

费圣翔, 陈子龙, 王冲, 等. 基于图神经网络的异构网络信息安全漏洞深度检测方法[J]. 华南地震, 2024, 44(3): 180–186. [FEI Shengxiang, CHEN Zilong, WANG Chong, et al. Depth Detection Method for Information Security Vulnerabilities in Heterogeneous Networks Based on Graph Neural Network [J]. South China journal of seismology, 2024, 44(3): 180–186]

## 基于图神经网络的异构网络信息安全漏洞 深度检测方法

费圣翔<sup>1</sup>, 陈子龙<sup>2</sup>, 王冲<sup>2</sup>, 王睿<sup>3</sup>, 刘新鹏<sup>4</sup>

(1. 山东九州信泰信息科技股份有限公司, 济南 250101; 2. 山东慢雾信息技术有限公司, 济南 250102; 3. 国网山东省电力公司电力科学研究院, 济南 250003; 4. 恒安嘉新(北京)科技股份公司, 北京 100080)

**摘要:** 受到连接设备多样性以及互操作性特点的影响, 异构网络节点之间的关联关系较为复杂, 因此在进行安全漏洞检测时, 通常会引起缺乏对节点关联关系的有效捕捉而导致检测精度不佳。对此, 提出基于图神经网络的异构网络信息安全漏洞深度检测方法。以异构网络实体作为图节点, 并以不同实体之间的关联关系作为边, 将异构网络转换为图表示, 并分别采用邻接矩阵以及权重矩阵对节点以及边信息进行提取。采用图神经网络领域中的 GraphSAGE 网络模型对异构网络的节点和边进行处理, 并引入注意力机制以学习节点特征表示。将异构网络中节点和边的特征向量作为数据输入, 结合随机森林算法构建一个分类器, 并通过对其进行训练, 使其能够根据边和节点的属性信息对是否存在安全漏洞进行判断, 最后结合投票法对输入样本的所属类别进行确定。在实验中, 对提出的方法进行了检测精度的检验。最终的测试结果表明, 采用提出的方法对异构网络安全漏洞进行检测时, 漏洞风险等级的匹配度较高, 具备较为理想的检测精度。

**关键词:** 图神经网络; 异构网络; 安全漏洞; 检测方法; 检测精度

中图分类号: TP393

文献标识码: A

文章编号: 1001-8662(2024)03-0180-07

DOI: 10.13512/j.hndz.2024.03.20

## Depth Detection Method for Information Security Vulnerabilities in Heterogeneous Networks Based on Graph Neural Network

FEI Shengxiang<sup>1</sup>, CHEN Zilong<sup>2</sup>, WANG Chong<sup>2</sup>, WANG Rui<sup>3</sup>, LIU Xinpeng<sup>4</sup>

(1. Shandong Jiuzhou Xintai Information Technology Co., Ltd., Jinan 250101, China; 2. Shandong Slow Mist Information Technology Co., Ltd., Jinan 250102, China; 3. Electric Power Research Institute of State Grid Shandong Electric Power Company, Jinan 250003, China; 4. Hengan Jiaxin(Beijing)Technology Co., Ltd., Beijing 100080, China)

**Abstract:** Influenced by the diversity and interoperability of connected devices, the relationship between heterogeneous network nodes is complex. Therefore, it usually leads to the lack of effective capture of the relationship between nodes when detecting security vulnerabilities, resulting in poor detection accuracy. To solve this problem,

收稿日期: 2024-06-05

作者简介: 费圣翔(1987-), 男, 工程师, 主要研究方向为网络安全运营、信息安全风险评估。

E-mail: nformati@163.com

this paper proposed a depth detection method for information security vulnerabilities in heterogeneous networks based on a graph neural network. Heterogeneous network entities were regarded as graph nodes, and the relationship between different entities was regarded as edges. The heterogeneous network was transformed into a graph representation, and the node and edge information were extracted by adjacency matrix and weight matrix, respectively. GraphSAGE network model in the field of graph neural network was used to deal with the nodes and edges in the heterogeneous network, and an attention mechanism was introduced to learn the feature representation of nodes. The feature vectors of nodes and edges in the heterogeneous network were used as data inputs, and a classifier was constructed by using the random forest algorithm and trained to make it determine whether there are security vulnerabilities based on the attribute information of edges and nodes. Finally, the input samples were classified by voting method. In the experiment, the detection accuracy of the proposed method was tested. The final test results show that when the proposed method is used to detect security vulnerabilities in the heterogeneous network, the matching degree of vulnerability risk levels is high, and the detection accuracy is ideal.

**Keywords:** Graph neural network; Heterogeneous network; Security vulnerabilities; Detection method; Detection accuracy

## 0 引言

网络空间的开放性和复杂性使得信息安全问题日益凸显,其中信息安全漏洞是网络攻击的主要突破口。传统的信息安全漏洞检测方法多依赖于专家经验和规则匹配,但在面对复杂多变的网络环境和攻击手段时,这些方法往往显得力不从心。因此,如何高效、准确地检测信息安全漏洞,是信息安全领域需要解决的关键问题。深度学习技术的崛起为信息安全漏洞检测提供了新的思路。图神经网络(Graph Neural Networks, GNNs)作为深度学习领域的一种创新模型,能够处理图结构数据,已在社交网络分析、个性化推荐以及生物信息学等多个领域显露出其巨大的应用潜力和价值。考虑到信息安全漏洞往往存在于由不同实体和关系构成的异构网络中,基于图神经网络的异构网络信息安全漏洞深度检测方法逐渐成为研究的热点。

在信息安全漏洞检测领域,已有学者从不同角度开展了较为深入的研究。例如,文献[1]通过构建时间卷积网络(TCN)来捕获软件漏洞在时间序列上的特征。并引入深度残差收缩网络(DRSN)来优化模型结构,减少冗余信息并提高特征提取能力。尽管该方法在多个数据集上取得了较高的检测精度,但在处理复杂多变的网络攻击模式时,由于TCN的局限性,模型可能无法准确捕捉攻击行为在时间维度上的细微变化。文献[2]通过遗传算法对通信网络中的潜在漏洞进行编码和进化,以寻找最优的漏洞检测策略。但启发式搜索算法

在复杂网络环境中的性能受到挑战,尤其是当网络结构动态变化时,遗传算法的适应性和收敛速度可能受到影响,导致漏洞检测的实时性和准确性不足。文献[3]通过图卷积网络捕获网络拓扑结构中的漏洞特征,并利用注意力机制对关键特征进行加权处理。但由于网络结构的复杂性和多样性,图卷积网络可能无法完全覆盖所有可能的漏洞模式,导致某些特殊类型的漏洞被遗漏。文献[4]提出构建多棵孤立树来检测异常数据点,从而识别出潜在的网络安全漏洞。但随着数据维度的增加,孤立树构建过程的复杂性和计算成本都会显著增加。

本文提出了一种基于图神经网络的漏洞检测架构,该架构集成了注意力机制,以捕捉节点间的关联关系,并有效利用异构网络中的特征信息,从而实现对潜在漏洞的精准预测。

## 1 基于图神经网络的异构网络信息安全漏洞深度检测方法

### 1.1 异构网络图表示及节点/边信息提取

在异构网络中,不同类型的实体(如服务器、用户、应用程序等)和关系(如通信、访问、控制等)具有不同的属性和特征。通过信息提取可以区分这些差异,使GNN模型能够适应异构网络的特性,进行更准确的漏洞检测<sup>[5]</sup>。因此在进行异构网络信息安全漏洞检测之前,本文首先针对异构网络进行图表示以及节点/边信息提取,提取出的节点和边信息可以作为GNN模型的输入特征,帮助

模型学习节点之间的关联关系, 进而进行漏洞检测。

首先, 将异构网络信息安全漏洞相关的数据转化为图表示。图数据由节点(Node)和边(Edge)组成, 节点可以代表网络中的不同实体(如服务器、用户、设备等), 边则代表实体之间的关联关系(如通信、访问等)。因此可以将节点表示为一个特征向量  $\text{Node}_i = [a_1^i, a_2^i, \dots, a_n^i]$ ,  $\text{Node}_i$  其中代表第  $i$  个节点,  $a_j^i$  代表第  $i$  个异构网络节点的第  $j$  个属性。边可以表示为一个三元组  $\text{Edge}_{ij} = (\text{Node}_i, r_{ij}, w_{ij})$ , 其中,  $r_{ij}$  和  $w_{ij}$  分别代表边的关系类型以及边的权重<sup>[6]</sup>。为对异构网络的节点信息进行提取, 本文从数据源中对节点属性进行提取, 具体数据源包括日志文件、配置文件以及异构网络扫描结果等, 因此可以获得节点的IP地址、MAC地址、CPU使用率、内存占用率等静态属性以及动态属性<sup>[7]</sup>。提取后的节点信息可以表示为一个特征矩阵  $X$ , 其中每一行均对应一个异构网络节点, 每一列对应一个节点属性, 其具体矩阵表达式如下所示。

$$X = \begin{bmatrix} \text{Node}_1 \\ \text{Node}_2 \\ \dots \\ \text{Node}_m \end{bmatrix} = \begin{bmatrix} a_1^1 & a_2^1 & \dots & a_n^1 \\ a_1^2 & a_2^2 & \dots & a_n^2 \\ \dots & \dots & \dots & \dots \\ a_1^m & a_2^m & \dots & a_n^m \end{bmatrix} \quad (1)$$

对于边信息提取, 本文选择采用邻接矩阵  $R$  以及权重矩阵  $W$  对其进行表示, 邻接矩阵反映了图中节点间的相邻状态, 而权重矩阵则用于量化这些边的权重。两个矩阵表达式如下所示。

$$R = \begin{bmatrix} 0 & r_{12} & \dots & r_{1N} \\ r_{21} & 0 & \dots & r_{2N} \\ \dots & \dots & \dots & \dots \\ r_{N1} & r_{N2} & \dots & 0 \end{bmatrix} \quad (2)$$

$$W = \begin{bmatrix} 0 & w_{12} & \dots & w_{1N} \\ w_{21} & 0 & \dots & w_{2N} \\ \dots & \dots & \dots & \dots \\ w_{N1} & w_{N2} & \dots & 0 \end{bmatrix} \quad (3)$$

在邻接矩阵  $R$  中, 如果异构网络节点  $i$  和  $j$  之间存在边, 则  $r_{ij}$  的值为 1, 如果不存在边, 则  $r_{ij}$  的值为 0。

通过上述步骤即可完成对于异构网络中节点以及边信息的提取, 并对其进行图表示处理<sup>[8]</sup>。以异构网络实体作为图节点, 并以不同实体之间的关联关系作为边, 将异构网络转换为图表示, 并分别采用邻接矩阵以及权重矩阵对节点以及边信息进行提取。

## 1.2 基于图神经网络的异构网络节点/边映射处理

在完成节点以及边信息提取后, 本文通过图神经网络模型, 将异构网络中的节点和边映射到向量空间中, 得到它们的特征表示。

本文采用图神经网络领域中的 GraphSAGE 网络模型对异构网络的节点和边进行处理, 并引入注意力机制以学习节点特征表示。首先需要对节点邻域进行采样处理, 对于一个给定节点, 本文从其邻居中随机采样固定数量的节点, 作为该节点的邻域。假设节点  $v$  的  $k$  阶邻域为  $N_k(v)$ , 那么 GraphSAGE 通过聚合函数 AGGREGATE 对信息进行聚合, 从而更新该节点的标识<sup>[9]</sup>。该函数将邻域节点的特征作为输入, 并输出一个固定大小的向量作为聚合结果。假设  $h_u^{k-1}$  代表节点  $u$  在  $k-1$  层的标识,  $a_{vu}^k$  代表从节点  $v$  到其邻接节点  $u$  的注意力系数, 则节点  $v$  在  $k$  层的聚合表示  $h_v^k$  可以通过以下的形式表示。

$$h_v^k = \sigma \left( W^k \cdot \text{AGGREGATE} \left( \{ a_{vu}^k \cdot h_u^{k-1} | u \in N_k(v) \} \right) \right) \quad (4)$$

式(4)中,  $\sigma$  代表激活函数,  $W^k$  代表可学习的权重矩阵。为了更精确地捕捉节点间的相互关联性, 本文引入注意力机制, 以便为不同的邻居点赋予差异化的权重<sup>[10]</sup>。注意力机制可以计算出权重  $a_{vu}^k$  的具体数值, 具体表达式如下所示。

$$a_{vu}^k = \frac{1}{\exp(f(h_v^{k-1}, h_u^{k-1}))} \quad (5)$$

式(5)中,  $f(\cdot)$  代表注意力得分函数, 用于计算节点  $v$  以及邻居节点  $u$  之间的注意力得分<sup>[11]</sup>。在节点特征整合与更新的流程中, GraphSAGE 算法通过抽样邻居节点、整合这些节点的特征, 并更新目标节点的特征, 从而生成每个节点的嵌入表示。这个过程捕获了节点的局部邻域信息, 并将其编码到一个向量表示中, 以此可以在异构网络中将节点和边映射到向量空间中, 这些表示可以作为后续模型的输入或特征, 为漏洞分类与检测提供帮助<sup>[12]</sup>。

## 1.3 安全漏洞判断与检测

在获取了异构网络节点和边的特征表示后, 本文选取这些特征作为输入, 利用随机森林算法构建分类模型, 实现异构网络信息安全漏洞深度检测。随机森林算法的分类预测流程如下图所示。

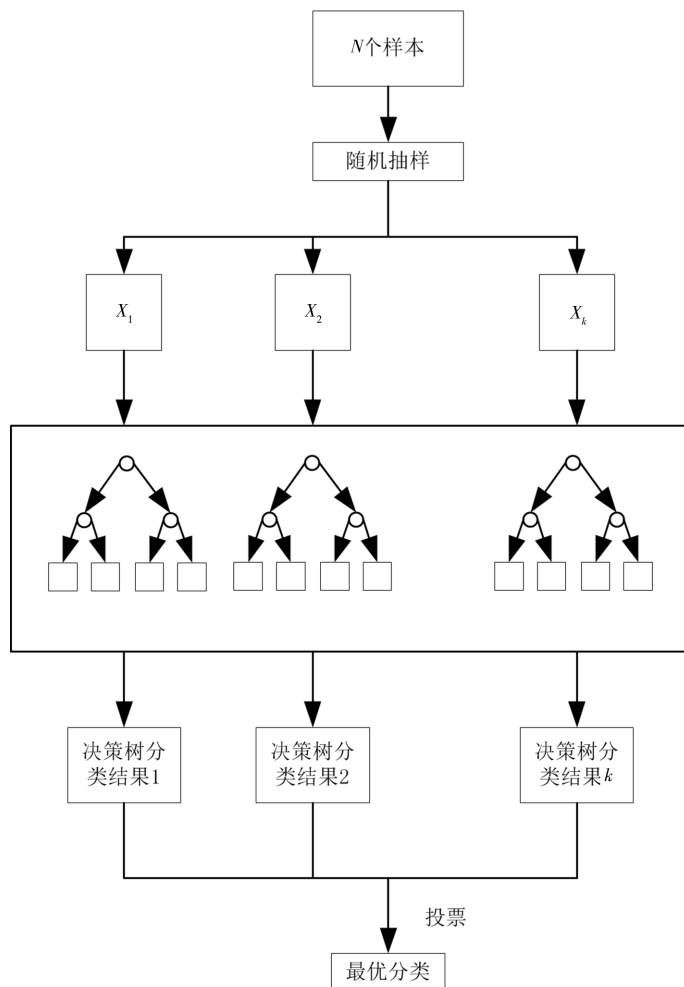


图1 随机数森林算法分类预测流程

Fig.1 Classification and prediction flow of random forest algorithm

首先本文构建了一个带有标签的样本集。每个样本可以是一个节点或者一条边，对应的标签可以是该节点或边是否包含安全漏洞。对于节点样本，本文选择直接使用节点的特征向量作为输入，并附上相应的标签。对于边样本，本文选择使用之前计算得到的边的特征向量作为输入，并附上相应的标签<sup>[13]</sup>。然后可以对随机森林进行构建，对于一个包含  $m$  个样本和  $n$  个特征的数据集  $D$ ，首先本文从数据集  $D$  中随机选取  $m$  个样本作为基决策树的初始训练集  $D_t$ ，然后随机选择  $k$  个特征作为候选特征集。从  $k$  个特征中挑选出最佳特征进行节点划分，以构建基决策树。这一过程将持续进行，直到达到停止条件，即叶子节点数达到最大值。对于新的样本  $x$ ，即异构网络信息数据，本文选择将其输入到每个基决策树中，以此可以得到  $M$  个预测结果  $y_t (t = 1, 2, \dots, M)$ <sup>[14]</sup>。通过采用投票的方式，可以对最终的预测类别进行确定，最终预测结果  $y_{\text{final}}$  表达式如下所示。

$$y_{\text{final}} = \frac{\sum_{t=1}^M y_t}{M} \quad (6)$$

通过上述步骤即可完成对于安全漏洞的判断以及预测。通过整合异构网络中节点和边的特征向量作为输入数据，利用随机森林算法来构建和优化分类器模型，并通过对其进行训练，使其能够根据边和节点的属性信息对其是否存在安全漏洞进行判断，最后结合投票法对输入样本的所属类别进行确定。将本节内容与上述提到的图表示以及节点/边映射处理等相关内容进行结合，至此，基于图神经网络的异构网络信息安全漏洞深度检测方法设计完成<sup>[15]</sup>。

## 2 实验论证

为了证明本文提出的基于图神经网络的异构网络信息安全漏洞深度检测方法在实际检测效果方面优于常规的网络信息安全漏洞检测方法，在



完成算法方面的设计后，通过构建实验对比环节，对本文方法的实际检测效果进行检验。

2.1 实验说明

为验证本文提出的基于图神经网络的异构网络信息安全漏洞深度检测在实际检测效果方面的优越性，本次实验选取了两组常规的网络信息安全漏洞检测方法作为对比对象，分别为基于遗传算法的网络信息安全漏洞检测方法，以及基于注意力机制的网络信息安全漏洞检测方法。为了确保实验的可操作性和可复制性，本实验在精心配置的硬件和软件环境下进行。实验硬件环境如表1所示。

表 1 实验硬件环境	
Table 1 Experimental hardware environment	
组件	描述
处理器	Intel Core i9-9900K, 3.60GHz, 16核 32线程
内存	64GB DDR4 RAM
存储	1TB NVMe SSD
CPU	NVIDIA GeForce RTX 3090, 24GB GDDR6X

在软件层面，基于 Ubuntu 20.04 LTS 操作系统，使用 Python 3.8 作为编程语言，并选用了 PyTorch 1.8.0 深度学习框架，结合 PyTorch Geometric 1.7.0，以支持图神经网络的实现。此外，利用 Pandas、NumPy 进行数据处理，以及 Matplotlib 和 NetworkX 进行结果的可视化分析。构建一个包含多种类型安全漏洞的测试数据集，该数据集融合了真实网络数据模拟与合成方法生成的内容，以模拟真实世界中的复杂网络环境和多样化的安全威胁。通过构建实验平台，采用三种检测方法对同一个异构网络结构中的安全漏洞进行检测，对比不同方法的实际检测效果。

2.2 实验对象

本实验模拟了一个具有典型特征的异构网络，包含三种不同类型的节点：用户节点、服务节点和数据节点。网络中的边表示不同节点之间的交互关系，具体分为用户与服务之间的访问关系、服务之间的依赖关系以及服务与数据之间的存储关系。网络中共包含 10 000 个节点，其中用户节点占 40%，服务节点占 30%，数据节点占 30%。边的数量根据不同类型的节点及其交互关系进行随机生成，确保网络的连通性和复杂性。网络拓扑结构如图 2 所示。

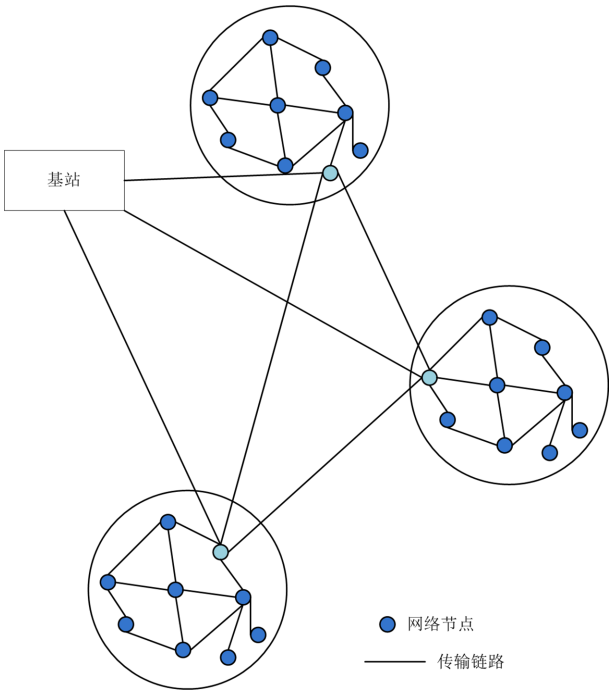


图 2 异构网络拓扑结构  
Fig.2 Topology of heterogeneous network

为了保证网络的稳定性，本实验在模拟过程中设置了合理的参数限制，如节点的最大度数、边的最大权重等。同时，通过实时监测网络的连通性和性能，确保网络在动态变化中保持一定的稳定性。同时，为了模拟真实网络中的动态变化，本实验在模拟过程中引入了节点和边的动态增删机制。节点的增删模拟了用户的加入和退出，边的增删模拟了服务间的依赖关系变化和数据的存储迁移。同时，针对模拟出的异构网络，本文在其中添加了不同类型安全漏洞，以供算法进行检测与分析，具体模拟漏洞分布情况如表 2 所示。

根据网络规模和参数配置，生成初始的异构网络结构，并在该网络结构中添加不同类型的安全漏洞。本文利用三种不同的方法对异构网络模型进行了安全漏洞检测。在实验中，设定图神经网络的节点嵌入维度为 64，边嵌入维度为 32，学习率则设定为 0.001。对于随机森林模型，设定包含 100 棵决策树，并且每棵决策树的最大深度为 10。通过对本文算法的参数进行配置，并进行模拟仿真测试。

2.3 检测精度对比结果

本文方法所得到的异构网络信息安全漏洞深度检测结果如表 3 所示。

表 2 模拟漏洞分布情况

Table 2 Distribution of simulated vulnerability

漏洞名称	漏洞类型	漏洞风险等级	漏洞模拟占比/(%)
硬编码密码泄露	信息泄露	高危	15
SQL注入	代码执行	高危	20
跨站脚本攻击(XSS)	跨站脚本	中危	18
文件包含漏洞	远程文件执行	高危	12
认证绕过	身份验证	中危	10
路径遍历	文件访问	中危	8
远程命令执行(RCE)	远程代码执行	高危	10
跨站请求伪造(CSRF)	会话劫持	低危	5
HTTP头注入	协议篡改	中危	2
不安全的直接对象引用	访问控制	中危	10

表 3 本文方法下的安全漏洞深度检测结果

Table 3 Results of depth detection of security vulnerabilities by proposed method

样本编号	预测标签/0:不存在漏洞/1:存在漏洞	预测漏洞类型
01	1	SQL注入
02	1	信息泄露
03	0	-
04	1	跨站脚本
05	1	跨站脚本攻击(XSS)
06	0	-
07	1	远程命令执行(RCE)
08	1	跨站请求伪造(CSRF)

通过上述实验结果可以看出，本文提出的方法能够有效针对不同类型的安全漏洞进行检测，通过结合节点以及边的属性特征，判断出当前网络是否存在安全漏洞。为提高实验结果的对比性，本次实验以不同检测结果的漏洞风险等级匹配度作为对比指标，对方法的实际检测精度进行衡量。该值代表检测出的漏洞的风险等级与实际漏洞风险等级的匹配程度，其具体对比结果如图3所示。

通过上述实验结果可以看出，在针对相同的异构网络进行安全漏洞检测时，不同算法的实际检测精度也有所不同。通过数值上的对比可以明显看出，本文提出的检测方法在实际检测精度方面明显优于两种常规的漏洞检测方法，检测出的漏洞等级与实际风险等级一致度更高。

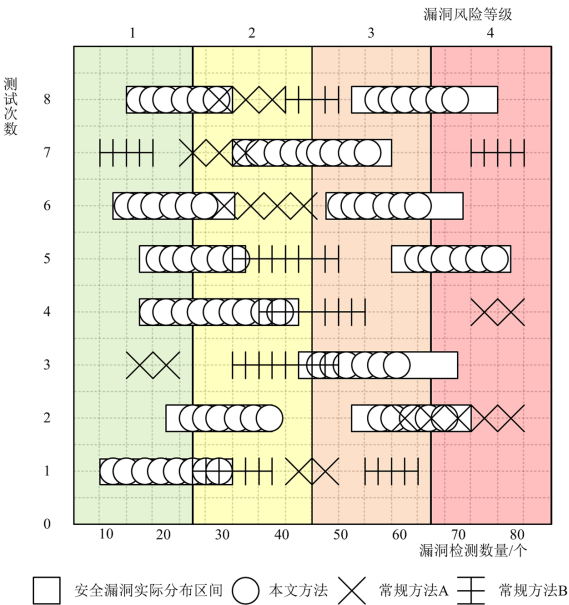


图3 漏洞风险等级匹配度对比结果

Fig.3 Comparison results of matching degrees of vulnerability risk level

### 3 结语

本研究的意义在于,通过构建异构网络模型,能够更全面地描述网络环境中不同实体和它们之间的复杂关系,从而更准确地理解网络的行为和特征。而图神经网络的应用,则使得本文能够自动学习网络中的特征信息,并通过深度学习的方式来预测和发现潜在的安全漏洞。

### 参考文献

- [1] Chen J, Lin W, Cai S, et al. BiTCN\_DRSN: An effective software vulnerability detection model based on an improved temporal convolutional network[J]. Journal of Systems and Software, 2023(204): 111772–111776.
- [2] 潘超,吕翹楚,肖巍. 基于启发式遗传算法的即时通信网络漏洞检测[J]. 计算机仿真, 2023, 40 (08): 191–195.
- [3] 肖鹏,张旭升,杨丰玉,等. 基于深层图卷积网络与注意力的漏洞检测方法[J]. 计算机工程与应用, 2024, 60 (03): 292–298.
- [4] 刘悦. 基于孤立森林算法的计算机网络信息安全漏洞检测方法[J]. 信息与电脑(理论版), 2024, 36 (04): 68–70.
- [5] 陈锦富,王震鑫,蔡赛华,等. 基于蜕变测试的区块链智能合约漏洞检测方法[J]. 通信学报, 2023, 44 (10): 164–176.
- [6] 马莺姿,陈哲,殷家乐,等. 结合模糊测试和动态分析的内存安全漏洞检测[J]. 计算机科学, 2024, 51 (02): 352–358.
- [7] 吕连,谢东刚. 基于权重k邻近的通信网络安全漏洞自动化检测[J]. 自动化与仪器仪表, 2024, (04): 21–24+31.
- [8] 董继平,郭启全,高春东,等. 基于图深度学习的漏洞检测[J]. 科技导报, 2023, 41 (13): 41–59.
- [9] 张和伟,王奉章. 基于被动分簇算法的即时通信网络安全漏洞检测方法[J]. 智能计算机与应用, 2023, 13 (07): 119–122.
- [10] 王璇,王馨彤,陈燕俐,等. 基于 DistilBert-LSTM 与多项朴素贝叶斯的漏洞检测方法[J]. 南京邮电大学学报(自然科学版), 2023, 43 (02): 102–110.
- [11] 王泽旭,文斌. 关键路径预搜索的符号执行智能合约漏洞检测[J]. 应用科学学报, 2024, 42 (02): 364–374.
- [12] 何杰,蔡瑞杰,尹小康,等. 面向 Cisco IOS-XE 的 Web 命令注入漏洞检测[J]. 计算机科学, 2023, 50 (04): 343–350.
- [13] 朱丽娜,马铭芮,朱东昭. 基于图神经网络和通用漏洞分析框架的 C 类语言漏洞检测方法[J]. 信息安全, 2022, 22 (10): 59–68.
- [14] 徐晓君,常会丽. 多线程交互学习软件系统安全漏洞自动化检测[J]. 计算机仿真, 2022, 39 (04): 335–340.
- [15] 马艺新,唐时博,谭静,等. 基于信息流分析的密码核设计安全验证与漏洞检测[J]. 西北工业大学学报, 2022, 40 (01): 76–83.