

基于流量交互图分析的Web服务威胁检测方法

余北缘¹, 曾广杰², 彭浩¹, 刘建伟¹, 李洪亮³, 谭学士³

(1. 北京航空航天大学网络安全学院, 北京 100191; 2. 北京航空航天大学计算机学院, 北京 100191;
3. 奇安信科技集团股份有限公司, 北京 100088)

摘要: 随着Web服务应用功能的不断扩展, 其面临的安全威胁日益严峻, 对服务安全性与可靠性的要求也逐步提高。在服务资源规模持续增长的同时, 攻击面不断扩大, 攻击者的能力不断增强, 使得未知威胁与群体性攻击逐渐增多。特别是在实际网络环境中存在大量无标签流量数据的情况下, 实现Web服务流量的轻量化交互关系表征、有效检测多源威胁, 以及在无标签环境下构建具备良好的可解释性的检测模型, 成为突破当前安全瓶颈的关键。为此, 提出了一种基于流量分析的轻量化流量交互图构建方法, 以实现高效表征。通过引入结构熵博弈划分机制, 实现了对流量交互图社区的自适应划分。在此基础上, 通过分析社区子图的拓扑特性, 并借助图指标排序识别关键社区。进一步提出了一种基于Z分数的威胁顶点自适应检测方法, 以有效识别关键社区中的高威胁顶点。同时, 提出基于结构熵的群体威胁检测方法, 以精准发现群体威胁实体。该方法无须依赖先验知识与数据标签, 兼具对未知威胁的适应能力、对加密流量的鲁棒性、模型的可解释性。在公开数据集与实际网络流量数据上的测试结果表明, 该方法能够有效识别多种威胁Web服务可用性的实体与攻击行为, 具有较高的检测准确率和实际工程应用价值。

关键词: Web安全; 威胁检测; 流量交互图; 结构信息理论

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.AQ25264

Web service threat detection method based on traffic interaction graph analysis

Yu Beiyuan¹, Zeng Guangjie², Peng Hao¹, Liu Jianwei¹, Li Hongliang³, Tan Xueshi³

1. School of Cyber Science and Technology, Beihang University, Beijing 100191, China
2. School of Computer Science and Engineering, Beihang University, Beijing 100191, China
3. Qi An Xin Technology Group Inc., Beijing 100088, China

Abstract: With the continuous expansion of Web service functionalities, the security threats they face have become increasingly severe, leading to growing demands for service security and reliability. As service resources scale up, the attack surface widens, and attacker capabilities strengthen, resulting in a rise in unknown threats and swarm attack. Particularly in real-world network environments where large amounts of unlabeled traffic data exist, key challenges include achieving lightweight characterization of Web service traffic interactions, effectively detecting multi-source threats, and constructing a detection model with good interpretability in an unlabeled environment. These is-

收稿日期: 2025-10-23; 修回日期: 2026-02-08

通信作者: 刘建伟, liujianwei@buaa.edu.cn

基金项目: 国家重点研发计划资助项目 (No.2024YFB3108901); 国家自然科学基金资助项目 (No.U21B2021, No.62472015, No.62202027)

Foundation Items: The National Key Research and Development Program of China (No. 2024YFB3108901), The National Natural Science Foundation of China (No.U21B2021, No.62472015, No.62202027)

sues are critical to overcoming current security bottlenecks. To address these challenges, a lightweight traffic interaction graph construction method based on traffic analysis for efficient characterization was proposed. By introducing the structural entropy game partitioning mechanism, the adaptive partitioning of the communities in the traffic interaction graph has been achieved. On this basis, the topological characteristics of communities subgraphs were analyzed, and key communities were identified through graph metric ranking. Furthermore, a Z-score-based adaptive threat vertex detection method was proposed to effectively identify high-threat vertices in key communities. Simultaneously, a structural entropy-based swarm threat detection method was introduced to accurately detect swarm threat entities. The proposed method operates without relying on prior knowledge or data labels, while maintaining adaptability to unknown threats, robustness to encrypted traffic, and good interpretability. Experimental results on public datasets and real-world network traffic data demonstrated that the method could effectively identify various entities and attack behaviors that threaten the availability of Web services, achieving high detection accuracy and practical engineering application value.

Key words: Web security, threat detection, traffic interaction graph, structural information theory

0 引言

为应对 Web 服务功能扩展带来的安全挑战,尤其是在无标签流量数据环境下实现高效、可解释威胁检测的迫切需求,基于图分析的威胁检测技术因能够表征实体间的交互关系、揭示群体性攻击模式而受到学术界与工业界的广泛关注。然而,现有方法在应用于实际 Web 服务环境时仍存在若干局限:其一,依赖高复杂度的全图分析,计算开销过大,难以满足实时响应要求,存在明显的性能瓶颈;其二,过度依赖标注数据与先验知识,导致其在面对未知威胁时泛化能力不足;其三,缺乏对异常子图的安全语义解释,难以为安全研判提供有效支撑,致使检测与研判环节脱节。

针对上述挑战,本文提出一种基于流量交互图分析的威胁检测方法,基于结构熵的社区攻击与恶意流量检测 (SECAMTD)。该方法立足于 Web 服务部署的网络交互整体视角,旨在系统识别针对 Web 服务的潜在攻击实体及其构成的协同威胁群体。具体而言,首先构建轻量化流量交互图,在保留 Web 服务通信关键特征的基础上压缩图规模,从而捕捉攻击行为的结构化模式;然后引入基于结构熵的博弈划分机制,实现社区的自适应发现,并依据社区子图属性识别高风险子图;接下来采用 PageRank 算法评估顶点的影响力,结合结构熵特征定位潜在威胁群体及高风险威胁顶点;最后通过聚焦高影响力顶点及其关联子图结构,实现对威胁实体的精准检测与图结构

层面的行为解释。实验结果表明,该方法在多威胁场景下不仅具备较高的检测效率,还能够从理论和实际交互关系两个层面提供直观的可解释依据,从而为威胁分析与研判提供有效支撑。

本文的主要贡献如下。

1) 提出基于流量交互图分析的 Web 服务威胁检测方法 SECAMTD。该检测方法通过构建轻量化流量交互图,实现了对 Web 服务加密流量的高效表征,并在开源数据集上完成了验证测试。实验结果表明,该检测方法在保持 Web 威胁高检测精度的同时,在安全外壳 (secure shell, SSH) 暴力破解数据集上的 F1 分数较最优基线方法提升约 28%,在恶意软件活动检测任务中的表现更优 (F1 分数较最优基线方法提升约 7%);此外,在 Web 攻击与暴力破解等检测场景中,该检测方法的检测耗时较基线方法平均减少约 90%。

2) 提出一种基于图指标排序的关键社区识别方法。该识别方法能够从复杂的流量交互图中自动识别并定位关键社区,通过关联社区发现与威胁检测,在图结构层面为检测结果提供可解释的依据,增强了模型的安全语义可理解性。

3) 提出一种融合 Z 分数与图结构熵的无监督威胁检测方法。该检测方法能够从流量交互图中同步识别威胁顶点与攻击群体,有效提升对复杂威胁活动的研判与处置能力。在真实网络环境中的部署验证结果表明,所提方法的检测结果 (验证通过率达 98.06%) 可与现有规则引擎形成互补,能够在无标签数据场景下增强实网的安全防护能力。

1 相关工作

1.1 基于签名规则的威胁检测技术

基于签名规则的威胁检测是Web安全领域的传统技术,它通过预定义特征实现对已知威胁的识别。Bronte等^[1]采用遗传算法实现签名的自动变形,进而完成对常见Web攻击的检测。Díaz-Verdejo等^[2]在真实Web攻击数据集上系统评估了多种基于规则签名的入侵检测系统的检测率与误报率,指出了入侵检测系统默认规则存在的局限性。Yang等^[3]借助轻量级分类与字符过滤高效筛选良性流量,结合语法分析,解决了传统规则对混淆攻击检测能力不足的问题。在3 500个Web漏洞测试用例的实验中,该方法的表现优于部分商用入侵检测系统。

随着Web技术逐步部署加密基础设施,基于规则的检测方法在实际应用中暴露出诸多局限,包括对加密流量的解析能力有限、高度依赖签名库的持续维护及对未知威胁的检测能力不足等。

1.2 基于机器学习的威胁检测技术

基于机器学习的威胁检测技术通过数据驱动模型实现威胁的自动识别。Kumar等^[4]使用卷积神经网络将跨站点攻击脚本字符转换为特征矩阵以完成特征的自动提取,实现了98.62%的威胁检测准确率。Alazab等^[5]通过分层特征提取、信息增益特征选择及数据平衡策略,结合支持向量机模型实现对JavaScript恶意样本的检测。Zhou等^[6]通过编码器提取超文本传输协议(hypertext transfer protocol, HTTP)请求载荷特征,结合深度学习从数据分布角度估计不确定性,从而实现了对Web攻击威胁的检测。基于机器学习的威胁检测方法对部分未知攻击具备一定的检测能力,但在Web服务场景落地时仍面临明显挑战:一方面,模型依赖高质量标注数据与复杂的特征工程;另一方面,模型可解释性较差,不利于Web攻击事件的溯源分析与应急响应处置。

为提升检测结果的可解释性,捕捉实体间的复杂交互关系并提取结构化模式,基于图机器学习的威胁检测方法得到广泛研究与应用。Song等^[7]借助程序依赖图和JavaScript语义切片,结合双向长短期记忆网络,实现了恶意脚本的检测。Liu等^[8]将HTTP隧道流量检测转化为异构信息图

顶点分类问题,并引入层次注意力机制自动学习顶点的重要性,使其在流量整形与噪声干扰环境下仍能保持较高的检测性能。Karbab等^[9]基于IP地址白名单对恶意软件与交互实体间的通信模式进行建模,构建恶意软件交互图,并采用Louvain算法实现恶意软件社区的有效检测。Li等^[10]设计交互行为图对网络通信行为进行表征,通过学习局部交互特征,实现了对加密流量的有效分类。

2 本文方法

2.1 架构设计

在Web服务环境下,将系统抽象为由通信实体及其交互关系构成的流量交互图 $G=(V,E,w)$,具体定义如下。

1) 实体: Web服务运行所依赖的基础网络设备(如Web应用服务器、负载均衡器),对应交互图中的一个顶点 $v \in V$ 。

2) 交互关系: 若实体 i 与 j 之间存在流量交互,则在两者之间构建一条连边, $e_{ij} \in E$ 。

3) 权重 w : 以实体间的交互数据量的聚合值作为图边的权重。

与依赖IP地址白名单预过滤或预定义资产标签的方案不同,本文通过全量实体建模消除对先验知识的依赖,有效规避了标签更新滞后导致的检测盲区。区别于构建高维异构图的思路,本文采用同质化建模策略,通过降低构图的复杂性,实现了对跨协议、跨业务通用通信模式的抽象,在提升大规模图计算效率的同时,增强了模型对网络环境动态变化的鲁棒性。此外,本文主动避免采用复杂的流方向、包级时序等细粒度特征,转而通过宏观流量交互强度的聚合实现对交互行为的建模。该方法不但能够实现对海量报文的结构化压缩,而且由于不依赖应用层载荷,能够有效适配加密流量环境,解决了传统特征在加密背景下失效的问题。

所提方法的核心检测目标是识别并定位Web服务部署网络中活跃的威胁实体:在交互图 G 中,非空顶点子集 $A \subseteq V$ 表示潜在的威胁实体集合,其包含的顶点 $v_i \in A$ 均存在威胁行为。

SECAMTD的总体框架如图1所示。首先,解析原始流量,提取并聚合通信模式以构建流量

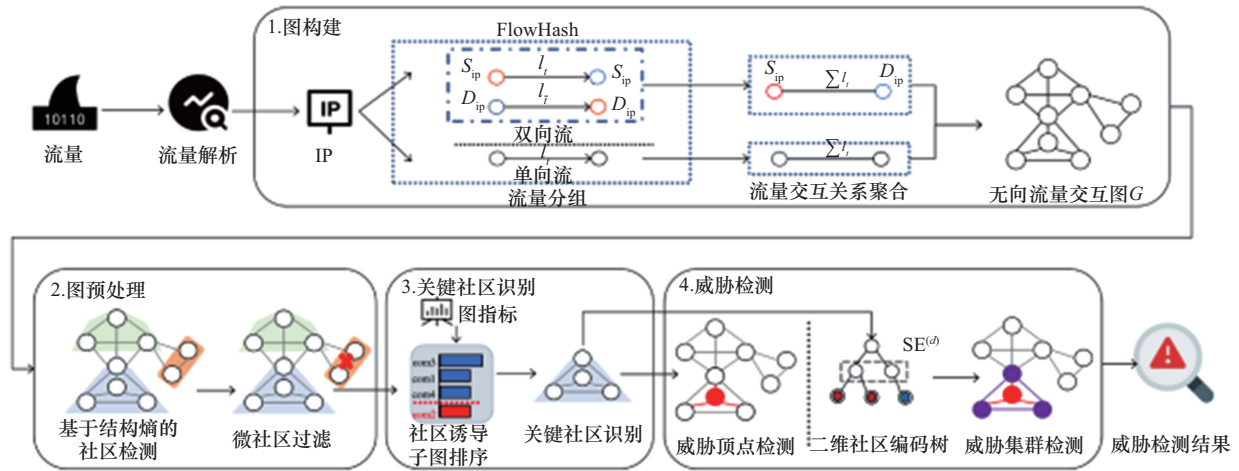


图1 SECAMTD的总体框架

交互图 G 。其次，基于结构熵博弈划分机制识别图中的社区结构，并过滤微社区以降低临时性交互干扰。然后，依据预定义的图结构属性指标对社区子图进行排序，筛选出最具分析价值的关键社区子图，从而避免对全量社区逐一开展深入研判。通过结构指标排序实施关键性分析，既能有效消除海量常态化业务背景的干扰，又能将有限的分析资源聚焦于拓扑结构最复杂的疑似威胁群体。最后，通过分析关键社区子图中的顶点影响力，实现对潜在威胁实体的检测；同时，构建二维社区编码树以度量关键社区子图的动态不确定性，进而实现对威胁群体活动的检测。

2.2 相关定义

结构信息理论由Li等^[11]提出，其核心概念为结构熵。本质上，结构熵衡量的是在图随机游走过程中，确定顶点所对应的 K 维编码所需的最小信息量（即最小位数）。该层级编码体系通过编码树实现具体表征。对于给定的图 G ，其编码树是一棵具有层级结构的根树，并满足以下性质：①根节点 λ 所关联的节点的顶点集为全体顶点集，关联的点集表示为 $V_\lambda = V$ ；②每个叶节点 v 仅关联单个顶点，记该顶点为 $V_v = \{v\}$ ，其中 $v \subseteq V$ ；③非根非叶节点 α 所关联的顶点集 V_α 是其父节点 α^- 对应集合的子集，满足 $V_\alpha \subseteq V_{\alpha^-}$ ；④对于每个非叶节点 α ，其子节点表示为 L_α ，其第 i 个子节点为 $\alpha^{<i>}$ ，所有节点子集 $V_{\alpha^{(i)}}$ 均不相交并覆盖 V_α 。

在无分层分区结构的前提下，一维结构熵能够对图 G 的动态不确定性进行度量，其计算过程

如式(1)所示。

$$H^1(G) = - \sum_{v \in V} \frac{d_v}{\text{vol}(G)} \cdot \log_2 \left(\frac{d_v}{\text{vol}(G)} \right) \quad (1)$$

其中， d_v 表示顶点 v 的加权重， $\text{vol}(G) = \sum_{v \in V} d_v$ 表示图 G 的体积。一维结构熵通过顶点在随机游走过程中的稳态概率 $\frac{d_v}{\text{vol}(G)}$ ，量化单一层级下节点编码所需的不确定性。

对于编码树 Tree 中的非根节点 α ，其对结构熵的贡献为从父节点分区定位到当前分区所需的不确定性，其定义见式(2)。

$$H^{\text{Tree}}(G; \alpha) = - \frac{g_\alpha}{\text{vol}(G)} \log_2 \left(\frac{\text{vol}(V_\alpha)}{\text{vol}(V_{\alpha^-})} \right) \quad (2)$$

其中， $\text{vol}(V_\alpha)$ 表示分区 V_α 的体积， g_α 表示连接 V_α 中每个顶点与外部顶点的割边总权重。

$\frac{g_\alpha}{\text{vol}(G)}$ 表示通过随机游走进入该分区的概率。

d -维结构熵定义为在高度不超过 d 的编码树中，所有非根节点贡献之和的最小值，如式(3)所示。

$$\text{SE}^{(d)}(G) = \min_{\text{Tree} \in \mathbb{T}_d} \sum_{\alpha \in \text{Tree}, \alpha \neq \lambda} H^{\text{Tree}}(G; \alpha) \quad (3)$$

其中， $\mathbb{T}_d$ 为所有高度不超过 d 的编码树构成的集合。

2.3 流量交互图的构建

本文首先对网络流量进行采集与预处理，并在此基础上构建流量交互图。在流量交互图中，每个IP地址被抽象为一个顶点，用于表征网络中的通信实体。为降低图结构的复杂度，将每个

实体关联流量会话内的数据按照IP地址与通信方向进行聚合,进而构成代表实体间具体交互关系的图边;同时,提取并聚合网络交互过程中传输的数据包长度,以此刻画实体间的交互强度。

设 T 表示所有捕获的网络流量集合,每个流量实例 $t \in T$ 使用三元组 $(v_{\text{prot}}, S_{\text{ip}}, D_{\text{ip}})$ 表示,即 $t = (v_{\text{prot}}, S_{\text{ip}}, D_{\text{ip}})$ 。其中, v_{prot} 表示协议版本, S_{ip} 和 D_{ip} 分别表示流量的源IP地址和目的IP地址。此外,每个流量条目还包含传输数据长度度量 l_t 。为提高流量处理效率,本文基于三元属性构建了一个哈希函数,用于构建哈希表FlowHash。对于任意服务流量数据 t ,其哈希值计算如式(4)所示。

$$H(t) = \text{Hash}(v_{\text{prot}}, \min(S_{\text{ip}}, D_{\text{ip}}), \max(S_{\text{ip}}, D_{\text{ip}})) \quad (4)$$

基于哈希值将流量数据集 T 划分为若干流量分组集合 $S_K = \{t \in T | H(t) = K\}$ 。映射关系如式(5)所示。

$$\text{FlowHash}: K \rightarrow \{(v_i, v_j, \sum l_t) | t \in S_K\} \quad (5)$$

其中,满足 $v_i = \min(S_{\text{ip}}, D_{\text{ip}})$, $v_j = \max(S_{\text{ip}}, D_{\text{ip}})$ 。每个键 K 对应一个交互标识符,通过键索引的值对应该交互的流量特征。 l_t 则表示流量数据 t 的数据包长度。算法1描述了FlowHash构建算法。

算法1 FlowHash构建算法

- 1) Require: T
- 2) **for** t in T **do**
- 3) $(\text{ip1}, \text{ip2}) \leftarrow \text{sort}(t.S_{\text{ip}}, t.D_{\text{ip}})$
- 4) $K \leftarrow \text{Hash}(t.v_{\text{prot}}, \text{ip1}, \text{ip2})$
- 5) **if** K in FlowHash
- 6) $\text{FlowHash}[K].\text{sum} += t.l_t$
- 7) **else**
- 8) 创建 $\text{FlowHash}[K]$
- 9) $\text{FlowHash}[K].\text{sum} \leftarrow t.l_t$
- 10) $\text{FlowHash}[K].\text{prot} \leftarrow t.v_{\text{prot}}$
- 11) $\text{FlowHash}[K].\text{ip1} \leftarrow \text{ip1}$
- 12) $\text{FlowHash}[K].\text{ip2} \leftarrow \text{ip2}$
- 13) **end if**
- 14) 返回 FlowHash

基于FlowHash,本文采用算法2构建一个结构紧凑且语义一致的轻量化流量交互图,该流量交互图满足同构图性质,为后续的图预处理奠定基础。

算法2 流量交互图构建算法

- 1) Require: FlowHash

- 2) $V \leftarrow \emptyset$
- 3) $E \leftarrow \emptyset$
- 4) **for** K in FlowHash **do**
- 5) $u \leftarrow \text{FlowHash}[K].\text{ip1}$
- 6) $v \leftarrow \text{FlowHash}[K].\text{ip2}$
- 7) $w \leftarrow \text{FlowHash}[K].\text{sum}$
- 8) $V \leftarrow V \cup \{u, v\}$
- 9) $E \leftarrow E \cup \{(u, v, w)\}$
- 10) **end for**
- 11) 返回 V, E

2.4 图预处理

在预处理后的流量交互图上,本文应用结构熵理论进行非重叠社区检测。该方法通过迭代最小化流量交互图的结构熵,直至达到纳什均衡^[12],从而实现对图的稳定划分。基于结构熵博弈划分机制能够有效地将流量交互图划分为若干社区,显著简化后续的威胁识别过程。此外,本文引入了微社区过滤策略,用于去除规模较小或缺乏代表性的低相关性子图。

2.4.1 基于结构熵博弈的社区检测

为识别复杂网络流量交互图中的高密度连接子结构,本文采用基于结构熵博弈划分机制的CoDeSEG方法^[13]执行流量交互图社区检测任务。设图 G 的社区划分为 $P = \{C_1, C_2, \dots, C_k\}$,则图 G 的二维结构熵定义如式(6)所示。

$$H^2(P) = - \sum_{c \in P} \left(\frac{g_c}{v_\lambda} \log_2 \left(\frac{v_c}{v_\lambda} \right) + \sum_{x \in C} \frac{d_x}{v_\lambda} \log_2 \left(\frac{d_x}{v_c} \right) \right) \quad (6)$$

其中, d_x 表示顶点 x 的度, v_λ 表示整个图的体积, v_c 表示社区 c 的体积, g_c 表示社区割边权重。该方法的创新在于构建了以流量交互图二维结构熵最小化为目标的潜在博弈框架。与Louvain等侧重于局部连接密度的传统方法不同,CoDeSEG利用结构熵对网络动态不确定性的表征能力,实现对社区的自适应检测。设 P 为执行顶点迁移策略前的社区划分, P' 为执行顶点迁移策略后的社区划分。该方法通过关联顶点迁移策略与二维结构熵函数的变化量 $\Delta = H^2(P) - H^2(P')$,在确保算法收敛至纳什均衡点的同时,通过缓存社区体积、割边权重等统计量实现了常数级效用计算,有效兼顾了检测精度与大规模网络的实时性需求。

该方法主要包含以下4个关键步骤。

1) 初始化: 每个顶点初始被视为一个独立的社区, 其社区体积和割边信息基于顶点度数进行初始化。

2) 社区重分配: 每个顶点作为博弈参与者, 通过启发式函数 Δ 计算留在当前社区、转移至相邻社区、独立为新社区 3 种策略对应的结构熵变化量。顶点选择能够最大程度地降低全局结构熵的策略, 优先转移至使结构熵减少最多的相邻社区, 实现社区划分的迭代优化。

3) 社区统计信息更新: 待顶点迁移后, 算法实时更新源社区与目标社区的体积和割边统计数据, 以准确反映结构变化。

4) 迭代终止: 迭代执行步骤 2) 与 3), 直至顶点归属不再变化或结构熵的变化量低于预设阈值 τ_n 。

结构熵博弈划分机制的时间复杂度为 $O(I_t \cdot d_{\max} \cdot N_u)$, 其中 I_t 为迭代次数, $d_{\max}$ 为最大顶点度, N_u 为图所包含的顶点数。该机制具有近线性的计算效率, 适合对轻量化流量交互图进行实时社区检测。

2.4.2 基于规模的社区过滤策略

由于复杂流量交互图中的连接模式具有高度的异质性, 社区检测所生成的图划分结果 P 中往往包括大量顶点数量极少的小规模子图 (即微社区)。这类微社区规模小且结构离散, 缺乏代表性, 成为制约后续社区排序与威胁检测效率的瓶颈。

为提升分析效率与检测结果的有效性, 本文引入了一种基于规模的过滤策略, 仅保留满足最小规模要求的社区子图。具体过滤标准如式(7)所示。

$$C_i^{\text{filtered}} = \begin{cases} C_i, & |C_i| \geq N_{\min} \\ \emptyset, & \text{其他} \end{cases} \quad (7)$$

P 被过滤为 $P^{\text{filtered}} = \{C_1^{\text{filtered}}, \dots, C_M^{\text{filtered}}\}$, 满足 $M \leq |P|$ 。该策略通过剔除由噪声或临时性连接模式产生的小规模社区^[14], 有效降低了图结构的复杂性。图 2 展示了微社区过滤的过程。

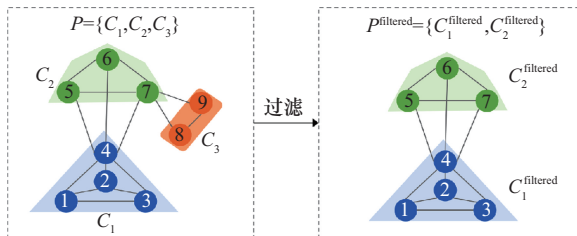


图 2 微社区过滤

2.5 关键社区识别

本节通过分析流量交互图各社区子图的连接性、交互强度等指标, 识别流量交互图中的关键社区。

2.5.1 基于图指标的诱导子图排序方法

本文使用图指标对经过微社区过滤后的 P^{filtered} 进行排序, 筛选可能包含威胁行为的社区子图用于执行后续威胁检测任务。

为评估和排序各社区的诱导子图^[15], 本文引入以下 3 个关键指标, 旨在无监督条件下刻画社区的结构特征及其潜在威胁程度。

1) 社区内的平均度数: 衡量社区内部顶点的平均连接数, 反映其内部的连通性水平。该指标有助于识别结构紧密的社区, 即成员之间存在较强结构关联的子图。

2) 社区内的平均边权重: 表示社区内部边的平均权值, 刻画顶点间交互的强度。该指标有助于辨别交互频繁或信息流密集在社区。

3) 社区规模: 社区中包含的顶点数量, 用于估计其在整体网络中的相对体量与潜在影响范围。

2.5.2 基于排序的关键社区识别方法

图指标为社区的结构分析提供了量化依据。在此基础上, 本文引入社区排名机制, 旨在识别并优先处理最具信息价值的社区诱导子图, 从而提升威胁检测效率。

对于每个社区 $C_i^{\text{filtered}} \in P^{\text{filtered}}$, 先计算其对应各项图属性的综合分数 $\text{score}(C_i^{\text{filtered}})$ 以生成社区子图的整体评分, 再提取评分排名前 k 位的社区构建 Top- k 社区集合 $C_{\text{ranked}} = \{C_{\text{sort}_1}^{\text{filtered}}, C_{\text{sort}_2}^{\text{filtered}}, \dots, C_{\text{sort}_k}^{\text{filtered}}\}$, 满足 $\text{score}(C_{\text{sort}_1}^{\text{filtered}}) \geq \text{score}(C_{\text{sort}_2}^{\text{filtered}}) \geq \dots \geq \text{score}(C_{\text{sort}_k}^{\text{filtered}})$ 。 C_{ranked} 中的社区子图将作为后续威胁检测任务的重点分析对象。图 3 展示了一个 $k=2$ 的关键社区的识别流程。

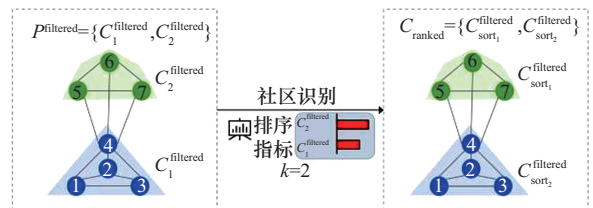


图 3 关键社区识别流程

2.6 基于关键社区的威胁检测

为实现对关键社区中高影响力顶点的识别,以支持威胁实体检测,本文基于PageRank算法^[16]对顶点的重要性进行建模。该方法将边视作顶点之间的信任投票,顶点的重要性由其在社区内部的连接结构与交互强度共同决定。

2.6.1 基于Z分数差异的威胁顶点检测

首先,将所有经特定图指标进行Top- k 排序后得到的关键社区 $C_{\text{sort}_i}^{\text{filtered}}$ 所对应的诱导子图 $G_i = G[C_{\text{sort}_i}^{\text{filtered}}] = (V_{\text{sort}_i}, E_{\text{sort}_i}, w)$ 合并为一个总图 $G_{\text{merged}} = (V_{\text{merged}}, E_{\text{merged}}, w)$, 满足 $V_{\text{merged}} = \bigcup_{i=1}^k V_{\text{sort}_i}$ 及 $E_{\text{merged}} = \bigcup_{i=1}^k E_{\text{sort}_i}$ 。

在合并图 G_{merged} 上,顶点 u 的PageRank得分计算如式(8)所示。

$$\text{PR}_{G_{\text{merged}}}(u) = (1 - y) + y \sum_{v \in M_{G_{\text{merged}}}(u)} \frac{\text{PR}_{G_{\text{merged}}}(v)}{L_{G_{\text{merged}}}(v)} \quad (8)$$

其中, $M_{G_{\text{merged}}}(u)$ 表示在图 G_{merged} 中与顶点 u 相邻的全部顶点的集合, $L_{G_{\text{merged}}}(v)$ 表示顶点 v 在 G_{merged} 中的出边数量。通过顶点PageRank计算过程,能够在合并图中量化各顶点的相对重要性,从而识别在多社区交互中发挥核心作用的实体。该识别机制为后续恶意行为的定位与深入分析提供了结构性支持和决策依据。

基于合并图 G_{merged} 计算得到的PageRank分数,本文提出了一种自适应阈值方法,用于自动检测潜在的恶意顶点集合。该方法利用PageRank值在合并图内的分布特性,实现威胁检测。

具体而言,首先计算合并图中顶点PageRank值的全局均值 μ_{PR} 与标准差 σ_{PR} 。其中,全局均值按照式(9)进行计算,标准差按照式(10)进行计算。

$$\mu_{\text{PR}} = \frac{1}{|V_{\text{merged}}|} \sum_{u \in V_{\text{merged}}} \text{PR}_{G_{\text{merged}}}(u) \quad (9)$$

$$\sigma_{\text{PR}} = \sqrt{\frac{1}{|V_{\text{merged}}|} \sum_{u \in V_{\text{merged}}} (\text{PR}_{G_{\text{merged}}}(u) - \mu_{\text{PR}})^2} \quad (10)$$

随后,基于全局均值 μ_{PR} 和标准差 σ_{PR} 对合并图 G_{merged} 中所有顶点的PageRank值进行Z分数标准化处理,以消除尺度差异并突出相对异常值。

计算公式如式(11)所示。

$$Z(u) = \frac{\text{PR}_{G_{\text{merged}}}(u) - \mu_{\text{PR}}}{\sigma_{\text{PR}}}, \quad \forall u \in V_{\text{merged}} \quad (11)$$

在完成Z分数标准化后,将所有顶点按照其Z分数进行降序排列,得到有序顶点序列 $Z_{\text{merged}} = \{u_1, u_2, \dots, u_n\}$,且满足条件 $Z(u_i) \geq Z(u_{i+1})$ 与 $n = |V_{\text{merged}}|$ 。接着计算差分序列 Δ_{merged}^i ,用于刻画有序序列中相邻顶点Z分数之间的成对差异。计算公式如式(12)所示。

$$\Delta_{\text{merged}}^i = Z(u_i) - Z(u_{i+1}), \quad i = 1, \dots, n-1 \quad (12)$$

为识别Z分数分布中最显著的跃迁位置,基于差分序列 Δ_{merged}^i 确定其最大差值所对应的索引 k^* ,其计算过程如式(13)所示。

$$k^* = \arg \max_{1 \leq i \leq n-1} \Delta_{\text{merged}}^i \quad (13)$$

索引 k^* 为Z分数序列中下降最陡的拐点,反映了高排名与低排名顶点之间的自然分界,有助于自动确定潜在异常顶点的分布阈值。自适应阈值 τ_{merged}^* 计算差分序列最大间隙处相邻两顶点Z分数的平均值,求解过程如式(14)所示。

$$\tau_{\text{merged}}^* = \frac{Z(u_{k^*}) + Z(u_{k^*+1})}{2} \quad (14)$$

基于所确定的自适应阈值 τ_{merged}^* ,识别潜在威胁顶点集合 $A = \{u \in V_{\text{merged}} | Z(u) > \tau_{\text{merged}}^*\}$ 。分析关键社区子图的结构连通性与交互强度,识别与恶意流量活动相关的威胁群体。该集合包含在影响力上表现出显著异常的顶点,为后续威胁处置提供了参考。图4展示了基于Z分数差异的威胁检测过程。

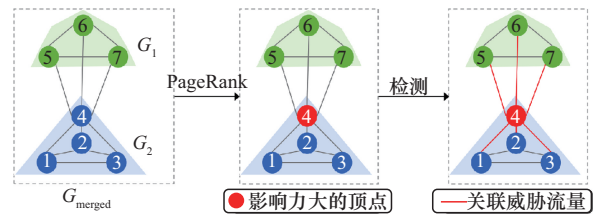


图4 基于Z分数差异的威胁检测

该合并图由两个关键社区诱导子图 G_1 和 G_2 构建而成,为网络中潜在威胁的识别提供了全局统一视角下的分析与检测能力。在成功识别出影响力大的潜在威胁攻击源后,可以据此实施针对性的防御措施(包括阻断其关联流量、隔离所在社区或增强监控)。

综上所述,通过将PageRank算法引入关键

社区诱导子图的影响力分析, 本文实现了图结构指标与 Web 服务威胁检测的有机结合。在系统化检测独立威胁活动的同时, 能够依据图拓扑与影响力分布对威胁判定结果进行归因分析, 从而为威胁处置决策提供明确依据。

2.6.2 基于结构熵的群体威胁检测

基于顶点重要性的分析方法难以揭示群体威胁。为应对这一挑战, 本文引入结构熵图结构度量方法用于刻画关键社区子图的结构不确定性。该方法能够有效捕捉威胁交互行为引发的图结构异常, 有助于揭示隐蔽的威胁模式, 并辅助实现复杂群体威胁的检测。对于更加复杂的威胁方式(如僵尸网络活动、恶意软件传播), 其攻击行为通常呈现为结构高度复杂、节点连接密集且分布不规则的社区级模式^[17]。为此, 本文基于社区结构熵对威胁群体活动进行识别。具体而言, 对排名前 Top- k 的社区诱导子图 $G_i (i = 1, 2, \dots, k)$ 进行结构熵分析, 量化由威胁行为引发的动态不确定性。通过分析 G_i 的结构熵, 识别偏离正常阈值 thr_{SE} 的图结构, 从而有效定位 $A = \{v | \exists i, v \in C_{\text{sort}_i}^{\text{filtered}}, \text{SE}^{(2)}(G_i) \geq \text{thr}_{\text{SE}}\}$ 。图 5 展示了基于结构熵分析的威胁社区检测过程。

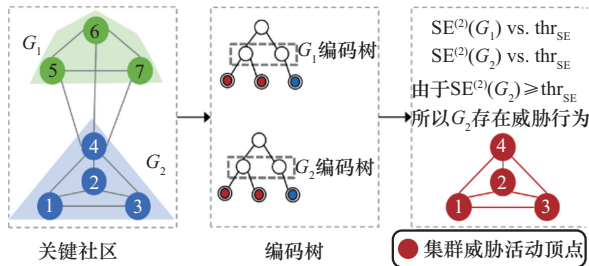


图 5 基于结构熵分析的威胁社区检测过程

3 测试验证

3.1 本地测试

3.1.1 本地威胁检测测试配置

(1) 硬件与软件环境

在硬件环境方面, 本地威胁检测测试在操作系统为 MacOS Sonoma 14.6.1 的 2021 款 MacBook Pro 上开展。该设备搭载 Apple M1 Pro 处理器(10 核心, 包括 6 个性能核心和 4 个能效核心)、16 核 GPU, 配备 16 GB 内存及 1 TB 固态硬盘, 可为大规模图数据的高效并行计算提供支持。

在软件环境方面, 本文所提检测方法基于 Python 3.12.7 实现, 采用 NetworkX 3.3 库构建流量交互图。社区检测模块采用开源 C++ 版本的 CoDeSEG 算法, 通过 GNU Make 3.81 编译为可执行文件进行调用。

(2) 数据集

本地威胁检测测试使用 HyperVision^[18]数据集进行评估。该数据集涵盖多种网络协议的流量数据, 覆盖 Web 服务、在线服务器、内网等场景, 为验证本文所提检测方法的鲁棒性与通用性提供了有效支撑。在数据预处理阶段, 通过预定义规则对采集的原始流量数据进行预处理, 移除具有明显攻击模式的流量样本, 以提升数据质量。该数据集包含以下 3 类典型威胁流量。

1) Web 服务攻击流量: 该类流量包括结构化查询语言 (structured query language, SQL) 注入、跨站脚本、跨站请求伪造攻击^[19]和 WebShell 攻击等行为。

2) 暴力破解攻击流量: 攻击者通过凭据采集获取 Web 服务器的未授权访问权限, 危害 Web 服务的可用性。暴力破解攻击流量主要包括 SSH 端口扫描、SSH 口令破解及安全套接字层 (secure socket layer, SSL) 扫描等类型。

3) 恶意软件攻击流量: 通过重放多个公开恶意软件流量数据^[20]构建而成, 涵盖对等网络 (peer-to-peer, P2P) 病毒感染、垃圾邮件发送等恶意行为。

本地威胁检测测试所使用的数据集信息见表 1。

表 1 本地威胁检测测试数据集信息

攻击类型	数据集	流量样本/条
Web 服务攻击	SQL	12 902 998
	跨站脚本攻击 (XSS)	12 747 369
	跨站请求伪造攻击 (CSRF)	12 717 008
	WebShell	12 716 314
暴力破解攻击	SSH	13 18 221
	SSH 口令破解攻击 (PWD)	13 071 776
	SSL	12 749 361
恶意软件攻击	Salinity	12 897 064
	Spam50	14 115 634

(3) 基线模型和评价指标

为评估本文模型在不同场景下的检测性能与泛化能力,研究人员选取了以下3种具有代表性的基于图的威胁检测模型作为对比基线。所有基线模型均基于本文构建的流量交互图开展威胁检测。

1) K-means 模型:该模型采用无监督聚类算法^[21],需要预先设定簇的数量,并初始化各个簇的质心,然后通过欧几里得距离度量将数据样本划分为多个球形簇。通过这种方式,K-means 将特征相似的数据点聚集在以均值向量为中心的簇中,适用于识别特征分布相对规则的攻击行为。

2) 脱氧核糖核酸(DNA)模型:该模型采用基于字符串的序列建模方式。具体而言,首先将顶点之间的交互行为编码为类似DNA序列的符号串,然后通过计算序列之间的相似度来衡量不同顶点在行为模式上的一致性^[22]。DNA模型能够有效识别具有高度相似交互模式的实体簇,适合检测具有周期性规律或高度伪装特征的攻击行为。

3) ToGather 模型:该模型采用基于图理论的威胁建模方法。该模型首先依据实体标签从样本中提取关键网络属性,结合噪声过滤与白名单对比机制,构建具有上下文语义的威胁网络;随后,在该网络基础上应用社区检测算法,实现对潜在威胁簇的识别^[23]。

本文基于HyperVision数据集开展测试。鉴于该数据集提供了流量标签,为方便评估所提模型的威胁检测性能,本文采用宽松实体映射策略进行标签对齐。具体而言,若模型将实体 V 判定为恶意,则将实体 V 在整个评估周期内发送的所有流量均判定为威胁,并将其与数据集的真实标签进行比对,从而验证检测结果的准确性。本文选取准确率、F1分数作为评估指标,旨在从不同维度定量分析各模型在Web服务威胁检测任务中的性能表现。

(4) 图变体模型

为评估所提模型中流量交互图的构建策略对整体威胁检测性能的影响,本文设计了3种图模型变体,并通过消融实验对其进行系统分析。各变体在图构建方式或检测流程上进行了局部调整,旨在量化图构建策略与检测方法对模型整体性能的贡献程度。

1) 不聚合双向边(NB)变体:该变体在构建流量交互图 G 时,不对双向会话流进行边聚合操作,从而保留了原始流量的方向信息。所得图为加权有向图,用于评估边方向性对威胁检测性能的影响。

2) 不聚合边权重(WEW)变体:该变体将流量交互图 G 转换为无权图,通过去除边权重以探究其在网络威胁行为表征与威胁检测中的作用,从而评估权重特征对检测性能的贡献。

3) PR 变体:该变体仅在流量交互图 G 上应用PageRank算法进行顶点影响力分析,而不引入基于结构熵的群体威胁检测模块。该设计旨在考察单一顶点影响力特征在缺乏社区上下文信息时的威胁检测能力。

3.1.2 本地威胁检测测试

研究人员使用Web服务攻击流量对所提模型进行评估,Web威胁检测结果见表2。结果表明,本文模型在威胁检测效果上与K-means基线方法表现相当,验证了所构建的流量交互图在保留威胁特征方面的有效性。DNA模型在WebShell数据集上将流量交互图中的所有顶点均判为恶意。ToGather模型在所有Web攻击流量数据集构建的交互图中均未检测到威胁顶点,故未在表2中列出其检测结果。

表2 Web威胁检测结果

模型	指标	数据集			
		SQL	XSS	CSRF	WebShell
K-means	准确率	100%	99.65%	99.89%	98.02%
	F1分数	100%	92.84%	97.65	97.98%
DNA	准确率	99.99%	93.31%	97.66%	—
	F1分数	99.99%	92.83%	97.61%	—
本文模型	准确率	100%	99.65%	99.89%	98.02%
	F1分数	100%	92.84%	97.65%	97.98%

研究人员使用暴力破解攻击流量对所提模型进行评估,暴力破解威胁检测结果见表3。结果显示,本文模型在SSH数据集上的F1分数为100%,较DNA模型提升约28%,较K-means模型提升约39%,显著优于各基线模型。值得注意的是,ToGather模型在所有暴力破解流量数据集构建的交互图中也未检测到威胁顶点,故未在表3

中列出其检测结果。经分析,其主要原因在于 To-Gather 模型的检测范式难以实现社区内的角色剥离。具体而言, ToGather 采用 Louvain 算法进行社区检测,该算法旨在挖掘网络中的稠密子图结构,虽能将攻击实体与受害实体聚类至同一社区,但缺乏对社区内节点角色的优先级判定能力。在后续的威胁排名阶段,由于所构建的轻量级流量交互图不包含载荷特征,攻击顶点的拓扑显著性被海量的受害顶点掩盖,最终导致威胁检测失效。

表 3 暴力破解威胁检测结果

模型	指标	数据集		
		SSH	PWD	SSL
K-means	准确率	72.01%	93.25%	93.22%
	F1 分数	61.15%	92.76%	92.74%
DNA	准确率	77.98%	93.25%	93.22%
	F1 分数	71.76%	92.76%	92.74%
本文模型	准确率	100%	93.25%	93.22%
	F1 分数	100%	92.76%	92.74%

研究人员使用恶意软件攻击流量对所提模型进行评估,恶意软件威胁检测结果见表 4。结果表明,本文模型在恶意软件威胁检测任务中的性能显著优于 K-means 和 DNA 等基线模型。在 Spam50 数据集上, ToGather 的检测性能与本文模型相近,这一结果验证了本文所构建的流量交互图能够有效支持基于模块度的威胁社区检测。同时,本文模型的威胁检测性能也得到验证。

表 4 恶意软件威胁检测结果

模型	指标	数据集	
		Sality	Spam50
K-means	准确率	73.86%	32.28%
	F1 分数	64.62%	0%
DNA	准确率	71.25%	70.35%
	F1 分数	59.71%	60.75%
ToGather	准确率	90.90%	99.99%
	F1 分数	89.99%	99.99%
本文	准确率	99.96%	99.99%
	F1 分数	96.90%	99.99%

图 6 展示了 Sality 威胁群体检测结果。从社区划分结果可以看出,该威胁群体呈现出显著的

拓扑独立性(即群体内部顶点之间连接紧密,而与其他社区之间几乎不存在交互边)。这一清晰独立结构的形成,可以从本文所采用的结构熵博弈划分机制的角度予以解释。每个顶点在评估其迁移至任一相邻社区的潜在收益时,由于其与群体内部邻居的连接密度远高于与外部社区的连接密度,任何离开当前社区的迁移尝试都将导致局部熵值增大,保持现有归属则能够维持更优的局部熵状态。根据决策规则,每个顶点均会选择使整体结构熵值最小化的社区。在此机制下,所有与 Sality 威胁相关的顶点在博弈过程中自然达到了稳定的社区划分状态。最终,通过对社区子图进行排序并计算子图结构熵,实现了对 Sality 威胁群体的有效检测。



图 6 Sality 威胁群体检测结果

3.1.3 性能评估测试

为验证所提图构建模块及基于会话流的聚合机制在不同攻击数据集上的处理效率,本文开展了性能评估测试,从流量交互图构建效率、图社区检测效率与威胁检测效率 3 个维度对整体处理性能进行了评估。

(1) 流量交互图构建效率和图社区检测效率

流量交互图的构建及社区检测时间开销如图 7 所示。在构建效率方面,大多数数据集的图构建操作^[24]能够在 12 s 内完成。其中,基于 Sality 数据集构建的图规模较小,构建时间最短;而在较大规模数据集上,图构建时间保持在 16 s 左右。测试结果表明,本文提出的图构建方法在处理大规模流量时具有较高的效率与良好的可扩展性。此外,构建完成的图可复用于后续的威胁检测与关联分析,有效避免了重复计算开销。

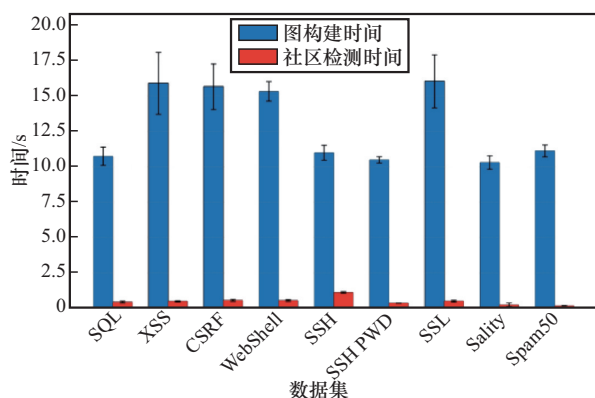


图7 流量交互图构建与社区检测时间开销

在社区检测效率方面，基于CoDeSEG的社区检测算法整体执行效率较高。在大多数数据集构建的流量交互图上执行无重叠社区检测，可在0.6 s左右完成；基于Sality与Spam50数据集构建的图规模相对较小，社区检测时间少于0.3 s。值得注意的是，对于数据规模较大的SSH数据集，其构建的流量交互图在结构熵博弈划分阶段存在较多的顶点跨社区迁动，导致其社区检测时间相比其他数据集明显增加。

(2) 威胁检测效率

表5汇总了本文模型与各基线模型在10次独立威胁检测任务中的平均执行时间。总体来看，本文模型在检测准确性与威胁检测效率之间实现了良好的平衡。值得注意的是，对于表5中以“*”注明的数据集，若使用K-means和DNA对其构造的流量交互图 G 进行威胁检测，需先对图 G 进行随机游走采样；否则，检测时间将超过10 min。

表5 威胁检测平均执行时间

数据集	K-means 平均执行 时间/s	DNA 平均 执行时间/s	ToGather 平均执行 时间/s	本文模型 平均执行 时间/s
SQL*	11.48±0.44	23.23±12.39	1.42±0.37	1.18±0.24
XSS*	22.47±1.13	37.04±13.82	2.58±0.53	1.77±0.16
CSRF*	23.00±0.52	37.63±0.07	2.48±0.61	2.41±0.33
WebShell*	23.05±0.52	24.06±8.52	2.74±0.33	1.66±0.15
SSH*	30.43±0.53	78.03±44.84	5.63±0.52	6.22±0.38
PWD*	12.67±1.02	35.93±0.01	1.63±0.14	1.58±0.43
SSL*	21.10±1.02	29.98±7.26	3.05±0.15	1.82±0.09
Sality	0.32±0.16	0.50±0.26	0.28±0.28	1.04±0.23
Spam50	11.12±0.42	0.20±0.02	0.21±0.02	4.53±1.27

3.1.4 消融测试

为评估流量交互图各组成部分对威胁检测性能的影响，本文设计了3种图模型变体进行消融测试，各变体与完整模型的检测结果差异见表6。为简洁起见，表6中仅列出了与所提方法检测结果存在差异的变体及其对应的数据集，其余变体在同一数据集上的表现与完整模型一致，故未重复列出。分析测试结果，由于基于结构熵博弈划分机制的社区检测方法依赖边权重进行社区划分，WEW变体在构建图时省略了边权重信息，无法完成有效的社区划分，从而削弱了对关键社区的识别能力，并限制了利用结构熵检测群体威胁模式的能力。PR变体在Web攻击与暴力破解类流量上的检测效果与完整模型一致，但由于其仅依赖PageRank度量顶点影响力，无法从社区维度检测威胁，因此无法有效检测恶意软件活动攻击。NB变体的检测结果与完整模型保持一致，说明本文所提检测方法在有向图场景下同样能够有效应用，具备支持有向图威胁检测任务的能力。

表6 消融测试结果

变体	数据集	准确率	F1 分数
WEW	Sality	—	—
	Spam50	—	—
PR	Sality	—	—
	Spam50	—	—

注：“—”表示该模型变体在对应数据集上检测失效。

3.1.5 超参数敏感性测试

为评估超参数对模型威胁检测性能的影响，本文开展了超参数敏感性测试。每组测试在固定其余参数的前提下，仅调整单个超参数，通过重新支持威胁检测任务，观察其对检测性能的具体影响。

社区检测终止阈值 τ_n 作为社区检测过程的迭代终止控制参数，对社区划分粒度仅产生细微影响。测试结果表明， τ_n 的变化对各数据集的威胁检测准确率无显著影响。这主要归因于本文方法中基于Z分数差异的威胁顶点检测方法能够自适应识别影响力大的离群点。在基于结构熵分析的威胁群体检测过程中，社区划分粒度的细微差异并不影响关键社区的识别及结构熵计算，从而保

证了模型威胁检测能力的稳健性。

微社区规模过滤阈值 $N_{\min}$ 对威胁社区检测的准确性具有一定的影响。当 $N_{\min}$ 设为 50 时, 模型能够准确检测威胁社区; 而当 $N_{\min}$ 设为 60 时, Spam50 数据集中的部分威胁社区因规模未达阈值而被过滤, 进而影响后续基于结构熵的威胁社区检测。

社区子图排序指标用于对 Top- k 社区子图进行排序, 其取值直接影响最终的威胁检测结果。测试结果表明, 不同的排序指标适用于不同类型的攻击。对于 Web 攻击和暴力破解攻击, 以社区规模作为排序指标能够保证检测效果, 原因在于这类攻击通常表现为大规模扫描, 具有影响范围广的特点; 对于 Sality 这类恶意软件攻击, 以社区内的平均度数作为排序指标更加有效, 原因在于此类攻击的威胁行为集中在高连接度顶点, 平均度数能够反映关键社区的活跃程度; 对于 Spam50 数据集^[25], 以社区内平均边权重作为排序指标更加有效, 原因在于该类攻击的威胁行为主要通过高强度通信传播, 边权重能够较好地反映社区内的流量活跃度。

PageRank 算法中的阻尼因子 γ 会影响顶点重要性计算结果。测试结果表明, 该参数的变化对威胁顶点检测的准确性无影响。这种稳健性主要归因于本文提出的基于 Z 分数差异的检测方法, 该方法能够有效抵消阻尼因子 γ 变化引起的得分波动, 从而保持对影响力大的威胁顶点的识别能力。

3.2 实网测试

3.2.1 实网威胁检测测试设置

(1) 硬件与软件环境

硬件环境方面, 本次实网威胁检测测试在操作系统为 Windows 10 企业版的 ThinkPad C480 笔记本电脑上开展, 设备搭载 Intel Core i7-8550U 处理器与 16 GB 内存。测试设备通过网络接入某知名网络安全企业的探针系统, 完成真实网络流量采集、流量交互图构建与威胁检测任务。软件环境方面, 本文所提检测方法基于 Python 3.12.7 实现, 流量交互图采用 NetworkX 3.3 库完成构建。社区检测选用开源 C++ 版本的 CoDeSEG 算法, 借助 CMake 4.1.0 将其编译为可执行文件。

(2) 数据集

测试所用真实网络流量由某知名网络安全企业探针系统采集, 总计获取 1 亿条流量样本。数据覆盖公网 Web 服务、内网及网络边界资产等场景, 包含传输控制协议 (transmission control protocol, TCP)、HTTP、超文本传输安全协议 (HTTPS)、域名系统 (domain name system, DNS) 协议、传输层安全协议 (TLS) 等, 并在采集后完成脱敏处理。考虑到真实网络流量大多采用加密传输, 可用特征主要为流量五元组信息和上下行数据报文长度。经数据预处理后, 将其简化为本文方法兼容的三元组信息和数据报文长度。相较于开源流量数据集, 实网流量具有业务流量与威胁流量相互交叠、主机交互类型复杂多样的特点, 能够验证所提方法在真实环境下的鲁棒性和泛化能力。

3.2.2 实网威胁检测测试

由于探针采集的流量数据无标签信息, 在评估过程中, 本文结合资产标签、公开威胁情报数据及实网威胁规则防护引擎的处置结果, 对模型识别出的威胁实体进行分析。

表 7 展示了本文方法在实网部署后的部分威胁检测结果, 其中 PR 对应 2.6.1 节基于 Z 分数差异的威胁顶点检测, SE 对应 2.6.2 节基于结构熵的群体威胁检测。与网络安全企业威胁情报平台提供的开源情报、网络资产标签及威胁规则引擎的处置结果进行对比发现, 本文方法能够有效检测针对 Web 服务的多类威胁实体^[26], 覆盖目录遍历、垃圾邮件投递、暴力破解及分布式拒绝服务 (distributed denial of service, DDoS) 攻击等威胁行为。其中, 基于 Z 分数差异的威胁顶点识别方法成功检测出 1 个针对公网 Web 服务实施目录遍历与路径穿越的攻击实体; 基于结构熵的威胁群体检测方法则识别出 259 个呈现集中通信特征的 Web、僵尸网络及垃圾邮件攻击群体。为客观评估检测效能, 研究人员构建了多源交叉验证模型作为判定基准, 其匹配规则定义如下: 若目标 IP 地址被任一商用或开源威胁情报平台标记为恶意, 或其行为特征命中网络安全企业规则处置引擎, 则判定为验证通过。检测结果表明, 基于结构熵的方法具备良好的群体检测能力^[27], 259 个

威胁实体中有254个通过交叉验证，检测结果验证通过率达到98.07%。对5个（约1.93%）未命中标签的误报进行分析发现，该类实体多为新近上线的服务节点，且在监测期间正遭受潜在攻击。实网测试结果表明，本文提出的流量交互图分析方法能够在不依赖标签的情况下，在真实网络环境中检测出安全威胁实体，且能够通过流量交互图从图结构特征^[28]、图结构熵等维度对检测结果进行可解释性分析，为威胁研判提供支持。

表7 实网检测结果

IP	本文方法检出	规则引擎处置	威胁行为
111.7.100.67	PR	封禁	目录遍历、路径穿越
117.205.171.20	SE	封禁	僵尸网络
205.210.31.54	SE	封禁	Web、垃圾邮件攻击
65.49.1.29	SE	封禁	垃圾邮件攻击
198.235.24.114	SE	封禁	Web、垃圾邮件攻击
162.216.149.248	SE	封禁	Web、暴力破解攻击
92.204.173.24	SE	—	命令服务控制
198.235.24.114	SE	—	Web、垃圾邮件攻击
193.163.125.166	SE	—	Web、DDoS攻击
43.248.108.69	SE	—	Web、DDoS攻击
112.4.101.76	SE	—	DDoS、垃圾邮件攻击

4 结束语

针对Web服务环境中未知威胁与群体性攻击日益增多、传统检测方法难以在无标签场景下实现有效防御的问题，本文提出了一种基于流量交互图分析的威胁检测方法。该方法通过构建轻量化流量交互图，引入结构熵博弈划分机制实现网络社区的自适应划分，结合Z分数定位高威胁顶点，并利用结构熵变化特征识别群体威胁行为，从而在无监督条件下完成对威胁的检测与解释。测试结果表明，该方法在真实网络环境中能够有效识别目录遍历、僵尸网络、暴力破解及垃圾邮件等威胁，部分检出威胁未被现有规则引擎覆盖，体现了该方法在实际安全防护部署中的补充价值。受限于真实网络环境缺乏全量真实标签，本文通过在标注完备的公开数据集上进行性能评测，利用F1分数等综合指标间接验证

了所提模型在处理复杂威胁时的可靠性与召回能力，弥补了实网环境下漏报率难以精确统计的局限。本文方法不依赖先验知识与标签数据，兼具对未知威胁的适应能力、对加密流量的鲁棒性及模型的可解释性，为Web服务安全防护提供了一种新的无监督检测思路。未来工作计划引入时序演化建模与跨域威胁情报，进一步提升检测精度与场景泛化能力，为构建Web安全防护体系提供支撑。

参考文献：

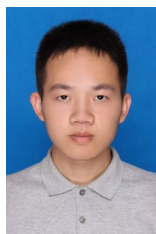
- [1] Bronte R, Bronte R, Shahriar H, et al. A signature-based intrusion detection system for web applications based on genetic algorithm[C]//Proceedings of the 9th International Conference on Security of Information and Networks. New York: ACM, 2016: 32-39.
- [2] Díaz-Verdejo J, Muñoz-Calle J, Estepa Alonso A, et al. On the detection capabilities of signature-based intrusion detection systems in the context of web attacks[J]. Applied Sciences, 2022, 12(2): 852.
- [3] Yang R, Wang X, Luo K, et al. SWIDE: a semantic-aware detection engine for successful web injection attacks[C]//Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2024: 540-554.
- [4] Kumar J, Santhanavijayan A, Rajendran B. Cross site scripting attacks classification using convolutional neural network[C]//Proceedings of the 2022 International Conference on Computer Communication and Informatics (ICCCI). Piscataway: IEEE Press, 2022: 1-6.
- [5] Alazab A, Khraisat A, Alazab M, et al. Detection of obfuscated malicious JavaScript code[J]. Future Internet, 2022, 14(8): 217.
- [6] Zhou Y H, Zhu H Y, Chai Y D, et al. Towards trustworthy web attack detection: an uncertainty-aware ensemble deep kernel learning model[PP]. arXiv [2025-10-13]. arXiv:arXiv.2410.07725.
- [7] Song X Y, Chen C, Cui B J, et al. Malicious JavaScript detection based on bidirectional LSTM model[J]. Applied Sciences, 2020, 10(10): 3440.
- [8] Liu M Y, Gou G P, Xiong G, et al. Enhanced detection of obfuscated HTTPS tunnel traffic using heterogeneous information network[J]. Computer Networks, 2025, 257: 110975.
- [9] Karbab E B, Debbabi M, Derhab A, et al. Scalable and robust unsupervised Android malware fingerprinting using community-based network partitioning[J]. Computers & Security, 2020, 96: 101932.
- [10] Li Y, Chen X S, Tang W Y, et al. Interaction matters: Encrypted traffic classification via status-based interactive behavior graph[J]. Applied Soft Computing, 2024, 155: 111423.
- [11] Li A S, Pan Y C. Structural information and dynamical complexity of networks[J]. IEEE Transactions on Information Theory, 2016, 62(6): 3290-3339.
- [12] Holt C A, Roth A E. The Nash equilibrium: a perspective[J]. Proceedings of the National Academy of Sciences of the United States of America, 2004, 101(12): 3999-4002.
- [13] Xian Y T, Xian Y T, Li P, et al. Community detection in large-scale complex networks via structural entropy game[C]//Proceedings of

- the ACM on Web Conference 2025. New York: ACM, 2025: 3930-3941.
- [14] Fenton A, Gillooly L, Vasilica C M. Female fans and social media: micro-communities and the formation of social capital[J]. European Sport Management Quarterly, 2023, 23(2): 370-390.
- [15] Montanari A. Finding one community in a sparse graph[J]. Journal of Statistical Physics, 2015, 161(2): 273-299.
- [16] Gleich D F. PageRank beyond the web[J]. SIAM Review, 2015, 57(3): 321-363.
- [17] Peng H, Zhang J Y, Huang X, et al. Unsupervised social bot detection via structural information theory[J]. ACM Transactions on Information Systems, 2024, 42(6): 1-42.
- [18] Fu C P, Li Q, Xu K. Flow interaction graph analysis: unknown encrypted malicious traffic detection[J]. IEEE/ACM Transactions on Networking, 2024, 32(4): 2972-2987.
- [19] Pellegrino G, Johns M, Koch S, et al. Deemon: detecting CSRF with dynamic analysis and property graphs[C]//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2017: 1757-1771.
- [20] Caballero J, Grier C, Kreibich C, et al. Measuring pay-per-install: the commoditization of malware distribution[C]//Proceedings of the USENIX Security Symposium. Berkeley: USENIX Association, 2011: 1-13.
- [21] Ahmed M, Seraj R, Islam S M S. The k-means algorithm: a comprehensive survey and performance evaluation[J]. Electronics, 2020, 9(8): 1295.
- [22] Qi X Q, Wu Q, Zhang Y S, et al. A novel model for DNA sequence similarity analysis based on graph theory[J]. Evolutionary Bioinformatics Online, 2011, 7: 149-158.
- [23] Karbab E B, Debbabi M. ToGather: automatic investigation of Android malware cyber-infrastructures[C]//Proceedings of the 13th International Conference on Availability, Reliability and Security. New York: ACM, 2018: 1-10.
- [24] 张子龙, 董卫宇, 王奕森. 保留因果关系的溯源图压缩方法[J]. 网络与信息安全学报, 2025, 11(6): 105-119.
- Zhang Z L, Dong W Y, Wang Y S. Causality-preserving compression method on provenance graph[J]. Chinese Journal of Network and Information Security, 2025, 11(6): 105-119.
- [25] Zhao Y, Xie Y, Yu F, et al. BotGraph: Large scale spamming botnet detection[C]//Proceedings of the USENIX Symposium on Networked Systems Design and Implementation. Berkeley: USENIX Association, 2009: 321-334.
- [26] Zeng X H, Peng H, Li A S. Proactive bot detection based on structural information principles[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2026, 48(4): 4726-4743.
- [27] Peng H, Huang X, Sun S, et al. Adaptive and robust DBSCAN with multi-agent reinforcement learning[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2025, 48(4): 4860-2877.
- [28] 李一凡, 李家印, 林兴澎, 等. 基于数据增强的多视图对比学习图异常检测[J]. 网络与信息安全学报, 2024, 10(5): 163-174.
- Li Y F, Li J Y, Lin X P, et al. Data augmentation based multi-view contrastive learning graph anomaly detection[J]. Chinese Journal of Network and Information Security, 2024, 10(5): 163-174.

[作者简介]



余北缘 (1996-), 男, 北京航空航天大学博士生, 主要研究方向为 Web 安全。



曾广杰 (1997-), 男, 北京航空航天大学博士生, 主要研究方向为图数据挖掘。



彭浩 (1987-), 男, 博士, 北京航空航天大学教授、博士生导师, 主要研究方向为事件检测。



刘建伟 (1964-), 男, 博士, 北京航空航天大学教授、博士生导师, 主要研究方向为密码学与网络安全。



李洪亮 (1980-), 男, 奇安信科技集团股份有限公司网络安全部总经理, 主要研究方向为企业安全防护体系建设、高级威胁对抗、安全基础设施。



谭学士 (1984-), 男, 奇安信科技集团股份有限公司网络安全部安全平台组负责人, 主要研究方向为网络安全算法与人工智能应用。