

网络空间拟态防御发展综述：从拟态概念到“拟态+”生态

马海龙¹, 王亮^{1,2}, 胡涛¹, 江逸茗¹, 曲彦泽¹

(1. 信息工程大学信息技术研究所, 河南 郑州 450003; 2. 66135 部队, 北京 100043)

摘 要: 网络空间拟态防御 (CMD, cyberspace mimic defense) 基于动态异构冗余架构实现多体执行、多模裁决和多维重构, 以不确定性系统应对网络空间泛在化的不确定性威胁。从纵向、横向、当前、发展和未来 5 个视角对其 8 年来的演进进行系统综述: 纵向观, 概述了 CMD 从概念提出, 到理论、实践层面形成发展的历程; 横向观, 阐述了 CMD 的 DHR (dynamical heterogeneous redundancy) 核心架构、以 CMD 三定理为支柱的原理、安全增益、性能开销, 将其与入侵容忍、移动目标防御、零信任架构、可信计算和计算机免疫学 5 类其他主动防御技术进行了综合对比辨析; 当前观, 综述了拟态路由器、拟态处理机、拟态 DNS 服务器、拟态云平台等 11 类现有主要拟态产品的实现要素、性能表现、系统架构、异构策略、调度策略、表决策略等共性技术模式与特性技术特点; 发展观, 结合人工智能、物联网、云计算、大数据和软件定义网络 5 类新型技术探讨了“拟态+”AICDS (拟态+AI/ IoT/Cloud/Data/SDN) 共生生态, 提出了相应技术结合点和交叉研究价值; 未来观, 展望了未来拟态基线 2.0 产品生态、“拟态+5G/6G”“拟态+边缘计算”“拟态+云”和“拟态+区块链”5 类“拟态+”应用场景, 分析归纳了拟态防御技术面临的存在多模决策攻击逃逸空间、异构与同步互制约、安全与功能难平衡和现有内生安全组件变换空间有限 4 点挑战。

关键词: 网络空间拟态防御; 系统架构; 异构策略; 调度策略; 非协同多模决策; 异构度增益

中图分类号: TP309

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2022018

Survey on the development of mimic defense in cyberspace: from mimic concept to “mimic+” ecology

MA Hailong¹, WANG Liang^{1,2}, HU Tao¹, JIANG Yiming¹, QU Yanze¹

1. Information Technology Research Institute, Information Engineering University, Zhengzhou 450003, China

2. Unit 66135, Beijing 100043, China

Abstract: Build upon the dynamic-heterogeneous-redundant architecture for multi-body execution, multi-mode ruling and multi-dimension reconstruction, cyberspace mimic defense (CMD) uses uncertain system to deal with the

收稿日期: 2021-11-22; 修回日期: 2022-03-01

通信作者: 王亮, 1747207681@qq.com

基金项目: 国家重点研发计划 (2020YFB1804803)

Foundation Item: The National Key R&D Program of China (2020YFB1804803)

引用格式: 马海龙, 王亮, 胡涛, 等. 网络空间拟态防御发展综述: 从拟态概念到“拟态+”生态[J]. 网络与信息安全学报, 2022, 8(2): 15-38.

Citation Format: MA H L, WANG L, HU T, et al. Survey on the development of mimic defense in cyberspace: from mimic concept to “mimic+” ecology[J]. Chinese Journal of Network and Information Security, 2022, 8(2): 15-38.

uncertain threat to cyberspace ubiquity. The evolution of CMD over the past 8 years were reviewed systematically from the vertical, horizontal, current, developing and future perspectives. From the vertical perspective, the development process of CMD from concept to theory and practice was summarized. From the horizontal view, it elaborated the core structure DHR (dynamical heterogeneous redundancy) of CMD, the principles based on CMD's three major theorems, safety gains and performance costs. A comparison was conducted between CMD and five other active defense technologies, namely intrusion tolerance, moving target defense, zero trust architecture, trusted computing and computer immunology. From the current perspective, it reviewed the implementation elements, performance, system architecture, heterogeneous strategies, scheduling strategies, voting strategies and other common technology patterns and characteristics of 11 types of main existing mimic products including mimicry router, mimicry processor, mimicry DNS server and mimicry cloud platform. From the developing perspective, it explored the “mimic+” AICDS (Mimic + AI/IoT/Cloud/Data/SDN) symbiotic ecology with respect to 5 types of new technologies, namely artificial intelligence, Internet of things, cloud computing, big data and software-defined network, and proposed the corresponding technology junctions and cross research value. From the future perspective, it looked into the future mimicry baseline 2.0 product ecology, “mimic +5G/6G”, “mimic + edge computing”, “mimic + cloud” and “mimic + blockchain” application scenarios. Besides, 4 types of challenges faced by CMD in the future were analyzed and summarized, including escape space of multi-mode decision attack, mutual restriction of heterogeneous and synchronous, difficult balance between security and function, and limited transformation space of existing endogenous security components.

Keywords: cyberspace mimic defense, system architecture, heterogeneous strategy, scheduling strategy, non-cooperative multi-mode decision-making, heterogeneous gain

0 引言

随着网络由单点通信快速驶向万物互联，各类网络软硬件因迭代、开放及成本等因素，体系结构趋于固化、功能逻辑趋于相似、系统配置趋于简易，在提高性能、降低开销的同时，使网络攻击表面相对确定，从根源上导致其对软件漏洞、硬件后门、服务拒绝、信息篡改等网络威胁缺乏内生安全能力，如图 1 所示。为形式化地认知这些泛在化网络威胁，可将其划分为已知威胁和未知威胁，前者尚可用风险概率描述、以先验知识支撑的针对性技术防范；而后者既不能用概率直接刻画又缺乏相关先验知识和防御靶标，造成网络空间攻防长期处于不平衡态势。

“拟态”本身为仿生概念，基于共识机制下的广义鲁棒控制构造，以拟态伪装为本质，以 DHR 机制为核心，旨在以具备视在不确定性的系统结构，应对广义不确定性的网络威胁。理论推导及系统测试^[1]证明，攻击者难以在拟态系统中实现可靠、持续的协同逃逸。自其被提出 8 年来，网

络空间拟态防御（CMD，cyberspace mimic defense）已在理论、技术、产品等层面取得许多进展，在与其他信息技术融合共生中产生较多结合点，正在向“拟态+”生态快速迭代、持续拓展新型应用场景，同时，其发展面临一些内在瓶颈及现实挑战。

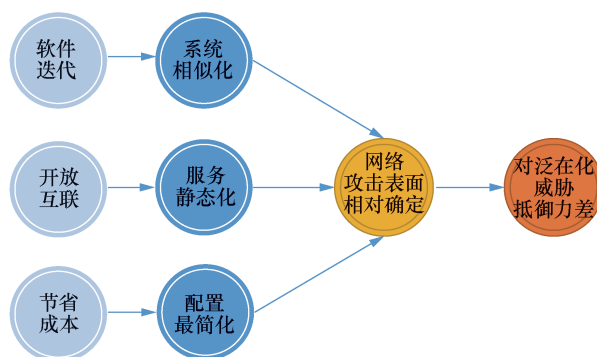


图 1 网络威胁泛在化成因
Figure 1 Causes of the ubiquity of cyber threats

为更好综述网络空间拟态防御发展及未来全景，本文试从纵向、横向、当前、发展及未来 5 个视角开展研究，分别介绍了其发展历程、与其他主动防御技术的异同、现有拟态平台实现、AICDS

共生生态、新型应用场景与未来挑战。本文贡献主要体现在3个方面:一是基于提出的CMD三定理更为直观地阐述了拟态原理,通过对比辨析CMD与其他主动防御技术凸显了CMD本质;二是综述了现有拟态平台的实现要素、性能表现、体系结构、异构策略、调度策略、表决策策略等共性技术,首次将其系统架构分为C式、D式两类,将其异构实现模式分为单源封闭异构实现、单源开放异构实现、多源封闭异构实现和多源开放异构实现4类;三是展望了“拟态+”AICDS未来图景,指出了拟态与AI、IoT、SDN等新型技术的技术结合点。

1 纵向观:CMD发展历程

1.1 概念提出

沙箱、蜜罐、防火墙等第1代安全技术和入侵检测等第2代安全技术,其本质是安全与功能松耦合的外壳式被动防御^[1],信息海量、异构、高维、动态的大数据时代^[2],面临高计算复杂度挑战、大规模存储量瓶颈和威胁泛在不确定性难题;靠封“门”、堵“漏”、杀“毒”、灭“马”,难以闭合安全链,使网络获取“后天免疫”;若强行推行复杂且无部署激励的安全套件,又将因有损网络性能而难以推广。为实现网络安全、功能深耦合,业界提出CMD等第3代内生式主动防御技术^[3],可用较低部署开销使网络获取“先天免疫”。CMD概念源于自然界中条纹章鱼、竹节虫等生物模仿其他生物特征而受益的拟态现象^[4],这些生物可在不改变其内在本质的前提下,改变自身行为、形态等表征特征,通过提升威胁来源对自身的认知难度来化解威胁;CMD技术机理与此类似,可视作旨在提供内生安全增益的主动防御,即在不改变网络功能本质的前提下,动态改变其攻击表面^[5]。

1.2 形成发展

CMD发展可分为理论和实践两条主线,前者衍生出调度重构、同质异构、多模裁决等拟态策略算法,可领先牵引指导实践路线的设计方向;后者孵化为拟态路由器、拟态服务器、拟态防火墙等拟态技术产品,可持续验证支撑理论路线的迭代创新。

1.2.1 拟态理论

拟态理论主要有调度重构、同质异构、多模裁决3个方面。

一是拟态同质异构实现,根据应用对象功能,其可分为存储系统异构、交换系统异构、服务系统异构、安全系统异构4类,如图2所示。其中,存储系统异构方面,如文献[6]针对分布式存储系统数据块校验机制单一、功能脆弱等安全隐患,提出了动态高效的拟态存储校验模型,如图2(a)所示,即在分块写入数据时,对原先固定的块校验逻辑进行动态变换,将请求分发至多个校验执行体进行校验,并将动态校验结果附加至数据块,使多个校验执行算法可在时域上并行随机执行,防止基于固有数据存储逻辑的暴力破解攻击。交换系统异构方面,如宋克等^[7]设计实现了拟态交换机原型样机,通过选用不同CPU、操作系统,以及对协议栈进行多样化编译引入异构,如图2(b)所示。服务系统异构方面,如仝青等^[8]提出在文件存储、SQL脚本、服务器软件、虚拟机操作系统和物理机操作系统进行全软件栈异构化处理,以构建异构服务器执行体池,如图2(c)所示,此时执行体异构性通过两种方式获得,一种是通过引入COTS级异构软件直接获得,另一种是对于SQL查询语句、文件(包括文件目录)等不具备多样性的数据,采用关键字标签化、文件标签化、目录随机化等异构方法人为产生,可在一定限度上避免同源软件漏洞。安全系统异构方面,如拟态蜜罐基于KVM产生上层应用相同而底层基础架构不同的异构虚拟蜜罐,如图2(d)^[9]所示,对外统一的Web应用为CMS系统(Catfish v4.8.54版本,运行库PHP v5.4.16),在操作系统(Windows Server 2012 x64、CentOS 7.8.2003 x64、Ubuntu20.04 x64)、Web中间件(IIS v8.0、Apache v2.4.6和Nginx v1.19.1)两个层面实现异构。

二是拟态多执行体调度。文献[10]系统分析了现有拟态调度算法采用的调度对象、数量和时机3个要素,其中,调度对象方面,将调度对象选取算法分为软件异构度量^[11-15]、异构体组件度量^[11,16-22]和软件相似度度量^[23-25]3类;调度数量方面,选取基于反馈的动态感知调度、基于效用的动态弹性调度、基于判决反馈调度3类调度算

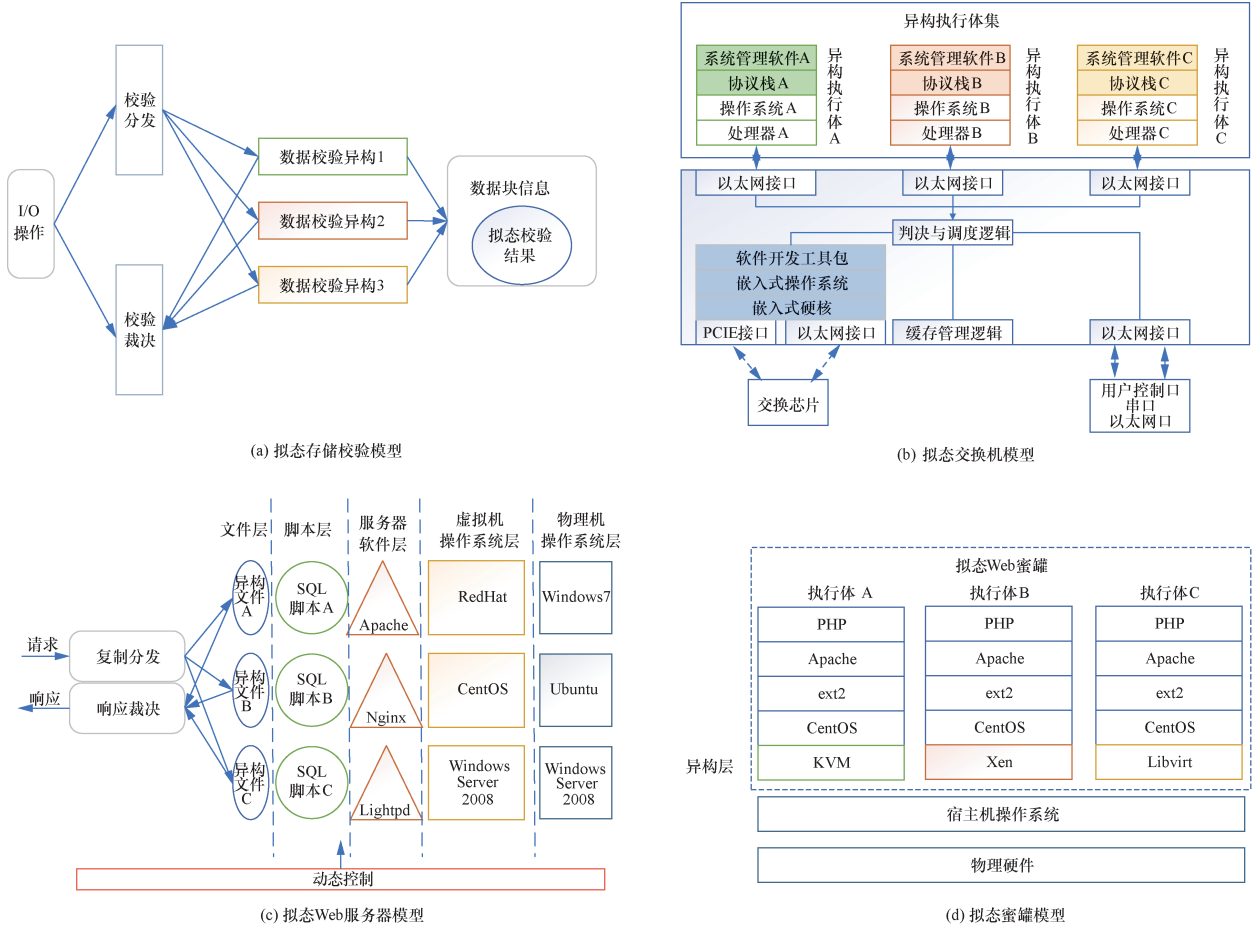


图 2 4 类拟态同质异构模型
Figure 2 Four kinds of mimicry homophily isomerism models

法进行对比分析；调度时机方面，选取最优调度时间算法^[26]、基于滑动窗口模型^[27]两类调度算法进行对比分析，基于动态性、可信任度（用平均失效率衡量）、异构度、系统开销和服务质量 5 个指标，将各类多执行体调度算法综合对比，结果如表 1 所示^[10]。

三是拟态多模表决裁决，传统上可基于大数表决等传统裁决算法，相关改良表决算法主要可分为基于信任度表决、基于定时表决、基于博弈策略表决 3 类。

1) 基于信任度表决所使用的信任度，可进一步分为基于历史表现的经验可信度、基于操作员倾向的权值可信度，如拟态处理机^[28]提出的经验可信度基于处理机表现确定，随每次输出与整体表决输出一致结果而递增，反之则递减；而权值可信度由操作员在对多执行体初始配置时按缺省值预设，随每次处理机清洗减半；再如拟态交换

机^[7]所采用自清洗大数表决算法（TAMA，trustiness based auto-cleanout majority algorithm），由基于信任度的大数裁决策略和定时策略两部分组成，其中，基于信任度的大数裁决子算法，实质也采用经验可信度，即将输出一致的执行体划入同一组 G_k ，按式(1)分别计算集合 G_k 的置信度 W_k 。

$$W_k = \sum_{i=1}^k e^{-\omega_i} \quad (1)$$

其中， ω_i 为执行体 i 的信任权值，初值为 0。选择 W_k 最大的集合 G_p 作为裁决输出，此时执行体 i 的输出与裁决输出的差异率若为 S ，则其信任权值 ω_i 按式(2)更新。

$$\omega_i = \beta S \omega_i \quad (2)$$

其中， β 为大于 0 的权值系数。同时，随机选择信任权值超过阈值 K 的执行体下线清洗。

表1 拟态多执行体调度算法综合对比
Table 1 Comprehensive comparison of mimicry multi-executor scheduling algorithms

调度算法	动态性指标（取值 1~5）	平均失效率	异构度	系统开销	服务质量
MD	1	1.14×10^{-4}	0.114 3	$O(1)$	—
OMD	1	3.60×10^{-4}	0.218 3	$O(1)$	0.450 3
随机调度	5	7.66×10^{-4}	0.272 3	$O(1)$	—
RSMS ^[9]	2	2.77×10^{-4}	0.155 0	$O(n)$	—
PSPT ^[21]	5	—	0.249 0	$O(1)$	—
RSMHQ ^[19]	2	—	0.376 8	$O(n)$	0.519 3
RSMHQH ^[22]	2	—	—	$O(1)$	—
基于正态分布 ^[13]	4	—	—	$O(2^n)$	—
基于BSG ^[16]	2	—	MOSS	$O(n)$	—
基于反馈判决 ^[25]	3	—	MOSS	$O(n)$	—
基于自学习 ^[17]	3	—	—	$O(2^n)$	—
基于安全策略 ^[26]	2	—	—	$O(n)$	—
基于滑动窗口 ^[27]	4	—	—	$O(n)$	—

注：动态性指标取值越大表示动态性越强，MOSS 表示采用基于软件相似性度量衡量执行体间异构度，“—”表示研究未衡量该指标。

2) 基于定时策略表决^[7]主要用于抵御共模协同攻击，该算法基于时间因子，每隔时间间隔 T 根据信任权值选择执行体下线清洗（清洗后信任权值归零），按式(3)计算执行体 i 选取概率 P 。

$$P = \frac{e^{-\omega_i}}{\sum_{i=1}^j e^{-\omega_i}} \quad (3)$$

3) 基于博弈策略表决，主要引入先验知识强化表决，如文献[29]运用了恶意控制器所占比例、系统误差等先验知识，采用字段分解的思想对拟态网络操作系统多控制器执行体输出进行细粒度对比表决，即按式(4)计算最优表决输出 f_i^* 。

$$f_i^* = \arg \max_f \prod_{k=1}^m ((1-\alpha)(1-\varepsilon)n_{eq}^k(i)\varepsilon^{h_i-n_{eq}^k(i)} + \alpha(1-\delta)n_{eq}^k(i)\delta^{h_i-n_{eq}^k(i)}) \quad (4)$$

其中，参数 α 为假设攻击者对所有控制器成功攻击、使其变为恶意控制器的概率； f_i 为正确表决输出 f 的第 i 个字段， h_i 为该字段的位数， $f_{i,j}$ 为该字段的第 j 位； $o_{i,j}^k$ 为控制器 k 输出报文中字段 i 的第 j 位， $r_{i,j}^k$ 为控制器 k 实际向判决器报告的输出报文； $\varepsilon = P(o_{i,j} \neq f_{i,j})$ ； $\delta = P(r_{i,j}^k \neq f_{i,j})$ ，

$$a^k = 1) ; n_{eq}^k(i) = \sum_{j=1}^{h_i} (r_{i,j}^k == f_{i,j})。$$

1.2.2 拟态实践

经各类仿真测试及实际网络部署试用验证，拟态技术产品可提供高可靠、高可用、高可信信息服务，如目前首次线上体系化部署拟态产品体系的景安网络，其主要运用的拟态产品有 5 类。一是拟态路由器，即引入多模异构冗余路由执行体，通过对各执行体维护的路由表项进行共识裁决生成路由表，通过对执行体的策略调度，实现拟态路由器表征的不确定变化。在差异化设计的前提下，多模异构路由执行体存在共模缺陷的概率极低，可通过裁决机制有效阻断对部分执行体的攻击致瘫后果。二是拟态 DNS 服务器。可在不淘汰已有域名协议和地址解析设施的前提下，通过增量部署拟态防御设备组件，有效遏制基于 DNS 服务后门漏洞的域名投毒、域名劫持等已知和未知攻击方法，大幅提高攻击者攻击代价。三是拟态 Web 虚拟机。Web 虚拟机可通过在云环境中部署虚拟机提供低成本解决方案，除面临账号盗用、跨站脚本、缓冲区溢出等传统 Web 威胁外，还面临引入虚拟层导致的侧信道攻击、虚拟层漏洞等新型威胁，引入拟态技术可利用云平台构建

功能等价、动态多样的异构虚拟 Web 执行体池，通过采用动态调度、数据库指令异构化、多余度共识表决等技术，建立多维动态变换的运行空间以阻断攻击链。四是拟态云服务器，通过构建功能等价的异构云服务器池，采用动态执行体调度、多余度共识表决、异常发现、线下清洗等技术，及时阻断基于执行体软硬件漏洞后门等的差模攻击。五是拟态防火墙，针对传统防火墙在 Web 管理和数据流处理层面可能存在的漏洞后门，通过对其架构进行拟态化构造，在管理、数据层面增加攻击者攻击难度，有效防御“安检准入”中的内鬼侵扰，提供切实可信的准入控制保障。

2 横向观：CMD 与其他主动防御技术对比

主动防御技术目前尚未形成公认概念，基于文献[1,3,30]，本文认为其是指不依赖漏洞后门发现和攻击特征分析等攻击先验知识，利用动态、异构、冗余、重构等内生安全机制，对攻击“主动感知、事前防御”的安全技术。在主动防御技术对比方面，文献[31]仅将 CMD 与移动目标防御、可信计算进行了比较，但缺乏与其他主动防御技术的对比分析。本节首先介绍 CMD，而后将其与其他主动防御技术进行对比辨析。

2.1 网络空间拟态防御

2.1.1 核心架构

如图 3 所示，CMD 核心架构为 DHR 架构^[1]，可记为六元组 $\Omega = \{C^n, E^m, K^t, I, V, S\}$ ，其中：

$C^n = \{C_i\}_{i=1}^n$ ，即异构构件池， n 为池内构件类数，所有构件功能的并集构成全系统功能集；

$E^m = \{E_j\}_{j=1}^m$ ，即异构执行体池， m 为池内执行体数，执行体间功能等价，由调度器从 C^n 中随机抽取 C_i 构成；

$K^t = \{K_i\}_{i=1}^t$ ，即服务集， t 为余度；

I ，即输入代理，负责将输入分发给 K^t ；

V ，即表决输出器，负责对 K^t 的输出矢量表决并输出，屏蔽攻击致错后果，并向调度器 S 反馈；

S ，即调度器，负责按调度策略执行调度，识别错误执行体，从 E^m 中随机选择 E_j 进入 K^t 作修

复替换；或使用 C^n 内构件重构 E_j ；或通过虚拟化改变 E_j 的组成配置、运行环境；或基于时间、策略等，选择 E^m 及 K^t 中异构执行体下线清洗。

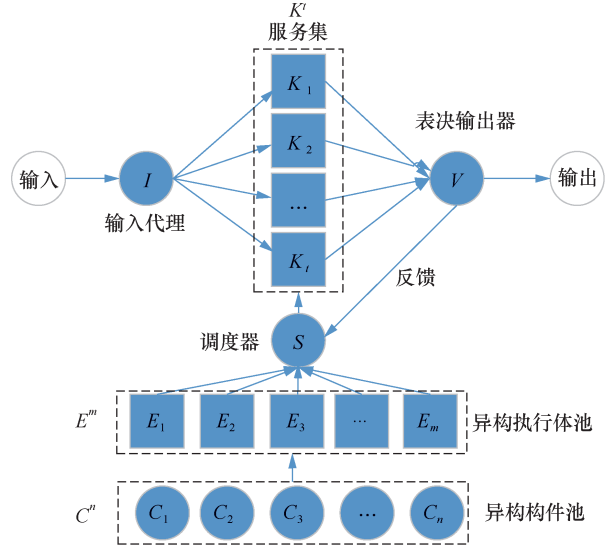


图 3 DHR 架构
Figure 3 DHR architecture

DHR 架构可用 IPO (input-process-output) 模型概述为 $I - K^t / S / E^m / C^n - V$ 。其中， K^t 为功能模块， E^m 、 C^n 为资源模块， S 为控制模块， I 、 V 为输入/输出模块，模块间逻辑独立、功能联动，具体来看，由 I 接收输入并将其复制分发至 K^t 中的冗余执行体 K_i 执行处理，得到的输出矢量由 V 表决并输出，得到的输出唯一且相对正确；由 S 控制 C^n 中的构件动态重构 E^m 中的执行体，根据运行信息选取 E^m 中的执行体进入 K^t ，并对下线执行体进行清洗恢复、重构重组等。可见，CMD 通过引入拟态裁决、策略调度、多维重构、反馈控制、去协同化等内生安全机制，使目标系统具备面向不确定性威胁的广义鲁棒控制能力，实现主动防御。

2.1.2 CMD 三定理

本小节着眼拟态防御效能、拟态风险可控性及拟态安全增益因子 3 个方面，提出 CMD 三定理，并将其作为论证 CMD 内生安全效应原理的支撑。

CMD 三定理间的关系为：CMD 第一定理从增益角度，正面表现拟态防御安全效能可通过控制指标而提升，进而证明其确实存在安全

效能; CMD 第二定理从风险角度, 反面表现拟态风险可控; CMD 第三定理作为前两项定理的补充, 提供设计实现拟态架构时提升其安全增益的途径。

在提出 CMD 第一、第二定理前, 给出定义 1~定义 3 作概念基础。

定义 1 攻击逃逸

将拟态系统 s 在某次广义不确定性攻击下 K' 的输出矢量记为 $\mathbf{O} = \{O^{C_1}, O^{C_2}, \dots, O^{C_i}\}$, 若表决输出错误结果, 则认为攻击产生逃逸, 其必要条件有 5 个 (无须同时成立):

- 1) 攻击者掌握服务集 K' 共模缺陷;
- 2) 输入代理 I 、表决输出器 V 被攻陷;
- 3) 系统产生通信误码、组件故障等随机错误;
- 4) 拟态系统执行环境具备侧信道攻击条件;
- 5) 攻击未导致服务集 K' 输出矢量不一致。

同时, 不将在拟态界外通过社会工程学等手段成功实施的攻击视为攻击逃逸。

定义 2 拟态效能与拟态风险

若对拟态系统 s 同条件攻击 x 次 ($x \geq 100$), y 次未逃逸, 则有式(5)。

$$P_e = \frac{y}{x} 100\% \quad (5)$$

其中, 记 P_e 为拟态防御效能, 简称拟态效能。若同条件攻击不足 100 次, 视 P_e 为拟态效能的近似指标。另有式(6)。

$$P_{\text{risk}} = 1 - P_e \quad (6)$$

记概率 P_{risk} 为系统在该条件下的攻击逃逸率, 简称拟态风险。可见, CMD 将难以量化的不确定性威胁映射为概率。

定义 3 拟态熵和拟态变换增益

若某系统性能指标 (如吞吐量、响应时间) 的归一化参数为 V_i , 则有式(7)。

$$\text{EN}_i = -\text{lb} V_i \quad (7)$$

其中, 记 EN_i 为该性能的性能熵^[32], 以反映其性能。若 V_b 变为 V_a , 则有式(8)。

$$\Delta \text{EN} = -\text{lb} \frac{V_a}{V_b} \quad (8)$$

记 ΔEN 为该系统性能的变换增益。

特别地, 若系统服务集异构度的归一化参数

为 V_h , 则有式(9)。

$$\text{EN}_h = -\text{lb} V_h \quad (9)$$

为反映拟态熵与异构度的正相关性, 修正式(9), 结果如式(10)。

$$\text{EN}_h = \text{lb} V_h \quad (10)$$

其中, 记 EN_h 为系统的拟态熵, 用于描述其服务集异构程度。若经某次调度 V_h 变为 $V_{h'}$, 则有式(11)。

$$\Delta \text{EN}_h = \text{lb} \frac{V_h}{V_{h'}} \quad (11)$$

其中, 记 ΔEN_h 为系统的拟态变换增益, 用于反映系统经调度获取的异构度增益。

基于定义 1~定义 3, 提出 CMD 第一、第二定理。

CMD 第一定理 拟态防御效能与服务集异构度非线性正相关。

证明 考虑 DHR 架构 A , 参考文献[19]提出的异构度量化方法, 若服务集的构件集类数为 M , 服务集的构件集所含构件类数为 S , 构件池 C^n 中构件 C_{ni} 、 C_{nj} 的比例分别为 p_{ni} 、 p_{nj} , 其特有漏洞及共有漏洞的数量依次为 v_{ni} 、 v_{nj} 和 v_{nij} , 则服务集异构度 H_A 可由其复杂度 CO_k 和差异度 FD_{Qn} 决定, 如式(12)所示。

$$H_A = \sum_{n=1}^M \text{CO}_n \cdot \text{FD}_{Qn} \quad (12)$$

其中, CO_n 通过香农多样性指数衡量, 由 S 与 p_{ni} 决定; FD_{Qn} 通过二次熵衡量, 由 S 、 p_{ni} 、 p_{nj} 、 v_{ni} 、 v_{nj} 与 v_{nij} 决定。当服务集中执行体的任意两个构件相异时, H_A 取最大值, 如式(13)所示。

$$H_{\max} = M \left(1 - \frac{1}{S} \right) \ln S \quad (13)$$

基于此, 本文对 H_A 进行 min-max 归一化^[33], 此时拟态熵计算结果如式(14)所示。

$$\text{EN}_h = \text{lb} \frac{H_A - H_{A_{\min}}}{M \left(1 - \frac{1}{S} \right) \ln S - H_{A_{\min}}} \quad (14)$$

考虑服务集共模缺陷逃逸 (拟态逃逸必要条件 1), 忽略偶然因素 2)、3)、4)、5), 此时服务集存在共模缺陷的概率 P_{cm} 与 FD_{Qn} 、 H_A 、 EN_h 均负

相关,即基于构件共有漏洞定义的服务集差异度越大,服务集异构度和拟态熵越大,共模缺陷存在概率越小。另由拟态风险 P_{risk} 定义可知有式(15)成立。

$$P_{cm} \propto P_{\text{risk}} \quad (15)$$

故 P_{risk} 与 H_A 负相关,又因式(6),故 P_e 与 H_A 正相关。且由 H_A 与 FD_{Qn} 正相关而非正比,为非线性正相关关系,而 P_{cm} 与 FD_{Qn} 线性负相关,与 P_e 线性负相关,故 P_e 与 FD_{Qn} 线性正相关,因此 P_e 与 H_A 非线性正相关。

证毕。

CMD 第二定理 拟态风险 P_{risk} 可控。

证明 设置拟态风险 P_{risk} 安全阈值 $P_{\text{risk}}^{\text{threshold}}$,由式(15)得,拟态风险可控实质是保证共模缺陷存在概率 P_{cm} 可控,且 P_{cm} 与 FD_{Qn} 线性负相关,即仅需控制 FD_{Qn} ,而 FD_{Qn} 由 S 、 p_{ni} 、 p_{nj} 、 v_{ni} 、 v_{nj} 与 v_{nij} 决定,与构件 C_{ni} 、 C_{nj} 直接相关,又因构件 C_{ni} 、 C_{nj} 可根据调度算法按阈值要求动态选择,以调整服务集差异度 FD_{Qn} ,可控制 P_{cm} 低于阈值 $P_{\text{risk}}^{\text{threshold}}$ 。

证毕。

在提出 CMD 第三定理前,提出定义 4 作为概念基础。

定义 4 拟态表面

根据 I/O 自动机模型,给定环境 E 下的拟态系统 s ,记三元组 $\{B^E, P^E, D^E\}$ 为该系统 s 的攻击表面^[34],简称拟态表面 AS_s ,即攻击者通过 E 对 s 攻击可触的系统资源集,如式(16)所示。

$$AS_s = \{B^E, P^E, D^E\} \quad (16)$$

其中, B^E 为 s 中 I 、 V 的接口集(如字符串输入接口); P^E 为 s 中 I 、 V 的通道集(如 socket), B^E 中的某接口 B_i^E 需通过 P^E 中的某通道 P_i^E 连接; D^E 为 s 中 K' 的非可信数据项集(如共享文件)。

基于定义 4,提出 CMD 第三定理。

CMD 第三定理 拟态安全增益完全来自其动态、异构、冗余特性,且与传统防御手段安全增益相独立。

证明 首先, CMD 不依赖先验知识和检测机、知识库等外挂防护组件,故与传统防御手段

弱关联,未使用 MTD 等其他主动防御机制;其次, CMD 允许使用不可信构件,因此其安全增益仅来自于架构本身,而架构引入的各类机制可规约为动态、异构、冗余 3 个特性,使组成拟态表面 AS_s 的 B^E 、 P^E 、 D^E 动态变换,进而使攻击链不可达;最后, CMD 可与蜜罐、防火墙等传统手段融合运用,实现拟态蜜罐^[9]、拟态防火墙^[35]等产品,其安全增益相对独立。

证毕。

基于 CMD 三定理阐述拟态原理:首先,基于 CMD 第一定理,由于拟态防御效能与服务集异构度正相关,而拟态 DHR 架构相比其他传统网络架构有显著的异构度增益,故具备拟态防御效能;其次,基于 CMD 第一、第二定理,攻击者连续攻击拟态系统时,基于扫描结果、已知漏洞等先验知识试错,其实质是通过动态变换使系统拟态熵进入熵减过程,而拟态调度通过动态提升拟态熵,抵消攻击者的试错效应,使攻击效应累积从连续过程转为独立过程,因此拟态风险动态平衡,未能超越阈值;再次,基于 CMD 第二定理,多模共识有小概率出现共模缺陷致错,但可通过多维动态迭代处理与裁决,控制拟态风险低于阈值;最后,基于 CMD 第三定理,证明拟态提供的安全增益与传统防御手段相对独立,并可通过强化其动态、异构、冗余特性提高安全增益。

2.1.3 CMD 安全增益

基于 CMD 第三定理,从 3 个层面分析架构安全增益。一是异构性。由于架构安全增益可由 P_e 直观反映,又由式(6)、式(9)、式(13)、式(14)可知, P_e 与服务集 H_A 正相关,理想情况下,在各异构执行体攻击面两两正交时实现绝对异构,可最大化安全增益。异构度量化方法,主要有漏洞量化、功能量化、熵量化和“复杂度-差异度”二维量化 4 类。漏洞量化,如文献[36]通过 CNVD (China national vulnerability database) 查询执行体共同漏洞数量以量化其异构度,但忽略了执行体对未知威胁的反映差异度^[37]。功能量化,如文献[38]利用功能等指标综合考量软、硬件异构度,但仅考量了控制器是否控制同一主机及类别是否一致,评估粒度较粗;熵量化,如文献[39]利用信

息熵^[40]衡量服务集异构度, 提出信息熵 H 与余度 t 正相关, 且 t 一定时各类执行体出现概率相同时 H 最大, 但未考虑异构执行体共模缺陷; “复杂度-差异度”二维量化, 即同时考虑执行体复杂度和差异度, 反映异构度差异较客观, 本文论证 CMD 第一定理时即参照该方法。二是动态性。可为异构性提供时间维度增益, 通过改变服务集异构度 H_A 而间接提供安全增益。为简化执行体异构实现、扩充构件池 C^n , 可对执行体进行重构、重定义、虚拟化等广义动态变换, 降低非绝对异构执行体间的显、隐性关联, 在控制拟态部署成本的基础上提供增量安全增益。三是冗余性。可为异构性提供空间维度增益, 通过改变服务集异构度 H_A 而间接提供安全增益。文献[28]提出冗余度与表决正确率非线性相关, 且余度增长导致成本提升、难以表决; 特别地, 文献[8,41]研究表明 3 模冗余度^[26]性能-开销比最优。

2.1.4 CMD 开销分析

由 CMD 架构机理知, 开销 Pay_{CMD} 可分为异构部件、策略调度、多模裁决、反馈控制、清洗恢复和状态同步 6 部分。其中, 异构部件开销与余度 t 正相关; 策略调度和反馈控制开销与调度策略 (SS, scheduling strategy) 算法性能相关; 多模裁决开销与表决策策略 (VS, voting strategy)、表决输出器性能和异构执行体最长响应时延 $\text{Delay}_{\max}$ 相关; 清洗恢复开销在网络效能未饱和时不直接迟滞网络性能; 状态同步开销与 t 、系统架构 (SA, system architecture) 相关。由 2.1.3 节知, 余度通常取 3, 与 $\text{Delay}_{\max}$ 同由异构策略 (HS, heterogeneous strategy) 决定, 表决输出器性能由硬件决定, 因此, Pay_{CMD} 的决定因素可规约为四元组 $\{\text{SA}, \text{HS}, \text{SS}, \text{VS}\}$, 如式(17)所示。

$$\text{Pay}_{\text{CMD}} \leftarrow \frac{F}{\{ \text{SA}, \text{HS}, \text{SS}, \text{VS} \}} \quad (17)$$

与其他防御技术开销对比, CMD 一是将攻击表面从系统整体缩减为“拟态括号”内的部分组件, 降低了对全体部件的更新升级频次、实时防护要求; 二是对短板组件弱敏感, 可利用 COTS 级构件、开源产品等非可信源构件组成可信系统, 降低系统固有安全开销; 三是可替代防火墙、入侵检测或其他专用安全部件, 节省了相关部署运维开销。

2.2 入侵容忍

1985 年提出“入侵容忍”概念, 旨在通过构建多样化冗余、N-模表决、系统重构、秘密共享及拜占庭一致性协商等机制为系统赋予容侵能力^[42], 使其在被入侵条件下确保安全、持续服务。入侵容忍典型系统架构分为 3 类, 一是基于入侵检测的容忍触发架构, 如 SITAR (scalable intrusion-tolerant architecture for distributed services)^[43], 用于保护商用服务器安全, 但其容忍机制依赖于入侵检测; 二是算法驱动架构, 如 MAFTIA (malicious and accidental fault tolerance for internet applications)^[44], 通过层次化架构保护应用, 但被保护应用需基于项目中间件给定的程序接口和协议平台开发; 三是周期性恢复架构, 如 SCIT (self-cleaning intrusion tolerance)^[45], 通过轮换在线服务器和清洗离线服务器实现容侵, 无须更改现有操作系统及应用程序。入侵容忍技术存在机制复杂度大、多样化执行体成本过高和支撑技术体系未成熟等缺陷, 其原理与 CMD 强相关, 均采用异构冗余、多模表决、系统重构等机制, 给攻击者制造了非协同条件下的异构多目标动态协同攻击困境; 但入侵容忍强调容忍, 仅满足于屏蔽错误, 而 CMD 除此之外还识别、定位、清除错误, 并自动恢复, 防御更为主动。

2.3 移动目标防御

移动目标防御 (MTD, moving target defense) 源自加密或扰码思想^[46], 通过动态调度、系统自清洗、动态域名、源代码多样化、实时编译、多核处理等^[47]技术机制, 为系统赋予多样性、动态性和随机性, 以持续移动攻击面、阻断攻击链。其中, 多样性可分为自然多样性、伪多样性和人工多样性^[48], 动态性为其核心特性, 可在网络层、平台层、运行环境层、软件层^[49]和数据层^[50]等实现; 随机性, 可通过地址空间随机化 (ASR, address space randomization)^[51]、指令集随机化 (ISR, instruction-set randomization)^[52]和内核数据随机化等实现。MTD 典型实现包括 MUTE (mutable network)^[53]和 MAS (moving attack surface) 系统^[54]等。CMD 与 MTD 的区别在于: 为阻断攻击链, MTD 将攻击表面移动, 而 CMD 将攻击表面不规则变换, 可视作 MTD 的拓展, 一方面引入负反馈控制, 可基于防御纠错; 另一方面引入非协同条件, 削弱了执行体间

资源共享,使攻击成功条件由可基于随机试错提高至需基于共模缺陷,提升了攻击难度。

2.4 零信任架构

零信任架构(ZTA, zero trust architecture)于 2010 年提出^[55],强调取消基于网络边界的传统安全模型(如防火墙、NAT、VPN)对网络内部组件授予的默认信任,以身份取代传统网络边界,其核心机制为强认证和最小特权授权,实行“将用户与设备绑定为网络代理,基于网络代理授予信任评分,根据信任评分认证并授权”的安全策略^[56]。ZTA 使用非可信组件构建可信网络的思想与 CMD 相通,二者区别在于实现方法,前者基于信任传递建立信任关系,后者基于多模裁决屏蔽攻击错误,但 ZTA 建立信任链时确立的信任根与加密认证方法均难以确保绝对可信;CMD 对非可信构件的准入门槛比 ZTA 低,更易部署推广。

2.5 可信计算

可信计算(TC, trusted computing)由美国国防部于 1985 年首次提出,其本质是使用基于硬件安全模块的可信计算平台,通过信任度量建立以信任根为锚、以信任关系为链的信任链^[57]。随着物联网、云计算、大数据推动网络快速转型,TC 相关技术标准尚需完善。和 ZTA 相似,TC 与 CMD 均使用非可信组件构建可信网络,区别一是在于安全原理,前者基于计算复杂度,后者基于多模动态异构;二是在于安全根基,前者以认为“绝

对安全”实则无法保证“绝对安全”的 TPM 或 TCM(trusted cryptography module)为可信根,而后者基于普适的“相对正确”公理;三是在于安全等级,TC 信任度量定级标准和测评技术还需健全,可信性有待提高,拟态防御可通过提升服务集异构度动态提高系统安全等级。

2.6 计算机免疫学

计算机免疫学即为计算机引入生物免疫功能,用于识别、隔离或处理网络威胁,具体是将待优化问题对应生物学中的抗原,将优化问题的可行解对应生物学中的抗体 B 细胞等,运用抗体对抗抗原的生物原理处理网络威胁^[58],相关模型有网络病毒免疫模型^[59]、Multi-Agent 免疫模型^[60]、免疫神经网络模型^[61]等。计算机免疫学与 CMD 均为仿生概念,区别在于前者激励计算机产生“代码抗体”主动优化求解问题,需面向多场景拓展适用性;后者因拟态伪装机制给攻击者造成认知困境,更易在计算设备、交换设备、操作系统等各层面推广。

2.7 综合对比

根据对主动防御技术概念的分析,设置攻击先验知识无关性、组件动态水平、风险感知能力、威胁预规避能力 4 个评估指标,按取值 1~5 进行粗粒度计分(分值大小仅反映相对水平,不反映指标绝对值),对当前主要主动防御技术进行对比,如表 2 所示,可见 CMD 较均衡地提高了 4 项主动防御特性,其他主动防御技

表 2 主要主动防御技术对比
Table 2 Comparison of major active defense technologies

技术	发布时间	技术本质	核心特性	典型架构	具体实现	先验知识无关性	组件动态水平	风险感知能力	威胁规避能力
CMD	2016 年	异构执行体策略裁决与动态调度	动态、异构、冗余	DHR	拟态交换机/路由器/处理机等	5	5	4	5
入侵容忍	1985 年	配置冗余资源容忍入侵	冗余	基于入侵检测的容忍触发、算法驱动、周期性恢复	SITAR/MAFTIA/SCIT	2	3	3	4
MTD	2009 年	移动攻击面	多样、动态、随机	动态网络+动态平台+动态环境+动态应用+动态数据	MUTE/MAS	5	5	3	5
ZTA	2010 年	基于信任传递建立信任关系	信任授权	强认证+最小特权授权	无	1	4	5	5
TC	1985 年	以身份取代传统网络边界	信任授权	TPM+TSS+应用	SGX ^[49] /可信云 ^[50]	5	1	1	5
计算机免疫学	20 世纪 90 年代	将网络威胁视为待优化问题求解	免疫	抗原识别+抗体群体产生+群体更新	IMMSIM/ARTIS/Multi-Agent	1	1	4	4

术虽具备较强威胁规避能力，但在其他指标方面还有一定不足。

3 当前观：现有拟态平台实现共性技术

基于 COTS 级产品、自有平台和开源平台，已形成含 10 余类不同功能平台的拟态平台族，经仿真推理和实体网络验证均能提升系统内生安全效应，根据拟态架构安全增益分析及式(17)，应着重关注其关键的四元组{SA, HS, SS, VS}共性技术，表 3 为主要拟态平台共性技术实现，在基于 CVE (common vulnerabilities and exposures) 等现有缺陷或构造漏洞的攻击向量下的性能表现如表 4 所示。

3.1 系统架构

拟态平台系统架构，大多未颠覆原有架构，通过对原架构核心部位增量设置拟态括号实现异构改造，按输入输出交互方式，可分为集中式架

构 (centralized architecture, 简称 C 式架构) 和分布式架构 (distributed architecture, 简称 D 式架构)。

3.1.1 集中式架构

C 式架构，以类 C/S 架构的“请求-应答”工作模式提供集中式拟态服务，分为组件式和分层式两类子架构。组件式子架构，如拟态 Web 服务器^[19]、拟态 DNS 服务器^[62]，由调度器、异构服务器池及请求分发均衡模块等其他组件组成；分层式子架构，如拟态云数据中心^[63]和拟态云服务架构^[64]，前者由基础设施层、异构网络交换层、拟态化括号层、拟态云管理器/拟态化 SaaS (software-as-a-service) 应用层和运维管理层构成，后者通过在原系统服务层构造 MSP (mimic service package) 提供节点式拟态云服务。如图 4 所示，C 式架构中，作为客户端的实体与作为服务端的元功能体交互时，信息流单线输出、链式处理，元功能体在接收实体服务请求后，分发输入、

表 3 主要拟态平台共性技术实现
Table 3 Realization of generic technology of main mimicry platform

拟态平台	系统架构	异构策略	调度策略	表决策略
拟态蜜罐 ^[9]	拟态蜜罐子系统+宿主机操作系统+物理硬件	Web 中间件+操作系统	状态回滚+轮换	行为记录、告警数据对比
拟态防火墙 ^[35]	分布式处理架构	硬件平台+操作系统+安全引擎	未明确	分层次、分阶段裁决
拟态交换机 ^[7]	异构执行体集+拟态调度器+交换芯片	CPU+操作系统	定时清洗+裁决清洗	基于信任权值的自清洗大数表决
拟态路由器	应用层+控制层+设备层	路由器+操作系统	执行体可信度+执行体性能权重	择多判决、权重判决、随机判决
拟态处理机 ^[28]	拟态调度器+异构处理机集+外围电路	操作系统	基于状态保存的两步清洗降级调度	基于可信度的比较择多策略+基于抽样择多的复合单选表决
拟态存储器	拟态调度器+异构处理机集+外围电路	存储编码	输出结果哈希值比对+纠删码	未明确
拟态 Web 服务器 ^[8,19]	中心调度器+动态执行体调度器+服务器池+请求分发均衡模块+表决器 ^[19]	服务器软件+文件系统+虚拟机操作系统+物理机操作系统 ^[19] ；关键字标签化+文件标签化+目录随机化 ^[8]	基于可构成异构构件集种类数的执行体调度 ^[19]	多模裁决前端表决+SQL 语句审查后端表决 ^[8]
拟态 DNS 服务器 ^[62]	异构 DNS 服务器池+选调器	DNS 软件	基于执行体可信度、负载量确定选取系数的调度	大数表决+预表决
拟态计算服务器	CPU+GPU+FPGA+DSP+HRCA+RIC 计算部件+其余部分	计算部件与结构	未明确	未明确
拟态云平台 ^[63-64]	基础设施层+异构网络交换层+拟态化括号层+拟态云管理器/拟态化 SaaS 应用层+运维管理层 ^[63] ；原系统结构+服务层 MSP 化改造 ^[64]	拟态存储+拟态云管+异构网络交换 ^[63] ；虚拟执行体 ^[64]	基于拟态表决、业务迁移和数据同步的调度 ^[63] ；裁决触发、人工触发和策略触发相结合的调度 ^[64]	大数表决 ^[63-64]
拟态网络操作系统 ^[29]	应用层+控制层+拟态层+数据层	NOS+控制器	基于异构度增益的调度	基于博弈策略

表 4 主要拟态平台性能表现
Table 4 Performance of major mimicry platforms

拟态平台	测试方案			安全性能（攻击成功概率）	开销（平均时延）
	扫描	漏洞利用	后门利用		
拟态交换机 ^[7]	✓	✓	—	5 项测试均通过	10 ms
拟态路由器 ^[65]	✓	✓	✓	漏洞利用率 35%（余度为 3）	32 ms（500 条路由）
				漏洞利用率 18%（余度为 7）	52 ms（1 500 条路由）
				后门利用率 4%以下	
拟态处理机 ^[28]	✓	✓	✓	3 个测试项均通过	未测试
拟态存储器	—	—	—	100 个文件经 1 000 次拟态变换持续可用	0.2~1s
拟态 Web 服务器 ^[8]	✓	✓	✓	13 项测试均通过	未测试
拟态 DNS 服务器 ^[62]	—	✓	✓	攻击难度提升 10^{10} 个数量级	506 ms（余度为 5）
拟态云平台 ^[64]	—	✓	—	3 项测试均通过	530 ms（余度为 3）
拟态网络操作系统 ^[29]	—	✓	✓	0.3%~2%	20 ms

多模执行、输出裁决及调度反馈等拟态服务均在元功能体进行，同信息链信息 I/O 位于架构同侧，在每级 I/O 界面实现归一化，通过在 I/O 界面直接引入拟态输入/输出模块实现拟态构造。

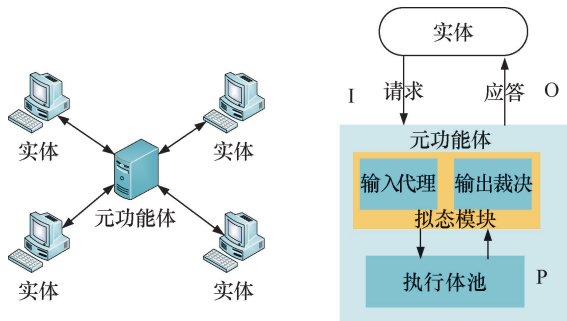


图 4 C 式架构及其信息流
Figure 4 Type C architecture and its information flow

3.1.2 分布式架构

D 式架构，采用类 P2P 架构的对等模式提供分布式拟态服务，分为组件式和分层式两类子架构。组件式子架构，如拟态工控处理机^[28]、拟态交换机^[7]，由异构执行体池、调度器、电路组件构成；分层式子架构，如拟态路由器^[65]，由应用层、控制层和设备层组成。如图 5 所示，D 式架构中，实体间彼此可两两交互，信息流多级多链并行，系统接收输入信息 I 后仅触发系统内部的输出信息 O_{internal} ，外部界面的输入 I 与输出信息 O 间逻辑无关，即同信息链信息 I/O 位于架构异侧，为便于裁决，内部输出矢量需归一化，通过直接在 I/O_{internal} 界面引入拟态输入/输出模块实现拟态构造。

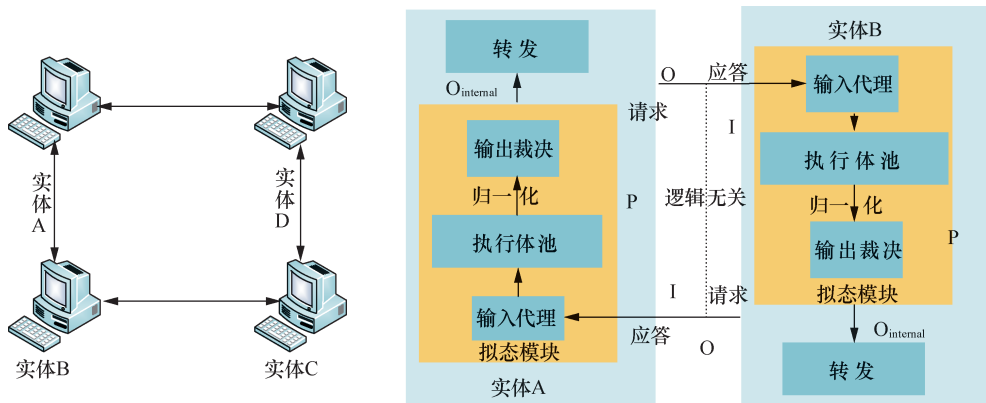


图 5 D 式架构及其信息流
Figure 5 Type D architecture and its information flow

3.1.3 小结

拟态平台系统架构，在信息流程上，符合 I{P}O 闭环控制模型，除输入输出通道外，拟态括号内部件与外界不互通；在子架构选用上，当前实现的组件式子架构多由调度器兼负调度和表决功能，对调度、表决功能一体化设计要求高，而分层式子架构以拟态化控制层为核心，实现较为完备。可见，对现有平台进行拟态化改造时，应着眼其服务模式选取确定异构服务集和多模裁决点，而后区分 C 式或 D 式架构展开改造。

3.2 异构策略

拟态平台异构策略，既可在基础设施、操作系统、文件系统、应用软件等层面实现全栈物理异构，还可通过虚拟化等策略增强虚拟异构度，应重点关注其实现模式、实现层次、构件选用和部件同步 4 个层面。

3.2.1 异构实现模式

根据平台厂商来源和拟态化改造时平台源码是否可控两项条件，可将拟态平台异构实现模式分为 4 类，如图 6 所示。一是单源封闭异构实现，即对于由单一厂商生产的非开源平台，通过直接采用该厂商的多型产品作为服务集并在 I/O 接口增加分发、裁决及调度等机制以进行拟态化改造^[63]。

二是单源开放异构实现，即在开源 COTS 级产品的核心部位，通过多样化编译产品源码等方式设置拟态界。三是多源封闭异构实现，即直接引入多厂商生产的非开源 COTS 级产品作为服务集，并在 I/O 接口设置拟态输入和裁决部件以构建拟态化子系统。四是多源开放异构实现，即对具备动态、异构、冗余特性的开源系统，因应用与平台松耦合且具备异构基础，通过直接引入拟态机制和组合多源应用实现异构。如拟态路由器架构^[65]通过基于 OpenFlow 协议的接口改造，控制未开源的思科、Juniper、中兴、迈普、烽火路由器，即多源封闭异构实现；通过开源软件 Routeflow^[58]直接迁移控制开源的 Quagga、XORP 等路由器，即多源开放异构实现。值得注意的是，这 4 类拟态异构实现模式均面向基于 COTS 级硬件和开源产品、需经拟态化改造才能生成内生安全能力的拟态基线 1.0 产品，而面向基于 DHR 构造、具备原生内生安全能力的拟态基线 2.0 产品，这些异构实现模式已不再需要。

3.2.2 异构实现方法

异构实现方法可分为编码异构、软件异构、硬件异构、软硬件协同异构和混合异构等，与异构实现模式并非一一对应，可结合实际情况灵活

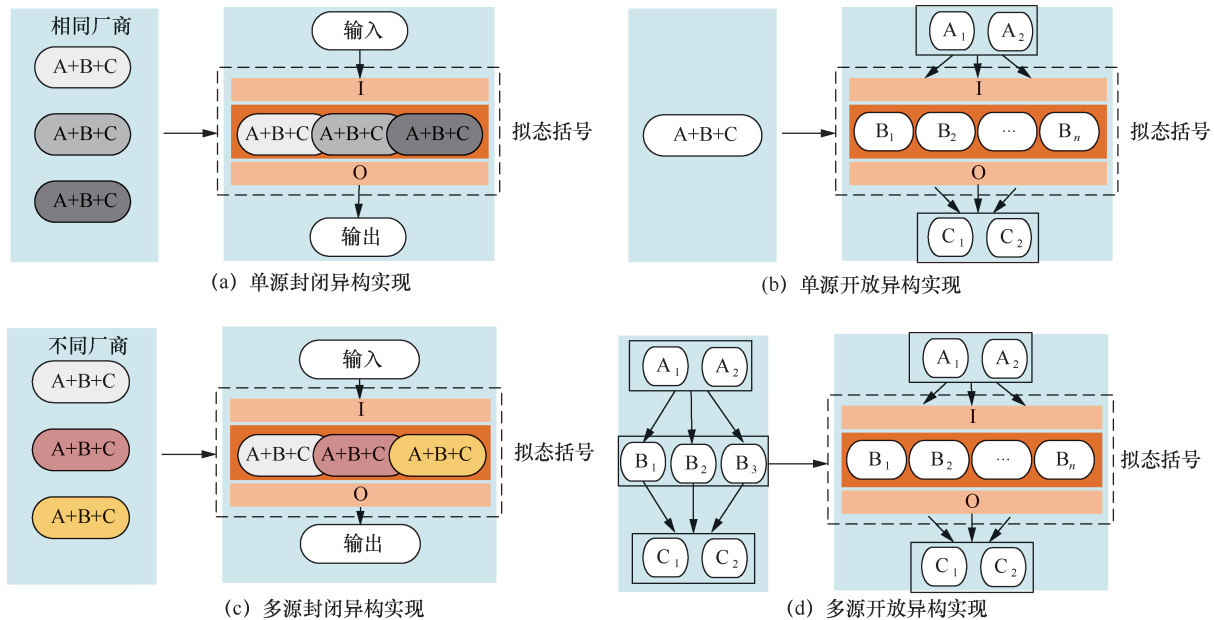


图6 拟态异构实现模式
Figure 6 Mimicry heterogeneous implementation mode

组合,如多源开放异构实现模式既可仅实现软件异构,也可实现软硬件协同异构。

一是编码异构。即采用不同数据编码实现异构,如拟态存储器将文件拆分为块,随机选择多种纠错码编码,实现存储编码异构^[6]。

二是软件异构和硬件异构。软件异构方面,实现手段上,可通过反向栈、ISR、堆布局随机化、栈基址随机化、栈保护、系统调用号随机化、库函数名随机化等^[66]手段实现;实现环节上,可在开发、编译、链接、安装、加载等环节^[67]实现。如拟态蜜罐^[9]在 Web 中间件、操作系统两个软件层设置异构;拟态 Web 威胁感知模型^[68]利用脚本拟态变换技术实现应用脚本异构;M-DNS^[62]采用不同 DNS 软件实现 DNS 服务器异构;拟态处理机采用不同操作系统实现处理机异构。针对拟态 Web 服务器的异构实现,文献^[19]将其设计实现为基于应用软件、服务器软件、数据库、文件系统和操作系统的 5 层异构,但未进行软件同源性分析^[69];而文献^[8]将其设计实现为基于文件系统、服务器软件、虚拟机操作系统的 3 层异构。可见,大多数异构平台通过选用成型异构软件或变换脚本,在开发而非编译、链接、安装、加载等阶段实现软件异构,操作可行性强,异构成本较低。硬件

异构方面,由于异构硬件接口不一,需额外引入对应控制软件,因此单纯硬件异构难以实现,目前尚未出现实例。

三是软硬件协同异构。如拟态交换机^[7]采用异构 {CPU+OS} 硬件模组,并通过多样化编译生成异构协议栈和管理软件族;拟态路由器^[65]采取多种软、硬件控制模式实现 7 模异构路由器;拟态防火墙^[35]针对业务处理逻辑等层面进行拟态化改造,实现 {硬件平台+操作系统+安全引擎} 3 层软硬件异构;拟态计算服务器^[68]按需求混合配置 CPU+GPU、CPU+FPGA、HRCA (hybrid reconfigurable computational array)、RIC (reconfigurable interconnection) 等通用、专用、柔性计算部件,在指令级、部件级、系统级实现软硬件变结构计算。因此,拟态平台可通过在数据接口等部位设置拟态括号,组合运用开源产品、自有产品和 COTS 级产品,实现软、硬件协同异构。

四是混合异构。即采用异构网络部件、异构网络交换等,实现多维混合异构,如拟态云数据中心^[63]除部署拟态部件外,还引入拟态存储、拟态云管、异构网络交换等异构策略。

3.2.3 异构构件选用

现有拟态平台异构构件测试集如表 5 所示。

表 5 现有拟态平台异构构件测试集
Table 5 Heterogeneous component test set of existing mimicry platforms

软件						硬件				
应用软 件 ^[8,19]	服务器软 件 ^[8,19,62]	数据库/ SQL 脚本 ^[8]	SDN 控制 器 ^[29]	文件系 统 ^[8,19]	虚拟/物理主机操作 系统 ^[8,19]	CPU ^[28]	其他计算 部件 ^[68]	路由器 ^[65]	路由器控 制方式 ^[65]	防火墙 ^[35]
	RedHat 7				Ubuntu					
	Windows 7		Floodlight		Windows Server 2003/					
	Debian 7.0		OpenDaylight		2008/2012/2016/2018	Intel	GPU	Quag- ga0.99.22.4	软件迁移 控制路由 器接口改 造组合运 用实体设 备和 SDN 交换机	Linux
PHP	Windows Server 2012	未异构化 处理	RYU	ext2	RedHat 7	Atom	DSP	XORP1.8.5		NGTOS
	IIS 6.0		ONOS	ext4	IIS 6.0	AMD	HRCA	思科 c2600		IPS
	Apache		BEACON	FAT	CentOS	E3930	RIC	Juniper10.2		SSL
	Lighttpd		MAESTRO		Windows XP	龙芯	FPGA	MP3900		DLP
	Ngix		RAW		Windows 7			ZXR10		
					Vx Works					
					中标麒麟					

3.2.4 异构同步模式

为提升拟态架构系统整体效能,应在状态保存、表项下发、故障恢复等时机,在隔离前提下同步异构执行体。同步模式主要有 3 种:一是直联模式,即异构执行体通过接口直接通信,如拟态计算服务器^[68]为实现高带宽数据通信,部件间

采用 FPGA 全互联;二是插件模式,即异构执行体通过调度器或其他拟态插件间接通信,如拟态处理机^[28]通过调度器管理用户请求、响应仲裁和执行体故障隔离、清洗复位;拟态路由器^[70]设置感知决策单元,通过收集状态信息主动调整运行参数;三是消息队列模式,如 MNOS^[29]采用

ZeroMQ 消息队列完成异构执行体间通信,拟态防火墙^[35]采用基于 TIPC (transparent interprocess communication) 集群协议的分布式消息传输。其中,直联模式效率最高,但可能面临协同攻击;拟态插件模式较安全,但造成一定效能损失;消息队列模式性能介于二者之间。同步粒度方面,已有拟态平台未予以明确,其他多变体架构使用的同步粒度按递减排序,有 BUDDY^[71]的应用级监控,ShadowExe^[62]的函数级监控,Detile^[72]的代码级监控,VARAN^[63]、DCL^[64]的系统调用级监控及指令级监控等^[61]。

3.2.5 小结

为提升系统变换安全增益,应侧重选用多源开放异构实现模式和混合异构实现方法,同时,为防范基于冗余体间互联端口链路、共享处理空间等通道或同步机制的多模协同攻击,应侧重选择插件模式或消息队列模式实现异构执行体同步。

3.3 调度策略

调度策略,可细分为下线、上线两项子策略。前者即调度选取特定旧执行体离开服务集的子策略,后者指调度选择适当新执行体进入服务集的子策略。

3.3.1 下线子策略

下线子策略主要有下线操作时机、下线清洗方法两个方面。

一是下线操作时机,可分为定时下线、裁决下线、人工下线、策略下线等。其中,定时下线,即定时选取执行体下线清洗,以防协同渗透、共模缺陷攻击;裁决下线,即每次裁决后令信任权重最低的执行体下线清洗;人工下线,即由操作员主观决策选择执行体下线;策略下线,即基于时间片、随机余度、异常告警监控等策略选择执行体下线。如拟态交换机采取定时下线、裁决下线相结合的下线策略^[7],拟态路由器基于执行体可信度和性能权重指标选择执行体进行下线,拟态云服务架构实行裁决下线、人工下线和策略下线相结合的下线策略^[64]。

二是下线清洗方法,可采用初始化、清零、重启等简易数据复位方式,但无法清除对系统底层软硬件的攻击后果,因此在重置数据后应对执

行体构件进行一定重构,或弃置后换用新执行体,如拟态蜜罐^[9]采用基于状态回滚和轮换的调度策略;拟态云数据中心实行基于业务迁移和数据同步的清洗策略^[63],在发现执行体异常后将其数据迁移至其他云执行体。

3.3.2 上线子策略

上线子策略可基于执行体可信度、负载量等指标,如 M-DNS 实行基于执行体可信度、负载量的选调策略^[62],即随机选择可信度、负载量满足选取系数阈值要求的执行体进入服务集;MNOS 使用基于异构度增益的调度策略^[29],使调度产生的软、硬件异构度增益和最大化。

3.3.3 小结

调度策略实质是对可信度、负载、性能、用户倾向等主、客观指标的平衡,以实现服务集攻击表面的动态变换,如何对其量化评估还需测试验证。值得注意的是,在选择异常降级清洗后的旧执行体重新进入服务集时,由于攻击者已打通对其攻击链,若将其直接加入工作队列后短时间内仍易被攻陷,因此考虑实施梯度回归。如拟态处理机实行基于状态保存的两步清洗降级调度策略,将服务集状态分为 7 级,对其逐级进行清洗、上线^[28]。

3.4 表决策略

表决策略应重点关注表决算法、表决层次和表决时延控制等因素。

3.4.1 表决算法

表决算法,可选用大数表决^[73]、一致表决^[74]、 n 中取 2 表决^[75]、随机表决、轮询表决、择多表决^[76]等传统算法,及自检测多数一致表决算法^[77]、自适应一致表决算法^[78-79]等改良算法,其中择多表决的可信度最高,虽无法保证绝对正确,但根据 CMD 第二定理知,择多错误概率随余度增加而非线性减小,风险可控,主要有 3 类。

一是静态算法,即表决策略确定后不再变动,如 M-DNS^[62]指定采用大数表决算法。

二是动态算法,即可灵活确定表决策略,如拟态路由器^[65]依据安全等级,可指定择多判决、权重判决、随机判决等算法。

三是复合算法,即复合运用多种表决策略,如拟态蜜罐^[9]基于行为记录、告警数据对比进行

表决；拟态防火墙^[35]采用分层次、分阶段表决；为应对时间协同、共模缺陷攻击，拟态交换机在大数表决中增加信任评估和定时扰动，实施基于信任权值的自清洗大数表决，即在表决时优先采用高信任权值执行体的输出，且信任权值随执行体表决输出差异度等历史表现动态更新；拟态处理机^[28]引入基于处理机历史表现的经验可信度和基于系统安全员主观倾向的权值可信度，实行基于可信度的比较择多算法，并提供了可选的基于抽样择多的复合单选判决算法；MNOS^[29]考虑到每次大数表决相互独立的缺陷，利用恶意控制器所占比例、系统误差等先验知识实现基于博弈策略的表决算法，提升了表决准确性，但提高了计算量和时延。

3.4.2 表决层次

应根据表决场景选取表决层次。由于异构执行体输出格式、信息内字段设置等不同，若在语义层表决，粒度难以掌握，需辅以智能语义分析算法，误报率较低，漏报率较高，适用于模糊表决；而数据层表决更为精确，漏报率降低，但误报率较高，适用于精确表决。如 Web 服务器实现两个表决器^[8]，即用于多模裁决的前端表决器和用于过滤非法 SQL 语句的后端表决器，前者在语义层表决，以屏蔽异构服务器响应的细节差异；后者在数据层表决，以屏蔽异构机制导致的 SQL 语句差异。

3.4.3 表决时延控制

拟态平台的时延开销主要来自表决^[8]，为降低表决时延，提高表决准确率，应对服务集输出矢量进行标准化、归一化。例如，文献[8]提出拟态 Web 服务器可通过模块硬件固化、非关键功能解耦，形成专用组件以降低开销。

3.4.4 小结

为提高拟态平台表决性能，应结合具体场景选用表决层次，着重采取动态表决策略，并对执行体输出矢量进行归一化。

4 发展观：“拟态+”AICDS 共生生态

随着拟态技术与 AI、IoT（internet of things）、Cloud、Data 和 SDN 等新型技术深度融合，将逐渐形成“拟态+”AICDS 共生生态，但目前存在较多

技术瓶颈、盲区。

4.1 拟态+AI

CNN^[80]、RNN^[81]、GNN^[82]、GRU^[83]等神经网络算法驱动的人工智能技术，可用于优化拟态多模裁决、态势感知、数据计算等性能，例如，技术结合点可通过流量分类检测异常的深度学习用于增强多模裁决准确率；可自主推测调度方案的强化学习用于优化调度策略。相关研究方面，英特尔于 2017 年开发了首款支持自监督学习和强化学习的神经拟态芯片 Loihi^[84]，并于 2020 年提出“神经拟态计算”架构^[85]，通过 EMIB^[86]、Foveros^[87]等技术封装多模异架构芯片，提高了对多源非结构化数据的识别准确率和能效比；文献[88]针对现有拟态裁决机制无法有效归纳分析拟态架构安全态势的不足，提出基于裁决差异性判别的 Web 威胁态势分析算法，将网络态势感知技术融入拟态架构，通过 LSTM 网络挖掘、分类、融合多层次拟态裁决告警日志特征，并根据分类结果实现威胁可视化展示，基于真实互联网环境的实验证明该方法可有效获取 CMD 架构安全态势。总体来看，目前拟态技术与各类神经网络结合运用的算法架构较少，在智能裁决、智能调度等方面有较大研究价值。

4.2 拟态+IoT

物联网^[89]中连接泛在、数据聚合、平台各异、设备复杂，可靠性存在较大隐患^[90]，而拟态 DHR 架构可为其提供可靠性保证，技术结合点如智能网联汽车拟态化控制/通信系统，或对多源传感器数据应用拟态化分析引擎。相关实例如第 4 届“强网”拟态防御国际精英挑战赛展示的具有内生安全属性的拟态高级智能驾驶辅助系统（ADAS），在高强度网络攻击中展现了相对传统商用产品的安全优势；再如车联网拟态防御系统^[91]通过采集、分析威胁数据建立拟态化分析引擎，可通过动态重构组合车载端与车载服务器端安全规则，产生内生安全效应。

4.3 拟态+Cloud

如上文所述，拟态架构可用于保护云平台^[63,68]，技术结合点主要是构建基于多模执行体的拟态云平台；此外，学术界对“拟态+云”的裁决策略、反馈控制、行为预测等展开了相关研究。裁决策

略方面,如文献[92]针对拟态云服务系统各异构执行体输出矢量因不一致而难以裁决的问题,提出了基于模板对比和置信度修正的异构执行体输出一致性裁决方法;再如文献[21]提出了基于相似性指标对服务集进行优先级预排序,并结合时间片策略进行调度的 PSPT 算法,平衡了系统动态性与异构性。反馈控制方面,如文献[93]通过对虚拟机进行拟态封装,基于异构虚拟机的异构度实现云执行环境的动态轮换反馈控制。行为预测方面,如文献[94]组合运用擅长处理线性关系的 ARIMA^[95]模型与擅长处理非线性关系的 RBF^[96]模型,优化了拟态调度组件对云应用行为的离线预测性能。

4.4 拟态+Data

Hbase^[97]、ES、RabbitMQ、Celery^[98]等大数据系统以 CPU 等通用处理器为核心,结构单一、能效比低,学术研究主要集中于通过混合异构平台提高加速比和能效比,无法保证计算任务与体系结构相匹配,要求计算架构和处理机制范式同步向多模化、动态化革新,这正是大数据与拟态防御的技术结合点,如基于拟态计算的大数据处理方法^[99]。此外,2018年,复旦大学与多家企业提出共同推进通用拟态大数据平台发展,为拟态计算在大数据分析处理和数据挖掘领域应用提供技术路径。在拟态大数据平台具体实现上,文献[100]设计提出了高效能拟态大数据平台,通过构造体系结构匹配矩阵将计算子任务动态分配至 CPU、GPU、FPGA 等组合处理部件,实验表明,相较纯 CPU 架构,CPU+FPGA 拟态架构可深度融合异构计算部件,能效比更高,还可灵活拓展;文献[101]提出基于拟态计算的大数据精准服务架构,主要分为数据源、数据导入、数据存储、拟态计算、精准数据分析、数据精准推荐技术等部分,使软硬件深度耦合;文献[102]提出综合运用多种拟态系统,构建包括数据源、拟态设备、拟态计算及数据应用服务等组件的拟态大数据应用平台。总体来看,“拟态+大数据”应用模式在异构部件编配、计算子任务切分等方面的研究还需深化。

4.5 拟态+SDN

一方面,SDN 有助于拟态异构通过 NFV^[103]实现、支撑拟态功能模块化、增量式部署,还可

增强拟态架构与业务功能耦合度,实现“功能即安全”;另一方面,SDN 服务部署面临服务链被篡改、截取、重放等威胁,对其控制层进行拟态化改造,可为其赋予内生安全效应,二者的技术结合点包括拟态控制器、SDN 流的多模裁决等。如文献[17,104]提出拟态 SDN 服务部署架构,由应用层/用户业务需求、控制层和网络层组成,对 SDN 控制层进行拟态改造;文献[105]针对 SDN 主控制器单点故障和异构控制器表项对比问题,提出拟态 SDN 控制层安全机制,引入多模异构控制器实现多样化民主监督,并提出基于转发语义的异构控制器流表项对比算法。面向“拟态+SDN”实现面临的各类问题,文献[106]聚焦现有基于 SDN 的 MNOS 流表不一致、调度算法泛用性差、缺少安全性能评估 3 项缺陷,分别提出了基于流表可信度和自清洗机制的流一致裁决方法,基于攻击信息的动态负反馈调度方法,以及基于攻防收益函数博弈的拟态控制平面安全性能评估方法;文献[107]针对异构控制器流规则一致性判别难题,提出基于流表规则管道图和边缘端口流矩阵对比的控制层裁决策略。

5 未来观:“拟态+”未来新型应用场景及挑战

在拟态化浪潮带动下,“拟态+”将激发更多应用可能,也将面临更多挑战。

5.1 新型应用场景

拟态基线 2.0 技术研发及其与 5G、6G、边缘计算、云服务、区块链等新兴技术深度融合,将产生更多新型拟态应用场景。一是拟态基线 2.0 产品生态,通过对软硬构件、信息系统、控制装置等通用对象,全面采用内生安全原生设计规范和晶圆级微封装工艺,实现多领域、微粒度、全维度多模异构,使内生安全成为新一代信息系统的基本功能,其重点包括拟态基线 2.0 拟态效能测试技术、原生内生安全开发工具链与开发环境、拟态构造测评标准等。二是“拟态+5G/6G”。随着 5G 通信应用部署和 6G 通信研究推进,拟态技术在大规模互联网络的机制同步和推广部署条件趋于成熟,便于其提供分布式广域移动安全服务,更好支撑高速异构网络跨域发展。同时,除网络

交换、处理设备外,拟态技术还将走向手机、平板等移动端平台,用于解决 5G/6G 通信网面临的云、移动边缘计算^[108]和垂直业务中的安全挑战。三是“拟态+边缘计算”。边缘计算因其网络复杂、设备分散、规模庞大,面临身份认证、访问控制、密钥管理等威胁^[109],拟态技术可为其提供跨设备、链路、网络层,覆盖分发、计算、存储业务流程的安全屏障,如拟态分布式多接入边缘计算架构^[110]将数据分割转发至多个边缘节点处理,并基于校验分析实现了 CMD 机制。四是“拟态+云”。云计算、云服务等“云化”服务模式中,集中管理资源和信息跨域传输客观导致攻击目标相对集中、普遍暴露,通过为云配备拟态调度管理组件,可支撑多个云应用与拟态服务组件集群的融合协同^[94],形成基于内生安全的“拟态云”服务模式,为“新基建+新安全”提供机遇;还可支撑云端一体协同防御,拓宽网络防御纵深。五是“拟态+区块链”。区块链虽具备去中心、去信任、不易篡改、防伪造、可溯源等特性,但在高价值数据存储流通中面临私钥丢失、合约代码漏洞^[111]、自私挖矿^[112]等安全威胁,拟态架构同样可为其提供保护。例如,拟态区块链^[113]借鉴 DHR 架构和密码抽签思想,提出了动态异构共识机制和动态异构冗余签名算法,测试表明该算法效率受限于 SM2 算法和共识算法。

5.2 未来挑战

CMD 虽具备颠覆性内生安全效应,但事实上其安全性能还有待提高,部署成本有待降低,其“拟态+”发展主要面临以下 4 类挑战。

(1) 非协同多模决策下存在攻击逃逸空间

一是拟态 DHR 架构可选的异构构件集相对确定,即架构最大变换空间有限,拥有足够攻击资源的攻击者可实现基于多模决策架构的攻击逃逸;二是基于 DHR 架构的各类拟态系统安全逻辑相同、机制相似,APT 攻击者可长期监控其变换规律,掌握其内部执行体的变换空间、轮换规律,伺机突破,若单纯靠增加冗余度强化防御,将损失较多网络性能;三是 DHR 防御范围仅限于拟态括号,通过侧信道攻击等方式实施跨物理域协同攻击,或不造成多模输出相异的窃密攻击,

都可绕过拟态架构;四是拟态化部署可能引入新系统子层,扩大攻击表面,提升原架构防御协同复杂度。

(2) 异构度增益与执行体同步互相掣肘

一方面,为提升系统变换安全增益,防范基于冗余体间端口链路、共享空间等通道或同步机制的多模协同攻击,要求执行体、构件尽量实现高度异构,如 MNOS 等拟态架构基于异构度增益调度需尽量提升执行体异构度;另一方面,同步异构执行体工作状态及输入输出矢量时,虽可选用较为安全的插件模式或消息队列模式,却因执行体高度异构增大了部署难度和同步时延,异构度增益与开销间掣肘制约了网络性能提升,又缺少成熟的量化验证和度量机制,难以取得可信平衡条件。

(3) 安全与功能难以平衡

一是异构设计及部署难度较大。拟态架构引入各类安全部件,必然带来一定软硬件开销及执行体异构设计部署难度。如拟态原理要求功能等价执行体间绝对异构,即空间隔离、逻辑独立、交集最小,难以设计实现,若直接使用 COTS 级异构执行体,不仅无法满足异构度要求,还带来一定公开漏洞风险,因此通常对其虚拟化改造后投入应用,以扩充异构执行体选择范围,将硬件成本缩减为软件成本,但这种改造短期内难以规模化实现、形成完整产业生态链。二是调度及表决策策略渐趋复杂。为增强调度及表决策策略可信性,研究者提出多种需软硬件支撑的多样化动态化指标和复杂算法,其开销及部署难度与其对网络发展的支撑度、规模化部署的激励度密切相关。

(4) 现有内生安全组件拟态熵有限

各类拟态架构平台使用的异构执行体,多选自代码不可控、不可信的 COTS 级组件和开源平台,难以实现全软件栈、底层硬件细粒度异构,调度变换产生的拟态熵空间有限,亟须开发按多源开放异构实现模式设计、具备原生内生安全属性的新型内生安全软硬件。

6 结束语

CMD 发展至今,已由单纯的“拟态猜想”发

展为繁复的“拟态+生态”,本文从纵向、横向、当前、发展和未来5个角度,综述其发展历程、原理本质、平台实现、技术增长点、未来挑战及应用场景,具体来说,推导阐述了基于CMD三定理的拟态原理,基于十余类现有拟态平台,分析了其系统架构模式、异构策略、调度策略和表决策策略,结合AI、IoT、云、大数据、SDN等新兴技术,提出了“拟态+”AICDS共生生态,展望了拟态发展面临的4大挑战和4类新型应用场景。可见,拟态技术虽已发展进入“拟态+生态”,但面临多重挑战,与各类技术结合的诸多研究点有待突破。

参考文献:

- [1] 郭江兴. 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
- [2] 王珊, 王会举, 覃雄派, 等. 架构大数据: 挑战、现状与展望[J]. 计算机学报, 2011, 34(10): 1741-1752.
WANG S, WANG H J, QIN X P, et al. Architecting big data: challenges, studies and forecasts[J]. Chinese Journal of Computers, 2011, 34(10): 1741-1752.
- [3] 陈钟, 孟宏伟, 关志. 未来互联网体系结构中的内生安全研究[J]. 信息安全学报, 2016, 1(2): 36-45.
CHEN Z, MENG H W, GUAN Z. Research on intrinsic security in future Internet architecture[J]. Journal of Cyber Security, 2016, 1(2): 36-45.
- [4] 郭江兴. 拟态计算与拟态安全防御的原意和愿景[J]. 电信科学, 2014, 30(7): 2-7.
WU J X. Meaning and vision of mimic computing and mimic security defense[J]. Telecommunications Science, 2014, 30(7): 2-7
- [5] 郭江兴. 网络空间拟态防御原理简介(下)[J]. 网信军民融合, 2017(2): 43-47.
WU J X. An introduction to principles of mimic defense in cyberspace(Part 2)[J]. Civil-Military Integration on Cyberspace, 2017(2): 43-47.
- [6] 余平, 李宁波, 谢彬, 等. 面向拟态防御系统的存储校验模型[J]. 数字技术与应用, 2018, 36(9): 54-56, 58.
SHE P, LI N B, XIE B, et al. The model of storage verification under mimic defense theory[J]. Digital Technology & Application, 2018, 36(9): 54-56, 58.
- [7] 宋克, 刘勤让, 魏帅, 等. 基于拟态防御的以太网交换机内生安全体系结构[J]. 通信学报, 2020, 41(5): 18-26.
SONG K, LIU Q R, WEI S, et al. Endogenous security architecture of Ethernet switch based on mimic defense[J]. Journal on Communications, 2020, 41(5): 18-26.
- [8] 全青, 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.
- [9] 王涵, 卜佑军, 江逸茗, 等. 一种拟态蜜罐系统的设计与研究[J]. 网络安全技术与应用, 2021(2): 1-3.
WANG H, BU Y J, JIANG Y M, et al. Design and research of a mimic honeypot system[J]. Network Security Technology and Application, 2021(2): 1-3.
- [10] 朱正彬, 刘勤让, 刘冬培, 等. 拟态多执行体调度算法研究进展[J]. 通信学报, 2021, 42(5): 179-190.
ZHU Z B, LIU Q R, LIU D P, et al. Research progress of mimic multi-execution scheduling algorithm[J]. Journal on Communications, 2021, 42(5): 179-190.
- [11] 姚文斌, 杨孝宗. 相异性软件组件选择算法设计[J]. 哈尔滨工业大学学报, 2003, 35(3): 261-264.
YAO W B, YANG X Z. The design of different software component selection algorithm[J]. Journal of Harbin Institute of Technology, 2003, 35(3): 261-264.
- [12] 吕迎迎, 郭云飞, 王祺鹏, 等. SDN 中基于历史信息的负反馈调度算法[J]. 网络与信息安全学报, 2018, 4(6): 45-51.
LYU Y Y, GUO Y F, WANG Z P, et al. Negative feedback scheduling algorithm based on historical information in SDN[J]. Chinese Journal of Network and Information Security, 2018, 4(6): 45-51.
- [13] 张震骁. 拟态防御动态调度策略研究[D]. 郑州: 郑州大学, 2018.
ZHANG Z X. Research on dynamic dispatch strategy of mimic defense[D]. Zhengzhou: Zhengzhou University, 2018.
- [14] LI J F, WU J X, HU Y X, et al. DSL: dynamic and self-learning schedule method of multiple controllers in SDN[J]. ETRI Journal, 2017, 39(3): 364-372.
- [15] 沈丛麒, 陈双喜, 吴春明, 等. 基于信誉度与相异度的自适应拟态控制器研究[J]. 通信学报, 2018, 39(S2): 173-180.
SHEN C Q, CHEN S X, WU C M, et al. Adaptive mimic defensive controller framework based on reputation and dissimilarity[J]. Journal on Communications, 2018, 39(S2): 173-180.
- [16] 王晓梅, 杨文喆, 张维, 等. 基于BSG的拟态Web服务器调度策略研究[J]. 通信学报, 2018, 39(S2): 112-120.
WANG X M, YANG W H, ZHANG W, et al. Research on scheduling strategy of mimic Web server based on BSG[J]. Journal on Communications, 2018, 39(S2): 112-120.
- [17] 李传煌, 任云方, 汤中运, 等. SDN 中服务部署的拟态防御方法[J]. 通信学报, 2018, 39(S2): 121-130.
LI C H, REN Y F, TANG Z Y, et al. Mimic defense method for service deployment in SDN[J]. Journal on Communications, 2018, 39(S2): 121-130.
- [18] TWU P, MOSTOFI Y, EGERSTEDT M. A measure of heterogeneity in multi-agent systems[C]//Proceedings of 2014 American Control Conference. 2014: 3972-3977

- [19] 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.
- [20] GARCIA M, BESSANI A, GASHI I, et al. Analysis of operating system diversity for intrusion tolerance[J]. Software: Practice and Experience, 2014, 44(6): 735-770.
- [21] 普黎明, 刘树新, 丁瑞浩, 等. 面向拟态云服务的异构执行体调度算法[J]. 通信学报, 2020, 41(3): 17-24.
PU L M, LIU S X, DING R H, et al. Heterogeneous executor scheduling algorithm for mimic cloud service[J]. Journal on Communications, 2020, 41(3): 17-24.
- [22] WU Z Q, WEI J. Heterogeneous executors scheduling algorithm for mimic defense systems[C]//Proceedings of 2019 IEEE 2nd International Conference on Computer and Communication Engineering Technology. 2019: 279-284.
- [23] QIU D H, LI H, SUN J L. Measuring software similarity based on structure and property of class diagram[C]//Proceedings of 2013 Sixth International Conference on Advanced Computational Intelligence (ICACI). 2013: 75-80.
- [24] 顾泽宇, 张兴明, 林森杰. 基于安全策略的负载感知动态调度机制[J]. 计算机应用, 2017, 37(11): 3304-3310.
GU Z Y, ZHANG X M, LIN S J. Load-aware dynamic scheduling mechanism based on security strategies[J]. Journal of Computer Applications, 2017, 37(11): 3304-3310.
- [25] 高明, 罗锦, 周慧颖, 等. 一种基于拟态防御的差异化反馈调度判决算法[J]. 电信科学, 2020, 36(5): 73-82.
GAO M, LUO J, ZHOU H Y, et al. A differential feedback scheduling decision algorithm based on mimic defense[J]. Telecommunications Science, 2020, 36(5): 73-82.
- [26] LU Z P, CHEN F C, CHENG G Z, et al. Towards a dynamic controller scheduling-timing problem in software-defined networking[J]. China Communications, 2017, 14(10): 26-38.
- [27] GUO W, WU Z Q, ZHANG F, et al. Scheduling sequence control method based on sliding window in cyberspace mimic defense[J]. IEEE Access, 2019, 8: 1517-1533.
- [28] 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.
- [29] 王祺鹏, 扈红超, 程国振. MNOS: 拟态网络操作系统设计与实现[J]. 计算机研究与发展, 2017, 54(10): 2321-2333.
WANG Z P, HU H C, CHENG G Z. Design and implementation of mimic network operating system[J]. Journal of Computer Research and Development, 2017, 54(10): 2321-2333.
- [30] 胡爱群, 方兰婷, 李涛. 基于仿生机理的内生安全防护体系研究[J]. 网络与信息安全学报, 2021, 7(1): 11-19.
HU A Q, FANG L T, LI T. Research on bionic mechanism based endogenous security defense system[J]. Chinese Journal of Network and Information Security, 2021, 7(1): 11-19.
- [31] 张启浩, 邓中, 周冬梅. 拟态防御与国外网络安全研究成果比较分析[J]. 智能建筑, 2018(8): 17-22.
ZHANG Q, DENG Z, ZHOU D M. Comparative analysis of mimic defense and foreign network security research results[J]. Intelligent Building, 2018(8): 17-22.
- [32] 张举, 耿海军, 刘洁琦. 基于网络熵的域内节能路由方案[J]. 计算机科学, 2019, 46(2): 76-80.
ZHANG J, GENG H J, LIU J Q. Intra-domain energy efficiency routing scheme based on network entropy[J]. Computer Science, 2019, 46(2): 76-80.
- [33] TAN P N, STEINBACK M, KUMAR V. Introduction to data mining[M]. Posts & Telecom Press, 2006.
- [34] 陈福才, 扈红超, 刘文彦, 等. 网络空间主动防御技术[M]. 北京: 科学出版社, 2018: 260-264.
CHEN F C, HU H C, LIU W Y, et al. Active defense technology in cyberspace[M]. Beijing: Science Press, 2018: 260-264.
- [35] 北京天融信网络安全技术有限公司, 等. 一种基于网络的数据处理方法及电子设备: 中国, 110311850A[P]. 2019-10-08.
Beijing Topsec Network Security Technology Co., Ltd., et al. A network-based data processing method and electronic equipment: China, 110311850A[P]. 2019-10-08.
- [36] 刘勤让, 林森杰, 顾泽宇. 面向拟态安全防御的异构功能等价体调度算法[J]. 通信学报, 2018, 39(7): 188-198.
LIU Q R, LIN S J, GU Z Y. Heterogeneous redundancies scheduling algorithm for mimic security defense[J]. Journal on Communications, 2018, 39(7): 188-198.
- [37] 杨维永, 廖鹏, 刘金锁, 等. 应对新型网络威胁下的数据保护技术研究[J]. 电力信息与通信技术, 2014, 12(5): 136-139.
YANG W Y, LIAO P, LIU J S, et al. Research on data protection technology in response to new cyber threats[J]. Electric Power Information and Communication Technology, 2014, 12(5): 136-139.
- [38] ZHENG L, NIE X Q, TAO Y, et al. Applications of intrusion-tolerance pre-response in the grid enterprises[C]//Proceedings of 2012 Fourth International Conference on Computational and Information Sciences. 2012: 985-988.
- [39] 扈红超, 陈福才, 王祺鹏. 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. Performances valuations on DHR for cyberspace mimic defense[J]. Journal of Cyber Security, 2016, 1(4): 40-51.
- [40] ROBERT M G. Entropy and information theory[M]. Berlin: Springer, 2011.
- [41] 潘计辉, 张盛兵, 张小林, 等. 三余度机载计算机设计与实现[J]. 西北工业大学学报, 2013, 31(5): 798-802.
PAN J H, ZHANG S B, ZHANG X L, et al. Design and implementation of airborne computer with triple degrees[J]. Journal of

- Northwestern Polytechnical University, 2013, 31(5): 798-802.
- [42] LI Z J, HU B, LU T Q, et al. Research on risk prevention and control strategy of power grid CPS system based on intrusion tolerance[J]. IOP Conference Series: Earth and Environmental Science, 2021, 675(1): 147-156.
- [43] WANG F Y, UPPALLI R. SITAR: a scalable intrusion-tolerant architecture for distributed services-a technology summary[C]//Proceedings of Proceedings DARPA Information Survivability Conference and Exposition. 2003: 153-155.
- [44] STROUD R, WELCH I, WARNE J, et al. A qualitative analysis of the intrusion-tolerance capabilities of the MAFTIA architecture[C]//Proceedings of International Conference on Dependable Systems and Networks. 2004: 453-461.
- [45] BANGALORE A K, SOOD A K. Securing web servers using self cleansing intrusion tolerance (SCIT)[C]//Proceedings of 2009 Second International Conference on Dependability. 2009: 60-65.
- [46] DAI Q N, TIAN Y H. Optimal design of MTD filter based on FIR[C]//Proceedings of 2019 IEEE International Conference on Signal, Information and Data Processing. 2019: 1-4.
- [47] KAMPANAKIS P, PERROS H, BEYENE T. SDN-based solutions for Moving Target Defense network protection[C]//Proceedings of Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014. 2014: 1-6.
- [48] 樊琳娜, 马宇峰, 黄河, 等. 移动目标防御技术研究综述[J]. 中国电子科学研究院学报, 2017, 12(2): 209-214.
- FAN L N, MA Y F, HUANG H, et al. The research summary of moving target defense technology[J]. Journal of China Academy of Electronics and Information Technology, 2017, 12(2): 209-214.
- [49] 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]//Proceedings of 2014 IEEE International Conference on Communications. 2014: 804-809.
- [50] HU P F, LI H X, FU H, et al. Dynamic defense strategy against advanced persistent threat with insiders[C]//Proceedings of 2015 IEEE Conference on Computer Communications. 2015: 747-755.
- [51] SEO J, LEE B, KIM S, et al. SGX-shield: enabling address space layout randomization for SGX programs[C]//Proceedings 2017 Network and Distributed System Security Symposium. 2017.
- [52] WANG J, YAO Y, ZHANG G F, et al. Defense method of ruby code injection attack based on instruction set randomization[C]//Proceedings of ICCCM'20: Proceedings of the 8th International Conference on Computer and Communications Management. 2020: 63-67.
- [53] WANG H X, SHU N N, WANG Y J, et al. Survey of software defined network and mutable network[C]//Proceedings of the International Conference on Communication and Electronic Information Engineering (CEIE 2016). 2017.
- [54] HUANG Y, GHOSH A K. Introducing diversity and uncertainty to create moving attack surfaces for Web services[R]. 2011.
- [55] TAO C, LV Y, QI Z, et al. An implementation method of zero-trust architecture[J]. Journal of Physics: Conference Series, 2020, 1651(1).
- [56] GARBIS J, CHAPMAN J W. Zero trust architectures[R]. 2021.
- [57] 秦中元, 胡爱群. 可信计算系统及其研究现状[J]. 计算机工程, 2006, 32(14): 111-113.
- QIN Z Y, HU A Q. Trusted computing system and its current research[J]. Computer Engineering, 2006, 32(14): 111-113.
- [58] 樊佩佩, 杨德义. 浅析计算机网络入侵检测中免疫机制的应用[J]. 科学技术创新, 2018(18): 69-70.
- FAN P P, YANG D Y. Analysis of the application of immune mechanism in computer network intrusion detection[J]. Scientific and Technological Innovation, 2018(18): 69-70.
- [59] 王亚奇, 蒋国平. 考虑网络流量的无标度网络病毒免疫策略研究[J]. 物理学报, 2011, 60(6): 6-13.
- WANG Y Q, JIANG G P. Epidemic immunization on scale-free networks with traffic flow[J]. Acta Physica Sinica, 2011, 60(6): 6-13.
- [60] 张楠, 张建华, 陈建英. WSN 中基于免疫 Multi-Agent 的入侵检测机制[J]. 计算机工程与科学, 2010, 32(5): 10-14.
- ZHANG N, ZHANG J H, CHEN J Y. An intrusion detection mechanism based on immune multi-agents in WSN[J]. Computer Engineering & Science, 2010, 32(5): 10-14.
- [61] 侯家利, 朱梅阶, 彭宏. 模块化免疫神经网络的模型研究[J]. 电子学报, 2005, 33(8): 1502-1505.
- HOU J L, ZHU M J, PENG H. Research on modular-based immune neural network model[J]. Acta Electronica Sinica, 2005, 33(8): 1502-1505.
- [62] 王祺鹏, 扈红超, 程国振. 一种基于拟态安全防御的 DNS 框架设计[J]. 电子学报, 2017, 45(11): 2705-2714.
- WANG Z P, HU H C, CHENG G Z. A DNS architecture based on mimic security defense[J]. Acta Electronica Sinica, 2017, 45(11): 2705-2714.
- [63] 张帆, 谢光伟, 郭威, 等. 基于拟态架构的内生安全云数据中心关键技术和实现方法[J]. 电信科学, 2021, 37(3): 39-48.
- ZHANG F, XIE G W, GUO W, et al. Key technologies and implementation methods of endogenous safety and security cloud data center based on mimic architecture[J]. Telecommunications Science, 2021, 37(3): 39-48.
- [64] 普黎明, 卫红权, 李星, 等. 面向云应用的拟态云服务架构[J]. 网络与信息安全学报, 2021, 7(1): 101-112.
- PU L M, WEI H Q, LI X, et al. Mimic cloud service architecture for cloud applications[J]. Chinese Journal of Network and Information Security, 2021, 7(1): 101-112.
- [65] 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. Router mimic defense architecture based on dynamic heterogeneous redundancy mechanism[J]. Journal of Information Security[J]. Journal of Cyber Security, 2017, 2(1): 29-42.
- [66] LARSEN P, HOMESCU A, BRUNTHALER S, et al. SoK: auto-

- mated software diversity[C]//Proceedings of 2014 IEEE Symposium on Security and Privacy. 2014: 276-291.
- [67] 姚东, 张铮, 张高斐, 等. 多变体执行安全防御技术研究综述[J]. 信息安全学报, 2020, 5(5): 77-94.
- YAO D, ZHANG Z, ZHANG G F, et al. A survey on multi-variant execution security defense technology[J]. Journal of Cyber Security, 2020, 5(5): 77-94.
- [68] 张铮, 李方云, 邬江兴, 等. 一种网络攻击防御方法及系统: CN110012038A[P]. 20190712.
- ZHANG Z, LI F Y, WU J X, et al. Network attack defense method and system: CN110012038A[P]. 20190712.
- [69] 信息处理装置及信息处理装置的控制方法: CN101963926A[P]. 2011-02-02.
- Information processing apparatus and control method of the information processing apparatus: CN101963926A[P]. 2011-02-02.
- [70] 马海龙, 江逸茗, 白冰, 等. 路由器拟态防御能力测试与分析[J]. 信息安全学报, 2017, 2(1): 43-53.
- MA H L, JIANG Y M, BAI B, et al. Tests and analyses for mimic defense ability of routers[J]. Journal of Cyber Security, 2017, 2(1): 43-53.
- [71] 王强, 姚磊, 李团营. 业务板间信息的同步方法、装置、存储介质及计算机设备: CN108093061A[P]. 2018-05-29.
- WANG Q, YAO L, LI T Y. Synchronization method and device of information between service boards, storage medium and computer equipment: CN108093061A[P]. 2018-05-29.
- [72] 崔冰萌, 倪明, 凌幸华. 基于 FPGA 的拟态服务器设计[J]. 计算机系统应用, 2018, 27(4): 219-225.
- CUI B M, NI M, LING X H. Design of mimicry computing server with FPGA[J]. Computer Systems & Applications, 2018, 27(4): 219-225.
- [73] LORCZAK P R, CAGLAYAN A K, ECKHARDT D E. A theoretical investigation of generalized voters for redundant systems[C]//Proceedings of the Nineteenth International Symposium on Fault-Tolerant Computing. Digest of Papers. 1989: 444-451.
- [74] BASS J M. Voting in real-time distributed computer control systems[D]. Sheffield, UK: The University of Sheffield. 1995.
- [75] KANEKAWAN, MAEJIMA H, KATO H, et al. Dependable on-board computer systems with a new method-stepwise negotiating voting[C]//Proceedings of the Nineteenth International Symposium on Fault-Tolerant Computing. Digest of Papers. Piscataway: IEEE Press, 1989: 13-19.
- [76] MOORE J S. A fast majority vote algorithm[J]. Springer Netherlands, 2000.
- [77] 周海涛, 朱纪洪. 基于自检测的多数一致表决算法[J]. 清华大学学报(自然科学版), 2005, 45(4): 488-491.
- ZHOU H T, ZHU J H. Majority voting algorithm based on self-test[J]. Journal of Tsinghua University (Science and Technology), 2005, 45(4): 488-491.
- [78] 俞功兵, 王俊峰. 基于自检测的自适应一致表决算法[J]. 电子设计工程, 2012, 20(21): 19-21.
- YU G B, WANG J F. Adaptive consensus voting algorithm based on self-test[J]. Electronic Design Engineering, 2012, 20(21): 19-21.
- [79] 欧阳城添, 王曦, 郑剑. 自适应一致表决算法[J]. 计算机科学, 2011, 38(7): 130-133.
- OUYANG C T, WANG X, ZHENG J. Adaptive consensus voting algorithm[J]. Computer Science, 2011, 38(7): 130-133.
- [80] 吴一凡, 冉晓旻. CNN 神经网络在航迹预测中的应用[J]. 电子设计工程, 2019, 27(12): 13-20.
- WU Y F, RAN X M. Application of CNN neural network in route forecasting[J]. Electronic Design Engineering, 2019, 27(12): 13-20.
- [81] KONG J, HUANG J, YU H, et al. RNN-based default logic for route planning in urban environments[J]. Neurocomputing, 2019, 338: 307-320.
- [82] BUSCH J, KOCHETUROV A, TRESP V, et al. NF-GNN: network flow graph neural networks for malware detection and classification[R]. 2021.
- [83] FU R, ZHANG Z, LI L. Using LSTM and GRU neural network methods for traffic flow prediction[C]//Proceedings of 2016 31st Youth Academic Annual Conference of Chinese Association of Automation (YAC). 2016: 324-328.
- [84] LIN C K, WILD A, CHINYA G N, et al. Programming spiking neural networks on intel's loihi[J]. Computer, 2018, 51(3): 52-61.
- [85] 宫学源. 英特尔发布神经拟态计算芯片, 可模拟人类大脑自主学习[J]. 科技中国, 2018.
- GONG X Y. Intel released a neuromorphic computing chip that can simulate the autonomous learning of the human brain[J]. Technology China, 2018.
- [86] MICHAUD F. EMIB-computational architecture based on emotion and motivation for intentional selection and configuration of behaviour-producing modules[J]. Clinical Advances in Hematology & Oncology, 2004.
- [87] PRASAD C, CHUGH S, GREVE H, et al. Silicon reliability characterization of intel's foveros 3D integration technology for logic-on-logic Die stacking[C]//Proceedings of 2020 IEEE International Reliability Physics Symposium. 2020: 1-5.
- [88] 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.
- [89] GUBBI J, BUYYA R, MARUSIC S, et al. Internet of things (IoT): a vision, architectural elements, and future directions[J]. Future Generation Computer Systems, 2013, 29(7): 1645-1660.
- [90] ZHANG Z K, CHO M C Y, WANG C W, et al. IoT security: ongoing challenges and research opportunities[C]//Proceedings of 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications. Piscataway: IEEE Press, 2014: 230-234.
- [91] 何意, 刘兴伟, 马宏亮. 车联网拟态防御系统研究[J]. 信息安全研究, 2020, 6(3): 244-251.

- HE Y, LIU X W, MA H L. Research on mimic defense system of Internet of vehicles[J]. Journal of Information Security Research, 2020, 6(3): 244-251.
- [92] 普黎明, 柏溢, 游伟, 等. 面向拟态云服务的异构执行体输出裁决方法[J]. 信息工程大学学报, 2020, 21(3): 344-351.
- PU L M, BAI Y, YOU W, et al. Heterogeneous executors output decision method for mimic cloud service[J]. Journal of Information Engineering University, 2020, 21(3): 344-351.
- [93] 陈福才, 周梦丽, 刘文彦, 等. 云环境下面向拟态防御的反馈控制方法[J]. 信息安全学报, 2021, 21(1): 49-56.
- CHEN F C, ZHOU M L, LIU W Y, et al. Feedback control method for mimic defense in cloud environment[J]. Netinfo Security, 2021, 21(1): 49-56.
- [94] 徐悦, 倪明, 余新胜, 等. 云环境下拟态应用行为预测方法研究[J]. 信息技术, 2021, 45(1): 53-59.
- XU Y, NI M, YU X S, et al. Research on prediction method of mimic application behavior in cloud environment[J]. Information Technology, 2021, 45(1): 53-59.
- [95] 于敏. 基于 ARIMA 的云资源编排优化[D]. 北京: 北京工业大学, 2019.
- YU M. ARIMA-based cloud resource orchestration optimization[D]. Beijing: Beijing University of Technology, 2019.
- [96] 赵双蕊, 闫弈棋, 韩晓丽. 基于云理论和 RBF 神经网络的预测模型[J]. 科学导报, 2016, (4): 255-256.
- ZHAO S R, YAN Y Q, HAN X L. Predictive model based on cloud theory and RBF neural network[J]. Science Herald, 2016, (4): 255-256.
- [97] GEORGE L. HBase-the definitive guide: random access to your planet-size data[C]//DBLP, 2011.
- [98] 黄方, 朱强, 李丽, 等. 一种基于 Web 框架的高性能地学计算服务系统: CN106371931B[P]. 2019-11-05.
- WANG F, ZHU Q, LI L, et al. A high-performance geoscience computing service system based on a Web framework: CN106-371931B[P]. 2019-11-05.
- [99] 顾青, 冯四风, 梁佐泉, 等. 大数据处理方法及其处理系统: CN110209631A[P]. 20190906.
- GU Q, FENG S F, LIANG Z Q, et al. Big data processing method and system: CN110209631A[P]. 20190906.
- [100] 李斌, 周清雷, 斯雪明, 等. 基于拟态计算的大数据高效能平台设计方法[J]. 计算机应用研究, 2019, 36(7): 2059-2064.
- LI B, ZHOU Q L, SI X M, et al. Design method of big data high-efficiency platform based on mimic computing[J]. Application Research of Computers, 2019, 36(7): 2059-2064.
- [101] 龙虎, 彭志勇. 基于拟态计算的大数据精准服务架构研究[J]. 信息与电脑(理论版), 2020, 32(5): 147-149.
- LONG H, PENG Z Y. Research on big data précis eservice architecture based on mimic computer[J]. China Computer & Communication, 2020, 32(5): 147-149.
- [102] 龙虎, 王振龙, 杨建菊. 基于拟态计算的高效能大数据应用平台构建研究[J]. 电脑知识与技术, 2021, 17(1): 36-37, 40.
- LONG H, WANG Z L, YANG J J. Research on the construction of high performance big data application platform based on mimic computing[J]. Computer Knowledge and Technology, 2021, 17(1): 36-37, 40.
- [103] BRISCOE B. Network functions virtualisation(NFV)[M]//Security Problem Statement. 2014.
- [104] 黄前森. 基于拟态防御的 SDN 服务路径配置及其验证机制研究[D]. 杭州: 浙江工商大学.
- HUANG Q M. Research on SDN service path configuration and verification mechanism based on mimic defense[D]. Hangzhou: Zhejiang Gongshang University.
- [105] 丁绍虎, 李军飞, 季新生. 基于拟态防御的 SDN 控制层安全机制研究[J]. 信息安全学报, 2019, 4(4): 84-93.
- DING S H, LI J F, JI X S. Research on SDN control layer security based on mimic defense[J]. Journal of Cyber Security, 2019, 4(4): 84-93.
- [106] 吕迎迎. 拟态 SDN 控制器架构安全关键技术研究[D]. 郑州: 信息工程大学, 2018.
- LYU Y Y. Research on the key technologies of mimic SDN controller architecture security[D]. Zhengzhou: Information Engineering University, 2018.
- [107] 高洁, 郭江兴, 李军飞, 等. 拟态化 SDN 控制层裁决机制研究[J]. 信息工程大学学报, 2018, 19(6): 641-646.
- GAO J, WU J X, LI J F, et al. Research on the arbitrament mechanism in the mimic SDN control layer[J]. Journal of Information Engineering University, 2018, 19(6): 641-646.
- [108] 雷波, 赵倩颖, 赵慧玲. 边缘计算与算力网络综述[J]. 中兴通讯技术, 2021, 27(3): 3-6.
- LEI B, ZHAO Q Y, ZHAO H L. Overview of edge computing and computing power network[J]. ZTE Technology Journal, 2021, 27(3): 3-6.
- [109] 梁启锋. 边缘计算安全威胁现状及防护技术分析[J]. 网络安全技术与应用, 2020(4): 9-10.
- LIANG Q F. The current situation of edge computing security threats and analysis of protection technology[J]. Network Security Technology and Application, 2020(4): 9-10.
- [110] 朱泓艺, 陆肖元, 李毅. 基于拟态防御原理的分布式多接入边缘计算研究[J]. 物联网学报, 2019, 3(3): 76-83.
- ZHU H Y, LU X Y, LI Y. Research on distributed multi-access edge computing based on mimic defense theory[J]. Chinese Journal on Internet of Things, 2019, 3(3): 76-83.
- [111] DELMOLINO K, ARNETT M, KOSBA A, et al. Step by step towards creating a safe smart contract: lessons and insights from a crypto currency lab[M]//Financial Cryptography and Data Security. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016: 79-94.
- [112] SAPIRSHTAIN A, SOMPOLINSKY Y, ZOHAR A. Optimal selfish mining strategies in bitcoin[M]//Financial Cryptography and Data Security. Berlin, Heidelberg: Springer Berlin Heidelberg, 2017:

515-532.

[113]徐蜜雪,苑超,王永娟,等.拟态区块链:区块链安全解决方案[J].软件学报,2019,30(6):1681-1691.

XUM X, YUAN C, WANGY J, et al. Mimic blockchain—solution to the security of blockchain[J]. Journal of Software, 2019, 30(6): 1681-1691



胡涛(1993-),男,陕西武功人,信息工程大学助理研究员,主要研究方向为新型网络体系结构,网络主动防御。

[作者简介]



马海龙(1980-),男,山东沂水人,信息工程大学副研究员,主要研究方向为网络空间内生安全、网络威胁智能感知及新型网络体系。



江逸茗(1984-),男,江苏南通人,信息工程大学副研究员,主要研究方向为网络安全、新型网络体系研究。



王亮(1995-),男,河南唐河人,信息工程大学助理工程师,主要研究方向为网络主动防御。



曲彦泽(1998-),山东烟台人,信息工程大学硕士生,主要研究方向为网络威胁感知。