拟态防御马尔可夫博弈模型及防御策略选择

张兴明，顾泽宇，魏帅，沈剑良
（国家数字交换系统工程技术研究中心，河南 郑州 450002）

摘 要：网络拟态防御通过冗余执行体动态性、多样性以及裁决反馈机制增强了主动防御顽健性，而对于其安全性评估尚缺少有效的分析模型，基于经典博弈模型无法满足于其多状态、动态性特点，不具有通用性等问题，提出拟态防御 Markov 博弈模型分析攻防状态间的转移关系以及安全可靠性度量方法，通过非线性规划算法计算攻防博弈均衡，以确定考虑防御代价的最佳防御策略。实验与多目标隐藏技术对比，结果表明拟态防御具有更高的防御效果，结合具体案例给出了针对利用系统漏洞攻击的具体攻防路径，验证了防御策略算法有效性。

关键词：网络拟态防御；Markov 博弈；冗余执行体；防御顽健性；主动防御策略
中图分类号：TP393
文献标识码：A
doi: 10.11959/j.issn.1000-436x.2018223

Markov game modeling of mimic defense and defense strategy determination

ZHANG Xingming, GU Zeyu, WEI Shuai, SHEN Jianliang
National Digital Switching System Engineering & Technological R&D Center, Zhengzhou 450002, China

Abstract: Network mimic defense technology enhances the robustness of active defense through the redundancy, dynamic and diversity as well as the decision feedback mechanism. However, little work has been done for its security assessment and existing classic game models are not suitable for its dynamic characteristics and lack of universality. A Markov game model was proposed to analyze the transfer relationship between offensive and defensive status and the measurement method of safety and reliability of mimic defense, and calculated the offensive and defensive game equilibrium through non-linear programming algorithm to determine the best defensive strategy considering performance. Experiments give a comparison with the multi-target hiding technique and shows that the mimic defense has a higher defensive effect. Combining with the specific network case, the specific attack and defense path for the exploit of the system vulnerability is given and the effectiveness of the defense strategy algorithm is verified.

Key words: network mimic defense, Markov game, redundant execution units, defense robustness, active defense strategy

1 引言

近年来，随着网络技术的发展，诸如勒索病毒、数据泄露等网络安全事件频发，造成了不可估量的利益损失。下一代网络基础设施建设已经逐步普及，设计研发人员将更多的精力集中于性能方面，网络安全未受到足够重视，如 2016 年思科爆出死亡之 Ping IPv6 协议漏洞，极易造成大面积地区网络切断的情况。另外，在 SDN 网络中，控制与数据分离强化了可编程，却造成了集中控制模式下单点脆弱性，一旦上层控制服务器受恶意控制，整片的网络区域将在攻击者的控制范围内。网络攻击大多基于系统、协议已有的漏洞、设计缺陷等[1]获取系统权限，进而实施非法行为，而基于目前的软硬

收稿日期：2017−12−06；**修回日期：**2018−09−22
基金项目：国家自然科学基金资助项目（No.61572520, No.61521003）；国家科技重大专项基金资助项目（No.2016ZX01012101）
Foundation Itesms: The National Natural Science Foundation of China (No.61572520, No.61521003), The National Science and Technology Major Project of China (No.2016ZX01012101)

件设计开发模式，系统弱点无法完全避免。同时，现有的安全防御技术如入侵检测系统、防火墙等对未知威胁，如 0-day 攻击收效甚微；另外，高级持续威胁（APT, advanced persistent treat）能够针对目标进行不断地探测与渗透攻击，而一旦遭受入侵，系统管理者则需要巨大的开销进行弥补，使网络攻击与防御态势严重不对称。基于诸如此类的问题，移动目标防御（MTD, moving target defense）思想作为美国政府提出的“改变游戏规则”的主动防御技术，旨在彻底打破被动的网络安全局面，通过随机化、多样性实现目标的动态隐藏，以破坏攻击链的连续性，从而提高攻击复杂度[2]。国内安全专家提出了拟态防御（MD, mimic defense）思想，将这种动态属性由单模扩展到多模，通过裁决机制增加防御顽健性[3]。

尽管国内外对于主动防御技术的研究已经取得了重大的突破与进展，但目前相关技术仍处于理论研究阶段，特别是拟态防御技术起步较晚，尚缺少有效的分析验证模型。对于现阶段主动防御技术有效性分析，多数的研究者通过经典博弈模型描述网络攻击者与防御者的博弈过程，常见的有领导者−跟随者博弈[4]、单控制随机博弈[5]、贝叶斯随机博弈[6]以及 Stackelberg 博弈模型[7]等。经典的博弈模型往往是静态、单一状态的，基于贝叶斯的随机博弈模型考虑了攻击者类型的不确定性，但仍不能满足主动防御场景中多状态、高动态性的特点。另一方面，现有的主动防御技术研究多从系统工程的角度描述架构问题，导致其防御动态变换具有盲目性、无指导的特点，往往导致较高的防御代价，未能充分考虑实际应用场景做出最佳的防御措施[8]。与本文研究最为接近的是文献[9]中所提出的移动目标防御 Markov 博弈模型，能够充分体现动态防御过程中攻防状态的多状态、马尔可夫性，然而文献[9]中给出的多目标隐藏模型并没有说明多个目标间的内在关系，且未给出具体的防御策略，尚不具有通用性。

基于以上对于主动防御技术的研究现状，本文针对网络拟态防御技术建立拟态 Markov 博弈模型（MGMD, Markov game model of mimic defense），以分析拟态防御中动态性、冗余多样性以及裁决机制对安全防御的有效性，基于 MGMD 模型构建非线性规划问题确定最佳防御策略，然后通过与多目标隐藏模型进行对比分析，并以 SDN 下的安全场景验证了策略选择算法。

本文主要贡献如下。

1) 从拟态冗余执行体容忍性的角度建立 Markov 博弈模型，通过定义多种状态路径转移描述执行体冗余性、多样性以及裁决反馈机制对攻防博弈过程的影响。

2) 根据攻防模型马尔可夫性建立安全度量模型，以分析拟态防御系统冗余执行体规模、可调度空间以及防御容忍度与防御效果的关系。

3) 针对利用系统已知或未知漏洞的攻击类型，考虑防御代价设计相应的最优主动防御策略确定算法，分析了拟态防御中多种多样化、动态性防御措施的混合策略。

2 网络拟态防御技术简介

拟态防御理念由国内邬江兴院士提出，旨在突破传统网络防御手段中静态、被动防御的局限，通过动态、异构、冗余思想构建主动防御特征[3]，具体防御思想主要体现为以下几个方面。

多样性冗余架构：结合拟态计算思想，拟态防御系统通过多个元功能相同的执行体共同完成任务处理。执行体间以不同等级不同层面的异构属性构造系统非相似余度，这种异构包括底层硬件、指令集、操作系统、上层应用编程语言以及程序多样化编译等层面。在同一异构冗余执行体集中，通过实现尽量多层面的异构属性，以达到系统所呈现的多样性特征，最大限度降低整个系统被控制的可能性，提高防御容忍性。

动态变换机制：系统动态特征通过动态变换机制实现主动防御动态属性，动态性的体现涵盖网络信息与主机系统信息的跳变、系统回卷与恢复等。

多模裁决机制：冗余执行共同完成任务处理输出数据，通过裁决反馈机制确定输出可靠性，同时实现执行体的异常检测与反馈，根据异常执行体的数量不同可将系统划分为多级安全工作模式[10]，以提高系统顽健性。

系统工作过程为输入—处理—输出模式，如图 1 所示，系统输入数据由数据分发器下发至冗余执行体，数据处理后由裁决机制进行判决并反馈，反馈的作用主要为根据当前安全等级与异常情况制定主动防御策略，最后输出正确的处理结果。拟态防御范围为整个数据处理模块，提高输出可靠性。

基于拟态防御的应用设计已经在多个网络基础设施平台进行了原型验证与测试，包括工控拟态处理器[10]、拟态 Web 服务器[11]、拟态路由器[12]等。

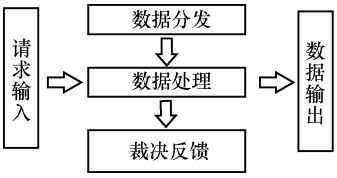


图 1　拟态防御系统工作流程

3　拟态防御攻防模型

3.1　拟态防御马尔可夫博弈模型

本节简要介绍拟态防御模型中的攻防策略，并通过马尔可夫链刻画攻防模型不同阶段的系统状态。

本文针对基于目前影响最广泛的已知或未知的系统、协议的漏洞以及不可控系统后门所造成的威胁情景，攻击者通过对这些系统弱点利用从而控制目标系统。攻击者为达到攻击目的所采取的攻击策略集涵盖目前常规攻击手段和高级持续攻击（APT）等，但不包括针对可用性的资源耗尽型攻击，如拒绝服务攻击等。防御者为阻断攻击者攻击过程、提高系统可靠性及保护系统安全性而采取一系列的防御策略。根据前文描述，防御者动态性因子包括应用级、内核级、操作系统级以及硬件指令级，根据实际应用场景限制及目前研究进展，暂不考虑硬件结构整体切换。

拟态防御马尔可夫博弈模型能够描述多阶段多状态的攻防博弈过程，针对一个特定的网络系统，其所处的系统安全状态与时间、攻击者采取的策略以及防御者采取的策略呈三维关系。可能用到的符号如表 1 所示。

表 1　**符号说明**

符号	说明
N	冗余执行单元（可调度）规模
K	执行单元规模
k	防御容忍度（突破防御所需攻击的最小执行体数量）
l	跳变深度（单个执行体中可动态跳变的种类）
$\boldsymbol{AV}$	攻击向量（N 网络或 L 本地）
AC	攻击复杂度
vul	系统弱点编号

定义 1　拟态防御马尔可夫博弈模型 MGMD 由六元组构成即 $\mathrm{MGMD}=\{C,S,A,\Psi,P,R\}$。

$C=\{att,def\}$ 为参与方，包括网络攻击者与防御者，防御者即拟态防御系统。

$S=\{S_0,S_1,\cdots,S_k\}$ 为攻防过程状态，根据防御容忍度模型共有 $k+1$ 个状态，各个状态表示系统在攻防双方采取一系列策略后所处的不同安全阶段，其中 S_0 为初始状态，即未受攻击时的安全状态，而 S_k 为终止状态，表示系统被攻击者完全突破，攻击者完成其攻击目的。

$A=\{a,\boldsymbol{d}\}$ 为双方动作集合，a 为攻击者动作，ε 为空动作，即不采取任何攻击动作。$\boldsymbol{d}$ 为防御者动作向量，同样地，防御者存在 ε 空动作，即不采取任何防御动作。

$\Psi=\{\lambda,\mu\}$ 分别为攻击者与防御者在当前状态的参与度，体现为随机化的混合策略。在本模型中，攻防双方按概率分布选择各自在当前状态的动作。那么，一个混合策略为某个博弈参与方采取相应动作的规则，即

$$\lambda=\{\lambda_i(a),a\in A,i=0,\cdots,k\}$$
$$\mu=\{\mu_i(\boldsymbol{d}),\boldsymbol{d}\in D,i=0,\cdots,k\}$$

其中，$\lambda_i(a)$ 为攻击者在状态 i 采取动作 a 的概率，且满足 $\sum_a\lambda_i(a)=1(0\leqslant\lambda_i(a)\leqslant 1)$，$\mu_i(\boldsymbol{d})$ 为防御者在状态 i 采取动作 $\boldsymbol{d}$ 的概率，且满足 $\sum_d\mu_i(\boldsymbol{d})=1,(0\leqslant\mu_i(\boldsymbol{d})\leqslant 1)$。

$P=P_{i,j}$ 为马尔可夫链状态转移概率，体现攻防博弈过程的马尔可夫性。其中，多阶段间的状态转移概率依赖于当前的系统状态以及攻防双方所采取的策略，即状态转移概率为当期状态与策略的函数。那么，在给定的策略组合 $\{\lambda,\mu\}$ 下，马尔可夫链 M 的状态转移概率 $P_{i,j}(\lambda,\mu)$ 可以表示为

$$\begin{aligned}P_{i,j}(\lambda,\mu)&=P\{S_{q+1}=S_j\mid S_q=S_i\}\\&=\sum P_{i,j}(a,\boldsymbol{d})\lambda_i(a)\mu_i(\boldsymbol{d})\end{aligned}\tag{1}$$

在实际场景中，当前的系统状态体现为系统的安全属性，如系统配置、网络通信模式以及开放服务和端口情况等。另一方面，通常情况下系统的状态转移很大程度上取决于防御者采取的策略，如端信息跳变、平台属性切换等。在本模型中由于安全属性的重要性，攻击者所采取的策略同样具有很大的决定因素，因此状态转移需要同时考虑攻防双方的策略。

在本文研究中，马尔可夫博弈模型通过转移状态描述攻防双方策略有效性，如对攻击者而言，一个有效的攻击策略能够使系统状态转移到终止 S_k 状态。

定义 2 MGMD 博弈过程由 $k+1$ 个不同状态的转移完成，且系统初始状态为 0，经攻击者与防御者双方混合策略决定状态转移过程。当系统状态达到 S_k 时，攻击者取得博弈胜利，即达到攻击目的，防御者在各个状态采取防御策略以阻止攻击者的攻击。

与 MTD 博弈模型不同的是，拟态防御博弈过程体现攻防双方更为复杂的策略与状态转移。一方面，拟态防御异构冗余架构将单模动态属性扩展到 N 模，攻击者控制系统所需要面对的不确定性因素随之线性增加；另一方面，由于拟态裁决反馈机制的作用，攻击者攻击单个执行体成功对于控制整个系统意义甚小，MD 具体攻防进程可以形式化为图 2 所示（实箭头为攻击进程，虚箭头为防御进程）。针对攻击者而言，不论是集中式或分布式的判决算法都需要同时获得一定规模的执行体控制权限才能破坏整个系统的安全性。本文在此不讨论具体的判决算法，为简化模型分析，作以下假设。

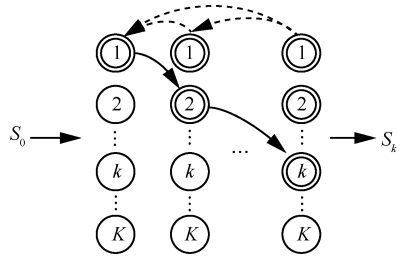


图 2 MD 攻防过程

假设 1 MGMD 博弈模型中时间是离散的，策略动作的执行可以看作是在同一时间片内进行，且由于 MGMD 模型策略的“随机化”特征，攻防双方仅能基于当前状态采取策略，而不能对对方的策略进行预测。

假设 2 拟态防御博弈模型 MGMD 中，拟态冗余体可调度空间规模为 N，当前执行体规模为 $K(K \leqslant N)$，当且仅当攻击者获知并成功利用 K 个目标系统中的 $k(k \leqslant K)$ 个攻击单元的组合，如利用系统弱点或漏洞等时，攻击者获得博弈胜利，即攻击者成功攻击目标系统所需要控制的目标数为 k，本文称 k 为防御容忍度。

3.2 拟态防御马尔可夫博弈过程

本节介绍并分析拟态防御马尔可夫博弈过程。假设防御系统采取的防御手段为主机信息、平台属性动态化跳变，防御者拥有 N 个异构冗余单元，其中，当前系统执行体规模为 K，单个执行体端信息或平台属性跳变深度为 l。实际场景下，由于端信息及平台多样性[13]的差异所构造的异构变体数量不等，如 IP 与端口资源池可以有几十甚至几百个，而元功能应用、编程语言则相对少些，为了便于定量分析，假设防御系统跳变深度 l=1，那么攻击者对该拟态系统攻击成功的条件为控制当前 K 个执行体中的 k 个。

本模型将攻防双方所采取的动作作以下说明。

1) 防御者动作：防御者采取无记忆的动作模式，当前状态所进行的防御动作与之前的攻击者动作、防御者动作以及系统状态均没有概率影响。在博弈过程中，防御者动作具有最优先权限，即当防御者采取动作时，系统随之立即进行状态的转移，而无视于攻击者的攻击进程。

2) 攻击者动作：攻击者通过弱点探测、漏洞利用以及提权等网络攻击手段对系统进行攻击。考虑高级攻击者类型，模型允许攻击者在攻击过程中是有记忆的，记忆内容为攻击者采取过的策略和系统历史信息，其中，系统历史信息包括防御者在当前执行单元所进行的端信息与平台属性跳变历史以及系统弱点信息历史等。

3) 空动作：没有任何动作的执行。模型允许攻防双方均存在空动作，其原因在于策略的“随机性”以及双方掌握对方的不完全信息。一方面，攻击动作包括并很大程度上依赖于前期的弱点探测过程，攻击动作的执行并不一定导致系统的崩溃，那么防御者可能将探测数据流误认为正常流量而不采取防御措施；另一方面，攻击者相对拥有更多的主动性与适应性，例如潜伏行为。

通常，防御者不能获知攻击者采取的攻击策略历史，以及当前时刻是否采取了攻击动作，但允许攻击者能够立即察觉到系统状态的改变，从而进行后续攻击进程。为了便于分析，由于存在攻防双方同时采取动作的情形，模型以排队队列的方式接收动作请求，请求队列服从参数为 γ 的泊松过程，此时当且仅当防御者未采取动作时，攻击者的动作请求才可以被满足。

图 3 为 MGMD 状态转移过程，其中，向右过程从攻击者的视角出发，S_0 为攻击者攻击进程初始阶段，该状态下攻击者控制的目标执行单元为 0 个。随着攻击的持续，后续的递推状态代表被攻击者攻击成功的执行单元数递增，直到最终状态 S_k 为系统执行体集中有 k 个执行单元被攻击者攻击成功并取得最高权限，即整个系统被攻击者突破。另一方面从防御者的角度看，防御进程是状态反向推进的过

程。有效防御动作的执行，意味着被攻击者控制的执行单元数量递减，直到防御策略覆盖所有被攻击者控制的执行单元，系统恢复到初始状态 S_0。暂不考虑攻防双方采取的行为策略，即认为博弈参与者所采取相应动作的概率为 1，则

1) 从攻击者的角度，假设攻击者在当前状态对于目标执行单元的选择是随机的，且仅能对单个目标进行探测。那么在状态 S_i 下，攻击者需要从 $K-i$ 个执行体中选择攻击目标并攻击成功，系统状态进入 S_{i+1}。即

$$P_{i,i+1}=\frac{\lambda(K-i)}{N-i},0\leqslant i\leqslant k-1 \tag{2}$$

2) 从防御者的角度，为区别于 MG-MTD 模型，分两种情况讨论。

① 假设防御者的一次防御策略只能对一个节点执行动作，即在状态 S_i 采取了有效防御动作，意味着被攻击者控制的 i 个执行体中的一个被选中并实施主动防御策略（如端信息跳变），那么攻击者在该执行体所获得的攻击资源被刷新，系统状态进入 S_{i-1}，即

$$P_{i,i-1}=\frac{\mu i}{K},0<i\leqslant k \tag{3}$$

② MGMD 需要考虑拟态防御系统多模裁决机制对攻击者的容忍与异常检测能力，即在一定的容忍范围内，系统防御策略存在对多个执行体同时执行防御动作的场景。而此情形区别于针对单个执行体防御动作的重复执行过程，多模裁决机制将异常执行单元判作受攻击目标而执行防御跳变策略，体现为有选择、更精确的防御动作。本文考虑相对脆弱性的防御者，裁决机制为多数一致性判决算法，一步防御跳变策略不保证完全刷新所有受控节点攻击痕迹，那么，此情况下受攻击节点数量 i 少于防御容忍度 k，且 i 越小，拟态裁决的能力越大，对被控节点的检测能力也就越大。本文定义拟态裁决能力随受攻击节点数量变化关系为凹函数 $\omega(i)\in(0,1]$，其中 $\omega(i)=\theta\exp(\alpha i),0\leqslant i\leqslant k$，$\theta$，$\alpha$ 为折扣参数。形式化地，MGMD 存在非相邻状态反向跳转路径，防御者对受攻击节点中的 $i-g$ 个成功进行了跳变刷新，即 MGMD 从状态 S_i 返回到状态 S_g，那么

$$P_{i,g}=\mu C_i^{i-g}\prod\omega^{i-g}(i)[1-\omega(i)]^g,0<i\leqslant k,0\leqslant g<i \tag{4}$$

3) 自转移：MGMD 存在状态自转移路径，当且仅当攻击者在当前状态 S_i 下采取空动作或未能对执行体集中剩下的 $k-i$ 个目标实施有效攻击策略，且防御者在状态 S_i 采取空动作或未能对被攻击者控制的 i 个执行体采取有效防御动作，那么，

$$P_{i,i}=1-P_{i,i+1}-\sum_g P_{i,g},0\leqslant i\leqslant k,0\leqslant g<i \tag{5}$$

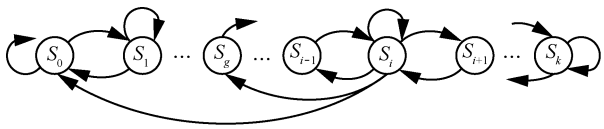


图 3　MGMD 状态转移过程

3.3　安全性分析

本节分析 MGMD 中的安全性问题。基于上节的分析，防御系统在状态 S_0 到状态 S_{k-1} 都是相对安全的，攻击者虽然对多个目标执行体进行了有效探测与控制，但未能突破拟态防御系统的最终防御能力。为了便于分析，本文通过攻击者攻击成功的概率刻画系统防御能力。

定理 1　在 MGMD 中，攻击者成功攻击拟态防御系统的概率 $P_{\text{att}}\leqslant\pi_k$，其中，$\pi_i,0\leqslant i\leqslant k$ 为 MGMD 在状态 i 的稳态概率。

证明 1　首先证明 MGMD 存在平稳分布。由上述分析，MGMD 存在 $k+1$ 个不可约状态，那么该马尔可夫链只有正常返态，故马氏链 MGMD 必存在平稳分布。

证明 2　若 $\{\pi_j,j\in S\}$ 是马尔可夫链 MGMD 的平稳分布，那么

$\pi_j=\sum_{i\in S}\pi_i P_{i,j}^{(n)}$，且 $\sum_{j\in S}\pi_j=1,\pi_j\geqslant 0$，则

$$\pi_j=\lim_{n\to\infty}p_j(n)=\lim_{n\to\infty}\sum_{i\in S}p_i P_{i,j}^{(n)}$$

其中，$p_j(n)$ 为马尔可夫 MGMD 链的绝对概率，p_i 为其初始概率，$P_{i,j}^{(n)}$ 为状态 i 经 n 步转移到状态 j 的概率。

综合证明 1 和证明 2，马尔可夫链 MGMD 中，状态 k 的稳态概率 π_k，表示 MGMD 过程中终到状态 k 的极限概率，即 MGMD 中攻击者攻击成功的概率。

下面对 MGMD 安全性进行定量分析。安全性的定量分析体现为攻击者达到状态 k 的最大概率，为了便于分析，且考虑相对脆弱性的防御者属性，本分析假设防御者不存在对多个执行体同时执行防御策略的情况，即

$$P_{i,g}=0,0<i\leqslant k,0\leqslant g<i$$

那么，MGMD 转化为一条生灭链，根据马尔可夫链平稳分布性质 $\pi_j=\sum_{i\in S}\pi_i P_{i,j}^{(n)}$ ，可得

$$\pi_0=\frac{\mu}{K}\pi_1+\left(1-\frac{\lambda K}{N}\right)\pi_0$$

$$\pi_i=\frac{\lambda(K-i+1)}{N-i+1}\pi_{i-1}+\frac{\mu(i+1)}{K}\pi_{i+1}+\left[1-\frac{\lambda(K-i)}{N-i}-\frac{\mu i}{K}\right]\pi_i,1\leqslant i\leqslant k-1$$

$$\pi_k=\frac{\lambda(K-k+1)}{N-k+1}\pi_{k-1}+\left(1-\frac{\mu k}{K}\right)\pi_k$$

推导得

$$\pi_k=\pi_0\prod_0^{k-1}\frac{\lambda K(K-i)}{\mu(i+1)(N-i)}\leqslant\left(\frac{\lambda K(K-k+1)}{\mu k(N-k+1)}\right)^k \quad (6)$$

由此可见，拟态防御模型的安全防御能力取决于多个系统参数：异构系统最大冗余规模 N 、冗余执行单元规模 K 以及防御容忍度 k 。本模型在上述讨论中认为攻击者选择执行体后攻击成功的概率为 1，且事实上拟态防御系统的反馈判决机制会大大降低攻击者的成功概率，因此 π_k 要远远小于该上界，这一点本文将在第 4 节进行验证。直观地，增加系统容忍度与最大冗余规模能够非线性地提高安全增益，但在实际场景中 N 无法达到足够大，那么可以通过改变容忍度 k 与执行单元规模 N 的关系以实现更高的安全收益。

3.4 优化防御策略选择

盲目、无指导的主动防御措施往往会导致过高的性能损失，降低防御性价比，优化的防御策略需要根据具体的安全状态进行有针对性的调整[14]。本节分析防御系统如何利用拟态防御马尔可夫模型选择最优的防御策略，其中，包括攻防双方不同策略的收益与代价评估标准，然后针对防御者分析系统最优防御策略，并给出策略选择算法。

拟态防御范围主要针对目标系统元功能的数据处理以及输出数据可信可靠，其跳变与动态变换过程能够对系统状态进行刷新，非相似冗余度执行体同时保证了元功能可用性。那么对于防御者而言，攻防博弈过程中的收益包括拟态防御所产生的系统动态性、冗余体同源关联度的降低、容忍度（输出可信度）的提高以及可利用攻击表面的刷新，而安全性的提高意味着可能存在的系统性能的下降或功耗的增加，由于冗余执行与拟态裁决机制，忽略动态变换过程对元功能可用性的影响；另一方面，从攻击者的角度，考虑高级攻击者能够对目标系统进行充分的弱点挖掘与渗透，那么针对防御系统的攻击过程会随系统的动态变化而进行策略进化[15]，这就要求防御系统做出针对特定攻击向量的策略，本文定义可利用攻击表面为攻击者为渗透目标系统所能够利用的攻击资源包括系统弱点和网络路径等。本文不考虑攻击者的攻击行为本身的消耗，即认为其可利用攻击资源不受限制，则攻击者的收益来源为目标系统可利用攻击表面的增加，同时本模型认为攻击者是适应型、有记忆的，对已利用攻击表面能够进行相似侦测与同源攻击，那么同防御者收益对应的冗余体相似性的增加作为攻击者的攻击收益。

定义 3 R 为 MGMD 过程中的收益函数。那么

$$\begin{aligned}R_i^A&=\Delta R-\Delta AS\\R_i^D&=\Delta AS-\Delta R-\Delta DC\end{aligned} \quad (7)$$

分别为攻击者与防御者博弈过程收益函数。其中，ΔAS 为可利用攻击表面的改变，ΔR 为容忍度的改变，被攻击者控制的执行体越多，体现为系统容忍度越小，ΔDC 为防御动作产生的性能损失。

以上收益函数为博弈过程中博弈参与者在状态 i 的策略收益，博弈双方在当前状态的策略不仅决定了当前状态双方收益，还对未来状态产生影响。攻防双方均追求收益最大化，那么博弈过程为马尔可夫决策过程，双方根据当前状态为最大化自身收益从策略集中选择一个动作，然后系统进行状态转移。由相关研究[16]，在马尔可夫博弈过程中，若博弈一方采取马尔可夫优化策略，那么博弈另一方必然也采取最优策略以实现收益最大化，那么博弈均衡策略为马尔可夫博弈过程双方的最优策略，下面证明纳什均衡策略的存在性。

定理 2 MGMD 博弈过程必然存在纳什均衡策略。

证明 MGMD 为二维马尔可夫博弈过程，其状态是有限的（k+1 个状态），且攻防双方采取有限的混合策略，那么根据相关研究[17-18]可证 MGMD 存在纳什均衡策略。

因此，以攻防双方收益函数作为各自评价函数 U ，即 $U=R$ ，由于拟态攻防模型的特殊性，状态并不是同普通攻防博弈一样随攻击链顺序递增，而

是反映真实系统受控状态，那么评估当前策略对未来收益的影响具有较复杂的关系，本文对此不作深入讨论。对于一个给定的 MGMD 模型，假设为博弈均衡策略 λ^*、μ^*，U^* 为该策略下的收益评价函数，那么 $U^* = R(\lambda_i^*, \mu_i^*)$。事实上博弈过程可能存在局部最优的中间状态使两者不能取得等值，而确定最优策略的问题通过优化过程中不断缩小 $U^n - R^n$ 的值解决，即非线性优化问题其目标函数为

$$\begin{aligned} &\min \sum_{n\in N, S_i\in S} U_i^n - R_i^n(\lambda_i, \mu_i) \\ &\text{s.t.}\ \ U_i^n \geqslant R_i^n(\lambda_i, \mu_i) \\ &\quad \forall S_i, \sum_a \lambda_i(a) = 1, \sum_d \mu_i(\boldsymbol{d}) = 1 \\ &\quad \lambda, \mu \in [0,1] \end{aligned} \tag{8}$$

根据以上分析，现给出基于 MGMD 博弈过程的最优防御策略选择算法 OSSA，详细过程如下所示。

输入　网络与系统配置参数

输出　MGMD 最佳防御策略

Begin

初始化网络系统配置信息，得到防御系统 N, K, k, l 等参数；

对攻击者攻击类型、防御系统脆弱性进行评估，建立可用的资源集合、威胁集合；

根据系统信息与威胁模型构造攻防策略集；

输入 MGMD 状态转移概率，建立 MGMD 博弈模型；

计算攻防双方动作收益；

解决非线性规划问题 $\min(U^n - R^n)$ 计算博弈均衡，得出相应均衡策略；

输出最优策略；

End

4　基于 SDN 的 MGMD 框架设计

SDN 分离了网络数据与控制，并将控制权限集中于控制服务器。控制服务器对外分为南向接口与北向接口，北向接口连接网络定制功能的应用服务器，南向接口连接交换机客户端，来自南向接口的网络流请求经过控制服务器处理下发至交换机产生特定的网络流规则，这种输入、处理、输出的工作模式吻合拟态防御系统的防御条件。因此，MGMD 基于 SDN 中控制服务器设计的防御框架如图 4 所示，框架包括网络状态监测模块、防御决策模块、裁决机制以及冗余执行体。

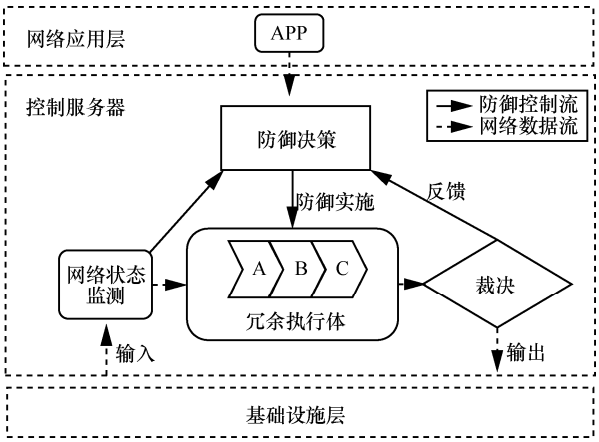


图 4　基于 SDN 的 MGMD 框架

MGMD 框架各个组成模块作用及工作过程如下：网络状态监测模块负责监听当前网络状态，并接收来自南向接口的网络数据请求；冗余执行体负责处理网络请求并输出；裁决机制对冗余执行体的输出数据进行一致性判决，输出判决后的数据并将冗余执行体的裁决结果反馈到防御决策模块；防御决策模块同时接收来自网络监测模块与裁决机制的信息，根据网络安全状态与反馈信息确定具体的主动防御策略，并将这一控制流下发至冗余执行体进行防御实施。

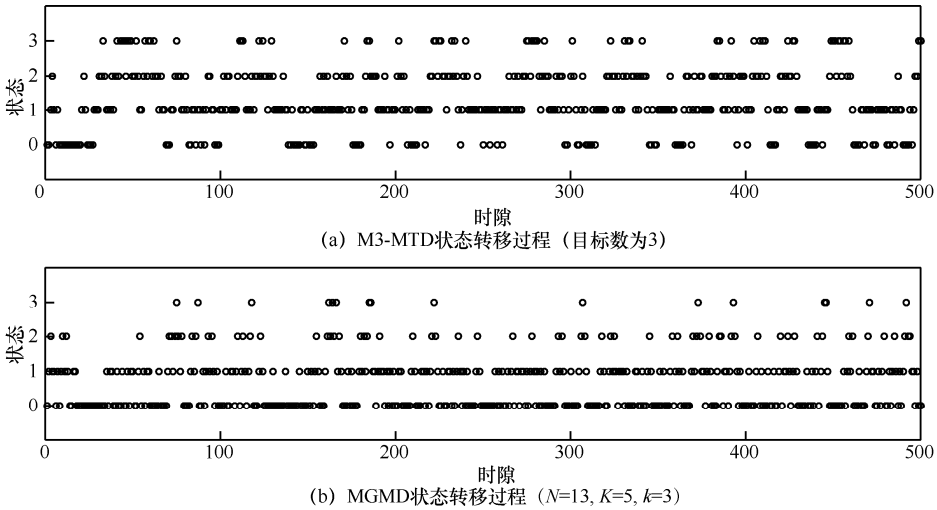
5　实验验证与分析

为验证拟态防御马尔可夫博弈模型以及防御策略选择算法的有效性，本文进行了相应的实验与分析。

5.1　MGMD 模型有效性与安全性分析

根据本文第 3 节分析，MGMD 模型体现拟态防御系统中攻防双方博弈过程，其中，攻击者以到达状态 k 作为攻击的最终目的，由于 MGMD 状态马尔可夫性，具体状态转移依赖于攻防双方所采取的当前策略。为更好地刻画模型安全性，以 MCMC（马尔可夫链蒙特卡洛）方法对博弈过程进行仿真，仿真平台为 Matlab R2014a。

实验仿真选择多目标隐藏[9]与拟态防御进行对比，其中，多目标隐藏中目标数量为 3，拟态防御实验参数中，冗余执行体数量为 5，执行体可调度空间为 13，攻击者达到攻击目的所需控制的目标数量均为 k=3，即防御容忍度为 3 且攻防双方对参与博弈进行的泊松过程参数相等，采取动作互斥且概率均为 0.5，在实际场景中攻击者与防御者博弈过程可能是瞬时的，仿真过程定义每次状态发生过程出现在一个时间片内。本文对 500 个状态进行抽样，详细状态转移过程结果如图 5 所示。



(a) M3-MTD状态转移过程（目标数为3）

(b) MGMD状态转移过程（N=13, K=5, k=3）

图 5　状态转移过程

根据前文描述，系统初始状态即状态 0 为未受到任何攻击的状态，攻防博弈过程从状态 0 开始，经过多次状态转移达到状态 k 为攻击完成状态。数据表明多目标隐藏 M3-MTD 过程更容易进入状态 k，而拟态防御 MGMD 过程在经历了 59 次状态转移之后首次到达状态 k，且在全局分布中较为稀疏；图 6 描述了两种马尔可夫博弈过程状态分布，可以看出多目标隐藏博弈状态多集中于中间状态，状态 0 与状态 k 数量相当，而 MGMD 则集中于状态 0，状态 k 分布明显少于 M3-MTD，那么从安全防御的角度，状态分布越集中于状态 0，系统防御有效性越优，相比多目标隐藏，拟态防御模型中攻击者控制多个目标攻击完成的概率更小。

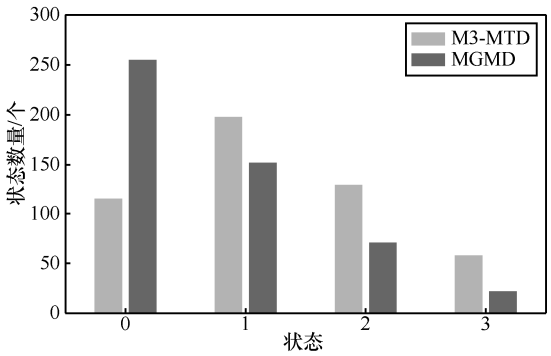


图 6　MGMD 与 M3-MTD 状态分布

拟态防御中对攻击容忍性体现在多模冗余执行体共同完成拟态裁决机制，即防御机制在数据输出顽健性提供了保证，个别执行体受到攻击对整体输出影响较低，同时拟态裁决实现对恶性执行体的攻击检测，当然这种机制还依赖于具体的判决方案如等价执行体、信任度执行体等。直观地，拟态调度资源池规模越大，拟态调度空间越大，通过调度所呈现的系统多样性越强，那么拟态防御效果越明显。拟态调度空间包涵多个层次的调度单元组合，包括从底层的硬件架构到上层应用多样性，以及执行单元端信息跳变等，由于不同层次的拟态调度所呈现的多样性特征不能一概而论，本文模型只是将各层次统一定义在调度规模 N 之内，具体内容将在下一步工作继续研究。

5.2　网络实例分析

为分析 MGMD 模型攻防双方的具体行为策略与博弈收益，以确定最优防御策略，验证第 4 节策略选择算法的有效性，本节实验仿真通过一个具体的网络拓扑探讨以上问题。

图 7 所示为软件定义数据中心网络部分网络节点拓扑，控制服务器作为拟态防御措施的应用目标，采取多个控制服务器作为冗余执行体协同工作，同时攻击者可以通过网络等途径访问控制服务器。应用服务器作为控制服务器的应用提供者。

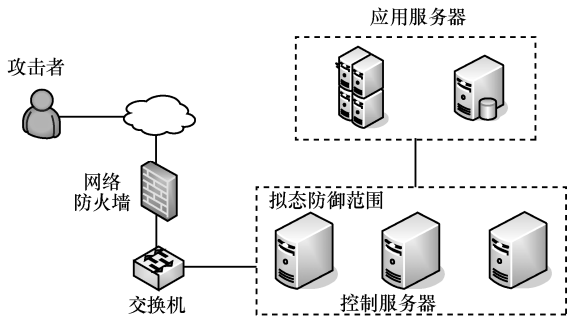


图 7　实验网络拓扑

威胁模型：本文假定攻击者能够实施高级持续威胁，能够绕过网络防火墙渗透到数据中心服务器集群，通过入侵控制服务器篡改控制器输出数据进

而改变网络流规则，达到控制目标网络的目的。

拟态防御范围：控制服务器集群，不包括控制器北向连接的应用数据服务器等。

本实验中，多控制器协同控制执行体规模为 K=5，多数一致性判决条件为达到 k=3 一致，那么基于此网络拓扑的 MGMD 状态为 S_0，S_1，S_2，S_3 的 4 种状态。本文假设网络基础设施如 SDN 控制器服务器已关闭系统自动更新功能，除了 0-day 漏洞外，系统仍存在已知的通用系统漏洞，实验通过漏洞扫描工具 Nessus 对系统进行弱点扫描。初始状态下多控制器执行体操作系统配置参数及弱点扫描结果如表 2 所示。

攻防过程中，攻击者能够对系统弱点进行扫描、发现，即拟态防御系统不能有效阻止全部的探测行为，包括针对网络的扫描，IP 端口、服务开放情况，针对主机的扫描，操作系统类型版本、系统漏洞等。攻击者每一次动作仅能对已扫描到的一个系统弱点进行利用，且对于已获取的系统弱点不再重复探测，那么 MGMD 的博弈过程不分析攻击链的扫描探测阶段，而侧重于针对漏洞弱点的系统防御顽健性，因此在实际部署的网络场景中，由于探测的复杂性，这种攻击成功率要低得多。防御手段主要为系统主动防御方法如 ASLR、ISR 以及其他提高系统多样性方式等，MGMD 博弈为不完全信息非零和博弈，那么防御者对攻击者当前的策略是未知的，因此防御动作存在空操作 NOP。综上列出针对漏洞的主要攻防策略如表 3 所示，CVSS 是对系统弱点类型、攻击复杂度以及所需权限等属性进行量化分析的工具[19]，实验使用 CVSS 3.0 对扫描到的系统漏洞进行评估，而相应的攻击成功概率在文献[20]中已经进行了研究。本文以此可以得出 MGMD 状态转移概率如表 4 所示。

表 2　　系统配置参数及弱点信息扫描结果

主机	操作系统	系统弱点信息	No.	CVSS 评分	弱点属性
C1	Windows Server 2008	CVE-2017-0299 KASLR	1	5.0	AV:L/AC:L
		CVE-2017-0148 SMB 远程缓冲区溢出	2	8.1	AV:N/AC:H
C2	Ubuntu 14.02	CVE-2016-10229 kernel 远程执行代码	3	9.8	AV:N/AC:L
		CVE-2017-1000367 本地覆盖提权	4	6.4	AV:L/AC:H
C3	Debian 7.0	CVE-2016-10229 内核远程执行代码	5	9.8	AV:N/AC:L
		CVE-2016-1247 web-root 提权	6	7.8	AV:L/AC:L
C4	OpenBSD 6.0	CVE-2017-1000364 远程内存破坏	7	7.4	AV:L/AC:H
C5	RedHat 6.0	CVE-2017-1000364 远程内存破坏	7	7.4	AV:L/AC:H
		CVE-2017-1000367 本地覆盖提权	4	6.4	AV:L/AC:H

表 3　　攻防双方策略集合

S_0	S_1
a ={buffer overflow, code injection, NOP}	a ={code injection, ROP, NOP}
d ={ASLR, ISR, NOP}	d ={ASLR, ISR, patch upgrade, system roll-back, NOP}
S_2	S_3
a ={privilege gain, NOP}	a ={ROP, NOP}
d ={diversified compilation, system roll-back, NOP}	d ={diversified compilation, NOP}

表 4　　状态转移概率

S_0	S_1	S_2	S_3
$P_{0,1}(a_1,d_2)=0.41$ $P_{0,1}(a_2,d_1)=0.78$ $P_{0,0}(a_3,d_3)=0.98$	$P_{1,2}(a_1,d_1)=0.37$ $P_{1,2}(a_2,d_3)=0.37$ $P_{1,0}(a_1,d_2)=0.90$ $P_{1,0}(a_2,d_4)=0.98$ $P_{1,1}(a_3,d_5)=0.98$	$P_{2,3}(a_1,d_2)=0.32$ $P_{2,1}(a_1,d_1)=0.86$ $P_{2,2}(a_2,d_3)=0.98$	$P_{3,2}(a_1,d_1)=0.82$ $P_{3,3}(a_2,d_2)=0.98$

在攻防双方收益量化分析方面，通常基于特定类型的系统弱点进行具体评估，主要包括漏洞发生频率、攻击复杂度，对于防御方通常考虑防御回报以及防御代价等，结合相关研究[20]以及拟态防御特殊性，根据收益函数计算各状态下的双方收益矩阵如表 5 所示。然后通过 Matlab 中的非线性规划工具集得出均衡策略与收益如表 6 所示。

本实验攻防状态主要以系统弱点（漏洞）信息为攻击切入点，不再区分具体的执行体而是将各个执行体作为等价的单元后为一个系统整体，攻击者可以通过网络访问服务器主机，通过漏洞利用提取主机管理员权限。状态转移如图 8 所示详细描述了攻防过程并具体到各个状态下每一条路径转移所采取的动作及所利用的系统弱点。其中，S_0 为系统初始状态，系统执行体均未被攻击者控制，S_3 为攻击者成功控制 3 个执行体的状态，即拟态防御系统防御有效性丧失。箭头实线表示各个状态间的转移路径，受关联于攻击者所利用的系统弱点、采取的攻击方式以及防御者采取的策略，状态上方路径均为攻击有效路径，下方路径均为防御有效路径（不包括自转移路径）。

攻击路径与策略分析：在攻防过程中，攻击者优先选择攻击复杂度较低的系统弱点，例如 SMB 缓冲区溢出漏洞，而防御者需要选择合适的防御措施以针对具体的攻击行为，例如基于应用内核级的地址空间布局随机化 ASLR 往往不能有效抵御对于 NOP slides 代码注入型攻击以及 ROP 代码重用攻击，路径 $S_0 \to a_2, vul_6, d_1 \to S_1$ 体现了基于该类型攻击防御失效。应用多样化编译对目标程序进行代码随机化可以有效地防范注入性攻击。通过收益矩阵与均衡策略可以看出，防御者采用 ASLR 与 ISR 针对具体的攻击类型时有较高的收益，但其防御的攻击类型有限，因此在均衡策略中防御者以较大概率选择了 patch upgrade 方式对漏洞进行修复。另一方面，system roll-back 能够刷新系统状态，对多数攻击有效，然而从收益矩阵看出其防御收益并不高，在于其造成的性能损耗较大。利用多个执行体共有的漏洞如 vul_4, vul_7，攻击者往往会获得更多的收益，

表 5　　**收益矩阵**

S_0	S_1	S_2	S_3
$\begin{pmatrix}-10 & 25 & 30\\ 25 & -10 & 30\\ -10 & -10 & 0\end{pmatrix}$	$\begin{pmatrix}25 & -10 & 0 & 0 & 30\\ 28 & 28 & 20 & 0 & 30\\ -10 & -10 & 0 & 0 & 0\end{pmatrix}$	$\begin{pmatrix}-15 & 30 & 30\\ -15 & 0 & 0\end{pmatrix}$	$\begin{pmatrix}-15 & 30\\ 15 & 0\end{pmatrix}$
$\begin{pmatrix}5 & -30 & -30\\ -30 & 5 & -30\\ 5 & 5 & 0\end{pmatrix}$	$\begin{pmatrix}-30 & 5 & -5 & -20 & -30\\ -33 & -33 & -25 & -20 & 0\\ 5 & 5 & -5 & -20 & 0\end{pmatrix}$	$\begin{pmatrix}5 & -50 & -30\\ 5 & -20 & 0\end{pmatrix}$	$\begin{pmatrix}5 & -30\\ -25 & 0\end{pmatrix}$

表 6　　**均衡策略与双方收益**

状态	攻击策略	防御策略	攻击收益	防御收益
S_0	[0.236 5　0.763 5　0]	[0.292　0.292　0.4159]	16.858 6	−19.777
S_1	[1　0　0]	[0　0　1　0　0]	20	−20
S_2	[1　0]	[0.5　0.5　0]	30	−40
S_3	[0.404 1　0.595 9]	[0.5　0.5]	7.5	−12.5

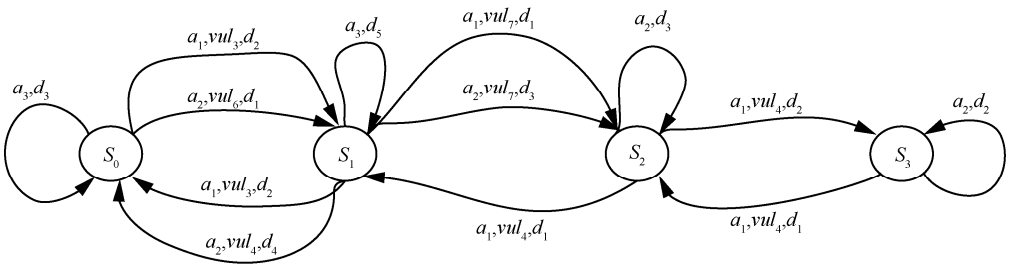


图 8　MGMD 攻防状态转移

因而被利用的概率较高。

为突出模型的有效性，以 Ubuntu 14.02 系统为例作为单控制器执行体的主动防御方案与 MGMD 模型进行对比分析，其攻防状态转移过程如图 9 所示。其中，S_0 为初始状态，S_1 为最终状态，即执行体被攻击成功。相比 MGMD 模型，单执行体攻防状态转移更加简单一些，并且由漏洞导致的某些攻击类型可能是无法避免的，例如 a_2,vul_4,d_1 攻击路径下的漏洞利用尚无有效的防御对策，而 MGMD 下异构冗余特征能够缓解这种由于单个系统漏洞攻击造成的威胁，即能够有效增加攻击者控制整个系统的复杂度。

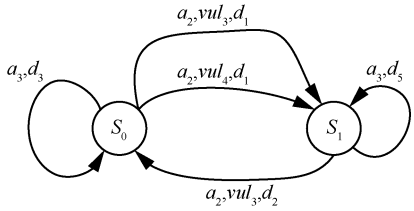


图 9　单执行体攻防状态转移

防御时效性分析：主动防御技术中如何选择防御动作执行频率以提高时效性是需要考虑的一个关键问题。由上文所述，对于单执行体防御系统而言，例如基于网络地址跳变的 MTD 技术，防御动作跳变频率越高，对攻击者所呈现的动态性越大，那么外部攻击者对该系统的渗透攻击难度就越大；与此不同的是，MGMD 模型的攻防过程中存在单个执行体被攻击者控制的状态，而由于异构冗余执行体结构，攻击者需要攻击足够多的执行体才能实现对整个系统的控制。那么，MGMD 模型对防御时效性的要求要弱于单执行体动态防御。

局限性分析：案例分析了拟态防御过程中对动态性策略的指导性，而对于具体的多样化方向未能体现；案例仅选择对提取权限均有直接利用价值的系统弱点；状态转移图未能体现所有的攻防交互过程，一些低收益的策略没有发生，因而不具完全性，例如由于防御者掌握不完全信息，状态自转移路径中存在防御者采取非恰当防御动作的情况；对于多个执行体共有漏洞，状态图仅显示了两次利用该漏洞实现多个目标控制，而未能体现出其更高级的协同攻击特点。

总之，从防御的角度讲，动态性策略不能采取盲目的随机化，均衡策略体现了最大化防御收益的策略选择，从而使防御更具针对性、有效性。

6　结束语

网络拟态防御技术通过其冗余执行体多样性、动态性以及裁决反馈机制增强了防御顽健性，而对于其安全性评估尚缺少有效的分析模型。现有的基于博弈论的分析方法多具有静态性局限，本文建立拟态防御 Markov 博弈模型，通过定义多种状态路径转移描述执行体冗余性、多样性以及裁决反馈机制对攻防博弈过程的影响，并根据攻防模型马尔可夫性质建立安全度量模型，以分析拟态防御系统冗余执行体规模、可调度空间以及防御容忍度与防御效果的关系，结合拟态防御特点将经典攻防博弈模型扩展为动态性、多阶段的 Markov 博弈模型。最后，考虑主动防御对性能的损耗，通过非线性规划解决攻防博弈混合策略选择问题。通过与移动目标防御中多目标隐藏技术对比验证了拟态防御具有更高的安全性，并基于 SDN 安全场景给出防御策略确定方案。

本文主要针对基于系统、协议漏洞的攻击类型，具有一定的通用性。下一步的工作主要解决两个方面的问题：一方面，拟态防御技术具有较为复杂的防御方案，文中所提的基于防御容忍度的状态转移尚为简单笼统，无法完全反映冗余执行体具体的动态防御路径；另一方面，针对具体的网络攻击行为，其在目标系统所呈现的攻击痕迹通常具有一定的特征，例如具体到系统某一特定层面上，而这一特征可以被裁决反馈机制捕获从而分析出攻击类型，本模型策略确定方案未充分体现拟态裁决反馈机制的作用。

参考文献：

[1] SUBRAHMANIAN V S, OVELGONNE M, DUMITRAS T, et al. The global cyber-vulnerability report[M]. Springer International Publishing, 2015.

[2] OKHRAVI H, HOBSON T, BIGELOW D, et al. Finding focus in the blur of moving-target techniques[J]. IEEE Security & Privacy Magazine, 2014, 12(2):16-26.

[3] 邬江兴. 网络空间拟态防御研究[J]. 信息安全学报, 2016, 1(4): 1-10.
WU J X. Research on cyber mimic defense[J]. Journal of Cyber Security, 2016, 1(4):1-10.

[4] PRAKASH A, WELLMAN M P. empirical game-theoretic analysis for moving target defense[C]//ACM Workshop on Moving Target Defense. 2015: 57-65.

[5] ELDOSOUKY A R, SAAD W, NIYATO D. Single controller stochastic games for optimized moving target defense[C]//ICC 2016 IEEE

International Conference on Communications. 2016:1-6.

[6] FARHANG S, MANSHAEI M H, ESFAHANI M N, et al. A dynamic bayesian security game framework for strategic defense mechanism design[M]//Decision and Game Theory for Security. Springer International Publishing, 2014:319-328.

[7] KAMBHAMPATI S, KAMBHAMPATI S, KAMBHAMPATI S, et al. Moving target defense for web applications using bayesian stackelberg games[C]//International Conference on Autonomous Agents & Multiagent Systems. 2016:1377-1378.

[8] LEI C, MA D H, ZHANG H Q. Optimal strategy selection for moving target defense based on markov game[J]. IEEE Access, 2017, PP(99):1-1.

[9] MALEKI H, VALIZADEH S, KOCH W, et al. Markov modeling of moving target defense games[C]//ACM Workshop on Moving Target Defense. 2016:81-92.

[10] 魏帅, 于洪, 顾泽宇, 等. 面向工控领域的拟态安全处理机架构[J]. 信息安全学报, 2017, 2(1):54-73.
WEI S, YU H, GU Z Y, et al. Architecture of mimic security processor for industry control system[J]. Journal of Cyber Security, 2017, 2(1): 54-73.

[11] 仝青, 张铮, 张为华, 等. 拟态防御 Web 服务器设计与实现[J]. 软件学报, 2017, 28(4):883-897.
TONG Q, ZHANG Z, ZHANG W H, et al. Design and implementation of mimic defense Web server[J]. Journal of Software, 2017, 28(4): 883-897.

[12] 马海龙, 伊鹏, 江逸茗, 等. 基于动态异构冗余机制的路由器拟态防御体系结构[J]. 信息安全学报, 2017, 2(1):29-42.
MA H L, YI P, JIANG Y M, et al. Dynamic heterogeneous redundancy based router architecture with mimic defense[J].Journal of Cyber Security, 2017,2(1):29-42.

[13] CARTER K M, RIORDAN J F, OKHRAVI H. A game theoretic approach to strategy determination for dynamic platform defenses[C]//ACM Workshop on Moving Target Defense. 2014:21-30.

[14] WANG H, LI F, CHEN S. Towards cost-effective moving target defense against DDoS and covert channel attacks[C]//ACM Workshop on Moving Target Defense. 2016:15-25.

[15] WINTERROSE M L, CARTER K M. Strategic evolution of adversaries against temporal platform diversity active cyber defenses[C]// Proceedings of the Agent-Directed Simulation Symposium at the Spring Simulation Multi-conference. 2014: 68-76.

[16] DORASZELSKI U, ESCOBAR J F. A theory of regular Markov perfect equilibria in dynamic stochastic games: genericity, stability, and purification[J]. Theoretical Economics, 2010, 5(3): 369-402.

[17] BORKOVSKY R N, DORASZELSKI U, KRYUKOV Y. A user's guide to solving dynamic stochastic games using the homotopy method[J]. Operation Research, 2010, 58(4): 1116-1132

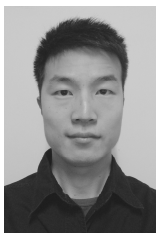
[18] 陈小军, 方滨兴, 谭庆丰, 等. 基于概率攻击图的内部攻击意图推断算法研究[J]. 计算机学报, 2014, 37(1): 62-72
CHEN X J, FANG B X, TAN Q F, et al. Inferring attack Intent of malicious insider based on probabilistic attack graph model[J]. Journal of Computer, 2014, 37(1): 62-72.

[19] SINGH U K, JOSHI C. Quantitative security risk evaluation using cvss metrics by estimation of frequency and maturity of exploit[C]// Proceedings of the World Congress on Engineering and Computer Science (WCECS2016). 2016.

[20] 姜伟, 方滨兴, 田志宏, 等. 基于攻防博弈模型的网络安全测评和最优主动防御[J]. 计算机学报, 2009, 32(4): 817-827.
JIANG W, FANG B X, TIAN Z H, et al. Evaluating network security and optimal active defense based on attack-defense game model[J]. Journal of Computer, 2009, 32(4): 817-827.

[作者简介]

张兴明（1963−），男，河南新乡人，国家数字交换系统工程技术研究中心教授，主要研究方向为拟态安全、高性能计算等。



顾泽宇（1993−），男，辽宁沈阳人，国家数字交换系统工程技术研究中心硕士生，主要研究方向为网络主动防御、网络安全等。

魏帅（1984−），男，河南南阳人，博士，国家数字交换系统工程技术研究中心讲师，主要研究方向为拟态安全、嵌入式计算等。

沈剑良（1982−），男，浙江德清人，博士，国家数字交换系统工程技术研究中心讲师，主要研究方向为可重构计算等。