网络空间拟态防御综述

李炳萱[1], 陈世展[2], 许光全[2], 贾云刚[3], 王 聪[2], 薛 飞[4],
王 晓[2,5], 王 伟[6], 李哲涛[7], 李建欣[8]

[1]天津大学国际工程师学院 天津 中国 300350
[2]天津大学智能与计算学部 天津 中国 300350
[3]国家计算机网络应急技术处理协调中心天津分中心 天津 中国 300100
[4]国网宁夏电力有限公司电力科学研究院 银川 中国 750001
[5]广东省安全智能新技术重点实验室 深圳 中国 518000
[6]北京交通大学计算机与信息技术学院 北京 中国 100044
[7]暨南大学信息科学技术学院 广州 中国 510632
[8]北京航空航天大学计算机学院 北京 中国 100191

摘要 随着网络技术的不断发展, 网络空间已经成为人们工作和个人生活中的重要组成部分。然而, 对网络空间的日益依赖也带来了一系列安全挑战, 数字领域的互联性质使其容易受到黑客攻击、数据泄露、身份盗窃等网络威胁, 确保网络空间安全已成为当务之急。为保障网络空间安全, 邬江兴院士基于拟态架构计算理论提出了网络空间拟态防御(Cyber Mimic Defense, CMD)理论体系, 这一开创性理念旨在改变长期困扰网络空间“易攻难守”困境的安全格局, 其内生安全效应彻底改变了拟态防御系统的防御能力, 使其能够有效应对未知的安全威胁。自概念提出以来, 众多学者致力于研究和推进网络空间拟态防御思想的概念框架和实际应用, 并通过严格的建模评估对其原理进行了充分验证。本文对网络空间拟态防御相关研究展开全面概述, 首先回顾了拟态防御思想的核心内涵; 接着详细介绍了应用场景、架构研究和建模评估三个维度的工作方法和显著成果; 最后, 分析了网络空间拟态防御技术面临的挑战, 并展望了未来发展方向和研究重点。通过总结该领域的研究工作与进展, 本文有助于推进网络空间安全战略的持续努力, 为从业者和研究人员提供宝贵参考。本文提供的全面概述旨在激发网络空间拟态防御领域的进一步探索和创新, 不断增强网络空间面对持续不断的网络威胁所具有的安全性能。

关键词 网络空间拟态防御; 动态异构冗余架构; 主动防御; 内生安全; 网络安全
中图法分类号 TP393.08 **DOI 号** 10.19363/J.cnki.cn10-1380/tn.2025.05.06

A Review of Cyberspace Mimic Defense Research

LI Bingxuan[1], CHEN Shizhan[2], XU Guangquan[2], JIA Yungang[3], WANG Cong[2],
XUE Fei[4], WANG Xiao[2,5], WANG Wei[6], LI Zhetao[7], LI Jianxin[8]

[1] Tianjin International Engineering Institute, Tianjin University, Tianjin 300350, China
[2] College of Intelligence and Computing, Tianjin University, Tianjin 300350, China
[3] Tianjin Branch of the National Computer Network Emergency Technology Handling and Coordination Center, Tianjin 300100, China
[4] Electric Power Research Institute of State Grid Ningxia Electric Power Co., Ltd, Yinchuan 750001, China
[5] Guangdong Provincial Key Laboratory of Novel Security Intelligence Technologies, Shenzhen 518000, China
[6]School of Computer and Information Technology, Beijing Jiaotong University, Beijing 100044, China
[7] College of Information Science and Technology, Jinan University, Guangzhou 510632, China
[8] School of Computer Science and Technology, Beihang University, Beijing 100191, China

Abstract With the continuous development of network technology, cyberspace has become an integral and pervasive aspect of people’s work and personal lives. However, the increasing dependence on cyberspace has also brought a series of security challenges. The interconnected nature of the digital field makes it vulnerable to cyber threats such as hacker attacks, data leaks, and identity theft. Ensuring cyberspace security has become a top priority. To address this pressing need, Academician Wu Jiangxing proposed the theoretical system of Cyberspace Mimic Defense (CMD) based on the theory of Mimic Structure Calculation(MSC). CMD aims to transform the security landscape of cyberspace, which has long been plagued by the predicament of being “easy to attack but difficult to defend” Its endogenous security mechanisms have

通讯作者: 许光全, 博士, 教授, Email: losin@tju.edu.cn
本课题得到国家重点研发计划(No. 2022YFB3102100), 国家自然科学基金项目(No. U22B202、No. 62172297、No. 62102262、No. 61902276、No. 62272311), 天津市智能制造专项资金(No. 20211097), 天津自然科学基金面上项目(No. 22JCYBJC01550), 广东省安全智能新技术重点实验室项目(No. 2022B1212010005), 广西科技计划项目(No. AD23026096)资助。
收稿日期: 2023-07-05; 修改日期: 2023-10-23; 定稿日期: 2025-04-14

revolutionized the capabilities of the mimic defense system, enabling it to effectively counter unknown security threats. Since the introduction of this concept, numerous scholars have conducted extensive research on the conceptual framework and practical implementation of cyberspace mimic defense, duly substantiating its principles through rigorous modeling and evaluation. This paper provides a comprehensive overview of research on Cyberspace Mimic Defense. First, it reviews the core connotation of mimic defense thought. It introduces the working methods and remarkable achievements in the dimensions of application scenarios, architecture research, and modeling evaluation. Furthermore, the paper analyzes the challenges faced by Cyberspace Mimic Defense technology, and provides an outlook on future development directions and research priorities in the field of Cyberspace Mimic Defense. By summarizing the research work and progress in this field, this paper contributes to the advancement of secure cyberspace strategies. It serves as a valuable reference for practitioners and researchers alike, providing insights into the principles, methodologies, and achievements of Cyberspace Mimic Defense. The comprehensive overview offered in this article aims to stimulate further exploration, innovation, and collaboration in the field, ultimately enhancing the resilience and security of cyberspace in the face of evolving cyber threats.

Key words cyber mimic defense; dynamic heterogeneous redundancy; active defense; endogenous safety and security; cybersecurity

1 引言

当今, 人类社会正大踏步迈入数字经济时代, 网络空间安全的重要性不断攀升。但由于软硬件设计缺陷无法避免、后门问题无法杜绝、网络攻击成本相对较低等原因, 网络空间的内源安全问题无处不在, 网络安全威胁无所不及。

传统网络安全框架模型, 如防火墙技术、加解密技术、访问控制技术, 入侵检测、日志审查, 蜜罐和密网技术等, 重在对目标系统的安全加固以及对已知威胁的识别和消除, 存在着无法避免后门植入、防御检测能力固定、单个安全组件所感知的信息有限等问题, 因而难以应对基于目标对象内生安全问题的未知攻击。

目前, 力图“改变游戏规则”的新型防御手段成为新的研究热点。可信计算技术通过基于信任根的信任链机制保证信息系统的安全性能, 但存在着兼容性差、防外而不能防内等安全问题; 区块链技术通过融合现代密码学、分布式架构、智能合约等理论, 解决了中心化模式安全性低、可靠性差等问题, 但面临着算法实现难、共识机制设计不当等安全挑战; 移动目标防御技术采取不断变化的、多样的策略极大增加了攻击者的攻击难度, 但对目标系统的性能存在一定的影响, 且难以防御未知的风险。2013 年, 邬江兴院士针对当前网络空间“易攻难守”的安全态势, 提出网络空间拟态防御思想[1], 其核心是实现基于网络空间内生安全机理的动态异构冗余架构(Dynamic Heterogeneous Redundancy, DHR), 从“构造决定安全”公理中寻求破解安全问题之路, 从而有效应对未知漏洞后门、病毒木马等不确定威胁。

类似于生物界的拟态防御, CMD 的基本思想是在保证服务功能和性能等价的前提下, 通过环境、硬件、软件、数据等结构组件的主动变换或快速迁移, 来实现一个动态、异构、非确定、不持续的环境, 从而增加攻击者的观察及预测难度, 进而使攻击成功的难度和成本增倍。邬江兴院士将 CMD 理论的核心内涵简单归纳为五个“一”:

1) 一个公理。每个人都存在着自身的缺点, 但在独立完成一个同样的任务时, 大多数人在同一时间、同一地点犯完全同样的错误的情形是极少出现的。给定一个功能与性能的目标, 往往有多种不同的实现方法, 同时这些实现方法的并集或者交集仍然能够达到功能与等价性能要求。因而在网络空间中, 具有不同后门、漏洞的异构执行体在同一时间发生共同错误的概率极低, 加上表决算法, 使得 CMD 系统防御未知风险成为可能。

2) 一种架构。CMD 思想是基于 DHR 的一体化技术架构实现的, 这种架构以攻击者无法预知的方式不规则的移动攻击表面, 使得攻击者的可用资源无论是在时间上还是空间上都具有极强的不确定性。尤其是一些需要多步传输数据包的攻击任务, 尤其难以完成。

3) 一种运行机制。即在“去协同化”条件下的多模表决和多维动态重构机制, 这种机制在一方面能够把复杂系统中攻击表面具有高难度、高代价特点的工程代价问题, 转变成为空间上独立、功能简单的“拟态括号”之软硬件攻击表面的缩小问题。另一方面, 能够使异构冗余体之间可能存在的关联性降到最低, 给攻击者造成非配合条件下的异构多目标动态协同攻击困境。

4) 一个思想。CMD 思想基于“移动攻击表面”思想, 该思想使得攻击表面的展现具有不确定性, 影响攻击者无法摸清系统运行的模式与规律, 干扰或中断攻击者与系统内部建立稳定的联系, 使攻击者的恶意行为无法稳定实施。

5) 一种非线性安全增益。现有的加密认证、防火墙、查毒杀毒、木马清除等攻击检测、隔离、预

防和清除措施, 在机理上无依赖关系, 漏洞修补、封堵后门或是恶意代码清除等传统的增量修补手段也只能作为攻击后的补充措施。而 CMD 思想则是纯粹通过架构内生机理获得的拟态防御增益, 将这些防御技术与 CMD 思想融合使用的系统, 能够在防御能力上获得非线性的增益。

目前, CMD 的相关理论研究与实践均处于快速发展阶段, 相关问题尚未形成统一的认识。本文将主要围绕 CMD 关键技术, 对目前相关研究进行综述, 本文剩余部分的组织如下:

在本文第 2 至 4 节分别就应用场景、架构研究、建模评估等三个方面, 梳理了现有围绕 CMD 思想的关键工作。总结为如图 1 所示的网络空间拟态防御技术研究框架图。在本文第 5 节, 全面探讨了 CMD 技术目前面临的挑战, 并在此基础上对未来的研究方向进行展望。

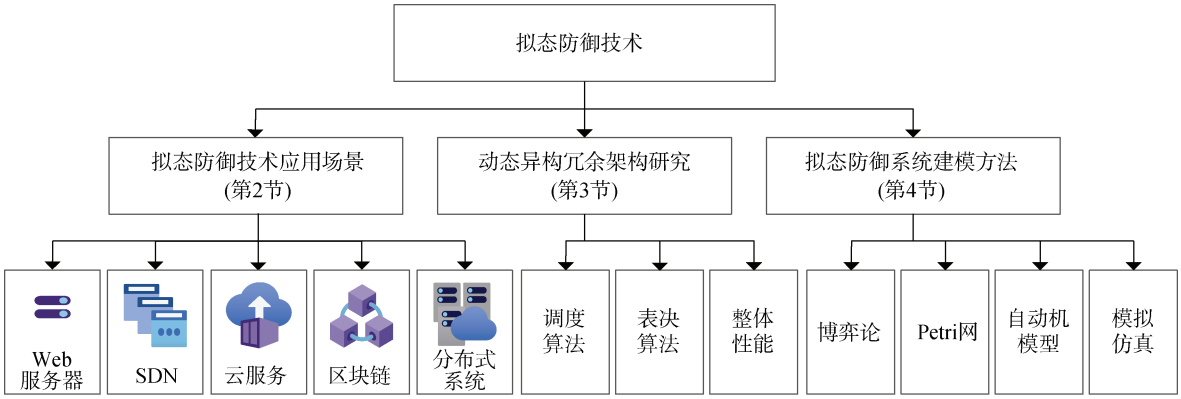

图 1　拟态防御技术研究框架

Figure 1　Research framework for Cyber Mimic Defense technology

2　拟态防御思想的应用

CMD 思想本身的设计并不依赖于特定的网络或信息系统, 因而其基本原理具有通用性。更重要的是, CMD 思想作为一种具有主动性的安全策略, 通过时空变化来干扰攻击者的观察和攻击链的构成, 能够有效增加攻击者的攻击成本和攻击难度。这种主动性作为拟态防御的核心特点, 使其在应对未知的威胁和漏洞时更具优势。因此, 对于目前采用静态的、被动的防御模式的网络信息系统架构, 将 CMD 思想引入其中, 不仅具有合理的充分性, 还显得十分必要。

影响网络信息系统安全性的要素包括硬件要素、操作系统要素、网络通信要素、应用软件要素、数据要素、用户和管理员要素、安全策略要素等。为方便讨论, 可将能够引入 CMD 思想的不同要素归纳为网络层、平台层、环境层、应用层和数据层五个层次。其中, 网络层包括网络地址、网络协议、网络端口等, 这些要素构成了信息系统的通信基础, 影响着数据的传输和交换; 平台层包括服务器、处理器架构、存储设备等负责信息的物理存储和传输的硬件元素, 以及操作系统、虚拟机等支持性软件要素; 环境层包括平台与上层应用的接口, 如指令集、地址空间等; 应用要素则包括不同软件执行体、程序指令序列、指令格式、内部数据等; 数据要素包括数据的形式、句法和编码等。将不同的要素进行拟态化改造, 可获得不同的安全效果, 也需考虑可能引入的问题, 本文将各层拟态构造策略的优缺点整理如表 1。在为不同的架构系统引入 CMD 思想时, 可综合考虑系统的具体需求和威胁情境, 按需选择不同的要素, 或是组合多个要素, 在系统内部构造拟态括号结构, 以保障网络信息系统的安全性。

CMD 思想的主要应用场景有 Web 架构、软件定义网络框架、云环境、区块链以及大数据下的分布式存储系统五个方向, 下面就分别介绍其具体的应用对象以及相应的异构方案。

2.1　在 Web 架构中的应用

Web 架构定义了 Web 应用程序的基本组成部分和交互方式, 通常包括客户端、Web 服务器、应用服务器、数据库服务器等要素, 这些要素协同工作, 使用户能够通过浏览器与 Web 应用程序进行交互, 获取信息或执行操作。但其面临着数据泄露、跨站点脚本攻击、跨站点请求伪造、SQL 注入等一系列潜在的安全漏洞。而引入 CMD 技术能够提高 Web 框架的安全性, 保护 Web 应用和用户的敏感信息, 确保其在不断变化的网络环境中保持安全。下将相关工作整理如表 2。

在针对 Web 服务器系统的改造方面, 文献[2]首先提出了基于 DHR 架构的拟态 Web 服务器模型, 其

表 1 网络信息系统的关键要素异构方案

Table 1 Heterogeneous approach to key elements of network information systems

层次	要素的异构方案	优点	可能出现的问题
网络层	改变目标系统的 IP 地址 改变目标系统使用的协议 改变目标系统的端口	可用于对抗各种网络攻击; 可对整个系统的通信和连接进行全面性保护; 可在攻击进一步深入系统之前拦截攻击; 可在不同的信息系统中使用相似的网络层拟态防御策略	可能影响网络的配置、管理和维护; 可能引入额外的性能开销; 可能导致网络延迟增加, 影响实时性能; 可能局限于特定的网络架构
平台层	切换硬件设备 改变操作系统 改变虚拟机实例 改变存储系统	可在不同的硬件平台上实施; 可实现资源隔离, 确保不同的应用程序或虚拟机之间的安全性; 可在攻击进一步深入系统之前拦截攻击	可能引入额外的硬件成本, 可能引入操作系统的兼容性和稳定性问题, 可能导致处理器、虚拟机性能降低、影响存储的读写速度
环境层	指令集随机化 地址空间随机化	可在各种信息系统中使用, 而无需大规模修改应用程序代码; 可保护系统的核心组件	需要考虑应用程序的兼容性问题, 可能会造成指令执行的延迟, 影响运行效率
应用层	切换应用软件变体 改变指令序列和形式 改变存储资源分配方案	可增加应用软件的动态性, 应对定向攻击, 降低攻击成功率; 可用于各种信息系统, 而不需要大规模的系统改造	可能导致软件的复杂性增加, 需要更多的开发和测试工作, 可能影响开发周期
数据层	改变数据的形式 改变数据的句法 改变数据的编码	可阻碍攻击者对数据进行挖掘和分析, 降低敏感信息的泄露风险, 有效保护存储在信息系统中的数据; 可应用在各种信息系统中	可能会对数据的读取和写入性能产生影响; 可能引入数据不一致性风险与兼容性问题; 增加数据管理的复杂性

表 2 CMD 技术在 Web 架构中的应用

Table 2 Application of CMD technology in web architecture

研究方案	异构层次					异构组件
	网络层	平台层	环境层	应用层	数据层	
拟态 Web 服务器[2]		√		√	√	操作系统+服务器软件+sql 脚本+文件
拟态构造 Web 系统[3]		√		√		硬件设备+物理机操作系统+虚拟化软件+虚拟机操作系统+服务软件
拟态 Web 应用安全框架[4]				√		随机化服务端
拟态 Web 防御体系[5]		√		√		操作系统+文件系统+服务器软件+执行脚本

能够在较小开销的前提下防御测试中的全部攻击类型, 说明拟态防御 Web 服务器能够有效地提升系统安全性, 验证了 CMD 技术的有效性和可行性。文献[3]基于 DHR 架构设计了新的拟态构造 Web 系统。文献[4]实现了拟态 Web 应用安全框架, 将部署了其改进防御架构的服务端抽象为随机化服务端, 构建等价异构冗余的随机化服务端执行体。这三者所提出的系统的区别在于, 文献[2]所提系统是在服务器内部, 分别构建物理操作系统、虚拟化、服务器软件、应用脚本和数据的等价异构冗余体; 工作[3]是对整 Web 服务器系统的改造, 构建多个等价异构的子网, 而文献[4]所提出的系统是构建异构冗余的服务器。此外, 文献[5]设计了拟态 Web 系统防御体系, 并在江苏电信 Web 防护系统进行了实践, 取得了较好防护效果。

2.2 在软件定义网络中的应用

软件定义网络 (Software Defined Network, SDN) 是一种新兴的网络架构, 它的核心思想是将网络控制平面(控制器)与数据转发平面(交换机/路由器)分离, 通过中央控制器集中管理和配置网络流量。和许多新兴技术一样, SDN 同样面临着诸多安全威胁, 例如控制器攻击、DDoS 攻击、流表规则注入攻击等, 引入 CMD 技术有助于提高 SDN 网络的安全性, 保护网络资源和数据的完整性, 确保网络正常运行。下将相关工作整理如表 3。

文献[6-7]分别针对 SDN 控制层面的安全问题, 提出拟态网络操作系统, 构建异构冗余的网络操作系统执行体, 但这两个系统还不适用于大规模的、复杂的网络环境, 同时还会造成一定的网络时延问题。文献[8-12]分别针对 SDN 控制器面临的漏洞与后门等安全威胁, 提出将 DHR 架构引入到 SDN 控制器系统中, 构建控制器的异构冗余体以及调度器等核心组件。但也带来了一定的资源开销与性能问题。文献[13]提出构建多个异构的主控制器, 共同处理数据层的 OpenFlow 请求。但其实现的原型系统自身的可靠性仍存在着例如崩溃、断接、疏漏响应等问题, 又构成了系统新的安全薄弱点。文献[14]提出一种基于 CMD 的 SDN 服务部署架构, 提出异构度保证的调度

表 3 CMD 技术在 SDN 架构中的应用

Table 3 Application of CMD technology in SDN architecture

研究方案	异构层次					异构组件
	网络层	平台层	环境层	应用层	数据层	
拟态网络操作系统[6,7]		√				网络操作系统
拟态 SDN 控制器[8-13,15]		√				SDN 控制器
拟态 SDN 控制器[14]		√				网络功能虚拟化编排器+SDN 控制器+操作系统
拟态 SDN 控制器[16]		√		√		处理器+SDN 控制器+操作系统+应用程序

机制以及 MD5 加密的判决机制。文献[15]针对 SDN 集中式管控的独裁特性可能会带来的问题, 提出一种基于 CMD 的 SDN 控制层安全机制, 在控制层和数据层之间加入代理, 同时在控制层部署多个异构的等价控制器用于监督主控制器。实验结果验证了该监督机制的有效性, 能及时准确检测出主控制器的恶意行为。文献[16]提出了一种面向 SDN 的拟态化架构, 该架构将应用程序、SDN 控制器、操作系统以及处理器置于拟态界内。

2.3 在云环境下的应用

云环境是一种基于互联网的计算模型, 允许用户通过网络访问和共享计算资源, 如服务器、存储、数据库等, 以便满足各种应用和服务需求。其虽然提供了强大的计算和存储能力, 但也伴随着虚拟化漏洞、数据隐私问题、身份验证与授权问题等一系列潜在的安全挑战。CMD 技术的引入可以帮助加强云环境的安全性, 保护用户的数据和资源免受各种威胁。下将相关工作整理如表 4。

表 4 CMD 技术在云环境中的应用

Table 4 Application of CMD technology in cloud environment

研究方案	异构层次					异构组件
	网络层	平台层	环境层	应用层	数据层	
拟态数据存储系统[17-19]		√				数据块
拟态云科学工作流系统[20-21]		√				虚拟机
拟态 SaaS 云内生安全系统[22]		√				容器组
拟态 SaaS 虚拟网络映射方法[23]		√				拟态服务功能链模型
拟态云服务系统[24-25]		√				云服务虚拟节点[24]; 执行虚拟机[25]

针对云存储系统, 文献[17]针对由于静态的存储架构和存储模式而带来的安全威胁, 提出了一种基于再生码的拟态存储方案。该方案利用网络编码方案将数据存储在云端数据节点上, 采用一种基于再生码的拟态变换机制, 可根据随机时变因素动态地改变数据的存储状态, 并能够持续保证数据的完整性和可用性。但该方法中运用到的一种随机性的启发式算法, 不能完全保证多项式时间复杂度。文献[18]同样提出了一种基于再生码的拟态存储机制, 通过对数据进行编码存储, 并在云端进行拟态变换, 增加攻击者获得数据的难度和成本。文献[19]提出一种自适应的 DHR 结构的云存储数据拟态防御架构, 由云存储服务器池和选调器构成, 其中云存储服务器池则由多层不同的异构体组成的服务器构成。

文献[20]为实现云科学工作流任务的入侵容忍, 提出基于 CMD 的云科学工作流系统。利用操作系统间的共同漏洞数量对虚拟机的异构度进行量化。周期性地回收和产生新的虚拟机, 消除潜伏的威胁, 保证科学工作流执行环境的纯净。文献[21]为加强云工作流的安全性, 提出了一种用于科学工作流的模拟云计算任务执行系统, 该系统能够有效增强云工作流执行的可靠性和可信度。文献[22]提出一种拟态化网络即服务(Software As A Service, SaaS)云内生安全系统架构。通过丰富拟态 SaaS 的异构性以避免冗余组件的共同脆弱点所引发的共模或同态安全问题; 结合网络欺骗、移动目标防御等机制对容器进行拟态伪装, 使得攻击者无法持续锁定攻击目标, 难以维持对攻击成功的持续控制和访问。但并没有考虑影子容器被攻击导致的服务终端信息泄露等方面的损失。文献[23]结合当前基于云网融合 SaaS 交付模式的特点, 提出一种面向 SaaS 安全的虚拟网络映射方法, 将基于 CMD 的组合服务模式建模为一个整数线性规划问题。文献[24]提出一种拟态云服务架构, 把云服务节点改造为拟态服务包, 以拟态服务包的模式向用户提供原节点的服务。其中的虚拟服务节点可以是服务虚拟机或容器, 也可以是物

理机。文献[25]针对云环境中虚拟机单一性、静态性等问题, 基于 CMD 技术设计了一个反馈控制方法, 对虚拟机进行拟态封装, 并针对这种架构设计了新的动态调度算法, 有效增加了云环境服务的安全性。

2.4 在区块链系统中的应用

区块链是一种分布式账本技术, 它通过去中心化的方式, 将交易数据以区块的形式连接起来, 形成一个不可篡改的链式结构。然而, 尽管区块链自身具有高度的安全性, 仍存在包括智能合约漏洞、51%攻击、私钥泄露等安全漏洞和威胁。为此, 已有研究工作将 CMD 技术引入区块链体系架构, 以保护用户的资产和数据, 提高整体区块链系统的安全性。下将相关工作整理如表 5。

文献[26]针对区块链的安全问题, 考虑区块链未来可能面临的隐私泄露风险和安全威胁。基于 CMD 思想, 提出了以拟态智能合约、拟态签名算法和拟态共识机制为核心的拟态区块链方案。文献[27]则设计了动态、异构的共识机制和动态、异构、冗余的签名机制, 从而搭建了拟态区块链架构。文献[28]提出了以拟态链码和拟态系统背书链码为核心的 Hyperledger Fabric 项目拟态区块链方案。但其给出的区块链安全保护方案效率相对较低, 且没有构造完整的区块链系统。

表 5 CMD 技术在区块链架构中的应用

Table 5 Application of CMD technology in blockchain architecture

研究方案	异构层次					异构组件
	网络层	平台层	环境层	应用层	数据层	
拟态区块链[26]		√		√		智能合约+签名算法+共识过程
拟态区块链[27]		√		√		签名算法+共识过程
拟态 Fabric 方案[28]				√		用户链码+系统背书链码[28]

值得一提的是, 对于区块链系统中的关键要素, 由于签名算法的功能是用于验证数据发送者的合法性, 以及数据的完整性, 而智能合约被用于在区块链平台执行特定的合同规则, 这两者都涉及到数据的处理和业务逻辑的执行, 因而将其映射到应用层。在 Fabric 中, 链码是访问账本的基本方法, 通常用于处理业务逻辑, 与智能合约类似, 因此也将其映射到应用层。对于共识机制, 由于其并不涉及具体的业务逻辑, 而是更多关注节点之间如何达成共识以验证和记录交易, 因而映射到平台层。

2.5 在分布式存储系统中的应用

分布式存储系统是一种设计用于存储和管理大规模数据的计算机系统, 它将数据分布在多个服务器或节点上, 以提高数据的可靠性、可扩展性和性能。针对数据泄露、数据损坏、拒绝服务攻击等漏洞, 以及数据完整性问题、数据窃听等安全威胁, 引入 CMD 思想同样能够帮助分布式存储系统主动防御, 大幅增加攻击难度。下将相关工作整理如表 6。

表 6 CMD 技术在分布式存储系统中的应用

Table 6 Application of CMD Technology in Distributed Storage System

研究方案	异构层次					异构组件
	网络层	平台层	环境层	应用层	数据层	
拟态防御分布式架构[29]		√				编码解码执行单元
拟态分布式文件系统[30]		√				分布式存储系统
拟态分布式存储模型[31]					√	纠删码
拟态 Ceph[32]			√	√	√	元数据+数据存储+数据校验+加密客户端
拟态 HDFS[33-35]		√				Namenode

文献[29]为解决分布式存储系统的安全风险, 提出了一种基于 DHR 架构的存储系统拟态防御架构, 增加了攻击者对系统进行攻击的成本。同时, 该团队提出一种基于 CMD 理论的分布式文件系统架构[30], 系统中构建了动态配置管理和异构功能模块, 事务的并行操作和多模式决策增强了不确定性, 但延长了响应时间。随后, 该团队又提出一种基于 CMD 和多纠删码的分布式对象存储框架[31], 通过增加系统的不确定性, 使系统漏洞和后门难以被利用和触发, 有效提高了分布式存储系统的安全性。

Ceph 和 HDFS 是两种主流的大型分布式存储解决方案。文献[32]就结合 Ceph, 提出了一种面向拟态

增强的分布式存储全新架构, 在元数据拟态化增强、数据存储拟态化增强、数据校验拟态化增强、客户端拟态化加密等方面进行了深入研究。但该拟态分布式存储系统只支持 Ceph 文件存储接口, 并没有统一考虑块、对象存储接口, 且实验环境较为简单。文献[33]则结合拟态思想并利用 Nginx 的反向代理技术对 HDFS 架构做出了调整改进。文献[34-35]为应对分布式存储系统的安全威胁, 提出将 DHR 架构引入到 HDFS 中, 设计面向元数据服务的拟态化架构, 将 HDR 模型应用到 Namenode 结构, 同时对 Datanode 集群异构化。

2.6 其他应用

CMD 思想的应用十分广泛, 除了以上几个研究热点, 其还可以应用到边缘计算网络中, 构建分布式多接入边缘计算的拟态防御架构[36]、边缘计算网络中数据传输的主动防御框架[37]、边缘计算终端拟态防御模型[38]等。

一些研究者还将 CMD 思想与传统的计算机与网络概念架构进行结合, 形成了路由器的DHR实现架构[39-40]、域间路由系统拓扑动态变换的防护方法[41]、拟态域名服务器架构[42]、拟态数据安全架构[43-44]和基于 CMD 的文件保护方法[45]、拟态数据库[46]、基于 CMD 理论的交换机内生安全体系架构[47]、拟态进程执行方法[48]等。

在实际的应用场景中, CMD 思想还可以被引入到工业控制网络[16,49-50]、天地网络架构[51]、政务网络[52]、政府门户网站[53]、全舰计算环境体系架构[54]、企业内网[55]、智能电网[56]、电力 Web 系统[57]、电力监控系统[58]、管理信息系统[59]、光传输系统[60]、车联网系统[61]、无人机飞控架构[62]等系统中。

除此之外, 有研究者将 CMD 思想与软件多样化技术[63]、基于混淆技术实现的程序多样化思想[64]、支持高效密文密钥同步演化的安全数据共享方案[65]、基于贝叶斯网络的攻击[66]、零信任安全架构[67]等相结合。或是引入到软件水印技术[68]、5G 网络[69]、MSISDN 号码[70]、QR 码[71-73]、M2M 直接认证方案[74]、传统蜜罐技术[75-76]、网络异常流量检测技术[77]中。再或者提出新的基于 GTP 协议的“动态隧道”防御方法[78]、基于 CMD 的零日攻击检测和响应框架[79]、拟态网络安全加密系统[80]、拟态通用运行环境框架[81]、网络多媒体数据安全的拟态加密盒[82]、元数据再同步方法[83]、基于红蓝对抗的拟态防御体系[84]、深度伪造语音检测系统[85]等。还有研究者论述了拟态防御系统下如何进行漏洞检测[86]等。

本节按照应用场景的不同, 整理了 CMD 思想在各方面的应用。总结来说, CDM 思想的应用场景十分广泛。DHR 机制能够为各个领域中的现有架构提供更强的安全保障, 针对网络攻击行为而言, 系统动态、异构、冗余程度越高, 攻击成功的难度越大, 即系统相对越安全。但 CDM 思想的引入在增强系统安全性的同时, 也不可避免的带来了资源开销与性能损失的问题。如何找到安全与性能的平衡, 是在为网络信息系统引入 CMD 思想时需要思考的关键问题。

3 DHR 架构研究

DHR 架构作为 CMD 技术的核心, 是实现 CMD 思想的基础构造。研究 CMD 思想, 始终无法脱离研究 DHR 架构的整体框架和关键要素。调度算法和表决机制作为 DHR 架构实现的核心组成部分, 其效果关乎拟态网络信息系统的安全与性能。下面就分别介绍围绕这两个关键要素的相关进展, 然后介绍已有工作针对 DHR 架构的其他研究。

3.1 拟态防御系统的调度算法研究

调度算法作为实现 CMD 思想的关键一环, 负责根据历史信息和负反馈内容有选择的更换执行体集, 实现执行体的替换、下线等操作, 使系统呈现不可预测的特性。

拟态调度算法主要从动态、异构、冗余三方面特性出发, 实现拟态系统的高稳健性和安全性, 这些特性在调度算法里可体现在调度对象(体现异构性)、调度时机(体现动态性)、调度数量(体现冗余性)三方面策略中:

调度对象的选择是指在调度方案初始化或更新时, 以怎样的标准筛选异构体进入执行体集。最基础的随机算法由于可能出现的共同漏洞等问题, 已逐渐被抛弃。现有的研究工作在选择执行体时, 主要根据异构程度进行筛选, 以降低执行体存在共有漏洞的可能性。也有部分工作选择依据在线的执行体被探测或攻击的次数等进行筛选。在对异构程度的度量上, 分为基于异构体异构度度量、基于组件异构度度量两种。其中, 基于异构体异构度的度量即从异构体自身的结构、属性出发进行度量; 基于组件异构度度量则是在异构体内部, 由各层次不同组件间的异构度来衡量异构体的整体异构度。选择异构程度大(相似程度小)的调度方案, 在理论上能够使在线执行体集的相异程度最大, 降低存有共同漏洞的可能, 从而降低同一漏洞被攻破所造成的瞬时逃逸概率, 但单纯的从硬件和资源的异构程度出发, 可能会出现资源不匹配、负载不均衡等问题, 因而很多方案都加入了对服务质量、负载的考量, 并且随着异构体数

量的增多, 异构程度的计算将会非常复杂。除此以外, 也有调度方案选择自己人工为不同的执行体赋予不同的调度概率, 或是基于执行体被探测、攻击的次数决定下轮被选择的权重, 以及基于执行体每次服务输出的相似程度等。具体被调度的对象, 即异构体, 则根据不同的算法与应用场景有所不同。

在调度时机的确定上, 主要分为设定时长和触发机制两种策略。设定时长机制是指提前设置每轮执行体集的服务时长, 到时后重新进行调度, 上线新的执行体集。当时长固定时, 则是最普遍的基本调度策略——周期调度, 即按照固定的时间间隔替换执行体集, 这种方法简单易懂, 实施容易, 但不足以应对突发情况; 每轮时长不固定时, 需要在上线执行体时为其分配可执行的时间长度或任务数量, 归零时自动下线, 并选择新的异构体上线, 时长的选择可由系统随机设定(随机时长), 也可基于上一轮的执行环境设定(最优时长), 这种方式适用于整个执行体集, 也可应用在单个执行体上, 通过加强执行体上下线的随机性, 更大程度的扰乱攻击者的观察, 为系统提供更强的安全保护, 但同样需要额外的调度逻辑和管理。而基于触发机制的调度则是在任务到来时(任务触发), 或是系统、已有的执行体集发现异常时(异常触发)执行调度策略, 选择新的执行体集: 任务触发策略能够根据任务需求动态选择符合要求的执行体上线, 从而更好的满足任务的性能需求, 但可能会引入一定的计算开销, 不适用于对实时性要求高的场景; 异常触发策略则是在发现部分执行体遭受攻击或异常时, 下线全部或部分执行体, 选择新的执行体上线, 以快速应对突发攻击, 但面临频繁的攻击时, 可能会导致频繁的上下线操作, 影响系统稳定性。此外, 也有调度策略借鉴滑动窗口机制动态分配资源, 从而减少频繁的上下线操作, 但需要更多的管理和调度策略, 复杂程度较高。

在调度数量的选择上, 普遍被选择的方式是固定每轮上线的执行体数量, 这种方法稳定性高, 有助于资源的提前规划。有相关研究工作通过实验研究发现, 当执行体数量为 3 时, 能够更好的平衡系统的安全性和性能开销。也有调度策略选择动态地规划执行体的数量, 通过随机设定、阈值筛选、根据历史任务完成情况(历史设定)等方式, 在规划调度方案之初先确定执行体集的大小。其中, 随机设定指每次选择随机数量的执行体, 但这种方式可能会导致不合理分配, 从而浪费资源。阈值筛选机制通过与调度对象的选择策略共同作用, 筛选出符合要求的异构体进入执行体集合, 这种方式能够满足不同的任务需求, 但手动设定阈值的方式缺少一定的灵活性。历史设定策略根据历史的任务完成情况, 动态调整下一轮所需要的执行体数量, 从而实现资源的合理分配, 但这种方法需要维护历史数据和分析算法。

调度对象、调度时机、调度数量的确定, 能够实现系统的动态变化, 对外呈现不确定性, 对内实现概率可控。下面就对已有的研究工作进行分析介绍, 探讨不同调度策略对系统性能和安全性的影响, 以及它们在各种应用场景中的适用性和局限性。本文按照应用场景将相关研究工作分为了通用态防御系统、拟态 Web 服务器、拟态 SDN 等, 并将其总结如表 7。

具体的, 针对拟态防御系统, 文献[87]提出一种基于最大异构性、服务质量和历史可信度的随机种子调度算法, 该算法通过随机选择满足阈值的历史可信度执行者作为种子执行者, 并根据最大异构性类型和服务质量指标确定调度方案, 在动态性、安全性和服务质量之间取得了很好的动态平衡, 但缺乏对系统安全性的评估。文献[88]提出随机种子最小相似度算法, 在确定调度方案时, 首先随机确定种子冗余体, 然后再根据相似度指标选择整体相似度最小的最终调度方案, 综合考虑了调度门限和周期, 动态性较高, 复杂度低, 但缺乏对多执行体调度的考虑。文献[89]提出一种冗余自适应的异构度优先调度算法。该算法在任务实时性约束下, 通过队列机制配合一种贪婪的任务调度策略选择满足平均异构度最大的目标; 同时对于系统任务负载大时, 冗余执行会影响任务可调度性的问题, 又提出有条件的丢弃策略来缓解问题。文献[90]针对现有调度方法的不灵活问题, 提出了一种基于滑动窗口的调度序列控制方法。文献[91]针对现有调度算法存在的调度被动和调度粒度大的问题, 提出了基于多级队列的动态调度算法, 首先初始化执行体组件间最小相似度方案, 然后下线到达随机时间阈值的执行体, 并基于任务随机阈值确定执行同一任务的执行体数量, 从而有效地防止异构执行体变换规律被攻击者掌握。但该算法较为复杂, 对系统性能要求高。文献[92]提出一种基于拟态防御的差分反馈调度决策算法, 并利用动态变换异构调度器和决策算法对现有调度决策算法进行改进。文献[93]从系统漏洞属性和攻击历史行为的角度, 针对不同的攻击场景, 提出了一种基于异构性和置信度的拟态调度算法, 该算法首先根据组件高阶异构度初始化调度方案, 当表决器

表 7 调度算法相关研究工作总结

Table 7 Summary of research work related to scheduling algorithm

调度算法	应用场景	调度对象	调度时机	调度数量
基于历史的随机种子算法[87]	—	基于组件异构度	—	随机设定
随机种子最小相似度算法[88]	—	基于异构体异构度	—	—
冗余自适应的异构度优先算法[89]	—	基于组件异构度	任务触发	—
基于滑动窗口算法[90]	—	—	滑动窗口	滑动窗口大小
随机阈值动态策略[91]	—	基于组件异构度	随机时长	阈值筛选
负反馈调度算法[92]	—	基于异构体异构度	—	历史设定
基于异构度和置信度算法[93]	—	基于组件异构度	异常触发	—
基于最小 L 阶错误概率算法[94]	—	基于组件异构度	—	—
负反馈动态人工赋权算法[95]	—	人工赋权概率	—	—
最优种子调度算法[96]	—	基于组件异构度	—	—
基于高阶异构度算法[97]	—	基于异构体异构度	—	—
基于 BSG 博弈算法[98]	拟态 Web 服务器	基于组件异构度	—	—
最大异构性及服务质量算法[99]	拟态 Web 服务器	基于异构体异构度	—	—
差异化反馈算法[100]	拟态 Web 服务器	基于异构体异构度	—	历史设定
基于负反馈管理框架[13]	拟态 SDN	基于异构体异构度	最优时长	历史设定
负载感知动态调度算法[102]	拟态 SDN	基于异构体异构度	—	阈值筛选
基于生物种群负反馈算法[103]	拟态 NOS	基于被攻击次数	—	历史设定
基于攻击信息负反馈算法[104]	拟态 NOS	基于被攻击次数	异常触发	—
基于优先级和时间片算法[105]	拟态云服务	基于异构体异构度	异常触发	—
基于负反馈调度算法[106]	拟态云服务	基于异构体异构度	异常触发	—
基于 SLA 协商机制算法[107]	拟态云服务	基于异构体异构度	任务触发	—
基于多级队列算法[108]	志愿服务系统	基于异构体异构度	随机时长	—
熵权分簇调度算法[109]	MCOE	基于风险值+熵权	—	—
基于差异距离算法[110]	工业网络	基于输出相似度	固定时长+异常触发	固定数量

注: “—”表示相关文献中未明确提及该机制

发现异常时, 就根据异构度和历史置信度替换调度方案, 并更新执行体的置信度, 该算法提高了系统在非均匀分布式攻击场景下的安全性和各攻击场景下的运行效率。文献[94]提出了一种基于最小 L 阶错误概率的异构体评价模型, 以增强调度算法的动态性。文献[95]基于动态人工赋权方法, 提出了一种具有负反馈功能的动态调度算法, 其在随机装载场景和负反馈装载场景下均有良好的表现, 但在碰撞率的提升方面效果不明显, 尤其是在负反馈装载场景中。文献[96]提出的最优种子策略调度算法, 在选择执行体时, 不仅依据执行体的异构程度, 还通过维护一个记录工作状态、安全性能的负反馈指标, 影响异构体被选择的优先级, 使得调度算法能够充分考虑执行体的初始性能、实时安全性能和异构性质。文献[97]提出了一种同时考虑执行体高阶异构度和历史信息的异构执行体动态调度算法——基于高阶异构度的负反馈调度算法, 该算法将执行体池中的异构执行体进行 n 阶异构度计算, 得到相互之间异构度最大的 n 模执行体集方案, 解决了当前动态异构冗余系统中异构体调度缺乏动态性和仅考虑二阶异构性, 导致系统易被攻击者找到共模漏洞从而攻破系统的问题, 但该算法复杂程度较高。

针对拟态 Web 服务器系统, 文献[98]利用 Bayesian-Stackelberg 博弈方法, 结合异构执行体之间的差异性, 构建出基于攻防博弈的执行体调度模型, 使防御者根据先验攻击者的类型和执行体间差异性, 总能选到收益最高的调度方案, 但该算法计算复杂度较高。文献[99]针对拟态 Web 服务器服务质量不稳定的问题, 提出一种基于最大异构性和 Web 服务质量的随机种子调度算法, 相较于文献[88]的随机最小种子调度算法, 该算法在选出种子执行体后, 不仅考虑了异构性指标, 同时还对 Web 服务的性能进行量化评估, 结合 Web 服务质量原则对调度方案进行选择。文献[100]针对服务器路径配置的安全问题, 提出一种基于 CMD 的差异化反馈调度算法, 利用 MOSS 算法[101]得到执行体间异构度, 根据执行体输出一致性的前后变化, 动态地更新调度器调度执行体的个数, 该方案动态性较好, 系统失效率和代

价低, 但缺乏对变换时间和变化条件的研究。

在拟态 SDN 应用场景下, 文献[13]提出基于负反馈的调度管理框架, 内部采用基于效用的动态弹性调度策略, 根据当前网络环境进而确定下一步在线执行体的数量和调度时机。文献[102]针对 SDN 控制流篡改攻击等安全威胁, 提出了动态安全调度机制。建立控制器执行体与调度体调度模型, 根据系统攻击异常、异构度等指标设计动态调度策略; 同时考虑了系统负载因素, 通过设计调度算法将调度问题转化为动态双目标优化问题, 以实现优化的调度方案。针对拟态网络操作系统的安全问题, 文献[103]在其设计的拟态网络操作系统中, 针对目前拟态防御采用的随机调度未考虑执行体安全状态问题, 提出了一种自适应的负反馈调度模式, 自动在系统的执行过程中根据各类型控制器的生存力(被攻击次数)确定调度权重, 在不同的时间周期内, 按照生成的安全系数以一定概率选择执行体。但该调度算法未考虑异构执行体间的异构程度。文献[104]则针对拟态网络操作系统架构缺乏自适应能力的问题, 提出了一种基于攻击信息的动态负反馈调度方法, 将控制器进行分类, 在分析表决信息和检测信息发现异常时, 统计执行体被探测次数和假设检验得到攻击者的攻击目标倾向, 依此进行调度, 但并未考虑异构执行体之间的异构程度。

在拟态云服务场景中, 文献[105]提出基于优先级和时间片的执行池调度算法, 基于执行体之间的异构度, 以及由时间片策略确定的调度优先级, 预备备选调度方案, 在构件集发生改变、执行体下线或者是动态策略触发时, 选择合适的调度策略。该算法在动态性和时间成本上优于文献[88]所提算法, 配合时间片策略也可在相似性上接近于该算法。文献[106]针对云环境下虚拟机的单一性、同质性和静态安全威胁问题, 提出一种基于拟态防御的负反馈动态调度算法, 由常见漏洞数量描述执行体的异构度, 在表决器报告异常时执行调度策略。文献[107]提出了一种面向拟态云服务系统的安全 SLA 协商机制, 在用户请求服务时, 按照 SLA 协议评估的服务质量与异构度选择执行体集。

文献[108]针对现有调度算法存在的被动调度和调度粒度大的问题, 结合时间阈值和随机阈值, 提出了一种基于多级队列的动态调度算法。该算法能够有效防止异构执行体的变换规则被攻击者掌握。文献[109]针对拟态通用运行环境的业务需求, 提出一种熵权聚类调度算法, 通过风险值筛选、负载均衡、熵权计算和聚类优化四个步骤筛选符合条件的最佳执行体, 该算法能够很好地服务于拟态通用运行环境, 但该工作缺少与其他调度算法的对比。文献[110]针对现有调度算法难以区分每次攻击行为的恶意程度, 也难以应对执行体输出为数值且允许存在误差的应用场景的问题, 提出基于运行时长、可信度和切换开销等构造收益函数的调度算法, 算法首先基于 MOSS 度量执行体间的异构度初始化调度方案, 然后分别于固定周期和紧急切换时, 基于执行体输出之间的差异距离更新执行体集, 有效降低目标电力系统失效率。

3.2 拟态防御系统的表决算法研究

表决器作为 CMD 系统的另一个核心模块, 负责将在线的多个执行体的输出映射成为唯一的系统输出, 对外呈现映射的不确定性, 从而迷惑攻击者, 同时增加系统的可靠性。拟态防御系统的表决算法改进研究如表 8 所示。

常用的表决算法包括多数表决、加权表决等。多数表决即选择输出最多的表决作为结果, 这种算法能够快速做出判断, 但无法应对平局问题, 且忽视了不同执行体输出的可信程度。在相关的研究工作中, 更多使用加权表决来判决异构执行体的输出, 这种算法考虑输出差异、异构度、历史信息等关键要素, 为每个要素分配合适的权重, 然后依据输出结果将执行体分组, 再计算各组的加权分数, 最终选择分数最高的组的结果作为表决输出。加权表决算法考虑了不同要素的权重, 使得更重要的因素能够更大程度地影响决策, 因而具有更高的决策准确性, 但也具有一定的计算复杂性, 且要求数据准备充分。这两种方式也可相互补充使用, 即当多数表决遇到票数相等的情况, 可再利用加权表决来进行判断, 以提高决策的可靠性和准确性。这种组合方法有助于克服多数表决中的平局问题, 同时充分考虑了异构度和历史信息等因素, 以综合评估执行体的性能和可靠性。

具体的, 针对拟态防御系统, 文献[111]为提高表决效率, 提出一种竞赛式的多数一致性表决模型, 不改变表决余度而增加执行余度, 选择领先的输出结果进行仲裁。然而该算法需要进一步研究如何实现余度增加与性能下降的折衷。文献[112]在现有基于历史信息的表决算法基础上, 通过赋予执行体输出结果在数量、历史置信度和异构度上不同的权重, 选择最大值作为输出。实验结果表明, 与多数表决算法相比, 该算法可有效提高表决器输出结果的正确率和算法执行效率。但未考虑执行体个数对参数的影响。文献[113]提出的条件概率投票算法, 按照输出

表 8　表决算法相关研究工作总结

Table 8　Summary of research work related to voting algorithm

工作	应用场景	思路	优缺点
竞赛式表决算法[111]	—	竞赛式多数表决	提高表决效率, 但并未提高正确率
基于执行体异构度算法[112]	—	加权表决	提高表决效率和正确率, 但未考虑系统规模的影响
条件概率表决算法[113]	—	条件概率投票	提升系统安全性, 但对攻击模型的假设较为严格
基于置信度修正算法[114]	—	加权表决	有效维护系统表决稳定性, 但还需研究参数设置
高阶异构度大数表决[115]	—	多数表决+加权表决	在执行体多、相似度高的情况下提高正确率, 但计算相对复杂
基于异常值表决算法[116]	—	加权表决	提高表决正确率, 但缺少权威训练集
基于 AHP-FCE 算法[117]	—	加权表决	提高表决正确率, 但还需优化运行效率
自适应表决算法[118]	—	滑动窗口+多数表决	面向持久性连接, 提升表决效率
基于流处理表决算法[119]	拟态 Web 服务器	定数表决	降低了时空复杂度, 改善空等待问题
差异化反馈表决算法[100]	拟态 Web 服务器	加权表决	提高正确率, 但未考虑执行体间差异
开放流表表决算法[120]	拟态 SDN	定数表决	降低了时空复杂度, 改善空等待问题
基于博弈论表决算法[103]	拟态 NOS	博弈表决	有效降低系统时延开销
流一致表决算法[104]	拟态 NOS	选择得分最高结果	提升系统安全性, 但需考虑计算开销
竞赛式表决优化算法[121]	拟态数据库系统	竞赛式多数表决+日志校验	提高表决正确率, 降低差模逃逸的概率, 但需额外维护执行体日志与分析算法
MCOE 表决算法[122]	MCOE	加权表决	提高表决正确率, 但可能存在数据闲置
模糊表决算法[89]	工业控制系统	二次表决	降低系统错误率, 但可能存在差模逃逸
基于差异距离表决算法[110]	工业网络	加权表决	有效降低系统失效率

结果分组, 然后选择错误概率较小的一组的输出作为结果, 相较于经典的多数投票算法, 具有更强的安全性和可靠性。但该算法对于攻击模型的假设比较严格。文献[114]针对现有的表决方法在计算置信度时面临攻击变化导致的置信度倾斜问题, 提出一种基于 Logistic 函数的置信度计算校正方法, 对不同历史时期的影响进行分级, 过滤掉“过热”异常输出的噪声, 从而对攻击序列的变化形成有效的收敛。文献[115]针对目前利用二阶异构度分析方式无法面对异构执行体较多的情况, 提出基于高阶异构度的多数表决算法, 在多数表决算法的基础上, 当存在投票数并列第一的输出时, 选择高阶异构度大的结果作为系统的最终输出, 该算法能够在执行体相似度高、执行体数量多的情况下有效提升其准确性。文献[116]针对目前表决策略无法抵御共模逃逸风险的缺陷, 提出了基于数据异常值检测的异常值表决算法, 通过搜集执行体输出数据集, 训练异常检测模型用以判断执行体的异常值, 并以赋权的方式使系统能够感受执行体结果的异常值。但该算法需要事先利用深度学习训练异常值检测模型, 而目前缺乏较为官方的拟态安全数据集。文献[117]改造了层次分析-模糊综合评价的判断矩阵, 进而提出了一种改进的考虑了结果一致性、历史置信度、异构度的多指标拟态表决算法, 将拟态表决的过程转化为了模糊评价的过程, 提高了表决准确率。但仍需对算法的运行效率和资源消耗进行进一步的优化。文献[118]等人设计实现了面向持久性连接的自适应拟态表决器, 在接收执行体输出的同时对现有数据进行表决和输出, 提升表决效率, 并引入了自适应的拟态表决算法选择策略集, 根据不同的数据变化情况动态选择不同的表决算法, 从而组合不同算法的优势, 提高表决准确率。以适应 HTTP 1.1 协议在持久性连接、分块传输编码的应用场景中开销过大的问题。

文献[119]在其 Web 动态异构冗余架构原型系统中, 提出了一种基于流处理的表决器模型, 该模型通过缓冲区临时存放后端执行体返回的数据包, 再为每个缓冲区域创建对应队列, 将数据包散列到哈希表中进行表决操作, 当哈希表某位置的数据包到达一定数量时, 则表决完成, 并实时的将已经完成的表决结果返回给用户, 从而尽可能降低延时、提高效率。文献[100]针对服务器路径配置的安全问题, 提出一种基于拟态防御的差异化反馈调度表决算法, 根据每个执行体的可靠度系数决定输出的权重, 降低了表决的出错率。

文献[120]基于 SDN 拟态控制器的整体架构, 提出了关键决策模块的控制器流表表决方法, 借助 Hash 表, 将先到达一定数量的流表作为输出, 大大提高了表决效率。此外, 针对拟态网络操作系统, 文献[103]在其提出的拟态网络操作系统中, 针对拟态防御采用的大数表决未考虑先验知识的情况, 提出

基于博弈论模型的表决机制, 提升表决结果的正确性。将表决的正确性作为攻击者和防御者的收益函数, 建模为零和博弈, 求解纳什均衡得到最优解。为解决表决机制带来的时延问题, 提出了预判决机制, 有效降低系统时延开销。文献[104]为提升 SDN 网络控制层的安全性能, 针对拟态网络操作系统架构中流表存在不一致的问题, 提出了一种细粒度的流一致表决方法, 分别计算各个流表的字段级匹配得分, 选择分数之和最高的流表作为结果下发给交换机。

文献[121]针对拟态数据库系统中, 竞赛式决策模型可能存在的 SQL 注入差模逃逸的问题, 提出一种竞赛式表决优化方案, 采用异构数据库执行体的二进制日志匹配结果对表决结果进行校验。在异常情况下该模型表决结果正确率更高。但还需考虑多个执行体共同失效的情况。文献[122]针对拟态通用运行环境的外部表决机制和内部表决机制分别进行了改进, 设计了基于历史置信度和异构度的多数表决算法, 并提出基于聚类的优化方案。文献[89]针对工业控制系统中, 执行体输出相同错误时影响表决正确性的问题, 给出一种利用执行体间异构度辅助表决的模糊表决算法。该算法首先根据执行体冗余数量及可能出现相同错误的情况, 改进了模糊规则, 接着利用执行体间的异构度信息辅助进行二次表决。但当多数执行体被攻击成功且输出结果一致时, 表决将输出错误结果, 甚至无法感知异常。文献[110]针对现有调度算法难以区分每次攻击行为的恶意程度, 也难以应对执行体输出为数值且允许存在误差的应用场景的问题, 提出基于差异距离的表决算法, 该算法根据归一化的执行体输出差异距离调整其可信度, 并将被攻击次数作为历史反馈信息, 量化执行体的输出以反映攻击行为的恶意程度, 有效提升系统的防护能力。

3.3 拟态防御系统的整体架构研究

针对通用的拟态防御系统, 文献[123]为改善系统中超时机制适应性差的问题, 提出了一种基于预测的自适应超时机制, 能够在相同系统超时率的情况下, 有效减少表决的时间消耗。文献[124]针对当前超时策略算法难以应对任务量起伏剧烈情况的问题, 提出了一种应用于拟态防御架构系统的基于等效比例执行时间的超时阈值预测算法, 该算法能够针对不同任务情况动态地预测并设定超时阈值, 有效地提高了超时表决效率。文献[125]提出了基于信誉度和相异度的自适应拟态控制器, 基于模块的相异度和信誉度选择执行体, 利用信誉度指标对现有的多模表决机制进行优化, 同时引入负反馈模块更新执行体的信誉度, 该模型防御成本相对较低。文献[119]实现了一种分发器模型, 并提出了一种分发器的改进模型, 该模型通过“头复制, 体链接”的方式, 改进了分发器复制请求过程中造成的时间、空间浪费, 通过映射表虚拟 Session 解决了分发器不支持 Session 机制的问题, 从而不仅可以更快速的对用户请求进行分发, 而且还能提供更加完善的功能。文献[126]提出一种增加异构评估的拟态防御体系改进模型, 将调度任务分解为并行简单调度和异构评估两个模块, 减少了调度时间损失。文献[127]针对 DHR 中执行体之间可能存在共同漏洞的特性, 提出增加执行体划分模块的防御增强型异构冗余架构, 相较于 DHR 在面对未知漏洞时有较为明显的改进。文献[128]为保障拟态防御系统的内部通信安全, 提出一种用于拟态防御的可跟踪匿名认证方法, 将分布式接入架构与拟态防御系统集成, 再添加 Track 进程, 实现面向拟态防御的可溯源匿名认证方法。文献[129]针对拟态防御系统在设计成本和安全性的防御策略方面仍然存在一些关键差距的问题, 提出了一种对偶模型来根据执行者的状态动态选择被重新配置的执行者的数量, 该模型能在保证安全性的同时降低防御成本。

针对 SDN 系统, 文献[130]针对 SDN 控制器调度防御模型, 提出一种基于增强学习的自适应防御策略确定机制, 适应性地选择防御动作执行的时间, 以解决面对未知攻击类型时防御方如何根据自身安全性与性能选择防御措施的问题。但该模型对于参数量化的程度尚不够细致。文献[16]针对目前拟态括号内, 拟态表决面临的传输协议数据的多态化冗余化问题, 将可编程协议解析思想应用到拟态括号的归一化处理中, 使得拟态括号具有更高的高效性和灵活性。

此外, 文献[131]针对网络攻防环境动态感知和适应性调整的问题, 并没有提出新的调度算法, 而是基于演化博弈理论, 提出能让系统在运行中根据历史信息动态优化调度算法的网络功能虚拟化拟态防御架构动态调度策略, 该模型添加了分析器模块分析异常执行体信息, 调度器则根据分析器的反馈信息和架构的系统组成, 利用演化博弈理论对调度算法不断优化。但其分析复杂度较高。

总体而言, 相关研究围绕执行体异构性的定义问题、差模逃逸、在复杂场景中的应用等问题, 分别提出了各自的调度或表决策略。本节则重点围绕调度对象的选择、调度时机的确定和调度的数量三个关键要素, 讨论不同调度算法的改进与不足, 然后围绕具体的表决思路, 分析不同的表决策略。

4 拟态防御系统的建模与评估

数学模型是支撑一个理论体系不断完善的重要基础, 也是促进相关研究工作的重要工具。为了验证拟态防御思想的正确性, 评估 DHR 架构及其应用的各方面性能, 需要搭建拟态防御系统的形式化描述方法和评估模型。拟态防御系统的建模与评估方法如表 9 所示, 在已有的研究工作中, 经典的建模方法, 如博弈论、Petri 网、自动机模型、模拟仿真等被引入到针对拟态防御系统的建模工作中, 其他的方法, 如安全本体理论、可视化、大数卷积方法在建模工作中也同样适用。

表 9 拟态防御系统建模评估方法相关研究工作总结

Table 9 Summary of research work related to modeling and evaluation methods for CMD system

描述	评估对象	建模方法	思路
基于马尔可夫博弈理论模型[132]	—	博弈论	描述为马尔可夫非合作完全信息动态博弈
拟态防御马尔可夫博弈模型[133]	—	博弈论	定义状态路径转移以描述各因素的影响
基于 M-FlipIt 博弈的评估模型[134]	—	博弈论	改进 FlipIt 模型, 建立策略和收益表
动态异构冗余系统安全性分析[135]	—	概率数学模型	从输出一致率、系统攻击成功率建模
基于概率分析安全性分析方法[136]	—	概率数学模型	构建矩阵模型量化分析安全性能
DHR 架构的 CMD 自动机模型[137]	—	自动机模型	使用有穷状态自动机为执行体建模
CMD 系统的时间自动机模型[138]	—	自动机模型	使用时间自动机描述拟态机制和过程
CMD 系统安全分析模型[139]	—	模拟仿真	量化攻击因子、异构程度、动态变化
CMD 结构的安全性量化方法[140]	—	模拟仿真	从动态、异构、冗余三方面进行量化分析
CMD 多样性系统综合评估[141]	—	模拟仿真	量化攻击步长和攻击容忍能力
CMD 系统服务质量的综合评估[142]	—	模拟仿真	综合量化安全性能与服务质量指标
多样化软件系统量化评估方法[143]	—	模拟仿真	构建可用性、安全性、性能层次评价体系
融合广义随机 Petri 网的二维模型[144]	—	Petri 网	分单节点攻击和链路攻击两个维度建模
大数卷积拟态防御数学模型[145]	—	大数卷积方法	分萃取层、卷积层和表决层以函数描述
基于本体的安全建模方法[146]	—	安全本体理论	抽象成拟态结构类和拟态概念类
拟态防御原理验证测试方法[147]	拟态 Web 服务器	模拟仿真	逐级测试系统的基础性能和安全性能
拟态 Web 服务质量量化方法[149]	拟态 Web 服务器	模拟仿真	量化服务质量并进行仿真分析
拟态 Web 服务器异构性量化方法[150]	拟态 Web 服务器	模拟仿真	量化 Web 服务器的异构性并进行仿真分析
拟态 Web 威胁态势分析方法[151]	拟态 Web 服务器	可视化方法	分析威胁分类与等级并可视化展示
路由器拟态防御原理验证系统[152]	拟态路由器	模拟仿真	验证路由器基础性能、防御机制和效果
基于 GSPN 建模方法[153-154]	拟态 DNS 系统	Petri 网	采用广义随机 Petri 网进行建模
拟态云服务的建模与仿真环境[155]	拟态云服务系统	模拟仿真	借助 CloudSim 工具进行建模仿真
大数卷积拟态防御数学模型[156]	拟态云服务系统	大数卷积方法	借助大素因子分解问题和卷积运算
拟态 MSISDN 的拟态自动机模型[157]	拟态 MSISDN	自动机模型	多种自动机模型按照一定逻辑关系结合
CMD 架构的多余度表决建模[158-159]	表决算法	模拟仿真	分析表决模型的安全增益、系统开销和恢复能力

4.1 拟态防御系统的通用建模方法

博弈论是常用的建模方法之一。针对拟态防御系统, 文献[132]从博弈论的角度出发, 根据网络空间拟态防御系统攻防对抗的动态特性, 将其描述为马尔可夫非合作完全信息动态博弈, 建立了一种基于马尔可夫博弈理论的拟态防御系统安全评估模型。但该方法缺少实验验证, 且随着执行体和攻防策略数量的增加容易产生状态爆炸。文献[133]建立了拟态防御马尔可夫模型, 是针对 DHR 架构本身建立的安全度量模型, 通过定义多种状态路径转移描述执行体冗余性、多样性以及表决反馈机制对攻防博弈过程的影响。文献[134]提出一种改进的 FlipIt 博弈模型, 以评估拟态防御模型面对高级持续性威胁时的表现。

从概率数学角度来看, 文献[135]针对 DHR 架构建立了安全模型, 以 L 阶漏洞一致率、系统攻击成功率等指标表征系统的安全性, 在此模型中, 却没有对构件的异构度进行建模, 该模型也不能指导调度方案更改时间间隔的选择。文献[136]提出了执行体-漏洞矩阵模型和服务体-漏洞矩阵模型用于描述 DHR 模型内部的结构和漏洞之间的关联。同时提出攻击序列法和服务体法并推导出非合谋盲攻击、合谋盲攻击、非合谋最优攻击和合谋最优攻击场景下安全性指标的计算公式。但该模型只考虑了一次攻

击的场景, 并未考虑多步骤多漏洞的场景, 且未考虑攻击者能力大小、漏洞攻击难度、漏洞探测验证等实际因素。

文献[137]提出将拟态防御自动机模型作为形式化分析 DHR 架构的手段, 使用有穷状态自动机及其并行组合自动机为一些拟态攻防行为建立计算模型, 由于是在全状态空间中全面搜索, 分析的运行时间远超其他分析模型, 但实验证明该模型能够全面地验证 DHR 拟态防御系统。文献[138]以时间自动机为形式化语言对拟态防御系统的架构和表决策略进行建模, 并使用 PAT 工具对拟态防御系统的不同方面进行分析。

模拟仿真法也是常用的建模方法之一。文献[139]提出一种结合动态特征、异构特征和冗余特征的方法, 通过概率分析对拟态防御系统进行安全分析。文献[140]提出一种拟态防御体系结构的安全量化方法, 从整体全局级别、架构本身系统级别和架构内部细节出发的基于异构机制的细节级三个层面构建对于拟态防御架构的整体安全性分析模型, 此外从平均可靠性寿命属性出发, 结合组合理论的思想, 给出拟态防御结构的最优冗余。文献[141]提出一种基于攻防实验的多样性系统评价方法, 将多样性系统分为时间多样性和空间多样性, 并通过特洛伊木马攻击实验, 对不同配置的多样性系统的防御能力、成本和响应延迟进行了评估和比较, 结果表明, 两种多样性的结合在防御能力上起到了互补作用, 但也增加了成本和响应延迟。文献[142]提出了结合性能指标和安全性的服务质量评价方法, 从不同的角度评价服务质量。文献[143]基于层次分析法的多样化软件量化评估方法, 在准则层综合考量安全性、可用性和性能三个特性, 为不同场景下执行体集的选择方案提供参考, 但只适用于小规模情况。

其他的, 文献[144]提出了二维分析模型, 将防御系统网络配置进行量化, 在第一维度对单节点攻击行为使用广义随机 Petri 网络建模, 在第二维度对链路攻击行为使用马尔可夫链和鞅理论建模, 该模型能够应用于不同的安全防御系统。文献[145]提出了一种大数卷积拟态防御数学模型, 它分为萃取层、卷积层和表决层, 各层以一个函数描述, 该模型能把网络空间攻防博弈问题转换成对应的数学问题。但该模型的部分组件还未完全形象化, 如系统输入组件较为抽象化且暂无形象的数学表述。文献[146]提出了一种基于本体的拟态防御系统安全建模方法。将防御架构抽象成拟态结构类和拟态概念类, 并引入动态选择算法描述攻击面移动, 但在其对动态选择算法的研究中, 本质上仍是人为规定的确定化的伪随机结果, 并未实现真正的随机化。

4.2 特定场景的建模方法

文献[147]提出针对引入拟态防御机制的 Web 服务器系统[148]的测试方法, 设计并实施了完整的测试方案, 验证了该系统的基础性能与安全性能。文献[149]针对难以量化评估拟态防御对 Web 服务器服务质量造成影响的问题, 基于“木桶”原理提出了拟态构造 Web 服务器服务质量的量化评估方法, 并利用向量相似度方法量化服务质量的损耗值。文献[150]又针对拟态构造的 Web 服务器的异构性难以量化的问题, 将拟态构造的 Web 服务器的异构性定义为其执行体集的复杂性与差异性, 提出了一种适用于量化异构性的量化方法。在理论上为拟态防御量化评估提供了一种新方法, 从而指导调度算法和表决算法的改进。文献[151]提出一种拟态 Web 威胁告警分类与可视化分析方法, 通过拟态防御的表决方法生成异常告警数据, 并按照表决一致程度进行等级划分和分类预测, 进而生成各种拟态防御态势展示图。但该模型针对异常访问无法给出更准确的分析结果。文献[152]提出针对引入拟态防御机制的路由器系统的测试方法。针对拟态 DNS 系统, 文献[153]采用广义随机 Petri 网对拟态 DNS 的攻击、干扰和防御进行建模, 并比较了不同干扰强度下不同冗余系统和模拟 DNS 的可用性和感知安全性。文献[154]提出的模型则采用可用概率、逃逸概率和非特殊感知概率对系统性能进行定量分析。

文献[155]基于 CloudSim 基本功能提出了一个云服务仿真系统, 帮助研究人员实施新的调度和表决机制。文献[156]基于大素因数和卷积运算的分解问题, 提出了一个大数卷积拟态防御数学模型。提出的模型可以清晰地表达 CMD 机制, 将 CMD 领域的攻防问题转化为相应的数学问题, 从而对 CMD 的安全能力进行定性评估。

文献[157]为 MSISDN 系统构建了一套拟态自动机模型与安全性验证方法, 分别使用有穷状态自动机、细胞自动机和层次自动机描述系统的状态迁移、变化结构和计算粒度, 能够高效的描述 MSISDN 系统在全状态空间内的安全性。

文献[158-159]根据拟态防御与多余度表决模型之间的关系, 针对多余度表决方法的防御能力、运行效率和系统恢复三方面进行建模和分析, 是对 DHR 架构内部表决方法的评估方法。

本节总结了概念提出以来在对拟态防御系统的建模和评估方法方向的研究成果。在建模与分析方

法中, 模拟仿真、博弈论、广义随机 Petri 网、自动机模型是研究人员分析评估拟态防御系统及其应用性能的常用方法。然而这些方法各有其优点和局限性。其中, 博弈论重点研究的是决策制定者之间的相互作用, 即攻防双方的策略选择和决策过程, 相对于其他方法, 可以分析多方参与的复杂网络攻防情景, 由于强调策略和均衡, 还有助于研究者理解攻击方和防御方之间的博弈动态, 但难以捕捉 CMD 系统的网络拓扑或技术细节, 且因其基于理性假设, 可能并不适用于分析非理性的攻击者行为。自动机模型是基于状态和状态转移的建模方法, 通过描述有限数量的状态和状态之间转移的方式定义系统的行为, 具有简单性和直观性, 易于理解和分析, 对于具有有限状态的问题, 可以提供准确的建模, 但不太适用于描述攻击者的策略性行为, 且其基于离散状态, 难以处理连续的事件。广义随机 Petri 网络同样以图形化的方式描述系统的状态转移和事件触发关系, 有助于直观理解系统的状态和事件之间的关系, 且允许进行形式化的分析, 有助于发现潜在的安全问题, 并且天生支持并发性和分布式系统的建模, 但对于大规模和复杂的系统, Petri 网模型可能变得异常庞大, 导致难以管理和分析。比较而言, 自动机模型适用于简单、有限状态的网络信息系统, 而广义随机 Petri 网模型适用于更复杂、随机性和并发性较强的系统。

对于 DHR 建模评估方法的研究, 具有重要的实践价值。一方面, 这些研究成果可以为研究人员和从业者提供有关如何构建或加强 DHR 架构模型的指导, 以满足不断变化的需求和威胁。另一方面, 这些研究还能够为人们提供评估系统可用性和安全性的有力工具, 有助于识别系统中的潜在问题和风险。

5 总结

本文总结了自概念提出以来有关 CMD 思想的研究成果, 分应用场景、架构研究和建模评估三方面展开综述。目前来看, 在已有的应用研究中, 针对传统的 Web 服务器架构和新兴的 SDN 系统、区块链系统、云环境和分布式存储系统的研究较为完善。为了提升 CMD 系统的安全性, 最小化引入 CMD 思想带来的性能损失与资源浪费, 并提升拟态防御系统的服务性能, 部分工作分别对调度算法以及表决机制等方面进行架构层面的改进。研究 CMD 思想的另一个方向是对模型的分析, 其中模拟仿真、博弈论、广义随机 Petri 网和自动机模型是分析 DHR 架构及其应用性能的主要方法。CMD 理论与方法仍在不断的研究和完善之中, 从技术发展的趋势来看, 未来的工作将可能在如下四个方面展开。

(1) 拟态防御在新兴技术场景中的应用

在 CMD 于已有的应用场景中持续发挥作用的同时, 还将创建更多的应用场景, 尤其是与新兴领域的深度融合。能够确定的是, 随着新兴技术的不断发展, 软硬件产品的种类和功能将会越来越多样化, 其复杂性也将日益增加, 我们无法完全避免产品出现内生安全漏洞。如本文第三节所述, 目前 CMD 思想已和云服务、区块链、分布式系统等已经广泛部署的新兴技术深度融合, 保障相关系统的安全性能, 以应对未知的安全威胁与漏洞。对于 6G 通信、元宇宙、量子计算机等正在推进研究的新技术, 提早引入 CMD 技术也可以更快一步有效应对不断变化的威胁和攻击手法。例如, 对于 6G 通信技术, CMD 思想除了在网络交换、处理设备中发挥作用外, 还可以与网络流量调控、频谱管理与分配、身份验证等阶段相结合, 通过增加随机性与动态特征, 增加攻击者侦听、破解、干扰的难度。而元宇宙作为一个多维度的虚拟世界, 各种虚拟实体、人类互动以及数字资产在其中广泛交织, 可以将 CMD 技术融入元宇宙的基础架构, 混淆攻击者对于开放信息的识别, 实现精准保护, 或将其应用到社交平台和虚拟聚会中, 可以确保用户的互动隐私和信息安全, 又或是嵌入到虚拟物品和数字资产中, 能够使这些物品具有自我保护能力, 防范盗窃与伪造。再如量子计算机, 其虽具有强大的并行计算能力, 能够快速破解传统的加密算法, 但在其内部, 同样存在着无法完全消除的内生安全问题, 而 CMD 技术的融入可以为量子计算环境提供更强韧的安全机制, 对于极其敏感的量子态, 可以通过引入 CMD 思想使其尽力避免攻击者扰动的影响, 在软件层面, 同样可以引入动态异构冗余的结构保护量子计算机的操作系统、应用程序和系统数据; 而反过来, 量子计算也能为拟态防御过程提供真正的随机性和不确定性, 使系统的行为更加难以预测, 其强大的计算能力则能够帮助拟态防御系统快速识别潜在的攻击模式。总的来说, 针对各类计算机系统的内生安全威胁无法完全消除的问题, 可以有针对性地引入 CMD 思想, 从而为新兴技术的可持续健康发展提供坚实的安全基础。

(2) 性能与安全的平衡关系研究

在网络空间领域, DHR 架构的引入为计算机系统的安全性和鲁棒性提供了有力的支持, 然而也不可避免的带来资源开销加重的问题, 如何追求性能与安全的平衡还将是相关研究工作需要持续探讨的

问题。DHR 架构的核心思想在于为计算机系统引入动态性、随机性和多样性, 使攻击者难以适应和预测系统的环境变化, 但这也意味着系统需要消耗更多的硬件、软件或是带宽资源, 这增加了资源的开销。特别是在大规模的网络环境中, DHR 架构的引入可能会占用大量的计算和存储资源, 影响系统的实时性和性能。因此, 在保证系统安全性的前提下, 可通过进一步优化调度与表决策略、划分异构等级、构建 DHR 架构的自适应机制等方式, 探索资源的有效管理和性能提升的可能, 使 CMD 技术更加可持续的应用于实际场景中, 为网络安全提供更强大的防御能力。

(3) 拟态防御与现有安全技术的融合

第三, 在将 CMD 技术引入实际系统中时, 可以与传统网络安全技术及新兴防御技术相结合, 共同构建一个多层次的防御体系, 全面提升系统的安全防护能力。一方面, 将 CMD 技术与防火墙、加解密技术、入侵检测等传统的网络安全技术相融合, 能够在基于已知的攻击特征进行防御的基础上, 引入不确定性和变化性, 从而增加攻击者的攻击成本, 同时兼顾防范已知和未知的威胁。而与机器学习、区块链等新兴防御技术的融合, 则使安全系统的防护能力提升到更多的维度, 能够增强系统对多样化攻击的适应性。另一方面, 构建多层次的防御体系还将有助于系统在安全与性能之间寻求平衡, 在引入 CMD 技术的系统中, 各层次的技术可以根据实际的外部环境与系统内部情况进行协同工作。有选择地将 CMD 技术应用于关键环节, 能够在较少的开销损失下求得更完备的安全性能。但由于在当前的网络系统中, 往往已经部署了已有的安全防御技术, 而新技术的引入有可能会改变原有的系统配置, 造成干扰, 因而在研究 CMD 技术与其他安全技术的结合时, 还需要考虑到其适应性, 使其更好的嵌入到网络信息系统中并发挥安全防护作用。综合而言, 将 CMD 技术融合于传统网络安全技术与新兴防御技术中, 打造多层次地综合性防御体系, 也将是 CMD 的重要研究方向之一, 这将能够最大限度地发挥各种技术的优势, 针对不断变化的网络威胁, 为网络安全系统提供更强大的应对能力, 从而保护网络空间的安全与稳定。

(4) 相关标准与规范的建立

在 CMD 技术的推广应用中, 还需加快相关标准的建立。目前, CMD 技术尚未有明确的标准与规范, 这可能导致技术的应用和交流受到限制。为此, 有必要尽快建立起严格的技术标准与规范, 以确保不同 CMD 系统之间的兼容性, 加速技术的发展与应用, 使 CMD 技术能够更好地融入国际技术体系, 同时也为评估技术的有效性和可行性提供了客观的依据。

今天, “改变网络空间游戏规则”的网络空间拟态防御理论及其内生安全效应正不断彰显出其勃勃生机与旺盛活力, 在软硬件无法彻底清楚其内生安全问题时, 也能依靠创新的内生安全机制规避或瓦解来自网络空间的不确定威胁。尽管拟态防御理论的研究仍处于初步探索阶段, 一些概念和具体技术也存在争议。然而, 主动防御技术无疑引领了未来网络防御技术的发展方向, 拟态防御理论的探索和研究将成为网络空间安全的重要基石, 人类也必将迎来以目标对象内生安全功能为核心的网络空间拟态防御技术新时代。

参考文献

[1] Wu J X. Cyberspace Mimicry Security Defense[J]. *Secrecy Science and Technology*, 2014(10): 4-9, 1.
(邬江兴. 网络空间拟态安全防御[J]. *保密科学技术*, 2014(10): 4-9, 1.)

[2] 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.
(仝青, 张铮, 张为华, 等. 拟态防御 Web 服务器设计与实现[J]. *软件学报*, 2017, 28(4): 883-897.)

[3] Liu X L, Huang J H, Luo W F, et al. Web Practice and Security Analysis under Dynamic Heterogeneous Redundant Architecture[J]. *Journal of Computer Applications*, 2021, 41(S1): 125-130.
(刘昕林, 黄建华, 罗伟峰, 等. 动态异构冗余架构下 Web 实践及安全性分析[J]. *计算机应用*, 2021, 41(S1): 125-130.)

[4] Wang J. Research on web malicious code injection defense method based on randomization[D]. Zhengzhou: Information Engineering University, 2021.
(王疆. 基于随机化的 Web 恶意代码注入防御方法研究[D]. 郑州: 战略支援部队信息工程大学, 2021.)

[5] Xing X F, Shang C L. Exploration and Practice of Web Protection Scheme Based on Mimicry Technology[J]. *Jiangsu Communication*, 2022, 38(2): 116-119.
(邢学锋, 尚春雷. 基于拟态技术的 Web 防护方案探索与实践[J]. *江苏通信*, 2022, 38(2): 116-119.)

[6] Qi C. Research on the key technologies of mimic network operating system architecture[D]. Zhengzhou: Information Engineering University, 2018.
(齐超. 拟态网络操作系统架构及关键技术研究[D]. 郑州: 战略支援部队信息工程大学, 2018.)

[7] 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.
(王禎鹏, 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.)

[8] Lu Z P. Research on proactive defense of SDN controller[D].

Zhengzhou: Information Engineering University, 2017.
(卢振平. SDN 控制器主动防御关键技术研究[D]. 郑州: 战略支援部队信息工程大学, 2017.)

[9] Gu Z Y. Research on proactive defense strategy for SDN controller[D]. Zhengzhou: Information Engineering University, 2018.
(顾泽宇. 面向 SDN 控制器的主动防御策略研究[D]. 郑州: 战略支援部队信息工程大学, 2018.)

[10] Gu Z Y, Zhang X M, Lin S J. Research on Security Mechanism for SDN Control Layer Based on Mimic Defense Theory[J]. *Application Research of Computers*, 2018, 35(7): 2148-2152.
(顾泽宇, 张兴明, 林森杰. 基于拟态防御理论的 SDN 控制层安全机制研究[J]. *计算机应用研究*, 2018, 35(7): 2148-2152.)

[11] Huang Q M. Research on SDN service path configuration and verification mechanism based on mimetic defense[D]. Hangzhou: Zhejiang Gongshang University, 2020.
(黄前淼. 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, 2020.)

[12] Chen L. An SDN Pseudo Defense Architecture for Path Configuration[J]. *Microcomputer Applications*, 2022, 38(1): 202-205.
(陈荔. 一种用于路径配置的 SDN 拟态防御架构[J]. *微型电脑应用*, 2022, 38(1): 202-205.)

[13] Li J F. Research on key technologies of mimic defense in software-defined network[D]. Zhengzhou: Information Engineering University, 2019.
李军飞. 软件定义网络中拟态防御的关键技术研究[D]. 郑州: 战略支援部队信息工程大学, 2019.

[14] 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.
(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.)

[15] 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.
(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.)

[16] Zhang W J. Research on key technologies of endogenous security for software-defined network[D]. Zhengzhou: Information Engineering University, 2021.
(张文建. 面向软件定义网络的内生安全关键技术研究[D]. 郑州: 战略支援部队信息工程大学, 2021.)

[17] Wang L J. Research on key technologies of network-coding-based mimic data storage[D]. Zhengzhou: PLA Information Engineering University, 2017.
(王龙江. 基于网络编码的数据拟态化存储关键技术研究[D]. 郑州: 解放军信息工程大学, 2017.)

[18] Chen Y, Wang L J, Yan X C, et al. Mimic Storage Scheme Based on Regenerated Code[J]. *Journal on Communications*, 2018, 39(4): 21-34.
(陈越, 王龙江, 严新成, 等. 基于再生码的拟态数据存储方案[J]. *通信学报*, 2018, 39(4): 21-34.)

[19] Hong H C. Dynamic attack surface defense technology based on data layer[D]. Nanjing: Nanjing University of Posts and Telecommunications, 2019.
(洪海诚. 基于数据层的动态攻击面防御技术[D]. 南京: 南京邮电大学, 2019.)

[20] Wang Y W. Research on key technologies of scientific workflow security in clouds[D]. Zhengzhou: Information Engineering University, 2019.
(王亚文. 云环境下面向科学工作流安全的关键技术研究[D]. 郑州: 战略支援部队信息工程大学, 2019.)

[21] Wang Y W, Wu J X, Guo Y F, et al. Scientific Workflow Execution System Based on Mimic Defense in the Cloud Environment[J]. *Frontiers of Information Technology & Electronic Engineering*, 2018, 19(12): 1522-1536.

[22] Li L S. Research on key technologies of mimic SaaS cloud security architecture[D]. Zhengzhou: Information Engineering University, 2021.
(李凌书. 拟态 SaaS 云安全架构及关键技术研究[D]. 郑州: 战略支援部队信息工程大学, 2021.)

[23] Li L S, Wu J X. SaaS Security Oriented Virtual Network Function Embedding Method under Cloud-Network Integration[J]. *Computer Engineering*, 2021, 47(12): 30-39.
(李凌书, 邬江兴. 面向云网融合 SaaS 安全的虚拟网络功能映射方法[J]. *计算机工程*, 2021, 47(12): 30-39.)

[24] Pu L M. Research on the key technologies of mimic cloud service architecture[D]. Zhengzhou: Information Engineering University, 2021.
(普黎明. 拟态云服务架构及关键技术研究[D]. 郑州: 战略支援部队信息工程大学, 2021.)

[25] 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.
(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]. *信息网络安全*, 2021, 21(1): 49-56.)

[26] Yuan C. Research on key technology of privacy protection in blockchain[D]. Zhengzhou: Information Engineering University, 2018.
(苑超. 区块链隐私保护关键技术研究[D]. 郑州: 战略支援部队信息工程大学, 2018.)

[27] Xu M X, Yuan C, Wang Y J, et al. Mimic Blockchain-Solution to the Security of Blockchain[J]. *Journal of Software*, 2019, 30(6): 1681-1691.
(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.)

[28] Zhang J H. Blockchain security protection method based on cyber mimic defense and ring signature[D]. Zhengzhou: Zhengzhou University, 2019.
(张君何. 基于拟态防御和环签名的区块链安全保护方法[D]. 郑州: 郑州大学, 2019.)

[29] Li H, Hu J W, Ma H J, et al. The Architecture of Distributed Storage System under Mimic Defense Theory[C]. *2017 IEEE International Conference on Big Data*, 2017: 2658-2663.

[30] Lin Z L, Li K D, Hou H X, et al. MDFS: A Mimic Defense Theory Based Architecture for Distributed File System[C]. *2017 IEEE International Conference on Big Data*, 2017: 2670-2675.

[31] Yu H Y, Li H, Yang X, et al. On Distributed Object Storage Architecture Based on Mimic Defense[J]. *China Communications*, 2021,

18(8): 109-120.

[32] Feng Xinrui. Research on mimic enhancement design for distributed storage system[D]. Beijing: China Academic of Electronics and Information Technology, 2019.
(冯馨锐. 面向拟态增强的分布式存储系统设计[D]. 北京: 中国电子科技集团公司电子科学研究院, 2019.)

[33] Wu Z Q. Research on metadata management technology for distributed storage system for big data[D]. Zhengzhou: Information Engineering University, 2019.
(武兆琪. 面向大数据的分布式存储系统元数据管理技术研究[D]. 郑州: 战略支援部队信息工程大学, 2019.)

[34] Guo W, Xie G W, Zhang F, et al. Design and Implementation of a Mimic Architecture for Distributed Storage System[J]. *Computer Engineering*, 2020, 46(6): 12-19.
(郭威, 谢光伟, 张帆, 等. 一种分布式存储系统拟态化架构设计与实现[J]. *计算机工程*, 2020, 46(6): 12-19.)

[35] Guo W. Research on mimic architecture and key technologies of distributed storage system[D]. Zhengzhou: Information Engineering University, 2019.
(郭威. 分布式存储系统拟态化架构与关键技术研究[D]. 郑州: 战略支援部队信息工程大学, 2019.)

[36] 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.
(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.)

[37] Wang S, Li Q M, Hou J, et al. Active Defense by Mimic Association Transmission in Edge Computing[J]. *Mobile Networks and Applications*, 2020, 25(2): 725-742.

[38] Sang X N, Li Q M. Mimic Defense Techniques of Edge-Computing Terminal[C]. *2019 IEEE Fifth International Conference on Big Data Computing Service and Applications*, 2019: 247-251.

[39] Ma H L, Yi P, Jiang Y M, et al. Dynamic Heterogeneous Redundancy Based Router Architecture with Mimic Defenses[J]. *Journal of Cyber Security*, 2017, 2(1): 29-42.
(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.)

[40] Yin Z N. Research on anomaly detection technology for mimic router[D]. Zhengzhou: Information Engineering University, 2022.
(尹梓诺. 面向拟态路由器的异常检测技术研究[D]. 郑州: 战略支援部队信息工程大学, 2022.)

[41] Miao F, Wang Z X, Guo Y, et al. AS Security Alliance Mechanism for Inter-Domain Routing System Based on Mimicry Protection[J]. *Computer Science*, 2017, 44(9): 148-155.
(苗甫, 王振兴, 郭毅, 等. 一种基于 AS 安全联盟的域间路由系统拟态防护机制[J]. *计算机科学*, 2017, 44(9): 148-155.)

[42] 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.
(王祯鹏, 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.)

[43] Fan Y W, Zhu W J, Ban S H, et al. Dynamic Heterogeneous and Redundancy Data Protection Architecture[J]. *Journal of Chinese Computer Systems*, 2019, 40(9): 1956-1961.
(樊永文, 朱维军, 班绍桓, 等. 动态异构冗余数据保护安全架构[J]. *小型微型计算机系统*, 2019, 40(9): 1956-1961.)

[44] Fan Y W. Research on data protection architecture based on mimic defense[D]. Zhengzhou: Zhengzhou University, 2019.
(樊永文. 基于拟态防御的数据保护安全架构研究[D]. 郑州: 郑州大学, 2019.)

[45] Li C Y. File protection method based on mimic defense and countermeasure test[D]. Zhengzhou: Zhengzhou University, 2019.
(李超洋. 基于拟态防御的文件保护方法及对抗测试[D]. 郑州: 郑州大学, 2019.)

[46] Wan S X, Zhao Y, Wu C R. Evaluation and Demonstration of Network Attack Resistance of Mimetic Database[J]. *Computer Applications and Software*, 2022, 39(1): 319-327.
(万仕贤, 赵瑜, 吴承荣. 拟态数据库的网络攻击抵御能力评估和实证[J]. *计算机应用与软件*, 2022, 39(1): 319-327.)

[47] Song Ke, Liu Qinrang, Wei Shuai, et al. Based on the proposed protection device endogenous safety state structure system[J]. *Journal of Communications*, 2020, 41(05): 18-26.
(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(05): 18-26.)

[48] Pan C X, Zhang Z, Ma B L, et al. Method Against Process Control-Flow Hijacking Based on Mimic Defense[J]. *Journal on Communications*, 2021, 42(1): 37-47.
(潘传幸, 张铮, 马博林, 等. 面向进程控制流劫持攻击的拟态防御方法[J]. *通信学报*, 2021, 42(1): 37-47.)

[49] 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.
(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.)

[50] Yang W J, Liu X Y, Zhang Y, et al. A Method for Arbitration and Scheduling of Mimicry Industrial Controllers[J]. *Journal of Information Security Research*, 2022, 8(6): 534-544.
(杨汶佼, 刘星宇, 张奕, 等. 一种针对拟态工业控制器的裁决及调度方法[J]. *信息安全研究*, 2022, 8(6): 534-544.)

[51] Ji X S, Liang H, Hu H C. New Thoughts on Security Technologies for Space-Ground Integration Information Network[J]. *Telecommunications Science*, 2017, 33(12): 24-35.
(季新生, 梁浩, 扈红超. 天地一体化信息网络安全防护技术的新思考[J]. *电信科学*, 2017, 33(12): 24-35.)

[52] Chen S X, Jiang X Y, Cai J J, et al. Research on Mimic Security Gateway Technology Based on Attack Diversion Model[J]. *Journal on Communications*, 2018, 39(S2): 72-78.
(陈双喜, 姜鑫悦, 蔡晶晶, 等. 基于攻击转移的拟态安全网关技术的研究[J]. *通信学报*, 2018, 39(S2): 72-78.)

[53] Ling Y, Yu X S, Xu L D, et al. Application of Mimicry Defense Technology in the Construction of Government Portal Website[J]. *Network Security Technology & Application*, 2022(5): 117-118.
(凌颖, 余新胜, 徐李定, 等. 拟态防御技术在政府门户网站建设中的应用[J]. *网络安全技术与应用*, 2022(5): 117-118.)

[54] Zhu W J, Fan Y W, Ban S H. Designing Security Architecture of Total Ship Computing Environment Based on Mimic Defense[J]. *Digital Technology and Application*, 2018, 36(1): 203-205.
(朱维军, 樊永文, 班绍桓. 基于拟态防御机制的全舰计算环境

安全架构设计[J]. *数字技术与应用*, 2018, 36(1): 203-205.)

[55] Lv Z Y, Chen L, Feng M, et al. Application of Mimic Security Defense on Enterprise Network Security[J]. *Journal of Chinese Computer Systems*, 2019, 40(1): 69-76.
(吕志远, 陈靓, 冯梅, 等. 拟态防御理论在企业内网安全防护中的应用[J]. *小型微型计算机系统*, 2019, 40(1): 69-76.)

[56] Xi Z S, Zhang B, Sun X, et al. Research on Mimic Defence Technology for Smart Unit Application Environment of Power Grid[J]. *Journal of Physics*: *Conference Series*, 2019, 1314(1): 012026.

[57] Sun X, Li Q Y, Zhou S, et al. Research on Mimic Defense Technology and Security Test Method of Electric Power Web Service System[J]. *IOP Conference Series*: *Materials Science and Engineering*, 2019, 569(4): 042011.

[58] Tang Z Y. Discussion on Inherent Security Technology and Application of Power Monitoring System[J]. *Automation Panorama*, 2022, 39(1): 22-25.
(汤震宇. 电力监控系统内生安全技术及应用探讨[J]. *自动化博览*, 2022, 39(1): 22-25.)

[59] Chang X L, Fan Y W, Zhu W J, et al. Management Information System Based on Mimic Defense[J]. *Computer Science*, 2019, 46(S2): 438-441.
(常啸林, 樊永文, 朱维军, 等. 基于拟态防御的管理信息系统[J]. *计算机科学*, 2019, 46(S2): 438-441.)

[60] Zhang Yongzhuang. Research and implementation of management control system based on redundant heterogeneous architecture[D]. Beijing: Beijing University of Posts and Telecommunications, 2021.
(张永壮. 基于冗余异构架构的管理控制系统的研究与实现[D]. 北京: 北京邮电大学, 2021.)

[61] Chen P, Su M C, Chen H X, et al. Research on Mimicry Defense Design of Internet of Vehicles System Based on Reinforcement Learning[J]. *Journal of Information Security Research*, 2022, 8(6): 545-553.
(陈平, 苏牧辰, 陈浩贤, 等. 基于强化学习的车联网系统拟态防御设计研究[J]. *信息安全研究*, 2022, 8(6): 545-553.)

[62] Ni X B, Liu J F. Application and Analysis of Mimicry Defense Technology in UAV Flight Control Field[J]. *Network Security Technology & Application*, 2022(2): 128-129.
(倪晓波, 刘进芬. 拟态防御技术在无人机飞控领域的应用与分析[J]. *网络安全技术与应用*, 2022(2): 128-129.)

[63] Pang J M, Zhang Y J, Zhang Z, et al. Applying a Combination of Mimic Defense and Software Diversity in the Software Security Industry[J]. *Strategic Study of CAE*, 2016, 18(6): 74-78.
(庞建民, 张宇嘉, 张铮, 等. 拟态防御技术结合软件多样化在软件安全产业中的应用[J]. *中国工程科学*, 2016, 18(6): 74-78.)

[64] Zhang Y J, Pang J M, Zhang Z, et al. Mimic Security Defence Strategy Based on Software Diversity[J]. *Computer Science*, 2018, 45(2): 215-221.
(张宇嘉, 庞建民, 张铮, 等. 基于软件多样化的拟态安全防御策略[J]. *计算机科学*, 2018, 45(2): 215-221.)

[65] Yan X C, Chen Y, Jia H Y, et al. Secure Data Sharing Scheme Supporting Efficient Synchronous Evolution for Ciphertext and Key[J]. *Journal on Communications*, 2018, 39(5): 123-133.
(严新成, 陈越, 贾洪勇, 等. 支持高效密文密钥同步演化的安全数据共享方案[J]. *通信学报*, 2018, 39(5): 123-133.)

[66] Hu Fei. Security processing and analysis of system security[D]. Sichuan: University of Electronic Science and Technology of China,2019.
(胡菲. 安全处理容器及系统安全性分析[D]. 四川: 电子科技大学, 2019.)

[67] Guo J L, Xu M Y, Yuan H Y, et al. Introduction of Endogenous Security of Zero Trust Model[J]. *Journal of Zhengzhou University* (*Natural Science Edition*), 2022, 54(6): 51-58.
(郭军利, 许明洋, 原浩宇, 等. 引入内生安全的零信任模型[J]. *郑州大学学报(理学版)*, 2022, 54(6): 51-58.)

[68] Zhang Mengyu. Research on new software watermarking MDW algorithm based on mimic defense[D]. Zhengzhou: Zhengzhou University, 2017.
(张梦宇. 基于拟态防御的新型软件水印 MDW 算法研究[D]. 郑州: 郑州大学, 2017.)

[69] Ji X S, Huang K Z, Jin L, et al. Overview of 5G Security Technology[J]. *Science China Information Sciences*, 2018, 61(8): 081301.

[70] Liu C X, Ji X S, Wu J X. A Mimic Defense Mechanism for Mobile Communication User Data Based on MSISDN Virtualization[J]. *Chinese Journal of Computers*, 2018, 41(2): 275-287.
(刘彩霞, 季新生, 邬江兴. 一种基于 MSISDN 虚拟化的移动通信用户数据拟态防御机制[J]. *计算机学报*, 2018, 41(2): 275-287.)

[71] Ban S H, Han Y J, Fan Y W, et al. QR Code Information Encryption Architecture Based on Mimic Defense[J]. *Journal of Chinese Computer Systems*, 2020, 41(4): 673-678.
(班绍桓, 韩英杰, 樊永文, 等. 基于拟态防御的QR码信息加密架构[J]. *小型微型计算机系统*, 2020, 41(4): 673-678.)

[72] Zhou Q L, Ban S H, Han Y J, et al. Mimic Defense Authentication Method for Physical Access Control[J]. *Journal on Communications*, 2020, 41(6): 80-87.
(周清雷, 班绍桓, 韩英杰, 等. 针对物理访问控制的拟态防御认证方法[J]. *通信学报*, 2020, 41(6): 80-87.)

[73] Ban Shaohuan. An applied research on mimic defense application in QR code encryption and physical access control[D]. Zhengzhou: Zhengzhou University,2020.
(班绍桓. 拟态防御在 QR 码加密和物理访问控制中的应用研究[D]. 郑州: 郑州大学, 2020.)

[74] Yu C, Chen L Q, Lu T Y. M2M Network Anonymous Attestation Scheme Based on Mimic Defense[J]. *Journal of Cryptologic Research*, 2021, 8(3): 468-477.
(郁晨, 陈立全, 陆天宇. 一种融合拟态防御的 M2M 远程匿名认证方案[J]. *密码学报*, 2021, 8(3): 468-477.)

[75] Zhang Shuangshuang, Bu Youjun, Chen Bo, et al. Research and design of a mimic web honeypot[J]. *Industrial Control Computer*, 2022, 35(01): 78-80.
(张双双, 卜佑军, 陈博, 等. 拟态 Web 蜜罐的研究与设计[J]. *工业控制计算机*, 2022, 35(01): 78-80.)

[76] Lu Xiangyu. Design and implementation of active defense enhanced honeynet system[D]. Henan: Information Engineering University, 2022.
(路祥雨. 主动防御增强的蜜网系统设计与实现[D]. 河南: 战略支援部队信息工程大学, 2022.)

[77] Zhu L L, Chen H Z, Cheng L F, et al. Anomaly Detection Architecture for Network Traffic Flow under Mimic Defense[J]. *Journal of Fuzhou University* (*Natural Science Edition*), 2022, 50(3): 293-300.
(朱龙隆, 陈翰泽, 程灵飞, 等. 拟态防御下的网络流量异常检测架构[J]. *福州大学学报(自然科学版)*, 2022, 50(3): 293-300.)

[78] Zhang Q, Liu C X. A "Dynamic Tunnel" defense Method Based on GTP Protocol[J]. *Application Research of Computers*, 2016, 33(11): 3442-3445.
(张青, 刘彩霞. 一种基于 GTP 协议的"动态隧道" 防御方法[J]. *计算机应用研究*, 2016, 33(11): 3442-3445.)

[79] Liu W Y, Chen F C, Hu H C, et al. A Novel Framework for Zero-Day Attacks Detection and Response with Cyberspace Mimic Defense Architecture[C]. *2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, 2017: 50-53.

[80] Li B, Zhou Q L, Si X M, et al. Mimic Encryption System for Network Security[J]. *IEEE Access*, 2018, 6: 50468-50487.

[81] Fu L, Shao P N, Ying F, et al. Framework Design of Mimic Common Operating Environment[J]. *Computer Engineering*, 2020, 46(3): 24-33.
(付琳, 邵培南, 应飞, 等. 拟态通用运行环境的框架设计[J]. *计算机工程*, 2020, 46(3): 24-33.)

[82] Zhou X B, Li B, Qi Y R, et al. Mimic Encryption Box for Network Multimedia Data Security[J]. *Security and Communication Networks*, 2020, 2020(1): 8868672.

[83] Yang K, Zhang F, Guo W, et al. A Method for Solving the Metadata Randomness Problem of Mimic Storage[J]. *Computer Engineering*, 2022, 48(2): 140-146, 155.
(杨珂, 张帆, 郭威, 等. 一种拟态存储元数据随机性问题解决方法[J]. *计算机工程*, 2022, 48(2): 140-146, 155.)

[84] Cui J, Xie L W, Ding X J. Construction of Mimic Defense System Based on Red-Blue Confrontation[J]. *Telecom Engineering Technics and Standardization*, 2021, 34(12): 34-39.
(崔晶, 谢丽伟, 丁晓君. 基于红蓝对抗的拟态防御体系构建[J]. *电信工程技术与标准化*, 2021, 34(12): 34-39.)

[85] Yang Xinlin. Research on deepfake speech detection based on improved mimic defense[D]. Liaoning: Liaoning University, 2022.
(杨鑫林. 基于改进拟态防御的深度伪造语音检测研究[D]. 辽宁: 辽宁大学, 2022.)

[86] Zhu X Q, Yang D. Research and Analysis on Attack Detection of Mimic Defense System[J]. *Software*, 2022, 43(1): 105-107.
(朱绪全, 杨盾. 拟态防御体系攻击检测研究与分析[J]. *软件*, 2022, 43(1): 105-107.)

[87] Wu Z Q, Wei J. Heterogeneous Executors Scheduling Algorithm for Mimic Defense Systems[C]. *2019 IEEE 2nd International Conference on Computer and Communication Engineering Technology*, 2019: 279-284.

[88] 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.
(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.)

[89] Ye Shengzhao. Research on the key technologies of mimic- structure-based heterogeneous processing system[D]. Henan: Information Engineering University, 2019.
(叶盛钊. 基于拟态构造的异构处理系统关键技术研究[D]. 河南: 战略支援部队信息工程大学, 2019.)

[90] 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.

[91] Sang Xiaonan. Research on Dynamic Scheduling Algorithm for Mimic Defense Architecture[D]. Jiangsu: Nanjing University of Science and Technology,2020.
(桑笑楠. 面向拟态防御架构的动态调度算法研究[D]. 江苏: 南京理工大学, 2020.)

[92] Ji Z, Gao M, Ying L. Research on Dynamic Scheduling Decision Algorithm in Mimic Defense[J]. *Telecommunications and Radio Engineering*, 2020, 79(17): 1563-1578.

[93] Zhang W J, Wei S, Tian L, et al. Scheduling Algorithm Based on Heterogeneity and Confidence for Mimic Defense[J]. *Journal of Web Engineering*, 2020, 19(7–8): 971-998.

[94] Chen G X, Shi G, Chen L Q, et al. A Novel Model of Mimic Defense Based on Minimal L-Order Error Probability[J]. *IEEE Access*, 2020, 8: 180481-180490.

[95] Yang L, Wang Y J, Zhang J. FAWA: A Negative Feedback Dynamic Scheduling Algorithm for Heterogeneous Executor[J]. *Computer Science*, 2021, 48(8): 284-290.
(杨林, 王永杰, 张俊. FAWA: 一种异构执行体的负反馈动态调度算法[J]. *计算机科学*, 2021, 48(8): 284-290.)

[96] Chen Z X, Lu Y Q, Qin J C, et al. An Optimal Seed Scheduling Strategy Algorithm Applied to Cyberspace Mimic Defense[J]. *IEEE Access*, 2021, 9: 129032-129050.

[97] Jia H Y, Pan Y F, Liu W H, et al. Executive Dynamic Scheduling Algorithm Based on High-Order Heterogeneity[J]. *Journal on Communications*, 2022, 43(3): 233-245.
(贾洪勇, 潘云飞, 刘文贺, 等. 基于高阶异构度的执行体动态调度算法[J]. *通信学报*, 2022, 43(3): 233-245.)

[98] 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.
(王晓梅, 杨文晗, 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.)

[99] 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.
(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.)

[100] 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.
(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.)

[101] Qiu D H, Li H, Sun J L. Measuring Software Similarity Based on Structure and Property of Class Diagram[C]. *2013 Sixth International Conference on Advanced Computational Intelligence*, 2013: 75-80.

[102] 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.
(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.)

[103] Wang Zhenpeng. Research on the scheduling and decision-making mechanism of mimic network operating system[D]. Henan: Information Engineering University, 2017.
(王禛鹏. 拟态网络操作系统调度与裁决机制研究及实现[D]. 河南: 战略支援部队信息工程大学, 2017.)

[104] Lv Yingying. Research on the key technologies of mimic SDN controller architecture security[D]. Henan: Information Engineering University, 2018.
(吕迎迎. 拟态 SDN 控制器架构安全关键技术研究[D]. 河南: 战略支援部队信息工程大学, 2018.)

[105] 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.
(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.)

[106] Zhou M L, Chen F C, Liu W Y, et al. Negative Feedback Dynamic Scheduling Algorithm Based on Mimic Defense in Cloud Environment[C]. *2020 IEEE 6th International Conference on Computer and Communications*, 2020: 2265-2270.

[107] Zeng W, Hu H C, Zhou D C. A Security SLA Negotiation Mechanism Oriented to Mimic Cloud[C]. *2021 International Conference on Machine Learning and Intelligent Systems Engineering*, 2021: 195-202.

[108] Li Q M, Meng S M, Sang X N, et al. Dynamic Scheduling Algorithm in Cyber Mimic Defense Architecture of Volunteer Computing[J]. *ACM Transactions on Internet Technology*, 2021, 21(3): 1-33.

[109] Huo L T, Shao P N, Ying F, et al. The Research on Task Scheduling Algorithm for the Cloud Management Platform of Mimic Common Operating Environment[C]. *2019 18th International Symposium on Distributed Computing and Applications for Business Engineering and Science*, 2019: 167-171.

[110] Yu F, Liu K, Geng Y Y, et al. Multi Executor Decision Algorithm and Scheduling Algorithm Based on Differential Distance Feedback[J]. *Application Research of Computers*, 2022, 39(5): 1437-1443.
(余飞, 刘可, 耿洋洋, 等. 基于差异距离反馈的多执行体裁决算法与调度算法[J]. *计算机应用研究*, 2022, 39(5): 1437-1443.)

[111] Lin S J, Liu Q R, Wang X L. Competitive Arbitration Model for Mimic Defense System[J]. *Computer Engineering*, 2018, 44(4): 193-198.
(林森杰, 刘勤让, 王孝龙. 面向拟态防御系统的竞赛式仲裁模型[J]. *计算机工程*, 2018, 44(4): 193-198.)

[112] Wu Z Q, Zhang F, Guo W, et al. A Mimic Arbitration Optimization Method Based on Heterogeneous Degree of Executors[J]. *Computer Engineering*, 2020, 46(5): 12-18.
(武兆琪, 张帆, 郭威, 等. 一种基于执行体异构度的拟态裁决优化方法[J]. *计算机工程*, 2020, 46(5): 12-18.)

[113] Wei S, Zhang H H, Zhang W J, et al. Conditional Probability Voting Algorithm Based on Heterogeneity of Mimic Defense System[J]. *IEEE Access*, 2020, 8: 188760-188770.

[114] Guo W, Zhang F, Wu Z Q, et al. Confidence Skewing Problem and Its Correction Method in Mimic Arbitration Mechanism[J]. *Chinese Journal of Electronics*, 2020, 29(3): 547-553.

[115] Wei S, Zhang H H, Su Y, et al. Majority Voting Algorithm Based on High-Order Heterogeneity for Mimic Defense System[J]. *Computer Engineering*, 2021, 47(5): 30-35.
(魏帅, 张辉华, 苏野, 等. 面向拟态防御系统的高阶异构度大数判决算法[J]. *计算机工程*, 2021, 47(5): 30-35.)

[116] Gao Z B, Jia G R, Zhang W J, et al. Mimic Ruling Optimization Method Based on Executive Outliers[J]. *Application Research of Computers*, 2021, 38(7): 2066-2071.
(高振斌, 贾广瑞, 张文建, 等. 基于异常值的拟态裁决优化方法[J]. *计算机应用研究*, 2021, 38(7): 2066-2071.)

[117] Lu Y Q, Huang J X, Cheng Z, et al. A Multi-Index Mimic Voting Algorithm Based on Improved AHP-FCE Model[J]. *Journal of Beijing University of Posts and Telecommunications*, 2021, 44(2): 8-13.
(陆以勤, 黄俊贤, 程喆, 等. 基于改进 AHP-FCE 模型的多指标拟态表决算法[J]. *北京邮电大学学报*, 2021, 44(2): 8-13.)

[118] Zhou D C, Chen H C, Cheng G Z, et al. Design and Implementation of Adaptive Mimic Voting Device Oriented to Persistent Connection[J]. *Journal on Communications*, 2022, 43(6): 71-84.
(周大成, 陈鸿昶, 程国振, 等. 面向持久性连接的自适应拟态表决器设计与实现[J]. *通信学报*, 2022, 43(6): 71-84.)

[119] Liang Huibing. Research on some key technologies in mimicry defense System[D]. Hangzhou: Hangzhou Dianzi University, 2018.
(梁惠兵. 拟态主动防御若干关键技术研究[D]. 杭州: 杭州电子科技大学, 2018.)

[120] Lei R, Li C H, Tang Z Y. Openflow Table Decision Method under Mimic Defense[J]. *Journal of Physics*: *Conference Series*, 2020, 1584(1): 012055.

[121] Wu Z J, Yao Q, Feng S F, et al. Optimization Scheme of Competitive Arbitration Based on Binary Database Log[J]. *Computer Engineering*, 2021, 47(5): 24-29.
(吴正江, 姚琪, 冯四风, 等. 基于数据库二进制日志的竞赛式仲裁优化方案[J]. *计算机工程*, 2021, 47(5): 24-29.)

[122] Dai Renjie. Research on voting mechanism of MCOE[D]. Beijing: China Academic of Electronics and Information Technology, 2022.
(戴人杰. 拟态通用运行环境裁决机制研究[D]. 北京: 中国电子科技集团公司电子科学研究院, 2022.)

[123] Lin S J, Liu Q R, Wu Y T, et al. A Self-Adaptive Timeout Mechanism in Mimic Defense System[C]. *2017 8th IEEE International Conference on Software Engineering and Service Science*, 2017: 588-591.

[124] Nie D L, Zhao B, Wang C, et al. Timeout Threshold Estimation Algorithm in Mimic Multiple Executors Architecture[J]. *Chinese Journal of Network and Information Security*, 2018, 4(10): 68-76.
(聂德雷, 赵博, 王崇, 等. 拟态多执行体架构下的超时阈值计算方法[J]. *网络与信息安全学报*, 2018, 4(10): 68-76.)

[125] 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.
(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.)

[126] Zhao Y F, Zhang Z, Nie G L, et al. An Improved Model of Mimic Defense Architecture Adding Heterogeneous Evaluation[C]. *2020 IEEE 9th Joint International Information Technology and Artificial Intelligence Conference*, 2020: 2094-2098.

[127] Wu T, Hu C N, Chen Q N, et al. Defense-Enhanced Dynamic Heterogeneous Redundancy Architecture Based on Executor Partition[J]. *Journal on Communications*, 2021, 42(3): 122-134.
(吴铤, 胡程楠, 陈庆南, 等. 基于执行体划分的防御增强型动态异构冗余架构[J]. *通信学报*, 2021, 42(3): 122-134.)

[128] Yang Z Y, Chen L Q. A Traceable Anonymous Authentication Method for Mimic Defense[C]. *2021 IEEE 5th Advanced Information Technology*, *Electronic and Automation Control Conference*, 2021: 1831-1836.

[129] Chen Z Q, Cui G, Zhang L, et al. Optimal Strategy for Cyberspace Mimic Defense Based on Game Theory[J]. *IEEE Access*, 2021, 9: 68376-68386.

[130] Gu Z Y, Zhang X M, Wei S. Adaptive Dynamic Defense Mechanism Based on Reinforcement Learning[J]. *Journal of Chinese Computer Systems*, 2019, 40(2): 401-406.
(顾泽宇, 张兴明, 魏帅. 基于增强学习的自适应动态防御机制[J]. *小型微型计算机系统*, 2019, 40(2): 401-406.)

[131] Zhang Q Q, Tang H B, You W, et al. Dynamic Scheduling Strategy of NFV Mimic Defense Architecture Based on Evolutionary Game[J]. *Computer Engineering*, 2022, 48(4): 30-38, 49.
(张青青, 汤红波, 游伟, 等. 基于演化博弈的 NFV 拟态防御架构动态调度策略[J]. *计算机工程*, 2022, 48(4): 30-38, 49.)

[132] Zhang Qinging, Tang Hongbo, You Wei, et al. Dynamic scheduling strategy of NFV mimic defense architecture based on evolutionary game[J]. *Computer Engineering*, 2022, 48(04): 30-38+49.
(张青青, 汤红波, 游伟, 等. 基于演化博弈的 NFV 拟态防御架构动态调度策略[J]. *计算机工程*, 2022, 48(04): 30-38+49.)

[133] Zhang X M, Gu Z Y, Wei S, et al. Markov Game Modeling of Mimic Defense and Defense Strategy Determination[J]. *Journal on Communications*, 2018, 39(10): 143-154.
(张兴明, 顾泽宇, 魏帅, 等. 拟态防御马尔可夫博弈模型及防御策略选择[J]. *通信学报*, 2018, 39(10): 143-154.)

[134] Ding S H, Qi N, Guo Y W. Evaluation of Mimic Defense Strategy Based on M-FlipIt Game Model[J]. *Journal on Communications*, 2020, 41(7): 186-194.
(丁绍虎, 齐宁, 郭义伟. 基于 M-FlipIt 博弈模型的拟态防御策略评估[J]. *通信学报*, 2020, 41(7): 186-194.)

[135] Wang W, Zeng J J, Li G S, et al. Security Analysis of Dynamic Heterogeneous Redundant System[J]. *Computer Engineering*, 2018, 44(10): 42-45, 50.
(王伟, 曾俊杰, 李光松, 等. 动态异构冗余系统的安全性分析[J]. *计算机工程*, 2018, 44(10): 42-45, 50.)

[136] Zheng Q H, Hu C N, Cui T T, et al. A Security Analysis Approach for Dynamic Heterogeneous Redundancy Model Based on Probability Analysis[J]. *Acta Electronica Sinica*, 2021, 49(8): 1586-1598.
(郑秋华, 胡程楠, 崔婷婷, 等. 一种基于概率分析的 DHR 模型安全性分析方法[J]. *电子学报*, 2021, 49(8): 1586-1598.)

[137] Zhu W J, Guo Y B, Huang B H. A Mimic Defense Automaton Model of Dynamic Heterogeneous Redundancy Structures[J]. *Acta Electronica Sinica*, 2019, 47(10): 2025-2031.
(朱维军, 郭渊博, 黄伯虎. 动态异构冗余结构的拟态防御自动机模型[J]. *电子学报*, 2019, 47(10): 2025-2031.)

[138] Wang T, Xiang L L, Chen T M. Time Automata Model and Verification of Mimic Defense System[J]. *Journal of Chinese Computer Systems*, 2020, 41(8): 1718-1724.
(王婷, 项露露, 陈铁明. 拟态防御系统的时间自动机模型和验证[J]. *小型微型计算机系统*, 2020, 41(8): 1718-1724.)

[139] Li Q Y, Han J J, Sun X, et al. Mimic Defense System Security Analysis Model[J]. *Journal of Physics*: *Conference Series*, 2019, 1187(5): 052038.

[140] Zhao Y F, Zhang Z, Tang Y, et al. A Security Quantification Method for Mimic Defense Architecture[C]. *2021 IEEE 5th Advanced Information Technology*, *Electronic and Automation Control Conference*, 2021: 36-40.

[141] Tong Q, Guo Y F. A Comprehensive Evaluation of Diversity Systems Based on Mimic Defense[J]. *Science China Information Sciences*, 2021, 64(12): 229304.

[142] Zhao Y F, Wang J C, Zhang J X. A Comprehensive Quality of Service Evaluation in Mimic System[C]. *2019 IEEE 8th Joint International Information Technology and Artificial Intelligence Conference*, 2019: 986-991.

[143] Yao Y, Pan C X, Zhang Z, et al. Method of Quantitative Assessment for Diversified Software System[J]. *Journal on Communications*, 2020, 41(3): 120-125.
(姚远, 潘传幸, 张铮, 等. 多样化软件系统量化评估方法[J]. *通信学报*, 2020, 41(3): 120-125.)

[144] Yang X, Li H, Wu J X, et al. A Two-Dimension Security Assessing Model for CMDS Combined with Generalized Stochastic Petri Net[J]. *Scientia Sinica* (*Informationis*), 2020, 50(12): 1944-1960.
(杨昕, 李挥, 邬江兴, 等. 融合广义随机 Petri 网的二维拟态安全评估模型[J]. *中国科学: 信息科学*, 2020, 50(12): 1944-1960.)

[145] Yang Xin, Li Hui, Wu Jiangxing, et al. Two-dimensional state model incorporating roughly broad anytime secure Petri nets[J]. *Science China Information Sciences*, 2020, 50(12): 1944-1960.
(杨昕, 李挥, 邬江兴, 等. 融合广义随机 Petri 网的二维拟态安全评估模型[J]. *中国科学:信息科学*, 2020, 50(12): 1944-1960.)

[146] Feng Feng. Research on modeling for mimic defense and mimic defense organization structure in application layer contain method of evaluation security level[D]. Zhengzhou: Zhengzhou University, 2019.
(冯峰. 拟态防御建模与应用层体系结构及安全评估方法研究[D]. 郑州: 郑州大学, 2019.)

[147] Zhang Z, Ma B L, Wu J X. The Test and Analysis of Prototype of Mimic Defense in Web Servers[J]. *Journal of Cyber Security*, 2017, 2(1): 13-28.
(张铮, 马博林, 邬江兴. web 服务器拟态防御原理验证系统测试与分析[J]. *信息安全学报*, 2017, 2(1): 13-28.)

[148] Web Server Mimic Defense Principle Verification System. Technical Report, National Digital Switching System Engineering Technology Research Center, 2015.
(Web 服务器拟态防御原理验证系统. 技术报告, 国家数字交换系统工程技术研究中心, 2015.)

[149] Zhang J X, Pang J M, Zhang Z, et al. QoS Quantification Method

for Web Server with Mimic Construction[J]. *Computer Science*, 2019, 46(11): 109-118.
(张杰鑫, 庞建民, 张铮, 等. 拟态构造 Web 服务器的服务质量量化方法[J]. *计算机科学*, 2019, 46(11): 109-118.)

[150] Zhang J X, Pang J M, Zhang Z. Quantification Method for Heterogeneity on Web Server with Mimic Construction[J]. *Journal of Software*, 2020, 31(2): 564-577.
(张杰鑫, 庞建民, 张铮. 拟态构造的 Web 服务器异构性量化方法[J]. *软件学报*, 2020, 31(2): 564-577.)

[151] 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.
(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.)

[152] 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.
(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.)

[153] Ren Q, Wu J X, He L. Performance Modeling Based on GSPN for Cyberspace Mimic DNS[J]. *Chinese Journal of Electronics*, 2020, 29(4): 738-749.

[154] He L, Ren Q, Ma B L, et al. Anti-Attacking Modeling and Analysis of Cyberspace Mimic DNS[J]. *China Communications*, 2022, 19(5): 218-230.

[155] Pu L M, Wu J X, Ma H L, et al. MimicCloudSim: An Environment for Modeling and Simulation of Mimic Cloud Service[J]. *China Communications*, 2021, 18(1): 212-221.

[156] Feng F, Zhou X B, Li B, et al. Modelling the Mimic Defence Technology for Multimedia Cloud Servers[J]. *Security and Communication Networks*, 2020, 2020(1): 8819958.

[157] Zhu W J, Fan Y W, Ban S H. A Mimic-Automaton-Based Model for the MSISDN Virtualization and Its Method for Verifying the Security[J]. *Netinfo Security*, 2018, 18(4): 15-22.
(朱维军, 樊永文, 班绍桓. 动态虚拟 MSISDN 的拟态自动机模型与安全性验证方法[J]. *信息网络安全*, 2018, 18(4): 15-22.)

[158] Zhang B, Li W C, Sun X, et al. Mimic Defense Structured Information System Threat Identification and Centralized Control[J]. *Journal of Physics*: *Conference Series*, 2019, 1187(3): 032102.

[159] Li W C, Zhang Z, Wang L Q, et al. The Modeling and Risk Assessment on Redundancy Adjudication of Mimic Defense[J]. *Journal of Cyber Security*, 2018, 3(5): 64-74.
(李卫超, 张铮, 王立群, 等. 基于拟态防御架构的多余度裁决建模与风险分析[J]. *信息安全学报*, 2018, 3(5): 64-74.)

李炳萱 于 2021 年在天津大学计算机科学与技术专业获得学士学位。现在天津大学计算机技术专业攻读硕士学位。研究领域为网络信息安全。研究兴趣包括: 网络空间拟态防御、人工智能安全。CCF 学生会员。Email: libingxuan0_0@163.com

陈世展 于 2010 年在天津大学计算机应用专业获得博士学位。现任天津大学智能与计算学部教授。研究领域为软件工程、服务计算。研究兴趣包括: 服务计算、软件生态系统挖掘与分析。Email: shizhan@tju.edu.cn

许光全 于 2008 年在天津大学计算机应用技术专业获得博士学位。现任天津大学智能与计算学部教授。研究领域为网络信息安全。研究兴趣包括: 移动安全、物联网安全、人工智能与安全、信任管理。Email: Losin@tju.edu.cn

贾云刚 于 2005 年在南开大学软件工程专业获得硕士学位。现任国家计算机网络应急技术处理协调中心天津分中心高级工程师。研究领域为网络信息安全。研究兴趣包括: 物联网安全、人工智能安全、大数据分析和处理。Email: jiayungang@cert.org.cn

王聪 于 2017 年在天津大学计算机应用技术专业获得博士学位。现任天津大学智能与计算学部讲师。研究领域为网络信息安全。研究兴趣包括: 网络安全与认证方案设计、物联网安全。Email: wangcongjcdd@163.com

薛飞 于 2017 年在天津大学电气工程专业获得硕士学位。现任国网宁夏电力有限公司电力科学研究院工程师。研究领域为人工智能与新能源发电。研究兴趣包括: 人工智能、区块链、新能源并网仿真技术。Email:tjuxf1010@126.com

王晓 于 2019 年在北京工业大学计算机科学与技术专业获得博士学位。现为天津大学智能与计算学部博士后。研究领域为网络信息安全。研究兴趣包括: 可信计算、人工智能安全、云计算安全、隐私计算、区块链安全与应用。Email: wangxiao8343@163.com

王伟 于 2006 年在西安交通大学控制科学与工程专业获得博士学位。现任北京交通大学单位计算机与信息技术学院教授。研究领域为网络信息安全。研究兴趣包括: 隐私保护计算理论与技术、区块链安全与应用、人工智能安全、智能物联网安全。Email: wangwei1@bjtu.edu.cn

李哲涛 于 2010 年在湖南大学计算机应用专业获得博士学位。现任暨南大学信息科学技术学院教授。研究领域为物联网、网络空间安全、人工智能。研究兴趣包括: 物联网、网络空间安全、人工智能。Email: liztchina@hotmail.com

李建欣 于 2008 年在北京航空航天大学计算机软件与理论专业获得博士学位。现任北京航空航天大学计算机学院教授。研究领域为大数据分析与处理、机器学习和可信计算。研究兴趣包括: 大数据分析与处理、机器学习和可信计算。Email: lijx@buaa.edu.cn