1,DS_2,…DS_n}表示防御者的可选策略集，AS＝{AS_1,AS_2,…AS_m}表示攻击者的可选策略集。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。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。传统博弈理论应用于网络安全防御策略选取存在以下缺点：(1)经典博弈模型中的行为者完全理性前提假设与实际情况不符，而现实中由于人的决策能力是有限的，即决策者实际属于非完全理性个体。忽视行为者有限理性条件会对最终的博弈结果产生重大影响，使最终的博弈均衡结果与实际相差较大，从而降低了模型和方法的有效性。(2)传统演化博弈理论以复制动态学习机制为基础，决策者通过学习调整自身策略，使自身收益达到最大，但并未考虑博弈过程中存在的各类随机因素的干扰问题。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，忽略对随机因素的考虑会降低模型和方法的有效性和准确性。

发明内容

[0004] 针对现有技术中的不足，本发明提供一种基于随机演化博弈模型的网络防御策略选取方法，解决传统确定博弈模型应用于网络防御策略选取不够准确等问题，能够更加准确地分析有限理性的攻防决策者之间的随机动态演化过程，增强安全防御策略选取的实用性和指导意义。

[0005] 按照本发明所提供的设计方案，一种基于随机演化博弈模型的网络防御策略选取方法，包含：

[0006] 基于随机动力系统，构建非对称网络攻防随机演化博弈模型；并借鉴高斯白噪声，采用Itô随机微分方程得到网络攻防随机演化博弈系统；

[0007] 采用Milstein方法对网络攻防随机演化博弈系统进行数值求解，获取攻防演化的均衡解；

[0008] 针对攻防演化的均衡解，根据随机微分方程解的稳定性定理对攻防双方的策略选取状态进行稳定性分析，并输出均衡解中的网络安全防御策略。

[0009] 上述的，所述的网络攻防随机演化博弈模型采用五元组表示。

[0010] 优选的，网络攻防随机演化模型ADEGM＝(N,S,P,Δ,U)，其中，N＝(N_D,N_A)是演化博弈的参与者空间，N_D表示防御方，N_A表示攻击方；S＝(DS,AS)是博弈策略空间，DS表示防御者的可选策略集，AS表示攻击者的可选策略集；P＝(q,p)是博弈信念集合，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；Δ＝{δ_1,δ_2}是随机干扰强度系数集合，δ_1表示随机干扰对防御方的影响强度系数，δ_2表示随机干扰对攻击方的影响强度系数，且满足$\delta_1>0$,$\delta_2>0$；U＝(U_D,U_A)是博弈收益函数集合，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。

[0011] 优选的，防御方的可选策略集DS＝{DS_1,DS_2}，其中，DS_1表示防御者采取强防御策略，DS_2表示防御者采取弱防御策略；攻击方的可选策略集AS＝{AS_1,AS_2}，其中，AS_1表示攻击者实施强攻击策略，AS_2表示攻击者实施弱攻击策略。

[0012] 优选的，网络攻防随机演化博弈系统的获取，包含如下内容：

[0013] A1)、构建防御方的类型空间集合D＝{d_i,i≥1}；构建防御者可选策略空间集合DS＝{DS_j,1≤j≤m}，其中，m为攻击方决策者可选策略数目；

[0014] A2)、针对攻击方所选攻击策略，以概率q_i选取防御策略DS_i，其中，$\sum_{i=1}^{m} q_i = 1$，1≤i≤m；

[0015] A3)、计算防御方的平均收益$\overline{U}_D$；构建攻防随机干扰强度系数集合Δ＝{δ_1,δ_2}，其中$\delta_1>0$,$\delta_2>0$；

[0016] A4)、借鉴高斯白噪声并采用随机微分方程描述攻防双方演化博弈的随机干扰，得到防御方和攻击方的随机复制动态微分方程；

[0017] A5)、联立防御方和攻击方的随机复制动态微分方程，得到网络攻防随机演化博弈系统。

[0018] 优选的，A3)中计算防御方的平均收益$\overline{U}_D$，包含：结合网络攻防博弈树，获取博弈收益矩阵；根据博弈收益矩阵，计算攻防双方的平均收益，其中，防御方的平均收益$\overline{U}_D = \sum_{i=1}^{n} q_i U_{DS_i}$，$U_{DS_i}$为防御方的期望收益。

[0019] 优选的，A5)中，网络攻防随机演化博弈系统表示为：

[0020] $$dq(t)=q(t)[(V_a-V_{ad})p(t)-C_d]dt+\delta_1\sqrt{(1-q(t))q(t)}d\omega(t)$$

[0021] $$dp(t)=p(t)[q(t)(V_{ad}-V_a)+(V_a-C_a)]dt+\delta_2\sqrt{(1-p(t))p(t)}d\omega(t),$$

[0022] 其中，C_d表示防御方选择强防御策略时所需的防御成本；C_a表示攻击方选择强攻击策略时所需的攻击成本；V_a表示防御方选取弱防御策略时，攻击方选择强攻击策略能够获得的攻击回报；V_{ad}表示防御方选取强防御策略时，攻击方选择强攻击策略能够获得的攻击回报，且满足$V_a>V_{ad}$；q(t)和1-q(t)分别表示选取不同防御策略的防御者数量和选取不同防御策略的人数比例关于时间的函数；ω(t)属于一维的标准Brown运动，描述网络攻防过程中博弈演化受随机干扰因素的影响。

[0023] 优选的，获取攻防演化的均衡解，具体包含：

[0024] B1)、根据Itô随机微分方程对网络攻防随机演化博弈系统中防御方和攻击方两者的随机演化微分方程进行随机泰勒展开；

[0025] B2)、采用Milstein方法对网络攻防随机演化博弈系统中微分方程进行数值求解，得到相应的攻防演化均衡解。

[0026] 进一步，B1)中，Itô随机微分方程表示为dx(t)＝f(t,x(t))dt+g(t,x(t))dω(t)，其中，$t\in[t_0,T]$，$x(t_0)=x_0$，$x_0\in R$，ω(t)属于一维的标准Brown运动，服从正态分布N(0,t)，dω(t)服从正态分布N(0,Δt)，其中，T表示时间维度的延续，R为实数。

[0027] 上述的，攻防双方的策略选取状态进行稳定性分析，验证网络攻防随机演化博弈系统的演化稳定策略，包含：当满足$p(t)\le\frac{C_d-1}{V_a-V_{ad}}$且$C_d\ge1$，$q(t)\ge\frac{C_a-V_a-1}{V_{ad}-V_a}$且$C_a-V_{ad}\ge1$时，网络攻防随机演化博弈系统存在唯一演化稳定策略ESS(0,0)；当满足$p(t)\ge\frac{C_d+1}{V_a-V_{ad}}$且$C_d-V_a+V_{ad}+1\le0$，$q(t)\le\frac{C_a-V_a+1}{V_{ad}-V_a}$且$C_a-V_a+1\le0$时，网络攻防随机演化博弈系统存在唯一演化稳定策略ESS(1,1)。

[0028] 本发明的有益效果：

[0029] 本发明针对攻防博弈系统中存在各类随机干扰因素的问题，为提高模型的有效性和准确性，通过借鉴高斯白噪声的概念，描述攻防博弈过程中存在的系统运行环境改变、网络拓扑结构变化以及攻防策略的改变等各类随机干扰，改进传统复制动态演化博弈方法，利用非线性Itô随机微分方程构建非对称条件下的随机网络攻防演化博弈模型，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，确定随机攻防演化博弈模型的安全防御策略；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，能够为网络攻击行为预测和安全防御策略选取提供一定的技术指导。与现有技术相比，本发明能够更加准确地分析有限理性的攻防决策者之间的随机动态演化过程，安全防御策略选取的实用性和指导意义更强。

附图说明：

[0030] 图1为现有的基本网络攻防博弈树；

[0031] 图2为本发明的方法流程示意图；

[0032] 图3为实施例中的网络攻防博弈树示意图；

[0033] 图4为实施例中网络攻防随机演化博弈系统的获取流程示意图；

[0034] 图5为实施例中攻防演化的均衡解获取流程示意图；

[0035] 图6为仿真实例中防御方的零解稳定策略演化趋势图；

[0036] 图7为仿真实例中攻击方的零解稳定策略演化趋势图；

[0037] 图8为仿真实例中防御方的零解非稳定策略演化趋势图；

[0038] 图9为仿真实例中攻击方的零解非稳定策略演化趋势图。

具体实施方式：

[0039] 为使本发明的目的、技术方案和优点更加清楚、明白，下面结合附图和技术方案对本发明作进一步详细的说明。实施例中涉及到的技术术语如下：

[0040] 演化博弈论(Evolutionary Game Theory)：源于Darwin的生物进化论，继承了生物学对于物种进化的理论阐述，从个体有限理性条件出发，以群体行为为研究对象，在阐述生物物种的发展历程和进化选择中，解释了生物行为的进化博弈过程。通过长期的试错、模仿和改进，所有的博弈方都会趋于某个稳定的策略，该策略可能在群体组织中长期稳定下来，这种稳定的策略均衡就与生物进化的进化稳定策略非常相似，以达到一种相对和谐的博弈均衡状态。复制动态(Replicator Dynamic)：在由有限理性博弈方组成的群体中，博弈者通过不断试错、学习、改进自身策略，使博弈结果比平均水平好的策略逐步被更多博弈方采用，从而群体中采用各种策略的博弈方的比例会发生变化。纳什均衡(Nash Equilibrium)：在博弈$G=\{S_1,\cdots,S_n;u_1,\cdots,u_n\}$中，各博弈方的各一个策略组成的某个策略组合$(s_1^*,\cdots,s_n^*)$中，任意博弈方i的策略$s_i^*$，若满足条件：$u_i(s_1^*,\cdots,s_{i-1}^*,s_i^*,s_{i+1}^*,\cdots,s_n^*)\geq u_i(s_1^*,\cdots,s_{i-1}^*,s_{ij},s_{i+1}^*,\cdots,s_n^*)$对任意的$s_{ij}\in S_i$都成立，则称$(s_1^*,\cdots,s_n^*)$为博弈G的一个纳什均衡。有限理性(Bounded Rationality)：指行为者在博弈过程中通过博弈分析而找到最优策略，且不会因为遗忘、失误、任性等原因偏离最佳选择。在传统博弈理论中，一般以行为者完全理性为前提，即行为者的判断选择能力有限，且在决策过程中会“犯错误”。演化稳定策略(ESS,Evolutionary Stable Strategy)：是指在具有明确定义下不会被突变体入侵的策略，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。它是生物进化理论中具有较强抗干扰能力且在受到干扰后仍能“恢复”的稳健性均衡概念，是演化博弈分析中最核心的均衡概念。

[0041] 现有网络攻防演化博弈模型ADEGM(Attack-Defense Evolutionary Game Model)可以表示为4元组，$ADEGM=(N,S,P,U)$，其中$N=(N_D,N_A)$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。$S=(DS,AS)$是博弈策略空间，$DS=\{DS_1,DS_2,\cdots DS_n\}$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。$P=(p,q)$是博弈信念集合，$p_i$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。$U=(U_D,U_A)$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$m,n\in N$且$m,n\geq 2$)，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。采用不同策略进行攻防对抗时，会产生相应的攻防收益值。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。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：$p_1+p_2+\cdots+p_m=1$。

[0042] 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$\overline{U}_D$。

[0043] $$U_{DS_i}=\sum_{i=1}^{m}p_i b_{ij},\quad \overline{U}_D=\sum_{j=1}^{n}q_j U_{DS_j}$$

[0044] 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，采用$q_i(t)$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进行表示：

[0045] $$D(q)=\frac{dq_i(t)}{dt}=q(U_{DS_i}-\overline{U}_D)$$

[0046] 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：

[0047] $$A(p)=\frac{dp_i(t)}{dt}=p(U_{AS_i}-\overline{U}_A)$$

[0048] 联立以上两个复制动态方程，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，可以实现安全防御策略选取的分析和预测。但是，演化博弈理论以复制动态学习机制为基础，决策者通过学习调整自身策略，使自身收益达到最大，但并未考虑博弈过程中存在的各类随机因素的干扰问题。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，忽略对随机因素的考虑会降低模型和方法的有效性和准确性。鉴于此，本发明实施例提供了一种基于随机演化博弈模型的网络防御策略选取方法，参见图2所示，包含：

[0049] 101、基于随机动力系统，构建非对称网络攻防随机演化博弈模型；并借鉴高斯白噪声，采用Itô随机微分方程得到网络攻防随机演化博弈系统；

[0050] 102、采用Milstein方法对网络攻防随机演化博弈系统进行数值求解，获取攻防演化的均衡解；

[0051] 103、针对攻防演化的均衡解，根据随机微分方程解的稳定性定理对攻防双方的策略选取状态进行稳定性分析，并输出均衡解中的网络安全防御策略。

[0052] 解决传统确定博弈模型应用于网络防御策略选取不够准确的问题。为提高模型的有效性和准确性，本发明借鉴高斯白噪声的概念，描述攻防博弈过程中存在的系统运行环境改变、网络拓扑结构变化以及攻防策略的改变等各类随机干扰。通过构建非对称条件下的随机网络攻防演化博弈模型，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Itô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。该模型和方法能够更加准确地描述网络攻防策略选取动态变化过程。

[0053] 基于随机动力系统，结合网络攻防特点，以演化博弈理论为基础，构建有限理性条件下的非对称网络攻防随机演化博弈模型。在本发明的另一个实施例中，所述的网络攻防随机演化博弈模型采用五元组表示。进一步地，网络攻防随机演化模型ADEGM＝(N,S,P,Δ,U)，其中，N＝(N_D,N_A)是演化博弈的参与者空间，N_D表示防御方，N_A表示攻击方；S＝(DS,AS)是博弈策略空间，DS表示防御者的可选策略集，AS表示攻击者的可选策略集；P＝(q,p)是博弈信念集合，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；Δ＝{δ_1,δ_2}是随机干扰强度系数集合，δ_1表示随机干扰对防御方的影响强度系数，δ_2表示随机干扰对攻击方的影响强度系数，且满足$\delta_1>0$,$\delta_2>0$；U＝(U_D,U_A)是博弈收益函数集合，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。

[0054] 针对网络攻防对抗过程，为方便分析，将防御策略按防御强弱程度划分为强防御策略和弱防御策略两类，构建防御方的可选策略集DS＝{DS_1,DS_2}，其中DS_1表示防御者采取强防御策略，DS_2表示防御者采取弱防御策略。同理，针对攻击方，将攻击策略划分为强攻击策略和弱攻击策略两类，构建攻击方的可选策略集AS＝{AS_1,AS_2}，其中AS_1表示攻击者实施强攻击策略，AS_2表示攻击者实施弱攻击策略。本发明的另一个实施例，如图4所示，网络攻防随机演化博弈系统的获取，包含如下内容：

[0055] 201)、构建防御方的类型空间集合D＝{d_i,i≥1}；构建防御者可选策略空间集合DS＝{DS_j,1≤j≤m}，其中，m为攻击方决策者可选策略数目；

[0056] 202)、针对攻击方所选攻击策略，以概率q_i选取防御策略DS_i，其中，$\sum_{i=1}^{m} q_i = 1$，1≤i≤m；

[0057] 203)、计算防御方的平均收益$\overline{U}_D$；构建攻防随机干扰强度系数集合Δ＝{δ_1,δ_2}，其中$\delta_1>0$,$\delta_2>0$；

[0058] 204)、借鉴高斯白噪声并采用随机微分方程描述攻防双方演化博弈的随机干扰，得到防御方和攻击方的随机复制动态微分方程；

[0059] 205)、联立防御方和攻击方的随机复制动态微分方程，得到网络攻防随机演化博弈系统。

[0060] 网络攻防对抗过程中，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。其对应的网络攻防博弈树如图3所示，p表示攻击者选取攻击策略AS_1的概率，1-p表示选取攻击策略AS_2的概率，且满足p∈[0,1]；q表示防御者选取防御策略DS_1的概率，1-q表示选取防御策略DS_2的概率，且满足q∈[0,1]。d_{ij}表示攻防策略对(AS_i,DS_j)所产生

的防御收益值，a_{ij}表示攻防策略对(AS_i,DS_j)所产生的攻击收益值，该博弈的收益矩阵如表1所示。

[0061] 表1网络攻防博弈收益矩阵

[0062]

	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

[0063] 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；

[0064] C_d表示防御方选择强防御策略时所需的防御成本；

[0065] C_a表示攻击方选择强攻击策略时所需的攻击成本；

[0066] V_a表示防御方选取弱防御策略时，攻击方选择强攻击策略能够获得的攻击回报；

[0067] V_{ad}表示防御方选取强防御策略时，攻击方选择强攻击策略能够获得的攻击回报，且满足$V_a>V_{ad}$。

[0068] 在博弈过程中，假设弱攻防策略的成本相对强攻防策略为0。

[0069] 基于此，分别计算出防御方的期望收益U_{DS_i}和平均收益$\overline{U}_D$。

[0070] $$U_{DS_1}=p(t)(V_n-C_d-V_{ad})+(1-p(t))(V_n-C_d)$$

[0071] $$U_{DS_2}=p(t)(V_n-V_a)+(1-p(t))V_n$$

[0072] $$\begin{aligned}\overline{U}_D&=q(t)U_{DS_1}+(1-q(t))U_{DS_2}\\&=q(t)[p(t)(V_n-C_d-V_{ad})+(1-p(t))(V_n-C_d)]+(1-q(t))[p(t)(V_n-V_a)+(1-p(t))V_n]\end{aligned}$$

[0073] 在攻防过程中，随着博弈的重复进行，不同防御决策者之间通过相互学习并调整自身策略，使自身策略达到最优。因此，选取不同防御策略的防御者数量处于动态变化中，选取不同防御策略的人数比例是关于时间的函数，分别表示为q(t)和1-q(t)。针对强防御策略(DS_1)，可以采用如下复制动态方程描述其动态演化过程：

[0074] $$\begin{aligned}dq(t)&=q(t)(U_{DS_1}-\overline{U}_D)dt\\&=q(t)(1-q(t))(U_{DS_1}-U_{DS_2})dt\end{aligned}$$

[0075] 由于$1-q(t)\in[0,1]$，可以推知其对防御策略选取的演化结果不会产生影响，因此，可以将上式转化为如下形式：

[0076] $$\begin{aligned}dq(t)&=q(t)(U_{DS_1}-U_{DS_2})dt\\&=q(t)[(V_a-V_{ad})p(t)-C_d]dt\end{aligned}$$

[0077] 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$\frac{dq(t)}{dt}$与选取强防御策略的期望收益和选取弱防御策略的期望收益差值幅度$(U_{DS_1}-U_{DS_2})$成正相关关系。

[0078] 为了更加准确地描述实际网络攻防博弈过程，借鉴高斯白噪声的概念，采用随机微分方程描述博弈系统中防御方存在的防御策略随机改变、信息系统环境改变以及网络结

构变化等各类随机干扰，即可得到防御方的随机复制动态微分方程

[0079] $$dq(t)=q(t)[(V_a-V_{ad})p(t)-C_d]dt+\delta_1\sqrt{(1-q(t))q(t)}d\omega(t)$$

[0080] 同理，针对攻击方，可以求得攻击方不同攻击策略的期望收益U_{AS_i}和平均收益$\overline{U}_A$。

[0081] $$U_{AS_1}=q(t)(-C_a+V_{ad})+(1-q(t))(-C_a+V_a)\qquad U_{AS_2}=0$$

[0082] $$\begin{aligned}\overline{U}_A&=p(t)U_{AS_1}+(1-p(t))U_{AS_2}\\&=p(t)[q(t)(-C_a+V_{ad})+(1-q(t))(-C_a+V_a)]\end{aligned}$$

[0083] 进而得到攻击方的演化博弈复制动态方程：

[0084] $$dp(t)=p(t)(U_{AS_1}-U_{AS_2})dt=p(t)[q(t)(V_{ad}-V_a)+(V_a-C_a)]dt$$

[0085] 同理可得，攻击方的随机复制动态微分方程：

[0086] $$dp(t)=p(t)[q(t)(V_{ad}-V_a)+(V_a-C_a)]dt+\delta_2\sqrt{(1-p(t))p(t)}d\omega(t)$$

[0087] 攻防双方的随机复制动态微分方程为随机分析理论中常用的Itô随机微分方程，分别表示攻防双方的动态演化过程，其中，ω(t)属于一维的标准Brown运动，即一种无规则的随机涨落现象，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。给定时间t，则ω(t)服从正态分布N(0,t)；dω(t)表示随机干扰，当t>0且步长h>0时，其增量Δω(t)＝ω(t+h)-ω(t)服从正态分布$N(0,\sqrt{h})$；δ_i表示攻防双方的随机干扰强度，且满足$\delta_i>0$。因此，p(t)和q(t)的演化也成为一种随机过程，从而使攻防双方的随机复制动态微分方程构成随机攻防演化系统。

[0088] 在攻防博弈演化过程中，存在诸多影响系统稳定性的扰动因素，既有外部因素也有内部因素，每个因素对系统稳定性都不起决定性作用。

[0089] $\sqrt{(1-q(t))q(t)}$和$\sqrt{(1-p(t))p(t)}$决定了p(t)和q(t)的取值在区间[0,1]之间，符合其实际意义。

[0090] $\sqrt{(1-q(t))q(t)}\le\frac{1}{2}$和$\sqrt{(1-p(t))p(t)}\le\frac{1}{2}$当且仅当1-q(t)＝q(t)和1-p(t)＝p(t)满足时达到最大值，即扰动最大。当两种防御策略选取的人数比例相当时，系统的稳定性最容易受到扰动，相反，若二者比例相差较大，则扰动较小。

[0091] 联立攻防双方的随机复制动态微分方程，即可得到网络攻防随机演化博弈系统：

[0092] $$\begin{cases}dq(t)=q(t)[(V_a-V_{ad})p(t)-C_d]dt+\delta_1\sqrt{(1-q(t))q(t)}d\omega(t)\\dp(t)=p(t)[q(t)(V_{ad}-V_a)+(V_a-C_a)]dt+\delta_2\sqrt{(1-p(t))p(t)}d\omega(t)\end{cases}$$

[0093] 由于上述建立的随机攻防演化微分方程系统由非线性Itô随机微分方程构成，无法直接求出方程的解析解，为此，本发明的另一个实施例中，参见图5所示，获取攻防演化的均衡解，具体包含：

[0094] 301)、根据Itô随机微分方程对网络攻防随机演化博弈系统中防御方和攻击方两者的随机演化微分方程进行随机泰勒展开；

[0095] 302)、采用Milstein方法对网络攻防随机演化博弈系统中微分方程进行数值求解，得到相应的攻防演化均衡解。

[0096] 结合随机泰勒展开式和Itô随机公式，对攻防双方的随机复制动态微分方程进行

展开求解。

[0097] 针对Itô随机微分方程:dx(t)=f(t,x(t))dt+g(t,x(t))dω(t),其中,t∈[t_0,T],x(t_0)=x_0,x_0∈R,ω(t)一维的标准Brown运动,服从正态分布N(0,t),而dω(t)服从正态分布N(0,Δt)。令h=(T-t_0)/N,t_n=t_0+nh,进行Itô随机微分方程进行随机泰勒展开,得到

[0098] $x(t_{n+1})=x(t_n)+K_0f(x(t_n))dt+K_1g(x(t_n))+K_{11}M^1g(x(t_n))+K_{00}M^0f(x(t_n))+R$

[0099] ,其中,R表示展开式的余项,且

[0100] $$M^0=f(x)\frac{\partial}{\partial x}+\frac{1}{2}g^2(x)\frac{\partial^2}{\partial x^2};\quad M^1=g(x)\frac{\partial}{\partial x};$$

[0101] $K_0=h;K_1=\Delta\omega_n;K_{00}=\frac{1}{2}h^2;\quad K_{11}=\frac{1}{2}[(\Delta\omega_n)^2-h]$。

[0102] 在此基础上,可以将Itô随机微分方程表示成

[0103] $$x(t_{n+1})=x(t_n)+hf(x(t_n))+\Delta\omega_n g(x(t_n))+\frac{1}{2}[(\Delta\omega_n)^2-h]g(x(t_n))g'(x(t_n))+\frac{1}{2}h^2[f(x(t_n))f'(x(t_n))+\frac{1}{2}g^2(x(t_n))f''(x(t_n))]+R$$

[0104] 由此,对防御方的随机演化微分方程进行随机泰勒展开,即可得到

[0105] $$q(t_{n+1})=q(t_n)+h[(V_a-V_{ad})p(t_n)q(t_n)-C_dq(t_n)]+\Delta\omega_n\delta_1\sqrt{(1-q(t_n))q(t_n)}+\frac{1}{2}[(\Delta\omega_n)^2-h]\delta_1\sqrt{(1-q(t_n))q(t_n)}\cdot\frac{1}{2}\delta_1\frac{1-2q(t_n)}{\sqrt{(1-q(t_n))q(t_n)}}+\frac{1}{2}h^2[((V_a-V_{ad})p(t_n)q(t_n)-C_dq(t_n))\cdot((V_a-V_{ad})p(t_n)-C_d)+\frac{1}{2}\delta_1^2(1-q(t_n))q(t_n)\cdot 0]+R_1$$

[0106] 即

[0107] $$q(t_{n+1})=q(t_n)+hq(t_n)[(V_a-V_{ad})p(t_n)-C_d]+\Delta\omega_n\delta_1\sqrt{(1-q(t_n))q(t_n)}+\frac{1}{4}[(\Delta\omega_n)^2-h]\delta_1^2\sqrt{(1-q(t_n))q(t_n)}\cdot\frac{1-2q(t_n)}{\sqrt{(1-q(t_n))q(t_n)}}+\frac{1}{2}h^2q(t_n)[((V_a-V_{ad})p(t_n)-C_d)^2]+R_1$$

[0108] 同理,针对攻击方的随机演化微分方程,对其进行随机泰勒展开可以得到

[0109] $$p(t_{n+1})=p(t_n)+hp(t_n)[(V_{ad}-V_a)q(t_n)+V_a-C_a]+\Delta\omega_n\delta_2\sqrt{(1-p(t_n))p(t_n)}+\frac{1}{4}[(\Delta\omega_n)^2-h]\delta_2^2\sqrt{(1-p(t_n))p(t_n)}\cdot\frac{1-2p(t_n)}{\sqrt{(1-p(t_n))p(t_n)}}+\frac{1}{2}h^2p(t_n)[(V_{ad}-V_a)q(t_n)+V_a-C_a)^2]+R_2$$

[0110] 其中,R_1和R_2分别表示攻防微分展开式的余项。随机泰勒展开式是随机微分方程数值求解的基础,在求解过程中,一般采用Euler方法和Milstein方法对模型进行数值求解,Euler方法和Milstein方法的求解过程均是在泰勒展开式的基础上截取部分项得到。针对本发明建立的网络攻防随机演化博弈模型,采用Milstein方法对攻防随机微分方程进行数值求解,Milstein方法的表达式如下:

[0111] $$x(t_{n+1})=x(t_n)+hf(x(t_n))+\Delta\omega_n g(x(t_n))+\frac{1}{2}[(\Delta\omega_n)^2-h]g(x(t_n))g'(x(t_n))$$

[0112] 根据上式可以实现对网络攻防随机演化微分方程(10)和(15)进行数值求解,得到相应的攻防演化均衡解。

[0113] 针对博弈系统存在的均衡解,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。

[0114] 给定一个随机微分方程：

[0115] $dx(t)=f(t,x(t))dt+g(t,x(t))d\omega(t),x(t_0)=x_0$

[0116] 记$x(t)=x(t,x_0)$属于上述微分方程的解，为方便分析，假设$x(t),f(t,x(t)),g(t,x(t))$均为标量。设存在函数$V(t,x)$与正常数c_1,c_2满足

[0117] $c_1|x|^p\leqslant V(t,x)\leqslant c_2|x|^p,t\geqslant 0.$

[0118] (1)若存在正常数γ，满足：

[0119] $LV(t,x)\leqslant-\gamma V(t,x),t\geqslant 0.$

[0120] 则微分方程(21)的零解p阶矩期望指数稳定，且成立

[0121] $E|x(t,x^0)|^p<(c^2/c^1)|x^0|^pe^{-\gamma t},t\geqslant 0.$

[0122] (2)若存在正常数γ，满足：

[0123] $LV(t,x)\geqslant\gamma V(t,x),t\geqslant 0.$

[0124] 则微分方程(21)的零解p阶矩期望指数不稳定，且成立

[0125] $E|x(t,x^0)|^p\geqslant(c^2/c^1)|x^0|^pe^{-\gamma t},t\geqslant 0.$

[0126] 根据上述内容，通过分析可以得到随机攻防演化系统的稳定性判据。

[0127] 针对防御方的随机演化微分方程，令$V(t,q(t))=q(t),q(t)\in[0,1],c_1=c_2=1,p=1,\gamma=1$，则$LV(t,q(t))=f(t,q(t))$，于是满足：

[0128] (1)当$p(t)\leq\frac{C_d-1}{V_a-V_{ad}}$且$C_d\geqslant 1$时，随机微分方程(10)的零解期望矩指数稳定；

[0129] (2)当$p(t)\geq\frac{C_d+1}{V_a-V_{ad}}$且$C_d-V_a+V_{ad}+1\leqslant 0$时，随机微分方程(10)的零解期望矩指数不稳定。

[0130] 针对防御方的随机演化微分方程，已知$c_1=c_2=1,p=1,\gamma=1,V(t,q(t))=q(t),q(t)\in[0,1],LV(t,q(t))=f(t,q(t))=q(t)[(V_a-V_{ad})p(t)-C_d]$，要使防御方的随机演化微分方程满足零解期望矩指数稳定，则需要满足

[0131] $LV(t,q(t))\leqslant-\gamma V(t,q(t))$

[0132] 即

[0133] $q(t)[(V_a-V_{ad})p(t)-C_d]\leqslant-q(t)$

[0134] 进一步可以得到

[0135] $q(t)[(V_a-V_{ad})p(t)-(C_d-1)]\leqslant 0$

[0136] 由$q(t)\in[0,1]$可知，

[0137] $(V_a-V_{ad})p(t)-(C_d-1)\leqslant 0$

[0138] 又因为$V_a>V_{ad}$，可得

[0139] $p(t)\leq\frac{C_d-1}{V_a-V_{ad}}$，且满足$\frac{C_d-1}{V_a-V_{ad}}\geq 0$

[0140] 即

[0141] $p(t)\leq\frac{C_d-1}{V_a-V_{ad}}$且$C_d\geqslant 1$.证毕。

[0142] (2)要使防御方的随机演化微分方程满足零解期望矩指数不稳定，则需要满足

[0143] $LV(t,q(t)) \geq \gamma V(t,q(t))$

[0144] 即

[0145] $q(t)[(V_a-V_{ad})p(t)-C_d] \geq q(t)$

[0146] 进一步可以得到

[0147] $q(t)[(V_a-V_{ad})p(t)-(C_d+1)] \geq 0$

[0148] 由$q(t) \in [0,1]$可得

[0149] $(V_a-V_{ad})p(t)-(C_d+1) \geq 0$

[0150] 根据$V_a > V_{ad}$可得

[0151] $p(t) \geq \frac{C_d+1}{V_a-V_{ad}}$，且满足$\frac{C_d+1}{V_a-V_{ad}} \leq 1$

[0152] 即

[0153] $p(t) \geq \frac{C_d+1}{V_a-V_{ad}}$且$C_d-V_a+V_{ad}+1 \leq 0$.证毕。

[0154] 由上述内容可知：当满足条件$p(t) \leq \frac{C_d-1}{V_a-V_{ad}}$且$C_d \geq 1$时，随着攻防博弈的重复进行，网络防御者最终将选择弱防御策略，达到演化稳定状态；相反，当满足条件$p(t) \geq \frac{C_d+1}{V_a-V_{ad}}$且$C_d-V_a+V_{ad}+1 \leq 0$时，随着攻防博弈的进行，网络防御者更倾向于选取强防御策略，弱防御策略选取者将不断调整自身策略，改选强防御策略，从而使自身收益达到最大。

[0155] 针对攻击方的随机演化微分方程，令$V(t,p(t))=p(t)$，$p(t) \in [0,1]$，$c_1=c_2=1$，$p=1$，$\gamma=1$，则$LV(t,p(t))=f(t,p(t))$，于是满足：

[0156] (1)当$q(t) \geq \frac{C_a-V_a-1}{V_{ad}-V_a}$且$C_a-V_{ad} \geq 1$时，随机微分方程(15)的零解期望矩指数稳定；

[0157] (2)当$q(t) \leq \frac{C_a-V_a+1}{V_{ad}-V_a}$且$C_a-V_a+1 \leq 0$时，随机微分方程(15)的零解期望矩指数不稳定。

[0158] 由此可知：当满足条件$q(t) \geq \frac{C_a-V_a-1}{V_{ad}-V_a}$且$C_a-V_{ad} \geq 1$时，随着攻防博弈的重复进行，网络攻击者最终将选取弱攻击策略，博弈系统达到演化稳定状态；当满足条件$q(t) \leq \frac{C_a-V_a+1}{V_{ad}-V_a}$且$C_a-V_a+1 \leq 0$时，攻击者有利可图，此时攻击者更倾向于强攻击策略，通过不断学习调整策略，使收益最大。

[0159] 结合攻防双方的随机演化微分方程的上述内容可知，当满足条件$p(t) \leq \frac{C_d-1}{V_a-V_{ad}}$且$C_d \geq 1$，$q(t) \geq \frac{C_a-V_a-1}{V_{ad}-V_a}$且$C_a-V_{ad} \geq 1$时，网络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；当满足条件$p(t)\geq\frac{C_d+1}{V_a-V_{ad}}$且$C_d-V_a+V_{ad}+1\leqslant 0$，$q(t)\leq\frac{C_a-V_a+1}{V_{ad}-V_a}$且$C_a-V_a+1\leqslant 0$时，博弈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。

[0160] 获取安全防御策略的基本思想是，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，基于求出的演化稳定均衡解进行安全防御策略选取。针对防御方，本实施例提供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所示：

[0161] 算法1：基于随机演化博弈模型的安全防御策略选取算法

[0162] Input:网络攻防博弈树

[0163] Output:安全防御策略

[0164] BEGIN

[0165] 1.Initialize;

[0166] 2.构建防御方的类型空间集合$D=\{d_i,i\geqslant 1\}$；

[0167] 3.构建防御者可选策略空间集合$DS=\{DS_j,1\leqslant j\leqslant m\}$；

[0168] 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$\sum_{i=1}^{m}q_i=1$；

[0169] 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}；

[0170] 6.计算各防御策略的期望收益$U_{DS_i}=p_1b_{1i}+p_2b_{2i}+\cdots+p_nb_{mi}$，其中n表示攻击方的策略个数；

[0171] 7.计算防御方的平均收益$\overline{U}_D=\sum_{i=1}^{n}q_iU_{DS_i}$；

[0172] 8.构建攻防随机干扰强度系数集合$\Delta=\{\delta_1,\delta_2\}$，其中$\delta_1>0$，$\delta_2>0$；

[0173] 9.建立防御方随机复制动态演化方程

$$dq(t)=q(t)[(V_a-V_{ad})p(t)-C_d]dt+\delta_1\sqrt{(1-q(t))q(t)}d\omega(t)$$；

[0174] 10.将防御方的随机演化微分方程进行随机泰勒展开，

[0175] $$q(t_{n+1})=q(t_n)+hq(t_n)[(V_a-V_{ad})p(t_n)-C_d]+\Delta\omega_n\delta_1\sqrt{(1-q(t_n))q(t_n)}+\frac{1}{4}[(\Delta\omega_n)^2-h]\delta_1^2\sqrt{(1-q(t_n))q(t_n)}\cdot\frac{1-2q(t_n)}{\sqrt{(1-q(t_n))q(t_n)}}+\frac{1}{2}h^2q(t_n)[((V_a-V_{ad})p(t_n)-C_d)^2]+R_1;$$

[0176] 11.采用Milstein方法对攻防随机微分方程进行数值求解；

[0177] 12.输出均衡解中的安全防御策略；

[0178] END

[0179] 该算法的时间复杂度主要集中于随机微分方程的求解，其时间复杂度为$O((m+n)^2)$；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)。

[0180] 为验证本发明的有效性，下面通过具体仿真实验做进一步分析：针对发明提出的随机攻防演化博弈模型及求解分析过程，采用Matlab 2014进行数值仿真。假定攻防双方均存在两种可选策略，AS＝{强攻击策略，弱攻击策略}，DS＝{强防御策略，弱防御策略}。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。

[0181] (1)在攻防博弈过程中，假定攻击成本为C_a＝10，防御成本为C_d＝10，防御方的资产收益为V_n＝20，当防御方选取弱防御策略时的攻击回报为V_a＝10，当防御方选取强防御策略时的攻击回报为V_{ad}＝5。此时，$\frac{C_d-1}{V_a-V_{ad}}=1.8$，针对防御方的随机演化过程，满足随机微分方程(10)的零解矩指数稳定条件$p(0)\le\frac{C_d-1}{V_a-V_{ad}}$且$C_d\ge1$，网络防御者将倾向于选取弱防御策略，随着博弈的进行，防御方最终将稳定在q(t)＝0的演化状态，即所有防御者选择弱防御策略。

[0182] 针对防御方的策略演化，采用Milstein方法进行数值模拟，对随机扰动强度系数取值δ_1＝0.5，δ_1＝2，δ_1＝5，用于分析不同随机干扰下防御策略的演化规律。图6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)表示选取强防御策略的比例。

[0183] 由图6可知，防御方强防御策略的选取在演化过程中呈现出一定的波动性，表明系统存在的随机干扰对防御策略的演化具有一定的影响。此外，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少(δ_1＝0.5时，防御策略在仿真16次即达到稳定状态；而δ_1＝5时，仿真31次才达到稳定状态)，说明随机因素干扰强度越小，防御方更倾向于选取弱防御策略。

[0184] 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，满足随机微分方程(15)的零解矩指数稳定条件$q(0)\ge\frac{C_a-V_a-1}{V_{ad}-V_a}$且$C_a-V_{ad}\ge1$，网络攻击者倾向于选取实施弱攻击策略，随着博弈的进行，攻击方最终将稳定在p(t)＝0的演化状态，即所有攻击者选择实施弱攻击策略。

[0185] 针对攻击方的策略演化，对随机扰动强度系数取值δ_2＝0.5，δ_2＝2，δ_2＝5，用于分析不同随机干扰下攻击策略的演化规律。图7为攻击方的零解稳定策略演化趋势，其中横坐标N表示采样次数，纵坐标p(t)表示选取实施强攻击策略的比例。

[0186] 由图7可知，随着干扰强度δ_2减小，强攻击策略演化达到稳定状态的次数越少(δ_2＝0.5时，攻击策略在仿真16次即达到稳定状态；而δ_2＝5时，仿真29次才达到稳定状态)，说明随机因素干扰强度越小，攻击方更倾向于选取实施弱攻击策略。

[0187] (2)在攻防博弈过程中，假定攻击成本为C_a＝4，防御成本为C_d＝5，防御方的资产收益为V_n＝20，当防御方选取弱防御策略时的攻击回报为V_a＝15，当防御方选取强防御策略时的攻击回报为V_{ad}＝2。此时，$\frac{C_d+1}{V_a-V_{ad}}=\frac{6}{13}$且$C_d-V_a+V_{ad}+1=-7$。针对防御方的随机演化过程，

满足随机微分方程(10)的零解矩指数不稳定条件$p(0)\geq\frac{C_d+1}{V_a-V_{ad}}$且$C_d-V_a+V_{ad}+1\leqslant 0$，网络防御者将倾向于选取强防御策略，随着博弈的进行，防御方最终将稳定在q(t)＝1的演化状态，即所有防御者选择强防御策略。

[0188] 基于上述条件，采用Milstein方法对防御方选取强防御策略的演化进行数值模拟，对随机扰动强度系数取值$\delta_1=0.5$，$\delta_1=2$，$\delta_1=5$，用于分析不同随机干扰强度下的防御策略演化规律。防御方的零解非稳定策略演化趋势如图8所示。

[0189] 由图8可知，防御方选择强防御策略在演化过程中呈现出一定的波动性，表明系统存在的随机干扰对防御策略的演化具有一定的影响。此外，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($\delta_1=0.5$时，防御策略在仿真39次即达到稳定状态；而$\delta_1=5$时，仿真27次才达到稳定状态)，说明随机因素干扰强度越小，防御方更倾向于选取弱防御策略。

[0190] 同理，$\frac{C_a-V_a+1}{V_{ad}-V_a}=\frac{10}{13}$且$C_a-V_a+1=-10$，针对攻击方的随机演化过程，满足随机微分方程(15)的零解矩指数不稳定条件$q(0)\leq\frac{C_a-V_a+1}{V_{ad}-V_a}$且$C_a-V_a+1<0$，网络攻击者倾向于选取实施强攻击策略，随着博弈的进行，攻击方最终将稳定在p(t)＝1的演化状态，即所有攻击者选择实施强网络攻击。

[0191] 针对攻击方的策略演化，对随机扰动强度系数取值$\delta_2=0.5$，$\delta_2=2$，$\delta_2=5$，用于分析不同随机干扰下攻击策略的演化规律。攻击方的零解非稳定策略演化趋势如图9所示。

[0192] 由图9可知，随着干扰强度δ_2减小，强攻击策略演化达到稳定状态的次数越多($\delta_2=0.5$时，攻击策略在仿真37次即达到稳定状态；而$\delta_2=5$时，仿真24次才达到稳定状态)，说明随机因素干扰强度越小，攻击方更倾向于选取实施弱攻击策略。

[0193] 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。本发明针对攻防博弈系统中存在各类随机干扰因素的问题，为提高模型的有效性和准确性，通过借鉴高斯白噪声的概念，描述攻防博弈过程中存在的系统运行环境改变、网络拓扑结构变化以及攻防策略的改变等各类随机干扰，改进传统复制动态演化博弈方法，利用非线性Itô随机微分方程构建非对称条件下的随机网络攻防演化博弈模型，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，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。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，能够为网络攻击行为预测和安全防御策略选取提供一定的指导。与现有技术相比，本发明能够更加准确地分析有限理性的攻防决策者之间的随机动态演化过程，安全防御策略选取的实用性和指导意义更强。

[0194] 本说明书中各个实施例采用递进的方式描述，每个实施例重点说明的都是与其他实施例的不同之处，各个实施例之间相同相似部分互相参见即可。对于实施例公开的装置而言，由于其与实施例公开的方法相对应，所以描述的比较简单，相关之处参见方法部分说

明即可。

[0195] 结合本文中所公开的实施例描述的各实例的单元及方法步骤，能够以电子硬件、计算机软件或者二者的结合来实现，为了清楚地说明硬件和软件的可互换性，在上述说明中已按照功能一般性地描述了各示例的组成及步骤。这些功能是以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。本领域普通技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不认为超出本发明的范围。

[0196] 本领域普通技术人员可以理解上述方法中的全部或部分步骤可通过程序来指令相关硬件完成，所述程序可以存储于计算机可读存储介质中，如：只读存储器、磁盘或光盘等。可选地，上述实施例的全部或部分步骤也可以使用一个或多个集成电路来实现，相应地，上述实施例中的各模块/单元可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。本发明不限制于任何特定形式的硬件和软件的结合。

[0197] 对所公开的实施例的上述说明，使本领域专业技术人员能够实现或使用本申请。对这些实施例的多种修改对本领域的专业技术人员来说将是显而易见的，本文中所定义的一般原理可以在不脱离本申请的精神或范围的情况下，在其它实施例中实现。因此，本申请将不会被限制于本文所示的这些实施例，而是要符合与本文所公开的原理和新颖特点相一致的最宽的范围。

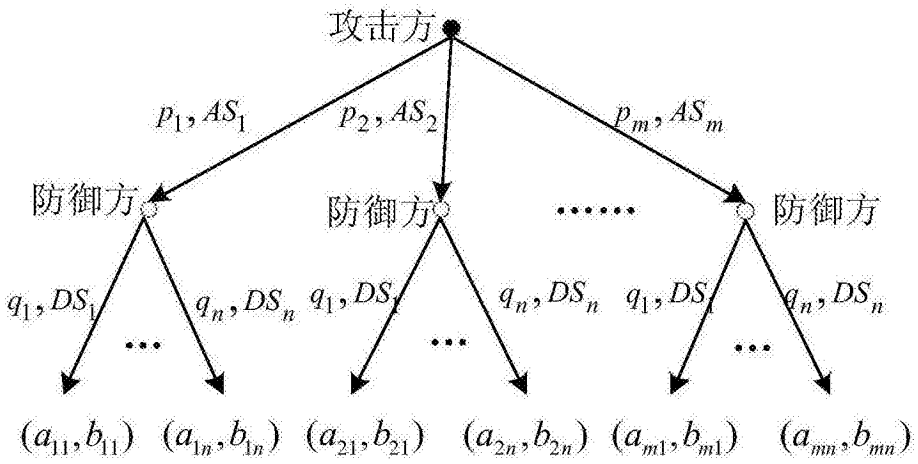

攻击方
p_1, AS_1
p_2, AS_2
p_m, AS_m
防御方
防御方
防御方
q_1, DS_1
q_n, DS_n
(a_{11}, b_{11})
(a_{1n}, b_{1n})
(a_{21}, b_{21})
(a_{2n}, b_{2n})
(a_{m1}, b_{m1})
(a_{mn}, b_{mn})

图1

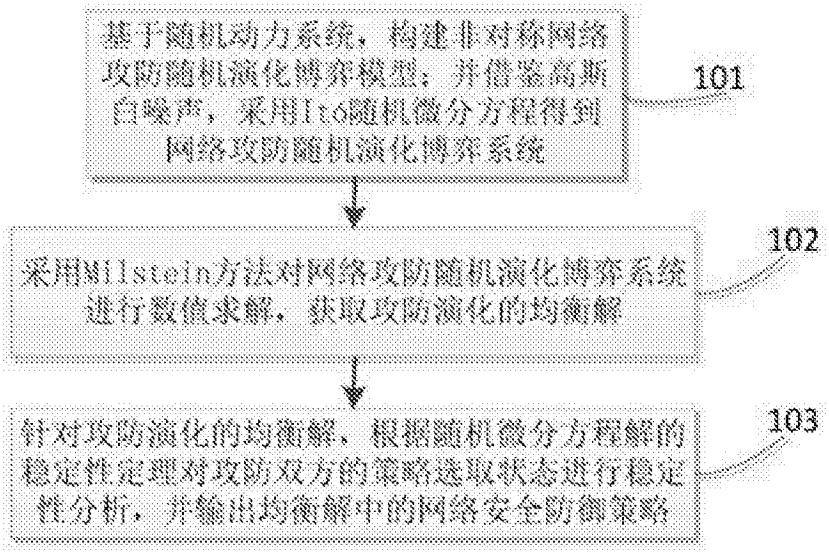

基于随机动力系统，构建非对称网络攻防随机演化博弈模型；并借鉴高斯白噪声，采用Ito随机微分方程得到网络攻防随机演化博弈系统
101
采用Milstein方法对网络攻防随机演化博弈系统进行数值求解，获取攻防演化的均衡解
102
针对攻防演化的均衡解，根据随机微分方程解的稳定性定理对攻防双方的策略选取状态进行稳定性分析，并输出均衡解中的网络安全防御策略
103

图2

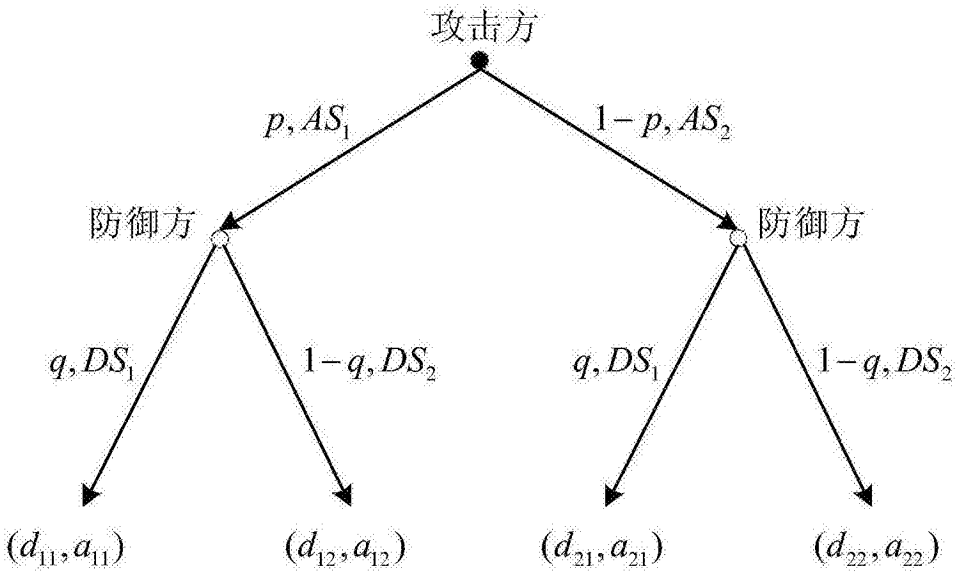

攻击方
p, AS_1
$1-p, AS_2$
防御方
防御方
q, DS_1
$1-q, DS_2$
q, DS_1
$1-q, DS_2$
(d_{11}, a_{11})
(d_{12}, a_{12})
(d_{21}, a_{21})
(d_{22}, a_{22})

图3

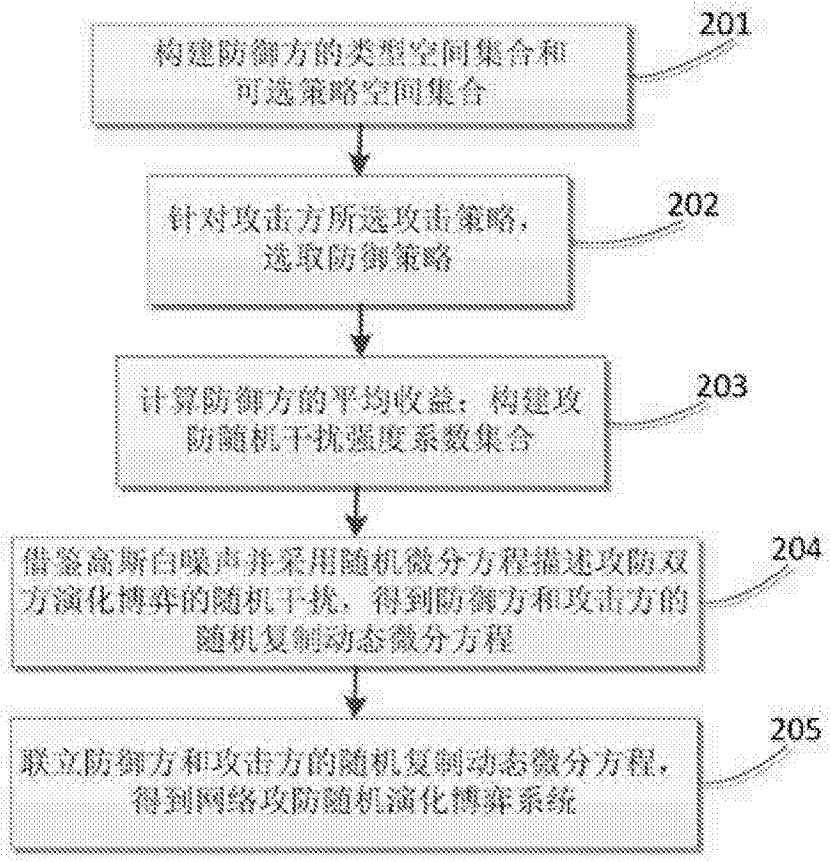

构建防御方的类型空间集合和可选策略空间集合
201
针对攻击方所选攻击策略，选取防御策略
202
计算防御方的平均收益；构建攻防随机干扰强度系数集合
203
借鉴高斯白噪声并采用随机微分方程描述攻防双方演化博弈的随机干扰，得到防御方和攻击方的随机复制动态微分方程
204
联立防御方和攻击方的随机复制动态微分方程，得到网络攻防随机演化博弈系统
205

图4

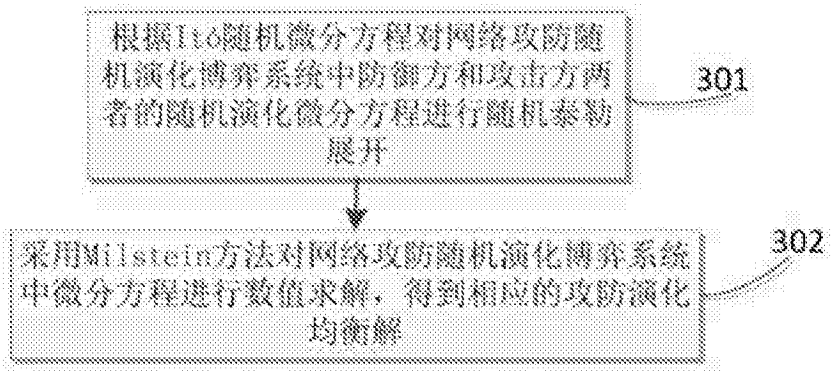

根据Ito随机微分方程对网络攻防随机演化博弈系统中防御方和攻击方两者的随机演化微分方程进行随机泰勒展开
301
采用Milstein方法对网络攻防随机演化博弈系统中微分方程进行数值求解，得到相应的攻防演化均衡解
302

图5

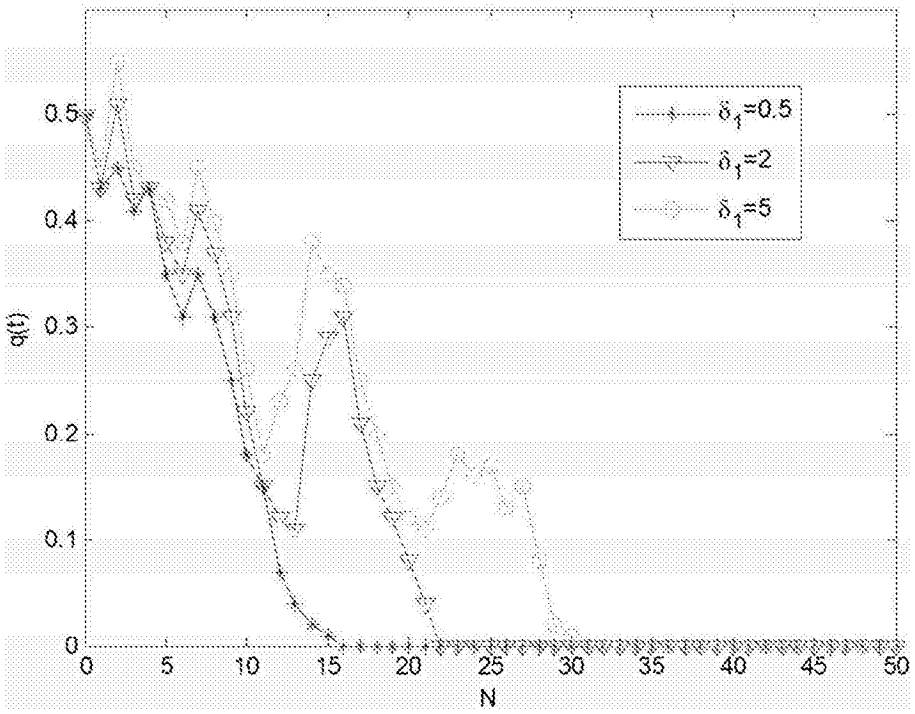

δ1=0.5
δ1=2
δ1=5
q(t)
N
0
0.1
0.2
0.3
0.4
0.5
0
5
10
15
20
25
30
35
40
45
50

图6

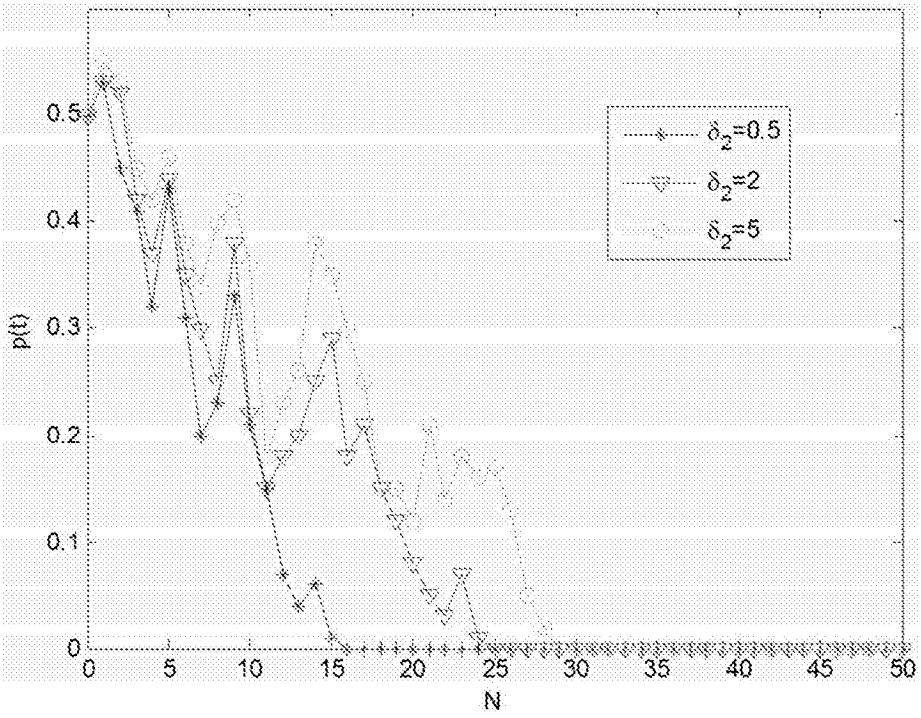


图7

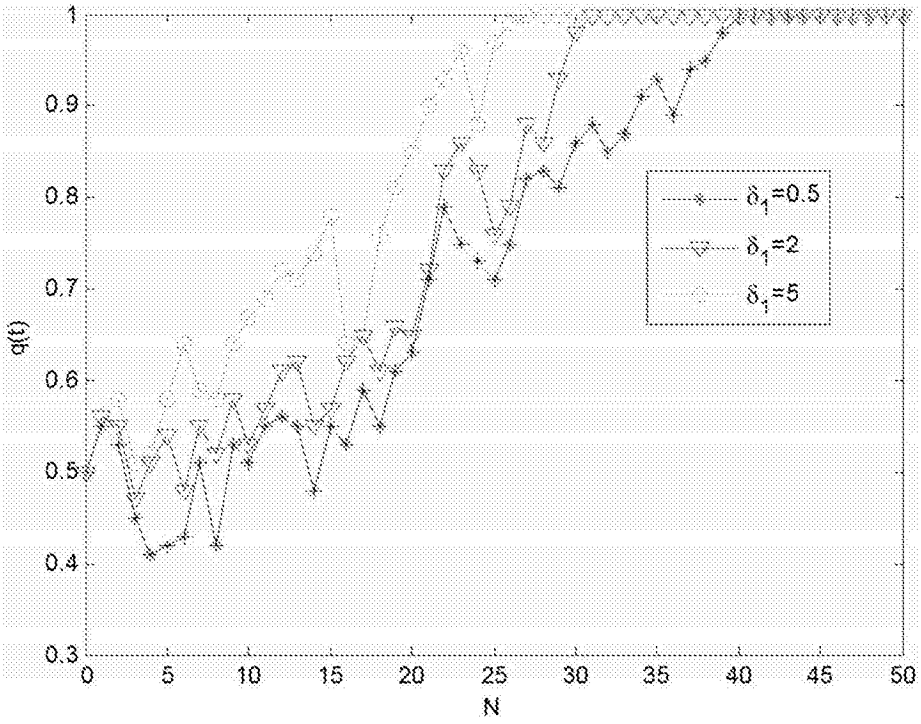


图8

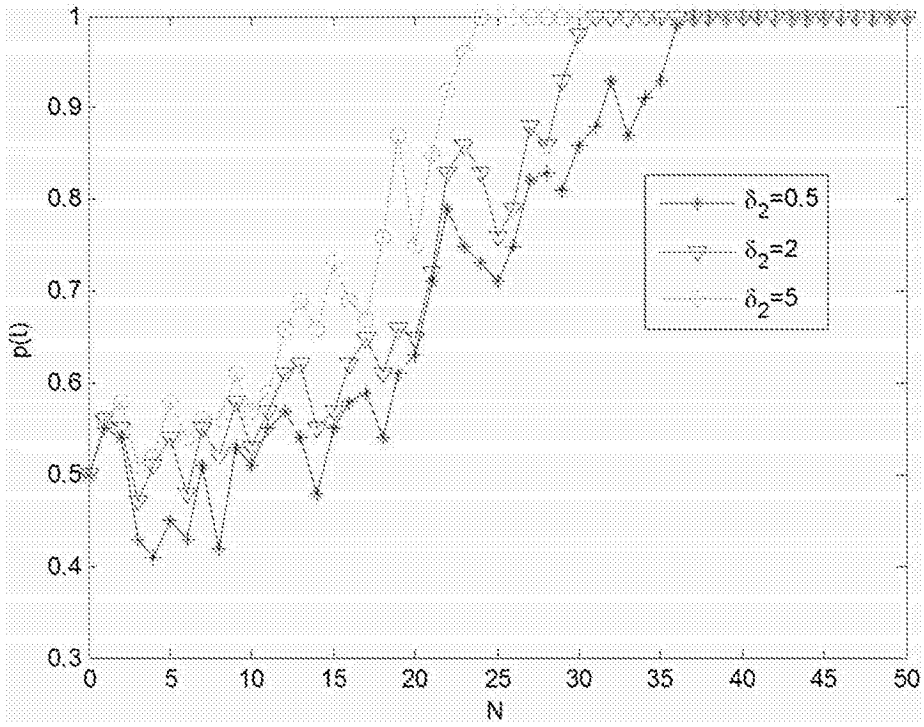


图9