(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 110417733 B
(45)授权公告日 2021.09.10

(21)申请号 201910549015.6

(22)申请日 2019.06.24

(65)同一申请的已公布的文献号
申请公布号 CN 110417733 A

(43)申请公布日 2019.11.05

(73)专利权人 中国人民解放军战略支援部队信息工程大学
地址 450000 河南省郑州市高新区科学大道62号

(72)发明人 谭晶磊 金辉 张红旗 杨英杰 刘小虎 雷程

(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)
H04L 12/24(2006.01)
G06N 20/00(2019.01)
G06N 5/04(2006.01)

(56)对比文件
US 9471777 B1,2016.10.18
US 2013318616 A1,2013.11.28
CN 106446674 A,2017.02.22
CN 107070956 A,2017.08.18
刘伟等.一种入侵防御系统性能分析方法.《信息网络安全》.2015,(第9期),

审查员 楼芃雯

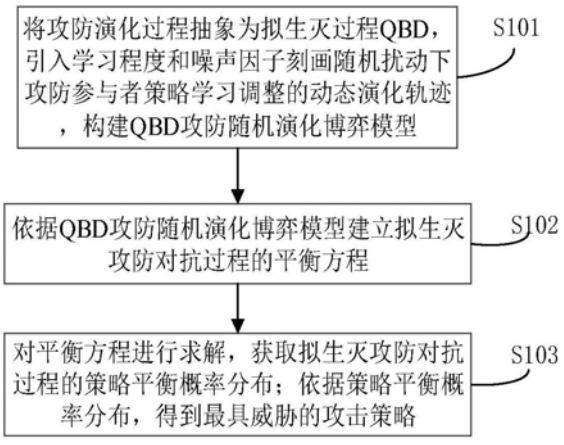
权利要求书2页 说明书11页 附图4页

(54)发明名称

基于QBD攻防随机演化博弈模型的攻击预测方法、装置及系统

(57)摘要

本发明属于网络安全技术领域,特别涉及一种基于QBD攻防随机演化博弈模型的攻击预测方法、装置及系统,该方法包含:将攻防演化过程抽象为拟生灭过程QBD,引入学习程度和噪声因子刻画随机扰动下攻防参与者策略学习调整的动态演化轨迹,构建QBD攻防随机演化博弈模型;依据QBD攻防随机演化博弈模型建立拟生灭攻防对抗过程的平衡方程;对平衡方程进行求解,获取拟生灭攻防对抗过程的策略平衡概率分布;依据策略平衡概率分布,得到最具威胁的攻击策略。本发明更贴近于实际攻防对抗场景,考虑攻防演化过程中随机扰动影响,提出拟生灭攻防随机演化博弈模型,增强预测攻击行为能力,提升攻击预测准确性和模型有效性,对于网络安全技术发展都具有重要指导意义。



CN 110417733 B

1.一种基于QBD攻防随机演化博弈模型的攻击预测方法,其特征在于,包含如下内容:

将攻防演化过程抽象为拟生灭过程QBD,引入学习程度和噪声因子刻画随机扰动下攻防参与者策略学习调整的动态演化轨迹,构建QBD攻防随机演化博弈模型;

依据QBD攻防随机演化博弈模型建立拟生灭攻防对抗过程的平衡方程;

对平衡方程进行求解,获取拟生灭攻防对抗过程的策略平衡概率分布;依据策略平衡概率分布,得到最具威胁的攻击策略;

其中,依据QBD攻防随机演化博弈模型,构造对应的拟生灭过程,获取拟生灭过程的状态空间,建立平衡方程;

建立平衡方程过程如下:首先,定义攻击者和防御者策略选择的转移概率;依据转移概率矩阵,构造出拟生灭攻防演化过程,得到攻防演化过程的平衡方程;

QBD攻防随机演化博弈模型通过七元组表示:QBD-ADSEGM=(Γ,N,S,x(t),α,β,U),其中,Γ表示攻防博弈群体,N表示攻防参与者数量,S表示攻防参与者策略空间,x(t)表示t时刻攻防状态空间,α表示攻防参与者学习程度集合,β表示攻防参与者噪声因子,U表示攻防双方受益函数集合。

2.根据权利要求1所述的基于QBD攻防随机演化博弈模型的攻击预测方法,其特征在于,攻防参与者学习程度集合包含用于描述攻击者对攻防信息掌握程度的学习参数和用于描述防御者对攻防信息掌握程度的学习参数;攻防参与者噪声因子,用来描述攻防过程中的随机扰动,并设定攻防参与者噪声因子大于0。

3.根据权利要求1所述的基于QBD攻防随机演化博弈模型的攻击预测方法,其特征在于,平衡状态求解过程中,首先对平衡方程进行初等变换并求解,由正常返条件获取QBD攻防演化过程平稳概率分布,从而得到攻防随机演化博弈的平稳概率分布。

4.根据权利要求3所述的基于QBD攻防随机演化博弈模型的攻击预测方法,其特征在于,依据平衡方程的非线性齐次方程组性质,采用高斯消元法对平衡方程进行初等变换。

5.根据权利要求3所述的基于QBD攻防随机演化博弈模型的攻击预测方法,其特征在于,平衡方程求解中,通过分析博弈群体间的对抗分析和相互学习,获取博弈信息,计算不同策略博弈产生的收益,以期望收益、学习程度和噪声因子决定转移概率。

6.一种基于QBD攻防随机演化博弈模型的攻击预测装置,其特征在于,包含:模型构建模块、方程建立模块和分析求解模块,其中,

模型建立模块,用于将攻防演化过程抽象为拟生灭过程QBD,引入学习程度和噪声因子刻画随机扰动下攻防参与者策略学习调整的动态演化轨迹,构建QBD攻防随机演化博弈模型;

方程建立模块,用于依据QBD攻防随机演化博弈模型建立拟生灭攻防对抗过程的平衡方程;

分析求解模块,用于对平衡方程进行求解,获取拟生灭攻防对抗过程的策略平稳概率分布;依据策略平稳概率分布,得到最具威胁的攻击策略;

其中,依据QBD攻防随机演化博弈模型,构造对应的拟生灭过程,获取拟生灭过程的状态空间,建立平衡方程;

建立平衡方程过程如下:首先,定义攻击者和防御者策略选择的转移概率;依据转移概率矩阵,构造出拟生灭攻防演化过程,得到攻防演化过程的平衡方程;

QBD攻防随机演化博弈模型通过七元组表示:QBD-ADSEGM＝(Γ,N,S,x(t),α,β,U),其中,Γ表示攻防博弈群体,N表示攻防参与者数量,S表示攻防参与者策略空间,x(t)表示t时刻攻防状态空间,α表示攻防参与者学习程度集合,β表示攻防参与者噪声因子,U表示攻防双方受益函数集合。

7.一种网络安全系统,其特征在于,包含权利要求6所述的基于QBD攻防随机演化博弈模型的攻击预测装置。

基于QBD攻防随机演化博弈模型的攻击预测方法、装置及系统

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QBD攻防随机演化博弈模型的攻击预测方法、装置及系统。

背景技术

[0002] 在网络安全领域中攻击者利用多种攻击手段对防御系统实施攻击获取更多有价值的信息资源，而防御者则针对攻击者的意图采取不同的防御手段对防御系统进行保护，防止信息资源被攻击者窃取。为了对信息系统进行有效防御，防御者需要事先对攻击行为进行准确预测以避免信息资源遭受巨大损失。网络攻防对抗过程中攻防双方所体现出的目标对立性、策略依存性和关系非合作性与博弈论的基本特征完美契合。因此，博弈论在网络安全领域的研究和应用已成为近年来各专家学者研究的重点和热点。

[0003] 目前，有关博弈论在网络安全领域的研究成果均基于完全理性的假设，认为博弈的攻防参与者完全掌握对手的可选策略及收益结构，通过求解纳什均衡，得到最优响应策略。但是，上述成果并没有考虑现实攻防参与者有限理性的特点，即攻防参与者具备的安全知识、技能水平和获取的博弈信息有限，决策时并不总是推理正确，也不可能在任何情况下根据决策环境的变化做出最优反应，理想化的完全理性假设与实际网络攻防情况不符，实用效果偏差。随着演化博弈理论在网络安全领域的研究和应用，以基于有限理性的演化博弈思想分析攻击行为预测和防御策略选取，更符合网络攻防对抗场景。演化博弈考虑攻防参与者有限理性的特点，通过策略的不断学习调整，参与者逐渐掌握决策环境、对手信息及不同策略博弈产生的收益差等信息，最终动态演化到稳定均衡状态。目前的研究中，从信息安全中的攻防成本出发，建立了信息安全攻防对抗演化博弈模型，根据攻防群体复制动态的关系，得出信息安全攻防对抗的演化稳定策略；结合演化博弈和系统动力学建立攻防演化博弈模型，从系统边界、有效性和参数灵敏度方面对模型进行检验，证明了模型具有客观性、科学性和实用性；从攻防参与者有限理性的角度出发研究防御策略选取问题，并构建攻防演化博弈模型，利用复制动态学习机制提出了演化稳定策略的求解方法并对其进行分析；建立物联网的多阶段攻防演化博弈模型，对攻防策略的收益/成本进行量化，并利用复制动态学习机制确定最优防御策略。然而，上述研究均基于复制动态学习机制，这是一种确定性的、无变异的自然选择学习模型，总是确定选择期望收益比平均收益高的策略。而实际攻防对抗过程在攻击行为和意图不确定、决策环境变化等随机扰动的影响下，确定性的复制动态机制难以准确估计和预测攻防动态演化。

发明内容

[0004] 为此，本发明提供一种基于QBD攻防随机演化博弈模型的攻击预测方法、装置及系统，更加贴近实际攻防对抗场景，增强预测攻击行为能力，提升攻击预测的准确性和有效性，具有很强的应用前景。

[0005] 按照本发明所提供的设计方案，一种基于QBD攻防随机演化博弈模型的攻击预测

方法,包含如下内容:

[0006] 将攻防演化过程抽象为拟生灭过程QBD,引入学习程度和噪声因子刻画随机扰动下攻防参与者策略学习调整的动态演化轨迹,构建QBD攻防随机演化博弈模型;

[0007] 依据QBD攻防随机演化博弈模型建立拟生灭攻防对抗过程的平衡方程;

[0008] 对平衡方程进行求解,获取拟生灭攻防对抗过程的策略平衡概率分布;依据策略平衡概率分布,得到最具威胁的攻击策略。

[0009] 上述的,QBD攻防随机演化博弈模型通过七元组表示:QBD-ADSEGM=(Γ,N,S,x(t),α,β,U),其中,Γ表示攻防博弈群体,N表示攻防参与者数量,S表示攻防参与者策略空间,x(t)表示t时刻攻防状态空间,α表示攻防参与者学习程度集合,β表示攻防参与者噪声因子,U表示攻防双方受益函数集合。

[0010] 上述的,攻防参与者学习程度集合包含用于描述攻击者对攻防信息掌握程度的学习参数和用于描述防御者对攻防信息掌握程度的学习参数;攻防参与者噪声因子,用来描述攻防过程中的随机扰动,并设定攻防参与者噪声因子大于0。

[0011] 上述的,依据QBD攻防随机演化博弈模型,构造对应的拟生灭过程,获取拟生灭过程的状态空间,建立平衡方程。

[0012] 上述的,建立平衡方程过程如下:首先,定义攻击者和防御者策略选择的转移概率;依据转移概率矩阵,构造出拟生灭攻防演化过程,得到攻防演化过程的平衡方程。

[0013] 上述的,平衡状态求解过程中,首先对平衡方程进行初等变换并求解,由正常返条件获取QBD攻防演化过程平稳概率分布,从而得到攻防随机演化博弈的平稳概率分布。

[0014] 优选的,依据平衡方程的非线性齐次方程组性质,采用高斯消元法对平衡方程进行初等变换。

[0015] 优选的,平衡方程求解中,通过分析博弈群体间的对抗分析和相互学习,获取博弈信息,计算不同策略博弈产生的收益,以期望收益、学习程度和噪声因子决定转移概率。

[0016] 进一步地,本发明还提供一种基于QBD攻防随机演化博弈模型的攻击预测装置,包含:模型构建模块、方程建立模块和分析求解模块;其中,

[0017] 模型建立模块,用于将攻防演化过程抽象为拟生灭过程QBD,引入学习程度和噪声因子刻画随机扰动下攻防参与者策略学习调整的动态演化轨迹,构建QBD攻防随机演化博弈模型;

[0018] 方程建立模块,用于依据QBD攻防随机演化博弈模型建立拟生灭攻防对抗过程的平衡方程;

[0019] 分析求解模块,用于对平衡方程进行求解,获取拟生灭攻防对抗过程的策略平稳概率分布;依据策略平稳概率分布,得到最具威胁的攻击策略。

[0020] 进一步地,本发明还提供一种网络安全系统,包含上述的基于QBD攻防随机演化博弈模型的攻击预测装置。

[0021] 本发明的有益效果:

[0022] 本发明引入学习程度参数和噪声因子,刻画在随机扰动下攻防参与者策略学习调整的动态演化轨迹,通过建立拟生灭攻防对抗过程的平衡方程,求解拟生灭攻防演化过程的策略平稳概率分布给出最具威胁的攻击策略;针对攻防群体在博弈过程中受随机扰动的影响,通过引入学习程度参数和噪声因子,基于拟生灭过程对攻防随机演化博弈进行建模,

对所构建的攻防博弈拟生灭过程的平衡方程进行求解，得到攻防群体极限情况下策略的平稳概率分布，从而可知最具威胁的攻击策略，达到攻击预测的效果；更贴近于实际攻防对抗场景，考虑攻防演化过程中随机扰动的影响，提出拟生灭攻防随机演化博弈模型，增强预测攻击行为的能力，并通过仿真实验验证攻击预测的准确性和模型的有效性，对于网络安全技术发展都具有重要的指导意义。

附图说明：

[0023] 图1为实施例中攻击预测方法流程示意图；

[0024] 图2为实施例中攻击预测装置示意图；

[0025] 图3为实施例中网络信息实验系统拓扑图；

[0026] 图4为实施例中α＝0.1时攻击群体的平稳概率分布；

[0027] 图5为实施例中α＝0.1时防御群体的平稳概率分布；

[0028] 图6为实施例中不同α取值下使用攻击策略A_1的平稳概率分布；

[0029] 图7为实施例中不同α取值时使用防御策略D_1的平稳概率分布；

[0030] 图8为实施例中β取不同值时攻击群体的平稳概率分布；

[0031] 图9为实施例中β取不同值时防御群体的平稳概率分布。

具体实施方式：

[0032] 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。

[0033] 针对现有实际攻防对抗过程在攻击行为和意图不确定、决策环境变化等随机扰动的影响下，确定性的复制动态机制难以准确估计和预测攻防动态演化等的情形，本发明实施例，参见图1所示，提供一种基于QBD攻防随机演化博弈模型的攻击预测方法，包含如下内容：

[0034] S101、将攻防演化过程抽象为拟生灭过程QBD，引入学习程度和噪声因子刻画随机扰动下攻防参与者策略学习调整的动态演化轨迹，构建QBD攻防随机演化博弈模型；

[0035] S102、依据QBD攻防随机演化博弈模型建立拟生灭攻防对抗过程的平衡方程；

[0036] S103、对平衡方程进行求解，获取拟生灭攻防对抗过程的策略平衡概率分布；依据策略平衡概率分布，得到最具威胁的攻击策略。

[0037] 拟生灭过程以二维随机变量$x(t)=(x_A(t),x_D(t))$定义状态，描述攻防群体中参与者使用各自某一策略的人数，通过使用策略的人数变化(增加、减少或者不变)刻画状态转移过程。第t+1次博弈，攻防参与者根据第t次博弈群体间的对抗分析和群体内的相互学习，直接或间接地获取博弈信息，计算不同策略博弈产生的收益，以期望收益、学习程度和噪声因子决定的转移概率随机地选取高收益策略，则使用高收益策略的参与者数量增加，其中学习程度描述攻防参与者对决策环境、对手信息及不同策略博弈产生的收益差等信息的掌握程度，噪声因子刻画攻防过程中的随机扰动。经过多次博弈之后，随着参与者学习程度的提升，在策略学习调整的机制下，直到状态空间上的策略概率分布趋近于稳定，即平稳概率分布，是群体行为意义上纳什均衡的实现，随着时间的推移，攻防参与者经过策略博弈、学习、改进，最终群体中各个策略选取的比例达到稳定状态，其概率越大，说明在群体中演化

稳定策略的认同度越高。

[0038] 进一步地，本发明实施例中，QBD攻防随机演化博弈模型通过七元组表示：QBD-ADSEGM＝(Γ,N,S,x(t),α,β,U)，其中，

[0039] 1)Γ＝(attackers,defenders)表示参与博弈的群体，attackers表示攻击群体，defenders表示防御群体；

[0040] 2)N＝(N_A,N_D)表示博弈参与者的数量，N_A表示攻击群体中攻击者的数量，N_D表示防御群体中防御者的数量；

[0041] 3)S＝(S_A,S_D)表示攻防参与者的策略空间，其中攻击策略集S_A＝{A_1,A_2,…,A_m}，防御策略集S_D＝{D_1,D_2,…,D_n}，m和n表示攻防策略数量，满足m,n∈Z且m,n≥2；

[0042] 4)$\chi(t)=(\chi_A^i(t),\chi_D^j(t))$表示t时刻的攻防演化的状态空间，是一个二维随机变量，其中$\chi_A^i(t)$表示攻击群体中选择策略A_i的攻击者数量，满足$\sum_{i=1}^{m}\chi_A^i(t)=N_A$且$0\le\chi_A^i(t)\le N_A,1\le i\le m$，$\chi_D^j(t)$表示防御群体中选择策略$D_j$的防御者数量，满足$\sum_{j=1}^{n}\chi_D^j(t)=N_D$且$0\le\chi_D^j(t)\le N_D,1\le j\le n$，状态空间x(t)的规模为($N_A$+1)($N_D$+1)；

[0043] 5)α＝(α_1,α_2)表示攻防参与者的学习程度集合，用于描述攻防参与者对决策环境、对手信息及不同策略博弈产生的收益差等信息的掌握程度，其中α_1是攻击者的学习程度，α_2是防御者的学习程度，且满足α_1∈[0,2]，α_2∈[0,2]；

[0044] 6)β表示攻防参与者的噪声因子，用来描述攻防过程中的随机扰动，满足β＞0；

[0045] 7)U＝(U_A,U_D)是攻防双方收益函数的集合，它由攻防双方的策略共同决定，不同的攻防策略组合所获得的收益也不同。

[0046] 当攻击者采用策略A_i，防御者采用策略D_j时，攻击者和防御者的策略收益分别用a_{ij}和d_{ij}表示。由此可得，攻击者在博弈中使用策略A_i的期望收益为$U_{A_i}(\chi(t))$和防御者在博弈中使用策略D_j的期望收益$U_{D_j}(\chi(t))$。

[0047] $$U_{A_i}(\chi(t))=\sum_{j=1}^{n}\frac{a_{ij}\chi_D^j(t)}{N_D},1\le i\le m \tag{1}$$

[0048] $$U_{D_j}(\chi(t))=\sum_{i=1}^{m}\frac{d_{ij}\chi_A^i(t)}{N_A},1\le j\le n \tag{2}$$

[0049] 并且在攻防参与者对对手博弈信息不确定的情况下，均以策略$\psi_A(t)$,$\psi_D(t)$参与博弈，即：

[0050] $$\psi_D(t)=(\frac{\chi_D^1(t)}{N_D}D_1,\cdots\frac{\chi_D^j(t)}{N_D}D_j,\cdots,\frac{\chi_D^n(t)}{N_D}D_n) \tag{3}$$

[0051] $$\psi_A(t)=(\frac{\chi_A^1(t)}{N_A}A_1,\cdots\frac{\chi_A^i(t)}{N_A}A_i,\cdots,\frac{\chi_A^m(t)}{N_A}A_m) \tag{4}$$

[0052] 进一步地，本发明实施例中，依据QBD攻防随机演化博弈模型，构造对应的拟生灭过程，获取拟生灭过程的状态空间，建立平衡方程。

[0053] 根据QBD攻防随机演化博弈模型，构造出与其对应的拟生灭过程，记为{x(t),t≥0,$\chi(t)=(\chi_A^i(t),\chi_D^j(t))$}。由此可知这个拟生灭过程的状态空间为：Θ＝{(0,0),(0,1),...(0,

N_D)；(1,0)，(1,1)，...(1,N_D)；...；(N_A,0)，(N_A,1)，...(N_A,N_D)}。

[0054] 进一步地，本发明实施例中，建立平衡方程过程如下：首先，定义攻击者和防御者策略选择的转移概率；依据转移概率矩阵，构造出拟生灭攻防演化过程，得到攻防演化过程的平衡方程。

[0055] 首先，定义攻击者策略选择的转移概率$\varphi_\beta^A(\theta_1)$， $\rho_\beta^A(\theta_1)$。

[0056] $$\varphi_\beta^A(\theta_1)=\beta+\alpha_1*\max\left\{U_{A_i}(\theta_1)-U_{A_{-i}}(\theta_1),0\right\},\ \theta_1\in\{0,1,\ldots,N_D\} \tag{5}$$

[0057] $$\rho_\beta^A(\theta_1)=\beta+\alpha_1*\max\left\{U_{A_{-i}}(\theta_1)-U_{A_i}(\theta_1),0\right\},\ \theta_1\in\{0,1,\ldots,N_D\} \tag{6}$$

[0058] 其中，$A_{-i}=(A_1,\cdots,A_{i-1},A_{i+1},\cdots,A_m)$表示除i之外的所有攻击策略组成的向量，$U_{A_{-i}}(\theta_1)=\max\left\{U_{A_1}(\theta_1),\cdots,U_{A_{i-1}}(\theta_1),U_{A_{i+1}}(\theta_1),\cdots,U_{A_m}(\theta_1)\right\}$表示$A_i$之外的其它策略的期望收益中的最大值，$\varphi_\beta^A(\theta_1)$表示选取策略$A_{-i}$的攻击者将改变策略，转而选取策略$A_i$的概率，$\rho_\beta^A(\theta_1)$表示选取策略$A_i$的攻击者改变策略，转而选取策略$A_{-i}$的概率。

[0059] 同理，防御者策略选择的转移概率$\varphi_\beta^D(\theta_2)$， $\rho_\beta^D(\theta_2)$。

[0060] $$\varphi_\beta^D(\theta_2)=\beta+\alpha_2*\max\left\{U_{D_j}(\theta_2)-U_{D_{-j}}(\theta_2),0\right\},\ \theta_2\in\{0,1,\ldots,N_A\} \tag{7}$$

[0061] $$\rho_\beta^D(\theta_2)=\beta+\alpha_2*\max\left\{U_{D_{-j}}(\theta_2)-U_{D_j}(\theta_2),0\right\},\ \theta_2\in\{0,1,\ldots,N_A\} \tag{8}$$

[0062] 其中，$\varphi_\beta^D(\theta_2)$表示选取策略$D_j$的防御者将改变策略，转而选取策略$D_{-j}$的概率，$\rho_\beta^D(\theta_2)$表示选取策略$D_{-j}$的防御者将改变策略，转而选取策略$D_j$的概率。

[0063] 则拟生灭攻防演化过程$\chi(t)=(\chi_A^j(t),\chi_D^j(t))$的转移概率矩阵为：

[0064] $$Q_\beta=\begin{bmatrix} C_1^0(\beta) & C_0^0(\beta) & & & \\ C_2^1(\beta) & C_1^1(\beta) & C_0^1(\beta) & & \\ \ddots & \ddots & \ddots & & \\ & C_2^{N_A-1}(\beta) & C_1^{N_A-1}(\beta) & C_0^{N_A-1}(\beta) & \\ & & C_2^{N_A}(\beta) & C_1^{N_A}(\beta) \end{bmatrix} \tag{9}$$

[0065] 上述矩阵中，$C_1^k(\beta),0\le k\le N_A$表示矩阵$Q_\beta$主对角线上的子矩阵，记为：

[0066] $$C_1^k(\beta)=\begin{bmatrix} -\gamma(k,0) & \varphi_\beta^D(k) & & & \\ \rho_\beta^D(k) & -\gamma(k,1) & \varphi_\beta^D(k) & & \\ & \ddots & \ddots & \ddots & \\ & & \rho_\beta^D(k) & -\gamma(k,N_D-1) & \varphi_\beta^D(k) \\ & & & \rho_\beta^D(k) & -\gamma(k,N_D) \end{bmatrix} \tag{10}$$

[0067] 当k＝0时，记：

[0068] $$\gamma(k,l)=\begin{cases} \varphi_\beta^D(l)+\varphi_\beta^A(l), l=0 \\ \rho_\beta^D(k)+\varphi_\beta^D(k)+\varphi_\beta^A(l), 1\le l\le N_D-1 \\ \rho_\beta^D(k)+\varphi_\beta^A(l), l=N_D \end{cases} \tag{11}$$

[0069] 当1≤k≤N_A-1时，记：

[0070] $$\gamma(k,l)=\begin{cases}\varphi_\beta^D(k)+\varphi_\beta^A(l)+\rho_\beta^A(l),l=0\\ \rho_\beta^D(k)+\varphi_\beta^D(k)+\varphi_\beta^A(l)+\rho_\beta^A(l),1\le l\le N_D-1\\ \rho_\beta^D(k)+\varphi_\beta^A(l)+\rho_\beta^A(l),l=N_D\end{cases} \tag{12}$$

[0071] 当k＝N_A时，记：

[0072] $$\gamma(k,l)=\begin{cases}\varphi_\beta^D(k)+\rho_\beta^A(l),l=0\\ \rho_\beta^D(k)+\varphi_\beta^D(k)+\rho_\beta^A(l),1\le l\le N_D-1\\ \rho_\beta^D(k)+\rho_\beta^A(l),l=N_D\end{cases} \tag{13}$$

[0073] 此外，$C_0^{r_1}(\beta),0\le r_1\le N_A-1$是矩阵$Q_\beta$右上次对角线的子矩阵，记为：

[0074] $$C_0^{r_1}(\beta)=\begin{bmatrix}\varphi_\beta^A(0) & & & \\ & \varphi_\beta^A(1) & & \\ & & \ddots & \\ & & & \varphi_\beta^A(N_D)\end{bmatrix} \tag{14}$$

[0075] $C_2^{r_2}(\beta),1\le r_2\le N_A$表示矩阵$Q_\beta$左下次对角线的子矩阵，记为：

[0076] $$C_2^{r_2}(\beta)=\begin{bmatrix}\rho_\beta^A(0) & & & \\ & \rho_\beta^A(1) & & \\ & & \ddots & \\ & & & \rho_\beta^A(N_D)\end{bmatrix} \tag{15}$$

[0077] 进一步地，本发明实施例中，平衡状态求解过程中，首先对平衡方程进行初等变换并求解，由正常返条件获取QBD攻防演化过程平稳概率分布，从而得到攻防随机演化博弈的平衡概率分布。优选的，依据平衡方程的非线性齐次方程组性质，采用高斯消元法对平衡方程进行初等变换。优选的，平衡方程求解中，通过分析博弈群体间的对抗分析和群体内的相互学习，获取博弈信息，计算不同策略博弈产生的收益，以期望收益、学习程度和噪声因子决定转移概率。

[0078] 令$P(\beta)=(p_0,p_1,\ldots,p_{N_A-1},p_{N_A})$表示QBD的平稳概率分布，其中$p_k=(p_k^0,p_k^1,\ldots,p_k^{N_D-1},p_k^{N_D})$。假定QBD过程正常返，则平衡方程P(β)$Q_\beta$＝0，P(β)e＝1，并且可知$Q_\beta^TP^T(\beta)=0$。为方便理解，令$R_k=C_1^k(\beta),0\le k\le N_A$，$H_{r_1}=C_0^{r_1}(\beta),1\le r_1\le N_A$，$B_{r_2}=C_2^{r_2}(\beta),1\le r_2\le N_A$，则平衡方程等价于

[0079] $$\begin{cases}R_0^Tp_0^T+B_1^Tp_1^T=0\\ H_{i-1}^Tp_{i-1}^T+R_i^Tp_i^T+B_{i+1}^Tp_{i+1}^T=0\\ H_{N_A-1}^Tp_{N_A-1}^T+R_{N_A}^Tp_{N_A}^T=0\\ \sum_{i=0}^{N_A}p_i^T=1\end{cases} \tag{16}$$

[0080] 本发明实施例中所构建的平衡方程实际是一个非线性齐次方程组，通过采用基于分块矩阵的Guass消元法，对平衡方程进行初等变换，求解QBD平衡方程，由正常返的条件可知P(β)为QBD平稳概率分布，从而得到攻防随机演化博弈的长期稳定均衡。

[0081] 进一步地，本发明实施例还提供一种基于QBD攻防随机演化博弈模型的攻击预测装置，参见图2所示，包含：模型构建模块101、方程建立模块102和分析求解模块103，其中，

[0082] 模型建立模块101，用于将攻防演化过程抽象为拟生灭过程QBD，引入学习程度和噪声因子刻画随机扰动下攻防参与者策略学习调整的动态演化轨迹，构建QBD攻防随机演化博弈模型；

[0083] 方程建立模块102，用于依据QBD攻防随机演化博弈模型建立拟生灭攻防对抗过程的平衡方程；

[0084] 分析求解模块103，用于对平衡方程进行求解，获取拟生灭攻防对抗过程的策略平衡概率分布；依据策略平衡概率分布，得到最具威胁的攻击策略。

[0085] 进一步地，本发明实施例还提供一种网络安全系统，包含上述实施例中的基于QBD攻防随机演化博弈模型的攻击预测装置，用于对网络系统中的攻击行为进行预测分析。

[0086] 为验证本发明实施例中提出的QBD随机演化博弈模型的有效性和攻击预测的准确性，在特定的网络信息系统环境进行实验，如图3所示，网络系统环境主要由外网攻击群、DMZ域和内网组成，其中网络安全防护设备有防火墙、入侵防御设备和堡垒主机，用于保护内网的数据库服务器，防止数据资源被窃取。通过Nessus对系统环境进行扫描，参照美国MIT的攻防行为数据库，根据国家信息安全漏洞库(CNNVD)信息，设计实验中采用的攻防策略集，即攻击策略为A_1(数据库监听)和A_2(端口扫描攻击)，防御策略为D_1(数据库升级)和D_2(关闭闲置的端口服务)。

[0087] 基于建立的QBD随机演化博弈模型，考虑到攻防参与者有限理性的特点，在追求信息安全的风险和投入之间均衡的前提下，使各自的收益最大化，由此，参考收益量化方法，结合拟生灭过程的特点，计算不同攻防策略博弈产生的收益，可得表1的攻防策略收益矩阵。

[0088] 表1攻防策略收益矩阵

[0089]

策略收益矩阵		防御者	
		D_1	D_2
攻击者	A_1	$a_{11}=10,\ d_{11}=15$	$a_{12}=-10,\ d_{12}=10$
	A_2	$a_{21}=2,\ d_{21}=8$	$a_{22}=0,\ d_{22}=-30$

[0090] 并且假设攻击者的数量为$N_A=8$，防御者的数量为$N_D=10$。

[0091] 考虑攻防对抗过程中受到一定随机扰动的影响，假定噪声因子$\beta=0.5$。在这样的仿真场景下，通过改变学习程度参数α_i(i＝1,2)，观察攻防双方学习程度的提升对攻击预测的影响，即当$\alpha_1=\alpha_2=\alpha=0.1,0.5,1.0,2.0$时，研究攻防双方博弈的演化规律。

[0092] 求解本组QBD攻防随机演化博弈模型的平稳概率分布。当$\alpha=0.1$，通过计算可得平稳概率分布的P矩阵为：

$$P=\begin{bmatrix} p_0^0 & p_1^0 & p_2^0 & \cdots & p_{N_A}^0 \\ p_0^1 & p_1^1 & p_2^1 & \cdots & p_{N_A}^1 \\ p_0^2 & p_1^2 & p_2^2 & \cdots & p_{N_A}^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ p_0^{N_D} & p_1^{N_D} & p_2^{N_D} & \cdots & p_{N_A}^{N_D} \end{bmatrix}$$

[0093]

$$=\begin{bmatrix} 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 \\ 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 \\ 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 \\ 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0001 & 0.0001 & 0.0001 \\ 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0001 & 0.0001 & 0.0003 & 0.0004 \\ 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0001 & 0.0001 & 0.0004 & 0.0009 & 0.0016 \\ 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0001 & 0.0003 & 0.0010 & 0.0026 & 0.0053 \\ 0.0000 & 0.0000 & 0.0000 & 0.0001 & 0.0002 & 0.0008 & 0.0025 & 0.0072 & 0.0166 \\ 0.0000 & 0.0000 & 0.0001 & 0.0002 & 0.0007 & 0.0022 & 0.0069 & 0.0197 & 0.0492 \\ 0.0000 & 0.0001 & 0.0003 & 0.0009 & 0.0026 & 0.0074 & 0.0203 & 0.0546 & 0.1399 \\ 0.0003 & 0.0006 & 0.0020 & 0.0051 & 0.0127 & 0.0300 & 0.0694 & 0.1590 & 0.3748 \end{bmatrix}$$

[0094] 设：

[0095]

$$\begin{cases} prob\{\chi_A^1(\infty)=i\}=\sum_{j=0}^{j=N_D} p_i^j, i=0,1,2,\ldots,N_A \\ prob\{\chi_D^1(\infty)=j\}=\sum_{i=0}^{i=N_A} p_i^j, j=0,1,2,\ldots,N_D \end{cases} \tag{17}$$

[0096] 其中，p_i^j表示攻击群体中采用策略A_1的攻击者数量为i，同时防御群体中选取策略D_1的防御者数量为j的平稳概率。$prob\{\chi_A^1(\infty)=i\}$表示多次博弈后攻击群体中采用策略$A_1$的攻击者数量为i的平稳概率；$prob\{\chi_D^1(\infty)=j\}$表示多次博弈后防御群体中采用策略$D_1$的防御者数量为j的平稳概率。由此可得攻防群体演化博弈的策略平稳概率分布如图4和5所示，其中，图4为α＝0.1时攻击群体的平稳概率分布，图5为α＝0.1时防御群体的平稳概率分布

[0097] 图4中攻击群体的平稳概率分布，横坐标表示攻击者的数量，即选择策略A_1或者A_2的攻击者数量，纵坐标表示策略A_1的平稳概率。α＝0.1时，攻击群体中所有攻击者选择策略A_1的概率仅为58.79％，也就是说，7个攻击者选取策略A_1但有1个攻击者选取策略A_2的概率为24.44％，有6个攻击者选取策略A_1但有2个攻击者选取策略A_2的概率为10.07％。因此，数值结果表明攻击策略选取产生了显著的分歧。同理，由图5可知，所有防御者选择策略D_1的概率仅为65.39％，而其中有1个防御者选取策略D_2的概率为22.61％，策略选取明显不一致。

[0098] 同理可得，当α＝α_1＝α_2＝0.1,0.5,1.0,2.0时，即攻防群体演化博弈在不同学习程度参数下的平稳概率分布结果，见表2和表3。其中$\chi_A^1(\infty)=i(i=0,1,...,N_A)$表示攻击群体中选取策略$A_1$的攻击者数量为i；$\chi_D^1(\infty)=j(j=0,1,...,N_D)$表示防御群体中选取策略$D_1$的防御者数量为j。

[0099] 表2在不同学习程度参数下，攻击群体演化博弈的平稳概率分布结果

[0100]

α_1 \ $\chi_A^1(\infty)$	0	1	2	3	4	5	6	7	8
$\alpha=0.1$	0.0003	0.0007	0.0024	0.0063	0.0164	0.0409	0.1007	0.2444	0.5879
$\alpha=0.5$	0.0000	0.0000	0.0000	0.0000	0.0001	0.0013	0.0115	0.1010	0.8861
$\alpha=1.0$	0.0000	0.0000	0.0000	0.0000	0.0000	0.0002	0.0033	0.0561	0.9404
$\alpha=2.0$	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0009	0.0297	0.9694

[0101] 表3在不同学习程度参数下,防御群体演化博弈的平稳概率分布结果

[0102]

α_2 \ $\chi_D^1(\infty)$	0	1	2	3	4	5	6	7	8	9	10
$\alpha=0.1$	0.0000	0.0000	0.0000	0.0003	0.0009	0.0031	0.0093	0.0274	0.0790	0.2261	0.6539
$\alpha=0.5$	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0001	0.0015	0.0123	0.1043	0.8818
$\alpha=1.0$	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0002	0.0039	0.0606	0.9353
$\alpha=2.0$	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0011	0.0328	0.9661

[0103] 通过Matlab2016b仿真得到如图6和7所示的不同学习程度参数下的攻防群体演化的平稳概率分布图,可以直观地分析和比较表2、表3所示的两组数值结果。

[0104] 根据学习程度α在区间[0,2]的取值变化,由图6和7可以看出,攻防群体中选取攻击策略A_1和选取防御策略D_1分别对应的平稳概率分布变化趋势。当α趋向于2时,攻击策略选取收敛于最优策略A_1,防御策略选取收敛于最优策略D_1,即攻击群体中所有攻击者选取策略A_1的概率为96.94%(误差小于5%),而防御群体中所有防御者选取策略D_1的概率为96.61%(误差小于5%)。

[0105] 由上述数值结果可以得出以下结论:通过群体间的对抗分析和同一群体内的相互学习,收集并分析博弈信息,逐渐增强了攻防参与者对对手行为和意图以及决策环境的了解。随着学习程度α的提升,选取最优攻击策略A_1达到了稳定,从而可知攻击策略A_1为预测到的最具威胁的攻击策略。当α值较小时,表明攻防参与者缺乏对博弈结果和决策环境的了解,如果攻防决策过程中有明显的随机性,则演化博弈的平稳概率分布不一定收敛于某一特定的策略。

[0106] 假定学习程度为固定常数$\alpha_1=\alpha_2=0.7$,$\beta=0.2,1.2,2.2,5.0$,在这样的仿真场景下,观察不同噪声因子β对攻防双方博弈演化的影响。求解该组模型所对应的拟生灭过程的平稳概率分布,可得到在不同噪声因子下,攻防群体的内部演化博弈结果如表4、表5所示。

[0107] 表4在不同噪声因子下,攻击群体演化博弈的平稳概率分布结果

[0108]

β \ $\chi_A^1(\infty)$	0	1	2	3	4	5	6	7	8
$\beta=0.2$	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0011	0.0336	0.9653
$\beta=1.2$	0.0000	0.0000	0.0000	0.0001	0.0009	0.0050	0.0272	0.1501	0.8167
$\beta=2.2$	0.0000	0.0001	0.0004	0.0015	0.0052	0.0185	0.0626	0.2103	0.7014
$\beta=5.0$	0.0013	0.0026	0.0068	0.0150	0.0318	0.0649	0.1296	0.2541	0.4939

[0109] 表5在不同噪声因子下,防御群体演化博弈的平稳概率分布结果

[0110]

β \ $\chi_D^1(\infty)$	0	1	2	3	4	5	6	7	8	9	10
$\beta = 0.2$	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0001	0.0014	0.0370	0.9615
$\beta = 1.2$	0.0000	0.0000	0.0000	0.0000	0.0000	0.0001	0.0008	0.0048	0.0266	0.1479	0.8198
$\beta = 2.2$	0.0000	0.0000	0.0000	0.0000	0.0002	0.0010	0.0038	0.0143	0.0534	0.1969	0.7304
$\beta = 5.0$	0.0000	0.0000	0.0003	0.0009	0.0024	0.0065	0.0162	0.0403	0.0982	0.2401	0.5951

[0111] 图8和图9可直观地得出攻防群体的内部演化规律。当β＝0.2时，攻击者(防御者)的行为受随机扰动的影响较小，策略选取具有高度一致性，即攻击群体中所有攻击者选择策略A_1的概率为96.53％，防御群体中所有防御者选取D_1的概率为96.15％。然而，随着β逐渐增大，当β＝5.0时，受随机扰动的影响明显，群体中的攻击者在策略选取上产生分歧。攻击群体中所有攻击者选择A_1的概率仅有49.39％，有1个攻击者选择策略A_2的概率为25.41％，有2个攻击者选择A_2的概率为12.96％；同样地，防御群体的数据结果也表明，β＝5.0时，所有防御者采用策略D_1的概率仅有59.51％，而群体中有1个防御者选择策略D_2的概率为24.01％，策略选取明显不一致。

[0112] 本发明针对攻防群体在博弈过程中受随机扰动的影响，通过引入学习程度参数和噪声因子，基于拟生灭过程对攻防随机演化博弈进行建模，利用Gauss消元法对所构建的攻防博弈拟生灭过程的平衡方程进行求解，得到攻防群体极限情况下策略的平稳概率分布，从而可知最具威胁的攻击策略，达到攻击预测的效果。研究结果表明，随着攻防演化的推进，攻防群体通过收集对方博弈特征信息，逐步加深对决策环境和对手的了解，学习程度不断增强，在参与者选择策略方面没有出现明显的分歧，所有参与者倾向于选择演化稳定的策略。但是，随着随机扰动的增强，使博弈系统趋于不稳定，博弈结果主要受到随机扰动的影响，攻防群体在策略选择上出现明显分歧。在实际攻防场景中，随机因素不可避免，但尽可能地降低随机因素的影响，增强学习程度，对于指导实际网络攻击预测具有指导性意义。

[0113] 除非另外具体说明，否则在这些实施例中阐述的部件和步骤的相对步骤、数字表达式和数值并不限制本发明的范围。

[0114] 基于上述的方法，本发明实施例还提供一种服务器，包括：一个或多个处理器；存储装置，用于存储一个或多个程序，当所述一个或多个程序被所述一个或多个处理器执行，使得所述一个或多个处理器实现上述的方法。

[0115] 基于上述的方法，本发明实施例还提供一种计算机可读介质，其上存储有计算机程序，其中，该程序被处理器执行时实现上述的方法。

[0116] 本发明实施例所提供的装置，其实现原理及产生的技术效果和前述方法实施例相同，为简要描述，装置实施例部分未提及之处，可参考前述方法实施例中相应内容。

[0117] 所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统和装置的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

[0118] 所述功能如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个处理器可执行的非易失的计算机可读取存储介质中。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备(可以是个人计算机，服务器，或者网络设备等)执行本发明各个实施例所

述方法的全部或部分步骤。而前述的存储介质包括:U盘、移动硬盘、只读存储器(ROM,Read-Only Memory)、随机存取存储器(RAM,Random Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

[0119] 最后应说明的是:以上所述实施例,仅为本发明的具体实施方式,用以说明本发明的技术方案,而非对其限制,本发明的保护范围并不局限于此,尽管参照前述实施例对本发明进行了详细的说明,本领域的普通技术人员应当理解:任何熟悉本技术领域的技术人员在本发明揭露的技术范围内,其依然可以对前述实施例所记载的技术方案进行修改或可轻易想到变化,或者对其中部分技术特征进行等同替换;而这些修改、变化或者替换,并不使相应技术方案的本质脱离本发明实施例技术方案的精神和范围,都应涵盖在本发明的保护范围之内。因此,本发明的保护范围应所述以权利要求的保护范围为准。

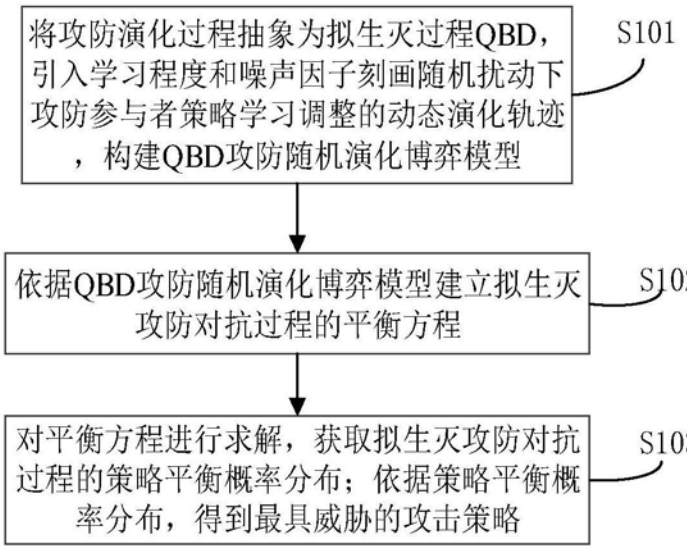

将攻防演化过程抽象为拟生灭过程QBD，引入学习程度和噪声因子刻画随机扰动下攻防参与者策略学习调整的动态演化轨迹，构建QBD攻防随机演化博弈模型
S101
依据QBD攻防随机演化博弈模型建立拟生灭攻防对抗过程的平衡方程
S102
对平衡方程进行求解，获取拟生灭攻防对抗过程的策略平衡概率分布；依据策略平衡概率分布，得到最具威胁的攻击策略
S103

图1

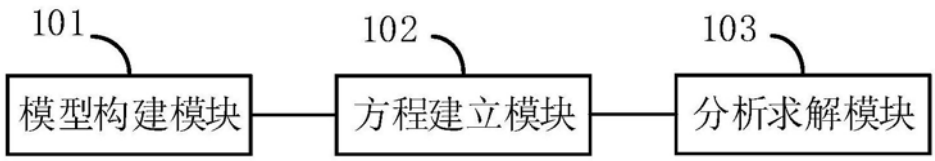

101
模型构建模块
102
方程建立模块
103
分析求解模块

图2

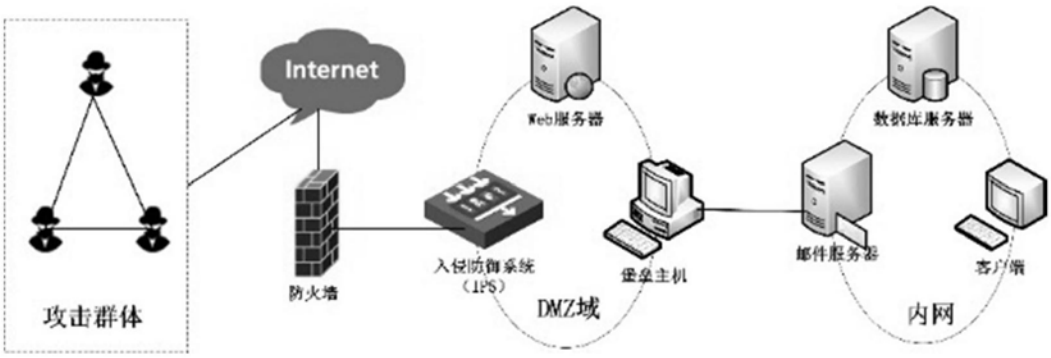

攻击群体
Internet
防火墙
入侵防御系统
（IPS）
Web服务器
堡垒主机
DMZ域
数据库服务器
邮件服务器
客户端
内网

图3

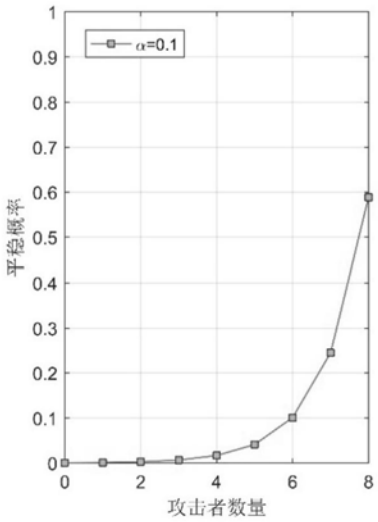

α=0.1
平稳概率
攻击者数量
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
0
2
4
6
8

图4

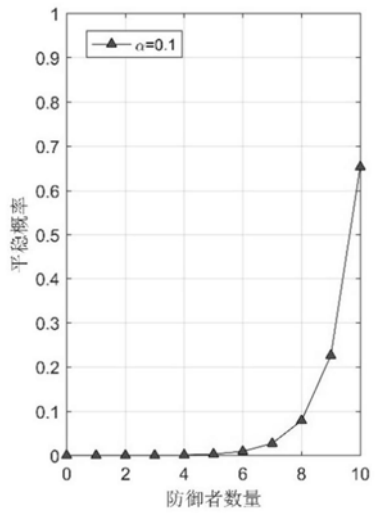

α=0.1
平稳概率
防御者数量
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
0
2
4
6
8
10

图5

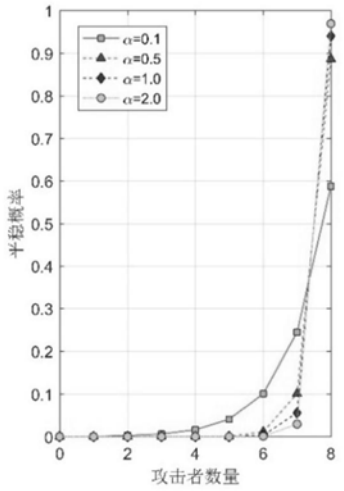


图6

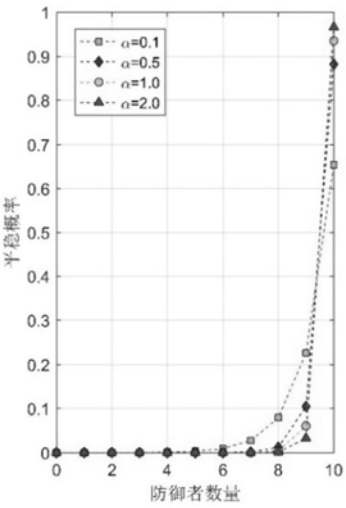


图7

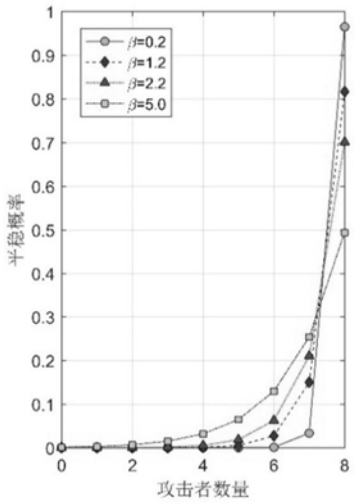


图8

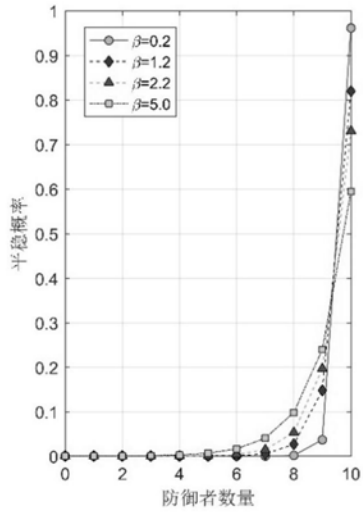


图9