计 算 机 研 究 与 发 展
Journal of Computer Research and Development

https://crad.ict.ac.cn
63(9): 2371−2385, 2026

本期推荐

基于深度嵌入聚类与遗传进化的蜜点效能评估方法

张志强[1,2] 王海燕[1] 杜 磊[1] 段晨芸[2] 李嘉瑞[2] 顾钊铨[1,2] 方滨兴[2]

[1]（鹏城实验室 广东深圳 518055）

[2]（哈尔滨工业大学（深圳）计算机科学与技术学院 广东深圳 518055）

（zhangzhiqiang@stu.hit.edu.cn）

Deep Embedded Clustering and Genetic Evolution Based Honey Point Effectiveness Assessment Method

Zhang Zhiqiang[1,2], Wang Haiyan[1], Du Lei[1], Duan Chenyun[2], Li Jiarui[2], Gu Zhaoquan[1,2], and Fang Binxing[2]

[1]（*Pengcheng Laboratory*, *Shenzhen*, *Guangdong* 518055）

[2]（*College of Computer Science and Technology*, *Harbin Institute of Technology* (*Shenzhen*), *Shenzhen*, *Guangdong* 518055）

Abstract With the deep integration of 5G, artificial intelligence, and the Internet of things, network infrastructure is facing the dual challenges of an expanding dynamic attack surface and increasing threat stealthiness. Traditional static defense mechanisms are no longer capable of effectively countering the evolving attack strategies. Although the existing active deception defense systems have enhanced threat detection capabilities through honey point technology, they still have significant shortcomings, particularly the lack of dynamic effectiveness evaluation and resource optimization mechanisms, which leads to a severe imbalance between defense costs and security benefits. Current research primarily focuses on the initial deployment strategies and architectural improvements of honey points; however, these studies have not effectively addressed the periodic attenuation of defense effectiveness in dynamic confrontation scenarios. There are also obvious deficiencies in the quantitative modeling of multidimensional security indicators and closed-loop optimization mechanisms. To address this research gap, we propose a multi-dimensional effectiveness representation mechanism for honey point cluster defense systems. The mechanism constructs a comprehensive effectiveness evaluation system with three core indicators: redundancy risk index, cross-honey point IP repetition rate, and threat entrapment effectiveness score. Specifically, the method first uses deep embedded clustering technology to obtain the prior labels of honey point effectiveness, providing basic data for subsequent effectiveness evaluation. It then introduces a weight adaptive optimization mechanism driven by genetic evolutionary strategies to dynamically adjust the weights of the core indicators according to the actual threat environment and defense requirements, thereby achieving precise and efficient effectiveness evaluation. On this basis, a closed-loop defense system of “evaluation-feedback-optimization” is further established, enabling the defense system to adjust defense strategies and resource allocation promptly based on real-time effectiveness evaluation results, thereby significantly enhancing the intelligence level of active deception defense systems. This closed-loop defense system provides a feasible theoretical paradigm for promoting the intelligent development of active deception defense systems and is expected to play an important role in the field of future network security defense.

收稿日期：2025-08-08；**修回日期**：2026-04-01

基金项目：鹏城实验室重大攻关项目（PCL2024A05）；深圳市科技计划项目（KJZD20240903103811016）

This work was supported by the Major Key Project of PCL (PCL2024A05) and the Shenzhen Science and Technology Program (KJZD 20240903103811016).

通信作者：顾钊铨（guzhaoquan@hit.edu.cn）

Key words deception defense; honey point cluster; effectiveness characterization; deep embedding clustering; genetic evolution

摘 要 随着5G、人工智能和物联网技术的深度融合,网络基础设施正面临动态攻击面持续扩大和威胁隐蔽性不断增强的双重挑战。传统静态防御机制已难以应对攻击策略的不断演变。尽管现有的主动式欺骗防御体系通过蜜点技术提升了威胁感知能力,但仍存在显著缺陷,尤其是缺乏动态效能评估与资源优化机制,导致防御成本与安全效益严重失衡。当前研究大多集中在蜜点的初始部署策略和架构改进上,但这些研究未能有效解决防御效能在动态对抗场景下周期性衰减的问题,且在多维度安全指标量化建模和闭环调优机制方面存在明显不足。针对这一研究空白,提出了一种蜜点集群防御体系的多维效能表征机制。该机制以冗余风险指数、跨蜜点IP重复率和威胁诱捕效能评分为核心指标,构建了一套完整的效能评估体系。具体而言,该方法首先利用深度嵌入聚类技术获取蜜点效能的先验标签,为后续效能评估提供基础数据;然后引入基于遗传进化策略的权重自适应优化机制,根据实际威胁环境和防御需求动态调整各核心指标的权重,以实现精准高效的效能评估。在此基础上,进一步构建了“评估—反馈—调优”的闭环防御体系,使防御系统能够依据实时效能评估结果,及时调整防御策略和资源配置,从而显著提升主动式欺骗防御系统的智能化水平。这一闭环防御体系为推动主动式欺骗防御系统的智能化发展提供了切实可行的理论范式,有望在未来网络安全防御领域发挥重要作用。

关键词 欺骗防御;蜜点集群;效能表征;深度嵌入聚类;遗传进化

中图法分类号 TP391

DOI: 10.7544/issn1000-1239.202550584 **CSTR:** 32373.14.issn1000-1239.202550584

随着5G通信、人工智能算法和物联网技术的深度整合,全球数字化转型正以指数级的速度推进。智能城市、工业互联网和边缘计算等新兴技术的广泛应用,推动了网络基础设施向智能化方向快速发展。然而,这种技术融合在显著提升社会生产效率的同时,也极大地扩展了网络攻击的潜在范围[1-4]。攻击者利用生成对抗网络(generative adversarial network, GAN)和强化学习(reinforcement learning, RL)等先进工具,不断优化其攻击策略,导致网络威胁的变异速度和隐蔽性呈指数级增长[5-7]。

传统边界防御机制在应对新型攻击技术时暴露出显著局限性,其静态防护架构难以应对攻击策略的动态演化。由方滨兴等人[8]提出的盾立方(shield cube)网络安全防御体系,通过构建“四蜜(蜜点、蜜庭、蜜阵、蜜洞)联动”的协同机制,创新性地实现了网络安全态势的全域感知与主动防御。该系统基于多维度数据融合框架,不仅在“蜜点”等诱捕技术识别威胁后进行深度行为分析与跨域关联研判,精准掌握攻击意图与路径;更能根据研判结果,通过联动“蜜庭”“蜜阵”等节点实施实时的设障阻截,如访问控制或流量净化。整个系统将威胁诱捕、行为分析、态势评估、关联研判与响应处置等模块深度耦合,形成“感知—决策—响应”的动态防御闭环,可有效应对日益复杂和隐蔽的网络威胁。

随着边缘计算场景中分布式节点数量呈指数级增长,防御体系对部署单元的弹性扩展能力提出了更高的要求。为此,盾立方体系创新性地提出了蜜点(honey point)技术。该技术通过在被保护系统的外围关键位置预设多个仿真接入节点,其内部架构包含具备行为感知能力的哨兵监控进程,而表层协议栈则完全模拟真实业务系统的特征。当攻击者进行漏洞探测时,蜜点能够通过协议级交互仿真实现对攻击行为的无感知捕获。与传统单点式部署方案相比,蜜点集群通过拓扑混淆机制将防御触角延伸至网络边缘。在保持诱捕环境高保真度的同时,其离散式拓扑结构能够根据业务负载动态调整节点规模,从而在终端资源受限的场景下构建出弹性可扩展的轻量化防御矩阵。

图1描述了基于蜜点集群协同的动态欺骗防御体系架构。该架构通过在网络边缘部署欺骗防御矩阵,主动诱导渗透攻击。当攻击者突破边界防护体系时,其攻击流量会被动态重定向至由蜜点集群组成的虚拟化诱捕场域。该场域利用拓扑仿真算法、服务指纹模拟引擎以及流量镜像技术,构建了一个具有多层次诱骗能力的拟态网络拓扑空间。在战术实施层面,系统通过自适应诱捕策略实现攻击路径

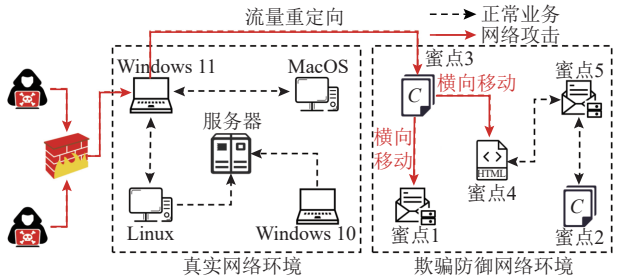


Fig. 1 Dynamic deceptive defense architecture based on honeypots and honeytoken clusters

图 1 基于蜜罐和蜜点集群的动态欺骗防御体系架构

的动态重构，诱导攻击者产生路径误判，并在虚拟化诱捕场域内实施横向渗透行为。所有攻击交互过程都在经过协议级编排的虚拟资产集群中完成，从而形成了一个集攻击行为全要素捕获、攻击特征深度提取以及攻击路径实时追踪于一体的主动防御体系。

在动态对抗升级的网络安全态势下，上述防御架构的持续运行效能面临严峻挑战。蜜点集群因静态拓扑配置及冗余节点分布，导致算力资源与存储空间的低效占用，尤其在物联网与边缘计算场景下，该问题加剧了防御成本与安全效益的失衡。当前学术界针对欺骗防御技术的研究主要集中于体系架构优化[9-10]与应用场景拓展[11-12]。尽管已有学者提出蜜罐部署策略[13-14]，但其研究视角多聚焦于初始部署阶段的静态约束。然而，当研究客体演进至蜜点集群时，其防御效能的维持机制面临新的技术鸿沟。在动态网络环境下，蜜点集群的欺骗防御效能会随攻击模式演变、业务流量波动及网络拓扑重构等因素产生周期性衰减，而现有研究尚未建立针对蜜点运行状态的持续性效能评估机制。当前研究空白集中体现为 2 方面：1）缺乏对“蜜点有效性”的多维度量化评价指标体系；2）未形成基于动态评估结果的防御资源再优化机制。这 2 方面使得欺骗防御系统难以通过自适应调整维持最佳防御状态。因此，构建蜜点有效性动态评估模型并建立周期性策略优化机制，成为突破主动防御体系效能瓶颈的核心研究方向。

针对上述问题，本文提出一种融合多维效能表征与智能优化机制的蜜点防御体系动态评估方法，通过构建数据驱动的评估模型与闭环优化框架，突破现有主动防御体系的技术瓶颈。具体而言：首先，构建蜜点冗余风险指数、跨蜜点 IP 重复率及威胁诱捕效能评分 3 项核心指标，继而建立多指标协同蜜点防御表征值，实现防御效能的量化评估；其次，针对蜜点效能评估中缺乏先验分类标签的客观约束，引入深度嵌入聚类（deep embedded clustering, DEC）算法实现无监督分类判别，通过特征空间重构与概率分布建模揭示蜜点效能的内在分布规律；进而设计遗传算法（genetic algorithm, GA）驱动的多指标权重自适应优化机制，以深度嵌入聚类结果为监督信号，通过进化策略实现防御表征值的周期性校准；最终形成“评估—反馈—调优”的闭环防御体系，支持蜜点集群在复杂攻击场景下的资源动态配置与效能持续提升。

本文的主要贡献可归纳为 4 个方面：

1）提出了蜜点冗余风险指数、跨蜜点 IP 重复率及威胁诱捕效能评分 3 项核心指标，并突破传统单维度评估框架的局限性，构建了多指标协同蜜点防御表征值，实现了防御效能的动态量化评估。

2）设计了一种基于深度嵌入聚类的无监督学习框架，通过高维特征重构、软分配概率建模与 KL 散度优化，构建数据驱动的蜜点自动化分类模型，实现蜜点效能精准判别，为权重系数优化提供可靠的先验知识支撑。

3）提出了融合深度嵌入聚类与遗传算法的混合优化框架，通过染色体编码、适应度函数动态匹配及交叉变异操作，实现多指标权重系数的全局自适应调整，实现多指标协同蜜点防御表征值的定期校准。

4）建立了基于周期性评估与资源再配置的闭环防御体系，通过定期效能反馈及部署策略优化机制，提升蜜点集群在复杂攻击场景下的诱捕效率与资源利用率，为主动式欺骗防御系统的智能化演进提供可落地的理论范式。

1 相关工作

随着网络攻击技术的不断发展，盾立方网络安全防御体系中的蜜点诱捕技术通过模拟漏洞环境吸引攻击者并收集威胁情报，已经成为主动防御体系中的关键手段，并发挥了重要作用。然而，当前的研究在蜜点分类、效能评估和动态优化等方面仍存在明显不足，尤其是在蜜点集群防御效能的量化和自适应优化机制方面，亟待取得突破性进展。本节将从 3 个方面进行系统性综述：首先是网络边界防御范式的演变，其次是盾立方体系中的欺骗防御机制，最后是动态对抗环境中蜜点效能的评估方法。通过这些综述，旨在为本文提出的蜜点防御效能表征值和闭环优化框架奠定坚实的理论基础。

1.1 网络边界防御的范式迁移

传统网络边界防御体系以防火墙技术为架构核

心，其理论范式源自访问控制列表所构建的静态安全框架[15-16]。该模型依托预定义策略规则，在开放系统互连(open systems interconnection, OSI)模型的网络层至传输层实施基于二元逻辑(允许/阻断)的流量过滤机制，形成刚性防御边界。技术演进过程中，状态检测防火墙通过动态维护会话状态表实现了协议上下文感知能力的提升[17]，而深度包检测技术则借助应用层协议解析将防御纵深扩展至数据包载荷语义层面[18-20]。传统边界防御体系因受限于静态策略引擎的刚性判定范式而难以实现攻击向量空间多维扩展的动态适配性，在加密混淆攻击语义解析盲区持续累积的同时，其离散式防护节点布局因缺乏态势感知协同机制，致使横向渗透攻击链路的暴露面呈现非线性扩张态势。

盾立方网络安全防御体系通过内生安全与护卫模式的深度融合，实现了防御机制从刚性策略向动态协同的范式跃迁[8]。该体系依托多维态势感知网络构建分布式探针矩阵，基于网络欺骗技术形成主动式诱捕拓扑，通过攻击语义的多维度关联解析突破传统加密混淆攻击的检测盲区。在此基础上，其核心机制是构建超大规模网络安全知识图谱驱动的智能协同防御系统，采用攻击链上下文感知的动态策略生成引擎，实现攻击向量空间的实时映射与防御策略的自主演化。相较于传统离散式防护架构，盾立方体系通过威胁情报的全网协同共享与防御资源的弹性调度，实现攻击向量空间的实时动态映射与防御策略的自主演化，为新型加密流量攻击和高级持续性威胁(advanced persistent threat, APT)防御提供了体系化解决方案。

1.2 盾立方体系中的欺骗防御

网络安全领域对欺骗防御技术的系统性研究长期聚焦于蜜罐系统的体系构建。基于协议栈镜像仿真和流量动态调度技术，蜜罐系统能够构建具有时序特征的动态化欺骗防御环境[21]。当前研究依据交互深度差异构建了低交互型、中交互型与高交互型蜜罐3级分类体系[22-25]，其中分布式低交互蜜罐通过弹性攻击面扩展技术显著提升网络威胁的感知覆盖率[22-23]；中交互蜜罐通过在交互真实性与资源开销间建立平衡，利用协议模拟与动态策略配置(如服务行为仿真、流量诱骗因子调整)增强对抗反侦察能力，从而实现对多阶段攻击行为链的捕获[24-25]；而高交互蜜罐系统则依托攻击行为全链路重构能力，实现基于多维度行为特征的攻击者画像建模[10-12]。传统蜜罐技术因资源密集型架构与高开销部署的制约，在攻击面弹性扩展能力及多阶段攻击链动态适配层面呈现固有局限性，其跨系统协同机制缺失与攻防响应异步性延迟的叠加效应，最终引发加密混淆攻击场景下的防御资源动态调度失效及攻击行为语义解耦盲区。

盾立方的欺骗防御体系则通过“四蜜联动”协同机制与护卫模式的深度融合，构建了层次化动态防御范式[8]。该体系依托多维态势感知网络构建分布式探针矩阵，其中蜜点作为网络诱捕单元主动部署高交互诱饵系统实现业务环境快速克隆，通过协议栈镜像生成与真实业务拓扑同构的诱饵节点，在保障交互深度的同时显著降低部署复杂度；蜜庭基于沙箱化环境构建攻击行为分析矩阵，运用动态行为追踪技术重构攻击链路，为多阶段攻击意图推理提供基础数据支撑；蜜洞则通过深度流量重定向实现攻击行为的全景捕获；蜜阵网络通过探针集群的跨域协同机制，实现攻击流量的智能调度与威胁情报共享，其弹性资源分配策略可动态适配网络拓扑变化；蜜洞模块采用协议逆向解析与流量重定向技术，建立加密会话与沙箱环境的映射通道，有效扩展攻击行为捕获维度。盾立方系统的多层次动态防御体系，在实现攻击行为协同感知与弹性调度能力的同时，依托蜜点的轻量化部署特性有效克服了传统蜜罐技术存在的资源密集型架构局限与加密攻击语义盲区问题。

1.3 动态对抗环境中的蜜点效能评估

在欺骗防御技术框架下，工业控制网络[26-28]与物联网[29-30]等特殊场景的防御节点部署研究已取得阶段性进展，但仍面临系统性优化难题。以Mohammadzad等人[31]的工业控制网络动态诱捕方案为例，其通过Rootkit隐匿技术降低设备指纹特征熵值的核心思路，在物联网边缘计算场景下的实践表明，静态化部署策略易引发进程注入机制的流量特征异常风险，揭示了传统部署模式在资源利用效率层面的固有缺陷。类似地，Maesschalck等人[32]基于软件定义网络的协议混淆方法，虽通过逆向指纹识别与流量重定向技术构建虚实融合防御体系，但复杂工控协议交互场景下的单向诱捕机制仍存在高交互性攻击特征泄露隐患，反映出当前技术路线在动态行为适应能力方面的不足。

作为欺骗防御体系的核心节点，蜜点部署面临3重递进式优化矛盾：1)传统静态配置范式导致防御节点长期占用边缘计算资源，形成防御成本与安全收益的边际效益递减[12]；2)现有技术体系缺乏基于

威胁情报实时感知的节点调度机制，难以实现防御资源与攻击态势的动态匹配[33]；3）当前评估方法多聚焦于功能验证维度，而对诱捕质量指标与攻击持续吸引力等核心效能参数缺乏系统性量化模型[34]。这些矛盾共同制约了蜜罐技术在实际攻防对抗中的主动防御价值。

蜜点有效性评估体系仍存在两大关键理论缺口：1）现有指标（如唯一踩蜜率、伪装度）多为单一维度，缺乏跨维度关联模型，难以协同表征蜜点冗余风险、跨节点 IP 重复率及威胁捕获能力。例如，Suratkar 等人[35] 提出的基于自适应 Q-Learning 的动态欺骗防御模型，虽通过状态空间驱动的强化决策框架优化了初始资源分配策略，并利用动态奖励函数实现局部节点伪装度自适应调整，但其状态转移机制未建模攻击模式演驱动的蜜点效能周期性衰减，导致蜜网拓扑的动态适应性优化能力受限（尤其在长期对抗场景中）；2）现有优化机制多依赖静态权重参数和人工经验配置，未能构建数据驱动的闭环反馈架构。以 Anwar 等人[36] 和陈军[37] 的研究为例，其采用的启发式规则引擎（基于固定权重与环境假设）既未整合实时攻击模式演化数据与动态环境反馈，也缺乏基于威胁情报流和蜜点效能衰减模型的在线强化学习框架，导致欺骗防御环境的拓扑调整滞后于攻击者行为模式迁移（如 APT 攻击中的多阶段策略演化）。

值得注意的是，2022 年的研究尝试引入强化学习[12] 与博弈论[33] 优化欺骗防御框架部署，但其模型仍局限于初始配置阶段，未能构建“评估—反馈—调优”的闭环防御体系（例如动态威胁响应与资源重分配的实时性不足）。为此，本文提出融合冗余风险指数、跨蜜点 IP 重复率与威胁诱捕效能评分的多维指标体系，结合深度嵌入聚类与遗传进化策略，实现蜜点防御效能的动态量化与闭环优化，最终填补“动态评估—实时反馈—自适应调优”的全周期研究空白。

1.4 大语言模型驱动下的欺骗防御范式演进

近年来，随着大语言模型（large language model, LLM）在自然语言理解与生成领域展现出强大能力，其与网络安全的交叉融合已逐渐成为值得关注的探索方向。然而，在欺骗防御的动态优化场景中，相关研究仍处于概念验证与机制推演阶段，尚未形成可与传统机器学习或深度学习框架直接对比的成熟体系。当前，大语言模型的应用主要体现于对高维威胁情报的语义解析、攻击行为的自然语言摘要生成以及防御策略的辅助编排等环节，其角色更多表现为对既有模型的语义增强与决策支持，而非独立或替代性的技术路径。相较于依赖数值特征与行为模式的传统评估方法，大语言模型在未来更可能承担“语义补充层”的功能，通过解析攻击链上下文、推断攻击者意图描述或融合跨源威胁情报，提升欺骗策略的可解释性与部署规划的辅助决策能力。尽管如此，在实际工程部署中，大语言模型仍面临推理延迟显著、对抗鲁棒性不足、难以适应高频动态攻防环境等现实约束，其在轻量化、确定性防御架构中的深度融合仍需进一步研究与体系化验证。

2 基于深度嵌入聚类与进化协同的蜜点防御效能评估模型

在本节中，我们将系统阐述蜜点防御效能评估的理论框架与实现机理。通过融合多维指标体系构建、深度特征嵌入聚类与智能进化优化方法，提出一种面向复杂网络威胁环境的蜜点效能量化评估模型。该方法突破传统单维度评估的局限性，实现蜜点防御效能的协同表征与自适应优化，为网络欺骗防御体系的智能化演进提供理论支撑。图 2 系统化展示了我们提出的基于深度嵌入聚类与进化协同优化的蜜点效能评估框架。该框架构建了一套以冗余风险指数、跨蜜点 IP 重复率和威胁诱捕效能评分为核心的多维复合指标体系，从而形成具有动态感知能力的蜜点效能基线评估模型。在蜜点效能标签生成方面，利用深度自编码器对高维特征空间进行非线性映射与降噪，并通过深度嵌入聚类算法实现蜜点效能分布的无监督预训练。在优化决策层面，构建遗传进化策略驱动的优化引擎，以聚类生成的效能类别标签作为先验知识指导多指标权重的自适应调优，从而构建“特征表征—效能评估—策略迭代”的动态反馈环路。最终形成具有环境感知能力的闭环防御体系，实现防御资源配置的动态优化与安全态势的持续适配。

2.1 蜜点防御系统实现架构

盾立方是一套基于协同欺骗与主动防御理念构建的网络安全框架，由蜜点、蜜庭、蜜阵与蜜洞 4 个功能模块协同组成，形成覆盖“感知—研判—调度—解析”全流程的动态威胁对抗体系。其中，蜜点作为前沿诱捕与数据采集节点，负责在网络边缘构建高仿真业务诱饵环境并对扫描探测、协议交互及横向渗透等入侵行为进行无感知捕获与高保真记录；蜜庭作为高交互沙箱环境，负责对捕获的攻击流量进行深度行为分析与意图研判；蜜阵则是由分布式探

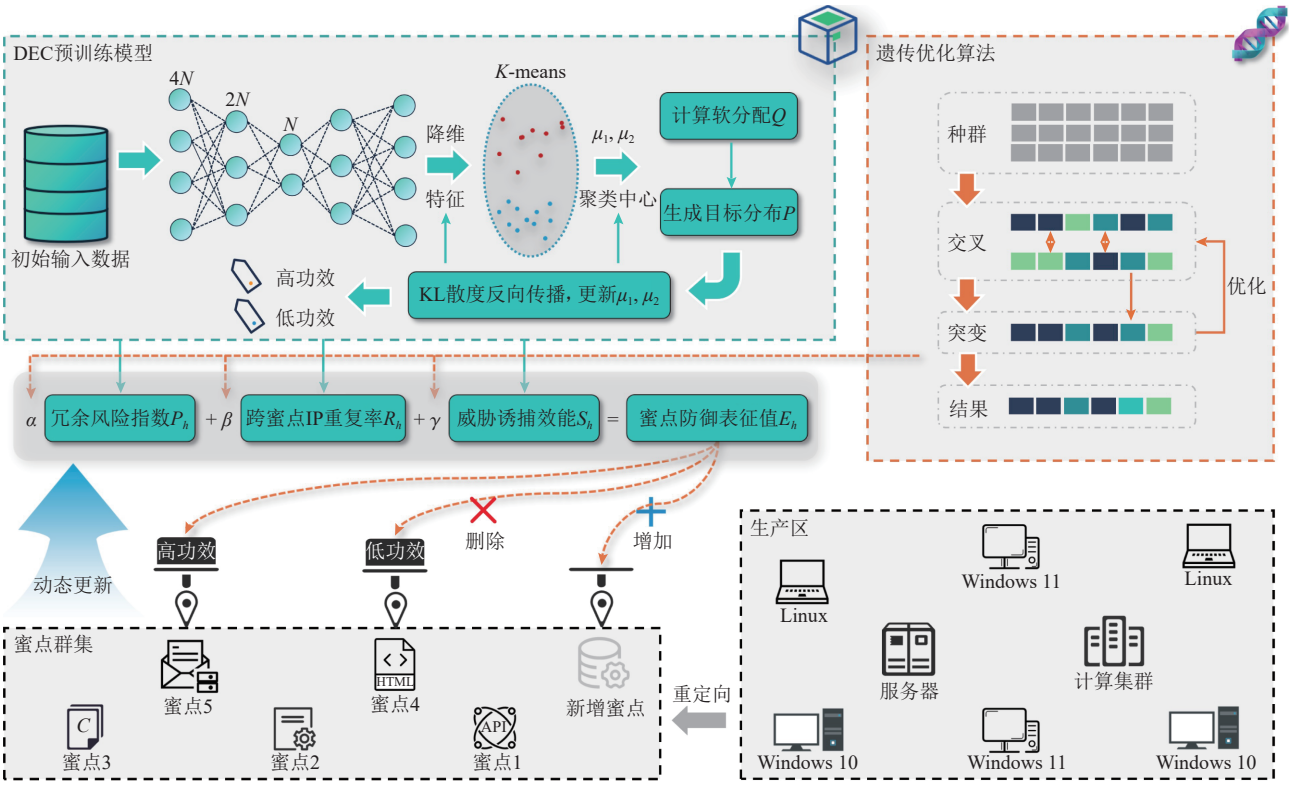


Fig. 2 Honeypot effectiveness evaluation framework based on deep embedded clustering and evolutionary collaborative optimization

图 2 基于深度嵌入聚类与进化协同优化的蜜点效能评估框架

针构成的协同感知网络，侧重于全局威胁情报的实时汇聚、跨域攻击关联与弹性资源调度；蜜洞作为面向加密流量与深度协议重定向的隐蔽诱捕通道，其侧重于协议逆向解析的完整性、诱捕环境的隐匿性以及攻击流转发的透明度。上述模块通过协同联动构建多层级诱捕网络，实现对复杂攻击行为的闭环防御。

本文所研究的蜜点集群防御体系基于盾立方框架中的自适应诱捕节点实现，包含哨兵监控进程、协议栈仿真引擎、流量镜像调度器与动态拓扑混淆模块。在实现层面，蜜点通过容器化技术（如 docker 与 kubernetes）进行智能预置与弹性扩缩。每个蜜点实例内嵌具有行为感知能力的哨兵进程，实时监控并记录攻击交互行为。其表层协议栈通过高保真服务指纹模拟引擎实现对 HTTP, SSH, Modbus 等多种协议的动态仿真。为进一步增强欺骗隐蔽性，系统采用软件定义网络（software-defined networking, SDN）技术实现流量动态调度与重定向，并结合拓扑混淆策略构建虚拟化诱捕场域，从而在资源受限场景下实现高交互、低开销的分布式欺骗防御能力。

2.2 蜜点效能指数多维指标体系构建

为全方位、精准刻画蜜点在网络欺骗防御中的综合表现，亟需构建多维复合量化评估体系。本文创新性地提出蜜点冗余风险指数、跨蜜点 IP 重复率及威胁诱捕效能评分 3 项核心指标，并通过深度融合多维指标，构建多指标协同的蜜点防御表征值，以系统性反映蜜点防御的整体效能。

2.2.1 蜜点冗余风险指数

蜜点冗余风险指数旨在定量评估单一蜜点在整个蜜点防御体系中的冗余配置现象。该指标考察在一定时间窗口内，是否存在某个踩蜜 IP 同时激活多个蜜点的情况，从而揭示防御体系中因冗余蜜点部署造成的资源浪费问题。其数学表达式定义为

$$P_h = \frac{\sum_{\mathrm{IP}\in I(h)} \Phi(\exists r \neq h, \mathrm{IP} \in I(r))}{|I(h)|}, \tag{1}$$

其中 $I(h)$ 表示与蜜点 h 关联的 IP 地址集合，$I(H)$ 为整个蜜点体系涉及的 IP 地址集合；指示函数 $\Phi(\cdot)$ 在满足给定条件时取值为 1，否则取值为 0。较高的 P_h 值表明在一段时间窗口内，同一踩蜜 IP 有可能激活多个蜜点，从而反映出防御体系中存在显著的蜜点冗余配置效应。

2.2.2 跨蜜点 IP 重复率

跨蜜点 IP 重复率用于定量分析蜜点之间的相互影响，具体通过衡量在特定时间段内，同一 IP 地址同时触发多个蜜点的频率来实现。如果跨蜜点 IP 重复

率较高，这通常意味着这些 IP 可能来自进行广泛扫描的攻击者，也反映出不同蜜点在吸引攻击者方面存在较高的相似性。这一指标能够有效评估蜜点之间的独立性，为优化蜜点的部署策略提供重要依据。其数学定义如下：

$$R_h = \frac{\sum_{r \neq h} |I(h) \cap I(r)|}{|I(h)|} 。 \tag{2}$$

2.2.3 威胁诱捕效能评分

为了全面评估蜜点在面对复杂攻击情境下的响应能力，本文还提出了威胁诱捕效能评分。该指标基于威胁情报中的风险标签体系，量化蜜点应对攻击的欺骗防御效果。具体而言，该指标通过计算每次踩蜜事件所关联的威胁标签集合及其对应的风险严重性分值 *severity*(*l*)，从而衡量蜜点对不同威胁的感知与捕获能力。其数学定义如下：

$$S_h = \frac{\sum_{i \in T(h)} \sum_{l \in L_i} severity(l)}{|T(h)|}, \tag{3}$$

其中 L_i 表示第 i 次踩蜜事件所关联的威胁标签集合，$|T(h)|$表示蜜点 h 在观测期内被踩蜜的总次数。该指标反映了其在多种攻击类型下的适应性和诱捕效果，有助于评估蜜点在防御体系中的实际效能。

2.2.4 多指标协同蜜点防御表征值

根据各项指标和实际应用需求，本文进一步构建了多指标协同蜜点防御表征值，以量化评估蜜点的整体有效性及部署优先级。该指标综合考虑蜜点冗余风险指数 P_h、跨蜜点 IP 重复率 R_h 以及威胁诱捕效能评分 S_h，从多个维度衡量蜜点的实际部署价值。其数学定义如下：

$$E_h = \alpha S_h - \beta P_h - \gamma R_h, \tag{4}$$

其中 α、β、γ 分别表示各指标的权重系数，用于量化和调节不同因素对蜜点综合防御效能的贡献。较高的 E_h 值表明该蜜点在欺骗防御中的表现优异，应该维持其部署状态；相反，较低的 E_h 值则反映了该蜜点在当前防御环境中的响应能力较弱，需将其从防御体系中剔除，以优化资源配置，提升整体防御效能。

通过定期计算多指标协同蜜点防御表征值，可实时评估蜜点效能并据此优化部署策略，确保防御系统高效运行，避免资源浪费。该方法提升了欺骗防御体系的灵活性与智能化水平，有助于应对不断变化的网络安全威胁。

2.3 基于深度潜入聚类的蜜点有效性评估

在复杂网络威胁环境下，蜜点防御效能的精准评估是优化资源分配、提升威胁诱捕能力的关键环节。本文提出基于深度聚类的蜜点有效性评估框架，通过无监督深度嵌入聚类技术，结合蜜点冗余风险指数 P_h、跨蜜点 IP 重复率 R_h、威胁诱捕效能评分 S_h 核心指标，构建数据驱动的蜜点自动化分类模型，为后续多指标协同蜜点防御表征值 E_h 中权重系数 α，β，γ 的全局优化提供可靠的类别标签。

2.3.1 面向蜜点评估的特征重构机制

DEC 模型首先通过自编码器（autoencoder）将原始高维特征映射至低维潜在空间。编码器网络由 3 层全连接层构成，输入层维度与蜜点多指标特征维度一致（d=3）。隐含层逐步压缩至编码维度（d'=2），数学表达为

$$\boldsymbol{z}_h = Encoder(\boldsymbol{x}_h; \theta_e) = \sigma(\boldsymbol{W}_3 \cdot \sigma(\boldsymbol{W}_2 \cdot \sigma(\boldsymbol{W}_1 \boldsymbol{x}_h + \boldsymbol{b}_1) + \boldsymbol{b}_2) + \boldsymbol{b}_3), \tag{5}$$

其中 $\boldsymbol{x}_h \in \mathbb{R}^3$ 为蜜点 h 的原始特征向量，σ 为 ReLU 激活函数，$\theta_e = \{\boldsymbol{W}_i, \boldsymbol{b}_i\}$ 为编码器参数。低维嵌入 $\boldsymbol{z}_h$ 通过非线性映射在一定程度上去除了噪声干扰，同时保留蜜点间的判别性差异。

自编码器通过最小化输入特征与重构输出之间的均方误差进行参数优化，其重构损失函数定义为

$$\mathcal{L}_{rec} = \frac{\sum_{h=1}^{N} \| \boldsymbol{x}_h - \hat{\boldsymbol{x}}_h \|^2}{N}, \tag{6}$$

其中 $\hat{\boldsymbol{x}}_h = Decoder(\boldsymbol{z}_h; \theta_d)$ 为解码器重构输出，θ_d 为解码器参数。该损失函数通过逐点误差平方和计算，有效保留特征空间中的几何结构信息。

2.3.2 基于软分配的蜜点类别概率建模

在低维空间基础上，DEC 模型引入聚类层，通过学生 t 分布（student's t-distribution）计算蜜点 $\boldsymbol{z}_h$ 与聚类中心 $\boldsymbol{u}_k$ 的相似性，生成软分配概率矩阵 $\boldsymbol{q}_{hk}$：

$$\boldsymbol{q}_{hk} = \frac{\left(1 + \frac{\| \boldsymbol{z}_h - \boldsymbol{\mu}_k \|^2}{\omega}\right)^{-\frac{(\omega+1)}{2}}}{\sum_{k'=1}^{K} \left(1 + \frac{\| \boldsymbol{z}_h - \boldsymbol{\mu}_{k'} \|^2}{\omega}\right)^{-\frac{(\omega+1)}{2}}}, \tag{7}$$

其中 ω 为自定义的自由度参数，K=2 对应高效和低效 2 个蜜点类别，其中 h 表示样本索引（即蜜点），k 表示聚类中心的编号。软分配概率不仅量化了蜜点归属的置信度，还通过概率分布刻画类别边界的模糊性。

2.3.3 动态聚类中心优化与防御策略迭代

在蜜点效能评估中，为了实现精确区分高效与低效蜜点，DEC 模型在聚类阶段引入了基于 KL 散度

(Kullback-Leibler divergence)的损失函数,该损失函数旨在缩小软分配概率 $\boldsymbol{q}_{hk}$ 与目标分布 $\boldsymbol{p}_{hk}$ 之间的差距,从而进一步强化不同类别之间的区分度。KL 散度损失函数定义为

$$\mathcal{L}_{\mathrm{KL}}=\sum_{h=1}^{N}\sum_{k=1}^{K}\boldsymbol{p}_{hk}\ln\frac{\boldsymbol{p}_{hk}}{\boldsymbol{q}_{hk}}, \tag{8}$$

其中,$\boldsymbol{p}_{hk}$ 通常由对当前软分配概率 $\boldsymbol{q}_{hk}$ 经过平滑处理(如归一化或加权调整)得到,其目的在于"强化"正确类别的置信度,降低类别间的模糊边界。模型在训练过程中通过反向传播算法,不断更新编码器参数 θ_{e} 与聚类中心 $\boldsymbol{u}_k$,使得 KL 散度损失函数达到最小值,从而实现聚类结果的收敛和优化。整个训练流程可划分为 2 个阶段:

1)预训练阶段。利用自编码器重构损失函数对原始高维特征进行降噪和有效表达,将特征映射到低维嵌入空间。此过程保证了低维表示不仅保持了原始特征的主要信息,还消除了部分噪声干扰。

2)微调阶段。在固定解码器参数的基础上,针对聚类目标对编码器和聚类层参数进行精细调整,在这个过程中采用 KL 散度损失作为主要优化目标,以确保聚类中心能够自适应地捕捉蜜点在低维空间中的内在分布特性。

模型训练完成后,通过计算各蜜点特征向量 $\boldsymbol{z}_h$ 与聚类中心 $\boldsymbol{u}_k$ 的隶属度概率 $\boldsymbol{q}_{hk}$,采用最大概率准则生成最终类别标签:

$$\boldsymbol{Y}_h=\arg\max_{k}\boldsymbol{q}_{hk},\ k\in\{0,1\}。 \tag{9}$$

算法 1 给出了 DEC 模型的训练过程,步骤包括参数初始化、预训练、聚类中心的初始化(通常利用 *K*-means 对低维嵌入结果进行初步划分获得初始聚类中心),以及在微调阶段对聚类层参数的更新。

算法 1. 基于深度嵌入聚类的蜜点有效性评估。

输入:特征矩阵 $\boldsymbol{X}=(P_h, R_h, S_h)\in\mathbb{R}^{N\times 3}$,聚类数 $K=2$,预训练周期 T_{p},微调周期 T_{f};

输出:聚类标签 $\boldsymbol{Y}\in\{0,1\}^N$。

① for $t=1$ to T_{p} do

② $\boldsymbol{Z}\leftarrow Encoder(\boldsymbol{X};\theta_{\mathrm{e}}), \boldsymbol{X}_{\mathrm{rec}}\leftarrow Decoder(\boldsymbol{Z};\theta_{\mathrm{d}})$;

③ $\theta_{\mathrm{e}};\theta_{\mathrm{d}}\leftarrow\arg\min_{\theta_{\mathrm{e}},\theta_{\mathrm{d}}}\|\boldsymbol{X}-\boldsymbol{X}_{\mathrm{rec}}\|_{\mathrm{F}}^2$; /*Adam 优化*/

④ end for

⑤ $\{\boldsymbol{\mu}_k\}\leftarrow K\text{-}means(Encoder(\boldsymbol{X};\theta_{\mathrm{e}}))$; /*初始化聚类中心*/

⑥ for $t=1$ to T_{f} do

⑦ $\boldsymbol{Z}\leftarrow Encoder(\boldsymbol{X};\theta_{\mathrm{e}})$;

⑧ $\boldsymbol{Q}\leftarrow ComputeSoftAssignments(\boldsymbol{Z},\{\boldsymbol{\mu}_k\})$; /*$t$ 分布*/

⑨ $\boldsymbol{P}\leftarrow GenerateTargetDist(\boldsymbol{Q})$; /*目标分布*/

⑩ $L\leftarrow KL(\boldsymbol{P}\|\boldsymbol{Q})$;

⑪ $\theta_{\mathrm{e}}\leftarrow\theta_{\mathrm{e}}-\eta\nabla L$;

⑫ $\boldsymbol{\mu}_k\leftarrow UpdateCentroids(\boldsymbol{Q},\boldsymbol{Z})$; /*反向传播,质心更新*/

⑬ end for

⑭ $\boldsymbol{Y}\leftarrow\arg\min_{k}\boldsymbol{Q}$; /*硬分配*/

⑮ return $\boldsymbol{Y}$。

2.4 基于遗传算法的蜜点效果指数优化

在网络欺骗防御体系的动态部署中,蜜点效能评估是保障资源配置优化与威胁诱捕能力持续提升的核心环节。然而,基于深度嵌入聚类的蜜点有效性评估方法虽能有效区分高效蜜点与低效蜜点,但其特征重构与软分配计算过程存在计算资源密集型特点,难以满足实际部署场景中对实时性与敏捷性的要求。为此,本文提出一种融合深度嵌入聚类与遗传优化的协同框架,通过动态调整多指标协同蜜点防御表征值 E_h 的权重系数 α, β, γ,实现蜜点效能的快速量化评估。

2.4.1 染色体编码与种群初始化

在遗传算法中,每个个体通过权重向量 $\boldsymbol{w}=(w_1, w_2, w_3)$ 表征蜜点效能指数中各核心指标的贡献权重,其中 w_1, w_2, w_3 分别对应于 2.2 节中蜜点冗余风险指数 P_h、跨蜜点 IP 重复率 R_h、威胁诱捕效能评分 S_h 在多指标协同表征值中的贡献权重。为了保证各权重满足非负及归一化条件,初始种群采用 Dirichlet 分布进行随机生成,其数学表达式为

$$\boldsymbol{w}\sim Uniform(\tau_{\min},\tau_{\max}), \tag{10}$$

其中 $\tau_{\min}$ 和 $\tau_{\max}$ 分别代表权重向量的上界约束与下界约束。在离线优化阶段,执行全域搜索策略,根据 2.3 节中 DEC 聚类获得的先验分类标签,遗传算法可筛选出使蜜点综合效能评分与聚类标签匹配程度最高的权重向量,作为定期蜜点效能评估的参数基准。

2.4.2 适应度函数设计与评价标准

适应度函数的设计机理在于量化给定权重配置向量 $\boldsymbol{w}$ 计算得到的蜜点综合效能评分 E_h 与 DEC 聚类获得的先验分类标签之间的一致性。如 2.3 节所述,基于 DEC 算法能够将蜜点划分为高效能与低效能两大类别。本文通过遗传算法优化权重组合,使得 2.2 节建立的综合效能计算模型的输出值 $E_h(\boldsymbol{w})$ 与 DEC 聚类特征空间实现最大程度映射对齐。

定义蜜点 h 在权重配置 $\boldsymbol{w}$ 下的多指标协同蜜点防御表征值为 $E_h(\boldsymbol{w})$, 其对应的 DEC 聚类标签记为 C_h。在此基础上, 引入指示函数 $\mathbb{I}(\cdot)$ 来衡量预测分类与聚类标签的一致性(当 $\mathbb{I}(\cdot)$ 的括号内条件成立时 $\mathbb{I}(\cdot)$ 取值为 1, 否则为 0)。适应度函数定义为

$$F(\boldsymbol{w})=\frac{\sum_{h=1}^{N}\mathbb{I}\left(\operatorname{sgn}(E_h(\boldsymbol{w}))=C_h\right)}{N}。\tag{11}$$

2.4.3 遗传操作与优化流程

为提升权重参数空间的全局寻优效率, 遗传算法在种群进化过程中采用了选择、交叉与变异等操作。进化过程中, 通过基于适应度比例的概率选择机制遴选亲本个体, 为交叉操作提供优质基因源。交叉阶段实施带边界约束的模拟二进制交叉(simulated binary crossover, SBX)操作, 数学表达式为

$$\begin{aligned}\boldsymbol{w}_i^{\text{new}}&=0.5\left((1+\lambda)\boldsymbol{w}_i^{p_1}+(1-\lambda)\boldsymbol{w}_i^{p_2}\right),\\ \boldsymbol{w}_j^{\text{new}}&=0.5\left((1-\lambda)\boldsymbol{w}_j^{p_1}+(1+\lambda)\boldsymbol{w}_j^{p_2}\right),\end{aligned}\tag{12}$$

其中扩展因子 λ 的计算公式由随机数 $\delta\sim Uniform(0,1)$ 决定:

$$\lambda=\begin{cases}(2\delta)^{\frac{1}{\eta_c+1}}, & \text{if } \delta\leqslant 0.5,\\ \left(\dfrac{1}{2(1-\delta)}\right)^{\frac{1}{\eta_c+1}}, & \text{其他},\end{cases}\tag{13}$$

其中 η_c 为交叉分布指数, 该参数控制子代个体在父代附近的分布范围。参数 λ 反映了亲本个体间的基因型差异度, 通过平衡子代个体对优势遗传特征的继承强度与空间探索能力, 有效维持解空间遍历的广域性。为提升种群多样性并规避局部最优收敛风险, 算法在交叉阶段后嵌入了多项式变异(polynomial mutation)算子, 对候选解向量的特定维度施加随机扰动, 其数学表达式为

$$\boldsymbol{w}_i^{\text{new}}=\boldsymbol{w}_i+\Delta\cdot(\boldsymbol{w}_i^{\text{upper}}-\boldsymbol{w}_i^{\text{lower}})。\tag{14}$$

扰动参数 Δ 的计算满足以下分段约束:

$$\Delta=\begin{cases}(2\delta)^{\frac{1}{\eta_m+1}}-1, & \text{if } \delta\leqslant 0.5,\\ 1-(2(1-\delta))^{\frac{1}{\eta_m+1}}, & \text{其他}。\end{cases}\tag{15}$$

基于多项式分布的变异算子通过引入可控随机扰动机制, 增强了种群在解空间中的遍历能力, 构建了全局收敛保障机制以突破局部极值约束。此外, 交叉与变异生成的新个体均会通过边界截断机制确保权重处于合法可行域内。算法 2 给出了整个基于遗传算法的蜜点效果指数优化流程, 在经过若干迭代后, 种群内个体逐步向使蜜点综合效能评分 $E_h(\boldsymbol{w})$ 与 DEC 聚类结果高度一致的最优权重向量靠拢, 最终确定出一组唯一最优的权重系数。

算法 2. 基于遗传算法的蜜点效果指数优化。

输入: 特征矩阵 $\boldsymbol{X}=(P_h, R_h, S_h)\in\mathbb{R}^{N\times 3}$, 聚类标签 $\boldsymbol{Y}\in\{0,1\}^N$, 种群规模 M, 迭代数 G, 概率阈值 p_c, p_m;

输出: 最优权重 $\boldsymbol{w}^*=\{\alpha^*,\beta^*,\gamma^*\}$。

① $\boldsymbol{P}(0)\leftarrow\{\boldsymbol{w}_i\mid i=1,2,\cdots,M\}$; /*种群初始化*/

② for $g=1$ to G do

③ $F(\boldsymbol{P}(g))\leftarrow AssessFitness(\boldsymbol{P}(g),\boldsymbol{X},\boldsymbol{Y})$; /*适应度评估(式(11))*/

④ $\boldsymbol{P}_{\text{sel}}\leftarrow TournamentSelect(\boldsymbol{P}(g-1),F(\boldsymbol{P}(g-1)),M)$; /*锦标赛选择最佳个体*/

⑤ for each $(\boldsymbol{w}_a,\boldsymbol{w}_b)\in\boldsymbol{P}_{\text{sel}}$ do

⑥ if $U(0,1)<p_c$ then

⑦ $(\boldsymbol{w}_c^1,\boldsymbol{w}_c^2)\leftarrow SBXCross(\boldsymbol{w}_a,\boldsymbol{w}_b)$; /*模拟二进制交叉*/

⑧ end if

⑨ end for

⑩ for each offspring $\boldsymbol{w}_c$ do;

⑪ if $U(0,1)<p_m$ then

⑫ $\boldsymbol{w}_c'\leftarrow PolyMutate(\boldsymbol{w}_c,\eta_m)$; /*多项式边界扰动及约束修复*/

⑬ end if

⑭ end for

⑮ $\boldsymbol{P}(g)\leftarrow UpdatePopulation$(all offsprings);

⑯ end for

⑰ return $\arg\max_{\boldsymbol{w}\in\boldsymbol{P}(G)}F(\boldsymbol{w})$, $\boldsymbol{w}^*$。

3 实验分析

为验证基于深度嵌入聚类与进化协同优化的蜜点效能评估在真实网络防护场景中的有效性, 本实验基于盾立方系统在 2025 年亚洲冬季运动会一段时间内的网络安全运营数据开展实证研究。原始数据通过分布式蜜点集群动态捕获, 共获取 473 265 条踩蜜事件日志, 每条记录覆盖攻击源 IP 地址、时间戳、地理位置、代理状态、攻击类型(如漏洞扫描、暴力破解)等核心字段。基于多维聚合操作, 以攻击源 IP 为基准单元, 统计其首次与最近活跃时间窗口、累计踩蜜日志数量、攻击类型分布(基于情报标签字段的复合分类, 如“DDoS 攻击”“WEB 攻击”“僵尸网络”等)。经数据清洗与聚合后形成结构化分析数据集 12 466 条, 每条记录表征独立攻击实体的行为轮廓, 包含时序活跃特征(首次/最近时间)、空间传播特征(地理位置、代理状态)、攻击模式特征(攻击类型、

情报标签、触发攻击告警标识)。

实验采用双重数据划分策略(训练集数量(N_{Tr})与测试集数量(N_{Te})的比值等于 6: 4 和 5: 5)构建验证框架。基于训练集数据构建基于深度嵌入聚类与进化协同优化的蜜点效能评估: 首先深度嵌入聚类获取蜜点效能标签并与活动中蜜点真实标签对比; 随后利用遗传算法优化多维指标的权重系数。在测试集验证阶段, 通过对比蜜点效能评估模型的输出结果与赛时实际高价值诱捕节点的一致性, 从实际防护效能维度证实提出的闭环评估体系对网络威胁的适应性。

本文实验基于 Python 3.9.12 构建技术框架, 并采用 scikit-learn 1.5.2 进行特征标准化与聚类验证。深度嵌入聚类模型由 tensorflow 2.18.0 搭建, 包含 4 层全连接结构, 输入层维度为 3, 经 64 维与 32 维编码层的非线性变换后映射至 2 维潜在空间, ReLU 作为激活函数实现特征转换。聚类层基于学生 t 分布计算软分配概率, 并通过 KL 散度损失函数优化聚类中心。遗传算法采用 deap 1.4.2 实现, 初始种群规模设为 100, 使用锦标赛选择策略(竞赛规模为 3), 结合模拟二进制交叉算子(概率为 0.7)和多项式边界变异算子(初始概率为 0.3), 并引入动态衰减机制优化参数搜索空间。模型训练分为 2 个阶段: 第 1 阶段, DEC 预训练采用 300 轮自编码器重构优化, 以获取初始特征表示。第 2 阶段, 通过 200 轮迭代优化聚类分布, 同时结合遗传算法进行前沿分析, 筛选全局最优权重组合。

3.1 多维指标协同分析

基于双重数据划分策略(N_{Tr}与N_{Te}的比值等于 6∶4 和 5∶5), 本文系统量化了蜜点防御效能的 3 维评价体系: 威胁诱捕效能评分、跨蜜点 IP 重复率与蜜点冗余风险指数。在 2 组实验场景下分别选取了 7 个典型蜜点作为分析样本, 其综合防御表征值由正向指标(威胁诱捕效能评分)与负向指标(跨蜜点 IP 重复率、蜜点冗余风险指数)共同确定。实验数据表明, 蜜点 A(图 3(a))和蜜点 D(图 3(b))在威胁诱捕效能评分分别达到 74.22 和 73.26 的显著高位, 同时跨蜜点 IP 重复率(分别为 1.08 和 1.13)与蜜点冗余风险指数(分别为 0.36 和 0.31)均处于低位区间, 展现出最优综合防御效能; 而蜜点 E, F(图 3(a))及蜜点 D, G(图 3(b))则因正向指标衰减伴随负向指标攀升, 导致防御效能显著降低。该 3 维分析有效揭示了防御效能与资源冗余之间的均衡关系, 为后续深度嵌入聚类与进化协同优化的动态调参奠定了量化基准。

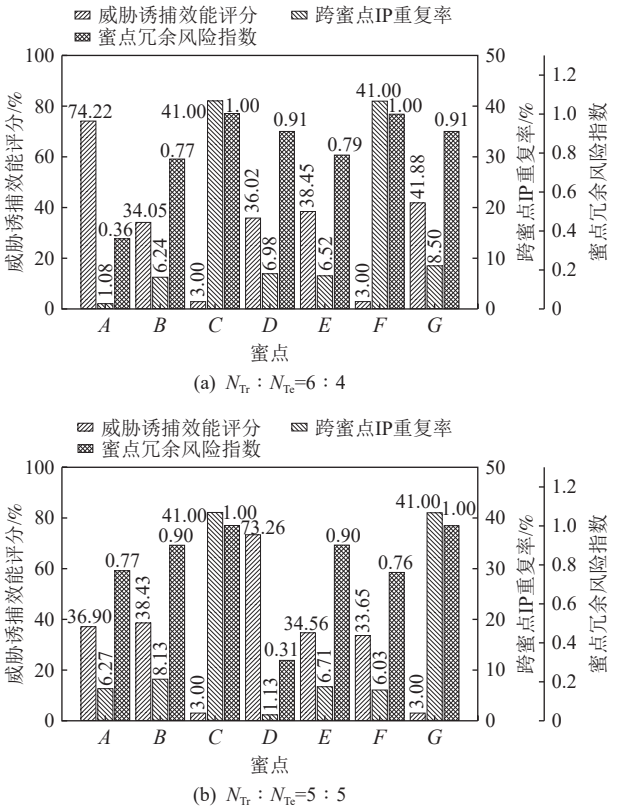


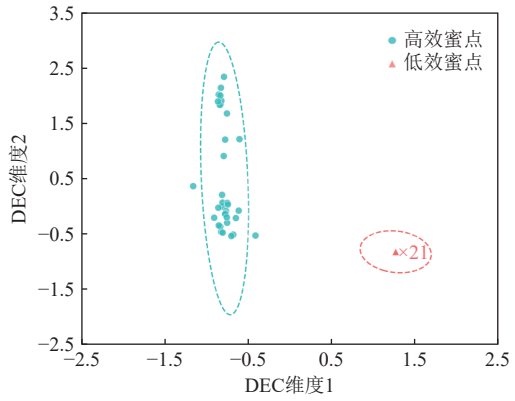
Fig. 3 Comparison of multi-dimensional metrics for honey point defense effectiveness

图 3 蜜点防御效能多维指标对比

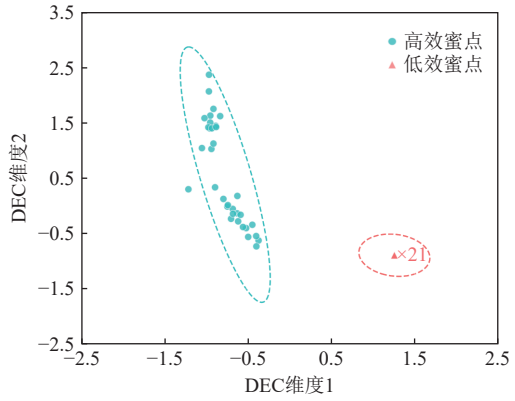
3.2 深度嵌入聚类性能分析

本文基于 DEC 算法构建蜜网效能评估框架, 通过多模态数据划分策略的对照实验, 系统性地验证了模型在异构数据分布下的无监督表征学习能力。可视化分析表明(图 4(a)与图 4(b)), DEC 算法在潜在空间中实现了高效蜜点与低效蜜点的几何可分性解耦, 2 类样本的分布呈现显著空间异质性。实验观测到, 低效蜜点簇在 DEC 维度 1 的正值区间(>0)形成独立聚集区, 其中 21 个样本(标识为“×21”)因冗余风险指数、跨蜜点 IP 重复率与威胁诱捕效能评分的欧氏距离均值趋近于零, 呈现单峰聚集分布特征(频次达 21)。相较之下, 高效蜜点在 DEC 维度 1 的负值区间展现出非线性分布特性, 其空间拓扑结构与动态防御场景中的节点行为多样性呈严格映射关系。值得注意的是, 不同划分模式下聚类决策边界(DEC 维度 1 等于 0)均与亚冬会实际场景下的蜜点效能结果完全一致, 表明 DEC 算法通过非线性流形学习构建的评估体系对数据分类具有强可靠性。

进一步通过维度特征频次分布的系统性分析(图 5(a)与图 5(b))发现, DEC 维度 1 作为核心判别维度呈现严格的双极分化特性, 其正负值域分别精准



(a) N_{Tr} : N_{Te}=6 : 4

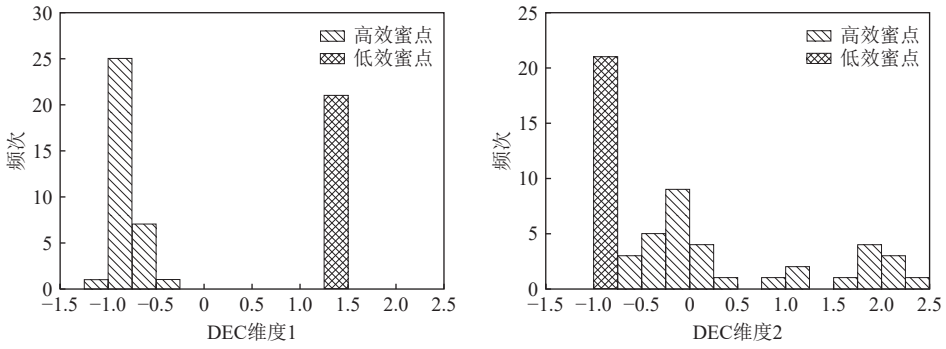


(b) N_{Tr} : N_{Te}=5 : 5

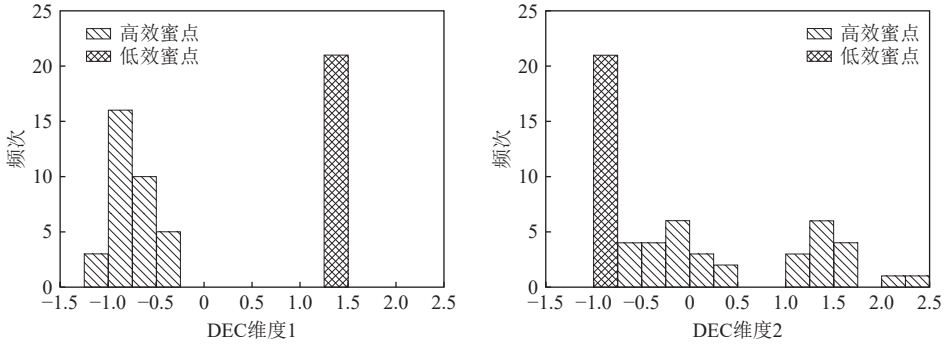
Fig. 4 Feature space mapping via deep embedded clustering

图 4 基于深度嵌入聚类的特征空间映射

对应不同防御效能的蜜点集群。DEC 维度 2 的分布模式揭示低效蜜点存在显著的同质化问题，在 [−1.0, −0.75] 区间的频次稳定维持在 21 次，该同质化分布特性表明低效蜜点在攻击响应机制与资源调度维度存在系统性战术冗余。相比之下，高效蜜点在 DEC 维度 2 的 [0.0, 2.0] 区间展现宽幅分布格局，表明该类蜜点的诱捕策略具备动态自适应调节能力。综上所述，低效蜜点由于冗余风险指数与跨蜜点 IP 重复率显著偏高的双重叠加效应，呈现出明显的同质化分布特征，其诱捕效能已被高效蜜点完全覆盖，进一步暴露出防御体系中存在的资源冗余问题；相比之下，高效蜜点凭借更高的威胁诱捕效能评分与对动态攻击场景的强适配能力，在特征空间中展现出明显的非线性拓扑分异特性。通过对比 DEC 无监督分类结果与亚洲冬季运动会蜜点的实际运维标签，进一步验证了模型输出的效能预标签与实际高价值节点分布高度一致，分类准确率达到 100%。本节构建的基于 DEC 的无监督分类框架，不仅为蜜点效能差异提供了量化判别依据，也为后续遗传算法优化过程中蜜点防御表征值权重系数的动态校准（聚焦威胁诱捕效能评分、跨蜜点 IP 重复率与蜜点冗余风险指数的协同优化）提供了高置信度的监督信号与优化准则，从而为“评估—反馈—调优”闭环防御体系的实现奠定分类基准。



(a) N_{Tr} : N_{Te}=6 : 4



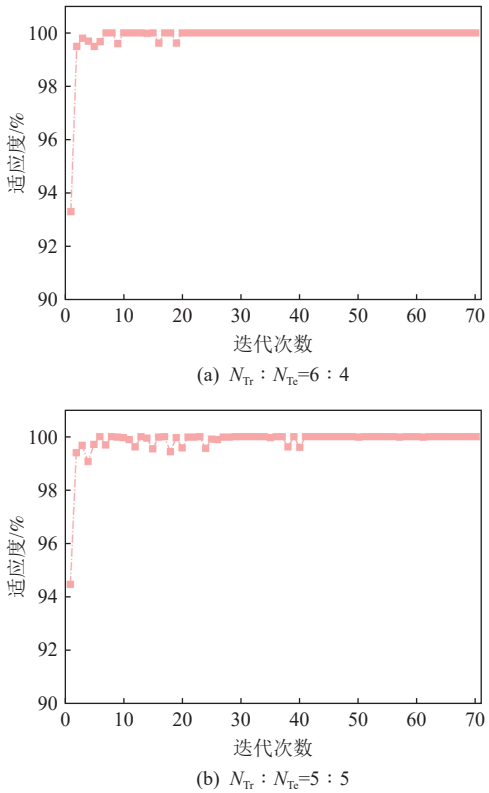
(b) N_{Tr} : N_{Te}=5 : 5

Fig. 5 Frequency divergence patterns of honey point defense efficacy in dual-dimensional statistic characteristics

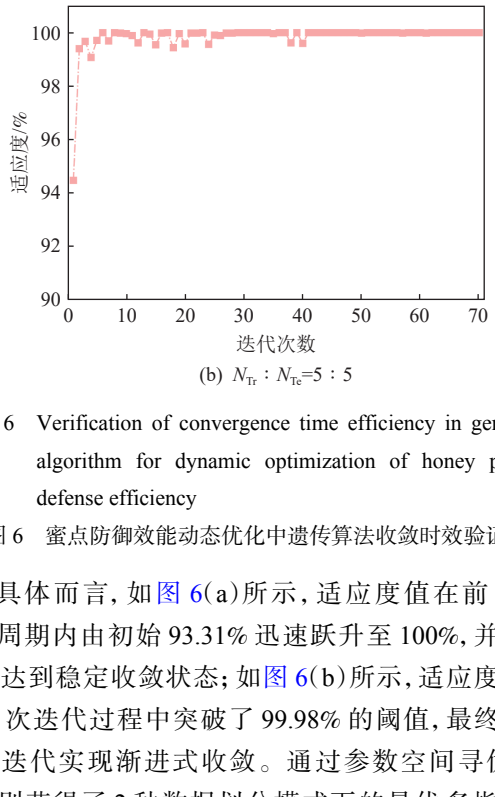
图 5 双维度统计特性下蜜点防御效能频次分异规律

3.3 遗传算法优化过程分析

本文基于 DEC 的无监督预分类框架，构建了基于动态权重调优机制的防御效能量化评估体系。通过引入遗传算法实现蜜点防御表征值权重系数的自适应优化。如图 6 所示，在 2 种训练集与测试集划分模式下，遗传算法的适应度函数均呈现超线性收敛特性。



(a) N_{Tr} : N_{Te}=6 : 4



(b) N_{Tr} : N_{Te}=5 : 5

Fig. 6 Verification of convergence time efficiency in genetic algorithm for dynamic optimization of honey point defense efficiency

图 6 蜜点防御效能动态优化中遗传算法收敛时效验证

具体而言，如图 6(a)所示，适应度值在前 10 次迭代周期内由初始 93.31% 迅速跃升至 100%，并在第 22 代达到稳定收敛状态；如图 6(b)所示，适应度值在前 15 次迭代过程中突破了 99.98% 的阈值，最终经过 40 代迭代实现渐进式收敛。通过参数空间寻优，实验分别获得了 2 种数据划分模式下的最优多指标协同蜜点防御表征值计算公式，具体如下：

$$E_h = 0.645\,2S_h - 0.667\,2P_h - 0.701\,8R_h 。 \quad (16)$$

$$E_h = 0.457\,8S_h - 0.128\,4P_h - 0.421\,3R_h 。 \quad (17)$$

将优化后的防御表征值模型分别应用于对应测试集，其蜜点效能二分类结果(E_h>0 为高效，E_h≤0 为低效)与亚洲冬季运动会期间蜜点实际标签(基于蜜点存活周期与威胁捕获量标注)的一致率达到 100%。该结果表明，提出的基于深度嵌入聚类与进化协同的蜜点防御效能评估模型不仅实现了无监督分类与监督优化的无缝衔接，更通过权重系数的自适应校准，精准捕获了攻防对抗场景下蜜点效能演化的本质规律。基于此，在工程部署过程中可直接采用优化后的线性表达式对蜜点防御效能进行周期性评估。通过定期计算 E_h 并动态调整节点部署策略，在保证评估精度的前提下有效降低计算开销与时间成本，从而为大规模蜜网防御体系的实时效能管理提供一种可落地的轻量化解决方案。

3.4 对比分析

为进一步从系统架构与机制演进层面阐释本文方法的性能优势，我们将所提出的方法与现有具有代表性的动态欺骗防御研究进行了多维度定性对比分析，相关研究涵盖基于静态博弈建模的方法[4]、容器化与编排驱动的防御框架[13]，以及强化学习与动态博弈优化等技术路线[14,33,35]，具体对比结果如表 1 所示。综合分析可见，传统依赖静态纳什均衡或预定义模板配置的防御策略通常受限于固定的策略空间，在高频演化的攻防对抗场景中难以维持有效性；而引入 Q-Learning 或动态信念更新机制的改进方案，尽管在局部交互层面提升了策略调整的灵活性，但在面对大规模、异构且高度动态的网络环境时，往往因状态空间急剧膨胀或反应式策略更新滞后而遭遇显著的可扩展性瓶颈。相比之下，本文提出的系统级蜜点集群优化框架从整体架构层面重构了欺骗防御的演进路径。通过构建多维效能表征体系，并引入深度嵌入聚类先验与遗传进化机制的协同优化，实现了防御策略由“被动响应”向“主动演进”的根本转变。该框架不仅支持基于实时效能评估的闭环自适应调优，还能够借助智能化资源编排机制实现超大规模蜜点集群的弹性伸缩，从而在动态攻防态势持续演化的条件下，有效保障防御策略的近最优性与系统架构的整体鲁棒性。

4 结 论

针对动态网络威胁环境中蜜点集群防御效能的持续衰减问题，本文提出了一种融合多维量化表征与智能优化机制的闭环防御体系。该体系以冗余风险指数、跨蜜点 IP 重复率和威胁诱捕效能评分为核心指标，构建了复合指标体系，并结合深度嵌入聚类驱动的效能分类模型以及遗传进化策略导向的权重自适应机制，实现了防御资源配置的动态优化和安

Table 1 Comparison of Dynamic Update and Optimization Capabilities of Dynamic Deception Defense Methods

表 1 动态欺骗防御方法动态更新优化能力对比

方法	研究层面	核心技术	动态适应性	可扩展性
文献 [4]	单点/静态防御策略选取	随机博弈建模 + 纳什均衡求解 + 攻防成本量化	[低] 静态均衡策略，缺乏在线适应	[中] 状态空间随节点增长，存在指数级扩展瓶颈
文献 [13]	蜜罐部署配置模板化	Kubernetes 容器编排 + Helm Chart 模板化管理	[低] 静态模板化配置，缺乏运行时自适应调整	[高] 依托容器编排平台原生能力，具备良好的架构弹性与横向扩展性
文献 [14]	网络级蜜罐部署优化	Q-Learning 强化学习 + 攻防效用博弈建模	[中] 反应式按需调整，策略更新滞后	[中] 模基于固定比例与静态环境建模，弹性扩展能力受限
文献 [33]	单点蜜罐交互策略优化	动态博弈建模 + 攻击方信念更新 + 近似混合策略均衡求解	[中] 基于信念与识别能力动态调整响应策略，支持多轮交互优化	[中] 基于简化场景与静态假设，大规模复杂环境扩展性受限
文献 [35]	单点蜜罐交互策略优化	Q-Learning 强化学习 + 攻击命令分类与严重性分析	[中] 基于 Q-Learning 的自适应动作选择，奖励函数硬编码且状态空间有限	[低] 基于单实例部署与表格型 Q-Learning，状态空间受限，难以扩展至大规模复杂环境
本文	系统级蜜点集群优化	多维效能表征体系 + 深度嵌入聚类先验标注 + 遗传进化权重自适应优化	[高] 基于实时效能评估的闭环动态调优与策略演进	[高] 支持面向动态攻防态势的超大规模集群自适应弹性部署与智能资源编排

全效能的持续提升，最终形成了“评估—反馈—调优”的闭环防御架构。该方法在 2025 年亚洲冬季运动会的网络安全工程实践中得到了验证。通过在赛事指挥系统、票务平台和媒体直播网络中部署蜜点集群，显著提高了威胁响应时效性和蜜点存活周期等关键运维指标，成功实现了防御策略与攻击态势的动态匹配。与传统静态防御架构相比，本文方案在超大规模网络场景下展示了智能欺骗防御体系的工程可行性，为关键信息基础设施的动态防护提供了一种创新性解决方案。未来我们的研究将重点关注在联邦学习框架下构建分布式蜜点效能协同优化机制，并进一步深化对抗生成网络在动态蜜点拓扑生成中的应用，以应对 APT 攻击的隐蔽渗透挑战。

作者贡献声明：张志强负责研究方案的整体设计、实验实施及论文撰写；王海燕、杜磊负责研究总体规划与论文指导；段晨芸、李嘉瑞负责数据处理与实验结果分析；顾钊铨、方滨兴提供项目支持与技术指导。

参 考 文 献

[1] Ding Hongwei, Sun Yu, Huang Nana, et al. TMG-GAN: Generative adversarial networks-based imbalanced learning for network intrusion detection[J]. IEEE Transactions on Information Forensics and Security, 2023, 19: 1156−1167

[2] Zhang Zhiqiang, Wang Le, Chen Guangyao, et al. STG2P: A two-stage pipeline model for intrusion detection based on improved LightGBM and K-means[J]. Simulation Modelling Practice and Theory, 2022, 120: 102614

[3] Tian Zhihong, Fang Binxing, Liao Qing, et al. From self-defense to guard: Construction and development suggestions of cybersecurity assurance system in the new era[J]. Strategic Study of CAE, 2023, 25(6): 96−105 (in Chinese)
(田志宏, 方滨兴, 廖清, 等. 从自卫到护卫: 新时期网络安全保障体系构建与发展建议[J]. 中国工程科学, 2023, 25(6): 96−105)

[4] Jiang Wei, Fang Binxing, Tian Zhihong, et al. Research on defense strategies selection based on attack-defense stochastic game model[J]. Journal of Computer Research and Development, 2010, 47(10): 1714−1723 (in Chinese)
(姜伟, 方滨兴, 田志宏, 等. 基于攻防随机博弈模型的防御策略选取研[J]. 计算机研究与发展, 2010, 47(10): 1714−1723)

[5] Sharon Y, Berend D, Liu Yang, et al. TANTRA: Timing-based adversarial network traffic reshaping attack[J]. IEEE Transactions on Information Forensics and Security, 2022, 17: 3225−3237

[6] Qiu Han, Dong Tian, Zhang Tianwei, et al. Adversarial attacks against network intrusion detection in IoT systems[J]. IEEE Internet of Things Journal, 2020, 8(13): 10327−10335

[7] Zhan Dazhi, Zhang Yanyan, Zhu Ling, et al. Enhancing reinforcement learning based adversarial malware generation to evade static detection[J]. Alexandria Engineering Journal, 2024, 98: 32−43

[8] Fang Binxing, Jia Yan, Li Aiping, et al. SARPPR: Reconstructing cyberspace security defense model[J]. Journal of Cybersecurity, 2024, 2(1): 2−12 (in Chinese)
(方滨兴, 贾焰, 李爱平, 等. 重构网络空间安全防御模型——SARPPR[J]. 网络空间安全科学学报, 2024, 2(1): 2−12)

[9] Fan Wenjun, Du Zhihui, Smith-Creasey M, et al. Honeydoc: An efficient honeypot architecture enabling all-round design[J]. IEEE Journal on Selected Areas in Communications, 2019, 37(3): 683−697

[10] Gupta C, Van Ede T, Continella A. Honeykube: Designing and deploying a microservices-based web honeypot[C]//Proc of the 44th IEEE Security and Privacy Workshops. Piscataway, NJ: IEEE, 2023: 1−11

[11] Sethuraman S C, Jadapalli T G, Sudhakaran D P V, et al. Flow based containerized honeypot approach for network traffic analysis: An empirical study[J]. Computer Science Review, 2023, 50: 100600

[12] Pashaei A, Akbari M E, Lighvan M Z, et al. Early intrusion detection system using honeypot for industrial control networks[J]. Results in Engineering, 2022, 16: 100576

[13] Kokolakis G, Ntousakis G, Karatsoris I, et al. HoneyChart: Automated honeypot management over Kubernetes[C]//Proc of the 27th

European Symp on Research in Computer Security, ESORICS 2022 Int Workshops. Cham: Springer, 2022: 321−328

[14] Radoglou-Grammatikis P, Sarigiannidis P, Diamantoulakis P, et al. Strategic honeypot deployment in ultra-dense beyond 5G networks: A reinforcement learning approach[J]. IEEE Transactions on Emerging Topics in Computing, 2022, 12(2): 643−655

[15] Wei Chengkun, Li Xing, Yang Ye, et al. Achelous: Enabling programmability, elasticity, and reliability in hyperscale cloud networks[C]//Proc of the 23rd ACM SIGCOMM Conf. New York: ACM, 2023: 769−782

[16] Fu Lirong, Ji Shouling, Lu Kangjie, et al. Cpscan: Detecting bugs caused by code pruning in IoT kernels[C]//Proc of the 21st ACM SIGSAC Conf on Computer and Communications Security. New York: ACM, 2021: 794−810

[17] Wei Chengkun, Meng Wenlong, Zhang Zhikun, et al. LMSanitator: Defending prompt-tuning against task-agnostic backdoors[C]//Proc of the 31st Network and Distributed System Security Symp (NDSS). San Diego, CA: The Internet Society, 2024: 1−18

[18] Liu Peiyu, Ji Shouling, Zhang Xuhong, et al. IFIZZ: Deep-state and efficient fault-scenario generation to test IoT firmware[C]//Proc of the 36th IEEE/ACM Int Conf on Automated Software Engineering. Piscataway, NJ: IEEE, 2021: 805−816

[19] Li Guoxi, Chen Wenzhi, Xiang Yang. Zweilous: A decoupled and flexible memory management framework[J]. IEEE Transactions on Computers, 2020, 70(9): 1350−1362

[20] Wei Chengkun, Gu Qinchen, Ji Shouling, et al. OB-WSPES: A uniform evaluation system for obfuscation-based web search privacy[J]. IEEE Transactions on Dependable and Secure Computing, 2019, 18(6): 2719−2735

[21] Guan Chongqi, Liu Heting, Cao Guohong, et al. HoneyIoT: Adaptive high-interaction honeypot for IoT devices through reinforcement learning[C]//Proc of the 16th ACM Conf on Security and Privacy in Wireless and Mobile Networks. New York: ACM, 2023: 49−59

[22] Franco J, Aris A, Canberk B, et al. A survey of honeypots and honeynets for Internet of things, industrial Internet of things, and cyber-physical systems[J]. IEEE Communications Surveys & Tutorials, 2021, 23(4): 2351−2383

[23] Ilg N, Duplys P, Sisejkovic D, et al. A survey of contemporary open-source honeypots, frameworks, and tools[J]. Journal of Network and Computer Applications, 2023, 220: 103737

[24] Cao Kanghua, Wang Yong, Zhou Lin, et al. Honeypot game model based on distributed denial of service attack in AMI network[J]. Computer Applications and Software, 2021, 38(3): 298−302,308 (in Chinese)
(曹康华, 王勇, 周林, 等. 基于 AMI 网络分布式拒绝服务攻击的蜜罐博弈模型[J]. 计算机应用与软件, 2021, 38(3): 298−302, 308)

[25] Srinivasa S, Pedersen J M, Vasilomanolakis E. Interaction matters: A comprehensive analysis and a dataset of hybrid IoT/OT honeypots[C]//Proc of the 38th Annual Computer Security Applications Conf. New York: ACM, 2022: 742−755

[26] Maesschalck S, Giotsas V, Green B, et al. Don't get stung, cover your ICS in honey: How do honeypots fit within industrial control system security[J]. Computers & Security, 2022, 114: 102598

[27] Kempinski S, Ichaarine S, Sciancalepore S, et al. ICSvertase: A framework for purpose-based design and classification of ICS honeypots[C]//Proc of the 18th Int Conf on Availability, Reliability and Security. New York: ACM, 2023: 1−10

[28] Yan Xinye, Li Xin, Zhang Bo, et al. Research progress and challenge of industrial control systems honeypot based on simulation[J]. Journal of Information Security Research, 2024, 10(4): 325−334 (in Chinese)
(颜欣晔, 李昕, 张博, 等. 基于仿真的工控蜜罐研究进展与挑战[J]. 信息安全研究, 2024, 10(4): 325−334)

[29] You Jianzhou, Lv Shichao, Sun Yuyan, et al. A survey on honeypots of Internet of things[J]. Journal of Cyber Security, 2020, 5(4): 138−156 (in Chinese)
(游建舟, 吕世超, 孙玉砚, 等. 物联网蜜罐综述[J]. 信息安全学报, 2020, 5(4): 138−156)

[30] Surber J G, Zantua M. Intelligent interaction honeypots for threat hunting within the Internet of things[J]. Journal of The Colloquium for Information Systems Security Education. 2022, 9(1): 1−5

[31] Mohammadzad M, Karimpour J. Using Rootkits hiding techniques to conceal honeypot functionality[J]. Journal of Network and Computer Applications, 2023, 214: 103606

[32] Maesschalck S, Fantom W, Giotsas V, et al. These are not the PLCs you are looking for: Obfuscating PLCs to mimic honeypots[J]. IEEE Transactions on Network and Service Management, 2024, 21(3): 3623−3635

[33] Song Lihua, Jiang Yangyang, Xing Changyou, et al. Optimization mechanism of attack and defense strategy in honeypot game with evidence for deception[J]. Journal on Communications, 2022, 43(11): 104−116 (in Chinese)
(宋丽华, 姜洋洋, 邢长友, 等. 带有欺骗证据的蜜罐博弈攻防策略优化机制[J]. 通信学报, 2022, 43(11): 104−116)

[34] Javadpour A, Ja'fari F, Taleb T, et al. A comprehensive survey on cyber deception techniques to improve honeypot performance[J]. Computers & Security, 2024, 140: 103792

[35] Suratkar S, Shah K, Sood A, et al. An adaptive honeypot using Q-Learning with severity analyzer[J]. Journal of Ambient Intelligence and Humanized Computing, 2022, 13(10): 4865−4876

[36] Anwar A H, Kamhoua C A, Leslie N O, et al. Honeypot allocation for cyber deception under uncertainty[J]. IEEE Transactions on Network and Service Management, 2022, 19(3): 3438−3452

[37] Chen Jun. Research on cloud honeypot service choreography based on BERT[J]. Computer & Digital Engineering, 2022, 50(9): 2042−2047 (in Chinese)
(陈军. 基于 BERT 的云蜜罐服务编排方法研究[J]. 计算机与数字工程, 2022, 50(9): 2042−2047)



Zhang Zhiqiang, born in 1997. PhD candidate. His main research interests include network intrusion detection and artificial intelligence.

张志强, 1997 年生。博士研究生。主要研究方向为网络入侵检测、人工智能。



Wang Haiyan, born in 1984. PhD, associate professor, master supervisor. Her main research interest includes information network security.

王海燕, 1984 年生。博士，副研究员，硕士生导师。主要研究方向为信息网络安全。



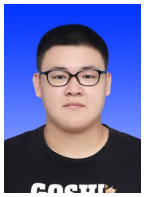
Du Lei, born in 1994. PhD, postdoc. His main research interests include cyberspace security, machine intelligence, and open-world learning.

杜　磊, 1994 年生。博士，博士后。主要研究方向为网络空间安全、机器智能、开放世界学习。



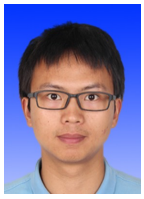
Duan Chenyun, born in 2001, Master candidate. His main research interests include network traffic detection, unknown network attack detection, and incremental learning.

段晨芸, 2001 年生。硕士研究生。主要研究方向为网络流量检测、未知网络攻击检测、增量学习。



Li Jiarui, born in 2002. Master candidate. His main research interests include network attack detection, rule generation of intrusion detection system, and optimization of network attack detection system.

李嘉瑞, 2002 年生。硕士研究生。主要研究方向为网络攻击检测、入侵检测系统规则生成、网络攻击检测系统优化。



Gu Zhaoquan, born in 1989. PhD, professor, PhD supervisor. Member of CCF. His main research interests include wireless networks, distributed computing, big data analytics, and AI security.

顾钊铨, 1989 年生。博士，教授，博士生导师。CCF 会员。主要研究方向为无线网络、分布式计算、大数据分析、人工智能安全。



Fang Binxing, born in 1960. PhD, professor, PhD supervisor. Academician of Chinese Academy of Engineering. His main research interests include computer architecture, computer networks, and information security.

方滨兴, 1960 年生。博士，教授，博士生导师。中国工程院院士。主要研究方向为计算机体系结构、计算机网络、信息安全。