基于 M-FlipIt 博弈模型的拟态防御策略评估

丁绍虎[1]，齐宁[1]，郭义伟[2]
（1. 信息工程大学信息技术研究所，河南 郑州 450002；
2. 河南信大网御科技有限公司研发部，河南 郑州 450002）

摘 要：针对先进持久性威胁场景中模拟防御系统安全性能评估的不足，基于 FlipIt 博弈论模型，提出了一种改进的博弈模型。对不同的异构性条件下的拟态防御动态策略进行评估，并设计案例进行仿真分析。仿真结果表明，不定周期的轮换能够弥补异构性的不足，维持防御者较高的博弈收益。

关键词：网络空间拟态防御；高级持续性威胁；博弈模型；仿真分析
中图分类号：TP393.1
文献标识码：A
doi: 10.11959/j.issn.1000−436x.2020136

Evaluation of mimic defense strategy based on M-FlipIt game model

DING Shaohu[1], QI Ning[1], GUO Yiwei[2]
1. Institute of Information Technology, Information Engineering University, Zhengzhou 450002, China
2. Research and Development Department of Henan Xinda Wangyu Technology Co., Ltd., Zhengzhou 450002, China

Abstract: To make up for the lack of security performance evaluation of the mimic defense systems in the advanced persistent threat scenarios an improved game model based on the FlipIt game theory model was proposed. The dynamic strategy of mimic defense under different heterogeneity conditions was evaluated, and a case study for the simulation analysis was conducted. The simulation results show that the rotation of indefinite period can make up for the lack of heterogeneity and maintain the higher game payoff of defenders.

Key words: cyberspace mimic defense, advanced persistent threat, game model, simulation analysis

1 引言

当前网络空间安全存在着易攻难守的问题，根本原因在于未知漏洞的数量较多且隐蔽性较强。在这种情形下，攻击者相比于防御者，处于更容易发现并利用漏洞开展攻击的有利地位。针对这种现状，不少研究者提出了新型防御技术用于提升网络空间安全性，包括美国国家安全战略大力支持发展的可定制信赖网络空间、移动目标防御、内在安全等为代表的“有望改变攻防游戏规则”的革命性技术[1]，以及 N-变体系统[2]、生物启发的安全技术[3]、软件定义安全[4]等。2013 年，邬江兴院士团队提出了“变结构提升系统安全性”的网络空间拟态防御（CMD, cyberspace mimic defense）[5]，其基本原理是在功能等价条件下，利用异构冗余和动态反馈机制改变系统自身架构或执行环境，从而在不依赖传统安全手段的情况下，对拟态界内基于已知或未知漏洞后门等安全威胁实现普遍而显著的防御效果。

目前，拟态防御技术已在 Web 服务器、路由器等原型系统研制中展现出其可行性，不少研究工作对拟态防御技术进行了理论、仿真和实验等不同方面的分析验证。虽然已有工作对拟态防御技术的安全性和

收稿日期：2020−01−08；**修回日期**：2020−05−07
基金项目：国家自然科学基金创新研究群体资助项目（No.61521003）
Foundation Item: The Foundation for Innovative Research Groups of the National Natural Science Foundation of China (No.61521003)

有效性进行了评估，然而不同的拟态防御系统通常根据业务需求制定特定场景下的防御策略，理论层面的具有普遍适用性的策略优化研究工作较少，不利于指导拟态防御系统的设计和多场景下的应用部署，因此需要开展关于拟态防御策略的优化研究。拟态防御技术的特点使系统能够抵御低水平攻击，当今网络空间面临着严峻的高级持续性威胁（APT, advanced persistent threat），现有的拟态防御安全性评估通常局限于低风险的普通攻击，缺少 APT 攻击场景下的策略分析和优化工作。本文以拟态防御系统应对 APT 攻击作为研究背景，提出了一种改进的 FlipIt 博弈模型——M-FlipIt（mimic defense FlipIt）。对不同的异构性条件下的拟态防御动态策略进行评估分析，并设计仿真案例，提出拟态防御在不同异构性条件下的动态策略制定建议。本文主要贡献如下。

1) 提出改进的 FlipIt 模型，建立博弈双方的策略和收益表。通过改进的博弈模型，在单次博弈和连续博弈下，分析了攻击者的收益变化以及防御者成功防御攻击的可能性。

2) 基于改进的 FlipIt 模型进行了案例分析。结合真实攻防情景，对博弈中的参数进行假设分析防御者收益变化。在连续博弈场景中，针对完全异构的轮换策略和有限异构的轮换策略，分析对比了防御者不同的轮换方式下收益的大小，提出拟态防御系统的部署和策略优化建议。

2　相关研究

拟态防御技术的提出是基于网络空间安全“易攻难守”的安全现状。拟态防御技术的动态异构冗余（DHR, dynamical heterogeneous redundant）架构融合了异构、冗余、动态特性，使拟态防御系统具有内生安全的特性。目前，已实现了拟态防御 Web 服务器、拟态防御路由器等多种类型的原型验证系统[5]，这些系统的测试与评估工作显示了拟态防御技术的有效性和可行性。实际系统的测试验证通常受限于特定的应用场景，评估方法缺乏通用性。也有不少文献对拟态防御系统进行了基于仿真和模型分析的评估。文献[6]采用广义随机 Petri 网对拟态防御域名服务系统在不同场景下的安全性和可用性进行建模分析，同时考虑了不同的拟态防御策略对域名服务系统性能和代价的影响，提出了对拟态防御系统部署策略的建议，但未对 APT 威胁场景下的拟态防御策略进行分析。文献[7]基于概率分析和仿真实验验证了拟态防御 DHR 架构的安全性，并评估了其性能，但重点集中于异构性方面，缺乏对动态性策略的分析。文献[8-9]分别提出了拟态构造 Web 服务器的异构性和服务质量量化评估方法，在此基础上，文献[10]提出了兼顾安全性与服务质量的执行体调度算法，但这一系列工作主要通过量化方法对拟态防御系统进行评估，未提出拟态防御策略的优化技术。文献[11]将网络态势感知技术融入拟态防御架构中，提出一种改进的 Web 威胁态势分析方法，通过感知技术的融入进一步提高安全性，但拟态防御策略本身依然存在可优化的空间。

博弈论模型作为一种经济学分析模型，在网络空间安全的模型分析中也具有显著价值。由于网络对抗行为最终是人与人之间的对抗，因此博弈论模型适用于网络攻防的分析。已有的应用于网络空间安全分析的博弈模型有多种，包括静态的囚徒困境博弈、零和博弈、斯塔克伯格博弈、联合博弈和进化博弈等[12]。文献[13]建立了马尔可夫博弈模型，在软件定义网络场景下对拟态防御技术的异构性、冗余性和动态性进行分析，通过求解模型中的非线性规划问题得到最佳防御策略。文献[14]提出了一种基于 Stackelberg 博弈的拟态网络操作系统安全评估方法，文献[15]通过博弈论论证了基于拟态防御机制的软件定义网络（SDN, software defined network）虚拟蜜网的有效性。然而，上述研究均未将攻击场景具体化到 APT 攻击下进行深入分析。拟态防御技术的内生安全性决定了普通攻击难以成功，且 APT 攻击已成为网络空间安全的主要威胁之一，因此对拟态防御的分析和评估应更侧重于 APT 攻击的场景。近年来提出的 FlipIt 博弈模型[16]是针对高级持续性威胁提出的一种分析模型，在分析 APT 攻击场景下的攻防行为具有显著的适用性。

现有的网络环境下，即使是最安全和隐蔽的网络和系统也会受到有动机和有策略的攻击者的破坏，并且这样的攻击结果可能不会被系统所有者立即检测到，这种威胁以 APT 攻击为典型代表。文献[16]提出了 FlipIt 博弈模型来研究 APT 攻击的影响。在 FlipIt 博弈中，博弈双方为防御者和攻击者，双方的博弈目标是争夺单一共享资源的控制权。博弈的任何一方都可以在任何时候通过“抢占”行为获取资源的控制权，然而，除此之外，双方无法得知任意时刻下资源的控制权被哪一方掌握。博弈双方采取抢占行为的代价是独立的，代价的大小是博弈的主要参

数。当博弈一方进行抢占，他会立即获得对资源的控制权（如果已经拥有控制权，则保留对资源的控制权）。每个玩家的效用即他们控制资源的时间减去所有抢占动作的代价。FlipIt 博弈过程如图 1 所示。对于一个 FlipIt 博弈，攻击者和防御者随时可以发起抢占，抢占动作瞬间完成并假设双方不同时进行抢占。抢占行为伴随着资源控制权的转移或者保留。在模型假设上，本文提出的 M-FlipIt 模型保留了上述 FlipIt 博弈的基本过程，其他 FlipIt 模型中的假设条件暂不作考虑。

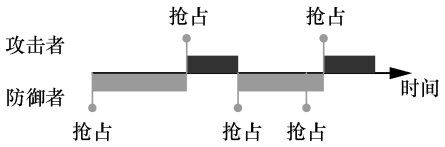


图 1 FlipIt 博弈过程示意

研究者对 FlipIt 模型进行了多种角度的扩展研究。在基本的 FlipIt 博弈中，攻击者和防御者争夺单个资源。然而，在实践中系统通常由多个可以被瞄准的资源组成。文献[17]提出了 FlipThem 模型，它是 FlipIt 对多个资源的抽象模型。为了形式化博弈者的目标和最佳策略，该研究引入了 2 种控制模型：在“与”模型中，攻击者必须占领所有资源才能接管整个系统；在“或”模型中，攻击者只需占领一个资源。该研究的分析和数值结果为多个资源的防御策略提供优化方法。拟态防御系统中虽然存在多执行体，类似于多资源模型，然而，表决机制取消了多执行体的独立性，且对拟态防御系统的“占领”行为也不等同于多执行体的同时“占领”，因此 FlipThem 模型不适用于拟态防御系统的分析。文献[18]关注攻击者的隐蔽性需求，即攻击者通常不希望已经成功的攻击被发现，例如网络间谍、僵尸网络等，攻击者不希望目标主机发现已被入侵或感染。基于该问题，研究者利用 FlipIt 模型研究了不同类型的攻击者行为模式下攻防双方的最优反应，并提出防御者的防御策略建议。该研究主要改进了 FlipIt 模型中的攻击者行为分析，防御者的行为模式延用普通的单节点静态系统。文献[19]利用 FlipIt 模型讨论了防御者能够探测当前资源占领状态的情形下，防御者的收益增益以及防御者的最优探测策略。该研究侧重于对探测策略的分析，而本文研究侧重于无检测机制介入下的策略分析。文献[20]改进了 FlipIt 模型，提出 PLADD（probabilistic learning attacker, dynamic defender）模型，探讨了移动目标防御系统的攻防双方博弈策略和收益，但缺少对轮换前后系统异构性的考虑，忽略了异构性对博弈双方收益可能造成的影响。

本文在 FlipIt 模型的基础上，针对拟态防御系统应对 APT 攻击的场景，提出改进的模型 M-FlipIt，主要改进内容包括：1) 具有更能反映真实攻防行为的博弈双方行为分析；2) 多个不同防御策略的攻防博弈进程；3) 映射博弈到拟态防御系统场景；4) 利用博弈的结果改进、优化防御者策略。

3 基于 FLIPIT 的拟态防御改进模型

3.1 M-FlipIt 博弈双方行为

基于 FlipIt 模型，本文针对拟态防御系统的攻防博弈场景提出改进模型 M-FlipIt，用于分析拟态防御系统在不同的异构性条件下对策略机制的要求。相较于 FlipIt，M-FlipIt 中博弈双方仍为攻击者和防御者，不同之处主要发生在博弈行为和收益上。由于防御方具备的异构性和动态性，M-FlipIt 的博弈进程中连续博弈进程中的收益成为分析重点。本文分析了防御方不同的异构性属性造成的收益期望变化，并据此制定动态策略。连续博弈中每轮博弈不完全独立，与防御者的异构性紧密相关，因此收益期望的计算方法不同于 FlipIt 模型。

3.1.1 防御者行为分析

典型拟态防御系统结构如图 2 所示。用户发送的请求消息通过输入代理器进行复制，并分发到 m 个异构的功能等价体上，每个功能等价体处理完以后，将输出汇总到输出裁决器，由裁决器输出唯一相对正确的响应返回给用户。当裁决中发现异常结果时，将异常信息报告给反馈控制器，由反馈控制器按照一定的调度策略动态轮换异构功能等价体，并修改输入代理器的相关调度策略配置。

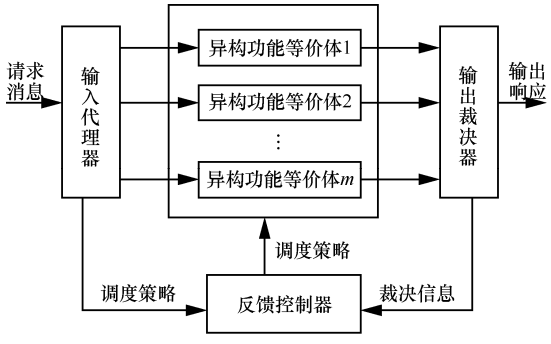


图 2 典型拟态防御系统结构

从拟态防御系统的系统结构中可以发现，决定系统安全性的重要因素在于功能等价体的异构性。理想情况下，完全异构的功能等价体能够避免相同漏洞出现在多个等价体上。然而，现有的软硬件无法达到完全异构性，因此动态调度策略的实现能够在一定程度上弥补异构性的不足所带来的安全性的隐患。当系统由于功能等价体共模漏洞的出现而被攻击时，反馈控制器可以通过调度相似的功能等价体下线，重新上线其他的功能等价体来排除共模漏洞的可利用性。实际情况中，拟态防御系统中的功能等价体是存在多种未知漏洞的，即使经过挑选的异构等价体，也存在着“相似”的可能性。未知的共模漏洞一旦出现，防御者将很难发现，因此在没有动态调度机制的条件下，拟态防御系统难以保证充分的安全性。

对于静态的拟态防御系统，即使在网络安全易攻难守的情形下，攻击依然难以顺利实施，因此拟态防御系统在动态调度策略上可以采取简单策略。在简单策略下，拟态防御系统可以采取固定周期调度功能等价体的策略，一方面，避免为了发现攻击而增大系统自身的复杂性；另一方面，固定周期的调度有利于系统定时的状态清洗和净化，以排除可能的未被发现的攻击的影响。在本文评估分析中，主要针对固定调度周期的拟态防御系统进行评估。在 FlipIt 模型中，防御者在一次博弈中既可以进行调度，也可以不进行调度；而在 M-FlipIt 博弈中，以防御者的一个调度周期为一个博弈周期，防御者采取固定策略，即博弈开始时（或结束时）发生一次调度，在此基础上分析攻击者的行为。

3.1.2　攻击者行为分析

对于以拟态防御系统为攻击目标的攻击者而言，可以通过不断探测、挖掘系统的指纹信息等来增大其发现共模漏洞并成功利用漏洞的概率。虽然异构的功能等价体难以被发现其共模漏洞，然而现实条件下很难构造完全异构的功能等价体，即使看似不同开发者开发维护的不同软件，也难以排除这些软件不同版本中存在相同漏洞的可能性，尤其在软件继承、软件架构模型有限的条件下，共模漏洞具有一定的出现概率。这种现状为攻击者提供了一定的成功的可能性。因此，假设静态的拟态防御系统能够被攻击者以一定的概率攻击成功，同时系统无法发现异常。拟态防御系统仅能够通过动态调度清除已发生的攻击使系统恢复安全状态。攻击成功的概率应随时间而变化，时间不断增长的情形下，攻击成功的概率也不断增长，设攻击成功的概率密度函数为 $f(t)$，t 表示时间，$f(t)>0$。同时，假设系统发生异构化的调度以后，攻击者需重新开始攻击尝试和探索新上线的功能等价体组合，攻击成功概率的概率密度函数依然为 $f(t)$。由于前期积累的攻击经验对新上线的等价体组合不可用，因此攻击时间也从 0 开始。当拟态防御系统上线了重复的功能等价体组合时，攻击者能够基于已有的对该组合的探测经验开展进一步的攻击行为，该种情形下，攻击难度在一定程度上降低了。假设在第一轮博弈中，对第一次出现的功能等价体组合的攻击成功，攻击成功时间为 t_0，即从攻击开始到攻击完成所用时间，则在该组合第 k 次出现时攻击首次成功的时间为 t_k，攻击成功概率的概率密度函数依然为 $f(t)$，然而在计算攻击成功概率时，应累计上攻击者在前 $k-1$ 次的探测和挖掘时间，因此攻击成功概率为 $\int_0^{(k-1)T+t_k} f(t)\mathrm{d}t$。

在一个博弈周期中，攻击者可以采取攻击和不攻击 2 种策略，而对于防御者而言，分析攻击者在攻击策略下的收益更有助于制定防御策略，降低攻击者收益，甚至将攻击者“驱逐”，即迫使攻击者采取不攻击策略。

3.2　M-FlipIt 博弈过程

在单次博弈中，攻击者发起攻击并攻击成功时，开始获得系统的资源占有权。单次博弈如图 3 所示。博弈开始时，以防御者拥有资源占有权为起点，在实际情形下该种假设是合理的，因为防御者为主动上线，攻击者在发现系统时对系统的各种信息处于未知状态，系统也处于未受攻击的状态，可以认为此时的资源占有权在防御者手中。为了简化博弈过程，认为博弈开始的同时，攻击者开始发动攻击。当攻击成功时，认为攻击者成功抢占资源。无论攻击是否成功，防御者都在轮换周期到达时，进行一次抢占，在防御者发起下一次抢占时，博弈结束。防御者下一次抢占发生以后，攻击者和防御者开始新一轮的博弈。对于以固定周期 T 轮换的拟态防御系统，每一轮博弈的时间即为轮换周期 T。在拟态防御系统无监督运行的情况下，攻防双方的行为可描述为连续博弈。

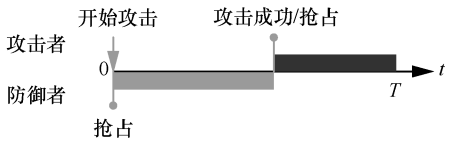


图 3 单次博弈示意

在单次博弈过程中，攻击者付出的代价主要存在于攻击代价，且攻击代价与时间相关。因为攻击耗费的时间越长，攻击者耗费的攻击资源越高，假设发起一次攻击的代价为 $C_A(t)$，$C_A(t)>0$，且为递增函数。为了便于计算，令攻击代价以时间为单位，若攻击者在 $t=t_0$ 时刻攻击成功，则攻击者收益可计算为 $u_A=-C_A(t_0)+T-t_0$，$0\leqslant t_0\leqslant T$。

防御者付出的代价主要为一次轮换的代价，在单次博弈中，由于假设了防御者采取固定策略，因此防御者的收益是固定的。拟态防御系统的轮换周期 T 影响着一次博弈的时长，也决定了攻击者在博弈中抢占到资源的可能性和攻击者占有资源的时长。理论上，轮换周期 T 越短，攻击者成功的概率越小，即使攻击成功，其占有资源的时长比例也较短。但对于防御者而言，单位时间付出的代价就越高。因此，防御者的收益需要考虑单位时间的收益。假设防御者发起一次抢占的代价为 C_D，该代价与拟态防御系统具体的实现相关，在博弈分析中可以认为该代价为固定值。同时，为了便于与攻击者收益进行比较，假设 C_D 以时间为单位。那么，若攻击者在 $t=t_0$ 时刻攻击成功，防御者在单次博弈中的收益为 $u_D=-C_D+t_0$，$0\leqslant t_0\leqslant T$。

根据上述分析，单次 M-FlipIt 博弈下攻击者采取攻击策略时攻防双方的收益如表 1 所示。

表 1 单次 M-FlipIt 博弈下攻击者采取攻击策略时攻防双方的收益

攻击结果	攻击者收益 u_A	防御者收益 u_D
攻击成功	$-C_A(t_0)+T-t_0$	$-C_D+t_0$
攻击失败	$-C_A(T)$	$-C_D+T$

3.3 M-FlipIt 连续博弈场景分析

拟态防御系统的功能等价体组合之间也存在异构性，不同的组合可以认为是对攻击者完全异构的 2 种组合，即攻击者在面临异构的 2 个组合时需要重新发起攻击，已有的攻击经验不可用，则攻击成功的概率密度函数在 2 个异构组合面前均为 $f(t)$。当拟态防御系统每次轮换上线的功能等价体组合均为异构时，则攻防博弈转换为以 T 为周期的独立的连续博弈。

实际的拟态防御系统实现中不能保证每次轮换上线的功能等价体组合都是全新的、未出现过的组合，因此存在一定的重复上线的可能性，这就为攻击者提供了降低攻击难度的可能性，从而缩短攻击成功时间。在这种情形下，攻防双方的多次博弈依然为连续博弈，但前后不同的博弈之间可能存在依赖性。

3.3.1 完全异构的轮换

在完全异构的轮换情景下，根据攻击者攻击成功的概率密度函数假设，可以将攻击者的收益期望 $\mathrm{E}(u_A)$ 具体计算为

$$\mathrm{E}(u_A)=\mathrm{E}(-C_A(t_0)+T-t_0)=-C_A(t_0)+(T-t_0)\int_0^{t_0}f(t)\mathrm{d}t$$

从防御者的角度考虑，防御周期应尽可能长，减少不必要的轮换代价。攻击者的收益预期应满足 $\mathrm{E}(u_A)\leqslant 0$，在这样的收益预期下，攻击者可能不采取攻击行动。对 $\mathrm{E}(u_A)$ 关于 T 进行求导，可得

$$\frac{\mathrm{dE}(u_A)}{\mathrm{d}T}=\int_0^{t_0}f(t)\mathrm{d}t$$

由于 $f(t)\geqslant 0$，且 $t_0\geqslant 0$，可知 $\mathrm{E}(u_A)$ 为单调递增函数，攻击者的收益预期随着防御周期 T 的增大而增大。$T\to 0,\lim_{T\to 0}\mathrm{E}(u_A)=-C_A(0)$，而 $T\to\infty,\lim_{T\to\infty}\mathrm{E}(u_A)=+\infty$。根据中值定理，存在 $T=T_0$，使 $\mathrm{E}(u_A)=0$，且对于 $T\leqslant T_0$，有 $E(u_A)\leqslant 0$。在轮换周期时，攻击者的收益为负值，该收益预期下，在博弈中理性的攻击者不会发动攻击。

3.3.2 有限异构的轮换

实际情况中，拟态防御系统可用于轮换的功能等价体组合是有限的，因此在运行时间足够长的情况下，会出现重复的组合上线工作，此时对于攻击者而言，可以借助以往对该组合的探测挖掘经验继续开展攻击，从而缩短攻击成功时间，提高攻击成功的概率。出现重复的组合时，攻击成功概率相比于未重复的组合增大，且重复次数越多，概率越高，当某一个执行体组合第 k 次出现时，假设攻击成功时间为 t_k。若该组合在前 $k-1$ 轮博弈中已被成功攻击过，则在第 k 次出现时，攻击成功概率为 1。为了不失一般性，本节探讨在第 k 次重复上线时攻击首次成功的情形。

依据前文假设，等价体组合前 $k-1$ 次的重复出现为攻击者提供了 $(k-1)T$ 的时间用于探测系统的组成和漏洞，每多一次重复，攻击者积累的经验就在前期重复的基础上累加，因此，在第 k 次重复上线时，攻防博弈时间虽然从 0 开始计算，但对于攻击者成功概率而言，则应累计 $(k-1)T$ 的经验时间；与此同时，第 k 次重复上线时的攻击代价值需要计算本轮所用代价，即为 $C_A(t_k)$，则攻击者的收益期望可计算为

$$\mathrm{E}_k(u_A)=\mathrm{E}(-C_A(t_k)+T-t_k)=-C_A(t_k)+(T-t_k)\int_0^{(k-1)T+t_k} f(t)\mathrm{d}t$$

在第 k 次重复的组合上线时，攻击者的收益预期出现一定的变化，通过对 T 求导，得到 $\dfrac{\mathrm{dE}_k(u_A)}{\mathrm{d}T}=\int_0^{(k-1)T+t_k} f(t)\mathrm{d}t$，该结果说明攻击者的收益依然为递增函数，随着防御周期的增大而增大。通过比较 $\mathrm{E}_k(u_A)$ 和 $\mathrm{E}(u_A)$ 的大小，可以看出攻击者收益期望在出现重复组合时的变化情况。

$$\begin{aligned}\mathrm{E}_k(u_A)-\mathrm{E}(u_A)=&-C_A(t_k)+(T-t_k)\int_0^{(k-1)T+t_k} f(t)\mathrm{d}t-\\&[-C_A(t_0)+(T-t_0)\int_0^{t_0} f(t)\mathrm{d}t]=\\&C_A(t_0)-C_A(t_k)+(T-t_k)\cdot\\&\int_0^{(k-1)T+t_k} f(t)\mathrm{d}t-(T-t_0)\int_0^{t_0} f(t)\mathrm{d}t\geqslant\\&C_A(t_0)-C_A(t_k)+(T-t_k)\cdot\\&\int_0^{t_0} f(t)\mathrm{d}t-(T-t_0)\int_0^{t_0} f(t)\mathrm{d}t=\\&C_A(t_0)-C_A(t_k)+(t_0-t_k)\int_0^{t_0} f(t)\mathrm{d}t\geqslant 0\end{aligned}$$

由于 $C_A(t)$ 为递增函数，且 $t_0\geqslant t_k$，因此 $C_A(t_0)-C_A(t_k)\geqslant 0$，进而可以得出 $\mathrm{E}_k(u_A)-\mathrm{E}(u_A)\geqslant 0$ 的结论。也就是说，当等价体组合重复上线时，攻防博弈向有利于攻击者的方向发展。在足够长的博弈轮次下，攻击者能够越来越轻松地攻破系统。因此，对于拟态防御系统而言，在轮换调度中保证每次上线组合的异构性与制定恰当的轮换周期同样重要。

4　案例研究

为了进一步探究 M-FlipIt 博弈下攻方双方具体策略对博弈结果的影响，本节对具体的攻防双方策略进行假设，通过仿真分析，评估对比攻击者不同的成功概率对防御者的轮换周期的影响，并评估在有限异构的场景下，防御者不同轮换周期和不同异构性对拟态防御系统的安全性的影响。

4.1　完全异构的轮换

首先，假设攻击者的成功概率 $P(t)$ 的概率密度函数服从于指数分布，即 $f(t)=\begin{cases}\lambda \mathrm{e}^{-\lambda t}, t>0\\ 0, t\leqslant 0\end{cases}$，则成功概率 $P(t)=\int_0^t f(t)\mathrm{d}t=1-\mathrm{e}^{-\lambda t}, t\in[0,+\infty)$。

为了简化分析模型，在不违背前述分析结论的条件下，假设 $C_A(t)=\alpha t(\alpha>0)$，即攻击代价与时间呈线性关系。当攻击的成功概率达到 X 时，如 X=80%，则认为攻击极有可能成功，此时对应的时刻 t_0 即作为攻击成功时间。

由 $P\leqslant X$，可得 $\int_0^{t_0} f(t)\mathrm{d}t\leqslant X$，解得 $t_0\leqslant\dfrac{-\ln(1-X)}{\lambda}$。

对于防御者而言，t_0 指示了一个动态调度周期的临界值，在动态调度周期 $T\geqslant t_0$ 的情形下，系统将处于极有可能被攻击成功的状态。在完全异构的场景下，令 $\mathrm{E}(u_A)\leqslant 0$，即 $\mathrm{E}(-C_A(t_0)+T-t_0)\leqslant 0$，得到 $-\alpha t_0+(T-t_0)\int_0^{t_0} f(t)\mathrm{d}t\leqslant 0$。在 $t_0=\dfrac{-\ln(1-X)}{\lambda}$ 的临界取值下，计算得到 $T\leqslant-\dfrac{X+\alpha}{X}\dfrac{\ln(1-X)}{\lambda}$，也就是说当调度周期符合该条件时，能够达到不被攻击成功的预期结果。影响到调度周期的主要因素在于 λ 和 α，这 2 个参数均与攻击者相关，因此在评估调度周期时需要对攻击者有较明确的掌握。

对于拟态防御系统而言，普通的攻击难以攻破系统，攻击者需要对系统进行持久的探测和攻击尝试，甚至时间可能长达数年。为了模拟这种 APT 类型的攻击行为，取一天为单位时间。假设 P=80% 时，令 λ 的取值范围为 $[0.01,0.05]$，则攻击者持续探测时间需要达到 30～160 天。同时，攻击代价的计算由 α 决定，令 $\alpha\in[0.1,2]$，在该范围内研究攻击者代价较低和较高的情形。由于采用的度量衡均为时间，因此 α 的取值范围足以为结果提供足够的分析空间。不同的 λ 取值下 $f(t)$ 的图像如图 4 所示，调度周期 T 随代价参数 α 和攻击概率密度参数 λ 的变化如图 5 所示。

结合图 4 和图 5 可以发现，当 λ 较小时，也就是攻击成功概率达到 P=80% 耗时较长时，调度周期 T 的下限值较大，允许拟态防御系统在较长时间内保持

静态性，同时被攻击风险较低。代价参数α较小时，即单位攻击代价较低时，调度周期则随λ变化较小。说明当攻击者对系统发起单位代价较低，且能在较短时间内成功的攻击时，拟态防御系统的调度周期需设置为较小值。在本文假设的参数取值范围内，调度周期最小值约为 72 天，而攻击成功概率达到 80%所需的时间约为 32 天。在博弈的情景中，攻防双方均假设为理性人，因此攻击时间虽然短于调度周期，由于攻击代价的存在，在调度周期$T<72$天时，攻击者会选择不攻击的策略来保证攻击不会出现负收益。

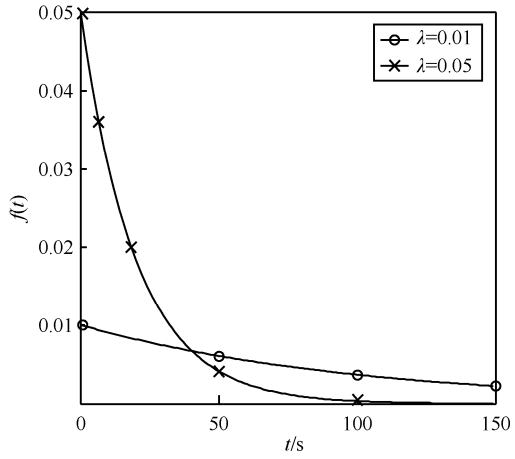


图 4 不同的λ取值下的$f(t)$

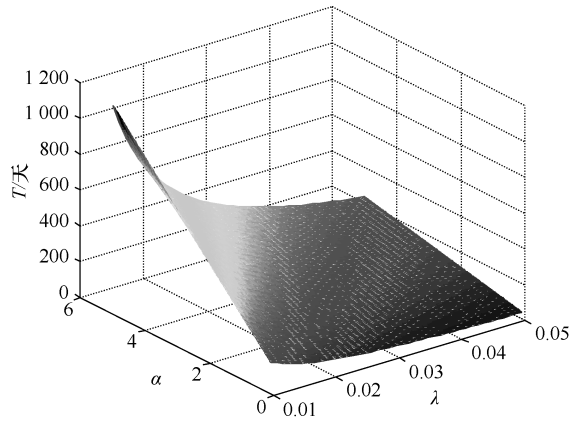


图 5 调度周期T随代价参数α和攻击概率密度参数λ的变化

4.2 有限异构的轮换

上述情形为无重复组合上线的单轮博弈结果，当拟态防御系统中出现了重复组合上线的情形时，攻防双方的博弈结果会放生变化。仍然采用 4.1 中的假设条件进行分析。

在某一组合第k次重复上线时，$\mathrm{E}_k(u_A)=-C_A(t_k)+(T-t_k)\int_0^{(k-1)T+t_k}f(t)\mathrm{d}t$。在该轮博弈中，攻击成功的概率函数为$P'(t)=\int_0^{(k-1)T+t}f(t)\mathrm{d}t=1-\mathrm{e}^{-\lambda[(k-1)T+t]}$，$t\in[0,+\infty)$。由$P'\leqslant X$，得$t_k\leqslant\frac{-\ln(1-X)}{\lambda}-(k-1)T$。由于分析中仅对调度周期的临界值进行分析，因此令$T=t_k$，可求解得到$T=t_k=\frac{-\ln(1-X)}{k\lambda}=\frac{t_0}{k}$。若令攻击者收益$\mathrm{E}(u_A)\leqslant 0$，即$-\alpha t_k+(T-t_k)\int_0^{(k-1)T+t_k}f(t)\mathrm{d}t\leqslant 0$。在$P'=X$的临界取值下，调度周期需满足$T\leqslant\frac{X+\alpha}{X}t_k$，$T=t_k$满足该条件。根据以上计算结果，发现调度周期相比于完全异构的轮换情形下大幅缩减了。

因此，在有限异构的轮换情形下，调度周期随重复组合上线次数而变化，固定的调度周期并非最有效的调度方式，可以采用动态的变化周期。在没有重复组合上线时，采用$T=t_0$的周期；随着等价体组合的重复上线次数增加，依据组合的平均重复上线次数$\bar{k}$修改调度周期为$T=\frac{t_0}{\bar{k}}$。

无论是完全异构的场景，还是有限异构的场景，周期的计算结果均为使攻击失败的周期设定，且满足攻击者收益$\mathrm{E}(u_A)\leqslant 0$和$\mathrm{E}_k(u_A)\leqslant 0$，理性的攻击者在该种情形下不会发起攻击。因此研究防御者的收益变化。对于每一轮次的博弈而言，假设该轮次的调度周期为T'，则防御者在该轮次的收益为$-C_D+T'$。

那么m为正整数，表示周期为t_0时全部组合重复上线的最大次数。

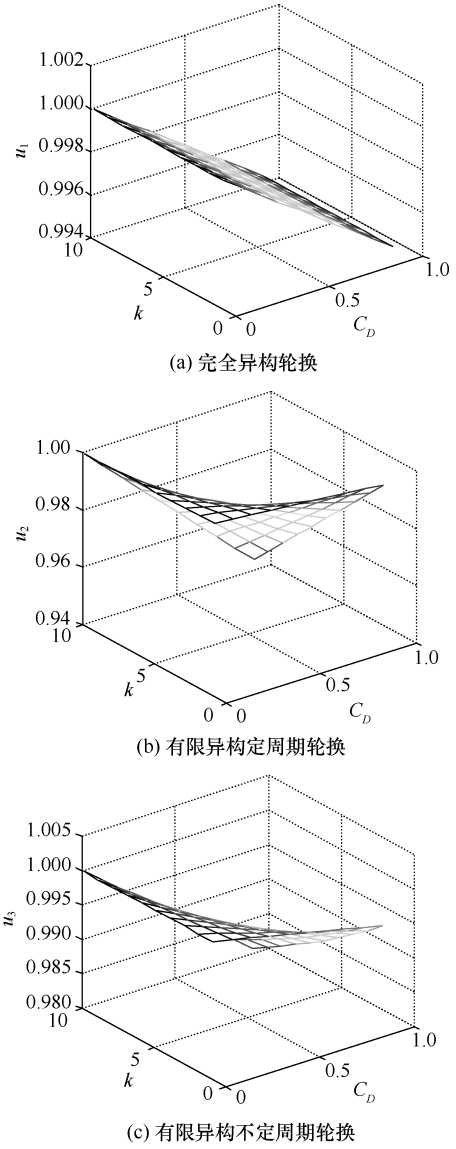
1) 对于完全异构的轮换情形，每次调度周期相同，均为$T=\frac{-\ln(1-X)}{\lambda}$，假设博弈轮次共计$n_1$次，总的收益$U_1=\sum\mathrm{E}(u_D)=\sum_{i=1}^{n_1}\left[-C_D+\frac{-\ln(1-X)}{\lambda}\right]=-n_1C_D+n_1t_0$，单位时间收益为$\bar{U}_1=\frac{U_1}{n_1t_0}=\frac{-C_D+t_0}{t_0}$。

2) 对于有限异构且固定调度周期的情形，假设β表示有限异构轮换时异构等价体组合的数量，异构的等价体组合按照一定的顺序轮换，全部轮换一次构成一个β轮次的博弈过程；当最大重复次数为$\max k$，则调度周期设定为$T=\frac{t_0}{\max k}=\frac{-\ln(1-X)}{\max k\lambda}$。

在所有组合均完成了第$\max k$次上线的情况下，博弈次数总计为$n_2=\max k\beta$。防御者的单位时间收益$U_2=\sum \mathrm{E}(u_D)=\sum_{i=1}^{n_2}\left[-C_D+\frac{-\ln(1-X)}{\max k\lambda}\right]=-n_2C_D+\max k\beta t_0$，单位时间收益为$\bar{U}_2=\frac{U_2}{n_2\frac{t_0}{\max k}}=\frac{-C_D\max k+t_0}{t_0}$。

3) 对于有限异构而变周期的情形，调度周期是变化的。沿用 2) 中关于β的假设，则在第一个包含β轮次博弈的过程中$\bar{k}=1$，$T=t_0$；第l个包含β轮次博弈的过程中$\bar{k}=l$，$T=\frac{t_0}{l}$。依然假设最大重复上线次数为$\max k$，在所有组合均完成了第$\max k$次上线的情况下，博弈次数总计为$n_3=\max k\beta$。防御者总收益$U_3=\sum \mathrm{E}(u_D)=-n_3C_D+\sum_{i=1}^{\max k}\frac{t_0}{i}\beta$，单位时间收益为$\bar{U}_3=\frac{U_3}{\sum_{i=1}^{\max k}\frac{t_0}{i}\beta}=\frac{-kC_D+\sum_{i=1}^{\max k}\frac{t_0}{i}}{\sum_{i=1}^{\max k}\frac{t_0}{i}}$。

取$X=80\%$，λ=0.01，则$t_0=\frac{-\ln(1-X)}{\lambda}=-100\ln 0.2$，在$1\leqslant k\leqslant 10$，$0<C_D\leqslant 1$的变化范围内，得到 3 种情形下单位时间收益的变化图像，如图 6 所示。



(a) 完全异构轮换

(b) 有限异构定周期轮换

(c) 有限异构不定周期轮换

图 6　3 种情形下防御者单位时间内平均收益的变化

由图 6 可以看出，平均收益$u_1\geqslant u_3\geqslant u_2$，说明完全异构场景在防御攻击者重复攻击方面最理想，有限的异构性会降低防御者收益，且定周期须采用最小周期才能够保证攻击者收益始终为负值，因此该策略防御者收益衰减最大，然而通过调节动态调度的周期（文中假设情形为逐渐减小调度周期），能够减轻防御者收益的衰减。该结果说明，等价体组合异构性的不足可以通过动态性的增强进行补充，不仅采用动态调度，同时采用动态的调度周期。而最终，异构性是拟态防御系统的根本追求目标，在完全异构的场景下，防御者收益相对而言最高且随着博弈轮次的增加衰减最小，动态性虽然能够弥补异构性的不足，却无法避免防御者收益的相对减弱。在实际的拟态防御系统设计中，可以结合异构性和动态性进行权衡。

5　结束语

动态异构冗余的特性使拟态防御具有防御基于漏洞和后门攻击的先天优势与内生防御效应。本文基于 FlipIt 模型，提出了针对拟态防御系统的攻防博弈场景改进模型 M-FlipIt，以分析在高级持续性威胁的场景下拟态防御系统的安全性表现。通过分别讨论在完全异构和有限异构条件下，防御者和攻击者的收益变化情况，提出了拟态防御在不同异构性条件下，应结合异构性和动态性进行权衡以制定动态策略。下一步，将在实际应用环境中验证 M-FlipIt 模型的有效性，在明确攻击模式的前提下研究拟态防御系统轮换周期的最优解，进一步提高模型的实际应用效力，并提出基于实际应用环境的动态策略。

参考文献：

[1] National Science and Technology Council. Trustworthy cyberspace: strategic plan for the federal cybersecurity research and development program[R]. Executive Office of the President of The United States, (2011-12)[2020-01-08].

[2] COX B, EVANS D, FILIPI A, et al. N-variant systems: a secretless framework for security through diversity[C]// Conference on USENIX Security Symposium. Berkeley: USENIX Association, 2006: 1-16.

[3] HOFMEYR S A, FORREST S. Architecture for an artificial immune system[J]. Evolutionary Computation, 2000, 8(4): 443-473.

[4] KAMPANAKIS P, PERROS H, BEYENE T. SDN-based solutions for moving target defense network protection[C]// The 2014 IEEE International Symposium on World of Wireless, Mobile and Multimedia Networks. Piscataway: IEEE Press, 2014: 1-6.

[5] 邬江兴. 网络空间拟态防御[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.

[6] 任权, 邬江兴, 贺磊. 基于 GSPN 的拟态 DNS 构造策略研究[J]. 信息安全学报, 2019, 4(2): 37-52.
REN Q，WU J X，HEI L. Research on mimic DNS architectural strategy based on generalized stochastic petri net[J]. Journal of Cyber Security, 2019, 4(2): 37-52.

[7] 扈红超, 陈福才, 王禎鹏. 拟态防御 DHR 模型若干问题探讨和性能评估[J]. 信息安全学报, 2016, 1(4):40-51.
HU H C, CHEN F C，WANG Z P. Performance evaluations on DHR for cyberspace mimic defense[J]. Journal of Cyber Security, 2016, 1(4):40-51.

[8] 张杰鑫, 庞建民, 张铮. 拟态构造的Web服务器异构性量化方法[J]. 软件学报, 2020, 31(2): 564-577.
ZHANG J X, PANG J M, ZHANG Z. Quantification method for heterogeneity on Web server with mimic construction[J]. Journal of Software, 2020, 31(2): 564-577.

[9] 张杰鑫, 庞建民, 张铮, 等. 拟态构造 Web 服务器的服务质量量化方法[J]. 计算机科学, 2019, 46(11): 109-118.
ZHANG J X, PANG J M, ZHANG Z, et al. QoS quantification method for Web server with mimic construction[J]. Computer Science, 2019, 46(11): 109-118

[10] 张杰鑫, 庞建民, 张铮, 等. 面向拟态构造 Web 服务器的执行体调度算法[J]. 计算机工程, 2019, 45(8): 14-21.
ZHANG J X, PANG J M, ZHANG Z, et al. Executors scheduling algorithm for Web server with mimic structure[J]. Computer Engineering, 2019, 45(8): 14-21.

[11] 李卫超, 张铮, 王立群, 等. 一种拟态构造的 Web 威胁态势分析方法[J]. 计算机工程, 2019, 45(8): 1-6.
LI W C, ZHANG Z, WANG L Q, et al. A web threat situation analysis method for mimic structure[J]. Computer Engineering, 2019, 45(8): 1-6.

[12] DO C T, TRAN N H, HONG C, et al. Game theory for cyber security and privacy[J]. ACM Computing Surveys, 2017, 50(2): 1-37.

[13] 张兴明, 顾泽宇, 魏帅, 等. 拟态防御马尔可夫博弈模型及防御策略选择[J]. 通信学报, 2018, 39(10): 143-154.
ZHANG X M, GU Z Y, WEI S, et al. Markov game modeling of mimic defense and defense strategy determination[J]. Journal on Communications, 2018, 39(10): 143-154.

[14] 齐超. 拟态网络操作系统架构及关键技术研究[D]. 郑州: 信息工程大学, 2018.
QI C. Research on the key technologies of mimic network operating system architecture[D]. Zhengzhou: Information Engineering University, 2018.

[15] 廉哲, 殷肖川, 席茜, 等. 一种基于拟态防御机制的 SDN 虚拟蜜网[J]. 计算机工程与应用, 2019, 55(1): 115-120.
LIAN Z, YIN X C, XI X, et al. SDN virtual honeynet based on mimic defense mechanism[J]. Computer Engineering and Applications, 2019, 55(1): 109-114.

[16] MARTEN V D, ARI J, ALINA O. FlipIt: the game of “stealthy takeover”[J]. Journal of Cryptology, 2013, 26(4):655-713.

[17] LASZKA A, HORVATH G, FELEGYHAZI M, et al. FlipThem: modeling targeted attacks with FlipIt for multiple resources[J]. Lecture Notes in Computer Science, 2014, 8840:175-194.

[18] ARON L, BENJAMIN J, JENS G. Mitigating covert compromises[C]// Web and Internet Economics. Berlin: Springer, 2013: 319-332.

[19] VIET P, CARLOS C. Are we compromised? modelling security assessment games[C]// Decision and Game Theory for Security. Berlin: Springer, 2012: 234-247.

[20] JONES S, OUTKIN A, GEARHART J, et al. Evaluating moving target defense with PLADD[R]. Sandia National Laboratories, (2015-09-1) [2020-01-08].

[作者简介]

丁绍虎（1979− ），男，北京人，信息工程大学博士生，主要研究方向为网络安全、新型网络体系结构。

齐宁（1983− ），男，山东单县人，博士，信息工程大学讲师，主要研究方向为新一代信息网络、信息安全等。

郭义伟（1983− ），男，河南商丘人，河南信大网御科技有限公司工程师，主要研究方向内生安全、云计算等。