研究与开发

ARDR：融合自适应选择与证据推理的拟态防御鲁棒决策架构

郑秋华[1,2]，孙振宇[1,2]，章坚武[3]，徐李定[4]，周迪[1,2]，程传慧[5]

（1. 杭州电子科技大学网络空间安全学院， 浙江 杭州 310018；
2. 浙江省全省敏感数据安全保护与保密治理重点实验室， 浙江 杭州 310018；
3. 杭州电子科技大学通信工程学院， 浙江 杭州 310018；
4. 中国电子科技集团第32研究所， 上海 201808；
5. 中南财经政法大学信息工程学院， 湖北 武汉 430073）

摘　要：动态异构冗余（dynamic heterogeneous redundancy，DHR）架构虽能增强系统弹性与容错，但基于多数表决的决策机制难以处理异构信息源的质量差异与潜在冲突，在关键安全场景中易导致性能下降或误判。为此，提出一种自适应与鲁棒决策冗余（adaptive & robust decision redundancy，ARDR）架构，通过自适应服务选择与基于证据的鲁棒裁决，实现对异构执行体输出的系统化评估与融合。ARDR构建综合评估模型，结合执行体异构性、历史性能、置信度及效率，利用鲸鱼优化算法选取最优组合；随后基于Dempster-Shafer理论设计高冲突感知裁决框架处理不确定性。拟态Web应用防火墙原型及多场景仿真实验结果表明，ARDR在准确率、F2值及平均执行时间上均优于传统动态异构冗余及防御增强型动态异构冗余（improved dynamic heterogeneous redundancy，IDHR）架构，尤其在高冗余与高冲突条件下性能稳定。消融实验进一步证明其自适应选择与鲁棒裁决的协同效应，为异构高不确定性环境下冗余系统设计提供可解释的高效方案。

关键词：动态异构冗余；拟态防御；自适应服务选择；证据融合；不确定性推理；移动目标防御

中图分类号：TP393.08；TN918.1

文献标志码：A

doi: 10.11959/j.issn.1000−0801.DXKX250636

ARDR: an adaptive service selection and robust decision framework for heterogeneous executor

Zheng Qiuhua[1,2], Sun Zhenyu[1,2], Zhang Jianwu[3], Xu Liding[4], Zhou Di[1,2], Cheng Chuanhui[5]

1. School of Cyberspace, Hangzhou Dianzi University, Hangzhou 310018, China
2. Zhejiang Provincial Key Laboratory for Sensitive Data Security Protection and Confidentiality Management, Hangzhou 310018, China
3. College of Communication Engineering, Hangzhou Dianzi University, Hangzhou 310018, China

收稿日期：2025−10−30；**修回日期：**2026−01−22

通信作者：周迪，zhoudi@hdu.edu.cn

基金项目：浙江省尖兵领雁项目（No.2023C01025）；浙江省全省敏感数据安全保护与保密治理重点实验室项目（No.2024E10048）

Foundation Items: Zhejiang “Pioneer” and “Leading Goose” Research & Development Program(No.2023C01025), Zhejiang Provincial Key Laboratory for Sensitive Data Security Protection and Confidentiality Management(No. 2024E10048)

4. The 32nd Research Institute of China Electronics Technology Group Corporation, Shanghai 201808, China
5. School of Information Engineering, Zhongnan University of Economics and Law, Wuhan 430073, China

Abstract: Dynamic heterogeneous redundancy (DHR) architectures enhance system resilience but majority-voting decisions struggle with heterogeneous source quality and potential conflicts, leading to performance drops or misjudgments in critical security scenarios. The adaptive and robust decision redundancy (ARDR) architecture was presented, which combined adaptive service selection with evidence-based robust decision-making to systematically evaluate and fuse heterogeneous executor outputs. ARDR employed a comprehensive evaluation model considering executor heterogeneity, historical performance, confidence, and efficiency, using the whale optimization Algorithm to select optimal combinations, and a dempster-shafer-based high-conflict-aware framework to handle uncertainty. Prototype and multi-scenario simulations show that ARDR outperforms conventional DHR and improved dynamic heterogeneous redundancy (IDHR) in accuracy, F2-score, and execution time, especially under high redundancy and conflict, with ablation studies confirming the synergy of adaptive selection and robust decision-making. The ablation study provides an interpretable and efficient solution for redundancy system design in heterogeneous, high-uncertainty environments.

Key words: dynamic heterogeneous redundancy, mimic defense, adaptive service selection, evidence fusion, uncertainty reasoning, moving target defense

0　引言

随着全球数字化转型的加速推进，金融、医疗和工业控制等关键基础设施日益依赖于复杂的信息系统。这种系统复杂性与开放性的同步增长显著加剧了网络安全风险，关键基础设施面临前所未有且愈发复杂的安全威胁。近年来，高级持续性威胁、零日漏洞以及供应链攻击等事件频发[1]，使得依赖精确防护边界与外围隔离的传统静态安全机制，在应对未知、隐蔽及持续性攻击时愈显乏力[2-3]。这些局限性严重制约了关键系统的安全韧性与持续可用性。

在此背景下，主动防御技术被认为是应对复杂威胁环境的潜在突破方向。通过引入动态性与操作不确定性，主动防御能够显著提高攻击成本和对抗复杂度，从而将防御姿态由“被动响应”转变为“主动博弈”[4-5]。其中，拟态防御（mimic defense，MD）[6-7]是该领域的代表性方法。其通过“动态变化、结构异构与功能冗余”三大特性，打破了传统“静态防御—静态攻击”的对抗模式，从而显著增强系统应对未知威胁与隐蔽攻击的内在弹性。

在拟态防御体系中，动态异构冗余（dynamic heterogeneous redundancy，DHR）是其核心运行机制之一[8]。DHR通过并行调度多个功能等价但实现方式异构的执行单元，并基于结果裁决实现动态执行路径的随机化与不确定性注入，从而提升系统对异常行为与未知攻击的防护能力。大量研究表明，DHR在应对未知漏洞和零日攻击的场景中表现出较强的鲁棒性，并在原型验证中取得了良好的防御效果[9-11]。

然而，DHR架构的关键瓶颈在于其核心裁决机制的局限性。该机制主要依赖于简单多数表决[12]，将所有执行体输出视作同质化投票单元，忽视了不同执行体在证据质量、置信度及信息强度上的差异。该机制将异构检测结果简化为“正确/错误”的二元判定，仅以计票结果作为最终裁决依据，难以充分建模复杂不确定性。在高异构性和信息冲突并存的环境下，这种过度简化不仅削弱了决策精度，还可能引发所谓的“冗余–性能悖论”，即冗余检测单元数量增加并未带来性能提升，反而导致整体性能退化。

针对传统DHR架构在裁决机制上的局限性，本文提出了一种自适应与鲁棒决策冗余（adap-

tive and robust decision redundancy，ARDR）框架，通过自适应执行体选择与基于证据的鲁棒裁决，实现对异构执行体输出的高效整合与稳健决策。具体而言，ARDR包含2项协同机制：一是自适应执行体选择机制，构建基于异构性、历史置信度、安全性与运行效率的四维综合评估模型，并通过鲸鱼优化算法动态调整指标权重，运行时自适应选取最优执行体子集，从源头提升证据质量；二是基于证据的鲁棒裁决机制，将裁决形式化为Dempster-Shafer（DS）不确定性推理任务[13]，通过多准则证据折扣策略和高冲突感知融合规则增强对高冲突证据的鲁棒性，并结合分层置信度评估与二次验证机制，进一步提升边界场景下裁决的精度与可解释性。

本文的主要贡献如下。

（1）提出并实现了ARDR框架，从机制层面系统性解决了传统DHR架构简单裁决导致的性能下降与误判风险问题。

（2）引入基于多维指标的动态服务体选择，首次在DHR架构中实现执行体的自适应组合，从源头提升决策源质量，增强系统适应性。

（3）设计了一种高冲突感知的DS证据裁决引擎，将裁决过程转换为不确定性推理，实现异构证据的鲁棒融合，有效缓解传统投票机制在高冲突场景下的脆弱性。

（4）通过拟态Web应用防火墙原型及多场景仿真系统，验证了ARDR在准确率、F2值（F2-score）和平均执行时间等指标上，相对于传统DHR/防御增强型动态异构冗余（improved dynamic heterogeneous redundancy，IDHR）架构的优异性。

（5）通过消融与参数敏感性分析，验证各子模块的独立与协同贡献，进一步证明了ARDR的理论创新性与工程应用价值。

1 相关工作

本节主要回顾DHR架构、多源信息融合以及主动防御中与智能裁决相关的研究工作。

1.1 动态异构冗余架构

动态异构冗余架构是拟态防御的核心支撑技术，其思想源自N-Variant执行系统[14-15]。该架构通过并行运行多个功能等价但实现方式异构的执行体，并在输出层通过裁决机制融合结果，有效缓解未知漏洞、潜在缺陷或恶意攻击引起的异常行为。凭借多样化冗余与动态调度能力，DHR已在车联网安全、工业物联网可靠性[16]及深度学习模型安全等领域展现出广泛应用前景。

然而，DHR的性能瓶颈集中在裁决机制上。裁决机制作为连接多执行体与系统输出的关键环节，直接影响冗余体系的一致性、容错能力及决策可靠性。现有设计多采用固定多数表决或一致同意策略[12]，通过对执行体输出的简单统计进行决策。尽管实现简便，但未充分考虑执行体在可信度、误差分布及任务敏感性等方面的差异，导致在动态环境、不确定输入或冲突证据下，系统的决策稳定性和准确性下降。

为缓解这一问题，部分研究提出了IDHR[9]及基于随机种子最小相似度（random seed minimal similarity，RSMS）的策略[17]。然而，这些方法仍沿用多数表决或一致同意的扁平化决策范式[18]，将所有执行体输出视为等权投票，忽略执行体间在置信度、稳定性及证据强度方面的差异，难以对异构证据进行有效区分与加权。在存在不确定性、模糊性或冲突的复杂环境中，这些裁决机制依然难以准确反映各执行体输出的可信度，从而削弱系统的鲁棒性与裁决精度。

1.2 多源证据融合与Dempster-Shafer理论

在不确定环境中，如何从多源信息中提取可信结论是智能决策系统面临的核心问题。DS证据理论因其在不确定性建模与证据融合方面的优势，被广泛应用于信息融合领域[19]。与经典概率论不同，DS理论将置信度分配给假设集合而非单一事件，从而能更准确地表达不完全、模糊或

未知状态信息。

在网络安全场景中，系统通常面临来自异构检测节点、不同数据源及多层防御机制的复杂告警信息。为此，研究者将DS理论应用于多源入侵检测结果的融合与推理，以降低误报率同时提升威胁识别可信度[20]。然而，DS理论在应用中仍存在若干挑战：一是组合爆炸导致的计算复杂度较高；二是在处理高度冲突证据时可能产生反直觉结果；三是理论假设证据源相互独立，限制了其在高相关性数据场景下的应用。

1.3　主动防御中的智能裁决

主动防御技术通过引入系统动态性和操作不确定性，显著增加攻击者入侵难度和成本[21]。在该背景下，智能裁决机制对于提升系统适应性和弹性具有重要作用。现有研究尝试将贝叶斯推断应用于安全事件推理[22]，并利用强化学习（reinforcement learning，RL）优化防御策略选择及DHR架构中的调度和裁决机制[23-24]。

然而，基于学习的方法通常依赖大量标注训练数据，模型结构复杂，且可解释性不足。在DHR场景下，由于执行体行为高度不确定且输出难以预测，其泛化能力与决策可解释性仍然是亟待解决的问题。相比之下，DS理论等形式化证据融合方法具备轻量级、可解释且不需要大规模训练数据的优势[25]，因此在处理稀疏且不确定的安全信号时，成为一种特别适用的智能裁决工具。

2　ARDR架构及其核心机制

本节介绍ARDR架构及其2个核心算法。ARDR的设计目标是突破传统DHR架构的“决策扁平化”瓶颈，不再对异构执行体的输出进行简单等权投票，而是构建“筛选–聚焦–融合”的闭环决策流程。通过自适应的证据源选择与基于证据理论的鲁棒裁决，ARDR将冗余系统从被动保障转向主动、可控且可解释的决策流水线。下文将依次介绍架构总体设计、服务体选择机制与基于DS理论的鲁棒裁决机制。

2.1　ARDR架构概述

ARDR架构如图1所示，ARDR对标准DHR模型的服务体构建、调度与裁决模块进行了深度改造，实现了从静态多数投票到基于证据推理的动态裁决转变。

为便于阐述，定义以下术语。

（1）执行体：独立的计算单元，各执行体功能等价，但在实现上存在差异（例如，源代码、依赖库、算法不同）。所有可用的执行体构成执行体池E。

（2）服务体：由调度器从执行体池中选出的n个异构执行体的组合，其中n为系统配置的冗余度。服务体并行处理相同的用户请求，服务体中

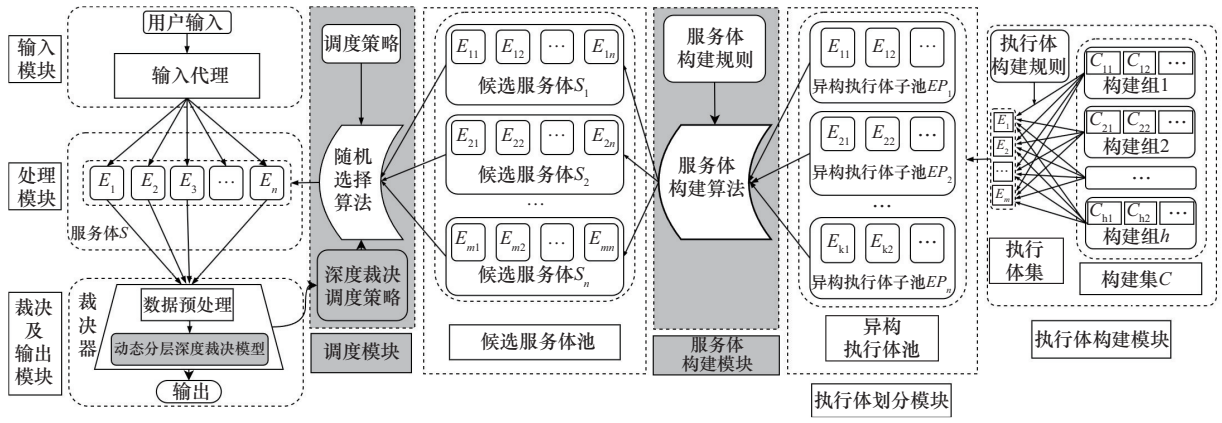


图1　ARDR架构

各执行体的输出共同作为单次裁决的证据源集合。

ARDR架构的核心模块如下。

（1）执行体构建与划分模块：该模块基于执行体池E中各执行体间的相似性进行聚类，形成组内相似度高、组间差异显著的执行体子池：$P=\{\mathrm{EP}_1,\mathrm{EP}_2,\cdots,\mathrm{EP}_i\}$，以降低共模漏洞风险。

（2）服务体构建模块：从不同子池随机选取执行体构建候选服务体集合，基于历史置信度、实时负载及网络状态计算综合得分，实现证据源质量的动态优化与自适应管理。

（3）输入与处理模块：将用户请求复制n份，分发给当前调度的服务体内的n个执行体，生成n个独立的子输出。

（4）调度模块：根据自适应评估机制（详见第2.2节）为当前请求选择服务体。深度裁决模式时（详见第2.3节），执行二次调度以增强裁决的可信度。

（5）裁决与输出模块：基于DS理论的鲁棒裁决器依据n个子输出产生带置信度的决策得分，决定是否直接返回结果、阻止请求，或进入深度裁决流程。

2.2 自适应服务体选择机制

传统DHR/IDHR框架在服务体选择中仅关注异构性，未考虑可靠性与性能。ARDR引入自适应服务体选择机制主动筛除低质量证据源，为后续裁决提供更纯净的输入，以降低冲突处理的复杂度与计算成本。

2.2.1 服务体的多维评估模型

为全面评估候选服务体的质量，本文定义了4个关键指标。

（1）异构度：使用漏洞向量来衡量服务体内执行体的多样性。设$V=\{v_1,v_2,\cdots,v_\lambda\}$为漏洞集，执行体$E_i$的漏洞向量为$\boldsymbol{\alpha_i}=[v_{i1},v_{i2},\cdots,v_{i\lambda}]$，若$E_i$存在漏洞$v_j$，则$v_{ij}=1$。执行体$E_i$和$E_j$间的异构度定义为其漏洞向量的Jaccard距离：

$$D(\boldsymbol{\alpha_i},\boldsymbol{\alpha_j})=1-\frac{\left|\boldsymbol{\alpha_i}\cap\boldsymbol{\alpha_j}\right|}{\left|\boldsymbol{\alpha_i}\cup\boldsymbol{\alpha_j}\right|} \tag{1}$$

服务体S_k的整体异构度是：

$$\mathrm{Heterogeneity}(S_k)=\frac{2}{n\cdot(n-1)}\sum_{i=1}^{n}\sum_{j=i+1}^{n}D(\boldsymbol{\alpha_i},\boldsymbol{\alpha_j}) \tag{2}$$

虽然已知的漏洞数据不能完美代表对未知漏洞的防御能力，并且依赖于漏洞数据库的及时性和完整性，但它目前依然是一个客观、可审计且可动态更新的工程选择，为实现多样性提供了一个合理的近似[26]。

（2）历史置信度：执行体在以往任务中的平均稳定性和正确性。

$$\mathrm{Confidence}(S_k)=\frac{\sum_{i=1}^{n}C_i}{n} \tag{3}$$

其中，C_i是执行体E_i的历史置信度。

（3）历史安全效能：评估服务体S_k在历史安全检测任务中的综合能力，尤其适用于网络安全场景，采用F2值作为度量，更侧重于召回率以减少漏报，即：

$$\mathrm{F2}(S_k)=\frac{\sum_{i=1}^{n}\mathrm{F2}(E_i)}{n} \tag{4}$$

其中，$\mathrm{F2}(E_i)$表示执行体E_i在历史安全检测任务中的F2值。

（4）执行效率：关注最慢执行体的性能瓶颈。设t_i为执行体E_i的执行时间，则：

$$\mathrm{ET}(S_k)=\begin{cases}0, & \max\{t_1,\cdots,t_i,\cdots,t_n\}>\mathrm{ET}_{\mathrm{Threshold}}\\ 1-\dfrac{\max(t_1,\cdots,t_i,\cdots,t_n)-\mathrm{ET}_{\min}}{\mathrm{ET}_{\mathrm{Threshold}}-\mathrm{ET}_{\min}}, & \text{其他}\end{cases} \tag{5}$$

其中，$\mathrm{ET}_{\min}$为最低的历史执行体执行时间，$\mathrm{ET}_{\mathrm{Threshold}}$为系统设定的最大容忍执行时间。

2.2.2 服务体的综合评估与权重优化

将上述4个指标线性加权，得到服务体S_k的综合得分：

$$\mathrm{SI}(S_k)=\omega_1\cdot\mathrm{Heterogeneity}(S_k)+\omega_2\cdot \mathrm{Confidence}(S_k)+\omega_3\cdot\mathrm{F2}(S_k)+\omega_4\cdot\mathrm{ET}(S_k) \quad (6)$$

权重向量 $\boldsymbol{W}=(\omega_1,\omega_2,\omega_3,\omega_4)$ 决定了系统在“安全多样性–可靠性–检测能力–性能”间的权衡。由于目标函数（如F2值）缺乏解析表达式且不可微，采用鲸鱼优化算法（WOA）[27]来求解最优权重。选择WOA不仅因其适用于无导数优化，还因其比粒子群优化算法（PSO）和遗传算法（GA）具有更快的收敛速度和更强的局部最优鲁棒性[28-29]。

2.2.3　动态服务体选择

根据优化后的权重向量 $\boldsymbol{W}$，系统计算每个候选服务体 S_k 的综合评分 $\mathrm{SI}(S_k)$，并将其转化为选择概率：

$$P(S_k)=\frac{\mathrm{SI}(S_k)}{\sum_j \mathrm{SI}(S_k)} \quad (7)$$

调度器基于此概率分布进行带权随机抽样，使得高评分的服务体更易被选中。随着历史置信度、性能等指标动态更新，系统可实现自适应优化。

2.3　基于Dempster-Shafer证据理论的鲁棒裁决机制

由于传统裁决方法难以处理不确定性，ARDR引入DS理论将裁决从简单投票扩展为形式化证据推理。

2.3.1　证据建模与多标准折扣

（1）识别框架

针对裁决任务，定义识别框架为 $\Theta=\{\mathrm{N},\mathrm{A}\}$，其中，N表示“请求正常”，A表示“请求异常”。其幂集 $2^{\Theta}=\{\varnothing,\{\mathrm{N}\},\{\mathrm{A}\},\{\mathrm{N},\mathrm{A}\}\}$ 包含了所有可能的假设。其中，$\{\mathrm{N},\mathrm{A}\}$ 代表“不确定”状态，即无法明确区分正常与异常。

（2）基本概率分配（BPA）构建

对每个执行体 E_i，根据其判断 $J(E_i)\in\{\mathrm{N},\mathrm{A}\}$ 与历史置信度为 $c_i\in[0,1]$ 构建BPA函数 m_i。

若 $J(E_i)=\mathrm{N}$：

$$m_i(\{\mathrm{N}\})=c_i\cdot\beta;\ m_i(\{\mathrm{A}\})=(1-c_i)\cdot\beta;\ m_i(\Theta)=1-\beta \quad (8)$$

若 $J(E_i)=\mathrm{A}$：

$$m_i(\{\mathrm{A}\})=c_i\cdot\beta;\ m_i(\{\mathrm{N}\})=(1-c_i)\cdot\beta;\ m_i(\Theta)=1-\beta \quad (9)$$

其中，$\beta\in(0,1]$ 为调节因子，控制初始不确定性的大小。$m_i(\Theta)$ 表示“完全不确定”的信念量。

（3）多准则证据折扣

标准的Dempster组合规则假设证据源相互独立，但在DHR场景中执行体间可能因共享代码库、运行环境等因素而存在相关性，直接融合会过度增强信念。为此，引入了多准则证据折扣机制基于以下3个准则对每个执行体 E_i 计算其可靠性因子 δ_i，以对每个证据源的可靠性进行动态评估和调整。

- 相似性（Sim_i）：基于漏洞向量距离计算 E_i 与服务体内其他成员的平均相似度。相似度越高，潜在相关性越大，可靠性应越低。

$$\mathrm{Sim}_i=1-\frac{1}{n-1}\sum_{j\neq i}D(\boldsymbol{\alpha_i},\boldsymbol{\alpha_j}) \quad (10)$$

- 一致性（Cons_i）：计算 E_i 的BPA(m_i)与其他所有成员融合后的BPA(m_i)之间的Jousselme距离。距离越大，说明 E_i 是一个“异类”，可靠性应越低。

$$\mathrm{Cons}_i=1-\mathrm{JousselmeDistance}(m_i,m_{\neg i}) \quad (11)$$

- 冲突性（Conf_i）：计算 E_i 的BPA与其他成员融合后的BPA之间的冲突因子 $K(m_i,m_{\neg i})$。频繁引发高冲突的证据源，其可靠性应越低。

$$\mathrm{Conf}_i=1-K(m_i,m_{\neg i}) \quad (12)$$

最终的折扣因子 δ_i 是3个准则的加权组合。

$$\delta_i=1-\left(\lambda_1\cdot\mathrm{Sim}_i+\lambda_2\cdot\mathrm{Cons}_i+\lambda_3\cdot\mathrm{Conf}_i\right) \quad (13)$$

其中，$\lambda_1,\lambda_2,\lambda_3$ 为超参数，且 $\sum\lambda=1$。

在此基础上，使用Shafer的折扣规则来调整原始的BPA(m_i)：

$$m_i'(X)=(1-\delta_i)m_i(X),\forall X\subset\Theta,X\neq\Theta \quad (14)$$

$$m_i'(\Theta)=(1-\delta_i)m_i(\Theta)+\delta_i \quad (15)$$

折扣过程将部分信念转移到不确定项Θ，从而抑制不可靠或相关性较高的证据源的影响。该多准则折扣机制隐含了一个动态、上下文感知的执行体信任模型，其评估维度会随当前服务体组合而自适应调整。

2.3.2 冲突感知证据融合

在获得所有经过折扣的BPA($m_1',m_2',\cdots,m_n'$)后，需将其融合成一个单一的BPA以供后续裁决使用。

（1）Dempster组合规则

对于2个证据m_a'和m_b'，其组合$m_{a\oplus b}$按Dempster规则定义为：

$$m_{a\oplus b}(Z)=\frac{1}{1-K}\sum_{X\cap Y=Z}m_a'(X)m_b'(Y),\forall Z\subseteq\Theta,Z=\varnothing, \quad (16)$$

其中，冲突因子$K=\sum_{X\cap Y=\varnothing}m_a'(X)m_b'(Y)$度量2个证据之间的矛盾程度。上述规则可以递归应用。

（2）高冲突感知融合

在高冲突场景（如$K\to1$）下，标准Dempster规则可能产生违背直觉的融合结果。为此，引入冲突感知融合策略，其流程如下：首先设定冲突阈值τ_K（如0.8），并在融合前计算冲突因子K。当$K<\tau_K$时，冲突程度可接受，可直接使用标准Dempster规则；当$K\geqslant\tau_K$时，则视为严重冲突，将因冲突产生的信念质量直接分配给不确定项Θ，而非通过归一化进行“消解”。此时得到的融合结果m_{fused}如下：

$$m_{\text{fused}}(Z)=(1-K_{\text{old}})\cdot m_{a\oplus b}(Z),\forall Z\subset\Theta,Z\neq\Theta \quad (17)$$

$$m_{\text{fused}}(\Theta)=(1-K_{\text{old}})\cdot m_{a\oplus b}(\Theta)+K_{\text{old}} \quad (18)$$

其中，两证据融合前的标准Dempster结果为$m_{a\oplus b}$，其原始冲突因子为K_{old}。

2.3.3 深度裁决方法

在获得候选服务体S_k的融合BPA(m_{S_k})后，需要将其转换为最终裁决结果。

（1）裁决评分生成（Pignistic转换）

采用Pignistic概率（BetP）将BPA转换为倾向于“正常”的裁决评分$J(S_k)\in[0,1]$。

$$J(S_k)=\text{BetP(N)}=m_{S_k}(\{\text{N}\})+\frac{1}{2}\times m_{S_k}(\Theta) \quad (19)$$

$J(S_k)$值越接近1表示越倾向于“正常”，越接近0则越倾向于“异常”。

（2）多层置信度裁决机制

设定2个自适应阈值τ_L和τ_H（$0<\tau_{\text{L}}\leqslant\tau_{\text{H}}<1$），将评分区间划分为3类。

- 高置信度异常区（$J(S_k)<\tau_{\text{L}}$）：判为异常，阻断请求。
- 高置信度正常区（$J(S_k)>\tau_{\text{H}}$）：判定为正常，放行请求。
- 模糊区（$\tau_{\text{L}}\leqslant J(S_k)\leqslant\tau_{\text{H}}$）：触发深度裁决。

（3）深度裁决流程（二次验证）

当评分落入模糊区时，为提高决策可靠性执行二次裁决。

- 二次服务体选择：调度器选择一个与当前服务体S_k异构度最大且历史性能优异的新服务体S_k'，以提高第二轮证据的独立性与代表性。
- 二次执行与评分：S_k'处理同一请求并生成新的融合BPA($m_{S_k'}$)，计算$J(S_k')$。
- 最终融合：若第二轮评分仍位于模糊区，则依据两轮裁决的置信度（即非Θ部分的信念总和）进行加权融合：

$$w_k=1-m_{S_k}(\Theta),w_k'=1-m_{S_k'}(\Theta) \quad (20)$$

$$J_{\text{final}}=w_k\cdot J(S_k)+w_k'\cdot J(S_k') \quad (21)$$

- 最终决策：根据J_{final}与阈值τ_{final}作出最终的放行或阻断决策。为避免过度迭代，深度裁决过程在实际系统中通常限制为至多执行一次。

3 实验和分析

本节通过原型系统和一系列仿真实验验证，

对ARDR架构的有效性进行系统化、量化评估。

3.1　实验方案设计

实验包括2类：

（1）基于拟态WAF的原型系统验证实验，用于评估ARDR在真实应用环境中的可行性；

（2）基于仿真的扩展实验，用于进行对比分析、消融实验以及参数敏感性分析。

3.1.1　评估指标

评估指标包括安全指标与性能指标2类，从安全性与系统效率两个维度对不同决策架构进行量化对比。

（1）安全指标

安全性方面采用准确率、检出率、误报率和F2值4项指标，具体定义如下。

- 准确率（accuracy，ACC）：衡量系统对正常请求与异常请求的整体分类正确性。

$$\mathrm{ACC}=\frac{\mathrm{TP}+\mathrm{TN}}{\mathrm{TP}+\mathrm{TN}+\mathrm{FP}+\mathrm{FN}} \tag{22}$$

- 检出率（true positives rate，TPR）：反映系统识别异常请求（攻击）的能力，即召回率。

$$\mathrm{TPR}=\frac{\mathrm{TP}}{\mathrm{TP}+\mathrm{FN}} \tag{23}$$

- 误报率（false positives rate，FPR）：衡量系统将正常请求误判为异常的比例。

$$\mathrm{FPR}=\frac{\mathrm{FP}}{\mathrm{FP}+\mathrm{TN}} \tag{24}$$

- F2值：在精确率（Precision）与召回率（Recall）之间引入加权偏向，强调召回率，更适用于对漏报敏感的安全场景（如网络入侵检测）。计算式如下：

$$\mathrm{F2}=\frac{5\cdot\mathrm{Precision}\cdot\mathrm{Recall}}{4\cdot\mathrm{Precision}+\mathrm{Recall}} \tag{25}$$

其中，$\mathrm{Precision}=\mathrm{TP}/(\mathrm{TP}+\mathrm{FP})$，$\mathrm{Recall}=\mathrm{TP}/(\mathrm{TP}+\mathrm{FN})$。TP为正确检测到的攻击样本数，TN（为正确识别的正常请求数，FP为误判的正常请求数，FN为漏检的攻击数。

（2）性能指标

系统效率方面采用平均执行时间（average execution time，AET），为用户请求从进入系统到完成最终裁决所需的平均时间（单位为ms）。

3.1.2　对比基准架构

为全面评估ARDR架构的性能优势，本文选取以下主流DHR作为对比基准：

（1）传统DHR架构：服务体选择策略有随机选择（randomly select，RS）[7]、最长相异性距离（maximum dissimilarity，MD）算法[30]、随机种子最小相似度（random seed & minimum similarity，RSMS）算法[17]；裁决机制有全体一致性裁决（consistency arbitrary，CA）[12]、多数裁决（majority arbitrary，MA）[18]。

（2）IDHR架构：采用执行体划分策略与多数裁决机制的IDHR架构[9]。由于ARDR继承了其执行体划分机制，因此选择IDHR作为重要的性能参考对象。

3.2　ARDR在拟态WAF原型中的应用实验

3.2.1　实验设计

为验证ARDR在真实环境下的可行性，本研究构建了一个基于拟态Web应用防火墙（WAF）的原型系统，集成了ARDR、IDHR和DHR架构。其中，DHR架构采用经典的随机调度与多数裁决算法。

（1）执行体池：选择了6种主流开源WAF引擎（ModSecurity、Coraza、Naxsi、SafeLine、uuWAF、Janusec），通过差异化配置构建出8种异构执行体。

（2）测试平台：后端为WordPress，反向代理网关为基于拟态Web应用防火墙的原型系统（冗余度$n=4$），改进版BlazeHttp工具用于生成混合测试流量。为评估不同负载下的系统性能，模拟了高、中、低3种负载水平并测量系统平均执行时间。

（3）测试流量：为确保评估的代表性与可靠性，本研究构建了一个综合测试数据集，融合了CSIC 2010数据集、真实校园网络日志及人工模

拟攻击流量。其中，CSIC 2010数据集提供了典型的攻击模式与高质量标注样本，校园网络日志则反映了实际运行环境中的正常行为特征，而模拟攻击流量用于补充特定场景下的威胁类型。综合流量数据集中约73%为正常流量，27%为攻击流量，覆盖OWASP TOP 10中的主要攻击类型。攻击样本共计25 657条，涵盖结构化查询语言（SQL）注入、跨站脚本攻击、拒绝服务攻击、命令注入、远程文件包含等多种常见威胁形式。数据集按照7:3的比例划分为训练集与测试集。

3.2.2 拟态WAF原型系统实验结果

拟态WAF原型系统整体性能对比如图2所示。结果表明，在安全性方面，动态异构冗余架构（ARDR、IDHR、DHR）在ACC、TPR、FPR和F2值等核心指标上均明显优于单一WAF架构；在动态架构中，ARDR的表现也显著领先于IDHR与DHR。在性能开销方面，ARDR的AET虽略高于部分轻量级WAF（如uuWAF与naxis），但增幅有限，仍满足实时检测需求。与Coraza等传统规则匹配型系统相比，ARDR在保持相近执行效率的同时显著提升了安全性，展现出良好的安全与性能平衡。其优势主要源于动态异构冗余与分层裁决机制：在常规请求上优先采用轻量级判决路径降低时延，仅在检测结果存在不确定性时才触发深度裁决，使额外计算开销集中于少量复杂样本，从而有效维持整体吞吐率与响应性能。

为进一步分析深度裁决的触发特性，本文对实验运行数据进行了事后统计。结果表明，约9.41%的请求进入深度裁决流程，主要集中于特征模糊或混淆的攻击样本（如变形SQL注入、跨层编码注入）以及少量边界型正常请求。这说明深度裁决策略能够有效识别并聚焦处理这类高不确定性请求，将额外计算资源投入在最需要精细判别的样本上，可在不显著增加整体开销的前提下提升复杂场景的检测鲁棒性。

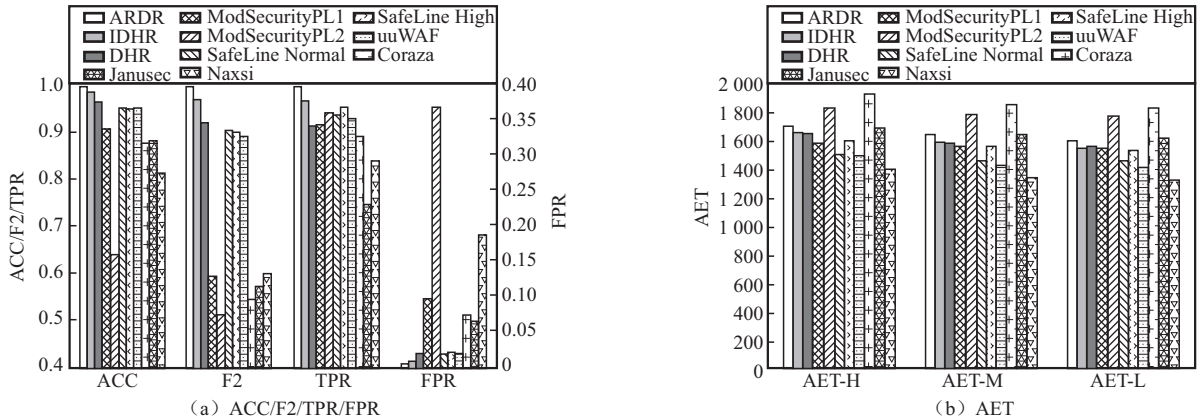
3.3 仿真实验

3.3.1 仿真实验设计

（1）执行体与数据集生成

为了创建多样化的异构执行体池E，采用2种方式[9]。

- 模拟生成：构建规模为$m=65,75,85$的异构执行体池。每个执行体E_i配置$\lambda=3\,000$维二进制漏洞特征向量α_i，每维以概率$p_v=0.1$倍赋值为1，并随机设置1%~10%范围内的误报率，以生成具备复杂结构和高异构性的虚拟环境。
- 基于Web服务器构建：组合不同操作系统、Web服务框架、后端语言和数据库系统，构建55种具有不同漏洞特征与组件依赖的Web服务器实例，模拟真实异构环境。



（a）ACC/F2/TPR/FPR　　（b）AET

图2 拟态WAF原型系统整体性能对比

历史数据生成：生成100万条请求数据，其中90%为正常请求，10%为攻击请求。每个执行体的平均响应时间服从典型Web请求处理延迟分布$N(\mu=1\,500\ \text{ms},\sigma=200\ \text{ms})$。每条记录包含请求类型、目标执行体及响应时间。

训练集与测试集划分：按照7:3的比例划分为训练集和测试集。训练集用于计算执行体性能指标（成本c_i、F2值F2(E_i)、响应时间t_i）及训练ARDR的权重和裁决模型参数；测试集用于评估ARDR的整体安全性（ACC、TPR、FPR、F2）和性能（AET）。

（2）架构配置

基线配置：保留原始的服务选择和裁决机制。

ARDR参数配置

- 权重优化：在满足平均执行时间AET≤$\text{ET}_{\text{Threshold}}$的前提下，使用WOA算法（种群规模为30，迭代次数为1 000次）最大化系统的F2值，求解最优权重向量$\boldsymbol{W}=(\omega_1,\omega_2,\omega_3,\omega_4)$。
- DS裁决模型：BPA生成因子$\beta=0.9$，折扣因子δ_i基于执行体相似度计算。
- 深度裁决参数：裁决阈值设为$\tau_L=0.5$和$\tau_H=0.65$，最终融合裁决阈值$\tau_{\text{final}}=0.5$。

3.3.2　安全与性能实验结果与分析

ARDR架构与典型DHR架构的整体性能对比实验在执行体模拟环境（调节冗余度n与执行体数量m）和Web场景模拟环境（固定执行体数量m调节冗余度n）中进行，实验结果如下。

模拟生成执行体方案下各架构不同执行体池规模的性能对比（固定冗余度$n=3$）如图3所示。

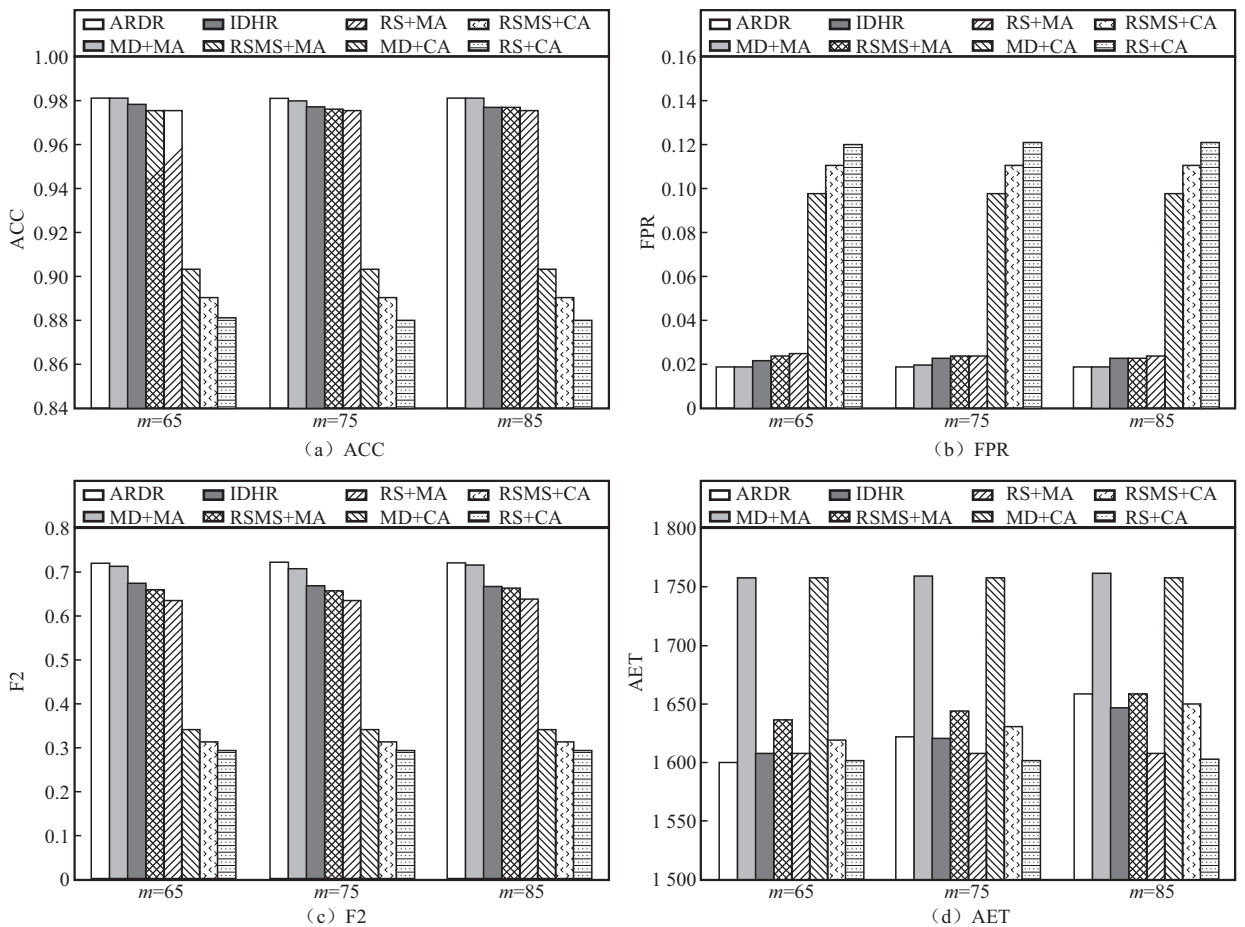


图3　模拟生成执行体方案下各架构不同执行体池规模的性能对比（固定冗余度$n=3$）

在固定冗余度$n=3$的条件下，ARDR在ACC、FPR与F2值等核心指标上均显著优于对比架构，实现了高检测率与低误报率的良好平衡。其他架构虽在个别指标上具有一定优势，但整体表现不稳定，难以在复杂攻击场景下兼顾准确性与可靠性。

模拟生成执行体方案下各架构不同冗余规模的性能对比（$m=65$）如图4所示，进一步验证了“冗余–性能悖论”以及ARDR的优势。对于传统多数表决类架构（IDHR、MD+MA、RSMS+MA、RS+MA），当冗余度从3增至5时，其F2值均持续下降，且FPR显著上升。CA系列架构虽保持一定检测率，但F2值下降更为明显，整体性能受限。

仿真Web方案下各架构不同冗余规模的性能对比（$m=65$）如图5所示。仿真Web场景中结论基本一致。随着冗余度提升，各多数表决架构的F2值亦出现明显退化（如MD+MA从0.827降至0.730），FPR普遍升高。这说明单纯增加执行体会引入更多噪声和判决冲突，而传统裁决机制缺乏有效处理能力，导致整体性能下降。

相比之下，ARDR的性能随冗余度提升呈现稳步上升趋势。在模拟执行体实验中，其F2值从0.720提升至0.934，ACC与TPR同步提升，FPR由0.019降至0.004。在Web仿真场景中，其F2值进一步从0.862提升至0.952，FPR从0.008降低至0.003。结果表明，ARDR的深度裁决机制与多异构执行体融合策略能够有效吸收多源信息，将冗余中的噪声转化为性能增益，从根本上突破传统架构的性能瓶颈。

3.3.3 消融实验结果及分析

为进一步评估ARDR中两大机制的独立贡献

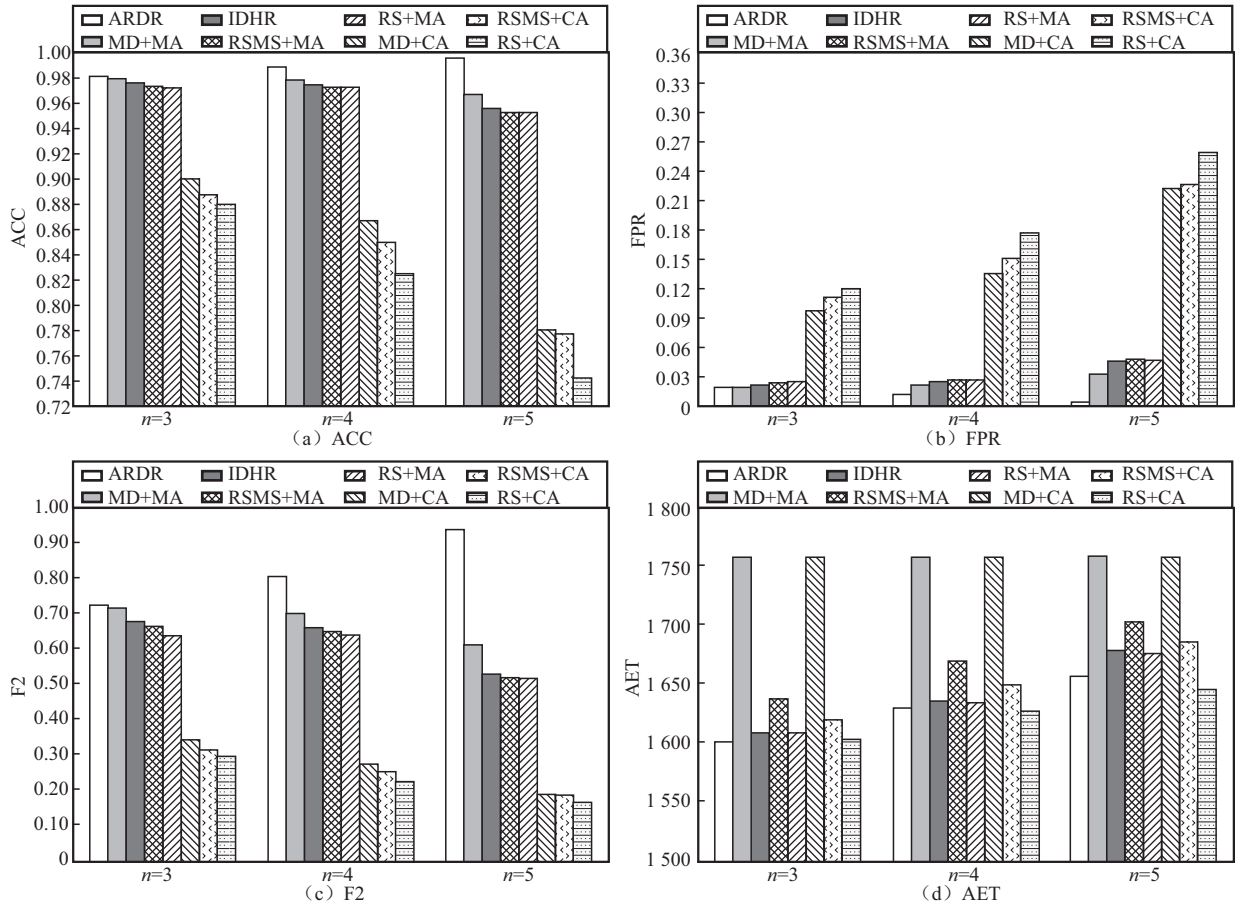


图4 模拟生成执行体方案下各架构不同冗余规模的性能对比（$m=65$）

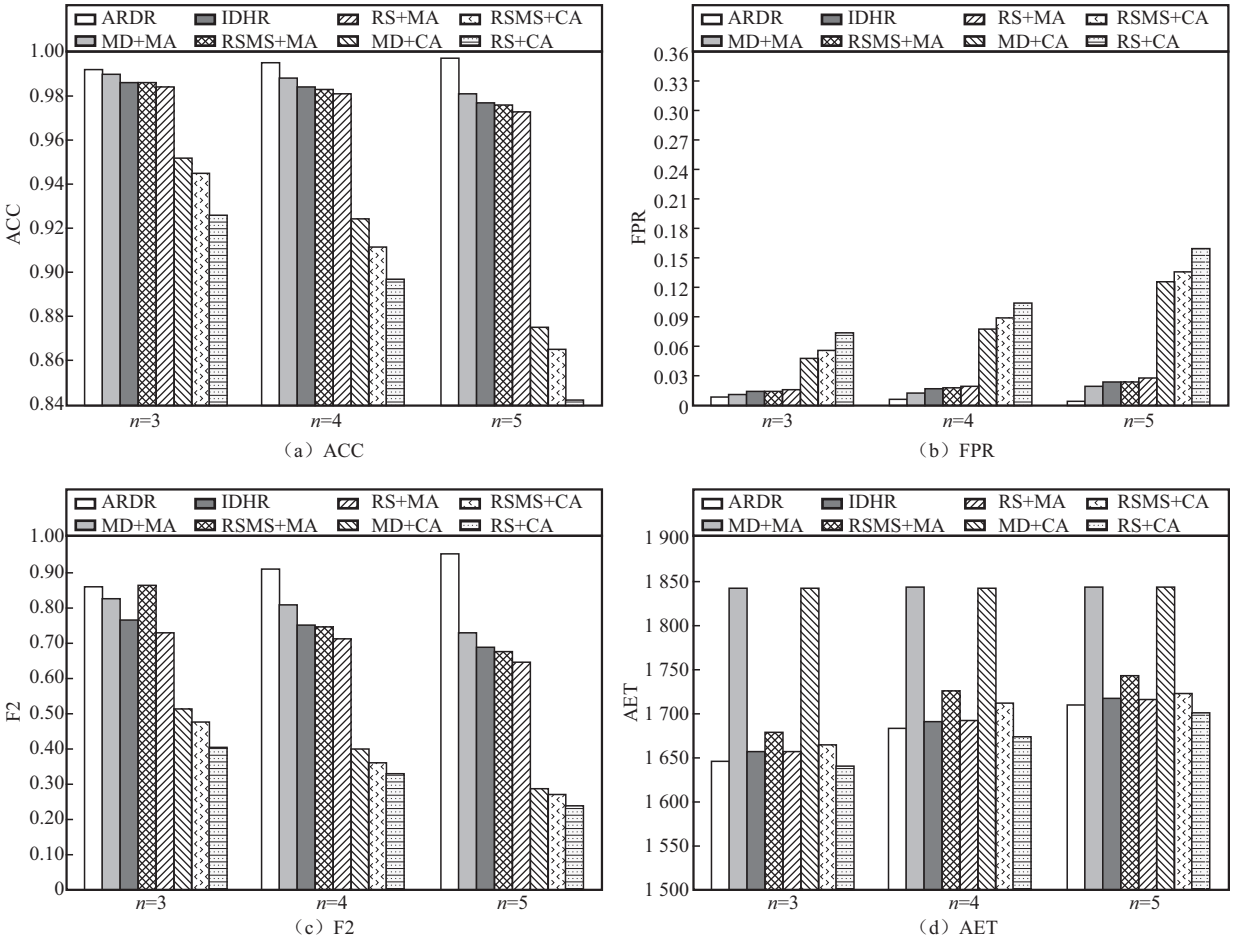


图5　仿真Web方案下各架构不同冗余规模的性能对比（$m=65$）

与协同效应，本研究设计了4种架构并进行了消融实验。

（1）基准组（IDHR）：未引入任何ARDR特有机制，采用传统多数裁决策略，为对照基线。

（2）综合评估指数组：仅引入基于服务体异构性、历史性能的自适应选择机制。

（3）深度裁决机制组：仅引入基于DS理论的深度裁决机制。

（4）完整ARDR组：同时集成选择机制与裁决机制，为完整实现版本。

模拟生成执行体方案下各架构性能对比（$m=65$）如图6所示，仿真Web方案下各架构性能对比（$m=65$）如图7所示，分析如下。

（1）自适应选择机制的贡献：引入“综合评估指数”后，系统交互时间AET显著下降，各组表现均优于基准，说明该机制能够有效识别高性能执行体组合，从源头上降低系统延迟。

（2）深度裁决机制的贡献：启用“深度裁决机制”后，系统安全性（F2值）大幅提升，显示其在处理冲突与不确定信息方面具有显著效果。但其AET略高，反映出证据推理与二次验证带来的计算开销。

（3）协同增益效应：完整ARDR组在安全性上全面领先，同时AET低于纯裁决组，甚至优于基准组。自适应选择机制提供高质量输入，降低裁决冲突与不确定性，间接提升裁决效率；深度裁决机制保证复杂场景下输出高可信判决。两者结合，使ARDR在安全性与性能上达到最优

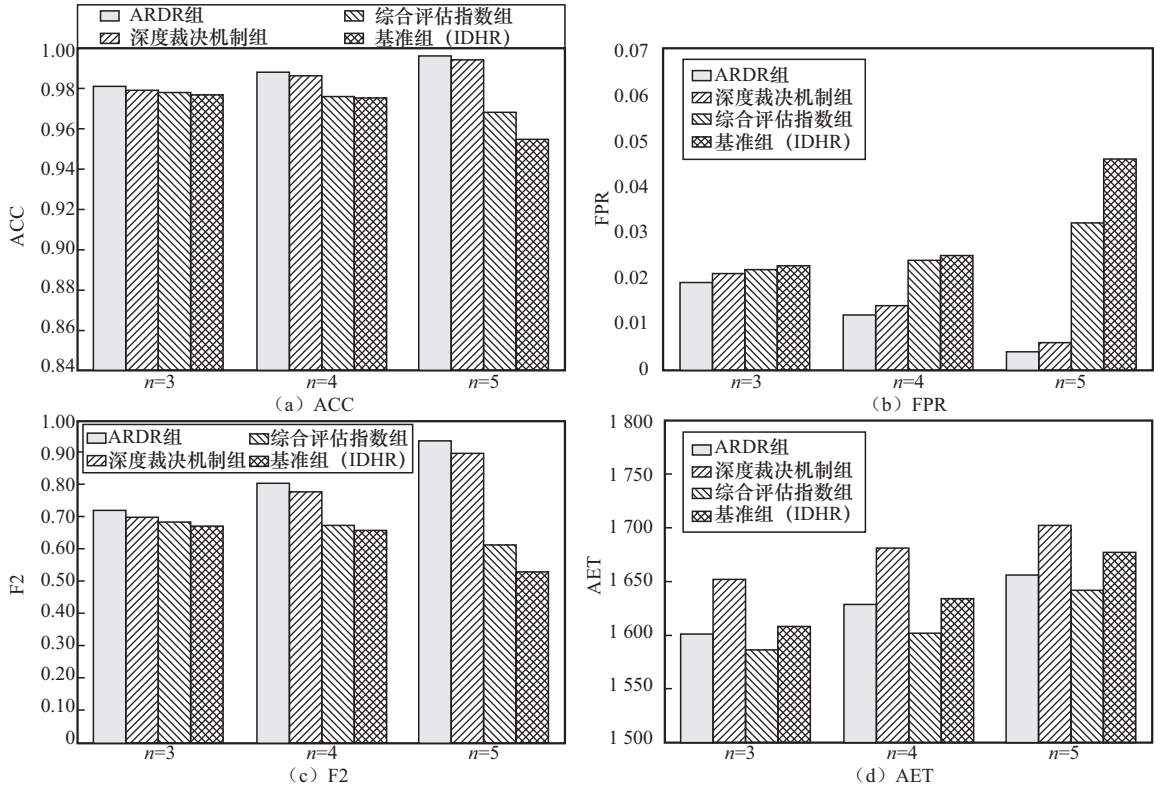


图6　模拟生成执行体方案 下各架构性能对比（$m=65$）

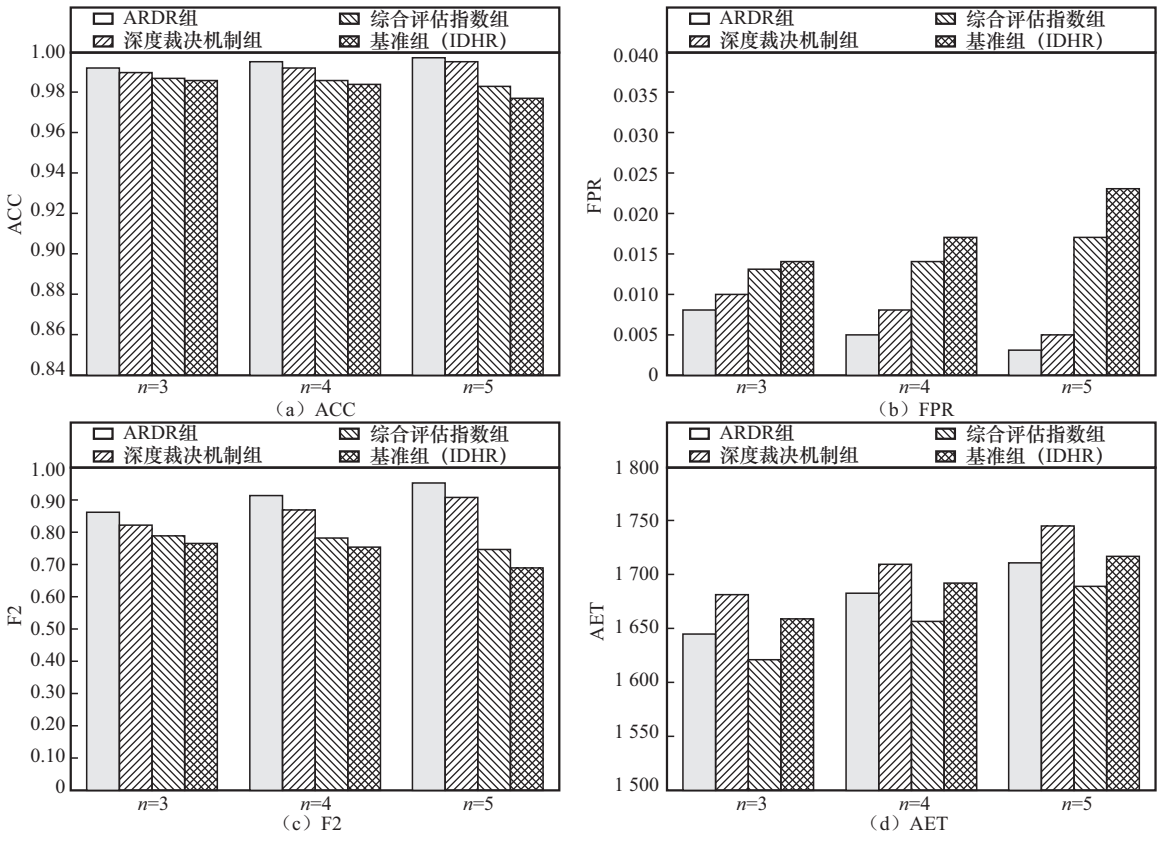


图7　仿真Web方案下各架构性能对比（$m=65$）

平衡。

为直观展示核心机制的协同效应，模拟生成执行体方案下 ARDR 核心机制协同增益分析（$n=5$）见表 1，仿真 Web 场景下 ARDR 核心机制的协同增益效应分析（$n=5$）见表 2，其中加粗数据为各列数据的最大值。结果显示，ARDR 的两大核心机制既能独立发挥作用，又能产生显著协同效应。

3.3.4　参数敏感性实验

为系统评估 ARDR 架构关键内部参数对性能的影响，本文在固定冗余度（$n=3$）和执行体数（$m=65$）的模拟生成场景下开展参数敏感性实验。实验采用控制变量法，每次仅调整一个参数以观察其对安全性（ACC、F2）与性能（AET）的影响，主要包括 3 类：服务体评估权重向量 $\boldsymbol{W}=\{w_1,w_2,w_3,w_4\}$（初始由 WOA 算法动态调整，目标为联合优化 ACC、F2 与 AET）；DS 理论中的 BPA 生成时的调节因子 β（取值范围[0.5, 0.9]）；深度裁决模块中的模糊区阈值对 (τ_L,τ_H)（取值范围[0.4, 0.65]，用于界定二次裁决触发）。

（1）权重向量 $\boldsymbol{W}$ 的敏感性分析。

权重向量 $\boldsymbol{W}=\{w_1,w_2,w_3,w_4\}$ 控制服务体历史指标在综合评估指数 $\mathrm{SI}(S_k)$ 中的贡献度。组合 A 为 WOA 优化后的权重，组合 B 为相等的初始权重，组合 C、组合 D 分别为 WOA 迭代 500、1 000 次时的权重。

权重参数(W)敏感性分析结果（$n=3$）如图 8 所示，显示系统在不同 WOA 优化配置的整体性能。结果表明，系统对权重 W 的设置具有较好的鲁棒性。WOA 优化后的权重组合 A，在所有安全指标上表现最优。但即使是最简单的等权重未优化组合 B，相较于优化后的组合 A，安全性与性能下降幅度仍较为有限。上述结果说明 WOA 优化能有效提升性能上限，但系统本身对权重配置不极端敏感。

（2）深度裁决阈值 τ_L,τ_H 的敏感性分析。

模糊阈值对 (τ_L,τ_H) 决定深度裁决的触发条件，其区间宽度反映系统对不确定判断的容忍度。实验设置 3 组配置：组合 A（$\tau_{\mathrm{L}}=0.5,\tau_{\mathrm{H}}=0.65$）、组合 B（$\tau_{\mathrm{L}}=0.45,\tau_{\mathrm{H}}=0.7$）和组合 C（$\tau_{\mathrm{L}}=0.55,\tau_{\mathrm{H}}=0.6$）。

裁决阈值（τ）敏感性分析结果（$n=3$）如图 9 所示，展示了各组合下的系统整体性能对比。结果表明，模糊区阈值是影响系统行为的关键参数。扩大模糊区（组合 B）会频繁触发深度裁决，FPR 和 AET 显著增加，F2 值下降，说明过于保守并非最优。收窄模糊区（组合 C）可降低 FPR 和 AET，但会显著降低 F2 和 TPR。组合 A 在

表 1　模拟生成执行体方案下 ARDR 核心机制协同增益分析（$n=5$）

架构配置	F2	AET /ms	F2 相较基线增益	AET 相较基线变化
基线（IDHR）	0.527	1 677	—	—
仅自适应选择	0.611	1 641	+15.8%	−2.2%
仅鲁棒裁决	0.895	1 702	+69.6%	+1.5%
完整 ARDR（协同增益）	**0.934**	**1 656**	**+76.9%**	**−1.2%**

表 2　仿真 Web 场景下 ARDR 核心机制的协同增益效应分析（$n=5$）

架构配置	F2	AET/ms	F2 相较于基线的增益	AET 相较于基线的变化
基线（IDHR）	0.688	1 717	—	—
仅引入自适应选择	0.746	1 689	+8.4%	−1.6%
仅引入鲁棒裁决	0.908	1 745	+32.0%	+1.6%
完整 ARDR（协同增益）	**0.952**	**1 710**	**+38.4%**	**−0.4%**

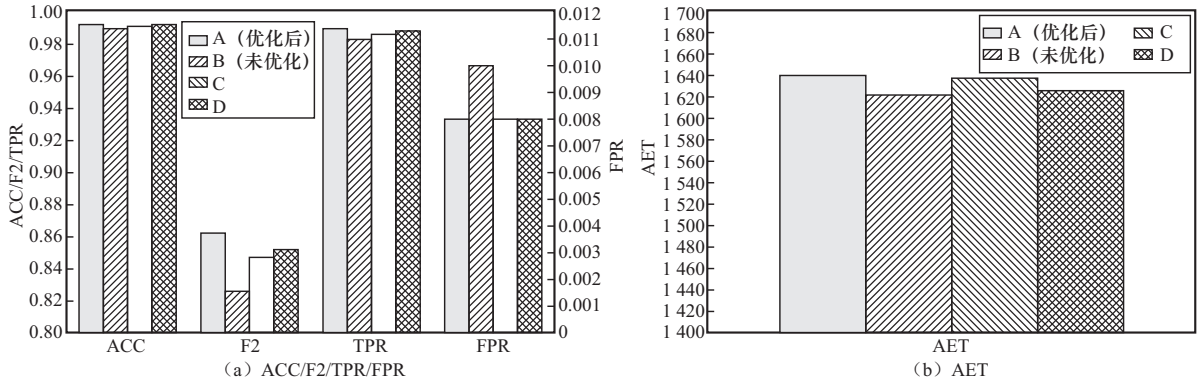


图8　权重参数(W)敏感性分析结果($n=3$)

安全性和效率之间取得了最佳平衡。实验表明，该参数对系统性能影响显著，应根据实际应用场景进行精细调整。

（3）BPA调节因子β的敏感性分析。

β控制BPA构建时初始信念的强度。BPA调节因子（β）敏感性分析结果（$n=3$）如图10所示，结果显示系统在一定范围内对β具备较好的鲁棒性，但过低的初始信念会显著影响判别效果与运行效率。当β较小（如0.5）时，信念过于分散，导致系统F2值极低，FPR、AET显著增大。随着β增大，系统性能迅速提升，并在$\beta\geq0.8$时趋于稳定且表现优异。结果表明，给予证据足够强的初始信念对于裁决模型的有效运作至关重要。基于结果，推荐$\beta=0.9$作为默认值。

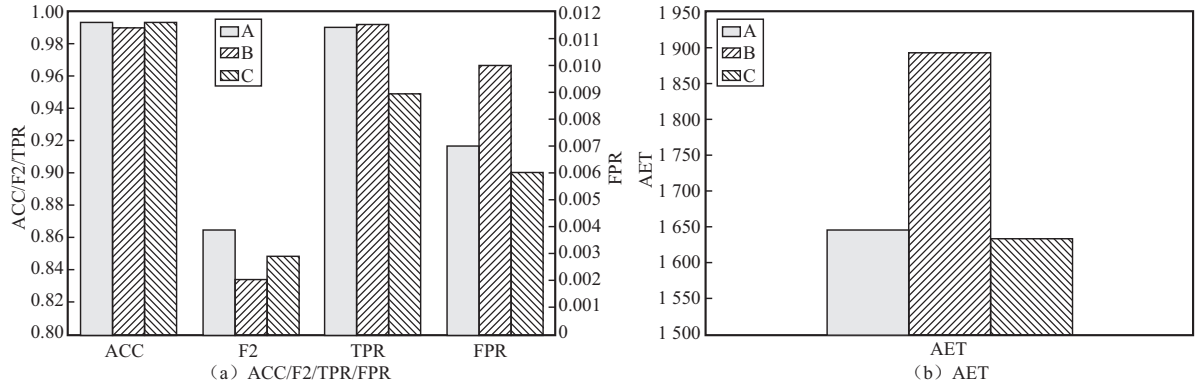


图9　裁决阈值(τ)敏感性分析结果($n=3$)

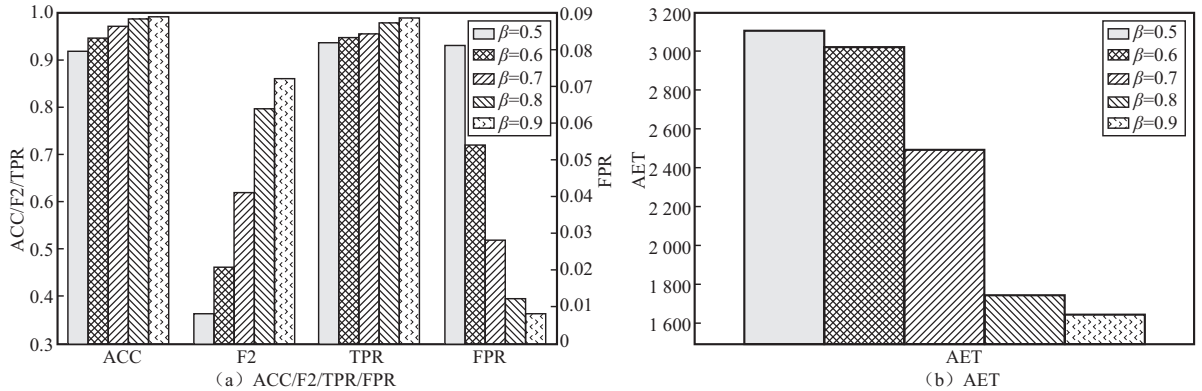


图10　BPA调节因子(β)敏感性分析结果(n=3)

3.4　讨论

本文实验结果为核心论点提供了有力实证支持：通过主动式证据筛选与反应式证据综合，ARDR 取代了传统 DHR 中扁平化的统计投票机制，有效解决了长期存在的“冗余-性能悖论”。如图 3 和图 4 所示，随着冗余度增加，传统多数表决架构性能下降明显，而 ARDR 性能稳步提升。表 3 和表 4 的协同增益分析进一步表明，自适应选择机制与鲁棒裁决机制结合，可在最大化安全性的同时几乎完全抵消性能开销，实现安全性与效率的最佳平衡。

消融实验进一步揭示了 ARDR 核心机制的协同效应。自适应服务选择机制结合执行体异构特征、历史信誉等信息，动态生成最优服务组合，实现资源的最优分配与策略匹配，可提升检测成功率和整体资源利用效率。鲁棒裁决机制基于 DS 证据理论，有效建模并融合模糊、不完全及冲突信息，通过信任函数分配与多源信息整合区分“信息缺失”与“明确冲突”。深度裁决策略针对低置信度或高冲突判决进行二次验证，显著降低误判率，提高裁决结果稳定性与可信度。

参数敏感性分析显示，ARDR 对权重配置扰动具有较高稳定性，这体现出优越的泛化能力与鲁棒性，使系统在不同环境下迁移和部署成本较低，并能灵活适配多类检测任务。同时，实验表明系统性能对深度裁决阈值和 BPA 调节因子高度敏感，其最优取值需结合具体应用场景定制，提示实际部署中应设计自适应参数优化机制，以实现性能与资源利用的最佳平衡。未来研究可探索基于学习驱动的参数自适应调节策略，以增强系统在复杂环境下的自调节能力和长期稳定性。

尽管 ARDR 在性能与鲁棒性方面表现突出，但该架构仍存在若干待优化的局限性。

（1）部署复杂性较高：系统参数敏感性要求应用者具备一定领域知识以支持初始部署与调优，增加了工程应用门槛。

（2）底层依赖性明显：ARDR 性能依赖于执行体池的质量与异质性，当底层执行体性能不足或同质化严重时，系统提升空间受限。

（3）冷启动问题：新执行体可通过“影子模式”缓解，即在初期仅被动运行、收集性能数据，待历史数据积累到一定程度后（如处理 10 000 条请求）再纳入主动选择池。

ARDR 的核心设计原则是通过智能信源选择实现不确定信息的鲁棒融合，这一机制具有超越拟态防御的广泛理论适用性，可应用于多种复杂场景。例如，在自动驾驶领域，该方法可融合摄像头、雷达和激光雷达的冲突或不确定数据，从而支持更安全的决策；在联邦学习场景中，可用于聚合来自不同客户端、质量参差不齐的模型更新；在医疗辅助诊断系统中，利用该框架来有效处理多专家冲突意见。

4　结束语

针对动态异构冗余架构中长期存在的“冗余-性能悖论”，本文提出端到端智能决策框架 ARDR。该框架通过自适应服务选择对高质量执行体进行筛选，并结合基于 DS 证据理论的鲁棒裁决与深度触发机制，从而提升裁决的准确性与可靠性。仿真与原型验证结果表明，ARDR 在 ACC、F2 值和 AET 等核心指标上整体优于传统 DHR 架构，尤其在高冗余条件下能够更高效地利用冗余信息提升系统性能。未来工作将重点关注多维属性的量化建模，通过非线性加权或基于机器学习的方法构建服务体综合评估指数，以捕捉指标间复杂相互作用；裁决机制的自适应优化，开发元学习或强化学习代理动态调整深度裁决的模糊阈值，实现裁决策略在线自适应；以及算法效率提升与跨场景适用性扩展，探索轻量化实现并将核心原则推广至其他多源信息融合场景，以进一步增强 ARDR 的工程实用性。

参考文献：

[1] Ouyang H W, Xu F, Chen Z X, et al. Advanced persistent threat detection and defense algorithm based on multi-source heterogeneity[C]//Proceedings of the 2025 7th International Conference on Electronics and Communication, Network and Computer Technology (ECNCT). Piscataway: IEEE Press, 2025: 280-284.

[2] Wan Y F, Qin L J, Qin J R, et al. Security risk identification model of power grid software supply chain based on data mining[C]//Proceedings of the 2025 International Conference on Electrical Drives, Power Electronics & Engineering (EDPEE). Piscataway: IEEE Press, 2025: 1277-1282.

[3] Merigala J, Kumar V, Gujjarlapudi J, et al. Analysis of supply chain attacks in open-source software and mitigation strategies[C]//2024 5th International Conference on Communication, Computing & Industry 6.0 (C2I6). Piscataway: IEEE Press, 2024: 1-5.

[4] Shaaban G, Fourati H, Kibangou A, et al. Active defense strategy in cyber-physical systems: misleading unauthorized observers[J]. IEEE Transactions on Control of Network Systems, 2025, 12(3): 2404-2415.

[5] Xu Y X, Li M H, Fang B X, et al. Neural honeypoint: an active defense framework against model inversion attacks[J]. IEEE Transactions on Neural Networks and Learning Systems, 2025, 36(9): 16186-16197.

[6] 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.
Wu J X. Cyberspace mimicry security defense[J]. Secrecy Science and Technology, 2014(10): 4-9, 1.

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

[8] Hu J J, Li Y, Li Z Z, et al. Unveiling the strategic defense mechanisms in dynamic heterogeneous redundancy architecture[J]. IEEE Transactions on Network and Service Management, 2024, 21(4): 4912-4926.

[9] 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.
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.

[10] Luo W Q, Ni M, Yu X S, et al. Design of mimic security integrated framework for embedded systems[C]//Proceedings of the 2025 5th International Symposium on Computer Technology and Information Science (ISCTIS). Piscataway: IEEE Press, 2025: 806-810.

[11] Shao S S, Gu T S, Nie Y J, et al. An active defense adjudication method based on adaptive anomaly sensing for mimic IoT[J]. IEEE Transactions on Services Computing, 2025, 18(1): 57-71.

[12] Parhami B. Voting algorithms[J]. IEEE Transactions on Reliability, 1994, 43(4): 617-629.

[13] Shafer G. A Mathematical Theory of Evidence[M]. Princeton, N.J.: Princeton University Press, 1976.

[14] Jones J, Hiser J D, Davidson J W, et al. Defeating denial-of-service attacks in a self-managing N-variant system[C]//Proceedings of the 2019 IEEE/ACM 14th International Symposium on Software Engineering for Adaptive and Self-Managing Systems (SEAMS). Piscataway: IEEE Press, 2019: 126-138.

[15] Tan L, Krings A. A hierarchical formal framework for adaptive N-variant programs in multi-core systems[C]//Proceedings of the 2010 IEEE 30th International Conference on Distributed Computing Systems Workshops. Piscataway: IEEE Press, 2010: 7-12.

[16] Wang Z H, Jiang D D, Lv Z H. AI-assisted trustworthy architecture for industrial IoT based on dynamic heterogeneous redundancy[J]. IEEE Transactions on Industrial Informatics, 2023, 19 (2): 2019-2027.

[17] 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.

[18] Choi J, Goh K I. Majority-vote dynamics on multiplex networks[J]. New Journal of Physics, 2019, 21(3): 035005.

[19] Ran H C, Zhou M, Du N, et al. Multi-view fusion based object detection approach using dempster-shafer evidence theory[C]//Proceedings of the 2024 IEEE 12th Asia-Pacific Conference on Antennas and Propagation (APCAP). Piscataway: IEEE Press, 2025: 1-2.

[20] Zhao K Y, Li L, Chen Z Q, et al. A survey: Optimization and applications of evidence fusion algorithm based on Dempster–Shafer theory[J]. Applied Soft Computing, 2022, 124: 109075.

[21] Qiu W C, Ma Y H, Chen X Z, et al. Hybrid intrusion detection system based on Dempster-Shafer evidence theory[J]. Computers & Security, 2022, 117: 102709.

[22] Yang W, Hou F Y, Jia Z Y, et al. A game-theory-based risk assessment method for industrial control systems *via* Bayesian attack graphs[C]//Proceedings of the 2025 10th International Conference on Signal and Image Processing (ICSIP). Piscataway: IEEE Press, 2025: 876-880.

[23] Cui P Y. Design of adaptive network defense mechanism combining reinforcement learning[C]//Proceedings of the 2025 4th International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE). Piscataway: IEEE Press, 2025: 1-5.

[24] Tan Z Y, Karakose M. Optimized deep reinforcement learning approach for dynamic system[C]//Proceedings of the 2020 IEEE International Symposium on Systems Engineering (ISSE). Piscataway: IEEE Press, 2020: 1-4.

[25] Wang S H, Sun C, Lin Y P. Human behavior recognition based on weighted voting - dempster shafer algorithm from fusion of multiple radars[C]//Proceedings of the 2024 17th International Convention on Rehabilitation Engineering and Assistive Technology (i-CREATe). Piscataway: IEEE Press, 2024: 1-4.

[26] 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.
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.

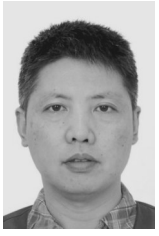
[27] Mirjalili S, Lewis A. The whale optimization algorithm[J]. Advances in Engineering Software, 2016, 95: 51-67.

[28] Liu R, Liang Z H, Wang Z Y, et al. Indoor visible light positioning based on improved whale optimization method with Min-max algorithm[J]. IEEE Transactions on Instrumentation and Measurement, 2023, 72: 2504910.

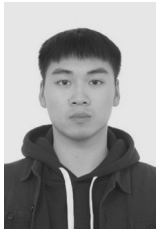
[29] Hussien A G, Heidari A A, Ye X J, et al. Boosting whale optimization with evolution strategy and Gaussian random walks: an image segmentation method[J]. Engineering with Computers, 2023, 39(3): 1935-1979.

[30] 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. Design of selective algorithm for diverse software components[J]. Journal of Harbin Institute of Technology, 2003, 35(3): 261-264.

[作者简介]

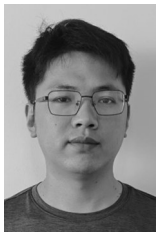


郑秋华（1973– ），男，博士，杭州电子科技大学网络空间安全学院副教授，主要研究方向为内生安全。



孙振宇（2000– ），男，杭州电子科技大学网络空间安全学院硕士生，主要研究方向为内生安全。

章坚武（1961– ），男，博士，杭州电子科技大学信息工程学院特聘教授，中国通信学会会士，主要研究方向为移动通信与信息安全、移动通信与AI融合技术。



徐李定（1988– ），男，中国电子科技集团第32研究所研究员，主要研究方向为拟态安全。

周迪（1975– ），男，博士，杭州电子科技大学网络空间安全学院研究员，主要研究方向为人工智能、物联网。

程传慧（1979– ），女，博士，中南财经政法大学信息工程学院副教授，主要研究方向为人工智能。