计算机科学与探索
Journal of Frontiers of Computer Science and Technology
1673-9418/2024/18(02)-0279-22
doi: 10.3778/j.issn.1673-9418.2304081

工业互联网安全知识图谱构建研究综述

常　钰,王　钢+,朱　鹏,孔令飞,何京恒
内蒙古工业大学 数据科学与应用学院,呼和浩特 010000
+ 通信作者 E-mail: wg@imut.edu.cn

摘　要:工业互联网安全知识图谱能够在丰富安全概念语义关系、提高安全知识库质量和增强安全态势可视化分析能力等方面发挥重要作用,已经成为认知、溯源和防护针对新能源工业控制系统攻击的关键。但是,与通用领域知识图谱构建相比,工业互联网安全知识图谱构建的各个环节仍然存在许多问题,影响了其实际应用效果。介绍了工业互联网安全知识图谱的概念、意义和其与通用知识图谱的区别;概括了工业互联网安全知识图谱本体构建的相关工作及其作用;重点研究了在工业互联网安全背景下,构建知识图谱的三个关键环节,即命名实体识别、关系抽取和共指消解的相关工作。对于每个环节,详细报告了该环节在领域背景下的发展历史和研究现状,深入分析了该环节面临的领域特有挑战,如非连续实体识别问题、候选词提取问题和缺乏领域高质量数据集等,并针对特有挑战展望了该环节未来的研究方向,为进一步提升工业互联网安全知识图谱的质量和实用性,从而更有效地应对新兴威胁和攻击提供借鉴和启示。

关键词:工业互联网安全;知识图谱;命名实体识别;关系抽取;共指消解
文献标志码:A　　**中图分类号:**TP391

Survey of Research on Construction Method of Industry Internet Security Knowledge Graph

CHANG Yu, WANG Gang+, ZHU Peng, KONG Lingfei, HE Jingheng
School of Data Science and Application, Inner Mongolia University of Technology, Hohhot 010000, China

Abstract: The industry Internet security knowledge graph plays an important role in enriching the semantic relationships of security concepts, improving the quality of the security knowledge base, and enhancing the ability to visualize and analyze the security situation. It has become the key to recognize, trace and protect against the attacks targeting new energy industry control systems. However, compared with the construction of the general domain knowledge graph, there are still many problems in each stage of the construction of the industry Internet security knowledge graph, which affect its practical application effect. This paper introduces the concept and significance of the industry Internet security knowledge graph and its difference from the general knowledge graph, summarizes the related work and role of the ontology construction of industry Internet security knowledge graph. Under the background of industry Internet security, it focuses on the related work of the three important components of knowledge graph construction, respectively named entity recognition, relationship extraction and reference resolution. For each compo-

基金项目:内蒙古自治区高校网络安全和教育管理信息化工程研究中心专项资金(PZ2022000016);内蒙古自治区高校基本科研项目(JY20230104)。
This work was supported by the Funds of the Engineering Research Center for Network Security and Education Management Informatization of Universities of the Inner Mongolia Autonomous Region (PZ2022000016), and the Basic Scientific Research Projects of Colleges and Universities in Inner Mongolia Autonomous Region (JY20230104).
收稿日期:2023-04-25　　**修回日期:**2023-10-24

nent, it detailedly reports on the development history and research status of this component in the domain, and deeply analyses the domain challenges in this component, such as non-continuous entity recognition, candidate word extraction, the lack of domain-quality datasets and so on. It predicts the future research directions of this component, provides reference and enlightenment to further improve the quality and usefulness of industry Internet security knowledge graph, so as to deal with emerging threats and attacks more effectively.

Key words: industry Internet security; knowledge graph; named entity recognition; relation extraction; coreference resolution

新能源行业以国家政策为导向近年来保持高速增长,根据国家能源局[1]和中国光伏行业协会[2]发布的数据显示:风电、光电对全国电力供应的贡献连年提升,大量新能源基础设施将于未来几年内建成。为了确保发电基础设施自动化运行、过程控制和监控的业务流程管控,新能源工业控制系统(industry control system,ICS)大量使用大数据、云计算和物联网等信息技术,形成多种多样的智慧系统、远程控制系统,实现了底层过程控制系统和上层信息监管系统之间的互联互通,不断打破工业控制系统原有的封闭性[3]。在提高效率、促进创新的同时,也显著增加了控制系统所面临的网络安全威胁。

工控系统网络安全面临的威胁主要包含工业软件系统、操作系统、工业控制硬件、工控通信协议等方面的漏洞,攻击者通常利用这些漏洞入侵工控系统[4]。360数字安全发布的《2022年全球高级持续性威胁(APT)研究报告》[5]显示APT组织“海莲花”在2022年的攻击中开始针对MIPS(microprocessor without interlocked piped stages)和ARM(advanced RISC machine)架构,攻击我国境内IoT(Internet of things)设备作为跳板,将使大量使用IoT设备的工业控制系统、智慧城市系统等作为APT(advanced persistent threat)攻击的下一阶段目标,对涉及国计民生的重要关键基础设施构成重大威胁。

由于在APT威胁分析和溯源中涉及的信息数据杂乱[6],自成体系,难以有效组织,导致在事件分析过程中耗费大量人力,无法对相关的专家知识进行保存形成可复用的知识库。与传统知识库相比,知识图谱可以体现工业互联网安全相关知识之间的隐藏属性关联,具体总结为以下三点:

(1)深化事件理解。以“结点”表示领域中的特定实体,如APT组织名称、漏洞名称、恶意软件名称、攻击技术细节、目标资产等,以“边”表示领域中的实体间关系,如漏洞利用方式、恶意软件传播方式、数据泄露方式等,可以更加形象地理解工业互联网安全事件整体流程。

(2)提高知识库质量。知识图谱将主机异常行为、网络威胁流量、开源网络威胁情报(cyber threat intelligence,CTI)、各种漏洞数据库、恶意软件数据库等多源异构数据融合,构建具有充足语义的结构统一的更高质量的数据库。

(3)增强可视化分析。以Neo4j等图数据库为基础,构建综合性可视化页面体现安全态势状态,辅助网络安全人员决策,可以有效降低网络安全人员工作难度,大大提高威胁、风险分析效率。

因此,工业互联网安全知识图谱(industry Internet security knowledge graph,IISKG)已经成为实现网络安全认知智能的关键[7],亦是应对网络空间高级、持续、复杂威胁与风险不可或缺的技术基础。

1 工业互联网安全知识图谱概述

1998年Berners-Lee[8-9]提出语义网(semantic web)的概念,希望利用语义链接替代无语义从而将互联网信息联系成一个整体。2006年,Berners-Lee等人[10]又提出数据链接(linked data)的思想,促进了资源描述框架(resource description framework,RDF)和网络本体语言(web ontology language,OWL)的发展和完善。2012年,谷歌公司为了支撑语义搜索,提高搜索引擎的能力,借鉴语义网技术,提出了知识图谱(knowledge graph,KG)的概念。

形式上,知识图谱通常可以定义为 $G=(E,R,T)$,G 是带标记的有向图;$E=\{e_1,e_2,\cdots,e_{|E|}\}$ 是实体的集合,$|E|$ 表示实体的数量;$R=\{r_1,r_2,\cdots,r_{|R|}\}$ 是关系的集合,$|R|$ 表示关系的数量。每个知识三元组表示为 $T=\{(e,r,e')|e,e'\in E,r\in R\}$,表明头实体 e 和尾实体 e' 之间存在关系 r 这样一个事实。

迄今为止,已经有比较多的成熟知识图谱(知识库)以及相应的应用产品。表1介绍了当前主流的通用领域知识图谱和类似产品。

表1　主流知识图谱和类似产品

Table 1　Common knowledge graphs and similar products

名称	时间	依赖资源	类型
WordNet[11]	1995	专家知识	英文词汇语义知识库
FrameNet[12]	1998	专家知识	英文词汇语义知识库
HowNet[13]	2003	专家知识	中英文常识知识库
ConceptNet[14]	2016	专家知识、互联网众包、游戏	多语言常识知识库
Freebase[15]	2008	Wikipedia、领域知识、群体智能	结构化大型百科知识图谱
DBpedia[16]	2007	各语言Wikipedia、Wikidata	多领域百科知识库
YAGO[17]	2007	WordNet、Wikipedia	大型语义、百科知识图谱
Wolfram Alpha[18]	2009	Mathematica	知识计算引擎软件
NELL[19]	2018	网络公开文本	持续性文本信息抽取系统
BabelNet[20]	2012	Wikipedia、WordNet	大型语义、百科知识图谱
Wikidata[21]	2014	Freebase、Wikipedia	多语言结构化大规模百科知识图谱
Knowledge Vault[22]	2014	YAGO、Freebase、Wikipedia、网络公开数据	大规模百科知识图谱
Zhishi.me[23]	2011	中文Wikipedia、百度百科、互动百科	中文百科知识图谱
XLore[24]	2013	中文Wikipedia、百度百科、互动百科	中英文百科知识图谱
OpenKG.CN[25]	2015	Zhishi.me、XLore	中文知识图谱社区联盟项目
CN-DBpedia[26]	2017	中文Wikipedia、百度百科、互动百科	大规模中文百科知识图谱

通用领域知识图谱在信息检索领域发挥重要作用的同时，垂直领域知识图谱在电商、金融、医疗、司法领域也表现出其整合异构化知识、支撑数据挖掘分析的作用。表2介绍了各个领域的知识图谱实践案例[27]。

表2　不同领域的知识图谱应用

Table 2　Application of KGs in different fields

名称	公司(机构)	领域
VTE智能评估系统	东软集团	医疗
海洋药物大数据信息检索平台	天津大学	医疗
天眼查大数据知识图谱系统	天眼查	商业安全
渊亭金融舆情分析平台	渊亭科技	金融舆情
电力运检知识管理与认知推理系统	中国电力科学研究院	电网
电力供应链领域知识图谱系统	联想	电网
基于知识图谱的油气综合管理和智能应用	国双科技	能源
国双智讼辅助办案平台	国双科技	司法
拓尔思公安知识图谱	拓尔思	公安

工业互联网安全知识图谱与通用知识图谱的结构基本一致，两者的区别在于：

(1)应用场景不同。通用领域知识图谱侧重于在智能问答、推荐系统、搜索引擎等场景中提升用户的体验感。而IISKG侧重于在工业互联网安全领域，基于知识图谱对信息的整合能力，IISKG主要帮助网安专家完成威胁发现与态势感知等工作。

(2)实体和关系不同。通用领域知识图谱的实体种类大多为日常生活中较为常见的实体，包括人(PER)、时间(TIME)、地点(LOC)、组织(ORG)等；关系种类一般为蕴藏在自然语言语句中的语义关系，包括出生于(born in)、位于(located in)、创建(found by)等。而IISKG的实体种类主要为涉及工业互联网安全的一些概念，包括安全团队(SecTeam)、恶意组织(AptOrg)、恶意软件(MalWare)、漏洞(CVE)、网络地址(IP)、网络协议(PROT)、文件(File)、校验码(MD5)等；关系种类主要为不同工业互联网安全实体之间的关系，包括攻击(Attack)、利用(Exploit)、防御(Defense)、发送(Send)、接收(Receive)等。

(3)知识来源不同。通用领域知识图谱的知识大多从新闻语料、网络百科等公开文本中提取。而IISKG的知识从相关专业漏洞数据库和专业技术文档中提取，所以IISKG更加需要基于相关专业知识的构建技术。

工业互联网安全数据包括：工业控制系统主机行为日志、相关防火墙流量记录、不同安全厂商或政府部门收集的漏洞数据库、开源网络威胁情报等。数据主要具有以下特点：①数据比重不均衡。工业互联网安全数据常常隐藏在海量正常数据中，例如主机异常行为和威胁流量往往隐藏在大量主机日常规范行为和正常网络流量中。②数据价值密度高。工业互联网安全数据是不同安全厂商或国家安全部

门的重要资产,需要经过长时间的分析、整理和积累。③数据类型复杂。工业互联网安全数据中,各种漏洞数据库基本是标准的结构化数据,主机行为日志和流量记录一般是半结构化数据,而各种开源网络威胁情报则是风格多变的非结构化数据。

(4)知识特点不同。通用领域知识图谱通常以事实型三元组知识为主,覆盖范围较广,对知识质量要求不高;而IISKG的知识、结构一般比较复杂,需要通过本体工程规范知识结构,要求知识覆盖层次足够深入,要求知识具有较高准确度。

知识图谱的构建需要多方面技术的支持,图1显示了构建知识图谱的关键步骤。针对工业互联网安全知识图谱的特点,董聪[28]、丁兆云[29]、尚文利[30]、王晓狄[31]等人从整体层面对IISKG进行综述研究,介绍了工业互联网安全领域本体构建、信息抽取、知识融合和知识推理的研究现状;Gao等人[32]从细节层面,介绍了工业互联网领域命名实体识别任务的研究现状;Liu等人[33]将IISKG的应用划分为9个大方向,18个小方向,详细介绍了IISKG的应用研究现状。

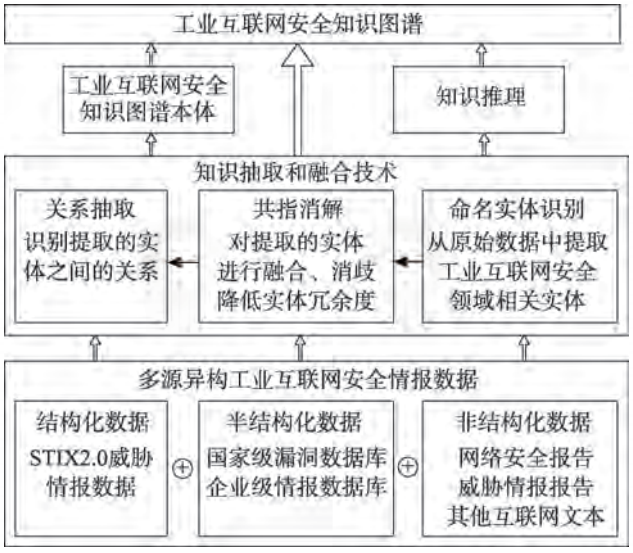

图1 工业互联网安全知识图谱构建框架

Fig.1 Construction framework of industry Internet security knowledge graph

本文与上述综述文章相比,主要对构建知识图谱涉及的命名实体识别、实体共指消解和实体关系抽取三个关键环节的相关技术进行了综述研究,在介绍工业互联网安全领域上述环节的研究现状外,还补充介绍通用领域上述环节的研究现状,为解决工业互联网安全领域背景下构建知识图谱面临的挑战提供可能的思路,具体可分为三个方面:

(1)命名实体识别(named entity recognition,NER):主要介绍工业互联网安全领域的NER方法,补充介绍针对嵌套实体和非连续实体识别问题的NER新方法,为解决工业互联网安全NER面临的挑战提供可能的思路。

(2)共指消解(coreference resolution,CR):主要介绍基于深度学习的CR方法,分析工业互联网安全CR面临的挑战和可能的解决思路。

(3)关系抽取(relation extraction,RE):主要介绍工业互联网安全领域的RE方法,补充介绍联合关系抽取新方法和基于远程监督学习的关系抽取新方法,为解决工业互联网安全RE面临的挑战提供可能的思路。

2 工业互联网知识图谱本体构建技术

工业互联网安全本体用于描述工业互联网安全领域乃至更广范围内的网络安全概念以及概念之间的关系。这些概念和关系在共享的范围内有着共同的、明确的、唯一的定义,这使得人和机器可以相互交流。

Oltramari等人[34]针对网络空间概念及其语义关系的理解挑战,在现有本体的基础上提出一种能够提高网络防御者态势感知的网络安全本体框架CRATELO。与其他领域描述框架结构相似,该框架也分为三个层次,顶层为简化版的语言与认知工程描述本体(descriptive ontology for linguistic and cognitive engineering,DOLCE-SPRAY),中层为经过扩展的安全核心本体(security core ontology,SECCO),底层为安全网络作战本体(ontologies of secure cyber operations,OSCO),一共包含223个类别和131个关系(116个类别关系和15个数据关系)。该框架致力于将错误告警众多、应对措施混乱的安全分析现状整合成一个有意义、可重复使用的知识框架,提高安全分析师的态势感知能力。

Ben-Asher等人[35]针对现有本体捕获和表示单个数据包之外的网络行为能力不足,特别是数据包流随时间变化的问题,在CRATELO的基础上扩展OSCO的数据包传输子本体(packet-centric ontology,PACO)。该子本体通过提取与网络行为、行为序列对应的网络数据包来构建网络行为特征(network behavior feature,NBF),并进一步利用多个NBF表示更复杂的网络行为。

Iannacone等人[36]针对网络安全文本数据结构、内容、命名方式不统一和不同类型实体数据集之间缺乏交叉引用的问题,提出一个集成数据资源的本

体STUCCO。该本体由13个不同格式的结构化数据来源和一些非结构化数据来源抽象而成，在威胁情报标准STIX（structured threat information expression）和CybOX（cyber observable expression）的基础上，最终生成包含15种实体类型和115种属性的本体框架，从知识图谱的角度构建了面向威胁情报数据的安全本体。

Syed等人[37]为了帮助网络安全标准从基于句法表示向基于语义表示发展，提出统一网络安全本体（unified cybersecurity ontology，UCO）。该本体将常用的多源异构网络安全系统数据和知识融合，将常用的信息共享和交换方面的网络安全标准统一，利用RDF/OWL规范描述以支持知识推理和SPARQL语言查询，提供了对网络安全领域的通用理解。除此之外，该本体还与DBpedia等通用百科知识图谱中的相关概念链接，旨在将网络安全领域知识和一般世界知识相统一。

本体框架在知识图谱构建和应用中起着关键作用：

（1）统一知识组织和语义。本体框架将工业互联网安全领域的知识进行抽象和组织，通过定义实体类别、属性类别和关系类别，提供一种统一的方式描述、储存工业互联网活动实体及其之间的关系，实现了工业互联网安全知识的语义一致性，实现了共享和交流工业互联网安全知识的基础。

（2）支持查询和推理。通过本体框架中的实体结构层次、关系和相关约束，工业互联网安全研究人员可以进行基于语义的复杂查询和推理，有助于深入理解工业互联网安全事件，发现领域实体潜在的关联和规律。

（3）细粒度知识图谱定制。由于工业互联网安全研究的进一步深入，需要针对更加细粒度的领域知识构建领域知识图谱。通过复用、修改现有的本体框架，可以快捷地对细粒度概念进行抽象、组织，确定实体类别和关系类别，快速构建细粒度知识图谱。

（4）知识扩展和填充。随着工业互联网安全威胁技术的不断发展，工业互联网安全知识图谱需要添加新的实体和关系。通过链接不同的本体框架，可以方便地对现有知识图谱进行更新、扩展和融合，以适应新的问题和需求。

3　命名实体识别

3.1　命名实体识别任务定义

命名实体识别的目标是根据领域需求预定义实体类别，再识别原始语料中的实体和所属实体类别。即给定一个单词数为 N 的句子 $S=\{w_1,w_2,\cdots,w_n\}$ 、给定一个预定义实体类别集合 $E=\{e_1,e_2,\cdots,e_k\}$ ，命名实体识别任务即确定某一子串 $\{w_a,\cdots,w_b\}\in e_i$ 。例如“我来自中国。”中的“中国”属于“国家实体”。

工业互联网安全的命名实体识别任务的主要目标是从海量网络威胁情报数据中抽取预先定义的实体信息，如APT组织名称、攻击技术、漏洞、恶意软件等安全实体，其目的是对多源异构的工业互联网安全数据进行细粒度的深度关联挖掘和分析。

3.2　命名实体识别研究现状

3.2.1　基于规则和词典的方法

基于规则的方法是通过规则模板匹配的方式完成识别任务，规则常由语言学家分析相关实体构词规律、标点符号规律、上下文用词规律等特征手工定制。基于词典的方法通过文本与词典匹配的方式完成识别任务，通常使用正向、逆向、双向最长匹配、字典树和AC自动机等各种算法进行匹配。

例如Krupka等人[38]针对文本提取系统的可定制性、可训练性、自动化提取等关键问题，提出一个英文命名实体识别系统SRA。Humphreys等人[39]提出基于人工定制的语义和句法规则的LaSIE-Ⅱ命名实体识别系统。除此之外，一些著名的基于规则的命名实体识别系统包括NetOwl[40]、Facile[41]、Fastus[42]和LTG[43]系统。

基于词典和规则的方法使用简单，无需提前对语料库进行标注，系统运行速度快，在线实时性能不会有任何瓶颈，结果准确率较高，在小规模语料库上效果较好。但是需要花费大量时间和人力建立词典和规则库，且识别不同领域实体需要定制不同的规则，移植性差。

3.2.2　基于统计的机器学习方法

基于统计的机器学习方法不需要人工定义复杂的规则，一般将命名实体识别任务看作序列标注问题或分类问题，从标注语料中提取多种特征，利用人工设计的特征向量训练机器学习模型，得到基于特征的判别模型，最后使用机器学习模型对未标注语料进行命名实体识别。

常用的基于统计的机器学习命名实体识别模型有隐马尔可夫模型（hidden Markov model，HMM），如Bikel[44]、Zhou[45]等；最大熵模型（maximum entropy model，MEM），如Borthwick[46]、Bender[47]等；支持向量机（support vector machine，SVM）模型和条件随机场（conditional random fields，CRF）模型等。

然而,网络安全NER却面临着缺乏专用数据集的问题。因此,Bridges等人[48]首先基于结构化文本(如NVD漏洞库等),利用数据库匹配、启发式规则、网络安全术语词典三种方式进行语料自动标注,构建了首个公开的网络安全领域NER任务数据集。同时提出一种基于MEM的网络安全NER方法,该方法通过MEM算法计算序列标签概率,实现从非结构化文本(如新闻文章、安全博客和推文)中自动化提取网络安全实体。

随后,针对网络安全领域实体信息难以识别的问题,研究人员根据领域特点改进相关模型,在一定程度上提高了网络安全实体的识别性能,但是OOV(out of vocabulary)问题较为严重,对于全新的安全实体,识别性能不高。

Joshi等人[49]针对网络安全领域大量关键信息保留在非结构化文本中提取困难的问题,提出一个基于CRF的信息提取框架。该框架首先从半结构化的漏洞数据库和非结构化的网络威胁情报文本中提取网络空间安全相关的实体、术语和概念。然后,使用OWL本体语言将这些概念映射并链接到Web上的相关资源;但是无法对从未出现过的网络安全概念进行很好的识别和链接。

贾焰等人[50]针对形式复杂多变的动态网络攻击难以检测、预测的问题,提出一个基于CRF的网络安全NER方法。该方法基于Stanford NER组件实现,该组件中集成了CRF序列模型,提供超过70个可用于训练模型的特征。经过对数据集的分析,该方法最终选取包括*N*-gram特征、词典特征在内的10个特征训练模型。但是不能很好识别无法通过领域词典识别的攻击后果实体和攻击手段实体。

Liao等人[51]针对从非结构化文本中自动抽取威胁指标(indicator of compromise,IOC)困难的问题,提出一种基于正则表达式和语法树相似度结合的IOC提取方法。该方法针对技术文章中的IOC通常与一组上下文术语有稳定语法关系的特点,首先利用网络安全术语频率、密度和文章长度等特征训练一个基于SVM的分类器,用于判断文本是否包含IOC信息。然后利用网络术语词典和正则表达式确定句子中潜在的IOC实体,再利用依存树解析实体之间的语法关系并提取最短依赖路径(shortest dependency path,SDP),再通过图相似计算构造特征矩阵,最后将特征矩阵输入线性分类器确定实体间关系。虽然该方法取得了很高的准确性和覆盖率,但是该方法还是无法正确理解长句子中单词之间的依赖关系,导致准确性下降;与此同时,该方法也无法处理由于拼写错误所带来的误差。

3.2.3 基于深度学习的方法

基于统计的机器学习NER模型的性能主要取决于研究人员人工设计的特征向量是否合适,而深度学习模型一般都具有较强的学习能力,无需人工设计特征向量就可以从原始语料中学习数据特征。基于深度学习的NER模型主要包括卷积神经网络(convolutional neural network,CNN)、循环神经网络(recurrent neural network,RNN)、双向长短期记忆(bidirectional long short-term memory,BiLSTM)网络和双向门控循环单元(bidirectional gated recurrent unit,BiGRU)等的多种变型和组合,例如Collobert[52]、Yao[53]、Strubell[54]、Huang[55]等。

除此之外,为了缓解网络安全NER面临的领域实体识别问题困难和OOV问题,研究人员通过不同深度学习模型提取多种特征,增强对领域实体和未知实体的理解能力。

Simran等人[56]针对网络安全命名实体识别,提出一种基于BiGRU-CNN-CRF的命名实体识别模型,并在一个公开的网络安全NER数据集上对一系列基于深度学习的NER方法进行评估。其结果显示,BiGRU-CNN-CRF模型的性能优于其他深度学习模型,且可以将该模型扩展到关系抽取任务上。

Qin等人[57]针对网络安全实体识别中存在的中英文混合、提取特征不足等问题,提出一种结合特征模板(feature template,FT)和神经网络模型的网络安全NER模型FT-CNN-BiLSTM-CRF。该模型利用特征模板提取局部上下文特征,利用神经网络模型提取字符特征和文本全局特征,虽然取得了不错的效果,但是特征提取仍然不足。

Gao等人[58]针对网络威胁情报中稀有实体和复杂实体难以识别的问题,提出一种将BiLSTM和领域词典相结合的NER方法。该方法通过构建领域词典帮助识别稀有实体,利用注意力机制和BiLSTM模型,丰富文本的局部特征,帮助识别复杂实体,虽然取得了较好的效果,特别是提高了领域稀有实体的识别效果,但也还存在领域嵌套实体、非连续实体识别等挑战。

Li等人[59]针对网络安全领域训练NER模型标注语料不足的问题,将对抗学习(adversarial learning)和主动学习(active learning)相结合,提出一种对抗式主

动学习框架，以增量的方式为待标注的语料选择有效信息样本进行进一步标注，降低训练集的标注代价。针对NLP远距离依赖问题，提出一种基于动态注意力机制的BiLSTM-LSTM模型，该模型利用动态注意力机制自适应地捕获两个标记之间的依赖关系，利用LSTM模型替换CRF作为解码模块，提高了模型的性能。

3.2.4　基于预训练模型的方法

预训练模型通过在海量语料上进行训练，能够学习到更加丰富的语言表示，更好理解上下文语义，具有较强的语言理解能力。

常见的预训练模型有以GPT（generative pre-trained transformer）[60-63]等为代表的自回归语言模型（auto-regressive language model，ARLM），以BERT（bidirectional encoder representation from transformers）[64]及其变体为代表的Mask语言模型（Mask language model，MLM），以XLNet[65]等为代表的排列语言模型（permuted language model，PLM）等。

然而，NER任务需要结合上下文信息，因此大部分NER模型使用能够更好理解上下文语义的BERT系列模型作为基础展开研究。

Jo等人[66]针对IOC作为威胁指标不能描述威胁的技术细节且时效性不足的问题，提出一种从非结构化文本中提取各种类型网络安全实体及其关系的框架Vulcan。该框架使用BERT-BiLSTM-CRF模型识别网络安全实体，利用BERT生成语义向量，利用BiLSTM提取上下文联系，进而构建关于勒索软件的知识图谱。

杨秀璋等人[67]针对APT分析报告未被有效用于构建网络安全知识图谱的问题，提出一种基于BERT-BiLSTM-Att-CRF的网络安全NER模型。该模型利用Attention机制突出关键特征，CRF输出最优标签序列，从APT分析报告中自动提取APT攻击知识，并生成常见APT组织的特征画像，为APT攻击知识图谱构建和APT攻击溯源分析提供基础。

Zhang等人[68]针对网络威胁情报中存在大量信息冗余、中英文混用、实体边界模糊和实体词语歧义等问题，提出一种网络威胁情报NER模型BERT-BiLSTM-SelfAtt-CRF。该模型利用自注意力机制（self-attention）计算词语之间的关联性，并根据关联程度赋予不同的权重，能够较好地解决远距离依赖问题。

Zhou等人[69]针对传统BERT预训练时基于子词遮蔽，导致BERT没有真正学习到单词基于上下文的语义特征的问题，提出一种基于全词遮蔽（whole word masking，WWM）的NER模型$BERT_{wwm}$-BiLSTM-CRF。该方法利用$BERT_{wwm}$提高对网络安全文本的语义学习能力，进而明显提升整个NER模型对网络安全实体的平均识别性能和细粒度实体识别性能。

谢博等人[70]针对开源网络威胁情报中网络安全实体识别困难，存在中英文混杂、缩略语等问题，提出一种基于BERT的残差空洞卷积网络（residual dilated CNN，RDCNN）的NER方法。该方法利用残差连接方式防止简单叠加卷积层产生的退化问题，虽然取得不错的效果，但是对一些稀少实体的识别效果仍然很低，需要改进文本语义嵌入表示，处理数据集不平衡等问题。

虽然预训练模型有效提升了工业互联网安全NER方法的性能，但是基于序列标注的方法无法解决嵌套实体和非连续实体的识别问题。因此，研究人员开始尝试其他的编解码方式。

苏剑林[71]针对嵌套实体和非连续实体识别问题，提出一种基于全局归一化编解码思想的NER模型。该模型通过片段提取和分类的方法直接实现Span级别的实体抽取，首先从句子中提取所有可能的片段（即句子的顺序子串），然后对每个片段进行多分类，判断其所属实体类别。该模型使用BERT提取片段的语义表示，并在BERT中采用RoPE相对位置编码方法增强位置特征信息，最后通过优化损失函数，提高嵌套实体的识别率，但是没有解决非连续实体的识别问题，模型性能还会受到Span最大长度的影响。

Yan等人[72]针对现有NER技术不能同时对扁平实体、嵌套实体和非连续实体实现较好识别的问题，提出一种基于实体Span生成思想的生成式NER模型。该模型将序列标注任务转化为序列生成任务，使用BART（bidirectional and auto-regressive transformers）预训练模型，并使用seq-to-seq的范式来进行序列生成。虽然该模型在多个数据集上实现了或接近了SOTA（state-of-the-art）的性能，但是其也存在解码效率和误差积累问题。

Li等人[73]针对NER模型中如何统一建模实体词相邻关系问题，提出一种基于词-词关系分类的统一NER模型W2NER。该模型将NER任务建模为词对关系分类任务，通过判断词与词之间的关系识别实体类别和实体边界，新设计了下邻词标签（next-neighbor-word，NNW）和尾首词-*标签（tail-head-

word-*,THW-*),并利用多粒度空洞卷积网络(multi-granularity dilated CNN,MGDCNN)细化二维词对网格表示,最后利用双仿射预测器(biaffine predictor)和多层感知机(multilayer perceptron,MLP)组成联合预测器充分推理词与词之间关系,同时提高了对嵌套实体和非连续实体的识别率。

虽然生成式模型并不适用于NER任务,但是随着GPT3[62]、GPT4[63]等超大规模模型的出现,研究人员开始探索生成式模型在NER任务上的表现。

Wang等人[74]针对NER任务和生成式模型的适配问题和幻觉问题,将NER任务转化为语言生成任务,并采用自我验证策略缓解幻觉问题。该方法首先将输入GPT模型的prompt构建成三部分:任务描述(task description),少量举例(few-shot demonstration),语句输入(input sentence)。首先要求GPT运用语言学知识,对NER任务进行描述,然后举例示范弥合NER任务和生成式模型之间的差异,降低模型生成目标文本的难度,最后将GPT的答案重新输入并询问GPT答案是否正确以缓解输入语句中不存在需求实体类型时的"幻觉"现象。

Li等人[75]针对ChatGPT和GPT4能否适用于专业领域的NER任务,在金融领域数据集上评估其性能。实验结果表明,ChatGPT和GPT4在处理特定领域的知识和术语时,局限性变得更加明显,可以通过补充相关知识,或者基于专业领域语料,重新训练GPT模型以提高模型性能。

表3对比了一些NER模型在经典数据集和领域数据集上的性能,表4对工业互联网安全领域的NER模型进行了对比。

3.3 工业互联网安全NER面临的挑战

3.3.1 嵌套实体和非连续实体识别问题

嵌套实体是指一个长实体内部嵌套一个或多个短实体,如表5的"Windows Credential Editor"整体属于"工具(TOOL)"实体,而其中的"Windows"属于操作系统(OS)实体;非连续实体是指一个实体的组成部分不是连续的,如表5"mail and USB stick worm"中的"mail stick worm"病毒(Virus)实体,其中"mail"和"stick worm"被单词隔开,属于非连续实体。

3.3.2 特殊形式实体识别问题

工业互联网安全领域中一些实体类别的表述形式和通用领域常见实体相比存在较大差异。例如:文件名/文件后缀(rundll32.exe,.dll)、文件绝对路径/相对路径(C:\Users\Default\Desktop,.\Desktop)、控制台命令(ls-a,certutil-decode)、特殊进制数/内存数据(0x7b,3c dd)等,通用领域命名实体识别方法不能准确识别这些特殊形式的实体。

3.3.3 未登录词问题

工业互联网安全领域知识的更新频率很高,不断出现的攻击技术概念、恶意软件名称、APT组织名称等都是模型在训练数据集中未曾见过的实体。因为传统词嵌入技术无法生成能够准确表示未登录词的语义特征,导致模型无法准确识别和分类这些未登录词,影响模型的准确性和鲁棒性,从而影响后续的IISKG构建和应用。

3.3.4 别名、缩写识别问题

工业互联网安全领域中存在数量众多的专业术语,由于撰写网络威胁情报的研究人员在知识背景、描述习惯等方面存在不同,同样的网络安全概念会

表3 不同NER方法在各数据集上的F1值对比

Table 3 Comparison of F1 values between different NER methods on different datasets 单位:%

论文	模型	数据集						
		MUC-7	CoNLL2003	ACE2005	OntoNotes5.0	Genia	ShARe13	CADEC
Borthwick[46]	MEM	88.80						
Bikel[44]	HMM	94.92						
Zhou[45]	HMM	94.10						
Bender[47]	MEM		89.58					
Yao[53]	CNN-CRF					71.01		
Strubell[54]	IDCNN-CRF		90.65		86.84			
Huang[55]	BiLSTM-CRF		84.74					
Wang[74]	GPT-3		90.91		82.20			
Yan[72]	BART		93.24	84.74	90.38	79.23	79.69	70.64
Li[73]	BERT-BiLSTM-MGDCNN		93.07	86.79	90.50	81.39	82.52	73.21

表4　工业互联网安全NER模型对比

Table 4　Comparison of industry Internet security NER models

阶段	论文	模型	数据来源	性能评价/%		
				精确率	召回率	F1
机器学习阶段	Joshi[49]	CRF	CVE、NVD、CWE、CPE Microsoft or Adobe security bulletins Security Blogs	83.00	76.00	80.00
	Bridges[48]	MEM	CVE、NVD、CWE Microsoft Security Bulletin Metasploit Framework	98.90	99.30	99.10
	贾焰[50]	CRF	CNVD、CVE、NVD、SCAP Security Focus、CXSECURITY Pediy BBS、Freebuf、Kafan BBS OWASP、360SRC、ASRC	85.20	80.50	82.80
	Liao[51]	SVM	IoC bucket、OpenIoC DB Security Blogs	98.00	92.00	95.00
深度学习阶段	Simran[56]	BiGRU-CNN-CRF	Bridges[48]	90.80	96.20	93.40
	Qin[57]	FT-CNN-BiLSTM-CRF	Freebuf网站、乌云漏洞数据库	88.45	83.68	86.00
	Li[59]	DyAtt-BiLSTM-LSTM	SemEval-2018 Task8 Security Communities and Blogs APT Reports	89.62	87.63	88.61
	Gao[58]	BiLSTM-Dic-Att-CRF	Bridges[48]	90.19	86.60	88.36
预训练模型阶段	Jo[66]	BERT-BiLSTM-CRF	ThreatPost、Malwarebytes、Twitter	96.80	97.70	97.20
	杨秀璋[67]	BERT-BiLSTM-Att-CRF	APT Reports form ATT&CK, FireEye, McAfee and Kaspersky	92.96	87.33	90.06
	Zhang[68]	BERT-BiLSTM-SelfAtt-CRF	CNVD、SCAP、360SRC、NIEC	92.45	94.20	93.32
	Zhou[69]	$BERT_{wwm}$-BiLSTM-CRF	Bridges[48]	97.03	96.71	96.87
	谢博[70]	BERT-RDCNN-CRF	Freebuf网站、乌云漏洞数据库、CNVD	88.72	91.07	89.88
	Wang[76]	Dic-BERT-BiLSTM-CRF	MalwareDB[77]、CVE、NISVD[78]	92.53	90.86	91.69

表5　网络威胁情报复杂实体举例

Table 5　Examples of complex entities for CTI

类型	文本	包含实体
嵌套实体	Windows Credential Editor	Windows-系统 Windows Credential Editor-工具
	mail and USB stick worm	USB-工具 USB stick worm-病毒
非连续实体	Mail Service Ports 25, 109 and 143	Ports 25-端口号 Ports 109-端口号 Ports 143-端口号
	mail and USB stick worm	mail stick worm-病毒 USB stick worm-病毒

在不同威胁情报中以各种形式的别名、缩写存在，例如“命令与控制服务器(command and control server)”有时被简写为“C2”，有时被简写为“C&C”。

当模型能够识别实体的多种表现形式时，模型会将这多种表现形式当作多个实体进行知识图谱构建，导致知识图谱中存在大量的重复和冗余结点；当模型不能识别上述多种表现形式时，构建的知识图谱则会遗漏知识。

针对上述问题与挑战，本文认为：(1)可以采用Li[73]、Wang[79]等人提出的实体标注方法和编解码方式，重新标注工业互联网安全领域数据集，使模型具有提取嵌套实体，特别是非连续实体的能力。(2)可以在原有语义特征的基础上，融合字符级别特征、词性特征和一些人工设计的特征，可以加强模型对特殊形式实体特征的学习能力，提高对特殊形式实体的识别能力，也可以提高对未登录词的识别能力。(3)可以采用以工业互联网安全相关语料为主的预训练模型，如SecBERT[80]、CySecBERT[81]等，生成具有上下文联系的语义特征向量，这样不仅能为文本生成贴近工业互联网安全领域语义的语义特征，还能为未登录词生成较为准确的语义特征，缓解未登录词的噪声影响。

4　共指消解

4.1　共指消解任务定义

给定一个单词数为 N 的句子 $S=\{w_1,w_2,\cdots,w_n\}$、预定义实体类别集合 $E=\{e_1,e_2,\cdots,e_k\}$，其中某一子串

$\{w_a,\cdots,w_b\}\in e_i$，另一子串 $\{w_a',\cdots,w_b'\}\in e_j$。共指消解任务就是确定两个子串是否表示某一实体中的相同实例。例如“中国”和“中华人民共和国”表示相同实例。

工业互联网安全领域共指消解的主要任务是对网络威胁情报文本中大量存在的别名和缩写进行辨别，简化知识图谱结构，丰富知识图谱内容。

4.2 共指消解研究现状

4.2.1 基于规则的方法

基于规则的共指消解方法，主要依靠人工设计的语言逻辑规则，完成文本中的代词消解，实施比较简单。

例如Hobbs等人[82]针对代词指代消解问题，提出一种基于句法分析树的代词CR方法。Grosz等人[83]针对局部连贯性对代词消解问题的关键作用，初步建立中心理论。Raghunathan等人[84]针对数量较多的一般特征会干扰数量稀少的关键特征的问题，提出一种基于多级筛选(multi-pass sieve)的CR方法。

然而由于语言学的复杂性和领域概念的差异性，针对某一特定领域文本中的名词消解规则无法适用于其他领域，需要重新构建消解规则，导致算法的泛化能力和可移植性较差。

4.2.2 基于统计的机器学习方法

随着机器学习算法的广泛应用，研究者们也尝试在共指消解任务中使用机器学习。总体而言，有监督的基于机器学习的CR方法可以分为4种基础模型框架[85]：表述对模型(mention pair model)，表述排序模型(mention ranking model)，实体表述模型(entity mention model)和实体排序模型(entity ranking model/cluster ranking model)，将CR问题转化为二元分类问题或排序问题，结合决策树(decision tree，DT)、朴素贝叶斯(Naive Bayes，NB)、MEM和SVM等模型处理共指消解问题。

Rahman等人[86]对比了各个模型框架的基线性能。实验结果表明，在训练数据集、机器学习模型和特征构造方式等方面基本相同的情况下，四种模型框架的性能由高到低依次为：实体排序模型>表述排序模型>实体表述模型>表述对模型。

McCallum等人[87]针对现有CR模型没有考虑多个前序表述之间的可能存在共指关系的问题，提出一种基于CRF的共指消解方法。该方法将CR问题建模为序列标注问题，输入为文本的多种特征信息，输出为单词所属的共指链(共指聚类)类别。CRF不作独立性假设，因此在一定程度上考虑表述之间依赖关系，使模型判断更为准确。

4.2.3 基于深度学习的方法

近年来，诸如Word Embedding、CNN、BiLSTM、Attention等深度学习组件在自然语言处理各个领域大放异彩，基于深度学习的方法也逐渐成为共指消解任务的研究热点[88]。基于深度学习的方法通过构建复杂的多层级神经网络模型，对数据进行多层级的抽象表示，更好地提取表述对及句子中的语义特征、语义依赖关系和语义相似性。

Wiseman等人[89]针对文本中代词共指消解困难的问题，提出一种融合全局特征的CR模型。该模型基于表述排序方法，认为所有前序表述的共指状态(全局特征)能够帮助判断当前表述是否和某一前序表述共指，因此利用LSTM模型来充分提取前序表述的共指状态特征，提高了模型对前指代词的共指消解能力。但是还存在错误解析后指代词和全局特征提取简单的问题。

Lee等人[90]针对现有CR模型需要设计语法分析器或实体检测器作为工作前提的问题，提出一种直接从原始文本提取表述并判断共指关系的端到端CR模型。该模型使用span-ranking方法(即句子子串，长度为 n 的句子有 $n(n-1)/2$ 个span)，将文本的单词特征和结构特征融合作为神经网络的输入，然后采用BiLSTM提取所有span的嵌入表示，通过计算span的表述得分判断span是否为有效表述，通过计算span对的共指得分判断span对是否共指。

Lee等人[91]又针对上述模型计算得分时只考虑一阶前序表述的问题，提出一种高阶共指消解算法，即计算当前表述是否和某一前序表述共指时，考虑前序表述已有的共指关系。为了处理由此产生的巨大计算量问题，该算法又引入了由粗到细(coarse-to-fine)的推断策略。首先通过表述得分提取前 M 个有效表述，然后通过一阶打分函数对每个表述提取前 K 个候选先行语，最后通过高阶打分函数选取最终的先行语。

随着预训练模型的出现，研究人员将其引入共指消解任务，提升共指消解模型的语义理解能力。Joshi等人[92]在Lee[91]的基础上，利用BERT模型替代ELMo(embeddings from language models)和GloVe(global vectors for word representation)生成词向量，在OntoNotes数据集上取得了良好的效果。随后，Joshi等人[93]又提出SpanBERT模型，该模型将随机遮蔽某个token修改为随机遮蔽某个连续跨度，能够更好表示和预测span，进一步提升了共指消解模型的性能。

虽然通用领域的共指消解研究已经取得了一定成就，逐渐以融合NER和CR的端到端模型为主。但是，工业互联网安全领域共指消解任务除了代词消解之外，还存在大量名词消解情况，因此工业互联网安全领域更多关注实体共指消解部分。

唐思宇等人[94]针对网络安全实体在不同厂商分析报告中可能具有不同名称的问题，提出一种基于相似性函数计算的CR方法。该方法将编辑距离（edit distance，ED）相似性和Jaccard相似性算法结合衡量字符串特征，又采用经典的余弦相似度算法计算两个实体间的语义相似度，最后加权融合作为判别实体共指与否的标准。

张晗等人[95]针对网络安全领域CR任务的特殊性问题，提出一种融合领域词典和深度学习网络的CR方法。该方法首先使用语法规则提取网络安全文本中的代词和非实体名词短语、使用BiLSTM-DictAtt-CRF模型提取网络安全实体，利用词典注意力机制（dictionary attention）增强文本特征，提高实体提取准确率，然后使用最短依赖原则和机器学习方法进行共指消解。

周宁等人[96]针对实体指代的多样性和不明确性问题，提出一种结合全局推理（global reasoning）思想的基于BiLSTM模型的CR方法。该方法使用GloVe算法提取词向量、使用一维卷积提取字符特征向量、使用ELMo模型提取文本语义特征向量，然后将三种向量拼接成特征向量输入BiLSTM模型中进行实体和候选词的提取并判断其是否共指，再通过句子上下文信息和文档信息对共指链进行推理和优化，最后将推理结果加入模型中提高该方法的性能。

Li等人[97]针对现有CR模型对不同形式的共指表述往往提取相似甚至相同特征，给共指表述区分带来噪声的问题，提出一种基于上下文感知的特征注意力模型。该模型首先利用BERT提取文本语义特征，然后融合词性特征识别网络安全实体，然后将实体包含所有token的融合特征的平均值作为实体特征，利用基于窗口滑动机制的CNN网络提取所有可能的共指实体对组合的深度特征，缓解远距离依赖问题，最后使用TanH激活函数计算共指概率。

4.3　工业互联网安全CR面临的挑战

4.3.1　候选词提取问题

通用领域内的实体类型多为人名、地名等，需要消解的多为代词（he，she，this，they等），而工业互联网安全领域内的实体类型多为“APT组织”“病毒”“漏洞”“攻击”等，需要消解的除了代词之外，更多包括一些名词短语（如“damage of the virus”中的“the virus”），所以仅凭语法规则或NER均不能满足工业互联网安全文本共指消解任务的需求。

4.3.2　深入理解上下文问题

现有的共指消解模型在共指消解方面的效果并不理想，而且由于工业互联网安全领域文本的复杂性，文本内的指代信息不明确且分布稀疏，仅考虑词级别信息不能满足共指消解模型的需求，还需要进一步融合句子上下文信息、前后句信息、其他篇章信息，甚至还需要加入相关外部知识。相关外部知识包括单词词性、单词领域语义、实体类型、语法树等，可以通过添加特殊标签、特征融合、模型融合等方法将外部知识整合至CR模型中，提高共指消解模型的性能。例如“The security analyst discovered a suspicious file on one of the compromised endpoints，and they immediately quarantined it to prevent further spread.”一句中的“it”指的是“a suspicious file”还是“one of the compromised endpoints”需要结合上下文信息及前后句信息进行判断。

针对上述问题与挑战，本文认为：（1）可以基于Lee[90-91]等方法，先提取句子中所有可能的表述，再进行共指判断，避免表述提取不完整的问题。（2）可以基于Li等人[97]的方法，以语义、词性等融合特征进行实体对共指判断，提升CR模型对上下文语义信息的学习能力。

5　关系抽取

5.1　关系抽取任务定义

给定一个单词数为N的句子$S=\{w_1,w_2,\cdots,w_n\}$、预定义实体类别集合$E=\{e_1,e_2,\cdots,e_k\}$、预定义关系类别集合$R=\{r_1,r_2,\cdots,r_l\}$，其中某一实体$\{w_a,\cdots,w_b\}\in e_i$，另一实体$\{w_a',\cdots,w_b'\}\in e_j$。关系抽取任务就是确定两个实体之间存在何种关系，即抽取$<e_i,r_t,e_j>$。例如“我来自中国。”中：“中国”属于“国家实体”，“我”属于“人物实体”，“我”和“中国”之间存在一种关系。

在工业互联网安全知识图谱构建过程中，网络威胁情报经过命名实体识别处理后，得到的是孤立的实体，关系抽取任务就是发掘实体之间的联系，将实体联系起来形成庞大的拓扑信息网。

5.2　关系抽取研究现状

5.2.1　基于模板匹配的方法

基于模板匹配的关系抽取方法，主要依靠语言

学家根据语言学知识和领域语料穷举关系表达,手工编制关系模式进行匹配。

例如Appelt等人[42]提出一种基于有限状态自动机(finite state automata,FSA)的信息抽取系统FASTUS,并在此基础上利用“宏”机制[98]优化FASTUS系统的可移植性。Grishman等人[99]提出一种融合语法知识的模板匹配信息抽取系统Proteus,并对Proteus系统在场景级别的可移植性进行优化[100]。

总体而言,基于模板匹配的关系抽取方法在小规模特定领域文本上效果较好,但是要求研究人员同时在语言学和特定领域具有深入的理解和认知。除此之外,还需要平衡信息抽取系统中的模板数量,模板数量太少时抽取覆盖范围不够,而模板数量太多时,模板之间容易产生冲突,也难以适应丰富的语言表达风格。

5.2.2 基于统计的机器学习方法

基于统计的机器学习关系抽取算法将关系抽取问题建模为分类问题,根据人工设计的各项特征训练分类器,常用的机器学习模型有MEM、SVM等,例如Kambhatla[101]、Zhou[102]、Sun[103]。

Jones等人[104]针对网络安全RE任务缺乏标注数据集的问题,提出一种基于Bootstrapping的关系抽取方法。该方法在网络安全NER数据集标注方法[48]的基础上,结合关系模板评分标准和主动学习算法提高标注数据可信度,只需要输入较少数据(关系或匹配模板)就可以在小语料库上得到不错的结果。

Banko等人[105]针对预定义实体、关系本体的未登录词问题,提出无需定义本体的开放式信息抽取框架(open information extraction,OIE)和一种基于自监督学习的开放式信息抽取系统TextRunner。传统RE框架针对预定义少量的关系种类进行抽取,而OIE是一种新的提取范式,理论上能够对无限的关系种类进行抽取,该框架首先基于非词典特征训练一个通用模型学习特定语言中关系的表达形式,然后将此模型作为提取器,提取语料中可能的关系三元组。

基于统计的机器学习RE方法的最大问题在于模型性能非常依赖人工设计的特征的规模和数量[106],只有人工设计的特征适合时,才能获得较好的实体关系抽取结果。

5.2.3 基于深度学习的方法

基于深度学习的模型能够更多地获取文本各种信息,具有更强大的特征抽取能力。目前基于深度学习的关系抽取研究主要集中在设计和使用不同的网络架构来获取文本的各种特征上,通常包括流水线(pipeline)抽取模式和联合(joint)抽取模式两种方法。

(1)流水线关系抽取模式

流水线关系抽取模式将NER和RE作为两个独立的任务进行处理,RE在NER完成的基础上进行,其过程可以描述为:把进行过命名实体识别的句子和实体单词及其标签作为模型输入,输出实体对之间的关系。

Pingle等人[107]针对网络安全RE任务,提出一种基于前馈神经网络模型(feed forward neural network,FFNN)的关系抽取方法RelExt。该方法使用在Cyber-Twitter系统中训练和使用的NER模型[108]提取网络安全实体,使用在网络安全语料库上训练的Word2Vec模型对网络安全实体进行词嵌入,然后利用神经网络进行关系分类。

Wu等人[109]针对预训练模型尚未应用于RE任务的问题,提出一种利用实体信息增强BERT预训练语言模型的实体关系抽取方法R-BERT。该方法给输入BERT的句子中的实体添加标记,然后通过BERT模型提取句子整体语义信息和两个实体的语义信息,最后通过全连接网络进行关系分类。实验结果表明,对实体的特殊标记确定了两个实体的位置信息,并将其传递到BERT模型中,使得BERT模型的输入也包含了两个实体的位置信息,能够有效提高关系分类的准确性。Jo等人[66]对R-BERT进行微调,将其用于工业互联网安全RE任务,取得了不错的效果。

Sarhan等人[110]针对目前网络安全领域信息抽取需要预定义本体,增加了丢失重要知识可能性的问题,提出一种基于开放式信息抽取的网络威胁情报知识图谱构建框架(open CSKG)。该框架首先利用基于注意力机制的OIE框架从非结构化的网络威胁情报中提取与领域无关的知识三元组,然后对提取的实体进行领域实体标注,即先进行关系抽取,再进行命名实体识别。该OIE框架将单词语义特征、词性特征和句子谓语动词特征融合输入BiGRU模型中,然后通过注意力机制学习每个单词的重要性,最后通过全连接层进行知识三元组提取。

Li等人[97]针对网络安全领域中实体之间的关系需要通过多个句子来提取的问题,提出一种文档级关系抽取方法。该方法首先利用BERT模型和NLTK(natural language toolkit)提取文档的语义特征和词性特征,然后进行命名实体识别。在此基础上,再融合实体的跨度特征、实体类型特征和实体对距离特

征，最后利用LogSumExp池化替代最大池化，更精确地表示实体之间的潜在关系，实现文档级别的关系抽取。

Soares等人[111]现有RE模型泛化能力依旧有限的问题，在Harris的分布假设扩展到RE领域和上下文语义特征学习的最新发展（特别是BERT）的基础上，提出一种通用的关系抽取方法$BERT_{EM}$-MTB。该方法的核心思想是：如果两个关系包含相同的实体对，那么两个关系应该是相似的，在BERT预训练过程中加入MTB（matching the blanks）任务，提升BERT预训练模型在关系抽取方面的性能。

Wan等人[112]提出生成式模型（如GPT3）用于RE任务的两个主要缺点：（1）例句中实体对和关系与测试句中实体对和关系相关程度较低，即例句中实体对和关系类型和测试句中的不一致问题；（2）将NULL示例错误地分类为其他关系类型的幻觉问题，提出一种基于实体感知检索和正确标签诱导推理的GPT-RE方法。该方法首先通过实体提示语句、微调关系表示两种方法，从训练集中检索包含更多RE任务信息的例句。然后生成判断例句中实体对关系类型的线索，将推理线索和原始例句结合加强示例演示。实验结果表明，两种策略能够有效弥合生成式模型在RE任务上与基线模型的性能差距。

（2）联合关系抽取模式

虽然流水线模式使NER任务和RE任务变得易于处理，但是它忽略了两个子任务之间和子任务内部的潜在依赖关系，禁止子任务之间的交互反馈[113-114]。首先，前序的NER任务无法通过学习实体之间的关系依赖提高准确率，前序NER中的误差还会传播到RE任务中；其次，后序的RE任务一般被建模为实体对上的多分类问题，忽略了实体对之间可能存在的依赖关系。因此，研究人员开始将两项任务融合成一个任务，加强任务之间的交互。联合关系抽取方法可分为参数共享但单独编解码、参数共享且统一编解码两种。

参数共享但单独编解码方法是指，通过统一构建深度学习神经网络模型、共享损失函数等方法，使两项子任务共享一份模型参数，但是一般使用两个独立的判别器进行标签预测，两项子任务的标签空间也相互独立，模型设计相对简单，但是交互性较弱。参数共享且统一编解码方法是指，通过设计统一的标签空间，使标签既能表示实体信息，也能表示关系信息，从而使模型通过一个判别器即可完成两项子任务，但标签设计难度和模型结构复杂程度均比较高。

Miwa等人[115]针对实体和关系信息存在密切联系的问题，提出一种同时抽取实体和关系的联合抽取方法。该方法在基于单词序列的BiLSTM层上叠加基于依存关系子树的BiTreeLSTM层，将BiLSTM隐层状态（即单词序列特征向量）、标签嵌入表示（即实体类别特征向量）和依存树结构特征融合输入BiTreeLSTM，使用共享参数表示实体和关系信息。该研究实验表明，使用共享参数进行训练可以提高关系抽取的准确性。

谢博[116]针对网络安全领域实体之间距离较远、关系较为复杂的问题，提出一种基于语义上下文过滤的网络安全实体关系联合抽取模型。该模型利用BERT模型作为实体和文本的语义特征编码器，并将实体语义特征、实体位置特征和句子语义特征融合，最后通过多头注意力机制进一步筛选实体信息、语义信息和关系信息最关联的特征信息。

Wang等人[117]针对重叠关系提取困难问题和流水线模式误差累计问题，提出一种一阶联合关系抽取模型。该方法将联合抽取问题建模为token对关系问题，引入一种新的标记配对方案，即为每种关系构建三个token关系矩阵，从而判别两个token是否为同一实体的起始/终止位置；判别两个token是否是具有关系的两个实体的起始位置；判别两个token是否为具有关系的两个实体的终止位置，使模型能够对齐每种关系类型的实体对的边界token，提升了模型识别各种重叠关系的准确性。

Yan等人[118]针对现有NER和RE联合抽取模型中两个子任务特征缺乏交互的问题，提出一种基于联合编码的能够区分子任务特征的联合抽取模型PFN（partition filter network）。该模型利用类似LSTM方法对文本进行编码，然后将特征向量拆分成只与NER相关、只与RE相关和共享部分，然后根据子任务组合特征向量进行实体和关系分类，既避免了两项任务之间的相互干扰，又利用了两个任务之间的相互支撑，提升了两项任务的准确率。

Wang等人[79]针对独立编解码可能会阻碍实体和关系之间信息交互的问题，提出一种统一的解码方式，成功使用一个统一的分类器完成两项任务。该方法首先利用BERT模型获得文本的上下文表示，在通过两个MLP网络降维后，利用深度双仿射机制（deep biaffine attention mechanism）提取文本之间的

依赖关系,进行实体和关系预测。最后,通过联合解码算法提取结果中的实体和关系,在模型性能和效率方面均表现良好。

表6总结了一些RE模型在经典数据集上的性能及其前序NER任务的方法。

5.2.4 基于远程监督的方法

因为大多数领域的关系抽取任务都面临着缺少标注数据集的问题,所以研究人员开始研究基于远程监督的关系抽取方法。远程监督(distance supervision)是指将已有知识库(如Freebase)和海量的非结构化文本进行对齐,自动化生成大量标注数据。

Mintz等人[119]首次提出基于远程监督学习的RE方法。该方法的主要假设是:如果两个实体之间存在某种关系,那么任何包含这两个实体的句子都可以表达这种关系。但该假设太过绝对,容易出现错误标注的问题。Riedel等人[120]对该假设进行放宽,提出多实例学习,即如果两个实体之间存在某种关系,那么在所有包含这两个实体的句子中,至少存在一个句子能够表达这种关系。

在此基础上,Hoffmann等人[121]对相同实体对之间只存在一种关系的假设进行放宽,缓解了实体对关系重叠的噪声问题。Surdeanu等人[122]提出多实例多标签学习(multi-instance multi-label learning)的思想,对一个实例包中只存在一种关系的假设进行放宽,进一步缓解了噪声数据的问题。

Zeng等人[123]针对基于统计的机器学习模型通过特定特征进行分类,但特定特征的噪声影响会导致模型效果较差的问题;针对远程监督学习方法中由于文本对齐不准确导致的错误标注问题,提出一种基于多实例远程监督学习的结合词汇特征的分段卷积神经网络(piecewise CNN,PCNN)关系抽取方法。该方法使用经典的最大池化CNN网络,将单词词义向量和位置向量融合后输入卷积神经网络,然后利用分段最大池化(piecewise max pooling)更加有效地提取用于关系抽取任务的结构信息,最后利用全连接网络进行关系分类。

王会勇等人[124]针对特定领域RE任务缺乏标注数据集的问题,提出一种基于远程监督学习的领域数据标注方法。该方法通过DBpedia和Wikipedia提取领域三元组,然后通过OpenIE和ReVerb扩充领域三元组,构建了金属材料领域数据集。又针对缺乏特定领域RE模型的问题,提出一种基于PCNN的关系抽取模型。该模型首先通过领域知识构建领域关系词典,通过词典匹配方式提取表达关系的先验词汇;然后将先验词汇的语义特征作为卷积核权重调整卷积层输出,加强了模型关系分类能力,提高了模型关系抽取性能。

Shen等人[125]针对全局特征提取和深度神经网络梯度消失的问题,提出一种基于深度残差卷积神经网络(ResNet)的远程监督关系抽取方法。该方法利用多实例学习和注意力机制降低远程监督中噪声数据的影响,利用深度分段卷积神经网络(ResPCNN)更好地提取句子中的深度语义特征。在具体工业控制场景上,提取工业互联网安全实体之间的语义关系,构建了工业控制系统安全知识图谱。

Wang等人[76]针对网络威胁情报中RE任务的问题,提出一种基于远程监督和强化学习的RE模型NR-RL-PCNN-ATT。该模型在Zeng等人[123]提出的

表6 不同RE方法在各数据集上的F1值对比

Table 6 Comparison of F1 values between different RE methods on different datasets 单位:%

阶段	论文	模型	前序NER方法	数据集				
				MUC-6	MUC-7	ACE2004	ACE2005	SemEval2010 Task8
模板匹配	Appelt[98]	FSA,“宏”	基于规则	54.60				
	Grishman[99]	基于模板	基于模板		42.73			
机器学习	Kambhatla[101]	MEM	数据集给定			52.80		
	Zhou[102]	SVM	数据集给定+基于词典			55.50		
深度学习	Miwa[115]	叠加BiLSTM	联合抽取			48.10	55.60	85.50
	Wu[109]	R-BERT	数据集给定					89.25
	Soares[111]	$BERT_{EM}$-MTB	数据集给定					89.50
	Wan[112]	GPT-RE	—				68.73	91.90
	Yan[118]	PFN	联合抽取			62.50	66.80	
	Wang[79]	统一编解码标签	联合抽取			63.00	67.80	

PCNN-ATT基础上，通过设计一个基于F1值的奖励函数，提高句子实例选择器的句子选择质量，降低错误标注的噪声影响，提高关系抽取的效果。但是该模型主要利用句子的语义特征，没有考虑句子语义特征和句子语法特征的融合问题。

Vashishth等人[126]针对现有远程监督RE方法忽略知识库中包含的其他相关辅助信息（如关系别名、实体类型等）的问题，提出一种利用知识库中附加边信息的RE方法。该方法使用BiGRU和图卷积神经网络（graph convolutional network，GCN）对文本的句法信息进行编码，使用知识库中的相关辅助信息为关系预测添加软约束。研究表明，加入辅助信息能够有效提高模型的性能。Moreira等人[127]在Vashishth[126]的基础上，使用BERT替代BiGRU和GCN对文本进行编码，简化了句子编码复杂度，提高了模型效率。

Alt等人[128]针对现有远程监督RE方法大多忽略长尾关系的问题，提出一种基于GPT的远程监督RE法。该方法通过选择性注意力机制处理多实例学习，直接微调GPT模型，最小化显式特征提取，降低误差积累风险。自注意力机制允许模型有效提取远距离依赖关系和利用模型在预训练期间获得的实体和概念之间的关系知识。

Tsoumakas等人[129]针对长尾关系抽取问题，提出一种基于远程监督和Transformer的关系抽取模型。该模型通过输入包括链接实体对和实体类型的子树在内的只表示实体关系的结构化数据微调BERT模型，使模型能够捕获更适合关系抽取任务的嵌入表示；使用注意力机制和标签嵌入编码，进一步减少噪声数据的影响。

Li等人[130]针对通过知识蒸馏的缓解远程监督的噪声影响时，还存在的隐藏知识精确传递问题和单一蒸馏温度限制问题，提出一种多实例动态温度蒸馏框架（multi-instance dynamic temperature distillation，MiDTD），并在基于BERT、PCNN和BiLSTM的句子级关系抽取任务模型上应用此框架。该框架主要包括两个模块，多实例目标融合和动态温度调节模块。多实例目标融合模块将教师模型对同一实体对的多个句子实例的预测结合起来，修正每个学生目标中隐藏知识的准确性；动态温度调节模块将不同的蒸馏温度分配给不同的训练实例，以使大多数学生目标的软标签达到一个合适的柔软范围。但是噪声较大的远程监督数据总是影响神经网络模型的性能，引入额外的神经网络也无法取得理想的效果，而引入人工标注的关系抽取数据可能会提高模型蒸馏的效果。

表7总结了基于远程监督的关系抽取方法，表8总结了工业互联网安全领域的关系抽取方法。

5.3　工业互联网安全RE面临的挑战

5.3.1　重叠关系识别问题

重叠关系指的是一条语句中可能只有一个实体对及其关系，也有可能一个实体同另一个实体之间存在着多种关系（entity pair overlap，EPO，实体对重叠），

表7　基于远程监督的关系抽取方法

Table 7　Methods of relationship extraction based on distance supervision

阶段	论文	方法	降低噪声方法	数据集	评价指标			
					P/%	*R*/%	*F*1/%	*AUC*
机器学习	Mintz[119]	机器学习（回归分类器）	—	ACE	43.80	36.80	40.00	0.107
	Riedel[120]	概率图模型	放宽假设、多实例	NYT	56.10	32.50	41.10	
	Hoffmann[121]	概率图模型	多实例	Riedel[121]	48.60	29.80	37.00	
	Surdeanu[122]	概率图模型	多实例、多标签	Riedel[121]	64.80	31.60	42.60	
深度学习	Zeng[123]	PCNN	多实例、PCNN	Riedel[121]	63.60			0.341
	王会勇[124]	Dic-PCNN	领域关系词典、数据增强	金属材料领域数据集			81.42	
	Vashishth[126]	BiGRU-GCN-ATT	多实例、知识库辅助信息	NYT-10, GDS	69.70			0.415
	Alt[128]	GPT	注意力机制、预训练模型	NYT-10	65.00			0.422
	Tsoumakas[129]	R-BERT-ATT	实体标签嵌入、注意力机制	NYT-10, GDS	67.60			0.424
	Li[130]	MiDTD-PCNN MiDTD-BiLSTM MiDTD-BERT	多实例标签融合 动态温度知识蒸馏	NYT-10 NYT-19	96.10			0.620

表8 工业互联网安全RE模型对比

Table 8 Comparison of industry Internet security RE models

阶段	论文	方法	前序NER方法	数据集
机器学习	Jones[104]	Bootstrapping 模板评分、主动学习	Bridges[48] 领域词典、正则表达式	Security Blogs、ThreatPost Malwarebytes
	Liao[51]	依赖子图相似性比较	领域词典、正则表达式	IoC bucket、OpenIoC DB Security Blogs
深度学习	Pingle[107]	FFNN	Mittal[108]	Security Blogs、CVE、NVD Microsoft Security Bulletins STIX Corpus
	Sarhan[110]	基于BiGRU的OIE框架	BiGRU-TDD-CRF	Bridges[48]、Kim[131] MalWareTextDB[132]
	Jo[66]	基于R-BERT	BERT-BiLSTM-CRF	ThreatPost、Malwarebytes、Twitter
	Li[97]	基于BERT-LogSumExp 池化的文档级关系抽取	BERT-BiLSTM-ATT	Threat Intelligence Documents
远程监督	Shen[125]	Res-PCNN-ATT	Qin[57]	Freebuf网站、乌云漏洞数据库
	Wang[76]	NR-RL-PCNN-ATT	Dic-BERTBiLSTM-CRF	MalwareDB[77]、CVE、NISVD[78]

还有可能一个实体与其他不同实体之间存在着多种关系(single entity overlap,SEO,单一实体重叠)。

5.3.2 计算资源消耗问题

随着BERT、GPT等预训练模型应用于关系抽取领域,关系抽取模型的参数量也随即增大,而从预训练阶段开始构建完全适用于领域关系抽取任务的模型所需的计算资源也急速增大。

5.3.3 领域标注数据集获取问题

关系抽取任务核心部分多采用有监督的深度学习模型来判断实体对之间是否存在某种关系,而这些深度学习模型的性能多取决于高质量的标注训练集,训练集的大小和标注质量都会影响关系抽取任务的效果。在通用领域存在一些公开的高质量的标注数据集,但是在专业领域,尤其是工业互联网安全领域,安全数据是各种安全服务提供商和国家安全部门的重要资产,所以很少有公开的高质量的标注数据集,给工业互联网安全领域关系抽取任务带来不小的困难。

针对上述问题与挑战,本文认为:(1)可以利用基于远程监督的RE算法,利用相关知识库对大量无标注语料进行标注,扩展工业互联网安全领域RE任务数据集。(2)可以通过与NER任务进行融合,设计统一的标注方法,将重叠关系抽取任务建模为端到端的序列标注任务,提高对重叠关系的识别准确率。(3)可以利用知识蒸馏的方法,将预训练模型中蕴含的相关知识蒸馏到BiLSTM等小模型中,减少模型复杂度,提高模型运行效率。

6 总结

工业互联网安全知识图谱作为一种使用图模型来描述、建模和推断网络安全概念及其之间关联关系的技术方法,有效地解决了网络安全领域多源异构数据的融合问题。本文调查研究了命名实体识别、共指消解和关系抽取三个构建知识图谱的关键环节,列举了现有研究针对的问题和依旧存在的缺陷,总结了IISKG在这些任务上面临的困难和挑战,并依据现有研究分析了未来可能的解决方案。

参考文献:

[1] 国家能源局. 2021年全国电力工业统计数据[EB/OL]. (2022-01-26) [2023-04-19]. http://www.nea.gov.cn/2022-01/26/c_1310441589.htm.
National Energy Administration. 2021 National power industry statistics[EB/OL]. (2022-01-26) [2023-04-19]. http://www.nea.gov.cn/2022-01/26/c_1310441589.htm.

[2] 王青, 孙峁, 张海霞, 等. 中国光伏行业2021年回顾与2022年展望[J]. 电气时代, 2022(5): 20-28.
WANG Q, SUN D, ZHANG H X, et al. A review of China's photovoltaic industry in 2021 and prospects for 2022[J]. Electric Age, 2022(5): 20-28.

[3] 徐伟, 孔坚, 毛庆梅, 等. 工业控制系统安全现状及应对策略[J]. 网络安全技术与应用, 2021(9): 115-117.
XU W, KONG J, MAO Q M, et al. Safety status and countermeasures of industry control system[J]. Network Security Technology & Application, 2021(9): 115-117.

[4] 郑少波, 徐伟, 石彬. 工业控制系统安全现状[J]. 网络安全技术与应用, 2020(5): 111-113.
ZHENG S B, XU W, SHI B. Safety status of industry con-

trol system[J]. Network Security Technology & Application, 2020(5): 111-113.

[5] 360数字安全集团. 2022全球高级持续性威胁(APT)研究报告[EB/OL]. (2023-01-08) [2023-04-19]. https://360.net/about/news/article63c8e20258f02a002a0d76de.
360 Digital Security Group. 2022 Global advanced persistent threat(APT) research report[EB/OL]. (2023-01-08) [2023-04-19]. https://360.net/about/news/article63c8e20258f02a002a0d76de.

[6] 绿盟科技. 践行安全知识图谱, 携手迈进认知智能[EB/OL]. (2022-05-23) [2023-04-19]. https://www.nsfocus.com.cn/html/2022/137_0523/179.html.
NSFOCUS. Practice the safety knowledge graph, and work together to advance cognitive intelligence[EB/OL]. (2022-05-23) [2023-04-19]. https://www.nsfocus.com.cn/html/2022/137_0523/179.html.

[7] 绿盟科技. 安全知识图谱[EB/OL]. (2022-01-07) [2023-04-19]. https://www.zhihu.com/column/c_1446900744649240576.
NSFOCUS. Security knowledge graph[EB/OL]. (2022-01-07) [2023-04-19]. https://www.zhihu.com/column/c_1446900744649240576.

[8] BERNERS-LEE T. What the semantic web can represent [Z]. 1998.

[9] BERNERS-LEE T. Semantic web road map[Z]. 1998.

[10] BERNERS-LEE T, CHEN Y, CHILTON L, et al. Tabulator: exploring and analyzing linked data on the semantic web [C]//Proceedings of the 3rd International Semantic Web User Interaction Workshop, Athens, Nov 6, 2006.

[11] MILLER G A. Wordnet: a lexical database for English[J]. Commun ACM, 1995, 38(11): 39-41.

[12] BAKER C F, FILLMORE C J, LOWE J B. The Berkeley framenet project[C]//Proceedings of the 36th Annual Meeting of the Association for Computational Linguistics, Montreal, Aug, 1998. Stroudsburg: ACL, 1998.

[13] DONG Z, DONG Q. HowNet—a hybrid language and knowledge resource[C]//Proceedings of the 2003 International Conference on Natural Language Processing and Knowledge Engineering, Beijing, Oct 26-29, 2003. Piscataway: IEEE, 2003: 820-824.

[14] SPEER R, CHIN J, HAVASI C. ConceptNet 5.5: an open multilingual graph of general knowledge[J]. arXiv:1612.03975, 2016.

[15] BOLLACKER K, EVANS C, PARITOSH P, et al. Freebase: a collaboratively created graph database for structuring human knowledge[C]//Proceedings of the 2008 ACM SIGMOD International Conference on Management of Data, Vancouver, Jun 10-12, 2008. New York: ACM, 2008: 1247-1250.

[16] AUER S, BIZER C, KOBILAROV G, et al. DBpedia: a nucleus for a web of open data[C]//Proceedings of the 6th International Semantic Web Conference, Busan, Nov 11-15, 2007. Berlin, Heidelberg: Springer, 2007: 722-735.

[17] SUCHANEK F M, KASNECI G, WEIKUM G. Yago: a core of semantic knowledge[C]//Proceedings of the 16th International Conference on World Wide Web, Banff, May 8-12, 2007. New York: ACM, 2007: 697-706.

[18] RESEARCH W. Wolframalpha[EB/OL]. (2023-01-03) [2023-07-28]. https://www.wolframalpha.com/.

[19] MITCHELL T, COHEN W, HRUSCHKA E, et al. Never-ending learning[J]. Communications of the ACM, 2018, 61(5): 103-115.

[20] NAVIGLI R, PONZETTO S P. BabelNet: the automatic construction, evaluation and application of a wide-coverage multilingual semantic network[J]. Artificial Intelligence, 2012, 193: 217-250.

[21] VRANDEČIĆ D, KRÖTZSCH M. Wikidata: a free collaborative knowledgebase[J]. Communications of the ACM, 2014, 57(10): 78-85.

[22] DONG X, GABRILOVICH E, HEITZ G, et al. Knowledge vault: a web-scale approach to probabilistic knowledge fusion[C]//Proceedings of the 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, New York, Aug 24-27, 2014. New York: ACM, 2014: 601-610.

[23] NIU X, SUN X, WANG H, et al. Zhishi.Me-weaving Chinese linking open data[C]//Proceedings of the 10th International Semantic Web Conference, Bonn, Oct 23-27, 2011. Berlin, Heidelberg: Springer, 2011: 205-220.

[24] WANG Z, LI J Z, WANG Z, et al. XLore: a large-scale English-Chinese bilingual knowledge graph[C]//Proceedings of the 12th International Semantic Web Conference and the 1st Australasian Semantic Web Conference, Sydney, Oct 21-25, 2013. Berlin, Heidelberg: Springer, 2013: 121-124.

[25] Openkg.Cn[EB/OL]. [2023-07-28]. http://openkg.cn/.

[26] XU B, XU Y, LIANG J, et al. CN-DBpedia: a never-ending Chinese knowledge extraction system[C]//Proceedings of the 30th International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems, Arras, Jun 27-30, 2017. Cham: Springer, 2017: 428-438.

[27] 中国电子技术标准化研究院. 认知智能时代: 知识图谱实践案例集[J]. 信息技术与标准化, 2021(3): 5.
China Electronics Standardization Institute. The era of cognitive intelligence: knowledge graph practice case set[J]. Information Technology & Standardization, 2021(3): 5.

[28] 董聪, 姜波, 卢志刚, 等. 面向网络空间安全情报的知识图谱综述[J]. 信息安全学报, 2020, 5(5): 56-76.
DONG C, JIANG B, LU Z G, et al. Knowledge graph for cyberspace security intelligence: a survey[J]. Journal of Cyber Security, 2020, 5(5): 56-76.

[29] 丁兆云, 刘凯, 刘斌, 等. 网络安全知识图谱研究综述[J]. 华中科技大学学报(自然科学版), 2021, 49(7): 79-91.
DING Z Y, LIU K, LIU B, et al. Survey of cyber security knowledge graph[J]. Journal of Huazhong University of Sci-

ence and Technology (Natural Science Edition), 2021, 49(7): 79-91.

[30] 尚文利, 朱鹏程, 王博文, 等. 面向威胁情报的知识图谱构建关键技术[J]. 自动化博览, 2023, 40(1): 15-19.
SHANG W L, ZHU P C, WANG B W, et al. Key technologies for building knowledge graphs for threat intelligence [J]. Automation Panorama, 2023, 40(1): 15-19.

[31] 王晓狄, 黄诚, 刘嘉勇. 面向网络安全开源情报的知识图谱研究综述[J]. 信息网络安全, 2023, 23(6): 11-21.
WANG X D, HUANG C, LIU J Y. A survey of cyber security open-source intelligence knowledge graph[J]. Netinfo Security, 2023, 23(6): 11-21.

[32] GAO C, ZHANG X, HAN M, et al. A review on cyber security named entity recognition[J]. Frontiers of Information Technology & Electronic Engineering, 2021, 22(9): 1153-1168.

[33] LIU K, WANG F, DING Z, et al. Recent progress of using knowledge graph for cybersecurity[J]. Electronics, 2022, 11 (15): 2287.

[34] OLTRAMARI A, CRANOR L F, WALLS R J, et al. Computational ontology of network operations[C]//Proceedings of the 2015 IEEE Military Communications Conference, Tampa, Oct 26-28, 2015. Piscataway: IEEE, 2015: 318-323.

[35] BEN-ASHER N, HUTCHINSON S, OLTRAMARI A. Characterizing network behavior features using a cyber-security ontology[C]//Proceedings of the 35th IEEE Military Communications Conference, Baltimore, Nov 1-3, 2016. Piscataway: IEEE, 2016: 758-763.

[36] IANNACONE M, BOHN S, NAKAMURA G, et al. Developing an ontology for cyber security knowledge graphs[C]// Proceedings of the 10th Annual Cyber and Information Security Research Conference, Oak, Apr 7-9, 2015. New York: ACM, 2015: 1-4.

[37] SYED Z, PADIA A, FININ T, et al. UCO: a unified cybersecurity ontology[C]//Proceedings of the Workshops of the 30th AAAI Conference on Artificial Intelligence: Artificial Intelligence for Cyber Security, Phoenix, Feb 12-17, 2016. Menlo Park: AAAI, 2016: 195-202.

[38] KRUPKA G R. SRA: description of the SRA system as used for MUC-6[C]//Proceedings of the 6th Message Understanding Conference, Columbia, Nov 6-8, 1995. Stroudsburg: ACL, 1995: 221-236.

[39] HUMPHREYS K, GAIZAUSKAS R, AZZAM S, et al. University of Sheffield: description of the LaSIE-II system as used for MUC-7[C]//Proceedings of the 7th Message Understanding Conference, Fairfax, Apr 29-May 1, 1998. Stroudsburg: ACL, 1998.

[40] KRUPKA G R, HAUSMAN K. Description of the NetOwl extractor system as used for MUC-7[C]//Proceedings of the 7th Message Understanding Conference, Fairfax, Apr 29-May 1, 1998. Stroudsburg: ACL, 1998.

[41] BLACK W J, RINALDI F, MOWATT D. Facile: description of the NE system used for MUC-7[C]//Proceedings of the 7th Message Understanding Conference, Fairfax, Apr 29-May 1, 1998. Stroudsburg: ACL, 1998.

[42] APPELT D E, HOBBS J R, BEAR J, et al. FASTUS: a finite-state processor for information extraction from real-world text [C]//Proceedings of the 13th International Joint Conference on Artificial Intelligence, Chambery, Aug 28-Sep 3, 1993. San Francisco: Morgan Kaufmann Publishers Inc, 1993: 1172-1178.

[43] MIKHEEV A, GROVER C, MOENS M. Description of the LTG system used for MUC-7[C]//Proceedings of the 7th Message Understanding Conference, Fairfax, Apr 29-May 1, 1998. Stroudsburg: ACL, 1998.

[44] BIKEL D M, SCHWARTZ R, WEISCHEDEL R M. An algorithm that learns what's in a name[J]. Machine Learning, 1999, 34: 211-231.

[45] ZHOU G, SU J. Named entity recognition using an HMM-based chunk tagger[C]//Proceedings of the 40th Annual Meeting of the Association for Computational Linguistics, Philadelphia, Jul 6-12, 2002. Stroudsburg: ACL, 2002: 473-480.

[46] BORTHWICK A, STERLING J, AGICHTEIN E, et al. NYU: description of the MENE named entity system as used in MUC-7[C]//Proceedings of the 7th Message Understanding Conference, Fairfax, Apr 29-May 1, 1998. Stroudsburg: ACL, 1998.

[47] BENDER O, OCH F J, NEY H. Maximum entropy models for named entity recognition[C]//Proceedings of the 7th Conference on Natural Language Learning at HLT-NAACL, Edmonton, May 31-Jun 1, 2003. Stroudsburg: ACL, 2003: 148-151.

[48] BRIDGES R A, JONES C L, IANNACONE M D, et al. Automatic labeling for entity extraction in cyber security[J]. arXiv:1308.4941, 2013.

[49] JOSHI A, LAL R, FININ T, et al. Extracting cybersecurity related linked data from text[C]//Proceedings of the 7th IEEE International Conference on Semantic Computing, Irvine, Sep 16-18, 2013. Washington: IEEE Computer Society, 2014: 252-259.

[50] 贾焰, 亓玉璐, 尚怀军, 等. 一种构建网络安全知识图谱的实用方法[J]. Engineering, 2018, 4(1): 117-133.
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): 117-133.

[51] LIAO X, YUAN K, WANG X, et al. Acing the IOC game: toward automatic discovery and analysis of open-source cyber threat intelligence[C]//Proceedings of the 23rd ACM Conference on Computer and Communications Security, New York, Oct 24-28, 2016. New York: ACM, 2016: 755-766.

[52] COLLOBERT R, WESTON J, BOTTOU L, et al. Natural

language processing (almost) from scratch[J]. Journal of Machine Learning Research, 2011, 12: 2493-2537.

[53] YAO L, LIU H, LIU Y, et al. Biomedical named entity recognition based on deep neutral network[J]. International Journal of Hybrid Information Technology, 2015, 8: 279-288.

[54] STRUBELL E, VERGA P, BELANGER D, et al. Fast and accurate entity recognition with iterated dilated convolutions[C]//Proceedings of the 2017 Conference on Empirical Methods in Natural Language Processing, Copenhagen, Sep 7-11, 2017. Stroudsburg: ACL, 2017: 2670-2680.

[55] HUANG Z, WEI X, KAI Y. Bidirectional LSTM-CRF models for sequence tagging[J]. arXiv:1508.01991, 2015.

[56] SIMRAN K, SRIRAM S, VINAYAKUMAR R, et al. Deep learning approach for intelligent named entity recognition of cyber security[C]//Proceedings of the 5th International Symposium on Signal Processing and Intelligent Recognition Systems, Trivandrum, Dec 18-21, 2019. Singapore: Springer, 2020: 163-172.

[57] QIN Y, SHEN G, ZHAO W, et al. A network security entity recognition method based on feature template and CNN-BILSTM-CRF[J]. Frontiers of Information Technology and Electronic Engineering, 2019, 20(6): 872-884.

[58] GAO C, ZHANG X, LIU H. Data and knowledge-driven named entity recognition for cyber security[J]. Cybersecurity, 2021, 4: 9.

[59] LI T, HU Y, JU A, et al. Adversarial active learning for named entity recognition in cybersecurity[J]. Computers, Materials and Continua, 2021, 66(1): 407-420.

[60] RADFORD A, NARASIMHAN K, SALIMANS T, et al. Improving language understanding by generative pre-training [Z]. 2018.

[61] RADFORD A, WU J, CHILD R, et al. Language models are unsupervised multitask learners[J]. OpenAI Blog, 2019, 1(8): 9.

[62] BROWN T B, MANN B, RYDER N, et al. Language models are few-shot learners[J]. arXiv:2005.14165, 2020.

[63] OPENAI. GPT-4 technical report[J]. arXiv:2303.08774, 2023.

[64] DEVLIN J, CHANG M W, LEE K, et al. BERT: pre-training of deep bidirectional transformers for language understanding[J]. arXiv:1810.04805, 2019.

[65] YANG Z, DAI Z, YANG Y, et al. XLNet: generalized autoregressive pretraining for language understanding[C]//Proceedings of the 33rd International Conference on Neural Information Processing Systems, Vancouver, Dec 8-14, 2019. Red Hook: Curran Associates Inc, 2019: 5753-5763.

[66] JO H, LEE Y, SHIN S. Vulcan: automatic extraction and analysis of cyber threat intelligence from unstructured text [J]. Computers and Security, 2022, 120: 102763.

[67] 杨秀璋, 彭国军, 李子川, 等. 基于Bert和BiLSTM-CRF的APT攻击实体识别及对齐研究[J]. 通信学报, 2022, 43(6): 58-70.
YANG X Z, PENG G J, LI Z C, et al. Research on entity recognition and alignment of APT attack based on BERT and BiLSTM-CRF[J]. Journal on Communications, 2022, 43 (6): 58-70.

[68] ZHANG K, CHEN X, JING Y, et al. Research on named entity recognition method of network threat intelligence[C]// Proceedings of the 19th China Cyber Security Annual Conference, Beijing, Aug 16-17, 2022. Singapore: Springer Nature Singapore, 2022: 213-224.

[69] ZHOU S, LIU J, ZHONG X, et al. Named entity recognition using BERT with whole world masking in cybersecurity domain[C]//Proceedings of the 6th IEEE International Conference on Big Data Analytics, Xiamen, Mar 5-8, 2021. New York: IEEE, 2021: 316-320.

[70] 谢博, 申国伟, 郭春, 等. 基于残差空洞卷积神经网络的网络安全实体识别方法[J]. 网络与信息安全学报, 2020, 6 (5): 126-138.
XIE B, SHEN G W, GUO C, et al. Cyber security entity recognition method based on residual dilation convolution neural network[J]. Chinese Journal of Network and Information Security, 2020, 6(5): 126-138.

[71] 苏剑林. Gplinker:基于globalpointer的实体关系联合抽取[EB/OL]. (2022-01-30) [2023-04-19]. https://spaces.ac.cn/archives/8888.
SU J L. Gplinker: entity relationship joint extraction based on globalpointer[EB/OL]. (2022-01-30) [2023-04-19]. https://spaces.ac.cn/archives/8888.

[72] YAN H, GUI T, DAI J, et al. A unified generative framework for various NER subtasks[C]//Proceedings of the Joint Conference of the 59th Annual Meeting of the Association for Computational Linguistics and the 11th International Joint Conference on Natural Language Processing, Aug 1-6, 2021. Stroudsburg: ACL, 2021: 5808-5822.

[73] LI J, FEI H, LIU J, et al. Unified named entity recognition asword-word relation classification[C]//Proceedings of the 36th AAAI Conference on Artificial Intelligence, Vancouver, Feb 22-Mar 1, 2022. Menlo Park: AAAI, 2022: 10965-10973.

[74] WANG S, SUN X, LI X, et al. GPT-NER: named entity recognition via large language models[J]. arXiv:2304.10428, 2023.

[75] LI X, ZHU X D, MA Z, et al. Are ChatGPT and GPT-4 general-purpose solvers for financial text analytics? An examination on several typical tasks[J]. arXiv:2305.05862, 2023.

[76] WANG X, CHEN R, SONG B, et al. A method for extracting unstructured threat intelligence based on dictionary template and reinforcement learning[C]//Proceedings of the 24th IEEE International Conference on Computer Supported Cooperative Work in Design, Dalian, May 5-7, 2021. Piscataway: IEEE, 2021: 262-267.

[77] NATIV Y T, SHALEV S. TheZoo aka malware DB[EB/OL]. (2023-04-04) [2023-04-19]. https://github.com/ytisf/theZoo.

[78] 李瑞科, 刘元, 廖雷, 等. 1999—2018年安全漏洞数据集[EB/OL]. (2019-12-30) [2023-04-19]. http://www.csdata.org/p/315/.
LI R K, LIU Y, LIAO L, et al. 1999—2018 security vulnerability dataset[EB/OL]. (2019-12-30) [2023-04-19]. http://www.csdata.org/p/315/.

[79] WANG Y, SUN C, WU Y, et al. UniRE: a unified label space for entity relation extraction[C]//Proceedings of the Joint Conference of the 59th Annual Meeting of the Association for Computational Linguistics and the 11th International Joint Conference on Natural Language Processing, Aug, 2021. Stroudsburg: ACL, 2021: 220-231.

[80] JACKADUMA. Secbert[EB/OL]. (2022-01-24) [2023-06-09]. https://huggingface.co/jackaduma/SecBERT.

[81] BAYER M, KUEHN P, SHANEHSAZ R, et al. CySecBERT: a domain-adapted language model for the cybersecurity domain[J]. arXiv:2212.02974, 2022.

[82] HOBBS J R. Resolving pronoun references[J]. Lingua, 1978, 44(4): 311-338.

[83] GROSZ B J, WEINSTEIN S, JOSHI A K. Centering: a framework for modeling the local coherence of discourse[J]. Comput Linguist, 1995, 21(2): 203-225.

[84] RAGHUNATHAN K, LEE H, RANGARAJAN S, et al. A multi-pass sieve for coreference resolution[C]//Proceedings of the 2010 Conference on Empirical Methods in Natural Language Processing, Cambridge, Oct 9-11, 2010. Stroudsburg: ACL, 2010: 492-501.

[85] 陈远哲, 匡俊, 刘婷婷, 等. 共指消解技术综述[J]. 华东师范大学学报(自然科学版), 2019(5): 16-35.
CHEN Y Z, KUANG J, LIU T T, et al. A survey on coreference resolution[J]. Journal of East China Normal University (Natural Science), 2019(5): 16-35.

[86] RAHMAN A, NG V. Narrowing the modeling gap: a cluster-ranking approach to coreference resolution[J]. Journal of Artificial Intelligence Research, 2011, 40(1): 469-521.

[87] MCCALLUM A, WELLNER B. Conditional models of identity uncertainty with application to noun coreference[C]//Proceedings of the 18th Annual Conference on Neural Information Processing Systems, Vancouver, Dec 1, 2004. Cambridge: MIT Press, 2004: 905-912.

[88] 黄伟民. 基于预训练语言模型的中文共指消解方法研究[D]. 广州: 华南理工大学, 2021.
HUANG W M. Research on Chinese coreference resolution based on pre-trained language model[D]. Guangzhou: South China University of Technology, 2021.

[89] WISEMAN S, RUSH A M, SHIEBER S M. Learning global features for coreference resolution[C]//Proceedings of the 15th Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Austin, Nov 1-5, 2016. Stroudsburg: ACL, 2016: 994-1004.

[90] LEE K, HE L, LEWIS M, et al. End-to-end neural coreference resolution[C]//Proceedings of the 2017 Conference on Empirical Methods in Natural Language Processing, Copenhagen, Sep 7-11, 2017. Stroudsburg: ACL, 2017: 188-197.

[91] LEE K, HE L, ZETTLEMOYER L. Higher-order coreference resolution with coarse-to-fine inference[C]//Proceedings of the 2018 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Louisiana, Jun 1-6, 2018. Stroudsburg: ACL, 2018: 687-692.

[92] JOSHI M, LEVY O, ZETTLEMOYER L, et al. BERT for coreference resolution: baselines and analysis[C]//Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing and the 9th International Joint Conference on Natural Language Processing, Hong Kong, China, Nov 3-7, 2019. Stroudsburg: ACL, 2019: 5803-5808.

[93] JOSHI M, CHEN D Q, LIU Y H, et al. SpanBERT: improving pretraining by representing and predicting spans[J]. Transactions of the Association for Computational Linguistics, 2020, 8: 64-77.

[94] 唐思宇, 李赛飞, 张丽杰. 基于neo4j的网络安全知识图谱构建分析[J]. 信息安全与通信保密, 2022(8): 60-70.
TANG S Y, LI S F, ZHANG L J. Research on the construction of cyber security knowledge graph based on neo4j[J]. Information Security and Communications Privacy, 2022(8): 60-70.

[95] 张晗, 胡永进, 郭渊博, 等. 信息安全领域内实体共指消解技术研究[J]. 通信学报, 2020, 41(2): 165-175.
ZHANG H, HU Y J, GUO Y B, et al. Research on coreference resolution technology of entity in information security [J]. Journal on Communications, 2020, 41(2): 165-175.

[96] 周宁, 靳高雅, 石雯茜. 融合神经网络与全局推理的实体共指消解算法[J]. 数据分析与知识发现, 2022, 6(8): 75-83.
ZHOU N, JIN G Y, SHI W Q. Algorithm for entity coreference resolution withneural network and global reasoning[J]. Data Analysis and Knowledge Discovery, 2022, 6(8): 75-83.

[97] LI Y, GUO Y, FANG C, et al. A novel threat intelligence information extraction system combining multiple models[J]. Security and Communication Networks, 2022: 8477260.

[98] APPELT D E, HOBBS J R, BEAR J, et al. SRI international FASTUS system MUC-6 test results and analysis[C]//Proceedings of the 6th Message Understanding Conference, Columbia, Nov 6-8, 1995. Stroudsburg: ACL, 1995: 237-248.

[99] GRISHMAN R. PROTEUS parser reference manual[Z]. PROTEUS Project Memorandum, 1986.

[100] YANGARBER R, GRISHMAN R. NYU: description of the Proteus/PET system as used for MUC-7 ST[C]//Proceedings of the 7th Message Understanding Conference, Fairfax,

Apr 29-May 1, 1998. Stroudsburg: ACL, 1998.
[101] KAMBHATLA N. Combining lexical, syntactic, and semantic features with maximum entropy models for extracting relations[C]//Proceedings of the 42nd Annual Meeting of the Association for Computational Linguistics, Barcelona, Jul 21-26, 2004. Stroudsburg: ACL, 2004.
[102] ZHOU G D, SU J, ZHANG J, et al. Exploring various knowledge in relation extraction[C]//Proceedings of the 43rd Annual Meeting of the Association for Computational Linguistics, Ann Arbor, Jun 25-30, 2005. Stroudsburg: ACL, 2005: 427-434.
[103] SUN X, DONG L. Feature-based approach to Chinese term relation extraction[C]//Proceedings of the 2019 International Conference on Signal Processing Systems, Singapore, May 15-17, 2009. Washington: IEEE Computer Society, 2009: 410-414.
[104] JONES C L, BRIDGES R A, HUFFER K M T, et al. Towards a relation extraction framework for cyber-security concepts[C]//Proceedings of the 10th Annual Cyber and Information Security Research Conference, Oak Ridge, Apr 7-9, 2015. New York: ACM, 2015: 1-4.
[105] BANKO M, CAFARELLA M J, SODERLAND S, et al. Open information extraction from the web[C]//Proceedings of the 20th International Joint Conference on Artificial Intelligence, Hyderabad, Jan 6-12, 2007: 2670-2676.
[106] 李涛. 威胁情报知识图谱构建与应用关键技术研究[D]. 郑州: 中国人民解放军战略支援部队信息工程大学, 2020.
LI T. Research on key technologies for construction and application of threat intelligence knowledge graph[D]. Zhengzhou: PLA Strategic Support Force Information Engineering University, 2020.
[107] PINGLE A, PIPLAI A, MITTAL S, et al. RelExt: relation extraction using deep learning approaches for cybersecurity knowledge graph improvement[C]//Proceedings of the 11th IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, Vancouver, Aug 27-30, 2019. New York: ACM, 2019: 879-886.
[108] MITTAL S, DAS P K, MULWAD V, et al. CyberTwitter: using twitter to generate alerts for cybersecurity threats and vulnerabilities[C]//Proceedings of the 2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, San Francisco, Aug 18-21, 2016. Piscataway: IEEE, 2016: 860-867.
[109] WU S, HE Y. Enriching pre-trained language model with entity information for relation classification[C]//Proceedings of the 28th ACM International Conference on Information and Knowledge Management, Beijing, Nov 3-7, 2019. New York: ACM, 2019: 2361-2364.
[110] SARHAN I, SPRUIT M. Open-CyKG: an open cyber threat intelligence knowledge graph[J]. Knowledge-Based Systems, 2021, 233: 107524.
[111] SOARES L B, FITZGERALD N, LING J, et al. Matching the blanks: distributional similarity for relation learning[C]//Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics, Florence, Jul 28-Aug 2, 2019. Stroudsburg: ACL, 2019: 2895-2905.
[112] WAN Z, CHENG F, MAO Z, et al. GPT-RE: in-context learning for relation extraction using large language models[C]//Proceedings of the 2023 Conference on Empirical Methods in Natural Language Processing, Singapore, Dec 6-10, 2023. Stroudsburg: ACL, 2023:3534-3547.
[113] LI Q, JI H. Incremental joint extraction of entity mentions and relations[C]//Proceedings of the 52nd Annual Meeting of the Association for Computational Linguistics, Baltimore, Jun 22-27, 2014. Stroudsburg: ACL, 2014: 402-412.
[114] MIWA M, SASAKI Y. Modeling joint entity and relation extraction with table representation[C]//Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing, Doha, Oct 25-29, 2014. Stroudsburg: ACL, 2014: 1858-1869.
[115] MIWA M, BANSAL M. End-to-end relation extraction using LSTMs on sequences and tree structures[C]//Proceedings of the 54th Annual Meeting of the Association for Computational Linguistics, Berlin, Aug 7-12, 2016. Stroudsburg: ACL, 2016: 1105-1116.
[116] 谢博. 基于深度学习的中文网络威胁情报信息抽取技术研究[D]. 贵阳: 贵州大学, 2022.
XIE B. Research on information extraction technology of Chinese network threat intelligence based on deep learning [D]. Guiyang: Guizhou University, 2022.
[117] WANG Y, YU B, ZHANG Y, et al. TPLinker: single-stage joint extraction of entities and relations through token pair linking[C]//Proceedings of the 28th International Conference on Computational Linguistics, Barcelona, Dec 8-13, 2020: 1572-1582.
[118] YAN Z, ZHANG C, FU J, et al. A partition filter network for joint entity and relation extraction[C]//Proceedings of the 2021 Conference on Empirical Methods in Natural Language Processing, Punta Cana, Nov 7-11, 2021. Stroudsburg: ACL, 2021: 185-197.
[119] MINTZ M, BILLS S, SNOW R, et al. Distant supervision for relation extraction without labeled data[C]//Proceedings of the Joint Conference of the 47th Annual Meeting of the ACL and the 4th International Joint Conference on Natural Language Processing of the AFNLP, Singapore, Aug 2-7, 2009. Stroudsburg: ACL, 2009: 1003-1011.
[120] RIEDEL S, YAO L, MCCALLUM A. Modeling relations and their mentions without labeled text[C]//Proceedings of the 2010 European Conference on Machine Learning and Knowledge Discovery in Databases, Barcelona, Sep 20-24, 2010. Berlin, Heidelberg: Springer, 2010: 148-163.
[121] HOFFMANN R, ZHANG C, LING X, et al. Knowledge-

based weak supervision for information extraction of overlapping relations[C]//Proceedings of the 49th Annual Meeting of the Association for Computational Linguistics: Human Language Technologies, Portland, Jun 19-24, 2011. Stroudsburg: ACL, 2011: 541-550.

[122] SURDEANU M, TIBSHIRANI J, NALLAPATI R, et al. Multi-instance multi-label learning for relation extraction [C]//Proceedings of the 2012 Joint Conference on Empirical Methods in Natural Language Processing and Computational Natural Language Learning, Jeju Island, Jul 12-14, 2012. Stroudsburg: ACL, 2012: 455-465.

[123] ZENG D, LIU K, CHEN Y, et al. Distant supervision for relation extraction via piecewise convolutional neural networks[C]//Proceedings of the 2015 Conference on Empirical Methods in Natural Language Processing, Lisbon, Sep 17-22, 2015. Stroudsburg: ACL, 2015: 1753-1762.

[124] 王会勇, 安康, 张晓明. 结合领域先验词汇的远程监督关系抽取模型[J]. 计算机应用与软件, 2022, 39(8): 34-43.
WANG H Y, AN K, ZHANG X M. Distant supervision relation extraction model combined with domain priori words[J]. Computer Applications and Software, 2022, 39(8): 34-43.

[125] SHEN G, WANG W, MU Q, et al. Data-driven cybersecurity knowledge graph construction for industrial control system security[J]. Wireless Communications and Mobile Computing, 2020: 1-13.

[126] VASHISHTH S, JOSHI R, PRAYAGA S S, et al. Reside: improving distantly-supervised neural relation extraction using side information[C]//Proceedings of the 2018 Conference on Empirical Methods in Natural Language Processing, Brussels, Oct 31- Nov 4, 2018. Stroudsburg: ACL, 2018: 1257-1266.

[127] MOREIRA J, OLIVEIRA C, MACEDO D, et al. Distantly-supervised neural relation extraction with side information using BERT[C]//Proceedings of the 2020 International Joint Conference on Neural Networks Held as Part of the IEEE World Congress on Computational Intelligence, Glasgow, Jul 19-24, 2020. Piscataway: IEEE , 2020: 1-7.

[128] ALT C, HUEBNER M, HENNIG L, et al. Fine-tuning pre-trained transformer language models to distantly supervised relation extraction[C]//Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics, Florence, Jul 28-Aug 2, 2019. Stroudsburg: ACL, 2019: 1388-1398.

[129] CHRISTOU D, TSOUMAKAS G. Improving distantly-supervised relation extraction through BERT-based label and instance embeddings[J]. IEEE Access, 2021, 9: 62574-62582.

[130] LI R, YANG C, LI T, et al. MiDTD: a simple and effective distillation framework for distantly supervised relation extraction[J]. ACM Transactions on Information Systems, 2022, 40(4): 1-32.

[131] KIM G, LEE C, JO J, et al. Automatic extraction of named entities of cyber threats using a deep Bi-LSTM-CRF network[J]. International Journal of Machine Learning and Cybernetics, 2020, 11(10): 2341-2355.

[132] LIM S K, MUIS A O, LU W, et al. MalwareTextDB: a database for annotated malware articles[C]//Proceedings of the 55th Annual Meeting of the Association for Computational Linguistics, Vancouver, Jul 31- Aug 5, 2017. Stroudsburg: ACL, 2017: 1557-1567.

常钰(1997—),男,山西忻州人,硕士研究生,主要研究方向为网络安全知识图谱、威胁情报分析等。
CHANG Yu, born in 1997, M.S. candidate. His research interests include cyber security knowledge graph, threat intelligence analysis, etc.

王钢(1971—),男,辽宁瓦房店人,硕士,正高级工程师,硕士生导师,CCF会员,主要研究方向为计算机网络、网络与信息安全等。
WANG Gang, born in 1971, M.S., senior engineer, M.S. supervisor, CCF member. His research interests include computer networks, networks and information security, etc.

朱鹏(1999—),男,浙江金华人,硕士研究生,主要研究方向为加密流量分析、异常流量检测等。
ZHU Peng, born in 1999, M.S. candidate. His research interests include encrypted traffic analysis, abnormal traffic detection, etc.

孔令飞(1997—),男,安徽亳州人,硕士研究生,主要研究方向为自然语言处理、知识问答等。
KONG Lingfei, born in 1997, M.S. candidate. His research interests include natural language processing, knowledge question and answer, etc.

何京恒(2001—),男,河南南阳人,硕士研究生,主要研究方向为网络安全攻击溯源、威胁情报分析等。
HE Jingheng, born in 2001, M.S. candidate. His research interests include cyber security attacks tracing, threat intelligence analysis, etc.