# 基于 GSPN 的拟态 DNS 构造策略研究

任 权, 邬江兴, 贺 磊

国家数字交换系统工程技术研究中心 郑州 中国 450001

**摘要** 网络空间拟态防御系统(Cyberspace Mimic Defense System, CMDS)采用动态异构冗余架构以及多模表决机制将不确定威胁转化为概率可控的事件, 从而实现了自主可控、安全可信。为进一步研究拟态构造策略在不同干扰场景下的稳态可用性和感知安全性, 本文采用广义随机 Petri 网(Generalized Stochastic Petri Net, GSPN)建模, 分析了不同干扰场景下采用不同拟态构造策略对系统性能和构造成本的影响, 实验结果表明拟态防御系统可以根据反馈控制信息对不同干扰场景进行策略替换, 从而实现系统的稳定可用性和感知安全性。同时通过反馈控制能有效控制不同服务器解析时延差值, 对实际拟态 DNS 系统部署有重要指导意义。

**关键词** 拟态防御; 广义随机 Petri 网; 建模; 策略与成本代价; 可用性和感知安全性
**中图法分类号** DOI 号 10.19363/J.cnki.cn10-1380/tn.2019.03.05

# Research on Mimic DNS Architectural Strategy Based on Generalized Stochastic Petri Net

REN Quan, WU Jiangxing, HE Lei

National Digital Switching System Engineering & Technogical R&D Center, Zhengzhou 450001, China

**Abstract** Cyberspace Mimic Defense System adopts dynamic heterogeneous redundant architecture with multi-mode voting mechanism to convert the deterministic or uncertain disturbance to a reliable event so as to achieve self-controllable, safe and reliable. To further study the reliability and awareness security of mimic constructing strategy in different interference scenarios, this paper establishes a model of cyberspace mimic defense system based on the generalized stochastic Petri nets (GSPN) and analyzes the effects of different strategies and interference scenarios in performance and cost. The results of simulations show that Mimic defense system can change strategy to make a tradeoff among stable availability, awareness security and cost in different interference scenarios based on feedback information.

**Key words** Mimic defense; generalized stochastic Petri net; model; architectural strategy and cost; availability and awareness security

## 1 引言

随着信息化和工业化的高层次的深度融合, 各类信息安全事件层出不穷, 网络空间安全问题成为信息时代日益严峻的挑战[1]。目前, 网络空间安全形式总体表现为: 网络空间技术架构具有静态性、相似性和确定性特征, 使得攻击方一旦突破防御机制便可持续掌控和利用; 系统漏洞的不可避免性和后门的易插入性, 使得攻击方始终具备攻防不对称优势; 网络环境开放性格局使得很难构建独立的自主可控体系; 网络空间现有的主动防御技术难以应对未知漏洞或后门带来的不确定性威胁[2-3]。为了提高网络架构的可靠性和安全性, 动态化、多样化、冗余化[4-5]技术被广泛采用。移动目标防御(MTD)[6]和网络空间拟态防御(CMD)[7]相继被提议作为网络安全“改变游戏规则”的研究主题之一。移动目标防御系统通过不断变化的攻击表面来增加攻击的难度。而拟态防御技术不试图解决网络空间所有安全问题, 也不拒绝通过器件、组件、部件、软硬件等构件层面的自主可控获得整体的安全增益。拟态安全防御(Mimic Security Defense: MSD)的基本思想是在各执行体功能等价条件下, 以提供目标环境的动态性、非确定性、异构性、非持续性为目的, 动态地构建网络、平台、环境、软件、数据等多样化的拟态环境, 以防御

**通讯作者:** 任权, 学历: 本科, 职称: Email: 213120463@seu.edu.cn。
本课题得到国家网络安全专项课题资助。
收稿日期: 2018-03-18; 修改日期: 2018-08-10; 定稿日期: 2019-03-06

者可控的方式在多样化环境间实施主动跳变或快速迁移, 对攻击者则表现为难以观察和预测的目标环境变化, 从而大幅增大攻击难度和成本, 大幅降低安全风险。此外, 拟态防御架构融合了动态多维重构和负反馈控制特性, 利用动态异构冗余架构和多模表决机制[8-9]将确定的或不确定的干扰转化为概率可控的可靠性事件。因此, 如何采用可靠性理论为拟态防御系统抗攻击扰动建模, 分析系统性能成为目前研究的重点。

在传统的可靠性分析中, 通常根据系统的结构和组成建立相应的可靠性框图或故障树[10-11]。Jin J 等[12]采用可靠性框图法对仪表系统的可靠性和可用性进行了分析。Ranjbar 等[13]采用马尔可夫动态模型来描述基于正常和失败两个假设状态和行为之间的关系。Hurdle E E 等[14]扩展了传统使用故障树进行故障检测和识别的能力, 通过减少故障发生时恢复系统工作状态所需的时间以适应动态变化系统的应用。然而, 基于故障树和可靠性框图模型只能描述系统元素失效的逻辑组合(如处理器, 软件, 硬件等), 无法反映特定攻击扰动过程中系统的特性。

在网络攻击建模方面, 攻击树模型[15]、攻击图模型[16]、脆弱性状态图[17]、风险传播模型[18]等从不同角度分析和评估了系统的安全性, 反映了攻击方与网络系统之间状态的变化。但这些模型在对网络攻击进行描述和评估时, 大多是从攻击者的角度来描述和建模研究攻击特性, 并侧重分析实施成功攻击的促进作用, 而很少考虑对攻击起抑制作用的防御动作。

在此情况下, Petri 网理论被广泛运用于非相似余度系统和防御系统建模。Petri 网是对信息处理系统进行描述和建模的数学工具之一, 性能评估是其最成功的应用之一[22]。Shi Jian 等[23]利用广义随机 Petri 网对非相似双余度系统进行了可靠性建模, 考虑了软硬件之间的相互作用, 分析了故障覆盖率和监测误报警率的影响。Wang Shaoping 等[24]采用广义随机 Petri 网模型分析了非相似余度系统的性能退化过程和故障监控策略。然而, 目前, 异构冗余模型只适用于描述和分析由系统随机性失效造成的故障, 无法反映攻击扰动与防御之间的动态特性。Robert Mitchell 等[25]采用随机 Petri 网模型对网络物理系统中攻击行为进行建模, 分析了系统平均失效时间与入侵检测时间的关系。然而, 该 Petri 网模型中并未考虑系统的动态防御过程。Guilin Cai 等[26]提出了一个广义抽象的绩效评估模型, 针对系统的动态性、多样性和冗余性, 分别建立广义随机 Petri 网(GSPN)模型来分析了移动目标防御系统的性能, 但并未分析不同攻击扰动与特定防御之间的关系。本文针对不同攻击扰动与拟态系统动态重构与负反馈控制防御特性, 将引入广义随机 Petri 网理论对拟态防御系统进行分析。

本文主要贡献是采用广义随机 Petri 网理论对拟态 DNS 服务攻击扰动与动态防御建模, 通过标记的流动来模拟实际系统的动态运行行为, 并利用广义随机 Petri 网与连续时间马尔科夫链同构特性, 得到目标系统在攻击扰动条件下的稳态可用性和感知安全性。此外, 我们综合考虑了不同干扰场景下随机调度、快速恢复构造策略、输出矢量相异度以及冗余度与拟态系统性能和成本之间关系, 仿真结果表明拟态 DNS 原型系统可以根据反馈控制信息对不同干扰场景进行策略替换, 实现系统稳定可用性和感知安全性, 同时通过反馈控制能有效控制不同服务器解析时延差值, 对实际拟态 DNS 系统部署有重要指导意义。

为了构建拟态系统的评估模型, 我们选择了 DNS 服务器平台。考虑这种情况有两个原因。其一是 DNS 服务器是网络中极易受攻击的目标, 通过 DNS 劫持攻击实现用户信息与数据的获取。其二是主要的拟态技术(动态平台、软件或硬件异构、冗余技术)可以同时部署在 DNS 服务器上。

本文的其余部分组织如下。第二部分对拟态防御系统架构和 GSPN 模型描述。第三部分针对不同构造策略对拟态防御系统的性能进行综合分析。第四部分测试了拟态 DNS 原型系统模型的有效性和域名查询的时延代价。第五部分为结论。

## 2 拟态 DNS 服务系统建模与分析

### 2.1 拟态防御系统架构描述

拟态防御系统利用动态异构冗余(Dynamic Heterogeneous Redundancy, DHR)架构与多模表决机制将不确定性扰动转化为概率可控的事件。动态异构冗余结构由输入代理、可重构的异构执行体集, 异构元素池、 异构构件集、负反馈控制器、拟态裁决器组成, 图 1 给出了拟态防御系统的总体架构。其中异构元素池主要包含组成网络、平台、系统、部件或模块、构件等不同层面的设备, 如软件、硬件、处理器等, 系统按照反馈策略从 $m$ 个功能等价的异构构件中选取 $n$ 个异构构件作为一个执行体集($A1, A2, \cdots, An$)。每个执行体集中的各个执行体接收来自输入代理的输入请求, 处理后的结果提交给裁决器进行判决, 裁决结果一致, 则将结果给输出代理, 若存在异

常, 则形成相应的操作日志, 再判决是否多数一致(多数情况下采用多模表决, 也可结合策略表决进行再裁决), 若满足, 再判断系统是否需要满足输出完全一致, 若否, 再判断系统是否需要消除一致状态进行重构与清洗, 若否则表明系统可以接受当前异常状态, 将结果输出给代理。通常一般性扰动的攻击效果只能单次作用, 拟态系统可以容忍异常, 一旦单个执行体出现持续性异常, 此时需要消除一致状态进行重构与清洗。如果发现判决出现多数不一致情况, 此时需要考虑是否更换裁决策略, 若更换则需根据指定策略实施拟态裁决, 最终得到输出响应[27]。图 2 给出了拟态系统的核心流程。

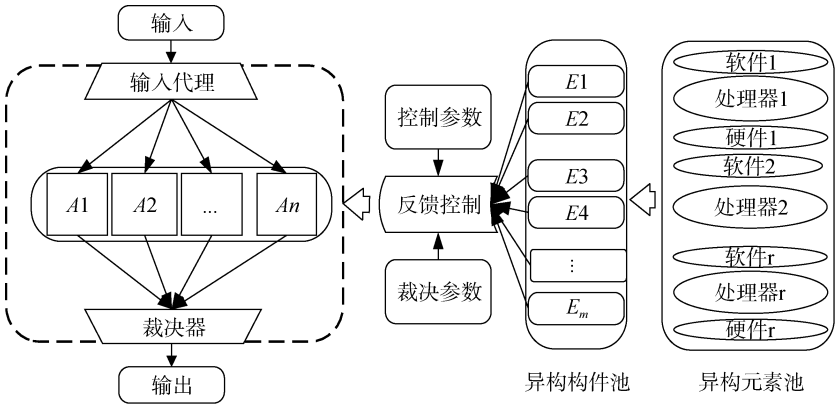



**图 1　拟态防御系统 DHR 架构**

Figure 1　The DHR architecture of mimic defense system

拟态裁决可以分为两个层面: 一是多模裁决, 二是策略裁决。当发现多模输出矢量出现不一致的情况需启动清洗恢复、重构重组等操作; 一旦系统无法通过多模裁决感知系统的状态, 系统将根据策略参数进行再裁决, 如选取历史置信度高的执行体输出结果。

多维动态重构的对象包括可重构或软件可定义的执行体实体或虚体资源。可以依据重组重构方案从异构元素池中抽取相应元素生成新的功能等价执行体, 或者将新的算法加载到可编程、可定义模块中改变系统的运行环境。策略调度则通过迁移或变换当前执行体集中的元素来变换防御场景。多维动态重构意味着执行体可以在空间上形成串行, 并行, 或串并联组合的重构形态; 在时间上, 执行体可以是静态, 动态, 和伪随机态; 在策略上, 可以考虑干扰环境、历史信息以及结构性能; 在生成方式上, 可以是重构, 重组和重定义。

反馈控制器根据通道内给定的算法和参数或通过自学习机制形成相应的控制策略, 并用策略生成输入代理器和可重构执行体的操作指令。一旦裁决器感知到不一致的状态, 反馈控制器将指令输入代理器替换执行体集, 或指令执行体进行初始化或重构操作, 直到系统处于稳定状态。同时为防止潜伏的威胁, 增加通过外部通道控制的参数是必要的。

拟态防御系统利用执行体在时空维度上的异构性来打破静态、确定性和相似性的网络技术架构。因此, 拟态系统可以容忍基于未知的漏洞和后门的外界扰动以及基于未知木马和病毒的渗透扰动, 实现内外防护一体化。

## 2.2　拟态 DNS 服务系统架构描述

在本文中, 我们选择了部署拟态 DNS 服务器作为评估方案。我们首先描述拟态场景的 DNS 服务和防御过程。当 DNS 服务器接收到请求时, 输入代理将请求分别发送给异构的 DNS 服务器进行处理, DNS 服务器将解析数据发送给裁决器进行大数判决和策略裁决, 最后将裁决结果返回服务请求方。此外, 裁决器将决策信息进行反馈控制, 为下一次 DNS 服务请求提供重构和调度策略, 图 3 给出了拟态 DNS 服务系统的总体架构。

根据 DNS 服务中攻击扰动和防御过程特性, 我们可以建立拟态 DNS 架构的 GSPN 模型。基于未知扰动驱动的变迁可以描述为时间转换, 基于拟态决策驱动的变迁可以描述为瞬时转换。其中库所对应于 DNS 服务干扰过程中系统的状态, 变迁对应于 DNS 服务过程中的干扰和防御动作[26]。

## 2.3　拟态 DNS 服务系统 GSPN 模型分析

### 2.3.1　假设

CMDS 的分析满足如下假设条件:

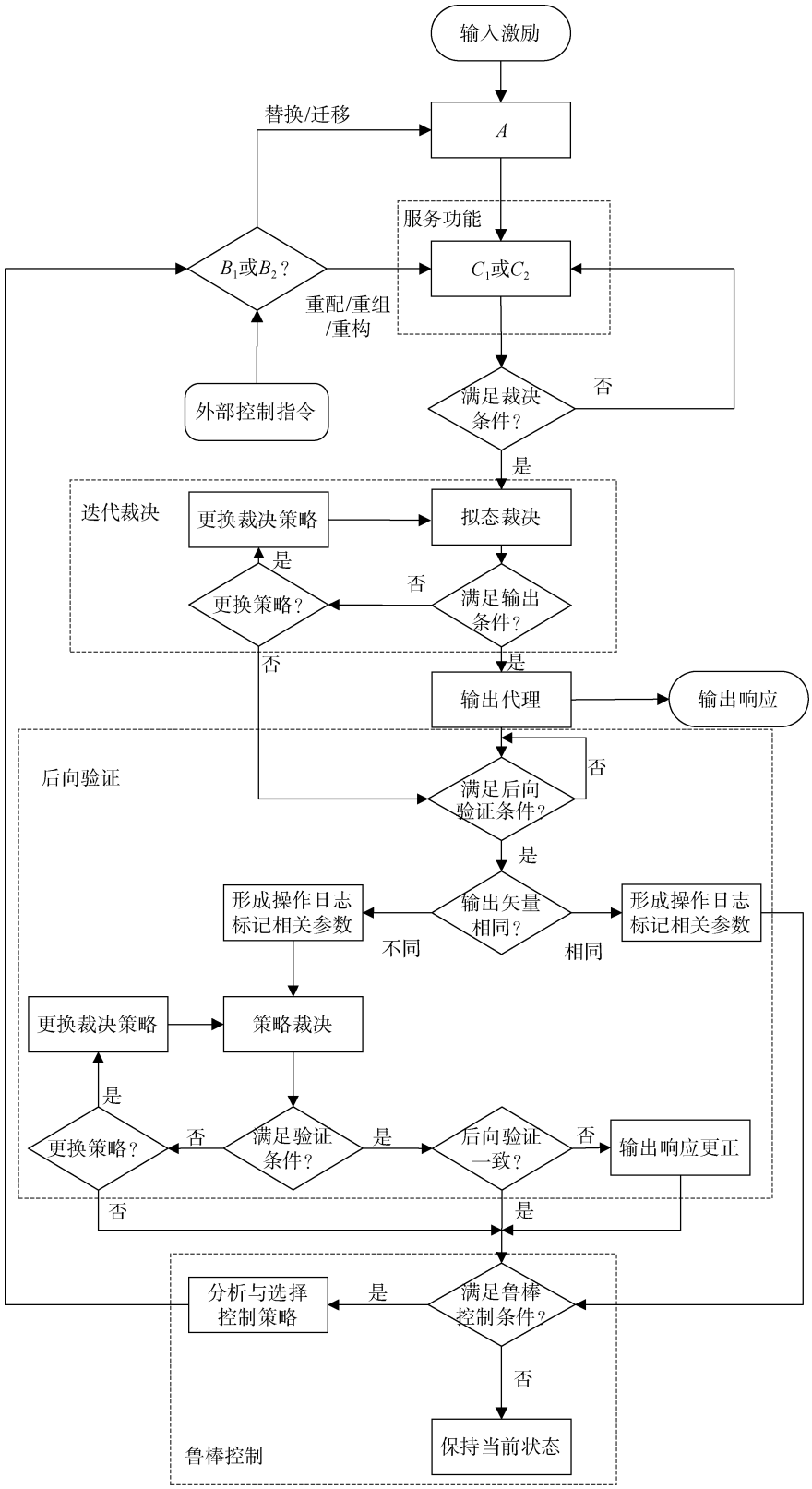



**图 2　拟态防御系统的核心流程**

**Figure 2　The core processes of mimic defense system**

注解: $A$ 代表输入代理分配输入序列; $B_1$ 代表替换或重构异常执行体; $B_2$ 代表更换或清洗执行体; $C_1$ 代表指定执行体处理输入序列; $C_2$ 代表执行重构、清洗和初始化动作指令

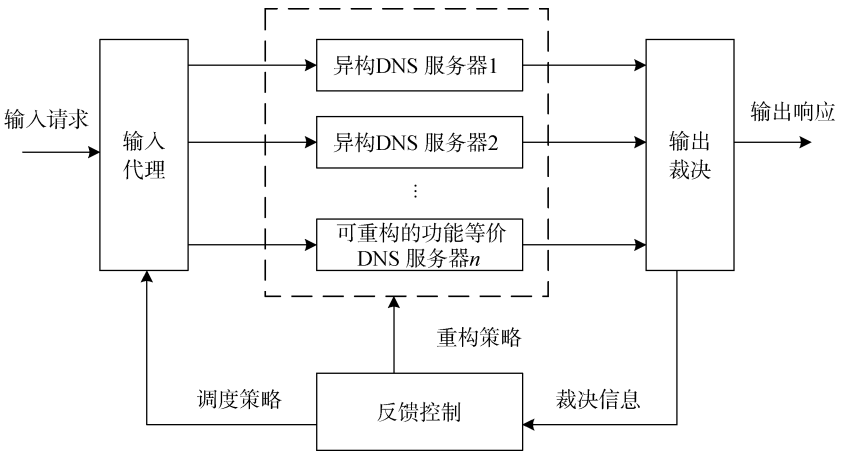



**图 3　拟态 DNS 服务系统的总体架构**

**Figure 3　The overall architecture of mimic DNS system**

本文CMDS模型针对动态异构三余度DNS服务器进行分析。其中传统的防御技术如入侵检测、防火墙和特定感知等均不被应用, 该系统通过拟态裁决机制可以感知输出不一致的服务器。此外, 执行体遭受扰动的强弱会直接影响输出响应的异常速率。一旦系统出现故障或异常感知, 拟态系统将启动动态置换或重构恢复, 也可以定期或不定期地对潜在的错误进行恢复; 成功干扰和恢复时间服从负指数分布, 并且协同扰动的不确定度 σ 等于$10^{-4}$ [28]。

### 2.3.2　定义

定义 1**:** 拟态 DNS 服务器扰动异常情况下的GSPN 模型

$$GSPN=(S,T,F,K,W,M_0,\Lambda) \tag{1}$$

其中库所 $S=\{P_1,P_2,\cdots,P_{24}\}$ 表示系统中状态元素的集合, 变迁 $T=\{T_1,T_2,\cdots,T_{42}\}$ 表示系统中状态迁移集合, $F$ 为模型中库所与变迁之间的有向弧集合, $W$ 是弧的权重集合, 各弧的权重为 1, $K=\{1,1,1,0,\cdots,0\}$ 定义了 $S$ 中各元素的容量, 状态标识 $M=\{M_0,M_1,\cdots,M_{12}\}$ ,其中 $M_0=\{1,1,1,0,\cdots,0\}$ 定义了模型的初始状态, $\Lambda=\{\lambda_1,\lambda_2,\cdots,\lambda_{15}\}$ 定义了与时间变迁相关联的平均实施速率集合。

定义 2: 感知安全

当不存在两台服务器输出响应异常且一致而使裁决器出现误判的情况时, 系统是感知安全的。

### 2.3.3　拟态 DNS 服务系统 GSPN 建模与分析

本文以 3 余度动态异构冗余系统为例, 由拟态系统的核心运作特性可知, 拟态系统在服务与防御过程存在多种状态, 不同状态系统需采取相应的反馈策略。在单个执行体出现异常时, 拟态系统可依据攻击特性采用重构或状态保持, 当多数执行体异常时则采取替换或动态重构进行防御, 对于拟态裁决无法感知的协同扰动则需采用周期或非周期性策略进行恢复。拟态系统的动态异构冗余性使得不同扰动表现出不同的动作特性, 其中包括 24 个状态, 42 个变迁, 为准确描述和分析这些状态和动作特性, 建立其 GSPN 模型如图 4 所示。不同变迁动作与状态具体描述如下:

$P_1,P_2,P_3$ 含有令牌表示该执行体处于漏洞后门休眠状态, 即各执行体均有漏洞后门但系统仍能正常响应; $P_4,P_5,P_6$ 含有令牌分别表示该执行体受干扰后发生故障; $P_7,P_8,P_9$ 含有令牌表示 2 个相关执行体发生故障且输出矢量异常; $P_{10},P_{12},P_{14}$ 含有令牌表示 2 个故障执行体输出矢量异常且一致; $P_{11},P_{13},P_{15}$ 含有令牌表示 2 个故障执行体输出矢量异常且不一致; $P_{16},P_{17},P_{18},P_{19},P_{20}$ 含有令牌表示 3 个执行体发生故障且输出矢量异常; $P_{22}$ 含有令牌表示 3 个故障执行体输出矢量异常且一致; $P_{23}$ 含有令牌表示 3 个故障执行体输出矢量异常且其中两个输出矢量一致; $P_{24}$ 含有令牌表示 3 个故障执行体输出矢量异常且均不一致。

$T_1,T_2,T_3$ 表示出现攻击导致执行体以速率 $\lambda_1,\lambda_2,\lambda_3$ 发生异常; $T_4,T_5,T_6$ 表示对攻击变换防御场景, $\lambda_4,\lambda_5,\lambda_6$ 表示执行体以速率值 $\mu_1$ 恢复到漏洞后门休眠状态; $T_7,T_8,T_9$ 表示两个执行体同时进入异常状态; $T_{10},T_{12},T_{14}$ 表示两个故障执行体的异常输出矢量以选择概率 $\sigma$ 进入协同一致状态; $T_{11},T_{13},T_{15}$ 表示两个故障执行体的异常输出矢量以选择概率 1-$\sigma$ 进入不一致状态; $T_{16},T_{17},T_{18},T_{19},T_{20},T_{21}$ 表示三个执行体同时进入故障且异常状态; $T_{22},T_{26},T_{30}$ 表示第三个

执行体的异常输出矢量以选择概率 $\sigma$ 进入与前两个执行体相同异常输出矢量的一致状态; $T_{23},T_{27},T_{31}$ 表示第三个执行体的异常输出矢量以选择概率 1-$\sigma$ 进入与前两个执行体相同异常输出矢量不一致状态; $T_{24},T_{28},T_{32}$ 表示第三个执行体的异常输出矢量以选择概率 $2\sigma$ 进入与前两个执行体中任何一个的异常输出矢量一致状态; $T_{25},T_{29},T_{33}$ 表示第三个执行体的异常输出矢量以选择概率 1-$2\sigma$ 进入与前两个执行体异常输出矢量均不一致状态。$T_{34}$ 表示通过系统周期性或随机性恢复机制, 以速率 $\lambda_7$ 使全部执行体恢复到漏洞后门休眠状态; $T_{35},T_{37},T_{39},T_{41}$ 表示通过策略性恢复机制, $\lambda_8,\lambda_{10},\lambda_{12},\lambda_{14}$ 表示以速率值 $\mu_2$ 使全部执行体恢复到漏洞后门休眠状态; $T_{36},T_{38},T_{40},T_{42}$ 表示通过负反馈和重构恢复机制, $\lambda_9,\lambda_{11},\lambda_{13},\lambda_{15}$ 表示以速率值 $\mu_4$ 使全部执行体恢复到漏洞后门休眠状态 (3 个执行体的异常输出矢量全都不一致时)。图 4 给出了拟态 DNS 服务系统异常 GSPN 模型, 表 1 描述了拟态 DNS 服务系统异常 CTMC 模型稳定状态。

**表 1　拟态防御系统异常 CTMC 模型稳定状态**

**Table 1　Stable state of abnormity CTMC model for mimic defense system**

| 编号 | 含义 |
|---|---|
| 1 | 各执行体均正常运行 |
| 2 | 执行体 1 受干扰后响应异常 |
| 3 | 执行体 2 受干扰后响应异常 |
| 4 | 执行体 3 受干扰后响应异常 |
| 5 | 执行体 1 和 2 异常输出矢量一致 |
| 6 | 执行体 1 和 2 异常输出矢量不一致 |
| 7 | 执行体 2 和 3 异常输出矢量一致 |
| 8 | 执行体 2 和 3 异常输出矢量不一致 |
| 9 | 执行体 1 和 3 异常输出矢量一致 |
| 10 | 执行体 1 和 3 异常输出矢量不一致 |
| 11 | 三个执行体异常输出矢量均一致 |
| 12 | 三个异常执行体中两个输出矢量一致 |
| 13 | 三个执行体异常输出矢量均不一致 |

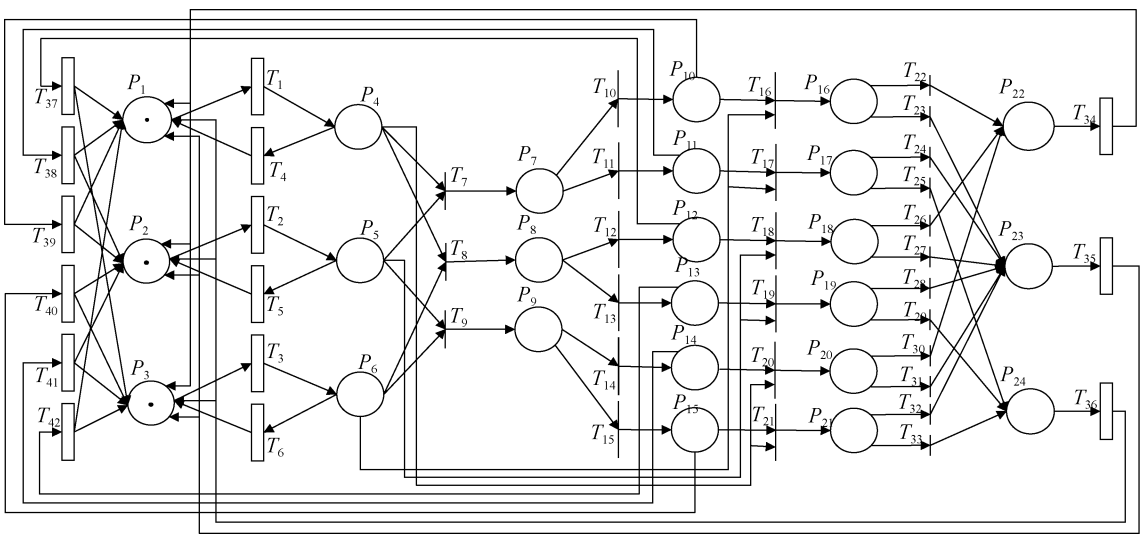


**图 4　拟态 DNS 服务系统扰动异常 GSPN 模型**

**Figure 4　Abnormity GSPN model for mimic defense system**

GSPN 模型可达集同构于连续时间马尔可夫链 (Continuous Time Markov Chain, CTMC), 图 5 给出了拟态 DNS 服务系统异常 CTMC 模型。设 GSPN 模型的可达集为 $R$, 其包含集合 $M_T$ 和 $M_V$。其中, $M_T$ 为实存状态, 实存状态下使能时间变迁; $M_V$ 为消失状态, 消失状态下使能瞬态变迁。系统状态转化过程中, 消失状态不耗费时间, 因此可以从可达集 $R$ 中消去, 将它们对系统的影响等效到实存状态之间。再对所有的状态进行排列, 消失状态在前, 实存状态在后。系统状态之间的转移概率矩阵可以表示为:

$$U = A + B = \begin{bmatrix} C & D \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ E & F \end{bmatrix} \tag{2}$$

其中 $A$ 中的元素是由消失状态向消失状态集 $C$ 和向实存状态集 $D$ 的转移概率, 由随机开关分布所确定。矩阵 $B$ 的元素表示实存状态向消失状态集 $E$ 和向实存状态集 $F$ 的转移概率,此矩阵由时间变迁的实施速率所确定。

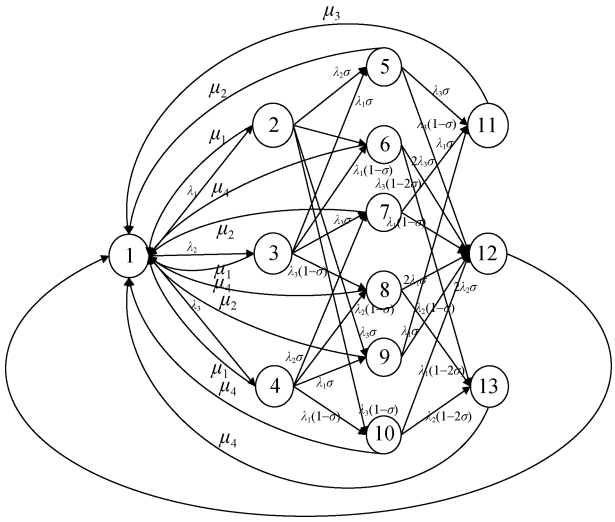


**图 5　拟态 DNS 服务系统扰动异常 CTMC 模型**

**Figure 5　Abnormity CTMC model for mimic defense system**

设 $i$, $j$ 表示马尔科夫链中任意实存状态, $i,j\in M_T$, $r$, $s$ 表示马尔科夫链中任意消失状态, $r,s\in M_v$。$c_{rs},d_{rj},e_{is},f_{ij}$ 表示U的子矩阵 $C,D,E,F$ 的元素。系统实存状态之间的转移概率矩阵为:

$$u_{ij}=f_{ij}+\sum_{r\in M_V}P_r\{r\to j\} \tag{3}$$

其中 $P_r\{r\to j\}$ 表示沿着一条全部由消失状态构成的中间状态的路径, 从消失状态 $r$ 转移到实存状态 $j$ 的概率, 其中路径可以包括任意步数。其中 $P_r\{r\to j\}$ 的求解依赖 $\boldsymbol{G}^{\infty}$ 矩阵, 矩阵 $\boldsymbol{G}^{\infty}$ 表达为:

$$\boldsymbol{G}^{\infty}=\begin{cases}(\sum_{h=0}^{k_0}C^h)D, \text{在消失状态之间无循环}\\ \left[I-D\right]^{-1}D, \text{在消失状态之间有循环}\end{cases} \tag{4}$$

$\boldsymbol{G}^{\infty}$ 的元素 $g_{ij}$ 表示从给定的消失状态 $r$ 出发经过任意步数首次到达实存状态 $j$ 的概率。于是有:

$$P_r\{r\to j\}=g_{ij} \tag{5}$$

$$u_{ij}=f_{ij}+\sum_{r\in M_V}e_{ir}g_{rj},\forall i,j\in M_T \tag{6}$$

转移概率矩阵 $\boldsymbol{U}$ 可以表示为:

$$\boldsymbol{U}=F+E\boldsymbol{G}^{\infty} \tag{7}$$

由 $\boldsymbol{U}$ 可以构造连续时间马尔可夫链的转移速率矩阵如下

$$q_{ij}=\begin{cases}\lim\limits_{\Delta t\to 0}\dfrac{u_{ij}(\Delta t)}{\Delta t}, i\neq j\\ \lim\limits_{\Delta t\to 0}\dfrac{u_{ij}(\Delta t)-1}{\Delta t}, i=j\end{cases} \tag{8}$$

则称 $q_{ij}$ 为由实存状态 $M_i$ 到实存状态 $M_j$ 的转移速率, 其中 $i,j\in[1,l],l=M_T$。$\mathbf{Q}$ 矩阵是以 $q_{ij}$ 为元素的矩阵。概率向量 $P(t)=(P_1(t),P_2(t),\cdots,P_i(t),\cdots,P_l(t))$, 其中 $P_i(t)$ 为系统处于实存状态 $M_i$ 的瞬时概率, 则有微分方程(9)成立:

$$\begin{cases}P'(t)=P(t)Q\\ P(0)=(P_1(0),P_2(0),\cdots,P_l(0))\end{cases} \tag{9}$$

实存状态的稳态概率满足:

$$\begin{cases}P\times Q=0\\ \sum\limits_{i=1}^{l}P_i=1\end{cases} \tag{10}$$

通过解此线性方程组可得到可达标识的稳态概率 $P_i(t=\infty)=P_i(1\leqslant i\leqslant l)$

状态概率初始值

$$P_i(0)=\begin{cases}0, i=2,3,4,\cdots,12\\ 1, i=1\end{cases} \tag{11}$$

$$\begin{bmatrix}\dot{P}_1(t)\\ \dot{P}_2(t)\\ \dot{P}_3(t)\\ \dot{P}_4(t)\\ \dot{P}_5(t)\\ \dot{P}_6(t)\\ \dot{P}_7(t)\\ \dot{P}_8(t)\\ \dot{P}_9(t)\\ \dot{P}_{10}(t)\\ \dot{P}_{11}(t)\\ \dot{P}_{12}(t)\\ \dot{P}_{13}(t)\end{bmatrix}=\begin{bmatrix}-\lambda_1-\lambda_2-\lambda_3 & \mu_1 & \mu_1 & \mu_1 & \mu_2 & \mu_4 & \mu_2 & \mu_4 & \mu_2 & \mu_4 & \mu_3 & \mu_2 & \mu_4\\ \lambda_1 & -\mu_1-\lambda_2-\lambda_3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ \lambda_2 & 0 & -\mu_1-\lambda_1-\lambda_3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ \lambda_3 & 0 & 0 & -\mu_1-\lambda_1-\lambda_2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & \lambda_2\sigma & \lambda_1\sigma & 0 & -\mu_2-\lambda_3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & \lambda_2(1-\sigma) & \lambda_1(1-\sigma) & 0 & 0 & -\mu_4-\lambda_3 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & \lambda_3\sigma & \lambda_2\sigma & 0 & 0 & -\mu_2-\lambda_1 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & \lambda_3(1-\sigma) & \lambda_2(1-\sigma) & 0 & 0 & 0 & -\mu_4-\lambda_1 & 0 & 0 & 0 & 0 & 0\\ 0 & \lambda_3\sigma & 0 & \lambda_1\sigma & 0 & 0 & 0 & 0 & -\mu_2-\lambda_2 & 0 & 0 & 0 & 0\\ 0 & \lambda_3(1-\sigma) & 0 & \lambda_1(1-\sigma) & 0 & 0 & 0 & 0 & 0 & -\mu_4-\lambda_2 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & \lambda_3\sigma & 0 & \lambda_1\sigma & 0 & \lambda_2\sigma & 0 & -\mu_3 & 0 & 0\\ 0 & 0 & 0 & 0 & \lambda_3(1-\sigma) & 2\lambda_3\sigma & \lambda_1(1-\sigma) & 2\lambda_1\sigma & \lambda_2(1-\sigma) & 2\lambda_2\sigma & 0 & -\mu_2 & 0\\ 0 & 0 & 0 & 0 & 0 & \lambda_3(1-2\sigma) & 0 & \lambda_1(1-2\sigma) & 0 & \lambda_2(1-2\sigma) & 0 & 0 & -\mu_4\end{bmatrix}\begin{bmatrix}P_1(t)\\ P_2(t)\\ P_3(t)\\ P_4(t)\\ P_5(t)\\ P_6(t)\\ P_7(t)\\ P_8(t)\\ P_9(t)\\ P_{10}(t)\\ P_{11}(t)\\ P_{12}(t)\\ P_{13}(t)\end{bmatrix} \tag{12}$$

通过系统所处状态可以计算系统的稳定可用性与感知安全性。拟态系统将不确定性攻击或扰动转化为概率可控的随机可靠性事件, 在部件攻击扰动异常服从负指数分布条件下, 单部件异常失效到达的平均时

间为$1/\lambda$, 根据文献[23,24]可取$\lambda_1=\lambda_2=\lambda_3=\lambda$降低求解复杂度。式(13)为各标识稳态概率的一般解。

$$\begin{cases} P_{M_0}=\dfrac{C_0}{C} \\ P_{M_1}=P_{M_2}=P_{M_3}=\dfrac{C_1}{C} \\ P_{M_4}=P_{M_6}=P_{M_8}=\dfrac{C_2}{C} \\ P_{M_5}=P_{M_7}=P_{M_9}=\dfrac{C_3}{C} \\ P_{M_{10}}=\dfrac{C_4}{C} \\ P_{M_{11}}=\dfrac{C_5}{C} \\ P_{M_{12}}=\dfrac{C_6}{C} \end{cases} \tag{13}$$

式中

$$C_0=2\lambda\mu_2{}^2\mu_3\mu_4{}^2+\mu_1\mu_2{}^2\mu_3\mu_4{}^2+2\lambda^2\mu_2{}^2\mu_3\mu_4+\lambda\mu_1\mu_2{}^2\mu_3\mu_4$$
$$+2\lambda^2\mu_2\mu_3\mu_4{}^2+\lambda\mu_1\mu_2\mu_3\mu_4{}^2+2\lambda^3\mu_2\mu_3\mu_4+\lambda^2\mu_1\mu_2\mu_3\mu_4$$
$$C_1=\lambda\mu_2{}^2\mu_3\mu_4{}^2+\lambda^2\mu_2{}^2\mu_3\mu_4+\lambda^2\mu_2\mu_3\mu_4{}^2+\lambda^3\mu_2\mu_3\mu_4$$
$$C_2=2\sigma\lambda^3\mu_2\mu_3\mu_4{}^2+2\sigma\lambda^3\mu_2\mu_3\mu_4$$
$$C_3=2\lambda^3(1-\sigma)\mu_2\mu_3\mu_4+2\lambda^2(1-\sigma)\mu_2{}^2\mu_3\mu_4$$
$$C_4=6\sigma^2\lambda^3\mu_2\mu_4{}^2+6\sigma^2\lambda^4\mu_2\mu_4$$
$$C_5=6\sigma(1-\sigma)\lambda^3\mu_3\mu_4{}^2+18\sigma(1-\sigma)\lambda^4\mu_3\mu_4$$
$$+12\sigma(1-\sigma)\lambda^3\mu_2\mu_3\mu_4$$
$$C_6=12\sigma^2\lambda^3\mu_2{}^2\mu_3+12\sigma^2\lambda^4\mu_2\mu_3+6(1-3\sigma)\lambda^3\mu_2{}^2\mu_3$$
$$+6(1-3\sigma)\lambda^4\mu_2\mu_3$$
$$C=C_0+3C_1+3C_2+3C_3+C_4+C_5+C_6$$

对于大规模系统的求解时, 可将大规模复杂系统拆分成多个子系统, 对每个子系统采用可修复系统等效理论分析[23], 再对整个系统采用广义随机 Petri 网理论进行一般性求解。

## 3 不同构造策略的性能分析

### 3.1 随机调度构造

随机调度策略, 即依据反馈信息随机从异构执行体集中分别挑选相异度较大的执行体替换故障执行体, 或对故障执行体进行随机重构、重组、重定义等。该构造主要影响系统中执行体受损后的反馈动作, 主要参数设置主要包括执行体的受干扰强度, 执行体的恢复能力, 执行体之间的异构性。在模型处于执行体异常状态后, 反馈控制器将会随机调度异构执行体使系统恢复到漏洞休眠态。表 2 给出了随机调度反馈策略下的参数设置。

弱扰动情况下拟态系统的感知安全概率:

$$P_S(t)=1-P_{M_4}(t)-P_{M_6}(t)-P_{M_8}(t)-P_{M_{10}}(t) \tag{14}$$

根据表 4 的实存状态概率, 有稳态感知安全概率:

$$P_S=1-P_{M_4}-P_{M_6}-P_{M_8}-P_{M_{10}}=9.999999999\times10^{-1} \tag{15}$$

拟态 DNS 服务系统的可用概率:

$$P_A(t)=P_{M_0}(t)+P_{M_1}(t)+P_{M_2}(t)+P_{M_3}(t) \tag{16}$$

稳态可用概率:

$$P_A=P_{M_0}+P_{M_1}+P_{M_2}+P_{M_3}=9.999999583\times10^{-1} \tag{17}$$

根据表 3 结果, 在弱攻击扰动条件下, 拟态系统能以稳态概率$9.997500624\times10^{-1}$处于初始漏洞休眠态, 体现出高抗干扰能力。同时拟态系统响应出现异常且完全不可感知概率为$8.884528138\times10^{-18}$, 因此, 协同攻击扰动突破拟态防御负反馈控制机制的难度极大。

**表 2 CMD 域名系统软件模型参数**

**Table 2 Parameters of mimic DNS software model**

| 参数 | 值 | 含义 |
|---|---|---|
| $\lambda_1$ | $5\times10^{-3}$ | 执行体响应出现异常的平均时间为 200 h |
| $\lambda_2$ | $5\times10^{-3}$ | 执行体响应出现异常的平均时间为 200 h |
| $\lambda_3$ | $5\times10^{-3}$ | 执行体响应出现异常的平均时间为 200 h |
| $\mu_1$ | 60 | 执行体重构或替换恢复的平均时间为 1 min |
| $\mu_2$ | 30 | 系统感知异常策略恢复的平均时间为 2 min |
| $\mu_3$ | 2 | 系统非周期性恢复的平均时间为 30 min |
| $\mu_4$ | 60 | 系统响应异常重构或替换恢复的平均时间为 1 min |
| $\sigma$ | $10^{-4}$ | 出现一致异常响应的输出矢量相异度 |

**表 3 拟态 DNS 服务系统弱扰动条件下稳定状态概率**

**Table 3 Stable probability of Mimic DNS under weak disturbance conditions**

| 编号 | 概率值 | $P_1$ | $P_2$ | $P_3$ | $P_4$ | $P_5$ | $P_6$ | $P_{10}$ | $P_{11}$ | $P_{12}$ | $P_{13}$ | $P_{14}$ | $P_{15}$ | $P_{22}$ | $P_{23}$ | $P_{24}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $M_0$ | $9.997500624\times10^{-1}$ | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $M_1$ | $8.329862210\times10^{-5}$ | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $M_2$ | $8.329862210\times10^{-5}$ | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $M_3$ | $8.329862210\times10^{-5}$ | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $M_4$ | $2.776156630\times10^{-12}$ | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $M_5$ | $1.388055866\times10^{-8}$ | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $M_6$ | $2.776156630\times10^{-12}$ | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| $M_7$ | $1.388055866\times10^{-8}$ | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 |
| $M_8$ | $2.776156630\times10^{-12}$ | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| $M_9$ | $1.388055866\times10^{-8}$ | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| $M_{10}$ | $8.884528138\times10^{-18}$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 |
| $M_{11}$ | $2.781257780\times10^{-15}$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| $M_{12}$ | $3.469446648\times10^{-12}$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |

## 3.2 热备份快速重构

快速恢复的热备份执行体是拟态系统的核心资源, 应当高效利用, 即在干扰较强的环境下, 对执行体进行快速替换、重构、重组等使系统达到正常状态。例如基于容器的执行体热备份快速调度和基于运行环境历史信息挑选权值高的执行体快速重构恢复。

主要参数设置主要包括拟态 DNS 服务系统中执行体的受干扰强度, 执行体的恢复能力, 执行体之间的异构性。该构造主要影响执行体受损后可感知情况下的反馈动作。当系统多数执行体处于异常状态后, 反馈控制器将会调用快速恢复策略使系统处于可感知条件下的异常恢复到漏洞休眠态。表 4 给出了快速恢复策略下的参数设置。

**表 4 中等扰动条件下拟态 DNS 服务系统模型参数**

**Table 4 Parameters of mimic DNS model under moderate disturbance conditions**

| 参数 | 值 | 含义 |
|---|---|---|
| $\lambda_1$ | 6 | 执行体响应出现异常的平均时间为 10 min |
| $\lambda_2$ | 6 | 执行体响应出现异常的平均时间为 10 min |
| $\lambda_3$ | 6 | 执行体响应出现异常的平均时间为 10 min |
| $\mu_1$ | 720(60) | 执行体热备份或权重替换恢复的平均时间为 5(60) s |
| $\mu_2$ | 360(30) | 系统感知异常策略恢复的平均时间为 10(120) s |
| $\mu_3$ | 2 | 系统非周期性恢复的平均时间为 30 min |
| $\mu_4$ | 720(60) | 系统响应异常重构或替换恢复的平均时间为 5(60) s |
| $\sigma$ | $10^{-4}$ | 出现一致异常响应的输出矢量相异度 |

根据表 5 的实存状态概率, 中强度扰动情况下拟态 DNS 服务系统的稳态感知安全概率:

$$P_S = 1 - P_{M_4} - P_{M_6} - P_{M_8} - P_{M_{10}} - P_{M_{11}} = \begin{cases} 9.999935878\times10^{-1}, \text{随机调度策略} \\ 9.999999213\times10^{-1}, \text{快速恢复策略} \end{cases} \tag{18}$$

稳态可用概率:

$$P_A = P_{M_0} + P_{M_1} + P_{M_2} + P_{M_3} = \begin{cases} 9.615340892\times10^{-1}, \text{随机调度策略} \\ 9.996001192\times10^{-1}, \text{快速恢复策略} \end{cases} \tag{19}$$

根据表 5 的结果可知, 在攻击扰动到达平均时间由 200 h 降为 10 min 后, 系统处于漏洞休眠态的概率为 $7.692272714\times10^{-1}$, 采用随机调度策略的系统

可用性由 $9.999999583\times10^{-1}$ 降 $9.615340892\times10^{-1}$, 而感知安全性变化相对较小。因此, 拟态 DNS 系统的可用性和感知安全性与干扰环境以及执行体自身品质相关。当扰动强度提高或执行体性能退化时, 系统的抗不确定性扰动能力变弱, 此时可引入快速恢复反馈策略, 对执行体进行更新或快速重构, 拟态 DNS 系统的可用性可恢复到 $9.996001192\times10^{-1}$。

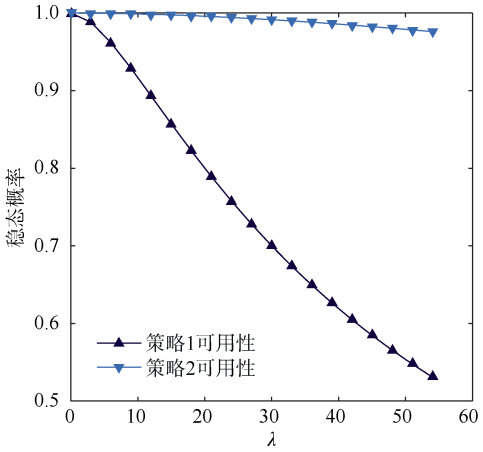
**表 5 拟态 DNS 服务系统在中强度扰动条件下的稳定状态概率**

**Table 5 Stable probability of Mimic DNS under moderate disturbance conditions**

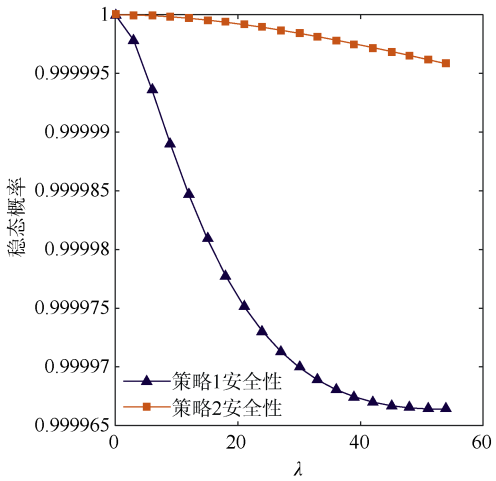
| 编号 | 策略 1 稳态值 | 策略 2 稳态值 |
|---|---|---|
| $M_0$ | $7.692272714\times10^{-1}$ | $9.756097164\times10^{-1}$ |
| $M_1$ | $6.410227261\times10^{-2}$ | $7.996800954\times10^{-3}$ |
| $M_2$ | $6.410227261\times10^{-2}$ | $7.996800954\times10^{-3}$ |
| $M_3$ | $6.410227261\times10^{-2}$ | $7.996800954\times10^{-3}$ |
| $M_4$ | $2.136742421\times10^{-6}$ | $2.621901952\times10^{-8}$ |
| $M_5$ | $1.165379316\times10^{-2}$ | $1.321653103\times10^{-4}$ |
| $M_6$ | $2.136742421\times10^{-6}$ | $2.621901952\times10^{-8}$ |
| $M_7$ | $1.165379316\times10^{-2}$ | $1.321653103\times10^{-4}$ |
| $M_8$ | $2.136742421\times10^{-6}$ | $2.621901952\times10^{-8}$ |
| $M_9$ | $1.165379316\times10^{-2}$ | $1.321653103\times10^{-4}$ |
| $M_{10}$ | $1.923068167\times10^{-9}$ | $2.359729229\times10^{-11}$ |
| $M_{11}$ | $2.680372427\times10^{-6}$ | $2.632472985\times10^{-9}$ |
| $M_{12}$ | $3.495438721\times10^{-3}$ | $3.303471931\times10^{-6}$ |

策略 1 指使用随机调度策略构造 DNS 服务器; 策略 2 指使用快速恢复策略构造 DNS 服务器

图 6 给出了不同扰动强度下两种策略的性能对比。根据图 6(a)仿真表明, 随着攻击干扰强度的增大, 系统的稳态可用性会不断减小, 当攻击平均到达时间 1/λ接近平均重构时间时, 系统可用性逐渐降至 0.5, 但执行体之间的异构性使得拟态系统一直保持在相对稳定的高感知安全性。不同于随机扰动引发的系统失效, 人为攻击扰动在一次获取系统权限后可能会对整个系统造成破坏性的影响, 根据图 6(b), 拟态系统利用动态异构冗余架构使系统的感知安全性保持在 0.999965 之上, 有效降低了非持续性成功扰动带来的风险。相比于随机策略构造, 引入热备份重构快速恢复策略的拟态 DNS 构造可以显著提升系统的可用性, 同时感知安全性可达到 0.999995。因此在工程实践中可根据历史反馈信息对干扰环境进行估计, 设置合理的变换策略使系统在可用和感知安全的前提下合理分配资源。




(a) 策略 1 和策略 2 在不同攻击扰动异常速率 λ 下可用性对比
(a) Comparison of availability between strategy 1 and strategy 2 under different disturbance rates




(b) 策略 1 和策略 2 在不同攻击扰动异常速率 λ 下感知安全性对比
(b) Comparison of awareness security between strategy 1 and strategy 2 under different disturbance rates

**图 6 可用性和感知安全性对比图**

**Figure 6 Comparison of availability and awareness security**

## 3.3 输出矢量相异度

输出矢量相异度 σ 主要由执行体异构性和输出响应的矢量长度决定。针对不同的扰动场景, 拟态系统可以从不同权重执行体集中挑选执行体进行信息处理, 通常, 不确定度权重可由执行体结构、处理环境、历史执行记录等共同决定, 选取合适权重的执行环境能有效提高系统在遭受攻击扰动时的稳定可用性和感知安全性, 同时还能减少资源调度的开销。在策略 1 和 2 仅改变单个执行体攻击扰动平均到达时间 T=10 min 的条件下, 图 7 给出了两种策略在不同 σ 权重下可用性和感知安全性的对比。

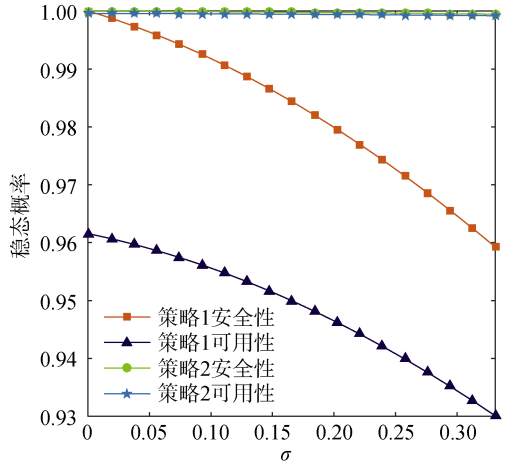



**图 7　策略 1 和策略 2 在不同输出矢量相异度 σ 下可用性和感知安全性对比**

**Figure 7　Comparison of availability and awareness security between strategy 1 and strategy 2 under different dissimilarity σ**

仿真结果表明, 随着执行体间异构性的降低, 系统整体的可用性降低, 同时, 系统的稳态感知安全值会逐渐逼近稳态可用值。对于较强攻击扰动场景, 随着执行体输出矢量相异度 σ 值不断增大, 策略 1 所能达到的感知安全性会逐渐降为 0.96, 对于关键核心基础设施等部署, 若变换策略 2, 系统的感知安全性可提高至 0.999。增大系统异构性能有效增加系统的感知安全性, 但不同异构执行体的设计需要消耗多个不同资源共同实现, 在工程实践中可根据不同安全需求进行设计。

## 3.4　冗余度

随着拟态系统执行体冗余度的增加, 系统的状态空间指数级增长, 为降低系统分析复杂度, 针对 $n$ 余度拟态系统执行体异常响应数的状态建立如图 8 连续时间马尔科夫模型。

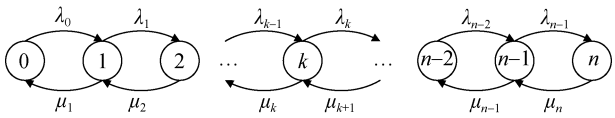



**图 8　$n$ 余度拟态防御系统连续时间马尔科夫链**

**Figure 8　Continuous-time Markov chain of $n$ redundant mimic defense system**

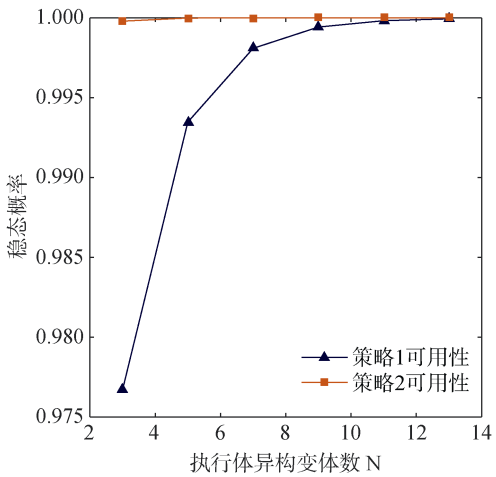
其中状态 $k$ 表示存在 $k$ 个执行体响应同时出现异常, $\lambda_k$ 表示 $n$–$k$ 个正常响应执行体中出现响应异常的速率, $\lambda_k=(n-k)\lambda, k=0,1,\cdots,n-1$; $\mu_k$ 表示 $n$ 个执行体中 $i$ 个被修复, $\mu_k=k\mu, k=1,\cdots,n$。$p_k$ 表示系统中存在 $k$ 个异构执行体出现异常的概率, $p_0$ 表示系统未受干扰的初始状态概率。该模型不同状态的稳定概率:

$$p_k=p_0\prod_{i=0}^{k-1}\frac{\lambda_i}{\mu_{i+1}}, k=1,2,\cdots,n \tag{20}$$

$$p_0=\left[1+\sum_{k=1}^{n}\prod_{i=0}^{k-1}\frac{\lambda_i}{\mu_{i+1}}\right]^{-1} \tag{21}$$

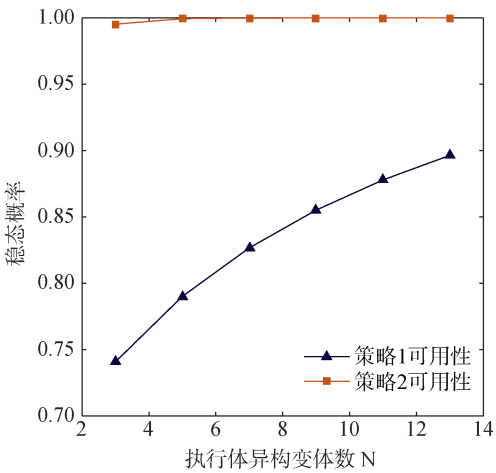
于是拟态系统稳态可用概率 $\pi_a$ 可用 $n$=2$m$+1 余度异构执行体中多数响应正常状态表示

$$\pi_a=p_0+p_1+\cdots+p_m, m=1,2,3,\cdots \tag{22}$$




(a) 攻击扰动 MTTF=10 min, 策略 1 和策略 2 在不同冗余度下可用性对比

(a) MTTF = 10 min. Availability comparison of strategy 1 and strategy 2 under different redundancies




(b) 攻击扰动 MTTF=2 min, 策略 1 和策略 2 在不同冗余度下可用性对比

(b) MTTF = 2 min. Availability comparison of strategy 1 and strategy 2 under different redundancies

**图 9　可用性对比图**

**Figure 9　Comparison of availability**

根据仿真结果, 随着异构变体数的增加, 拟态系统的可用性不断提高, 当执行体攻击扰动平均到达时间为 10 min 时, 策略 1 系统的可用性保持在 0.975 以上, 当攻击扰动平均到达时间降为 2 min 时,

策略 1 系统可用性明显降低, 在 3 冗余度时可用性低于 0.75, 而策略 2 的可用性则明显提高, 能有效抵抗攻击扰动。然而, 随着冗余度的增加, 系统设计成本和维护成本都会相应提高, 因此在实际应用中应考虑系统所处的环境干扰强弱以及系统资源的重要性去设计拟态系统的冗余度。

### 3.5 可用性构造成本分析

网络系统的可用性通常是在一定成本下考虑系统维持正常运行的能力。对于一个动态防御行为, 若实施该动作所花费的成本越高, 动作成功实施的概率也就越大[29]。为进一步分析不同构造对拟态系统可用性成本的影响, 考虑 $n$ 余度拟态防御系统, 动作 $A=\{A_1,\cdots,A_i,\cdots,A_n\}$ 中 $A_i$ 表示对第 $i$ 个异常执行体进行动态重构与控制, 同时用 $F$ 来表示在成本为 $c$ 的条件下成功实施动作 $A$ 的概率:

$$F(c)=P\{C<c\}=1-e^{-\mu c} \tag{23}$$

其中 $\mu$ 为动作 $A$ 成功实施速率。

当出现 $m$ 个执行体异常时, 完成动作 $\{A_1,A_2,\cdots,A_m\}$ 所需成本的期望值为

$$EC(m)=\sum_{i=1}^{m}EC_i=\sum_{i=1}^{m}\frac{1}{\mu_i} \tag{24}$$

其中 $EC_i$ 为原子动作 $A_i$ 所花费的成本。

于是根据式(20)和(21)可知 $n$ 余度拟态系统在整个运行过程中所需的平均成本值

$$E_c=\sum_{j=1}^{n}P(j)EC(j)=\sum_{j=1}^{n}\left[1+\sum_{k=1}^{n}\prod_{i=0}^{k-1}\frac{\lambda_i}{\mu_{i+1}}\right]^{-1}\prod_{i=0}^{j-1}\frac{\lambda_i}{\mu_{i+1}}\sum_{i=1}^{j}\frac{1}{\mu_i} \tag{25}$$

对不同攻击扰动 MTTF, 不同动态重构速率$\mu$以及不同异构变体数 $N$ 进行仿真分析如图 10 和 11, 结果表明: 在重构速率$\mu$=60 时, 随着执行体异构冗余度的增加, 拟态防御系统可用性利用平均成本呈线性增大, 同时随着攻击扰动平均到达时间的减小而增大。此外, 在异构变体数 $N$=3 时, 随着动态重构动作成功实施速率的增加, 系统可用性利用平均成本会不断降低, 因此在工程实践过程中需对不同的扰动环境综合考虑异构冗余度与动态重构率来设计拟态 DNS 服务架构。

## 4 实验结果与分析

针对拟态 DNS 正常和受攻击情况进行对比分析, 其中异构域名服务器主要借助不同的操作系统: Centos、Ubuntu、Windows 以及多样化的域名协议 Bind、nsd、WinDNS 来构建三个异构的执行单元, 服务器运行在 C++环境, inter i7 处理器, 12G 内存。

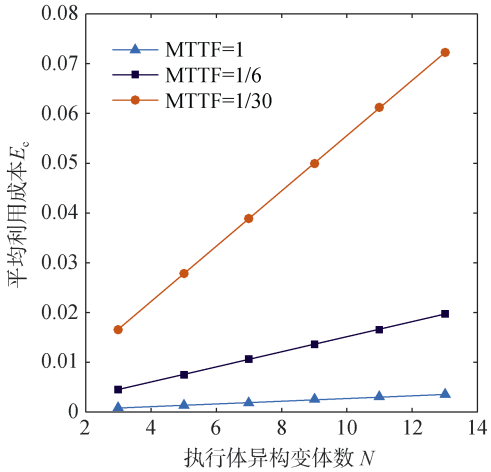



**图 10 在不同攻击扰动 MTTF 和异构变体数以及重构速率$\mu$=60 时拟态防御系统可用性构造成本对比**

**Figure 10 Comparisons of the construction cost of mimic defense systems with different attack perturbations, MTTF, heterogeneous variants and reconstruction rate $\mu$=60**

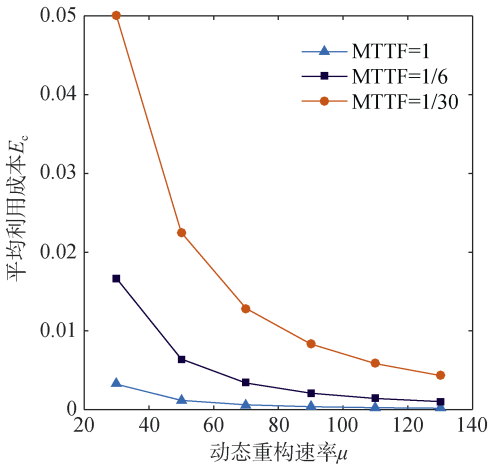



**图 11 在不同攻击扰动 MTTF 和重构速率 $\mu$ 以及异构变体数 $N$=3 时拟态防御系统可用性构造成本对比**

**Figure 11 Comparisons of the construction cost of mimic defense systems with different attack perturbations, MTTF, reconstruction rate and heterogeneous variants $N$=3**

域名服务器漏洞类型空间 100, 执行体动态热切换平均时间为 1s, 周期性重构平均时间为 60s, 不同攻击强度每秒钟可分别成功实现 2、4、6、8、10 次漏洞攻击, 域名服务到达平均时间间隔为 1s, 总共发送 10000 次域名请求。

拟态域名系统采用动态异构双余度架构接收正常服务请求, 当遭受攻击时, 系统会动态调度第三个执行体进行策略裁决, 测试表明, 当攻击采用黑盒测试时, 拟态系统能准确感知异常执行体从而采取相应策略。同时系统将切换到响应正常执行体继

续提供服务。

根据图 13 实验结果, 拟态系统在不同攻击强度下域名查询错误概率均低于 0.015, 而传统域名系统在遭受攻击后正确查询概率均低于 0.06, 相比传统域名系统, 拟态系统抗攻击能力具有非线性增益, 验证了该模型和方法的有效性。由此可见攻击者难以协同攻击异构的 DNS 服务器, 单次试错式攻击无法产生累积效果。当裁决感知到异常响应时, 拟态系统可以通过动态变换运行环境来阻断攻击链, 实现系统的高可用性。

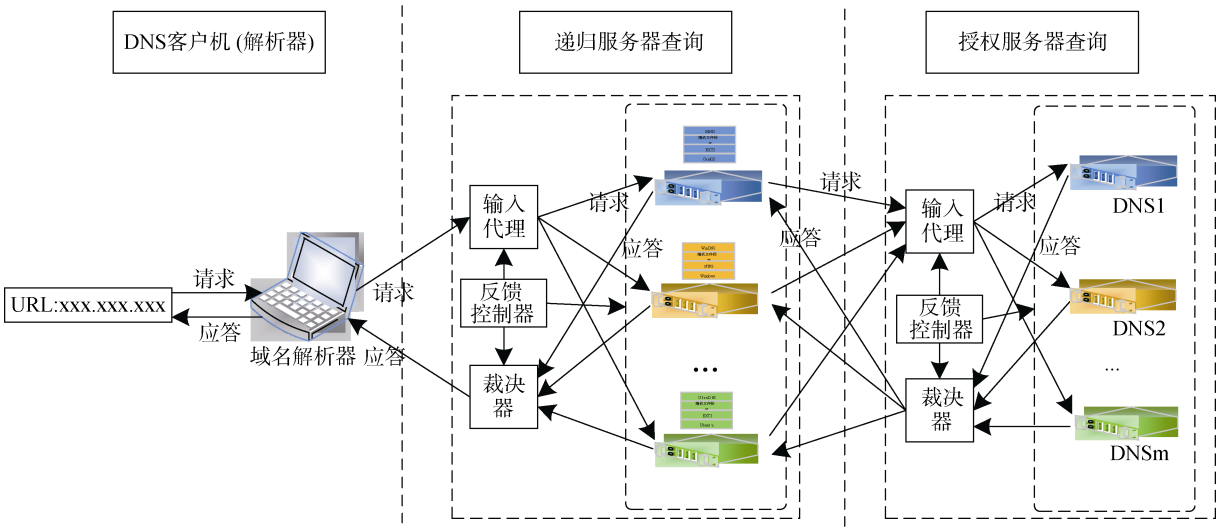
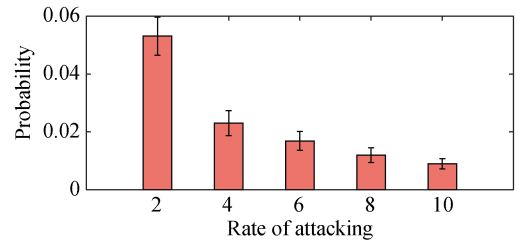


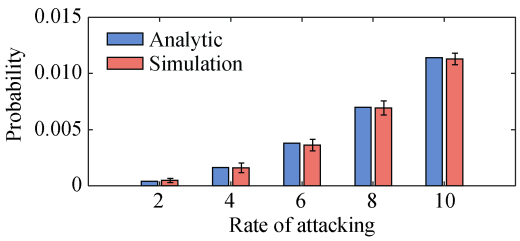

**图 12 拟态域名服务原型系统**

**Figure 12 A prototype system of mimic domain name service**




(a) 传统域名系统在遭受不同强度漏洞攻击时的查询正常概率

(a) The normal query probability of traditional DNS when being attacked by different strength vulnerabilities




(b) 拟态域名系统在遭受不同强度漏洞攻击时域名查询异常概率

(b) The abnormal query probability of mimic DNS when being attacked by different strength vulnerabilities

**图 13 查询对比图**

**Figure 13 Comparison of query**

与一般域名查询相比, 拟态域名需同时请求多个异构的域名服务器, 从而额外增加时延。一般域名请求时延包括用户与服务器间的传播时延 $T_{cs}$, 域名服务器的解析时延 $T_s$; 对于拟态域名系统, 时延主要包括用户与代理服务器 $T_{cf}$、代理服务器与域名服务器之间的传播时延 $T_{fs}$, 代理服务器的处理时延 $T_f$, 域名服务器的解析时延 $T_s$。

于是单余度和拟态域名时延代价分别为:

$$T_{S\_DNS} = 2T_{cs} + T_p + T_f \tag{26}$$

$$T_{M\_DNS} = 2T_{cf} + T_f + 2T_{fs} + T_p + T_s \tag{27}$$

当拟态系统感知到异常存在需进行快速切换执行体或重构执行体使潜在的威胁处于休眠状态, 其中热切换主要通过代理服务器配置初始化, 快速切换执行体。当域名递归服务器未命中缓存时, 需向权威域名服务发送请求, 该试验只针对本地域名服务器进行域名解析。

根据实验结果, 正常单余度 DNS 域名分发至裁决平均响应时间为 0.933ms, 启动拟态防御模式后, 分发至裁决平均请求时延增至 1.423ms, 相比传统域名请求拟态机制平均额外增加时延 0.49ms。拟态域名本地服务器(Local Mimic DNS,LMDNS)查询平均时延为 6.4ms, 实际拟态域名服务器(Real Mimic DNS,RMDNS)查询为 31.7ms, 相比本地查询, 实际拟态机制额外增加网络通信时延 25.3ms。当存在攻击条件时, 受攻击拟态域名服务器(Attacked Mimic DNS,AMDNS)查询时间为 32.8ms, 策略再判决需额外增加时延 1.1ms。图 14 拟态域名系统本地和实际

查询平均响应时间对比。通过反馈控制, 拟态域名系统可以根据不同场景合理选取时延差值较小的服务器进行域名解析, 确保服务的有效性。图 15 给出了拟态域名系统本地、递归和权威域名查询平均响应时间对比。

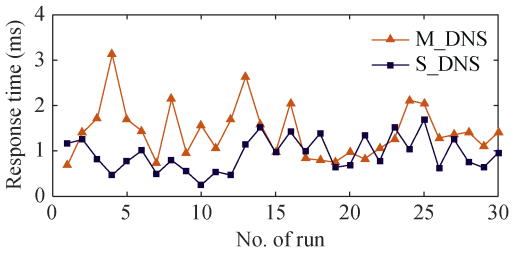



**图 14　单余度和拟态域名系统分发至裁决模块平均响应时间对比**

**Figure 14　Comparison of average response time between single redundancy and mimic DNS from distribution to decision module**

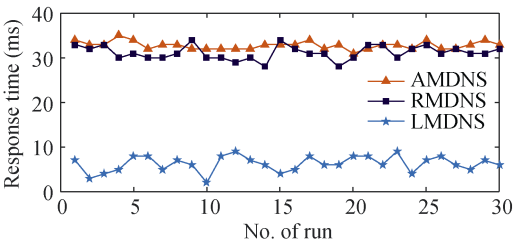



**图 15　拟态域名系统本地和实际查询平均响应时间对比**

**Figure 15　Comparison of average response time between local and real network queries in mimic domain name system**

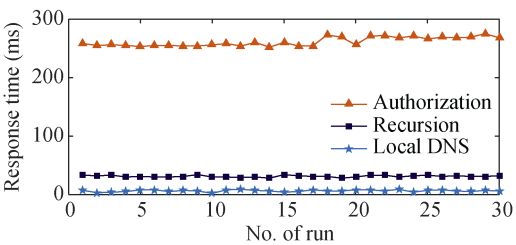



**图 16　拟态域名系统本地、递归和权威域名查询平均响应时间对比**

**Figure 16　Comparison of average response time of local, recursive and authoritative domain name queries in mimic domain name system**

因此, 拟态域名原型系统在提供高可靠高可用的服务情况下仅需额外增加较小的处理时延和网络通信时延, 同时, 在向不同异构域名服务器发送请求时, 网络通信时延会对实际域名查询平均时间产生重要影响, 因此, 拟态系统应根据反馈控制信息选取合理的时延代价。

## 5　总结

本文基于广义随机 Petri 网为拟态 DNS 服务系统攻击扰动与防御统一建模, 分析了不同干扰场景下随机调度、快速恢复策略以及不同异构冗余构造对拟态系统可靠性和感知安全性的影响。通过搭建拟态域名原型系统, 验证了拟态域名系统的高可用性能, 同时给出了系统引入的时延代价。本文的主要贡献如下:

(1) 网络空间拟态防御系统具有稳定高可用性, 且系统的性能与执行环境和执行体本身品质相关, 因此系统可以充分利用历史裁决信息对执行环境的扰动情况进行监控, 从而选取合适的反馈策略保证系统的稳定高可用性。

(2) 拟态系统的感知安全性不仅与执行环境和执行体本身品质相关, 而且还受执行体之间的异构性大小影响。为每个执行体配置相应的历史权重, 在扰动强度较大时, 可以选择合适异构性执行体组合实现快速恢复从而保证 DNS 服务系统在不同干扰场景的稳定高感知安全性。

(3) 拟态防御系统平均可用性构造成本与环境攻击扰动平均到达时间、执行体间的输出矢量相异度以及异构冗余度相关。在实际拟态系统设计中可利用拟态系统的反馈控制实现对网络环境的感知, 从而实现系统在保证高可用和感知安全的条件下降低平均时延和成本代价。

根据以上结果, 我们可以得出结论: 在拟态防御系统工程设计中, 动态性、异构性和冗余性是必不可少的, 通过对不同干扰场景的动态反馈选取合适构造策略能有效提高系统的稳态可用性和感知安全性, 同时降低平均时延和成本代价。

**致　谢**　该研究部分由国家网络安全专项课题(No.2017YFB0803201)、国家高技术研究发展计划(“863”计划)课题(No.2015AA016102)、国家自然科学基金群体创新项目(No.61521003)共同提供支撑。

## 参考文献

[1] Cram W A, Proudfoot J G, D'Arcy J. Organizational information security policies: a review and research framework[J]. *European Journal of Information Systems*, 2017(11): 1-37.

[2] Conteh N Y, Schmick P J. Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks[J]. *International Journal of Advanced Research in Computer Science*, 2016, 6(23): 31-38.

[3] Zuech R, Khoshgoftaar T M, Wald R. Intrusion detection and Big Heterogeneous Data: a Survey[J]. *Journal of Big Data*, 2015, 2(1): 3.

[4] Hu P, Li H, Fu H, et al. Dynamic defense strategy against advanced persistent threat with insiders[C]. *IEEE Computer Communications*, 2015: 747-755.

[5] Fang T, Shen L, He W, et al. Distributed Control and Redundant Technique to Achieve Superior Reliability for Fully Modular Input-Series-Output-Parallel Inverter System[J]. *IEEE Transactions on Power Electronics*, 2016, 32(1): 723-735.

[6] Jajodia S, Ghosh A K, Swarup V, et al. Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats[M]. Springer Publishing Company, Incorporated, 2011.

[7] Wu J. Meaning and Vision of Mimic Computing and Mimic Security Defense[J]. *Telecommunications Science*, 2014.

[8] Alotaibi B, Elleithy K. A majority voting technique for Wireless Intrusion Dtection Systems[C]// Long Island Systems, Applications and Technolog Conference. IEEE, 2016: 1-6.c

[9] Chi C,Zhang W, Liu X. Application of Analytic Redundancy-based Fault Diagnosis of Sensors to Onboard Maintenance System[J]. *Chinese Journal of Aeronautics*, 2012, 25(2): 236-242.

[10] Distefano S, Xing L. A new approach to modeling the system reliability: dynamic reliability block diagrams[C]// Rams '06 Reliability and Maintainability Symposium. *IEEE Computer Society*, 2006:189-195.

[11] Nystrom B, Austrin L, Ankarback N, et al. Fault Tree Analysis of an Aircraft Electric Power Supply System to Electrical Actuators[C]// *International Conference on Probabilistic Methods Applied To Power Systems*. IEEE, 2006: 1-7.

[12] Jin J, Pang L, Zhao S, et al. Quantitative assessment of probability of failing safely for the safety instrumented system using reliability block diagram method[J]. *Annals of Nuclear Energy*, 2015, 77: 30-34.

[13] Ranjbar A H, Kiani M, Fahimi B. Dynamic Markov Model for reliability evaluation of power electronic systems[C]// International Conference on Power Engineering, Energy and Electrical Drives. IEEE, 2011:1-6.

[14] Hurdle E E, Bartlett L M, Andrews J D. Fault diagnostics of dynamic system operation using a fault tree based method[J]. *Reliability Engineering & System Safety*, 2009, 94(9): 1371-1380.

[15] Schneier B. Attack Trees[J]. *Doctor Dobbs Journal*, 1999, 24(12).

[16] Dawkins J, Campbell C, Hale J. Modeling network attacks: extending the attack tree paradigm[J]. *Detection Johns Hopkins University*, 2002.

[17] Indrajit Ray, Nayot Poolsapassit. Using Attack Trees to Identify Malicious Attacks from Authorized Insiders[J]. *Lecture Notes in Computer Science*, 2005, 3679: 231-246.

[18] Ammann P, Wijesekera D, Kaushik S. Scalable, graph-based network vulnerability analysis[C]// ACM Conference on Computer and Communications Security, CCS 2002, Washington, Dc, Usa, November. DBLP, 2002: 217-224.

[19] Sheyner O, Haines J, Jha S, et al. Automated Generation and Analysis of Attack Graphs[C]// IEEE Symposium on Security and Privacy. IEEE Computer Society, 2002: 273.

[20] 冯萍慧, 连一峰, 戴英侠, 等. 基于可靠性理论的分布式系统脆弱性模型[J]. *软件学报*, 2006, 17(7): 1633-1640.

[21] 张永铮, 方滨兴, 迟悦,等. 用于评估网络信息系统的风险传播模型[J]. *软件学报*, 2007, 18(1): 137-145.

[22] 林闯. 计算机网络和计算机系统的性能评价[M]. 清华大学出版社, 2001.

[23] Shi, Jian, Meng, et al. Reliability and safety analysis of redundant vehicle management computer system[J]. *Chinese Journal of Aeronautics*, 2013, 26(5): 1290-1302.

[24] WangShaoping, CuiXiaoyu, ShiJian, et al. Modeling of reliability and performance assessment of a dissimilar redundancy actuation system with failure monitoring[J]. *Chinese Journal of Aeronautics*, 2016, 29(3): 799-813.

[25] Mitchell R, Chen I R. Modeling and Analysis of Attacks and Counter Defense Mechanisms for Cyber Physical Systems[J]. *IEEE Transactions on Reliability*, 2015, 65(1): 350-358.

[26] Cai G, Wang B, Luo Y, et al. A Model for Evaluating and Comparing Moving Target Defense Techniques Based on Generalized Stochastic Petri Net[M]. Springer Singapore, 2016.

[27] 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.

[28] Garcia M, Bessani A, Gashi I, et al. Analysis of operating system diversity for intrusion tolerance[J]. *Software—practice & Experience*, 2014, 44(6): 735-770.

[29] 冯萍慧, 连一峰, 戴英侠,等. 面向网络系统的脆弱性利用成本估算模型[J]. *计算机学报*, 2006, 29(8): 1375-1382.

**任权** 于 2016 年在东南大学信息工程专业获得学士学位。现在国家数字交换系统工程技术研究中心网络空间安全专业攻读硕士学位。研究领域为网络安全防御，鲁棒网络体系结构。Email: 213120463@seu.edu.cn

**邬江兴** 于 1982 年解放军工程技术学院计算机科学与工程专业获得学士学位。现任国家数字交换系统工程技术研究中心主任、教授, 中国工程院院士。中国信息通信与网络交换领域著名专家。2013 年首次在全球推出基于拟态计算原理的高效能计算机原型系统, 2016 年提出网络空间拟态防御理论并完成原理验证系统测试评估。研究领域为信息通信网络、网络安全。Email: ndscwjx@126.com

**贺磊** 于 1996, 2001 和 2008 年在信息工程大学软件工程专业获得学士、硕士和博士学位。现任国家数字交换系统工程技术研究中心副研究员。研究领域为网络安全防御, 网络体系结构。Email: hl.helei@163.com