基于系统先验信息的平台动态防御单阶段静态博弈策略

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

摘要　针对平台动态防御中节点选择迁移的复杂性，设计了基于系统先验信息的单阶段静态博弈策略。从平台动态防御原理分析入手，结合攻防双方博弈关系和完全信息条件下的防御需求，构建了单阶段静态博弈模型，提出了攻防效用关键参数和完全信息博弈流程，通过示例给出了策略的具体实施过程。仿真结果表明，经过 1 000 次攻防博弈实验后，防御方实际收益为 4.403×10^4，攻击方实际收益为 -1.625×10^5，所提策略能有效阻截网络攻击，防御方期望收益为 4.324×10^4，实际收益偏差约 1.8%，新策略的收益远高于无差别迁移策略，可解决传统平台动态防御中成本高、防御收支不平衡和节点迁移有效性等问题。

关键词　平台动态防御；完全信息博弈；攻击图；安全漏洞
DOI　10.3969/j.issn.1009-3516.2019.06.013
中图分类号　TP393.1　　**文献标志码**　A　　**文章编号**　1009-3516(2019)06-0084-07

A Single Stage Static Game Strategy of Platform Dynamic Defense Based on System Prior Information

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

Abstract: In view of the complexity of node selection and migration at platform dynamic defense, a single stage static game strategy is designed based on system prior information. Through analyzing from dynamic platform defense, a single stage static game model is constructed by combining the needs of the defense under conditions of game relationship between the two parties and complete information condition, and a process of the key parameters of the attack and defense utility and the complete information game is proposed. The demo and simulation results show that after 1 000 times of attack-defense game experiments, the actual revenue of the defense is 4.403×10^4, and the actual revenue of the attacker is -1.625×10^5, showing that the proposed strategy can effectively intercept cyber attacks. The expected revenue of the defense is 4.324×10^4, the deviation between the actual revenue and the expected revenue is about 1.8%. The revenue of the new strategy is much higher than that of the undifferentiated migration strategy. The single-stage static game strategy based on the system prior information can solve the problems of high cost, unbalanced defense budget and effective node migration in the traditional platform dynamic defense.

收稿日期：2019-07-16
基金项目：国家自然科学基金(61573017)
作者简介：陈彤睿(1992—)，男，陕西西安人，硕士生，主要从事网络空间安全理论与技术研究。E-mail:330606391@qq.com
通信作者：王　刚(1976—)，男，湖北浠水人，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：*陈彤睿，马润年，王刚，等. 基于系统先验信息的平台动态防御单阶段静态博弈策略[J]. 空军工程大学学报(自然科学版)，2019，20(6)：84-90. CHEN Tongrui, MA Runnian, WANG Gang, et al. A Single Stage Static Game Strategy of Platform Dynamic Defense Based on System Prior Information[J]. Journal of Air Force Engineering University (Natural Science Edition), 2019, 20(6): 84-90.*

Key words：platform dynamic defense；complete information game；attack graph；security vulnerability

平台动态防御（Platform Dynamic Defense，PDD）是网络安全动态目标防御（Moving Target Defense，MTD）新技术，它通过平台架构和系统软件等层面的动态迁移，使攻击者无法确定目标平台的运行环境，或者即使发现了可利用漏洞，也没有充裕时间展开攻击[1]。与传统防御相比，PDD 在解决攻防信息不对称、安全漏洞多样隐蔽等方面具有明显优势，可为目标系统提供规避攻击的“机动”条件，变被动防护为主动防御，使防御方动作不再滞后于攻击方，攻防双方行动转换为几乎同时决策的完全信息单阶段静态博弈。在传统防御模式下，防御方防御行动决策是建立在对攻击方先行行动信息观测分析基础上，攻击和防御表现为多阶段动态博弈。运用平台动态防御技术后，由于防御方经常主动迁移系统状态，攻击方对防御方系统的信息也同防御方对攻击方信息一样具有滞后性，其攻击无效的几率大大上升，攻击一旦失败，就又进入到杀伤链的第一步“侦察”阶段，由此攻防双方博弈的过程可始终保持在一个阶段上。

目前 PDD 研究主要集中在技术架构、策略及其评估等方面。如在技术实现方面，针对内核级、操作系统层面和硬件层面防御的 TALENT（Trusted Dynamic Logical Heterogeneity System，TALENT）技术架构[1]，流量和服务动态迁移技术[2]；针对服务器的多软件组合配置虚拟服务器栈技术[3]，自清洗容忍（Self-Cleansing Intrusion Tolerance，SCIT）技术框架[4]和 Web MTD 防御[5]等。在防御策略方面，有自适应移动目标防御转换策略[6]，面向隔离区异构平台的动态防御主动迁移策略[7]，基于事件驱动和定时迁移的 PDD 策略[8]；考虑攻防博弈关系的不完全信息动态博弈策略[9]，基于攻防信号博弈的高级持续性威胁（Advanced Persistent Threat，APT）攻击防御决策方法[10]，基于不完全信息马尔科夫博弈的策略生成方法[11]，基于马尔可夫鲁棒博弈的最优策略选择方法[12]，以及考虑了防御者偏好的竞争马尔可夫决策混合模型[13]等。性能评估是对 PDD 效能的度量[14]，如基于状态转移概率的有效性定量评估方法[15]，采用通用漏洞评分系统指标和贝叶斯推理等方法实现对目标网络整体安全性的评估[16]，基于时间图的图形安全模型[17]，通过划分资产集、漏洞集和威胁集对业务安全风险的评估[18]等。

研究表明，现有 PDD 策略通常依赖于网络入侵检测信息，实施的是平台统一迁移。随着网络安全环境和攻防行为的复杂化，传统 PDD 策略中成本高、防御收支不平衡和节点迁移有效性问题更加突出，应结合现实问题需求开展对 PDD 策略的针对性设计。①现有 MTD 防御策略通常是常规网络攻击下的普适性方案，结合平台动态防御特点考虑的较少，需要分析平台状态迁移带来的计算资源占用和业务负面影响，通过防御策略优化设计，避免因盲目跳变带来的资源浪费和过晚跳变带来的安全危害；②现有 PDD 博弈策略更多侧重博弈方法本身，随着网络技术和手段的复杂化，防御任务和需求呈现出新的特征和复杂性特点，应结合具体攻击意图和 PDD 迁移特点，利用既有系统信息进行防御决策，提升实际 PDD 网络中策略实施的可操作性，建立起规范的 PDD 博弈模型和关键指标参数，以及基于典型网络模型设计博弈策略步骤；③现有成果主要针对网络的安全性能、节点的重要程度和防御效果进行评估，缺乏对如何利用系统评估出的先验信息进行决策的深度研究，在完全信息单阶段静态博弈中，防御方如何准确的评估己方网络系统脆弱性，利用先验信息推断攻击策略，成为实施有效 PDD 的关键。

1　平台动态防御原理

PDD 主要从时间和不确定性 2 个方面来达成防御目的[7]。迁移频率越高，则留给攻击者完成攻击链的时间越短，平台越安全；候选平台的数量越多，迁移平台之间的系统版本差异越大，则让攻击者越无法确定目标环境，无法提早进行攻击准备。从成本上考虑，平台在进行迁移时，需要进行大量的同步和准备工作，系统需要付出一定的开销，将计算资源耗费在同步上，业务承载能力必然迅速下降，因此不能将迁移频率设置的过于频繁。综合安全性和成本考虑，结合攻击链步骤，平台的迁移时刻最好是在攻击者发送攻击代码的前一时刻，这样既能完美规避攻击，也能够不浪费系统资源进行无谓的迁移。在迁移方式上，如能预测攻击者即将选择的攻击路径，在路径的关键节点上进行攻击前的主动迁移，而其他不受攻击的节点保持现有工作状态不变，与检测到攻击就立即进行节点整体动态迁移相比，可大幅降低成本，增强防御的针对性。

以下假定防御方已掌握了己方系统漏洞等脆弱性先验信息，在此基础上，根据完全信息静态博弈理论，设计 PDD 单阶段静态博弈策略，推断攻击者攻击策略，通过在攻击路径关键节点开展针对性平台

动态迁移,阻断攻击杀伤链。

2 博弈策略设计

2.1 博弈模型

定义 1 PDD 完全信息博弈模型 PDDCIGM (Platform Dynamic Defense Complete Information Game Model)用五元组(N,A,D,P,U)描述。

1)$N=\{N_a,N_d\}$为博弈局中人空间,N_a 为攻击者,N_d 为防御者;

2)$A=\{a_1,a_2,\cdots,a_n\}$为攻击策略集, $n\in N^+$, N^+为正整数;

3)$D=\{d_1,d_2,\cdots,d_m\}$为防御者动态防御策略集,$m\in N^+$;

4)$P=\{p_1,p_2,\cdots,p_n\}$为攻击者攻击策略的先验信念集合,p_i 表示防御者对攻击者选用第 i 个攻击策略的判断,其中 $\sum_{i=1}^{n}p_i=1,1\leqslant i\leqslant n$。

5)$U=\{U_a,U_d\}$ 为攻防双方效用函数集合,$U_a=f_a(a_j,d_k)$ 和 $U_d=f_d(a_j,d_k),1\leqslant j\leqslant n,1\leqslant k\leqslant m$, 描述了攻防双方从博弈当中获得的收益,收益存在可正可负的现象。

2.2 攻防效用关键参数

定义 2 资源重要程度 C_r。平台在网络中所具有的重要程度,贡献程度越高,C_r 值越大。攻防双方的主要目标在于对资源的控制,其控制具有排外性,考虑将 C_r 作为攻防双方博弈收益的主要参考。

定义 3 PDD 成本 DC。由攻击面转移成本 $ASSC$ 和负面影响成本 NC 组成,即 $DC=ASSC+NC$。$ASSC$ 指平台迁移时需要付出的系统开销,平台间的相似度越小,意味着迁移前需要的准备工作越多,成本也就越高。NC 指平台发生迁移时,带来的工作或服务质量的下降。

定义 4 攻击路径成功概率 p_s。用 p_{s_i} 表示攻击策略 i 的成功概率,其中 $1\leqslant i\leqslant n$。攻击成功概率由系统脆弱性决定。考虑防御方若对将被攻击的目标采取迁移措施,则攻击无效,$p_{s_i}=0$。

定义 5 攻击方成本 AC。指攻击方侦察、访问、编写攻击代码和发起攻击等阶段所做的努力。

2.3 策略流程

博弈策略的流程如图 1 所示。

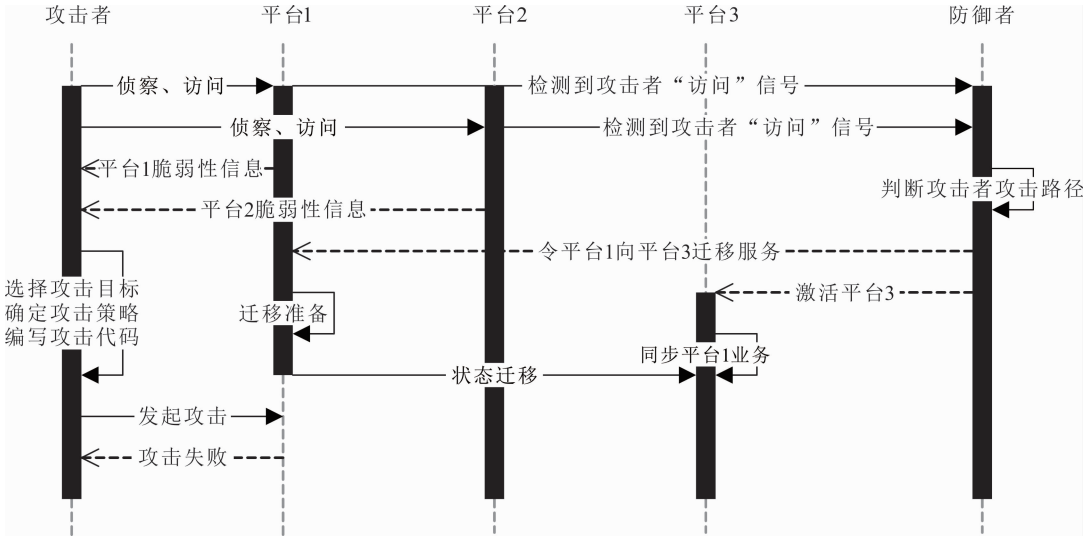

图 1 PDD 完全信息博弈流程

具体步骤如下:

步骤 1 攻击者先期侦察、访问我方目标系统;

步骤 2 防御者检测到攻击者释放的“访问”信号,根据系统脆弱性先验信息,计算每条攻击路径成功概率,列出支付矩阵;

步骤 3 根据每条攻击路径成功概率,经归一化运算得出攻击策略选择概率 $P=\{p_1,p_2,\cdots,p_n\}$;

步骤 4 求得防御策略期望收益,按照收益最大值策略实施防御;

步骤 5 防御者检测网络是否受到攻击,检测到攻击未成功,则说明防御有效;若检测到内网节点受到攻击,则可变化剩余关键节点,消除威胁。

传统 PDD 策略接收到预警信息后,以整体网络各平台的状态迁移来实现对攻击的规避,对攻击者即将攻击哪个节点不作考虑,这样使得一些节点的防御是没有必要的,既造成了资源的浪费,又影响了承载的业务。单阶段静态博弈平台动态防御策略,结合了系统漏洞的脆弱性信息,能够较为准确地判断攻击者即将进攻的节点,能够在保证安全的同时,最大程度的保证系统资源得到有效发挥。

3　示例与仿真分析

3.1　网络环境描述

实验采用 2 类操作系统搭建堡垒主机平台，堡垒主机 1 装载 Windows 7 系统，堡垒主机 2 装载 Linux 系统；在部署 Web 动态服务器方面，搭建 2 种 Web 服务器平台，具体内容如表 1 所示。使用 Nessus 工具扫描给定实验网络环境，获得平台漏洞信息如表 2 所示。

表 1　采用的 Web 平台具体架构

名称	虚拟化平台	操作系统	Web 服务器软件	Web 应用程序
Web 服务器 1	VMware	AIX	Apache	J2EE
Web 服务器 2	Virtualbox	Windows Server 2016	IIS	ASP

表 2　各平台漏洞信息及成功概率

序号	平台	环境	CVE 编号	漏洞类型	漏洞利用成功概率	攻击成功概率
1	堡垒主机 1	Windows 7	CVE-2013-2553	未知	0.39	0.85
2	堡垒主机 2	Linux	CVE-2018-14619	输入验证	0.39	1
3	Web 服务器 1	VMware	CVE-2018-6964	权限许可和访问控制	0.39	1
		AIX	CVE-2016-6079	权限许可和访问控制	0.39	0.9
		Apache	CVE-2017-14377	授权问题	1	0.9
		J2EE	CVE-2013-7364	权限许可和访问控制	1	0.9
4	Web 服务器 2	Virtualbox	CVE-2018-2909	权限许可和访问控制	0.34	0.9
		Windows Server 2016	CVE-2018-0749	权限许可和访问控制	0.39	1
		IIS	CVE-2015-7597	权限许可和访问控制	0.39	1
		ASP	CVE-2018-0787	权限许可和访问控制	0.86	1

3.2　参数计算

使用漏洞评估方法对各平台攻击面进行度量，攻击者使用漏洞发起攻击的概率分为漏洞利用成功概率和攻击成功概率 2 种，前者指该漏洞的可利用性，后者用来衡量利用该漏洞加载攻击代码的成功几率。查询国家信息安全漏洞库[19]和美国国家漏洞库[20]有关数据，参考文献[16]中漏洞利用成功概率计算方法，计算各漏洞利用成功概率。利用漏洞评分系统(CVSS)时效度量要素中提供的可利用性指标作为加载攻击代码成功概率参数。系统中 2 种概率数值见表 2。建立如图 2 的攻击图。设初始上线平台分别为堡垒主机 1 和 Web 服务器 1，考虑 Web 服务器包含 4 层架构，攻击者在扫描到 4 层架构上的漏洞后，会选择较容易利用的漏洞制定攻击策略，因此可对攻击图进行简化，其中实线表示现状态可行攻击路径，虚线表示经过平台迁移后可能存在的攻击路径，特别应该说明的是由于 Web 动态服务器的可信控制器在堡垒主机上，因此获得堡垒主机权限后，可控制 Web 服务器停止迁移，然后取得 Web 服务器权限。

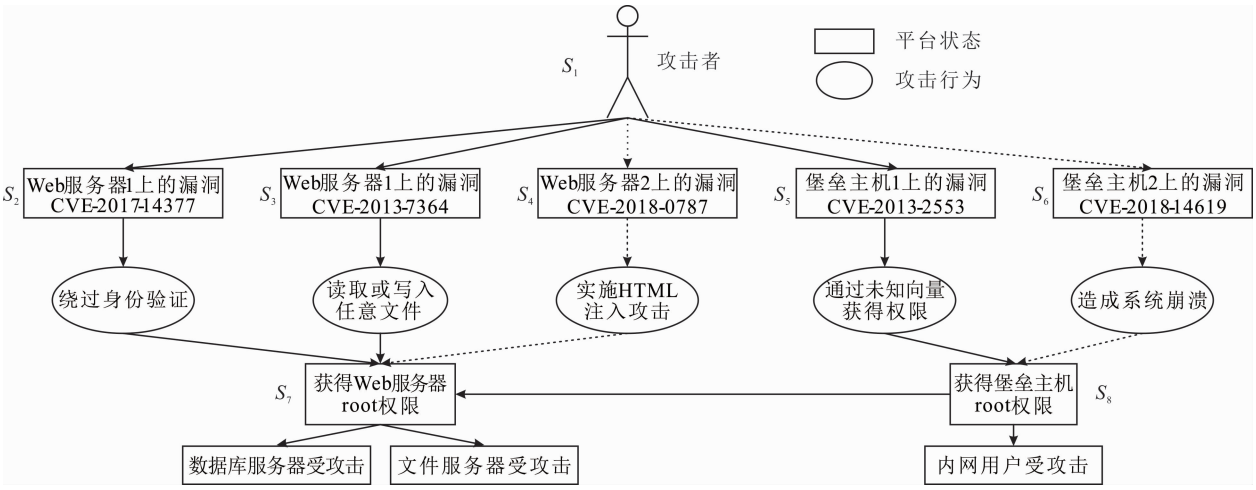

图 2　示例网络攻击图

攻击图各边概率值见表 3。设每条攻击路径和步骤相互独立，则各攻击路径成功概率为漏洞可利用成功概率与加载攻击代码成功概率之积。初始化外部属性节点 S_1 的先验概率 $P(S_1)=0.7$[16]，考虑

当前状态上线平台为堡垒主机 1 和 Web 服务器 1，因此无 S_4 和 S_6 节点，则攻击者在攻入内网共有 4 条路径可以选择，攻击策略可分为 3 种：①策略 a_1：针对 Web 服务器攻击；②策略 a_2：针对堡垒主机攻击；③策略 a_3：通过攻击堡垒主机获取 Web 服务器的权限。各攻击路径成功概率数值如表 4 所示。

表 3 攻击图各边概率值

边	概率取值	边	概率取值
(S_1,S_2)	1	(S_1,S_5)	0.39
(S_1,S_3)	1	(S_1,S_6)	0.39
(S_1,S_4)	0.86	(S_5,S_8)	0.85
(S_2,S_7)	0.9	(S_6,S_8)	1
(S_3,S_7)	0.9	(S_8,S_7)	1
(S_4,S_7)	1		

对防御者来说，有 2 种策略可分别应对这 3 种攻击：①策略 d_1：对 Web 服务器实施主动迁移；②策略 d_2：对堡垒主机进行主动迁移。在迁移完成后，系统局部节点形成新状态，如若未检测到内网遭受攻击，则表明防御成功。如在迁移完成后不久，内网检测到攻击，则表明采取了无效防御，为阻止攻击者进一步扩大战果，需立即采取另一策略再进行防御，则成本值是 DC_1+DC_2。列出攻防双方博弈支付矩阵，如表 5 所示，表中攻击策略 a_j 与防御策略 d_k 的相对收益以 $(U_{a_i\to d_k},U_{d_k\to a_i})$ 的形式表示，$U_{a_i\to d_k}$ 是攻击策略 a_j 在防御策略 d_k 下的支付数值，$U_{d_k\to a_i}$ 是防御策略 d_k 在攻击策略 a_j 下的支付数值。

表 4 各攻击路径成功概率

攻击策略	路径	攻击成功率
a_1	$S_1S_3S_7$	0.630
	$S_1S_2S_7$	0.630
a_2	$S_1S_5S_8$	0.232
a_3	$S_1S_5S_8S_7$	0.232

表 5 攻防双方支付矩阵

攻击方	防御方	
	策略 d_1	策略 d_2
策略 a_1	$-C_{r_1}-AC_1,C_{r_1}-DC_1$	$p_{s_1}C_{r_1}-(1-p_{s_1})C_{r_1}-AC_1$， $(1-p_{s_1})C_{r_1}-p_{s_1}C_{r_1}-DC_1-DC_2$
策略 a_2	$p_{s_2}C_{r_2}-(1-p_{s_2})C_{r_2}-AC_2$， $(1-p_{s_2})C_{r_2}-p_{s_2}C_{r_2}-DC_1-DC_2$	$-C_{r_2}-AC_2,C_{r_2}-DC_2$
策略 a_3	$p_{s_3}(C_{r_1}+C_{r_2})-(1-p_{s_3})(C_{r_1}+C_{r_2})-AC_3$， $(1-p_{s_3})(C_{r_1}+C_{r_2})-p_{s_3}(C_{r_1}+C_{r_2})-DC_1-DC_2$	$-(C_{r_1}+C_{r_2})-AC_3,(C_{r_1}+C_{r_2})-DC_2$

由于获取 Web 服务器权限后，会对数据库服务器和文件服务器造成威胁，设数据库服务器和文件服务器资源重要程度各为 100，则 Web 服务器的重要程度 $C_{r_1}=200$，另设攻击面转移成本 $ASSC_1$ 为 20，负面转移成本 NC_1 为 40，则 $DC_1=60$；获取堡垒主机权限后，会对数据库服务器、文件服务器、内网用户和 Web 服务器均造成威胁，设内网用户重要程度为 100，则堡垒主机的重要程度 $C_{r_2}=500$，另设攻击面转移成本 $ASSC_2$ 设为 50，负面转移成本 NC_2 设为 30，则 $DC_2=80$。攻击成本根据每条攻击路径的难度确定，路径攻击成功概率越高，需要经过的节点越少，攻击成本越低，可将 2 种策略的攻击成本分别设为 $AC_1=10,AC_2=30,AC_3=35$。

攻击者对策略的选择，一般由攻击路径的难度决定，攻击难度越高，选择的概率就越少，因此可依据路径攻击成功概率作归一化处理，计算出攻击者对策略选择的概率分布，得攻击者选择策略的概率为 $p(a_1)=0.58,p(a_2)=0.21,p(a_3)=0.21$。在当前状态下，将各参数带入表 5 中公式，攻击方 3 种策略的收益效用函数以 $U_{a_j}=\max\{U_{a_i\to d_k}\}$ 的原则取值，分别为 $U_{a_1}=42,U_{a_2}=-298,U_{a_3}=-410.2$，因为不清楚防御方的动态防御策略，若理性分析会选择收益最大的策略 a_1 为行动策略。对于防御方来说，根据攻击策略的概率分布，通过计算期望收益的效用函数得 $EY_{d_1}=157.472,EU_{d_2}=117.54$，防御方采取策略 d_1 将获得最大收益。

3.3 仿真分析

从攻防双方收益情况对比、防御方实际收益与期望收益对比和与无差别迁移策略[8]对比等 3 方面入手，验证所提策略的有效性和先进性。考虑到网络平台节点间的非线性耦合关系，全平台动态迁移时各平台业务承载能力必将因相互影响而急剧下降，因此无差别迁移中负面影响成本应较单一节点迁移时更高，设此策略下 Web 服务器 NC 为 80，堡垒主机 NC 为 60，$ASSC$ 与前文相同。攻击者按照 3.2 节中计算出的对策略选择概率选择攻击策略，防御方按照前文方法计算期望收益选择防御策略。进行 1 000 次蒙特卡洛仿真实验，对收益情况进行累加计算，统计新策略下的攻防双方实际收益和无差别迁移下防御方的实际收益情况，绘制防御方期望收益累计曲线以作对比，仿真结果见图 3～5。

图 3 为攻防双方实际收益比较图。由图中可

知，防御方收益始终处于增长状态，1 000 次攻防实验后，防御方实际收益达 4.403×10^4，而攻击方收益处于下降趋势，最终攻击方收益为 -1.625×10^5，证明单阶段静态博弈策略有效。

图 4 为防御方实际收益与期望收益比较图。由图中可知，防御方实际收益始终围绕期望收益变化，期望收益最终为 4.324×10^4，实际收益与期望收益偏差约 1.8%，证明实际收益与理论计算收益接近，理论收益计算方法正确。

图 5 为单阶段静态博弈策略与无差别迁移对比图。由图中可知，新策略收益上升迅速，无差别迁移策略上升缓慢，最终收益为 5 100，远低于新策略收益，表明新策略优于无差别迁移策略，能够改善无差别迁移成本过高的问题。

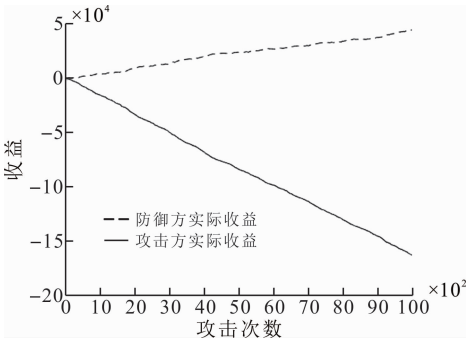

图 3　攻防双方实际收益

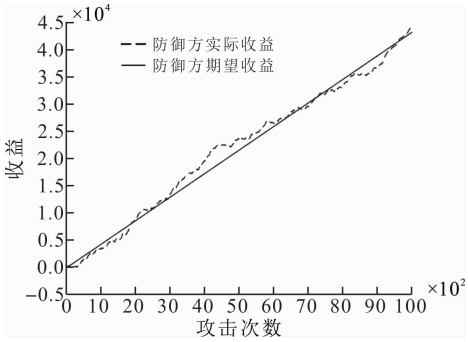

图 4　防御方实际收益与期望收益比较

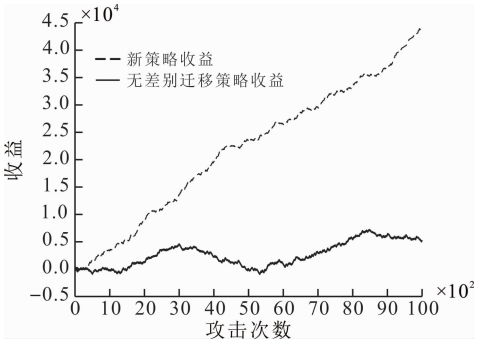

图 5　新策略与无差别迁移策略收益对比

4　结语

针对 PDD 策略设计中节点迁移的选择问题，从分析 PDD 原理入手，建立了 PDD 完全信息博弈模型，设计了 PDD 单阶段静态博弈策略，示例和仿真验证了新策略的优越性。下一步仍需对仿真验证环境进行改进，以实际网络环境中的 PDD 系统，收集更为贴切的数据。

参考文献(References)：

[1] OKHRAVI H, COMELLA A, ROBINSON E, et al. Creating a Cyber Moving Target for Critical Infrastructure Applications Using Platform Diversity[J]. International Journal of Critical Infrastructure Protection, 2012, 3(1): 30-39.

[2] PENG W, LI F, HUANG C T, et al. A Moving-Target Defense Strategy for Cloud-Based Services with Heterogeneous and Dynamic Attack Surfaces[C]// 2014 IEEE International Conference on Communications (ICC). Sydney, NSW, Australia: IEEE, 2014: 804-809.

[3] HUANG Y, GHOSH A K. Introducing Diversity and Uncertainty to Create Moving Attack Surfaces for Web Services[M]//JAJODIA S, GHOSH A K, SWARUP V, et al. Moving Target Defense-Creating Asymmetric Uncertainty for Cyber Threats, New York: Springer, 2011: 131-151.

[4] BANGALORE A K, SOOD A K. Securing Web Servers Using Self Cleansing Intrusion Tolerance (SCIT)[C]// DEPEND'09, the Second International Conference on IEEE. Athens, Glyfada, Greece: IEEE, 2009: 60-65.

[5] AMIRREZA N, JAFAR H J, MAMOUN A. Web-MTD: Defeating Cross-Site Scripting Attacks Using Moving Target Defense[J]. Security and Communication Networks, 2019(2): 1-13.

[6] 刘丹军，蔡桂林，王宝生. AMTD:一种适应性动态目标防御方法[J]. 网络与信息安全学报，2018，4(1)：15-25.
LIU D J, CAI G L, WANG B S. AMTD: A Way of Adaptive Moving Target Defense [J]. Chinese Journal of Network and Information Security, 2018, 4(1): 15-25. (in Chinese)

[7] 马润年，陈彤睿，王刚，等. 面向隔离区异构平台的动态防御主动迁移策略[J]. 火力与指挥控制，2019，44(3)：1-8，22.
MA R N, CHEN T R, WANG G, et al. Dynamic Defense Active Migration Strategy for Heterogeneous

Platforms of DMZ[J]. Fire Control & Command Control, 2019,44(3):1-8,22. (in Chinese)

[8] 陈彤睿,马润年,王刚, 等.基于事件驱动和定时迁移的平台动态防御策略[J].计算机工程,2019,45(9):105-111.
CHEN T R, MA R N, WANG G, et al. A Strategy of Platform Dynamic Defense Based on Events-Driven and Timing Migration[J]. Computer Engineering, 2019,45(9):105-111. (in Chinese)

[9] 刘江, 张红旗, 刘艺. 基于不完全信息动态博弈的动态目标防御最优策略选取研究[J]. 电子学报, 2018, 46(1): 82-89.
LIU J, ZHANG H Q, LIU Y. Research on Optimal Selection of Moving Target Defense Policy Based on Dynamic Game with Incomplete Information[J]. Acta Electronica Sinica, 2018, 46(1): 82-89. (in Chinese)

[10] 张恒巍, 杨豪璞. 基于攻防信号博弈的 APT 攻击防御决策方法[J]. 计算机工程与设计, 2019, 40(1): 59-64.
ZHANG H W, YANG H P. Defense Decision-making Method for Anti-APT Attack Based on Attack-defense Signaling Game[J]. Computer Engineering and Design, 2019, 40(1): 59-64. (in Chinese)

[11] LEI C, ZHANG H Q, WAN L M, et al. Incomplete Information Markov Game Theoretic Approach to Strategy Generation for Moving Target Defense[J]. Computer Communications, 2018, 116:184-199.

[12] TAN J L, LEI C, ZHANG H Q, et al. Optimal Strategy Selection Approach to Moving Target Defense Based on Markov Robust Game[J]. Computers & Security, 2019, 85:63-76.

[13] VAHID Z, MEHDI S. A Cost-Sensitive Move Selection Strategy for Moving Target Defense[J]. Computers & Security, 2018, 75:72-91.

[14] LI H R, GUO Y F, HUO S M, et al. Survey On Quantitative Evaluations of Moving Target Defense [J]. Chinese Journal of Network and Information Security,2018,4(9):66-76.

[15] 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.
LIU J, ZHANG H Q, YANG Y J, et al. Effectiveness Evaluation of Moving Network Defense Based on Host Security State Transition Model[J]. Journal of Electronics & Information Technology, 2017, 39(3): 509-517. (in Chinese)

[16] 高妮, 高岭, 贺毅岳, 等. 基于贝叶斯攻击图的动态安全风险评估模型[J]. 四川大学学报(工程科学版), 2016, 48(1): 111-118.
GAO N, GAO L, HE Y Y, et al. Dynamic Security Risk Assessment Model Based on Bayesian Attack Graph[J]. Journal of Sichuan University (Engineering Science Edition), 2016, 48(1): 111-118. (in Chinese)

[17] JIN B H, SIMON Y E, DONG S K, et al. Dynamic Security Metrics for Measuring the Effectiveness of Moving Target Defense Techniques[J]. Computers & Security, 2018,79:33-52.

[18] 孙奥, 殷肖川, 李小青. 一种面向任务的网络风险评估模型[J]. 空军工程大学学报(自然科学版), 2019, 20(5): 99-105.
SUN A, YIN X C, LI X Q. A Task-Oriented Network Risk Assessment Model[J]. Journal of Air Force Engineering University (Natural Science Edition), 2019, 20(5): 99-105. (in Chinese)

[19] 国家信息安全漏洞库. 漏洞信息[EB/OL]. (2018-11-03)[2019-07-16]. http://www.cnnvd.org.cn.
National Information Security Bulnerability Database. Vulnerability Information [EB/OL]. (2018-11-03)[2019-07-16]. http://www.cnnvd.org.cn. (in Chinese)

[20] National Vulnerability Database. Common Vulnerabilities and Exposures[EB/OL]. (2018-11-03)[2019-07-16]. https://nvd.nist.gov.

(编辑:徐楠楠)