融合双模态感知的漏洞知识图谱构建与补全方法

张 龑[1,2,3,4,5],罗翔宇[2],秦紫玥[1],张 森[1,3,4],李志飞[1,2,3,4,5*]

(1. 湖北大学计算机学院,湖北武汉 430062;2. 湖北大学网络空间安全学院,湖北武汉 430062;
3. 大数据智能分析与行业应用湖北省重点实验室,湖北武汉 430062;4. 智能感知系统与安全教育部重点实验室,湖北武汉 430062;
5. 智能网联汽车网络安全湖北省工程研究中心,湖北武汉 430062)

摘 要: 漏洞知识图谱作为网络安全知识建模的重要工具,在漏洞分析、威胁建模、安全态势感知和攻击链追踪等关键任务中发挥着日益重要的作用. 与通用知识图谱覆盖领域广、更新周期长,侧重于通用知识与关系建模不同的是,漏洞知识图谱更新频率高,面临着数据异构、语义歧义和知识稀疏的挑战,往往需要融合非结构化描述信息进行联合建模. 然而,现有方法仍局限于三元组建模范式,忽略了网络安全知识库中丰富的安全文本信息,导致漏洞知识图谱补全与攻击链预测精度受限. 为此,本文提出构建一种漏洞描述知识图谱(Vulnerability description Knowledge Graph,VKG-T),通过联合结构和语义信息,增强漏洞弱点信息的补全能力. 同时,本文设计了一种双模态感知聚合的漏洞描述知识图谱补全模型(Vulnerability description Knowledge Graph Completion, VKGC-ST),该模型结合图注意力网络(Graph ATtention networks,GAT)与预训练语言模型,综合考虑实体的结构邻接特征与文本描述信息,并结合多层次负采样与对比学习机制,提升实体语义判别能力和结构关联建模效果. 通过在漏洞描述知识图谱VKG-T以及通用数据集FB15K-237、WN18RR上的链接预测实验证明,VKGC-ST在所有指标上均取得最佳性能,其中在漏洞描述知识图谱数据集上平均提升率为9.42%,最大提升率15.51%,展现了优异的泛化能力与领域适应性.

关键词: 漏洞知识图谱;知识图谱补全;知识表示学习;双模态感知;对比学习;攻击链预测

基金项目: 国家自然科学基金(No.62207011,No.62407013);湖北省自然科学基金(No.2025AFB653);湖北省重大科技专项项目(No.2024BAA008)

中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112(2025)10-3579-14

电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20250485

Vulnerability Knowledge Graph Construction and Completion with Dual-Modality Perception

ZHANG Yan[1,2,3,4,5], LUO Xiang-yu[2], QIN Zi-yue[1], ZHANG Miao[1,3,4], LI Zhi-fei[1,2,3,4,5*]

(1. *School of Computer Science*, *Hubei University*, *Wuhan*, *Hubei* 430062, *China*;
2. *School of Cyber Science and Technology*, *Hubei University*, *Wuhan*, *Hubei* 430062, *China*;
3. *Hubei Key Laboratory of Big Data Intelligent Analysis and Application*, *Wuhan*, *Hubei* 430062, *China*;
4. *Key Laboratory of Intelligent Sensing System and Security*, *Ministry of Education*, *Wuhan*, *Hubei* 430062, *China*;
5. *Hubei Engineering Research Center of Cyber Security for Intelligent Connected Vehicles*, *Wuhan*, *Hubei* 430062, *China*)

Abstract: As a critical tool for cybersecurity knowledge modeling, vulnerability knowledge graphs play an increasingly important role in key tasks such as vulnerability analysis, threat modeling, security situational awareness and attack chain tracking. Unlike universal knowledge graphs, which cover a wide range of domains, have a long update cycle, and focus on generic knowledge and relationship modeling, vulnerability knowledge graphs are updated frequently, face the challenges of data heterogeneity, semantic ambiguity, and knowledge sparsity, and often need to incorporate unstructured descriptive information for joint modeling. However, the existing methods are still limited to the ternary formation modeling paradigm, ignoring the rich security text descriptions in the cybersecurity knowledge base, resulting in limited accuracy of vulnerability knowledge graph complementation and attack chain prediction. To address this, this paper proposes the construction of a vulnerability description knowledge graph (VKG-T), which enhances the ability to complete vulnerability and weakness information by combining structural and semantic data. Additionally, we present a dual-modality perception ag-

收稿日期:2025-06-06;录用日期:2025-10-09;责任编辑:覃怀银

*通讯作者:李志飞

gregated model for vulnerability description knowledge graph completion (VKGC-ST). This model integrates graph attention networks (GAT) with pre-trained language models, considering both the structural adjacency features of entities and their textual descriptions, and employs multi-level negative sampling and contrastive learning mechanisms to improve semantic discrimination and structural correlation modeling. Through link prediction experiments on vulnerability knowledge graph VKG-T and general datasets FB15K-237, WN18RR, VKGC-ST achieves the best performance across all metrics, specifically, on the vulnerability description knowledge graph dataset, the average improvement rate is 9.42%, with a maximum improvement rate of 15.51%, showcasing excellent generalization ability and domain adaptability.

Key words: vulnerability knowledge graphs; knowledge graph completion; knowledge representation learning; dual-modality perception; contrastive learning; attack chain prediction

Foundation Item(s): National Natural Science Foundation of China (No. 62207011, No. 62407013); Natural Science Foundation of Hubei Province (No.2025AFB653); Major Science and Technology Project of Hubei Province (No.2024BAA008)

1 引言

知识图谱作为一种用于表示和存储结构化与半结构数据的图形化模型,自2012年由谷歌提出以来已经得到了高度的发展,至今已形成了诸多不同语言和行业的知识图谱项目,被广泛应用于智能问答[1]、推荐系统等领域[2]. 知识图谱由实体和表示它们之间关系的边构成,每个实体和关系都具有各自的属性,知识图谱将现实世界中的各种知识转换为形如头实体、关系、尾实体的三元组进行存储,对海量数据进行组织和管理,拥有强大的表示与推理能力[3].

在网络安全领域,随着攻击技术不断演进、威胁形式日趋多样,传统单一的数据分析方式已经难以胜任复杂环境下的威胁检测与态势感知需求. 在此背景下,网络安全漏洞知识图谱应运而生,成为支撑智能化安全防护体系建设的重要手段之一[4]. 网络安全漏洞知识图谱以通用漏洞披露(Common Vulnerabilities and Exposures, CVE)、通用弱点枚举(Common Weakness Enumeration, CWE)、通用攻击模式枚举和分类(Common Attack Pattern Enumeration and Classification, CAPEC)、对抗性战术技术与常见知识库(Adversarial Tactics, Techniques, and Common Knowledge, ATT&CK)等标准化安全知识体系为基础,整合漏洞信息、攻击技术、受影响资产、补丁措施等多源异构数据,通过构建实体与实体间多维关系,实现对网络攻击链条、漏洞利用路径及潜在风险态势的全面建模和动态更新. 借助图谱强大的关联推理能力,安全运维人员不仅可以快速识别潜在威胁,分析攻击行为背后的逻辑关系,还能提前预判漏洞被利用的可能路径,从而制定更为精准的防御策略. 同时,随着自然语言处理、图神经网络等人工智能技术的融合应用,漏洞知识图谱在自动化威胁情报挖掘、零日漏洞发现、态势感知等方面展现出巨大潜力,为新时代的网络安全防护体系提供了强有力的技术支撑.

尽管漏洞知识图谱在网络安全威胁建模与智能防御中展现出重要价值,但实际应用中普遍存在知识不完整的问题. 一方面,受限于数据源的异构性、信息更新的滞后性以及知识抽取过程中的误差干扰,图谱中常存在大量缺失的实体及其关系,显著影响了其在推理、预测等下游任务中的有效性. 另一方面,漏洞知识库中的文本描述蕴含着丰富的语义信息,是补全实体间潜在关系的重要线索. 然而,当前大多数研究仍以结构三元组为核心建模单位,未能充分利用文本模态信息,导致对实体语义理解不足,限制了模型的表达能力与泛化效果. 因此,如何融合结构信息与语义内容,构建更加完整和鲁棒的知识图谱,成为当前漏洞知识图谱研究亟需解决的关键问题,也由此催生了漏洞知识图谱补全这一核心任务.

与通用百科类知识图谱补全任务相比,漏洞知识图谱补全面临更为复杂的建模挑战,主要体现在以下三个方面:首先,安全实体多以编号形式存在,其语义高度依赖于伴随的非结构化文本描述,而这些描述往往包含漏洞影响范围、利用方式、攻击路径等关键信息,造成结构模态与语义模态之间存在显著信息鸿沟,难以通过单一模态进行有效建模. 其次,漏洞知识图谱中实体关系类型丰富但结构分布高度不均,不同实体来自异构安全知识库,图结构存在严重的局部稀疏性,导致依赖结构邻接的表示学习方法难以捕捉到完整语义,需要借助语义建模进行补全支持. 再次,由于安全事件更新频繁、漏洞数量庞大,图谱中长尾实体广泛存在,传统方法往往无法获得足够训练信号,易导致模型对新颖或低频实体的泛化能力不足.

为解决上述问题,本文提出一种双模态感知聚合的漏洞知识图谱补全方法. 该方法分别采用关系感知的预训练语言建模和图结构感知建模提取漏洞实体的文本信息和结构特征. 通过模态嵌入融合得到头尾实体的特征表示,同时采用双编码器的多头注意力机制进行特征学习,进一步增强了头尾实体间的交互信息表达能力,有效捕捉了实体之间的深层语义关联. 此外,为增强模型判别能力,采用对比学习与负采样策

略,使用余弦相似度对头尾实体的特征表示进行打分,并以此作为链接预测的依据,从而实现关系识别与实体匹配的高效协同建模.

本文主要贡献如下:

(1)为支持基于结构与语义信息的联合建模任务,提升对漏洞弱点信息的补全能力,提出了网络安全漏洞描述知识图谱 VKG-T. 实体构建自 CVE、CWE、CAPEC 及 ATT&CK 等开源安全知识库,同时为每个安全实体补充文本描述信息,包括漏洞描述、弱点定义、攻击技术说明等内容,从而形成了结构化图谱与非结构化语义信息的融合表示基础.

(2)提出了一种双模态感知聚合表示的漏洞描述知识图谱补全方法 VKGC-ST,通过结构文本双感知聚合增强实体表示的语义表达能力和上下文关联性,有效提升了漏洞知识图谱中缺失实体的预测准确性与鲁棒性.

(3)通过实验验证了方法的有效性. 在漏洞描述知识图谱数据集 VKG-T 上的链接预测结果表明,该方法在所有指标上达到了最优效果,对比第二优的指标平均提升率为9.42%.

2　相关工作

2.1　知识图谱补全

知识图谱补全作为知识推理的关键技术,旨在通过推理和补充现有知识图谱中的缺失知识和关系来提高知识图谱的完性和准确性,为下游应用提供有力保障. 知识图谱补全可以分为基于翻译的模型、基于图神经网络的模型、基于卷积神经网络的模型、融合多模态信息的模型和采用大语言模型的方法.

基于翻译的模型将实体和关系映射至低维度向量空间,并将关系视作从头实体到尾实体的翻译,利用实体关系嵌入来推断知识图谱中缺失的头实体或尾实体. TransE 作为基于翻译的嵌入模型的先驱,将实体和关系编码到统一的向量空间,使得头实体和关系的嵌入向量之和近似于尾实体的嵌入向量[3]. 其后继者 TransH 通过为每个关系引入一个关系特定的超平面,来减少实体对齐中的歧义[5]. 基于图神经网络的知识图谱补全模型利用图结构信息来学习更好的实体和关系表示,从而改进知识图谱的补全能力. R-GCN[6]通过不同的关系类型对实体进行更新,在聚合邻居信息时,分别考虑不同的关系权重,可以有效处理多关系图. CompGCN[7]在利用图卷积网络传播信息时,同时对实体和关系进行建模,并使用关系变换来捕捉实体和关系之间的组合模式. 这使得实体表示更加灵活,并能更好地适应复杂的关系结构. 为了更好地利用外推信息,Li 等人[8]将三种语义证据融入邻域模式中,设计了一种新颖的图神经网络模型 SE-GNN 用于学习知识图谱嵌入表示. SHGNet[9]采用分层聚合的方式捕捉实体的结构信息. 基于卷积神经网络的知识图谱补全模型利用卷积操作从三元组的嵌入表示中提取局部特征,从而更有效地学习实体和关系的交互模式. ConvE[10]通过将实体和关系的嵌入转换为矩阵,并使用 2D 卷积进行特征提取,提升了模型的表达能力和预测性能. 另一种方法 ConvKB[11]直接在三元组的向量表示上进行一维卷积,以捕捉实体和关系之间的潜在模式,改进知识图谱补全效果. InteractE[12]通过特征置换、循环卷积等操作捕捉实体和关系嵌入之间的交互. Wang 等人[13]提出的 ConvHLE 提出基于注意力的高低层级特征交互卷积,使模型关注更丰富的实体信息.

随着多媒体和多模态信息的飞速增加,越来越多的研究关注多模态知识图谱补全,其通过整合多种模态数据的上下文信息,提升模型预测缺失实体的能力. DKRL[14]和 IKRL[15]率先为知识图谱补全任务引入了多模态信息. DKRL 采用双编码机制,将文本描述与知识图谱实体结构融合,通过联合训练最小化结构嵌入与文本嵌入的差异,使其在同一空间中对齐. IKRL 将实体关联的图像信息融入知识表示通过视觉特征补充结构信息,提升对实体属性的理解. MKBE[16]将三元组及多模态数据一起嵌入到向量空间,并且能够产生知识图谱中实体缺失的多模态数据. VBKGC[17]将 Transformer 引入多模态知识图谱补全,并且创造性地采用了一种双向负采样策略. VISTA[18]是一种结合视觉和文本信息的多模态知识图谱表示学习方法,其作者在实体的视觉特征基础上进一步提出视觉表示的关系信息指导学习.

大语言模型(Large Language Models,LLMs)因其强大的语言检索和推理能力,使其在知识图谱补全任务中展现出巨大的潜力,能够通过学习自然语言语义来推断知识图谱中缺失的信息,尤其适用于处理开放域知识、长尾实体和语义模糊的场景. Zhu 等人[19]系统评估了大语言模型在知识图谱构建与推理中的表现,并提出了虚拟知识提取任务与多智能体自动构图框架 AutoKG,为知识图谱研究提供了新方向与实证依据. Zhang 等人[20]提出了一种名为 KoPA 的知识前缀适配器方法,通过结构嵌入预训练将知识图谱的结构信息引入 LLMs,从而改进其对缺失三元组的预测性能,并通过实验证明该方法能有效增强 LLMs 的知识推理能力.

2.2　网络安全知识图谱

随着网络安全威胁的日益复杂化,如何高效组织和利用海量异构安全数据成为研究热点. 知识图谱在组织多源异构数据、表达实体及其语义关系方面展现出显著优势,为网络安全领域提供了新的建模思路. 特

别是在漏洞分析、攻击链推理、威胁情报融合等场景中,构建结构化的网络安全知识图谱,已成为提高安全分析自动化程度的重要技术手段.

在网络安全实际应用中,漏洞信息往往以半结构化或非结构化数据形式分散存在.通过构建知识图谱,可将这些碎片化的信息进行结构化整合,统一实体表示与关系建模,实现对漏洞信息的标准化组织与高效检索.现有研究已探索利用多种安全资源构建网络安全知识图谱.例如,Wang等人[21]基于通用攻击模式枚举和分类以及通用弱点枚举构建了攻击行为知识图谱,通过分析两者结构提取实体与关系,实现对攻击和漏洞的查询与分析.Li等人[22]通过收集各类报告中的威胁情报,构建了用于分析攻击行为和技术的知识图谱 AttacKG.针对弱点信息缺失问题,周莎等人[23]基于CVE、CWE、CAPEC 与 ATT&CK 四大开源安全知识库构建了一个综合性的弱点安全知识图谱 VulKG,以实现跨库的知识融合与实体关系构建.该图谱共包含11 817条三元组与7 199个安全实体,具体涵盖5 121个CVE实例、926个CWE 弱点类型、544个CAPEC攻击模式、565个 ATT&CK 技术,以及43项 ATT&CK 缓解措施.在关系建模方面,VulKG定义了15类语义关联关系,如AttackOf、InstanceOf、RelatedPattern等,用以表达实体间的攻击路径、抽象从属、逻辑关联等多样的语义连接方式,全面反映了安全实体之间的复杂语义网络结构.为了实现对威胁情报的自动化通用分析,Hu等人[24]利用大语言模型从非结构化开源威胁情报中构建了威胁情报知识图谱LLM-TIKG.Yin等人[25]构建了一个紧凑的漏洞知识图谱,用于实现基于人工智能的风险评估.这些方法根据不同的任务场景构建网络安全知识图谱,为网络安全领域的研究提供了思路.

仅构建静态的知识图谱难以满足动态安全威胁建模的需求.为了提升网络安全知识图谱的完整性与推理能力,网络安全知识图谱补全成为网络安全知识图谱领域的关键研究方向.网络安全知识图谱补全旨在基于已有的实体与关系信息,挖掘潜在的图谱结构,填补缺失的安全知识,辅助漏洞发现与攻击链路预测,为安全防御提供智能化的支持.已有许多研究者针对这一任务提出了解决方法,例如,Wang等人[26]提出了一种基于嵌入模型的知识图谱补全方法,采用图注意力网络进行链接预测,补充和完善软件安全数据.Zhang等人[27]开发了一种基于图神经网络的边传播模型,通过定义边的表示以及边传播算法增强表示能力,并应用于网络威胁情报知识图谱的链接预测上.周莎等人[23]基于安全知识图谱提出了一种逆向特征的漏洞信息补全方法,通过对不同邻域特征学习以补全缺失的漏洞信息.针对现有方法处理物联网威胁情报知识图谱遇到的表示能力不足、实体采样策略不合理等问题,程子栋等人[28]提出一种确定性采样的多模态异构图神经网络,提高威胁情报知识图谱上进行链接预测的准确性.

尽管上述研究在图谱补全精度和建模能力方面取得了一定进展,但对漏洞知识图谱中非结构化文本信息的建模仍然不足,导致补全效果受限,难以捕捉安全语义中潜在的攻击关系与上下文线索.本文所提出的漏洞描述知识图谱构建与补全方法,聚焦于网络安全知识图谱中的一个关键分支,专注于漏洞实体与漏洞文本描述的深度建模,通过融合网络安全知识库的结构化关系与非结构文本,增强漏洞语义补全能力,为安全分析提供更加精准的知识支撑.

3 漏洞描述知识图谱构建

为进一步支持基于结构与语义信息的联合建模任务,提升对漏洞弱点信息的补全能力,本文在原始VulKG的基础上进行了扩展与增强,构建漏洞描述知识图谱VKG-T.具体而言,在保留原有来自CVE、CWE、CAPEC 与ATT&CK四大开源安全知识库中丰富安全实体与语义关系的基础上,引入了中国国家信息安全漏洞共享平台(China National Vulnerability Database,CNVD)与国家信息安全漏洞库(China National Vulnerability Database of information security,CNNVD)中的漏洞数据.这一扩展显著增强了图谱在漏洞层级建模与攻击路径关联建模方面的覆盖广度和表示能力,尤其提升了对中文语义资源的支持能力.在实体构建阶段,我们针对六个安全知识源,采用基于正则模板匹配与规则驱动的命名实体识别方法,自动提取漏洞编号、弱点类型、攻击技术名称等实体信息.在关系建模阶段,参考攻击链上下游逻辑与弱点-利用-缓解之间的语义联系,本文共设计了16类语义关系类型,涵盖InstanceOf、AttackOf、TargetOf等常见安全语义关系.六类网络安全实体的名称以及具体含义与功能如表1所示.此外,为进一步提升图谱在语义补全与基于语言的推理任务中的适用性,我们采用官方API接口与爬取技术获取每个实体的官方文本描述信息,包括漏洞详情、弱点定义、攻击模式说明、攻击链上下文信息以及官方缓解建议等.这些描述性文本为图谱提供了非结构化语义支持,形成了结构图与语义语料联合建模的基础.

CNVD、CNNVD与CVE都是用于记录和管理信息安全漏洞的平台,为安全研究人员、厂商和用户提供漏洞信息,以便采取相应的安全措施CNVD和CNNVD中的漏洞通常会与CVE编号进行映射,以便于国际的信息对比和共享.因此,CNVD和CNNVD可以被视为CVE的平行实体,都可以通过EquivalentTo关系连接到CVE实体.在加入CNVD、CNNVD实体信息后,VKG-T

表1　网络安全实体信息

网络安全实体	全称	具体含义
CVE	Common Vulnerabilities and Exposures	提供统一编号用于标识已知的安全漏洞，使不同工具和数据库之间可以共享信息
CWE	Common Weakness Enumeration	一个关于软件安全缺陷的分类系统，用于帮助开发人员识别和避免安全漏洞的根本原因
CAPEC	Common Attack Pattern Enumeration and Classification	描述攻击者如何利用系统弱点的标准模式，帮助威胁建模与防御策略设计
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge	提供对现实世界攻击者行为的结构化描述，包括战术(Tactics)、技术(Techniques)、过程(Procedures)，广泛用于威胁检测、红队评估、蓝队防御
CNVD	China National Vulnerability Database	中国官方漏洞库，收录国内外漏洞信息，内容包括漏洞描述、影响范围、解决建议等，部分漏洞未公开细节
CNNVD	China National Vulnerability Database of Information Security	中国信息安全测评中心运营的国家级信息安全漏洞库，致力于建立统一的信息安全漏洞收集、发布、验证、分析及应急处置体系

包含七种类型的网络安全实体：CVE、CWE、CNVD、CNNVD、CAPEC、ATT&CK-T、ATT&CK-M，上述实体类型构成了一个覆盖漏洞全生命周期的知识结构体系，从早期的漏洞发现与披露(CVE、CNVD、CNNVD)、到漏洞成因的追溯(CWE)、攻击方式的建模(CAPEC、ATT&CK-T)，再到防御响应策略的制定与实施(ATT&CK-M)，形成了一个语义链路清晰、结构组织完备的网络安全知识体系. 漏洞描述知识图谱VKG-T的网络安全实体与关系结构如图1所示. 其中，CWE、CAPEC和ATT&CK-T同名实体之间的双向箭头所代表的关系ChildOf表示实体在知识库中的层级归属和继承关系，该设计有助于实现实体结构信息的跨库对齐.

为进一步提升VKG-T在知识服务与推理任务中的语义表达能力，本文在结构建模的基础上，针对图谱中的各类安全实体进行了系统性的文本语义增强. 具体而言，本文为每一个实体节点补充了来源于其对应安全知识库的标准化描述信息，以实现结构化知识与非结构化文本语义的深度融合，增强实体表示的语义完整性与上下文可解释性. 例如，CVE实体的文本描述主要来自NVD数据库(National Vulnerability Database，NVD)中的官方说明，聚焦于漏洞的技术细节、影响范围、利用方式及受影响组件等；CAPEC实体的描述信息详尽描绘了攻击者执行该攻击模式的策略、目标、前置条件与执行步骤，有助于理解其攻击链中的定位与作用；ATT&CK-T实体的文本则来自MITRE官方框架文档，通常包括技术用途、攻击目标、行为特征以及与其他技术的协同关系. 漏洞描述知识图谱VKG-T中安全实体、实体ID及其描述的部分实例如表2所示.

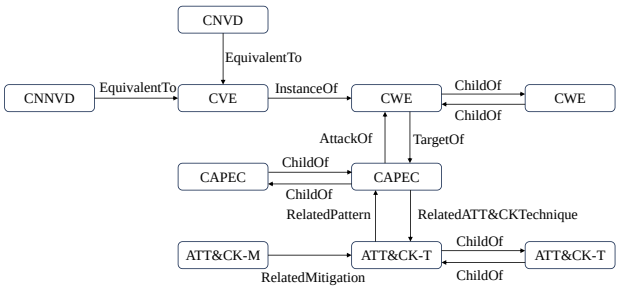

图1　VKG-T实体关系结构图

综上所述，漏洞描述知识图谱VKG-T在基于三元组的安全实体关系建模的基础上，引入多源文本信息实现结构与语义的深度融合，有效增强了漏洞知识图谱的语义表达能力. 然而，由于网络安全知识库的异构性，图谱中存在大量缺失的实体与关系. 同时，为了实现基于知识图谱的漏洞攻击链路预测和推理，本文提出基于双模态感知聚合的漏洞知识图谱补全方法VKGC-ST，进一步提升漏洞描述知识图谱的完整性和推理能力.

表2　VKG-T实体描述示例

实体编号	实体名称	实体描述
6045	CWE-269	The product does not properly assign, modify, track, or check privileges for an actor, creating an unintended sphere of control for that actor
264	CAPEC-43	An attacker supplies the target software with input data that contains sequences of special characters designed to bypass input validation logic
6954	CVE-2023-0106	Cross-site Scripting (XSS) - Stored in GitHub repository usememos/memos prior to 0.10.0

4 基于双模态感知聚合的漏洞描述知识图谱补全方法

基于双模态感知聚合表示的漏洞描述知识图谱补全方法VKGC-ST的模型架构如图2所示. VKGC-ST主要分为三个模块,结构文本信息提取、特征聚合、负采样与相似性打分. 其中,结构文本信息提取模块分别采用关系感知预训练语言建模和图结构感知建模,随后进行模态嵌入融合得到头尾实体的特征表示. 随后,在特征聚合模块采用双编码器的多头注意力机制进行特征学习,进一步增强了头尾实体间的交互信息表达能力,有效捕捉了实体之间的深层语义关联. 在负采样与相似性打分模块中,为了提升训练效率并增强模型的判别能力采用三种负样本策略,使用余弦相似度对头尾实体的特征表示进行打分.

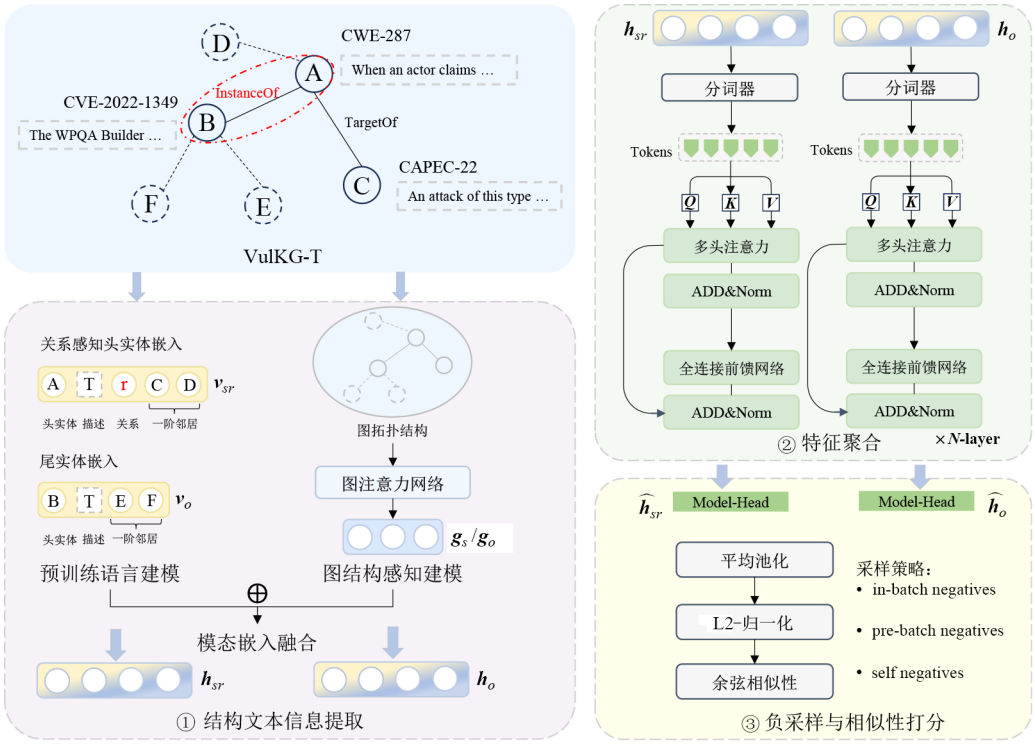

图2 VKGC-ST模型架构图

4.1 结构文本特征提取

在VKGC-ST模型中,结构文本信息提取模块作为整个知识补全流程的基础组件,承担着对图谱中实体语义和结构特征的初步建模任务. 针对网络安全漏洞知识图谱中既包含非结构化文本描述,又包含丰富的结构化图关系的双模态特征特点,该模块融合了关系感知的语言建模方法与图结构感知建模方法,以全面提取实体的多源语义信息.

在基于文本的知识图谱表示框架内有效聚合实体描述的基础上,针对关系感知的语言建模方法,提出关系感知的头实体嵌入和尾实体嵌入. 关系感知的头实体嵌入$\boldsymbol{v}_{sr}$不仅包括实体本身的信息和文本描述,还显式地引入当前关系r,以增强语义表示对三元组语境的感知能力,此外,为了充分捕捉上下文信息,将头实体的一阶邻居节点信息也集成至语言建模的输入序列中,以提供更全面的上下文语义提示. 类似的,尾实体嵌入$\boldsymbol{v}_o$包括尾实体信息、尾实体文本描述以及尾实体一阶邻居信息. 需要特别指出的是,在为头实体和尾实体引入邻居上下文时,有意识地排除了当前三元组中出现的另一个实体,反之亦然,以避免语义信息泄露造成训练偏差.

在语言建模模块构建了关系感知的文本语义表示后,VKGC-ST进一步引入图注意力网络以捕捉图谱结构中潜在的关系重要性及实体间的结构依赖. 具体而言,对于VKG-T中的每个安全实体节点的结构表示通过与邻居节点的交互建模得到,形式如下:

$$\boldsymbol{g}=\mathrm{ReLU}\left(\sum_{j\in\mathcal{N}_i}\alpha_{ij}\boldsymbol{W}_g\boldsymbol{v}_j\right) \tag{1}$$

其中,$\mathcal{N}_i$表示实体i的一阶邻居集合;$\boldsymbol{v}_j$是邻居节点j的初始表示;$\boldsymbol{W}_g$是一个可学习变换矩阵;α_{ij}是实体i和实体j之间的注意力权重,其计算公式如下:

$$\alpha_{ij}=\frac{\exp\left(\text{LeakyReLU}\left(\omega^{\mathrm{T}}\left[\boldsymbol{W}_g\boldsymbol{v}_i\|\boldsymbol{W}_g\boldsymbol{v}_j\right]\right)\right)}{\sum_{k\in\mathcal{N}_i}\exp\left(\text{LeakyReLU}\left(\omega^{\mathrm{T}}\left[\boldsymbol{W}_g\boldsymbol{v}_i\|\boldsymbol{W}_g\boldsymbol{v}_k\right]\right)\right)} \tag{2}$$

其中,ω是可学习权重;$\|$代表拼接操作. 该机制允许模型根据实体对在特定上下文中的语义兼容性,动态调整邻居的重要性,从而提升结构表示的语义适应性和判别能力. 为进一步增强模型对多种语义结构的感知能力,VKGC-ST采用多头注意力机制,分别学习不同视角下的结构特征,形成最终的头实体结构嵌入表示$\boldsymbol{g}_s$和尾实体结构嵌入表示$\boldsymbol{g}_o$.

4.2　特征聚合与学习

在完成对头实体与尾实体的关系感知语言建模与图结构感知建模后,本文设计了一种可学习的动态融合机制,通过引入一个模态融合权重参数,在语言嵌入与结构嵌入之间进行自适应加权,从而实现两种模态之间的深度融合. 具体来说,对于每个安全实体引入一个可训练参数λ以控制两种模态信息的融合比例,最终实体的统一表示形式为

$$\boldsymbol{h}_{sr}=\lambda\boldsymbol{v}_{sr}+(1-\lambda)\boldsymbol{g}_{sr} \tag{3}$$

$$\boldsymbol{h}_{o}=\lambda\boldsymbol{v}_{o}+(1-\lambda)\boldsymbol{g}_{o} \tag{4}$$

该融合权重λ在训练过程中通过反向传播机制自动学习,具备动态感知输入模态质量与内容差异的能力,从而实现个性化的模态融合策略. 相比于固定加权或简单拼接方式,该机制能更灵活地应对不同实体在语义表达和结构特征上的侧重点差异,提升模型在双模态场景下的表达能力与对齐精度.

在漏洞知识图谱补全任务中,实体通常包含复杂的上下游依赖关系、异构语义背景以及多源文本描述信息,如何从融合后的双模态表示中高效提取关键语义,构建具有上下文感知能力的紧凑实体表示,是实现高质量知识预测的关键. 为此,在获得融合后的实体统一表示之后,本文进一步引入了一个基于分词器与多头注意力机制的特征聚合模块,在保留语义多样性的同时,突出关键特征,以提升实体表示的上下文感知能力和全局判别性.

首先,我们将融合后的实体表示拆分为若干token令牌,通过可学习的分词器映射函数将其转换为更细粒度的嵌入单元,从而构建更富有结构层次的输入序列. 对于上文获得的头尾实体表示,有以下操作:

$$t_1^{sr},t_2^{sr},\cdots,t_n^{sr}=\text{tokenizer}(\boldsymbol{h}_{sr}) \tag{5}$$

$$t_1^{o},t_2^{o},\cdots,t_n^{o}=\text{tokenizer}(\boldsymbol{h}_{o}) \tag{6}$$

多头注意力机制是Transformer架构中的核心组件,旨在通过并行化的注意力计算从多个子空间中捕捉不同类型的语义关系. 与传统的单一注意力机制相比,多头注意力通过将输入嵌入分别映射为多个查询(Query)、键(Key)和值(Value)子空间,并在每个子空间上独立执行注意力操作,使模型能够在不同语义维度上关注输入序列中不同位置的信息. 本文利用多头注意力机制对token序列进行上下文建模,每一个注意力头的计算如下:

$$\text{att}(\boldsymbol{Q},\boldsymbol{K},\boldsymbol{V})=\text{softmax}\left(\boldsymbol{Q}\boldsymbol{K}^{\mathrm{T}}/\sqrt{d_K}\right)\boldsymbol{V} \tag{7}$$

其中,$\boldsymbol{Q}$、$\boldsymbol{K}$、$\boldsymbol{V}$分别表示从token序列中线性变换得到的查询、键和值. 在得到每一个注意力头的表示后,可以将整体多头注意力机制表示为

$$\text{MultiHead}(\boldsymbol{t})=\left(\text{head}_1,\text{head}_2,\cdots,\text{head}_n\right)\boldsymbol{W} \tag{8}$$

多头注意力输出后接入一个前馈神经网络(Feed Forward Network,FFN)和残差连接模块,形成标准的Transformer编码层结构:

$$\tilde{h}=\text{LayerNorm}\left(\boldsymbol{t}+\text{MultiHead}(\boldsymbol{t})\right) \tag{9}$$

$$\widehat{\boldsymbol{h}}=\text{LayerNorm}\left(\tilde{h}+\text{FFN}(\tilde{h})\right) \tag{10}$$

最终得到特征聚合后的头实体关系表示$\widehat{\boldsymbol{h}_{sr}}$和尾实体表示$\widehat{\boldsymbol{h}_{o}}$. 分别用于捕捉三元组中头实体与关系的联合语义特征,以及尾实体的上下文感知表示. 在具体建模过程中,将融合后的实体嵌入转化为token序列,不仅提升了表示的语义层次表达能力,还通过序列化过程引入了隐式的语义位置顺序,有助于学习实体与其上下文之间的依赖关系. 此外,多头注意力机制在多个子空间中并行计算语义相关性,能够从多个维度对token序列进行上下文编码,有效捕捉知识图谱中固有的语义与结构空间信息.

4.3　负采样与相似性打分

为了有效进行网络安全漏洞知识图谱的补全任务,需要在给定头实体s和关系r的情况下预测缺失的尾实体o. 为实现这一目标,通常需要制定一个评分函数$f(s,r,o)$用于衡量三元组(s,r,o)的合理性. 函数应能够对候选尾实体集合中的每一个实体进行打分,分数越高表示该实体越有可能与头实体s和关系r构成一个真实的知识图谱三元组. 最终,模型根据评分结果对所有候选实体进行排序,选取得分最高者作为预测结果.

对上一小节特征聚合与学习后的头实体向量和尾实体向量,首先进行平均池化操作和L2归一化操作,得到处理后的向量如下:

$$\boldsymbol{e}_{sr}=\text{L2Norm}\left(\text{pooling}(\widehat{\boldsymbol{h}_{sr}})\right) \tag{11}$$

$$\boldsymbol{e}_{o}=\text{L2Norm}\left(\text{pooling}(\widehat{\boldsymbol{h}_{o}})\right) \tag{12}$$

本文采用余弦相似度结合欧氏距离的评分函数,以同时捕捉实体表示间的方向一致性与空间距离差异,增强评分机制的判别性与鲁棒性. 具体而言,余弦相似度评分如下:

$$f(s,r,o)=\cos(\boldsymbol{e}_{sr},\boldsymbol{e}_o)=\boldsymbol{e}_{sr}\cdot\boldsymbol{e}_o/\|\boldsymbol{e}_{sr}\|\|\boldsymbol{e}_o\| \quad (13)$$

对于尾实体预测$(s,r,?)$,需要计算$\boldsymbol{e}_{sr}$与实体集$\mathcal{E}$中所有候选实体之间的余弦相似性,并预测分数最大的余弦相似性:

$$\operatorname{argmax}\cos(\boldsymbol{e}_{sr},\boldsymbol{e}_{o_i}),\quad o_i\in\mathcal{E} \quad (14)$$

为有效训练模型并提升其在尾实体预测任务中的判别能力,本文采用了多层次的负采样策略,在构建训练样本时引入多样化的负样本以增强模型对错误三元组的识别能力. 具体而言,在每个训练步骤中引入了三类负样本构造机制:预批次负样本、批次内负样本与自负样本. 其中,预批次负样本通过从最近2个训练批次中额外采用历史出现的尾实体构成,当批次大小为N时,每个样本获得$2\times N$个预批次负样本,并通过预批次权重控制其损失权重. 预批次负样本有效扩大了负样本多样性,避免模型陷入局部最优或对批次分布的过拟合. 批次内负样本基于当前批次通过双向对比自动生成,每个样本获得$(N-1)\times 2$个负样本,实现负样本的共享重用. 当添加自负样本策略时,每个样本利用当前自身三元组中的头实体或尾实体,通过扰动关系或替换实体构造伪负样本. 最终,采用具有加性裕度的InfoNCE损失作为整体损失函数:

$$\begin{aligned}\mathcal{L}&=\text{InfoNCE}(f(s,r,o),\theta,\sigma)\\&=-\ln\frac{\boldsymbol{e}^{(f(s,r,o)-\theta)/\sigma}}{\boldsymbol{e}^{(f(s,r,o)-\theta)/\sigma}+\sum_{i=1}^{|N|}\boldsymbol{e}^{(f(s,r,o_i')-\theta)/\sigma}}\end{aligned} \quad (15)$$

其中,加性裕度θ允许模型在预测中增加正确三元组(s,r,o)的比例,温度参数σ调节负样本的相对显著性,较低的温度值可以增加硬负样本的显著值,为避免过拟合,这里将温度参数设置为可学习的参数.

5 实验结果与分析

5.1 实验数据集

为了进行全面的实验,本文选取两方面的知识图谱数据集进行实验:公开的通用百科知识图谱数据集FB15K-237[29]和WN18RR[10]以及漏洞描述知识图谱数据集VKG-T. FB15K-237来源于知识库Freebase,该数据集中包含了来自多个领域的现实世界知识,实体类型和关系类型丰富,现在已经成为知识图谱补全领域最广泛应用的公开数据集之一. WN18RR源自语言知识库WordNet,主要应用于研究词汇级别的知识图谱推理任务. VKG-T数据集则基于六个主流网络安全知识库构建,在基于三元组的安全实体关系建模的基础上,引入多源文本信息实现结构与语义的深度融合. 为统一训练评估流程,本文将VKG-T数据集划分为约85%的数据作为训练集,5%作为验证集,剩下的10%作为测试集. 三个数据集的统计信息如表3所示.

表3 知识图谱补全数据集统计信息

数据集	实体	关系	三元组			
			训练集	验证集	测试集	合计
FB15K237	14 541	237	272 115	17 535	20 466	310 116
WN18RR	40 943	11	86 835	3 034	3 134	93 003
VKG-T	7 283	16	10 063	641	1 200	11 904

5.2 实验设置

本研究所提出的模型基于PyTorch框架实现,并在训练过程中对多个关键超参数进行了细致调优,以保障模型训练的稳定性与最终性能的最优化. 在模型训练阶段,为与baseline的设置保持一致,将批大小设置为1 024,这也对应了每轮训练中采样的负样本数量,有效提升了训练效率并增强了对负样本分布的建模能力.

为抑制过拟合风险,模型训练中引入了丢弃机制,参考图注意力网络和Transformer中防止过拟合的常规配置,我们将Dropout概率设置为0.1,用于在Transformer编码层及融合模块中进行激活单元的随机失活. 此外,在对比学习过程中,模型采用了基于InfoNCE的损失函数,对实体语义表示进行约束,其中温度系数初始设为0.05,用于调节对比分布的平滑程度. 加性裕度用于增强模型在对比学习中正负样本的区分边界,本文引入该参数以扩大正负样本嵌入间的判别间隔,提升语义判别力. 我们在0.1~0.4范围内进行调参,0.2在三个数据集上取得均衡表现.

所有实验均在配备Intel Xeon Gold 6430 CP与NVIDIA RTX 4090 GPU的高性能计算平台上进行,确保大规模训练过程中的计算效率与资源支持.

5.3 评价指标

为了评估模型的性能,本文选取了知识图谱补全任务中常用的三个评价指标:平均排名MR(Mean Rank)、平均倒数排名MRR(Mean Reciprocal Rank)以及前k命中率Hit@k. MR是指在链接预测任务中,正确结果所处的排名位置的平均值,MR越小表示正确结果在所有预测实体中的排名越高,其计算公式为

$$\text{MR}=\frac{1}{2|\mathcal{T}_{\text{TEST}}|}\sum_{i\in\mathcal{T}_{\text{TEST}}}\left(\text{rank}_i^h+\text{rank}_i^t\right) \quad (16)$$

其中,$\mathcal{T}_{\text{TEST}}$表示测试集三元组;$\text{rank}_i^h$和$\text{rank}_i^t$分别表示正确的头尾实体在所有预测实体中的排名. MRR是指将每个测试样本中正确结果的排名位置取倒数,然后取平均值,MRR值越大表示实验效果越好,其计算公式为

$$\text{MRR}=\frac{1}{2|\mathcal{T}_{\text{TEST}}|}\sum_{i\in\mathcal{T}_{\text{TEST}}}\left(\frac{1}{\text{rank}_i^h}+\frac{1}{\text{rank}_i^t}\right) \quad (17)$$

前k命中率Hit@k是指在所有预测中,模型返回的前k个候选结果中包含正确结果的占比,其值越大表示模型效果越好,计算公式如下:

$$\text{Hit@k}=\frac{1}{2|\mathcal{T}_{\text{TEST}}|}\sum_{i\in\mathcal{T}_{\text{TEST}}} I\left[\text{rank}_i^h\leqslant k\right]+I\left[\text{rank}_i^t\leqslant k\right] \quad (18)$$

其中,$I[\cdot]$表示指示函数,其结果为真实值为1,反之为0.

5.4　基线方法

为了验证本文所提出的基于结构-文本聚合表示的知识图谱补全方法的有效性和先进性,选取了一系列知识图谱补全方法作为基线方法进行实验对比,这些方法包括:基于平移距离的模型TransE、RotatE、PairRE,这类模型将关系量化为头尾实体在向量空间的位移进行建模;语义匹配的模型DistMult、ComplEx、TruckER,这类模型采用基于相似度的评分函数来计算三元组的匹配程度;基于卷积神经网络的模型包括ConvE、InteractE、ConvHLE,通过卷积来提取深层次语义特征;基于图神经网络的模型R-GCN、W-GCN、CompGCN、SE-GNN、SHGNet,通过消息传递的方式来捕捉图的结构信息.

5.5　基准实验结果分析

表4展示了在网络安全漏洞知识图谱VKG-T上进行链接预测任务的实验结果.表5和表6分别展示了在FB15K237以及WN18RR上进行基准实验的结果.

表4　漏洞描述知识图谱VKG-T上链接预测实验结果

模型	MRR(↑)	MR(↓)	Hit(↑)		
			@1	@3	@10
TransE	0.112	2 143	0.046	0.171	0.209
TransH	0.216	1 680	0.199	0.274	0.393
TuckER	0.381	2071.1	0.344	0.405	0.451
AdaProp	0.478	1 077.2	0.422	0.510	0.572
SimKGC	0.509	34.154	0.404	0.556	0.722
VKGC-ST	**0.551**	**28.858**	**0.430**	**0.629**	**0.782**
提升率	8.25%	15.51%	1.90%	13.12%	8.32%

注:各指标的最优结果用加粗表示,第二优结果添加下划线表示.

表5　FB15K237上基准实验结果

模型		MRR(↑)	MR(↓)	Hit(↑)		
				@1	@3	@10
基于平移距离的模型	TransE	0.294	357	—	—	0.465
	RotatE	0.338	177	0.241	0.375	0.533
	PairRE	0.351	160	0.256	0.387	0.544
基于语义匹配的模型	DistMult	0.241	254	0.155	0.263	0.419
	ComplEx	0.247	339	0.158	0.275	0.428
	TuckER	0.358	—	0.266	0.394	0.544
基于卷积神经网络的模型	ConvE	0.325	244	0.237	0.356	0.501
	InteractE	0.354	172	0.263	—	0.535
	ConvHLE	0.360	—	0.268	0.395	0.544
基于图神经网络的模型	R-GCN	0.248	—	0.151	—	0.417
	W-GCN	0.350	—	0.260	0.390	0.540
	CompGCN	0.355	197	0.264	0.390	0.535
	SHGNet	0.355	—	0.268	0.395	0.544
	SE-GNN	0.365	157	0.271	0.399	0.549
VKGC-ST		**0.383**	**112**	**0.295**	**0.414**	**0.563**
提升率		4.93%	28.66%	8.86%	3.76%	2.55%

注:各指标的最优结果用加粗表示,第二优结果添加下划线表示.

根据实验结果可以得知,本文所提出的基于结构-文本聚合表示的知识图谱补全模型VKGC-ST在所有评价指标上均达到了最优效果.相比于第二优的指标,VKGC-ST的平均提升率为9.42%,其中最大提升15.41%.该结果充分验证了VKGC-ST模型中"结构-文本双感知聚合机制"的有效性.通过引入关系感知语言建模和图结构感知建模,模型能够从多个语义与结构层次精准捕捉漏洞实体间的潜在关联,有效缓解传统方法中因模态割裂或结构稀疏带来的表示能力不足问题.同时,VKGC-ST在应对网络安全图谱中常见的实体信息缺失、描述异质性强、结构异构复杂等挑战时,表现出更强的鲁棒性与泛化能力.

根据表5和表6的结果显示,本文提出的VKGC-ST模型在通用数据集的所有指标上均达到了最高性能,取得了SOTA的效果.其中,在FB15K237数据集上MR指标取得了最高提升率,达到了28.66%,表明VKGC-ST

表6 WN18RR上基准实验结果

模型		MRR(↑)	MR(↓)	Hit(↑)		
				@1	@3	@10
基于平移距离的模型	TransE	0.226	3 384	—	—	0.501
	RotatE	0.476	3 340	0.428	0.492	0.571
基于语义匹配的模型	DistMult	0.430	5 110	0.390	0.440	0.490
	ComplEx	0.440	5 261	0.410	0.460	0.510
	TuckER	0.470	—	0.443	0.482	0.526
基于卷积神经网络的模型	ConvE	0.430	4 187	0.400	0.440	0.520
	InteractE	0.463	5 202	0.430	—	0.528
	ConvHLE	0.469	—	0.437	0.482	0.532
基于图神经网络的模型	W-GCN	0.470	—	0.430	0.418	0.540
	CompGCN	0.479	3 533	0.443	0.494	0.546
	SHGNet	0.476	—	<u>0.448</u>	0.496	0.549
	SE-GNN	<u>0.484</u>	<u>3 211</u>	0.446	<u>0.509</u>	<u>0.572</u>
VKGC-ST		**0.519**	**2 827**	**0.498**	**0.531**	**0.637**
提升率		7.23%	11.94%	11.16%	4.32%	11.37%

注:各指标的最优结果用加粗表示,第二优结果添加下划线表示.

在剔除高排名误差和长尾实体预测方面具有较强能力. 整体来看,在FB15K-237上的平均指标提升率达到了9.75%,展现出优秀的全局预测性能. 在WN18RR数据集上,VKGC-ST同样在所有指标上实现领先,其中最高提升率为11.94%,平均提升率为9.2%,进一步印证了本模型在语言类知识图谱中的适用性,尤其在处理抽象概念、语义关系稠密的场景下具备较强的表示能力与泛化效果.

综合两个数据集的实验结果可得,VKGC-ST在整体表现上稳定优于所有基准方法,其中在FB15K-237数据集上的优势尤为显著. 这一差异主要得益于VKGC-ST模型在面对关系多样、实体分布不均且结构复杂的图谱时,所具备的结构感知建模与语义融合能力,尤其是其对实体上下文信息的深层抽取与关系语义引导建模机制,使其在具挑战性的实体预测任务中展现出更强的表现力. 这一实验结果不仅进一步确认了VKGC-ST所提出的结构-文本聚合表示策略的有效性,也从横向对比角度强调了其在网络安全漏洞知识图谱实际应用中具有较强的适应能力与推广潜力.

5.6 消融实验结果分析

为了进一步验证模型中关键组件对VKGC-ST链接预测性能的影响,本文设计了三种模型的变体:w/o RS表示去除关系感知的语言建模的变体模型;w/o GS表示去除图结构感知建模的变体模型;w/o FA表示去除特征聚合模块的变体模型. 表7展示了在FB15K237数据集下进行关键组件消融的实验结果.

根据消融结果可以发现,当去除模型中某一关键组件时,模型的性能均会出现不同程度的下降. 具体来看,当关系感知的语言建模模块被移除时,模型退化为一个仅基于图结构进行建模的静态知识图谱补全模型,即不再考虑实体的文本语义描述信息. 该变体在所有评价指标上均出现明显性能下滑,表明在实体表示中加入自然语言描述能够为模型提供更丰富的语义特征,有效缓解实体之间语义重叠或结构稀疏所带来的判别困难. 这一结果进一步证明,在网络安全领域中,实体如漏洞、攻击技术、弱点类型等往往携带高度结构化的命名或编号信息,仅依赖图结构难以全面表达其潜在语义,而引入文本建模能够显著提升实体之间的可区分性与语义一致性.

表7 VKGC-ST关键组件消融实验结果

模型	FB15K237				
	MRR	MR	Hit@1	Hit@3	Hit@10
w/o RS	0.337	167	0.272	0.398	0.551
w/o GS	0.325	188	0.261	0.394	0.542
w/o FA	0.334	164	0.269	0.400	0.553
VKGC-ST	**0.383**	**112**	**0.295**	**0.414**	**0.563**

注:各指标的最优结果用加粗表示.

当去除图结构感知模块时,模型失去了对实体上下文结构信息的建模能力,仅依赖文本内容进行补全判断. 这种设置下的性能下降也进一步验证了结构信息在捕捉实体间深层语义关系、建模三元组潜在规则中的不可替代作用,尤其在缺乏完整文本描述的实体或结构化攻击链场景中,结构感知提供了重要的补充支持.

此外,针对本文设计的对比学习负采样策略,进一步设计消融实验验证其有效性. 我们设计了三种负采

样策略的变体:(1)w/o PB代表去除预批次负样本的模型变体;(2)w/o SN表示去除自负样本的变体;(3)w/o PB+SN表示去除预批次负样本和自负样本策略的模型变体. 我们分别在漏洞描述知识图谱VKG-T和通用知识图谱FB15K237和WN18RR上进行消融实验,并将实验结果如图3所示.

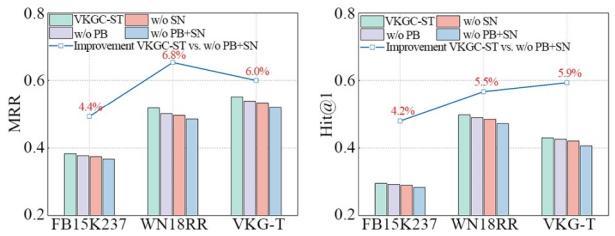

图3　负采样消融实验对比图

从结果中可以看出,完整模型VKGC-ST在所有数据集上的指标均取得最佳性能,这一结果验证了多样化负采样策略的有效性. 去除预批次负样本或自负样本后,模型性能均出现下降,说明这两类负样本对于提高模型对困难样本的识别能力具有关键作用. 当同时移除预批次负样本和自负样本时,模型出现更大幅度的下降,其中在VKG-T数据集上MRR指标下降了6.0%,Hit@1降低了5.9%,表明缺乏历史干扰样本和语义对抗样本将显著降低模型的学习广度与鲁棒性. 消融实验的结果充分验证了本文提出的多层次负采样机制在训练过程中提供了语义丰富性、难度层次性与时间维度多样性的支持,三者协同提升了模型对复杂实体关系与长尾样本的泛化能力,是VKGC-ST达成SOTA性能的核心训练策略之一.

5.7　漏洞知识图谱分析

为了分析我们提出的漏洞描述知识图谱VKG-T与当前主流网络安全知识图谱的特点,我们在表8中进行了系统的对比,涵盖数据来源、应用场景及模态信息等方面. 从数据来源来看,VKG-T整合了CAPEC、ATT&CK等多类权威网络安全知识库,数据覆盖范围更广,既包含漏洞信息,也涵盖攻击行为描述. 在模态信息方面,VKG-T不仅支持结构化数据建模,还引入了文本语义,实现了结构与文本的联合表达,突破了传统知识图谱仅限结构化信息的局限. 应用场景上,VKG-T能够支撑漏洞结构语义联合建模、漏洞归因分析等多种实际需求,展现出更强的知识表达力和应用灵活性.

表8　主流网络安全知识图谱对比

知识图谱名称	数据来源	应用场景	模态信息
AttacKG	CTI报告、ATT&CK	攻击行为分析	结构
VulKG	CWE、CVE、CAPEC、ATT&CK	弱点安全与缓解	结构
LLM-TIKG	开源威胁情报报告	攻击归因和行为分析	结构
Cyber-Attack Behavior Knowledge Graph	CWE、CAPEC	攻击预测与缓解	结构
Vulnerability KG	NVD、CVE、CWE、EDB	软件漏洞风险评估	结构
VKG-T	CVE、CWE、CNVD、CNNVD、CAPEC、ATT&CK	漏洞结构语义联合建模	结构+文本

为了更直观地展示漏洞描述知识图谱VKG-T的结构特征与语义关联,我们采用图数据库平台Neo4j对其进行了可视化分析. 在具体实现过程中,我们将VKG-T的部分知识图谱三元组数据按照CSV格式(Comma-Separated Values,CSV)整理,并通过数据处理脚本进行解析将其批量导入图数据库中. 随后,通过Cypher查询语言对节点类型及边的语义进行显式建模与关联定义,得到VKG-T的可视化展示如图4所示. 得益于Neo4j强大的图数据建模与可视化能力,VKG-T中所融合的多源异构网络安全数据通过图结构的形式进行清晰呈现. 通过可视化操作,我们不仅能够观察到不同安全实体之间复杂的语义关联和交叉指向关系,还进一步验证了VKG-T在知识融合深度与结构表达完整性方面的优势.

同时,在可视化分析过程中,我们验证了VKG-T中安全实体的漏洞生命周期链路完整性与语义连贯性,基于Neo4j图数据库进行了从成因、攻击方式到缓解措施的全流程语义路径查询结果如图5所示.

在该路径中,CVE-2022-24610("密码存储不安全"漏洞)实体首先通过InstanceOf关系关联到CWE-522("不安全的密码存储")实体,明确指出该漏洞的根本成因属于CWE-522定义的范畴. 随后,CWE-522通过TargetOf关系连接至CAPEC-551("针对弱密码存储的攻击"),表明该漏洞容易成为此类攻击方式的目标. 接着,CAPEC-551进一步通过RelatedATT&CKTechnique关系关联到ATT&CK攻击技术T1543.003("创建或修改系统进程:Windows服务"),具体描述了攻击者可能利用该漏洞实施的攻击技术手段. 最后,T1543.003通过RelatedMitigation关系指向ATT&CK缓解措施M1040("行为准则"),为防御此类攻击提供了相应的安全策略建议. 该路径完整地覆盖了漏洞的发现、成因分析、攻击方式、技术映射、防御对策的生命周期阶段,展现了VKG-T在语义连贯性和结构组织上的优势,为安全事件建模、攻击链识别与防护策略推荐等下游任务提供了结构化支撑和链式知识依据.

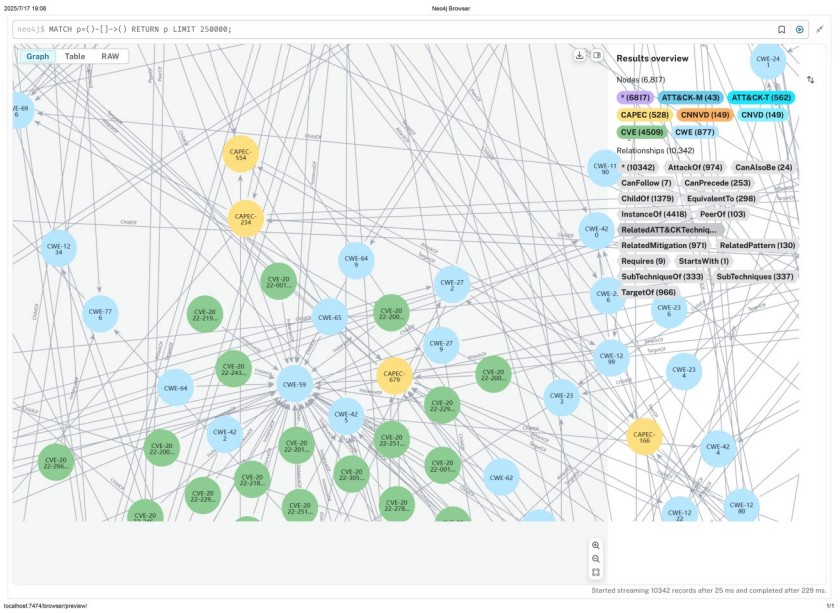

图4 VKG-T可视化展示图

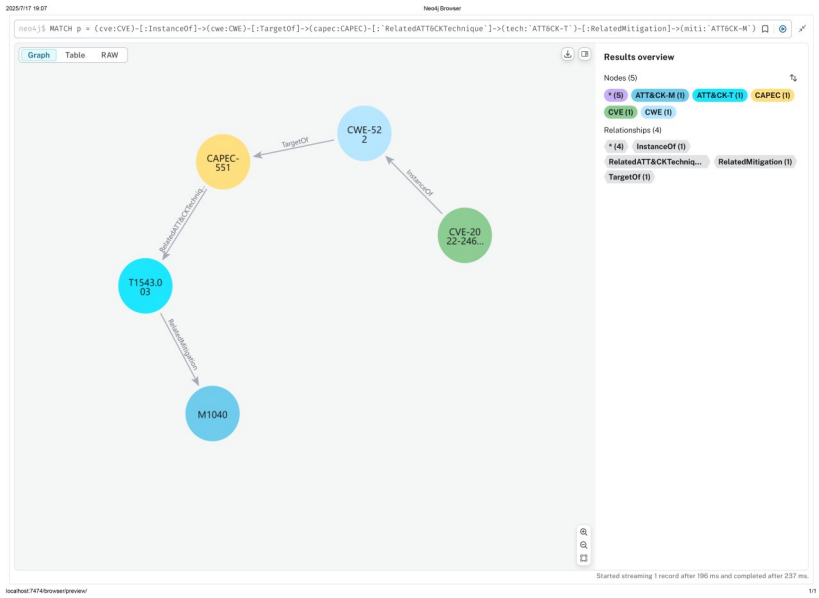

图5 VKG-T漏洞链路查询的可视化结果

6 结论

本文构建了一种漏洞描述知识图谱数据集VKG-T，通过开源网络安全知识库中的安全实体的关系建模以及描述文本的引入实现结构化图谱与非结构化语义信息的融合表示基础，增强图谱在漏洞层级与攻击路径建模方面的覆盖能力与表达深度. 在此基础上，进一步提出了一种双模态感知聚合表示的漏洞知识图谱补全方法VKGC-ST，通过关系感知预训练语言建模和图结构感知建模得到头尾实体特征表示，采用双编码器的多头注意力机制捕捉实体深层次语义关联，最终实现漏洞知识图谱的补全任务. 实验结果表明该方法在网络安全图谱补全任务中显著优于现有主流模型，并在通用知识图谱数据集上同样展现出强泛化性能，体现出广泛的适用性与实用价值.

当前研究以结构和文本为主要模态，尚未系统考虑视觉、代码、网络流日志等多源安全情报的异构性与潜在互补性. 后续工作可尝试构建多源多模态安全知识图谱，结合图像识别、代码语义分析、日志序列建模等技术，构建统一的信息融合框架，提升模型对复杂威胁情境的建模与应对能力.

参考文献

[1] DING Y, YU J, LIU B, et al. MuKEA: Multimodal knowl-

edge extraction and accumulation for knowledge-based visual question answering[C]//2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition. Piscataway: IEEE, 2022: 5079-5088.

[2] SUN R, CAO X Z, ZHAO Y, et al. Multi-modal knowledge graphs for recommender systems[C]//Proceedings of the 29th ACM International Conference on Information & Knowledge Management. New York: ACM, 2020: 1405-1414.

[3] BORDES A, USUNIER N, GARCIA-DURÁN A, et al. Translating embeddings for modeling multi-relational data[C]//Proceedings of the 27th International Conference on Neural Information Processing Systems. New York: ACM, 2013: 2787-2795.

[4] JIA Y, QI Y L, SHANG H J, et al. A practical approach to constructing a knowledge graph for cybersecurity[J]. Engineering, 2018, 4(1): 53-60.

[5] WANG Z, ZHANG J W, FENG J L, et al. Knowledge graph embedding by translating on hyperplanes[C]//Proceedings of the Twenty-Eighth AAAI Conference on Artificial Intelligence. New York: ACM, 2014: 1112-1119.

[6] SCHLICHTKRULL M, KIPF T N, BLOEM P, et al. Modeling relational data with graph convolutional networks[C]//Proceedings of the 18th Extended Semantic Web Conference. Cham: Springer, 2018: 593-607.

[7] VASHISHTH S, SANYAL S, NITIN V, et al. Composition-based multi-relational graph convolutional networks[EB/OL]. (2020-01-18)[2025-06-05]. https://arXiv.org/abs/1911.03082.

[8] LI R, CAO Y N, ZHU Q N, et al. How does knowledge graph embedding extrapolate to unseen data: A semantic evidence view[J]. Proceedings of the AAAI Conference on Artificial Intelligence, 2022, 36(5): 5781-5791.

[9] LI Z F, ZHANG Q, ZHU F F, et al. Knowledge graph representation learning with simplifying hierarchical feature propagation[J]. Information Processing & Management, 2023, 60(4): 103348.

[10] DETTMERS T, MINERVINI P, STENETORP P, et al. Convolutional 2D knowledge graph embeddings[EB/OL]. (2018-07-04)[2025-06-05]. https://arxiv.org/abs/1707.01476.

[11] NGUYEN D Q, NGUYEN T D, NGUYEN D Q, et al. A novel embedding model for knowledge base completion based on convolutional neural network[EB/OL]. (2018-03-13)[2025-06-05]. https://arXiv.org/abs/1712.02121.

[12] VASHISHTH S, SANYAL S, NITIN V, et al. InteractE: Improving convolution-based knowledge graph embeddings by increasing feature interactions[J]. Proceedings of the AAAI Conference on Artificial Intelligence, 2020, 34(3): 3009-3016.

[13] WANG J X, ZHANG Q, SHI F B, et al. Knowledge graph embedding model with attention-based high-low level features interaction convolutional network[J]. Information Processing & Management, 2023, 60(4): 103350.

[14] XIE R B, LIU Z Y, JIA J, et al. Representation learning of knowledge graphs with entity descriptions[C]//Proceedings of the Thirtieth AAAI Conference on Artificial Intelligence. New York: ACM, 2016: 2659-2665.

[15] XIE R B, LIU Z Y, LUAN H B, et al. Image-embodied knowledge representation learning[C]//Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence. International Joint Conferences on Artificial Intelligence Organization, 2017: 3140-3146.

[16] PEZESHKPOUR P, CHEN L Y, SINGH S. Embedding multimodal relational data for knowledge base completion[C]//Proceedings of the 2018 Conference on Empirical Methods in Natural Language Processing. Stroudsburg: ACL, 2018: 3208-3218.

[17] ZHANG Y C, ZHANG W. Knowledge graph completion with pre-trained multimodal transformer and twins negative sampling[EB/OL]. (2022-09-15)[2025-06-05]. https://arXiv.org/abs/2209.07084.

[18] LEE J, CHUNG C, LEE H, et al. VISTA: Visual-textual knowledge graph representation learning[C]//Findings of the Association for Computational Linguistics: EMNLP 2023. Stroudsburg: ACL, 2023: 7314-7328.

[19] ZHU Y Q, WANG X H, CHEN J, et al. LLMs for knowledge graph construction and reasoning: Recent capabilities and future opportunities[J]. World Wide Web, 2024, 27(5): 58.

[20] ZHANG Y C, CHEN Z, GUO L B, et al. Making large language models perform better in knowledge graph completion[C]//Proceedings of the 32nd ACM International Conference on Multimedia. New York: ACM, 2024: 233-242.

[21] WANG W L, ZHOU H C, LI K, et al. Cyber-attack behavior knowledge graph based on CAPEC and CWE towards 6G[C]//Proceedings of the 5th Mobile Internet Security. Singapore: Springer, 2022: 352-364.

[22] LI Z Y, ZENG J, CHEN Y, et al. AttacKG: Constructing technique knowledge graph from cyber threat intelligence reports[C]//Computer Security - ESORICS 2022. Cham: Springer, 2022: 589-609.

[23] 周莎, 申国伟, 郭春. 基于安全知识图谱与逆向特征的弱点信息补全[J]. 计算机工程, 2024, 50(1): 145-155.
ZHOU S, SHEN G W, GUO C. Vulnerability information completion based on security knowledge graph and reverse features[J]. Computer Engineering, 2024, 50(1): 145-155. (in Chinese)

[24] HU Y L, ZOU F T, HAN J J, et al. LLM-TIKG: Threat intelligence knowledge graph construction utilizing large language model[J]. Computers & Security, 2024, 145: 103999.

[25] YIN J, HONG W, WANG H, et al. A compact vulnerability knowledge graph for risk assessment[J]. ACM Transactions on Knowledge Discovery from Data, 2024, 18(8): 1-17.

[26] WANG Y, HOU X W, MA X, et al. A software security entity relationships prediction framework based on knowledge graph embedding using sentence-bert[C]//Proceedings of the 17th Wireless Algorithms, Systems, and Applications. Cham: Springer, 2022: 501-513.

[27] ZHANG Y, CHEN J R, CHENG Z, et al. Edge propagation for link prediction in requirement-cyber threat intelligence knowledge graph[J]. Information Sciences, 2024, 653: 119770.

[28] 程子栋, 李鹏, 朱枫. 物联网威胁情报知识图谱中潜在关系的挖掘[J]. 计算机应用, 2025, 45(1): 24-31.
CHENG Z D, LI P, ZHU F. Potential relation mining in Internet of Things threat intelligence knowledge graph[J]. Journal of Computer Applications, 2025, 45(1): 24-31. (in Chinese)

[29] TOUTANOVA K, CHEN D Q. Observed versus latent features for knowledge base and text inference[C]//Proceedings of the 3rd Workshop on Continuous Vector Space Models and Their Compositionality. Stroudsburg: ACL, 2015: 57-66.

作者简介

张 龑 男,1974年出生于湖北省宜昌市. 现为湖北大学计算机学院教授、博士生导师. 主要研究方向为代码安全.
E-mail: zhangyan@hubu.edu.cn

张 森 男,1993年出生于湖北省黄冈市. 现为湖北大学计算机学院副教授、硕士生导师. 主要研究领域为智能问答、语言模型、教育大数据、知识图谱等.
E-mail: zhangmiao@hubu.edu.cn

罗翔宇 男,2001年出生于湖北省宜昌市. 现为湖北大学网络空间安全学院硕士研究生. 主要研究方向为知识图谱、网络安全.
E-mail: xyluo@stu.hubu.edu.cn

李志飞 男,1993年出生于湖北省咸宁市. 现为湖北大学计算机学院副教授、研究生导师. 主要研究方向为知识图谱、推荐系统和智能问答.
E-mail: zhifei1993@hubu.edu.cn

秦紫玥 女,2002年出生于湖北省荆门市. 现为湖北大学计算机学院硕士研究生. 主要研究方向为知识图谱.
E-mail: 202421116012622@stu.hubu.edu.cn