平台动态防御演化博弈模型和状态迁移策略

王志屹，王　刚，陈彤睿，冯　云，马润年
（空军工程大学信息与导航学院，西安，710077）

摘要　为提升平台动态防御系统对病毒的适应性和防御效能，对基于有限理性假设的平台动态防御演化博弈模型和状态迁移策略进行研究。首先，从病毒传播感染机理入手，阐述了平台状态迁移动态防御和有限理性假设下的演化博弈原理，分析了平台动态防御中节点状态转移关系和影响因素；其次，定义了平台动态防御的演化博弈模型和关键参数，考虑迁移平台与病毒类型之间的免疫特性，提出免疫因子和防御节点收益计算方法；最后，通过算例给出了单个状态演化稳定分析流程和方法，设计了节点状态迁移演化均衡策略生成算法。理论分析和仿真结果表明：平台动态防御节点状态迁移演化均衡策略具有更好的防御效能，可有效解决平台动态防御系统在面对随机攻击病毒的平台迁移选择问题。

关键词　平台动态防御；动态目标防御；演化博弈；网络空间安全；防御策略
DOI　10.3969/j.issn.1009-3516.2020.03.014
中图分类号　TP393.1　　**文献标志码**　A　　**文章编号**　1009-3516(2020)03-0085-08

Platform Dynamic Defense Evolution Game Model and State Migration Strategy

WANG Zhiyi, WANG Gang, CHEN Tongrui, FENG Yun, MA Runnian
(Information and Navigation College, Air Force Engineering University, Xi'an 710077, China)

Abstract　In order to improve the adaptability and defense effectiveness of the platform dynamic defense system to virus, a platform dynamic defense evolution game model and state migration strategy based on the finite rational hypothesis are studied. First, the mechanism of virus transmission and infection is elaborated, and the state migration relationship in the platform dynamic defense is provided. Secondly, the PDD evolutionary game model is established, and immune factors are introduced in the income calculation while the immune characteristics between the migrating platform and the virus type are considered. At last, the flow chart and method of single state evolutionary stability strategy analysis are given in demo, and a novel node state migration strategy are presented as well as the corresponding algorithm. Theoretical analysis and simulation results show that the node state migration evolutionary equilibrium strategy of platform dynamic defense has better efficiency, and can effectively solve the platform migration selection problem of platform dynamic defense system in the case of random attack viruses.

Key words　platform dynamic defense (PDD); moving target defense (MTD); evolutionary game; cyberspace security; defense strategy

收稿日期：2019-08-27
基金项目：国家自然科学基金(61573017)
作者简介：王志屹(1996—)，男，安徽蚌埠人，硕士生，主要从事网络空间安全理论与技术研究。E-mail:491801209@qq.com
通信作者：王　刚(1976—)，男，湖北武汉人，教授，主要从事网络空间安全理论与技术研究。E-mail:wglxl@nudt.edu.cn

引用格式：王志屹，王刚，陈彤睿，等. 平台动态防御演化博弈模型和状态迁移策略[J]. 空军工程大学学报(自然科学版)，2020，21(3)：85-92. WANG Zhiyi, WANG Gang, CHEN Tongrui, et al. Platform Dynamic Defense Evolution Game Model and State Migration Strategy[J]. Journal of Air Force Engineering University (Natural Science Edition), 2020, 21(3): 85-92.

平台动态防御是网络平台层的动态目标防御[1],建立在虚拟化技术和多样化异构平台基础上,网络节点是平台动态防御的执行单元。在平台动态防御系统内,承载业务按照节点状态迁移规则在多样化异构平台间动态切换,通过改变系统环境,系统自身存在的漏洞和潜在缺陷随着状态跳变规则呈现出动态变化,增大了攻击方侦察定位和进一步实施攻击的难度和代价[2],降低了平台被病毒感染的概率。具体的手段包括改变文件扩展名[3]、主机状态迁移[4]和攻击面自适应转换[5]等。防御方通常先对攻击者的意图和行为进行分析、检测和预判[6-8],进而设计和实施针对性防御。

策略的制定是防御的关键,也是当下研究的热点问题。防御方和攻击方之间的目标对立性、策略依存性和关系非合作性等特征符合博弈的相关理论,其中动态目标防御的信号博弈[9-10]立足信息不对称性,微分博弈[11]侧重博弈的连续性,Stackelberg 博弈[12]重点考虑博弈次序的不对称性,马尔可夫鲁棒博弈[13]利用 Markov 过程的无后效性,简化了多阶段博弈的分析。这些成果是研究平台动态防御迁移策略的基础。对于平台动态防御的节点而言,攻防博弈的复杂性和难度更高,获得的攻防信息是不完全的,且节点对整体网络和系统的状态分析能力有限,网络的复杂环境和系统的计算能力限制,决定了防御者的行为属于一种有限理性行为[14],攻防双方需要适应对手的变化和动态调整博弈策略,具有典型演化博弈特征。真正意义上的“最优”策略可能难以达到,相较于完全理性的博弈类型,演化博弈模型拉近了预设条件与现实网络之间的距离[15],可利用复制动态方程和演化稳定分析[16-18],求解更贴近现实需求的状态迁移策略。

具体而言,平台动态防御演化博弈需考虑以下几个问题:①针对病毒的传播特性和作用机理,从破坏攻击方的攻击链入手,分析平台动态防御的防御机理、状态迁移关系和影响因素;②网络节点是网络拓扑基本单元和攻击者入侵的门户,节点的感染与状态迁移是攻防双方演化博弈的直观体现,节点状态迁移规则是防御的关键所在;③防御效能对平台动态防御演化博弈策略优劣的度量,应建立起科学的指标参数和评估体系。

1 平台状态迁移动态防御原理

病毒的传播依赖于系统的漏洞,不同类型的病毒,其工作环境也不同。通过部署平台动态防御系统实现上线平台的动态切换,避免对外网病毒免疫性较弱的平台上线,如果外网多为 Windows 平台易感病毒,则选择上线 Linux 系统平台,可最大程度避免病毒感染内网[19]。每一个防御节点无法准确预测入侵的病毒是哪一类型,只能根据历史信息和其他节点的状态不断试错、学习和调整迁移策略,直到防御的收益最大化,最终整个节点趋向于选择某一策略。节点的策略趋向稳定的过程,即为演化博弈的过程。

传统静态策略不会对平台的迁移概率产生影响[4],平台动态防御从平台的迁移入手,不同的防御策略对应的平台迁移概率也不同。在实际操作过程中,防御者对攻击者信息的了解是有限的,并且对网络环境的判断和认识也有局限性,平台的迁移过程是有限理性的。如图 1 所示,平台动态防御系统的一个节点由 3 个虚拟化平台组成。3 个虚拟平台的初始状态分别用 S_1^0、S_2^0、S_3^0 表示,在遭受病毒攻击后进入感染状态,箭头代表平台可选择的迁移策略。平台的迁移过程为:首先平台进入下线状态,此时平台不会接受新的任务请求,在处理完现有的任务后,平台进入离线状态,从候选平台中选择一个上线。离线的平台会将数据和文件进行重置处理,即“清洗”感染的病毒,回到初始状态。这样可以保证系统承载的业务不会被中断,并且将节点恢复至健康状态。

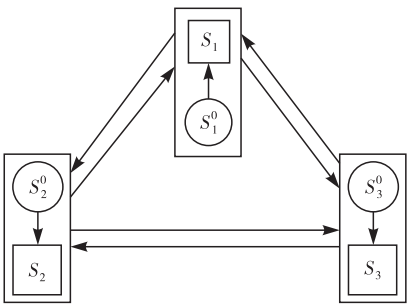


图 1 平台动态防御系统节点模型

由图 1 可知,平台有多个候选迁移策略,在进行防御时,平台动态防御系统可根据病毒的分布概率情况,有针对性地选择迁移策略。考虑双方的攻防过程符合博弈论的特点,且平台的迁移是有限理性的,可以建立平台动态防御演化博弈模型,对最优策略的选择进行研究。在模型的建立中,各种指标的量化是关键。平台动态防御技术的部署,同样需要消耗额外的开销,这些开销的量化需要建立在平台动态防御技术的原理分析上[1],包括平台迁移的成本和迁移带来的负面影响 2 个方面。演化均衡策略的选取需要综合考虑成本和收益 2 个方面的因素,有限理性的参与方难以选择严格最优的策略,通过不断调整以获得收益的提升。节点的演化过程需要

重点分析，在此基础上提炼策略选择算法，实现平台动态防御系统在外部病毒环境下对节点状态迁移的提前预测和最优控制。

2　平台动态防御演化博弈模型

2.1　博弈定义

定义 1　平台动态防御演化博弈模型（Platform Dynamic Defense Evolutionary Game Model，PDDEGM）可用七元组表示，PDDEGM＝(R,N,B,P,S^0,S,U)，其中：

1）$R=(R_D,R_A)$ 为演化博弈的参与者空间，其中 R_D 为平台动态防御系统，R_A 为攻击病毒。

2）N 是平台动态防御系统中某一节点的虚拟化平台总数，节点处在某一虚拟化平台的状态用 k 表示，$k\in\{1,2,\cdots,N\}$，$N\in\mathrm{N}^+$。

3）$B=(D_S,A_S)$ 是双方策略空间。其中攻击方策略 $A_S=\{A_{S_i}\mid 1\leqslant i\leqslant m\}$，$m$ 为攻击策略的总数；防御方策略 $D_S=\{D_{S_k^j}\mid j,k\in\{1,2,\cdots,N\},j\neq k\}$，策略 $D_{S_k^j}$ 表示节点从 k 平台迁移至 j 平台。

4）$P=\{(p_k^i,q_k^j)\mid j,k\in\{1,2,\cdots,N\},j\neq k\}$ 是博弈信念集合。其中，p_k^i 表示在节点处在 k 平台状态时 i 型病毒的分布概率，$p_k^i\in[0,1]$ 且 $\sum_{i=1}^{m}p_k^i=1$；q_k^j 表示节点从 k 平台迁移至 j 平台的概率，$q_k^j\in[0,1]$ 且 $\sum_{j=1,j\neq k}^{N}q_k^j=1$。

5）$S^0=\{S_1^0,\cdots,S_k^0,\cdots,S_N^0\}$ 表示节点初始安全状态集合。

6）$S=\{S_1,\cdots,S_k,\cdots,S_N\}$ 表示节点感染状态集合。

7）$U=\{U_D,U_A\}$ 是博弈收益函数集合。其中 $U_D(S_j^0\mid S_k)$ 表示节点通过 k 平台向 j 平台迁移，脱离感染状态后获得的收益，$U_A(S_j\mid S_j^0)$ 表示攻击病毒将 j 平台感染后获得的收益。

2.2　关键参数定义

平台在迁移时，需要进行迁移前的准备，在迁移过程中也会带来服务质量的下降，同时，不同平台针对不同类型病毒的免疫能力也各有差异。为体现平台迁移的成本和不同平台的免疫能力，参照平台动态防御原理[1]，给出关键参数定义。

定义 2　资源重要程度 C_r。即平台对网络安全的贡献度，由平台所在网络节点的度、数据量大小和单位时间访问次数决定。

定义 3　攻击面转移成本 ASSC。平台完成迁移所需要的成本。由平台间的相似度决定。

定义 4　负面影响成本 NC。指平台发生迁移时，带来的工作或服务质量的下降，资源重要程度越大，负面影响成本就越大。

定义 5　节点感染概率 λ。病毒通常利用系统漏洞进行传播，可采用漏洞 CVSS 评分标准中的可利用性作为 λ 的参考。$\lambda(S_k\mid S_k^0)$ 表示节点处于状态 S_k^0 时，被感染的概率。节点感染概率越大，平台的安全性越差，直接影响针对不同病毒的免疫效果。

定义 6　免疫因子 μ。指平台对病毒的免疫程度，Windows 病毒无法在 Linux 类操作系统中运行，反之亦然，若病毒与平台呈现异构性可定义 $\mu=1$，同构性则定义 $\mu=1-\lambda$。

综上，可定义防御节点的收益为：

$$U_D(S_j^0\mid S_k)=\mu C_r-ASSC-NC \tag{1}$$

攻击病毒的收益为：

$$U_A(S_j\mid S_j^0)=C_r(1-\mu)=C_r\lambda \tag{2}$$

3　节点状态演化稳定分析

在演化博弈均衡求解和分析基础上，设计平台状态迁移演化均衡策略的生成算法。

3.1　状态演化稳定求解

通过算例演示平台动态防御节点演化博弈模型均衡求解的具体方法。平台动态防御系统的一个节点上虚拟了 3 个平台，平台 1、3 搭载 Windows 类操作系统，平台 2 搭载 Linux 类操作系统，节点的初始上线平台为平台 1，此时已遭到攻击。A_{S_1} 表示 Windows 类病毒，A_{S_2} 表示 Linux 类病毒，节点可选迁移策略为 $\{D_{S_1^2},D_{S_1^3}\}$，$D_{S_1^2}$ 为从当前平台 1 向平台 2 迁移，$D_{S_1^3}$ 为从当前平台 1 向平台 3 迁移。其博弈扩展式见图 2。

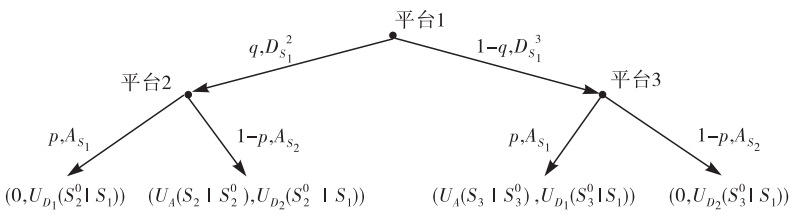


图 2　博弈扩展式

图 2 中,p 表示选择策略 A_{S_1} 的概率,即 Windows 类病毒的分布概率,$1-p$ 表示选择策略 A_{S_2} 的概率,即 Linux 类病毒分布概率;q 表示选择策略 $D_{S_1^2}$ 的概率,即从平台 1 迁移至平台 2 的概率,$1-q$ 表示选择策略 $D_{S_1^3}$ 的概率,即从平台 1 迁移至平台 3 的概率。攻防双方的收益分别由式(1)和式(2)计算得到。

计算防御方的期望收益和平均收益:

$$U_{D_{S_1^2}}=pU_{D_1}(S_2^0|S_1)+(1-p)U_{D_2}(S_2^0|S_1)$$

$$U_{D_{S_1^3}}=pU_{D_1}(S_3^0|S_1)+(1-p)U_{D_2}(S_3^0|S_1)$$

$$\overline{U_D}=qU_{D_{S_1^2}}+(1-q)U_{DS_1^3}=q(pU_{D_1}(S_2^0|S_1)+(1-p)U_{D_2}(S_2^0|S_1))+(1-q)(pU_{D_1}(S_3^0|S_1)+(1-p)U_{D_2}(S_3^0|S_1))$$

根据演化博弈理论,节点只能做出有限理性的决策,但是能够通过不断的调整、学习和改进最终达到演化博弈的稳定状态,对应的策略即为演化博弈均衡策略。分别用 $q(t)$ 和 $1-q(t)$ 表示系统随时间变化选择策略 $\{D_{S_1^2},D_{S_1^3}\}$ 的平台比例。则 $D_{S_1^2}$ 的动态变化速率用复制动态方程表示为:

$$\frac{\mathrm{d}q(t)}{\mathrm{d}t}=q(U_{D_{S_1^2}}-\overline{U_D})=q(1-q)(p(U_{D_1}(S_2^0|S_1)-U_{D_2}(S_2^0|S_1)-U_{D_1}(S_3^0|S_1)+U_{D_2}(S_3^0|S_1))+U_{D_2}(S_2^0|S_1)-U_{D_2}(S_3^0|S_1)) \tag{3}$$

令 $\frac{\mathrm{d}q(t)}{\mathrm{d}t}=0$,可得解:$q=0$,$q=1$,

$$p=\frac{U_{D_2}(S_3^0|S_1)-U_{D_2}(S_2^0|S_1)}{U_{D_1}(S_2^0|S_1)-U_{D_2}(S_2^0|S_1)-U_{D_1}(S_3^0|S_1)+U_{D_2}(S_3^0|S_1)}。$$

计算攻击方的期望收益和平均收益:

$$U_{A_{S_1}}=(1-q)U_A(S_3|S_3^0),U_{AS_2}=qU_A(S_2|S_2^0),$$

$$\overline{U_A}=p(1-q)U_A(S_3|S_3^0)+(1-p)qU_A(S_2|S_2^0)$$

对应的复制动态方程为:

$$\frac{\mathrm{d}p(t)}{\mathrm{d}t}=p(U_{AS_1}-\overline{U_A})=p(1-p)((1-q)U_A(S_3|S_3^0)-qU_A(S_2|S_2^0)) \tag{4}$$

令 $\frac{\mathrm{d}p(t)}{\mathrm{d}t}=0$,则可以得到解:

$p=0$,$p=1$,$q=\frac{U_A(S_3|S_3^0)}{U_A(S_3|S_3^0)+U_A(S_2|S_2^0)}$。

由 $\begin{bmatrix}\frac{\mathrm{d}q(t)}{\mathrm{d}t}\\ \frac{\mathrm{d}p(t)}{\mathrm{d}t}\end{bmatrix}=0$ 可求得其稳定状态为:$\begin{bmatrix}0\\0\end{bmatrix},\begin{bmatrix}0\\1\end{bmatrix},\begin{bmatrix}1\\0\end{bmatrix},\begin{bmatrix}1\\1\end{bmatrix}$,和

$$\begin{bmatrix}\frac{U_{D_2}(S_3^0|S_1)-U_{D_2}(S_2^0|S_1)}{U_{D_1}(S_2^0|S_1)-U_{D_2}(S_2^0|S_1)-U_{D_1}(S_3^0|S_1)+U_{D_2}(S_3^0|S_1)}\\ \frac{U_A(S_3|S_3^0)}{U_A(S_3|S_3^0)+U_A(S_2|S_2^0)}\end{bmatrix}。$$

式中:$\begin{bmatrix}0\\0\end{bmatrix}$ 表示向平台 3 迁移(纯策略 $D_{S_1^3}$),攻击病毒为 Linux 类病毒(纯策略 A_{S_2});$\begin{bmatrix}0\\1\end{bmatrix}$ 表示向平台 3 迁移(纯策略 DS_1^3),攻击病毒为 Windows 类病毒(纯策略 A_{S_1});$\begin{bmatrix}1\\0\end{bmatrix}$ 表示向平台 2 迁移(纯策略 $D_{S_1^2}$),攻击病毒为 Linux 类病毒(纯策略 A_{S_2});$\begin{bmatrix}1\\1\end{bmatrix}$ 表示向平台 2 迁移(纯策略 $D_{S_1^2}$),攻击病毒为 Windows 类病毒(纯策略 A_{S_1});

$$\begin{bmatrix}\frac{U_{D_2}(S_3^0|S_1)-U_{D_2}(S_2^0|S_1)}{U_{D_1}(S_2^0|S_1)-U_{D_2}(S_2^0|S_1)-U_{D_1}(S_3^0|S_1)+U_{D_2}(S_3^0|S_1)}\\ \frac{U_A(S_3|S_3^0)}{U_A(S_3|S_3^0)+U_A(S_2|S_2^0)}\end{bmatrix}$$

表示防御节点迁移平台 2 和 3 的概率组合为:

$$\begin{pmatrix}\frac{U_{D_2}(S_3^0|S_1)-U_{D_2}(S_2^0|S_1)}{U_{D_1}(S_2^0|S_1)-U_{D_2}(S_2^0|S_1)-U_{D_1}(S_3^0|S_1)+U_{D_2}(S_3^0|S_1)},\\ 1-\frac{U_{D_2}(S_3^0|S_1)-U_{D_2}(S_2^0|S_1)}{U_{D_1}(S_2^0|S_1)-U_{D_2}(S_2^0|S_1)-U_{D_1}(S_3^0|S_1)+U_{D_2}(S_3^0|S_1)}\end{pmatrix},$$

攻击病毒为 Windows 类病毒和 Linux 类病毒的概率分布为 $\begin{pmatrix}\frac{U_A(S_3|S_3^0)}{U_A(S_3|S_3^0)+U_A(S_2|S_2^0)},\\ 1-\frac{U_A(S_3|S_3^0)}{U_A(S_3|S_3^0)+U_A(S_2|S_2^0)}\end{pmatrix}$。

根据公式

$$\frac{\mathrm{d}q(t)}{\mathrm{d}t}=q(1-q)[p(U_{D_1}(S_2^0|S_1)-U_{D_2}(S_2^0|S_1)-U_{D_1}(S_3^0|S_1)+U_{D_2}(S_3^0|S_1))+U_{D_2}(S_2^0|S_1)-U_{D_2}(S_3^0|S_1)]$$

可知,当且仅当:

$$p=\frac{U_{D_2}(S_3^0|S_1)-U_{D_2}(S_2^0|S_1)}{U_{D_1}(S_2^0|S_1)-U_{D_2}(S_2^0|S_1)-U_{D_1}(S_3^0|S_1)+U_{D_2}(S_3^0|S_1)}$$

时,对任意的防御策略选择概率 q,有 $\frac{\mathrm{d}q(t)}{\mathrm{d}t}=0$,由演化博弈中对演化稳定状态定义,稳定状态应能够抵抗动态系统中的微小扰动。但是,此处 p 值一旦发生小的偏移,则状态会立即发生变化,因此不具有稳定性。

若 $p\neq\frac{U_{D_2}(S_3^0|S_1)-U_{D_2}(S_2^0|S_1)}{U_{D_1}(S_2^0|S_1)-U_{D_2}(S_2^0|S_1)-U_{D_1}(S_3^0|S_1)+U_{D_2}(S_3^0|S_1)}$,

则 $q=0$ 和 $q=1$ 是 2 个稳定状态,当 $\frac{\mathrm{d}q(t)}{\mathrm{d}t}=0$ 且 $\frac{\mathrm{d}^2q(t)}{\mathrm{d}t^2}<0$ 时,q 为防御节点的演化稳定策略。

当 $p<\frac{U_{D_2}(S_3^0|S_1)-U_{D_2}(S_2^0|S_1)}{U_{D_1}(S_2^0|S_1)-U_{D_2}(S_2^0|S_1)-U_{D_1}(S_3^0|S_1)+U_{D_2}(S_3^0|S_1)}$

时，$q=0$ 为防御节点的演化稳定策略，即纯策略 $D_{S_1^3}$；

当 $p>\dfrac{U_{D_2}(S_3^0|S_1)-U_{D_2}(S_2^0|S_1)}{U_{D_1}(S_2^0|S_1)-U_{D_2}(S_2^0|S_1)-U_{D_1}(S_3^0|S_1)+U_{D_2}(S_3^0|S_1)}$ 时，$q=1$ 为防御节点的演化稳定策略，即纯策略 $D_{S_1^2}$。

对于攻击病毒来说，同理可得，当 $q=\dfrac{U_A(S_3|S_3^0)}{U_A(S_3|S_3^0)+U_A(S_2|S_2^0)}$ 时，对于任意类型的病毒分布概率 p，有 $\dfrac{\mathrm{d}p(t)}{\mathrm{d}t}=0$，但同样不稳定；当 $q>\dfrac{U_A(S_3|S_3^0)}{U_A(S_3|S_3^0)+U_A(S_2|S_2^0)}$ 时，$p=0$ 为攻击病毒分布概率的演化稳定策略，即纯策略 A_{S_2}；当 $q<\dfrac{U_A(S_3|S_3^0)}{U_A(S_3|S_3^0)+U_A(S_2|S_2^0)}$ 时，$p=1$ 为攻击病毒分布概率的演化稳定策略，即纯策略 A_{S_1}。

3.2　策略生成算法设计

基于上述分析，设计平台动态防御节点演化均衡策略生成算法，具体如下：

输入：各状态博弈树或支付矩阵；

输出：平台动态防御节点演化均衡策略。

①初始化；

②构建防御节点状态空间集合 $D=\{d_k,1\leqslant k\leqslant T\}$；

③构建防御节点状态转移策略空间集合 $D_S=\{D_{S_k^j},1\leqslant j\leqslant N,k\neq j\}$；

④初始化节点受感染状态转移概率 $\eta(S_k|S_0^k)$；

⑤For($k=1;k\leqslant T;k++$)；

⑥构建攻击病毒类型，构建 k 平台状态时 i 型病毒的分布概率 p_k^i，$p_k^i\in[0,1]$ 且 $\sum_{i=1}^{m}p_k^i=1$，以概率 q_k^i 选取防御策略 $D_{S_k^j}$，其中 $\sum_{j=1}^{m}q_k^j=1$；

⑦计算 k 平台状态下双方期望收益和平均收益；

⑧建立双方复制动态方程；

⑨计算均衡解；

⑩输出 k 平台状态下的演化稳定策略；

⑪综合 N 个状态下的演化稳定策略，得出节点状态迁移演化均衡策略；

⑫end。

3.3　模型对比分析

表 1 给出了在模型构建、博弈类型和模型应用等方面与现有方法的对比。

表 1　对比分析

文献	模型构建	博弈类型	模型应用
[9,10]	静态攻防模型	信号博弈	防御策略选取
[11]	动态攻防模型	微分博弈	防御策略选取
[12]	动态攻防模型	Stackelberg 博弈	动态攻防分析
[18]	静态攻防模型	演化博弈	防御策略选取
本文	动态攻防模型	演化博弈	防御策略选取

4　仿真实验与分析

4.1　仿真实验环境

参照图 1 的平台动态防御系统节点模型，分别部署堡垒主机节点和 Web 服务器节点。其搭载的操作系统见表 2。利用 Nessus 工具挖掘漏洞信息，根据国家信息安全漏洞库[20]和美国国家漏洞库[21]数据，得出漏洞的利用成功概率[22]。

表 2　各平台漏洞信息

序号	平台	环境	CVE 编号	利用成功概率
1	堡垒主机 1	Windows 7	CVE-2013-2553	0.72
2	堡垒主机 2	FreeBSD	CVE-2017-1087	0.46
3	堡垒主机 3	Windows 10	CVE-2017-8642	0.43
4	Web 服务器 1	Apache	CVE-2017-14377	0.75
5	Web 服务器 2	Virtualbox	CVE-2018-2909	0.44
6	Web 服务器 3	Windows Server 2016	CVE-2018-0749	0.46

4.2　实验数值计算与分析

堡垒主机节点和 Web 服务器节点是平台防御系统中关键的 2 个节点，下面分别进行分析。

4.2.1　堡垒主机节点

根据部署的操作系统平台和对应的漏洞信息可知节点感染概率分别为：$\lambda(S_1|S_1^0)=0.72$，$\lambda(S_2|S_2^0)=0.46$，$\lambda(S_3|S_3^0)=0.43$。用 A_{S_1} 表示 Windows 类病毒，A_{S_2} 表示 Linux 类病毒。

由式(1)和式(2)计算可得双方支付矩阵见表 3。根据文献[1]对平台动态防御系统的分析，设堡垒主机资源重要程度为 600，同构平台间攻击面转移成本为 70，异构平台间攻击面转移成本为 100，负

面影响成本为 50。根据设计的算法求解该模型的演化博弈均衡解,得出结果见表 4。$D_{S_k^*}$ 表示防御方在 k 平台上的演化博弈均衡策略。

表 3 各状态的支付矩阵

$S_1^0\to S_1$		$S_2^0\to S_2$		$S_3^0\to S_3$	
攻击收益	防御收益	攻击收益	防御收益	攻击收益	防御收益
$\begin{bmatrix}0 & 432\\ 432 & 0\end{bmatrix}$	$\begin{bmatrix}450 & 48\\ 18 & 480\end{bmatrix}$	$\begin{bmatrix}276 & 276\\ 0 & 0\end{bmatrix}$	$\begin{bmatrix}174 & 174\\ 450 & 450\end{bmatrix}$	$\begin{bmatrix}258 & 0\\ 0 & 258\end{bmatrix}$	$\begin{bmatrix}222 & 450\\ 480 & 192\end{bmatrix}$

表 4 各状态博弈均衡策略

节点状态	防御策略 $D_{S_k^*}$	攻击策略 $A_{S_k^*}$
$S_0^1\to S_1$	$\begin{cases}q_1^2=0, p<0.535\\ q_1^2=1, p>0.535\end{cases}$	$\begin{cases}p_1^1=1, q<0.500\\ p_1^1=0, q>0.500\end{cases}$
$S_0^2\to S_2$	$q_2^1=$任意值	$p_2^1=1$
$S_0^3\to S_3$	$\begin{cases}q_3^1=1, p<0.558\\ q_3^1=0, p>0.558\end{cases}$	$\begin{cases}p_3^1=0, q<0.500\\ p_3^1=1, q>0.500\end{cases}$

将表 4 中的结果综合分析,可得堡垒主机节点的演化均衡策略为:

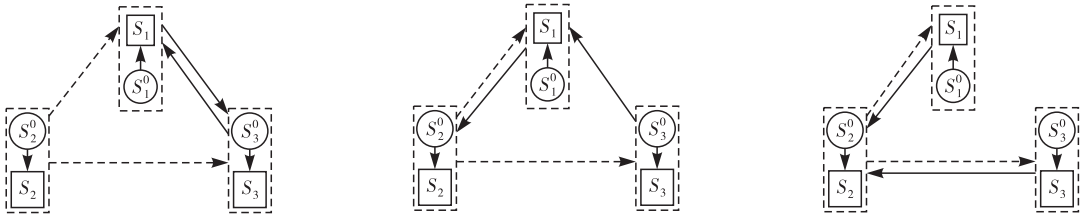
1)当 $0\leqslant p<0.535$,即 Windows 类病毒基本在一半以下时,对应的平台迁移状态见图 3(a),虚线表示迁移概率不确定。此时,节点倾向于向平台 1 和平台 3 迁移。

2)当 $0.535\leqslant p<0.558$,即 Windows 类病毒和 Linux 类病毒分布基本持平时,对应的平台迁移状态如图 3(b)所示。此时节点有形成“平台 1→平台 2→平台 3→平台 1”闭环的趋势。

3)当 $0.558\leqslant p\leqslant 1$,即大部分为 Windows 类病毒时,对应的平台迁移状态如图 3(c)所示。此时节点倾向于向平台 2 迁移。

4.2.2 Web 服务器节点

根据部署的操作系统平台和对应的漏洞信息可知节点感染概率分别为:$\lambda(S_1\mid S_1^0)=0.75$,$\lambda(S_2\mid S_2^0)=0.44$,$\lambda(S_3\mid S_3^0)=0.46$。由式(1)和式(2)计算可得双方支付矩阵见表 5。



(a) $0\leqslant p<0.535$ (b) $0.535\leqslant p<0.558$ (c) $0.558\leqslant p\leqslant 1$

图 3 堡垒主机节点演化均衡策略示意图

表 5 各状态的支付矩阵

$S_0^1\to S_1$		$S_0^2\to S_2$		$S_0^3\to S_3$	
攻击收益	防御收益	攻击收益	防御收益	攻击收益	防御收益
$\begin{bmatrix}0 & 300\\ 300 & 0\end{bmatrix}$	$\begin{bmatrix}300 & -30\\ 0 & 270\end{bmatrix}$	$\begin{bmatrix}0 & 176\\ 176 & 0\end{bmatrix}$	$\begin{bmatrix}300 & 94\\ 124 & 270\end{bmatrix}$	$\begin{bmatrix}0 & 0\\ 184 & 184\end{bmatrix}$	$\begin{bmatrix}270 & 270\\ 86 & 86\end{bmatrix}$

表 5 根据文献[1]对平台动态防御系统的分析,设 Web 服务器资源重要程度为 400,同构平台间攻击面转移成本为 60,异构平台间攻击面转移成本为 90,负面影响成本为 40。根据设计的算法求解该模型的演化博弈均衡解,得出结果见表 6。

表 6 各状态博弈均衡策略

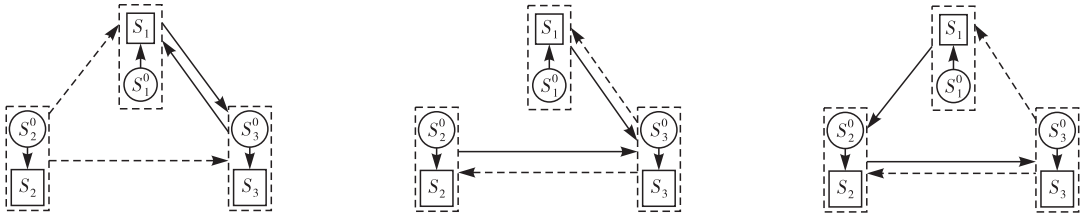
节点状态	防御策略 $D_{S_k^*}$	攻击策略 $A_{S_k^*}$
$S_0^1\to S_1$	$\begin{cases}q_1^2=0, p<0.450\\ q_1^2=1, p>0.450\end{cases}$	$\begin{cases}p_1^1=1, q<0.500\\ p_1^1=0, q>0.500\end{cases}$
$S_0^2\to S_2$	$\begin{cases}q_2^1=1, p<0.415\\ q_2^1=0, p>0.415\end{cases}$	$\begin{cases}p_2^1=1, q<0.500\\ p_2^1=0, q>0.500\end{cases}$
$S_0^3\to S_3$	$q_3^1=$任意值	$p_3^1=0$

综合分析表 6 中的结果,可得 Web 服务器节点的演化均衡策略为:

1)当 $0\leqslant p<0.415$,即 Windows 类病毒较少时,对应的平台迁移状态见图 4(a),虚线表示迁移概率不确定。此时节点有形成“平台 1→平台 3→平台 2→平台 1”闭环的趋势;

2)当 $0.415\leqslant p<0.45$,即 Windows 类病毒和 Linux 类病毒分布基本持平时,对应的平台迁移状态见图 4(b),节点倾向于向平台 3 迁移;

3)当 $0.45\leqslant p\leqslant 1$,即大部分为 Windows 类病毒时,对应的平台迁移状态见图 4(c),节点有形成“平台 1→平台 2→平台 3→平台 1”闭环的趋势。



(a) $0 \leqslant p < 0.415$　(b) $0.415 \leqslant p < 0.45$　(c) $0.45 \leqslant p < 1$

图 4　Web 服务器节点状态迁移演化均衡策略示意图

4.3　仿真条件与结果分析

4.3.1　状态演化稳定策略仿真

利用系统动力学仿真软件 Vensim，建立博弈双方收益、策略选取概率和策略选取次数比例等要素的关系模型，对堡垒主机节点和 Web 服务器节点分别进行仿真。其中，防御策略 1 和 2 分别对应在不同节点不同状态下相应的平台防御迁移策略，攻击策略 1 和 2 分别为 Windows 类病毒和 Linux 类病毒。设初始选择防御策略 1 的概率都为 0.5，即各状态下初始 $q=0.5$。

1）堡垒主机节点

以平台 1 为例，对堡垒主机节点迁移状态进行仿真分析。设病毒分布概率分别为为 $p=0.4$ 和 $p=0.55$，选择的防御策略为向平台 2 迁移，得仿真结果见图 6。分析可得，当 $p=0.55>0.535$ 时，平台 1 在 30 s 内到达稳定状态，选择向平台 2 迁移；当 $p=0.4<0.535$ 时，平台 1 在 6 s 内到达稳定状态，选择向平台 3 迁移。仿真结果符合 4.2 节的分析。此外，病毒的分布概率与平衡态 $p=0.535$ 偏差的越大，节点向稳态演化的速度就越快。

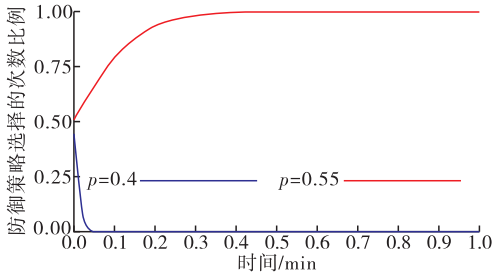


图 6　堡垒主机节点平台 1 迁移状态

2）Web 服务器节点

同样以平台 1 为例，对 Web 服务器节点迁移状态进行仿真分析。设病毒分布概率分别为 $p=0.41$ 和 $p=0.46$，选择的防御策略为向平台 1 迁移，得到仿真结果见图 7。分析可得，当 $p=0.46>0.45$ 时，平台 1 在 54 s 内达到稳定状态，选择向平台 2 迁移；当 $p=0.41<0.45$ 时，平台 1 在 18 s 内达到稳定状态，选择向平台 3 迁移。仿真结果符合 4.2 节的分析。与堡垒主机节点类似，病毒的分布概率与平衡态对应的概率偏差越大，节点向稳态演化的速度就越快。

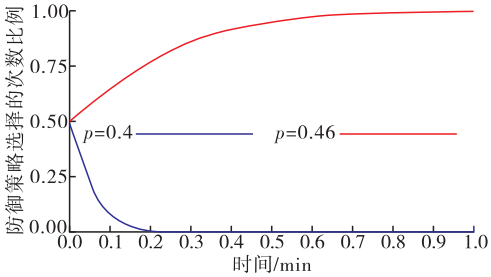


图 7　Web 服务器节点平台 1 迁移状态

4.3.2　节点状态迁移演化均衡策略效能仿真

为对比演化稳定均衡后的节点状态迁移策略效能情况，与现有的随机平台选择策略进行对比分析，随机平台选择策略即选择的迁移目标平台是随机的[7]。考虑攻击病毒类型分别为 $p=0$，$p=0.5$ 和 $p=1$ 时，2 种策略对堡垒主机和 Web 服务器 2 个节点防御收益的影响，以及与攻击病毒收益的对比，进行蒙特卡洛仿真实验 100 次，仿真结果见图 8～10。

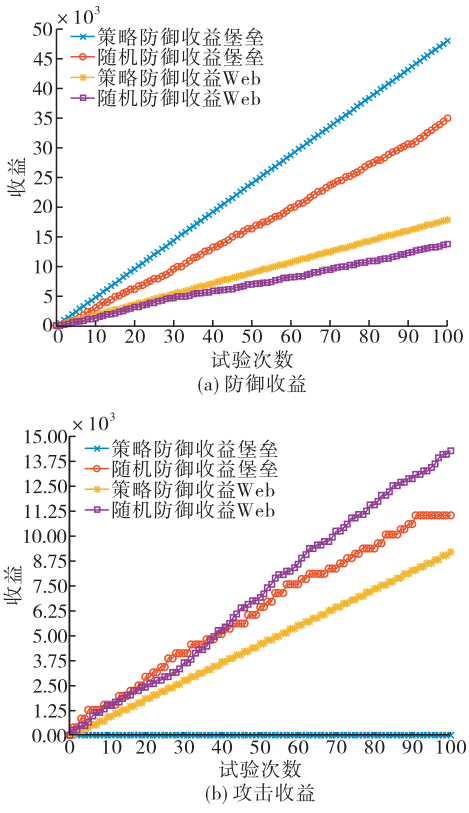
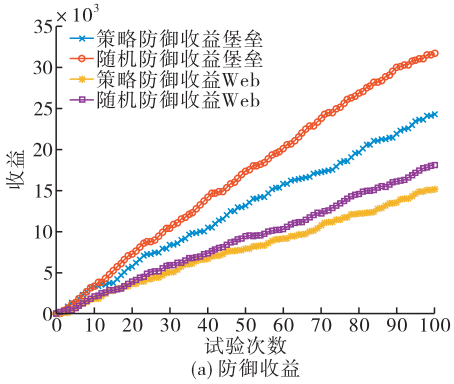
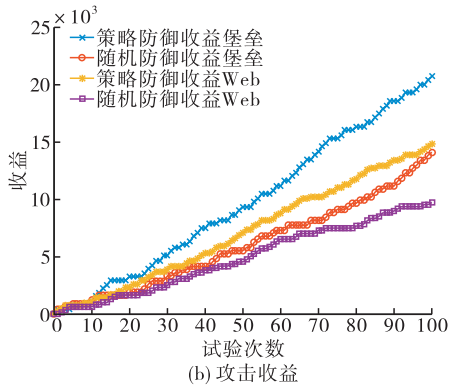


图 8　$p=0$ 时 2 种策略对比

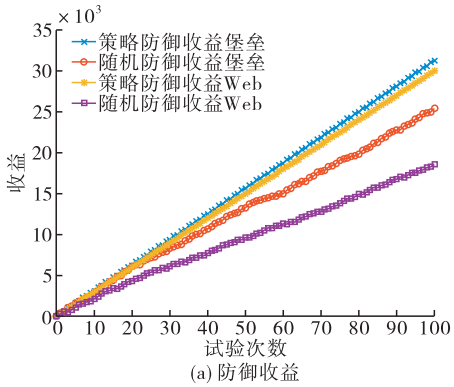


(a) 防御收益

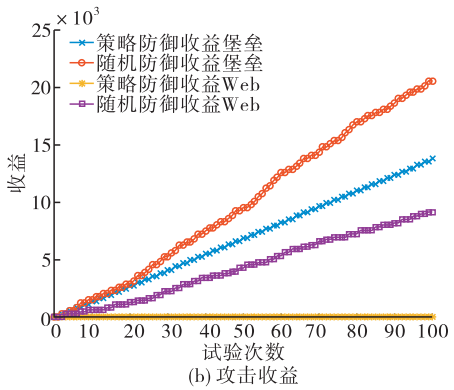


(b) 攻击收益

图 9 $p=0.5$ 时 2 种策略对比



(a) 防御收益



(b) 攻击收益

图 10 $p=1$ 时 2 种策略对比

由图 8(a)、9(a)和 10(a)可得,无论是 $p=0$、$p=0.5$ 还是 $p=1$,即攻击病毒类型分布分别为全是 Linux 类、Linux 类和 Windows 类各半以及全为 Windows 类 3 种情况下,堡垒主机和 Web 服务器的节点迁移演化均衡策略防御收益均高于随机平台选择策略。其中,在 100 次试验后,$p=0$ 的堡垒主机节点迁移演化均衡策略防御收益比随机平台选择策略高 25.3%,$p=0.5$ 时高 10.37%,$p=1$时高 97%,平均高 39.1%。$p=0$ 的 Web 服务器节点迁移演化均衡策略防御收益比随机平台选择策略高 13.64%,$p=0.5$ 时高 24.39%,$p=1$ 时高 75.92%,平均高 38.18%。验证了节点迁移演化均衡策略具有较高的防御效能。

由图 8(b)、9(b)和图 10(b)可得,无论是病毒攻击堡垒主机还是 Web 服务器,在节点迁移演化均衡策略下的攻击收益均小于随机平台选择策略,同样验证节点迁移演化均衡策略防御效能较好。其中图 8(b)表明,由于堡垒主机节点迁移演化均衡策略规定其迁移状态一直在 Windows 类平台间迁移,Linux 平台易感型病毒无法感染,可使病毒收益为 0。同理,图 10(b)中,病毒收益也为 0 的情况表明,Web 服务器节点迁移演化均衡策略为一直在 Linux 类平台间迁移,Windows 平台易感型病毒亦无法感染。

5 结语

基于网络攻防博弈的有限理性假设,建立了平台动态防御的演化博弈模型,对双方的具体变化参数进行了设计。通过算例分析了平台动态防御节点状态演化过程,利用复制动态方程分析了双方策略的演化稳定情况,在此基础上提出了平台状态迁移演化均衡策略生成算法。仿真实验验证了所提策略的有效性。下一步将重点开展多阶段的平台动态防御演化博弈问题研究,并提升模型对多类型网络环境和应用场景的适应能力。另一方面,在复杂的网络环境中,影响平台的迁移成本和病毒免疫能力的因素更加复杂,需要进一步对参数的设计进行优化调整,增强模型的可操作性。

参考文献

[1] 杨林, 于全. 动态赋能网络空间防御[M]. 北京: 人民邮电出版社, 2018: 40-51.

[2] 刘文彦, 霍树民, 陈扬, 等. 网络攻击链模型分析及研究[J]. 通信学报, 2018, 39(S2): 88-94.

[3] SUHYEON L, HUY K K, KYOUNGGON K. Ransomware Protection Using the Moving Target Defense Perspective[J]. Computers and Electrical Engineering, 2019, 78:288-299.

[4] 刘江, 张红旗, 杨英杰, 等. 基于主机安全状态迁移模型的动态网络防御有效性评估[J]. 电子与信息学报. 2017, 39(3): 509-517.

(下转第 98 页)