DDoS 攻击恶意行为知识库构建

刘飞扬，李坤，宋飞，周华春
（北京交通大学电子信息工程学院，北京 100044）

摘　要：针对分布式拒绝服务（distributed denial of service，DDoS）网络攻击知识库研究不足的问题，提出了DDoS 攻击恶意行为知识库的构建方法。该知识库基于知识图谱构建，包含恶意流量检测库和网络安全知识库两部分：恶意流量检测库对 DDoS 攻击引发的恶意流量进行检测并分类；网络安全知识库从流量特征和攻击框架对 DDoS 攻击恶意行为建模，并对恶意行为进行推理、溯源和反馈。在此基础上基于 DDoS 开放威胁信号（DDoS open threat signaling，DOTS）协议搭建分布式知识库，实现分布式节点间的数据传输、DDoS 攻击防御与恶意流量缓解功能。实验结果表明，DDoS 攻击恶意行为知识库能在多个网关处有效检测和缓解 DDoS 攻击引发的恶意流量，并具备分布式知识库间的知识更新和推理功能，表现出良好的可扩展性。

关键词：DDoS；分布式；知识图谱；恶意行为知识库
中图分类号：TP393
文献标识码：A
doi: 10.11959/j.issn.1000−0801.2021257

Construction of DDoS attacks malicious behavior knowledge base construction

LIU Feiyang, LI Kun, SONG Fei, ZHOU Huachun
School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing 100044, China

Abstract: Aiming at the problem of insufficient research on the knowledge base of distributed denial of service (DDoS) network attacks, a method for constructing a knowledge base of DDoS attacks malicious behavior was proposed. The knowledge base was constructed based on the knowledge graph, and contains two parts: a malicious traffic detection database and a network security knowledge base. The malicious traffic detection database detects and classifies malicious traffic caused by DDoS attacks, the network security knowledge base detects DDoS attacks from traffic characteristics and attack frameworks model malicious behaviors, and perform inference, tracing and feedback on malicious behaviors. On this basis, a distributed knowledge base was built based on the DDoS open threat signaling (DOTS) protocol to realize the functions of data transmission between distributed nodes, DDoS attack defense, and malicious traffic mitigation. The experimental results show that the DDoS attack malicious behavior knowledge base can effectively detect and mitigate the malicious traffic caused by DDoS attacks at multiple gateways, and has the knowledge update and reasoning function between the distributed knowledge bases, showing good scalability.

Key words: DDoS, distributed, knowledge graph, malicious behavior knowledge base

收稿日期：2021−08−12；修回日期：2021−11−15
基金项目：国家重点研发计划项目（No.2018YFA0701604）
Foundation Item: The National Key Research and Development Program of China (No.2018YFA0701604)

1 引言

分布式拒绝服务（distributed denial of service，DDoS）是目前针对网络应用程序最具破坏力的攻击之一[1]。5G 支持的海量终端设备接入使其受到的安全威胁进一步提升。为了应对不断发展的网络攻击，设计了一系列的网络安全数据集，如 KDDCup99 、 NSL-KDD 、 UNSW-NB15 、 CICDDoS2019 等，这些数据集为了反映现实网络的复杂性，都设计成包含正常数据和异常数据的综合数据集，但仍存在不足之处：这些数据集都以流量数据的形式存储，淡化了网络实体间的关系，难以描述网络攻击者的攻击行为和特征。因此，如何将网络现有的海量数据与知识进行规范化和集成化，设计出一个针对 DDoS 网络攻击的知识库成为了亟待解决的问题。

目前 DDoS 攻击检测方法主要有两种：一种是基于机器学习和神经网络的攻击检测方法[2]，通过分析正常流量与攻击流量在特征方面的差异来检测攻击；另一种是基于统计的检测方法[3]，对正常的网络流量进行建模，通过对比当前网络流量与正常流量模型之间的相似程度来检测攻击。现有的这些方法或基于已有的数据集检测算法，或利用常规统计模型，难以适应不断变化的 DDoS 攻击，并需要随攻击的变化调整模型和阈值等参数，难以动态适配网络攻击的变化。

网络攻击呈现复杂化和组合化的趋势，传统的流量信息难以适用于网络攻击的分析，因此需要结构化的知识体系描绘网络攻击的特征和属性，对网络攻击进行实体关系建模。随着网络知识呈指数增长，越来越多的研究人员开始使用知识图谱管理这些知识[4]。知识图谱将人类知识结构化形成系统，其中包含基本的知识、通用的规则以及其他结构化的信息，具有信息检索、推演决策等功能。从结构上看，知识图谱就是“实体–关系–实体”的三元组组成的一种带标记的有向属性图形。因其优秀的检索功能、高效的结构化存储功能、自适应的更新功能等特点受到了研究人员的关注。但现有的网络安全知识库，例如攻击类型枚举和分类数据库（common attack pattern enumeration and classification，CAPEC）、通用漏洞披露（common vulnerabilities andexposures，CVE）和常见缺陷列表（common weakness enumeration，CWE）等[5]关于 DDoS 攻击的记录较少。此外，关于分布式知识库的构建研究则更少。因此上述知识库面对海量知识表现出交叉的扩展性，无法提供系统的 DDoS 攻击知识。

为检测并缓解 DDoS 攻击，需要有不断更新的知识来做支撑。因此，本文基于知识图谱的概念构建了 DDoS 攻击恶意行为知识库。该知识库以知识图谱的形式存储了 DDoS 攻击行为的各种特征以及第三方数据库中的知识，并构建了一套知识库更新、推理和反馈的系统，用于在复杂多变的网络环境下的多个网关处识别出攻击者行为，提供缓解措施，降低 DDoS 攻击引发的恶意流量强度。

本文的主要贡献有以下 3 点。

（1）提出 DDoS 攻击恶意行为知识库模型，设计 5 种知识图谱的数据结构模型，导入结构化数据构建 DDoS 攻击恶意行为知识库。

（2）设计知识图谱间交互接口，实现图谱数据传输、更新、推理和反馈功能；结合图数据库构建知识图谱实现可视化表达与查询功能。

（3）基于分布式拒绝服务开放威胁信号（DDoS open threat signaling，DOTS）协议构建分布式知识库，实现知识库间通信，并探讨了分布式知识库在恶意流量检测与防御方面的应用场景。

2 研究现状

近些年将机器学习运用到 DDoS 攻击检测的研究取得了很多进展[6]，相比之下，利用知识图

谱技术构建知识库检测 DDoS 攻击以及面向 DDoS 攻击的分布式知识库构建的研究还处于初级阶段。

在网络安全知识图谱构建方向有很多研究。在网络安全本体构建方面，文献[7]阐述了一个分层次、由许多模块化子本体组成的网络安全本体论，从抽象到具体地分为了上层、中层和领域本体。文章提出了分层的本体框架，但并未具体定义领域本体中的概念。在知识推理方面，文献[8]论述了知识图谱的 3 类推理方法：基于规则的推理、基于分布式表示的推理和基于神经网络的推理，同时还探讨了知识图谱推理的问答、查询和关联分析的应用场景。在知识图谱可视化方面，文献[9]阐述了知识图谱可视表达的 4 种基本方法：空间填充、节点链接图、热图和邻接矩阵，并从数据检索、图构建、度量计算、布局和渲染 5 个阶段说明了大规模知识图谱可视化的方法。在 DDoS 攻击检测方面，文献[10]将知识图谱应用在 DDoS 检测中，从网络流量中抽取信息构成知识图谱，利用知识图谱描述两个主机之间的交互关系，然后通过对关系的分析检测出 DDoS 攻击源。

上述文献大多构建了新的网络安全本体和网络安全框架，并按照从网络安全知识图谱子系统到可视化子系统的顺序构建，缺乏在特定领域的适用性，因此对 DDoS 攻击这种需要对流量数据分析的模型没有很好地适配，针对 DDoS 攻击的知识图谱和知识库框架需要从流量数据开始分析建模。

此外，各种与网络安全知识图谱相关的平台也逐渐受到网络安全人员的关注。开放网络威胁情报平台（open cyber threat intelligence platform，OpenCTI）是一个开源平台，其基于结构化威胁信息表达（structured threat information expression，STIX）标准和攻击行为知识库模型（adversarial tactics, techniques, and common knowledge，ATT&CK）框架开发了网络威胁情报知识和可观察量，目的在于构造、存储、组织与可视化有关网络威胁情报的技术和非技术信息；开源威胁情报共享平台（malware information sharing platform，MISP）是一种开源软件，用于收集、存储、分发和共享有关网络安全事件分析和恶意软件分析的网络安全指标和威胁。但其数据导入受限于 STIX2.0 标准格式，并且其本体面向较高层的网络安全范畴，并未涉及底层的数据包数据等信息；而图数据库 Neo4j[11]具有高性能的图引擎，能够快速构建知识图谱，支持多种格式的数据导入和导出，是目前知识库图谱可视化使用最广泛的平台，因此将其作为本文的知识图谱构建工具。

目前的网络安全知识图谱和知识库构建工作大多集中在单点部署方案，无法适用大型网络结构。而分布式系统因其开放和灵活的体系结构等特点成为了现在网络的通用设计方案。分布式数据库拥有强大的可扩展性和透明性，能有效地提高数据传输的效率，同时缓解单个数据库的负载[12]。分布式数据库主要性能优化在于每个数据库可以存储相对较少的数据，执行一部分的任务，相对于单个数据库能够减少数据查找和读取时间，降低数据库负荷；但分布式数据库也存在数据库之间通信不安全、数据传输效率低等问题，因此，选择一种合适的安全传输协议是解决数据传输安全性的关键问题。

目前，DDoS 检测系统存在以下两点不足。

（1）传统检测方法只针对一种或几种 DDoS 攻击进行检测和分类，对细分类的 DDoS 攻击的检测和分类精确率不高；

（2）机器学习和神经网络的方法难以感知真实的网络结构与攻击完整路径，对于层出不穷的新型 DDoS 攻击的检测适配性较差。

针对以上不足，本文提出分布式 DDoS 攻击恶意行为知识库，其构建流程如图 1 所示。基于集成学习和神经网络等算法对细分类的 DDoS 攻击进行特征提取和检测，生成存储检测 DDoS 攻

击结果的恶意流量检测库；分析 DDoS 攻击的路径和特征，构建行为知识图谱攻击行为库，并基于图算法、聚类算法以及攻击溯源推理等方法实现恶意行为感知和分类，构建网络安全知识库；基于 DOTS 协议构建分布式知识库，实现分布式节点间的知识更新和交互功能，通过实验验证分布式知识库的数据传输性能和对 DDoS 检测的能效，并对知识库应用场景进行了设想。

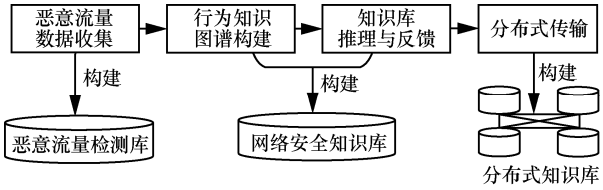

图 1　分布式 DDoS 攻击恶意行为知识库构建流程

3　知识库构建

DDoS 攻击恶意行为知识库结构如图 2 所示，由恶意流量检测库和网络安全知识库两部分组成。恶意流量检测库用于收集和存储来自检测模块的不同种类 DDoS 攻击流量数据，为网络安全知识库提供结构化的数据；网络安全知识库负责收集第三方异构数据库、构建网络攻击行为库、知识图谱推理、知识库反馈等工作[13]。

DDoS 攻击恶意行为知识库基于知识图谱构建，以三元组的形式构建，如式（1）所示。

$$\mathrm{KG}=\langle E,R,P\rangle \tag{1}$$

其中，$E=\{e_1,e_2,e_3,\cdots,e_i\}$ 表示知识图谱中实体的集合，是知识图谱存储对象的具体表示，共包含 i 种不同的实体；$R=\{r_1,r_2,r_3,\cdots,r_j\}$ 表示知识图谱中关系的集合，是知识图谱关联对象的具体表示，共包含 j 种不同的关系；$P=\{p_1,p_2,p_3,\cdots,p_n\}$ 表示知识图谱中属性的集合，是知识图谱存储数据的具体表示，每种实体 e 或关系 p 都可能拥有不同的 n 个属性。

3.1　恶意流量检测库

恶意流量检测库收集并存储原型系统中生成的实验数据，包括正常流量、DDoS 攻击恶意流量、

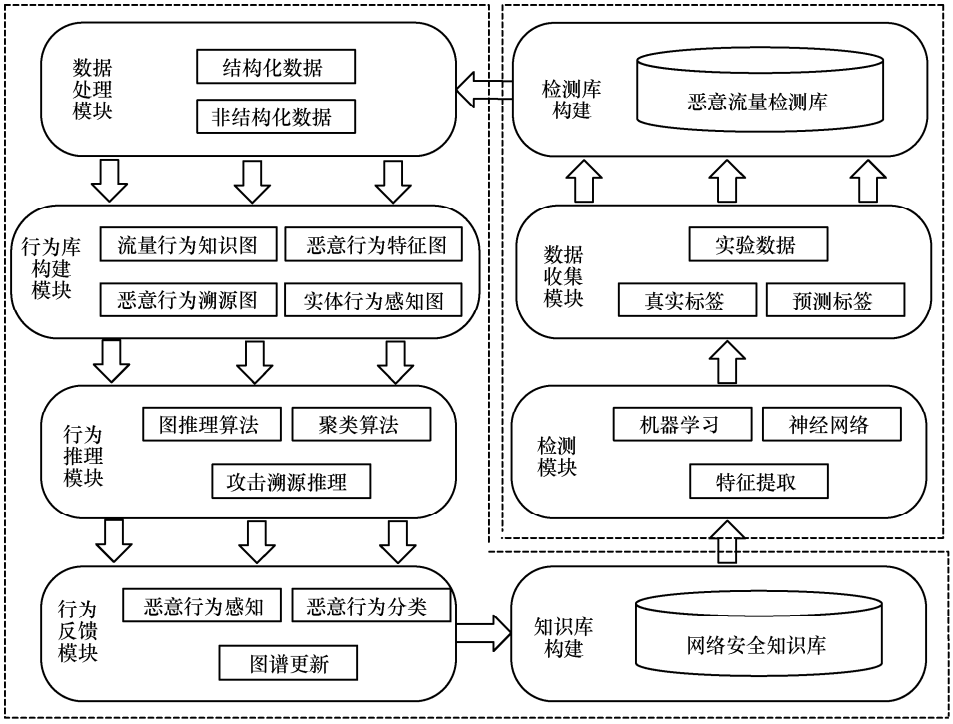

图 2　DDoS 攻击恶意行为知识库结构

真实标签和预测标签，并对同一流量的数据和标签进行整合，生成带有两种标签的流量数据。

恶意流量检测库以知识图谱的形式存储恶意流量数据并构建检测图谱，其图谱三元组构成见表 1。知识图谱主要由实体、关系和属性 3 部分组成，实体是最主要的元素，代表数据的集合体；属性包含属性名称和属性值，属性名称代表对象具有的特点和特征，属性值为对应属性所指定的值；关系用于连接两个实体，代表实体之间的关联性。

表 1　恶意流量检测图谱三元组构成

实体	属性	关系
DDoS 攻击流节点	流量特征名称、特征值	真实标签
		预测标签
攻击类型节点	攻击类型名称	真实标签
		预测标签

首先，经过检测模块的 CICFlowMeter 流量特征提取工具后生成 84 个流特征数据，检测图谱创建流量节点实体和攻击类型实体，将 84 种流特征作为流量节点实体的属性来存储数据；然后，构建真实标签和预测标签来连接流量节点实体和攻击类型实体。其中，真实标签表示所连接的流量节点实体的真实攻击类型；预测标签表示所连接的流量节点实体通过检测模块检测后被标记的攻击类型。恶意流量检测知识图谱将数据存储为实体的属性并构建流量数据与攻击类型之间的关系，用于统计和计算检测模块的检测精确率，并向检测模块反馈检测精确率较低的攻击类型信息。

3.2　网络安全知识库

网络安全知识库是 DDoS 攻击恶意行为知识库中最为核心的部分，包含了数据源处理模块、恶意行为知识库构建模块、行为推理模块和行为反馈模块，负责数据结构化处理、恶意行为知识图谱构建、行为推理和反馈的工作。

数据处理模块主要从与网络安全相关的第三方数据库获取与 DDoS 攻击相关的信息并整合为统一的结构化数据，作为网络安全知识库的数据补充和信息支持。

行为库构建模块基于DDoS攻击的攻击路径、攻击时序、攻击流特征和攻击行为分别构建了实体行为感知图、恶意行为溯源图、恶意行为特征图和流量行为知识图 4 张知识图谱；并定义了图谱之间的交互接口，实现数据的互通和输入、输出。

行为推理模块利用图推理算法和攻击溯源推理算法对实体行为感知图和恶意行为溯源图进行推理，为攻击主机溯源和攻击主机位置感知提供依据；利用聚类算法对不同种类 DDoS 攻击的特征进行筛选。

行为反馈模块将 4 张知识图谱输出信息进行反馈，实体行为感知图将网络环境中的正常流量和攻击流量一并反馈给检测模块进行 DDoS 攻击的检测；恶意行为特征图将筛选过后的不同种类 DDoS 攻击对应的特征反馈给检测模块以提高检测精确率；恶意行为溯源图接受检测模块检测的 DDoS 攻击信息，对攻击进行溯源推理；流量行为知识图则为整个知识库提供相应的 DDoS 攻击缓解措施等信息。

3.3　恶意行为知识图谱

如图 3 所示，构成恶意行为知识库的 4 张知识图谱有不同的功能，承担不同的任务并能够相互反馈、相互作用。

（1）流量行为知识图

该图主要负责恶意行为知识库中第三方知识的存储和更新，包含了网络安全领域的各类攻击库、漏洞库与弱点库。将这些库中的攻击、漏洞和弱点统一格式化并相互关联，从而形成流量行为感知图。将不断更新和丰富的第三方数据库作为知识储备，流量行为感知图不仅能为恶意行为知识库提供先验的攻击和漏洞知识，还能提供不

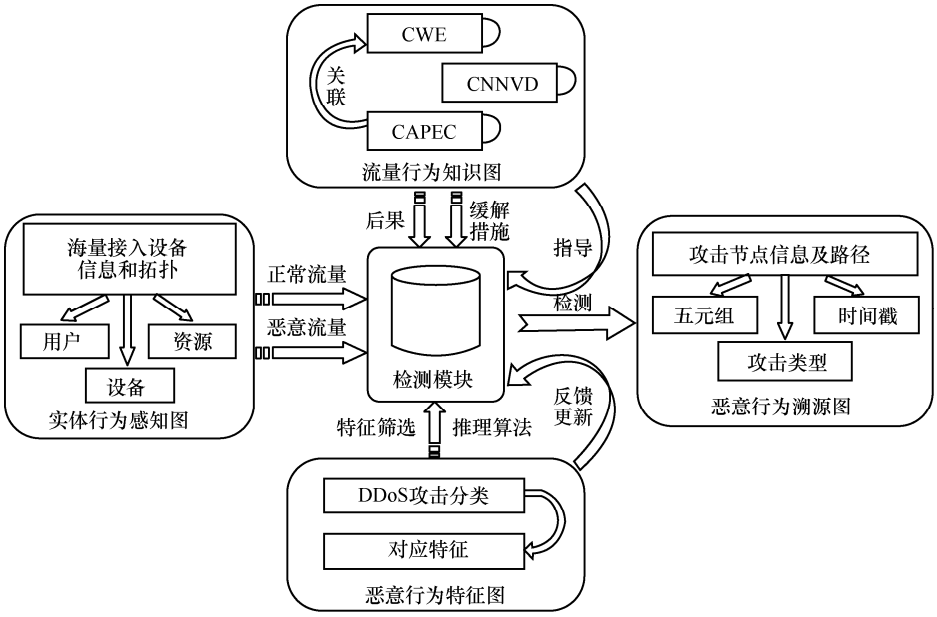

图 3　恶意行为知识库构建

同攻击产生的后果影响以及针对不同攻击的缓解措施，从而不断更新和扩展恶意行为知识库的知识，动态适配 DDoS 攻击的快速变化。

（2）恶意行为特征图

该图主要负责 DDoS 攻击的细致化分类和特征匹配，并能协助实现攻击类型识别和攻击路径检测等功能。该图包含了 5 类 DDoS 攻击、总计 21 种 DDoS 攻击类型以及基于 CICFlowMeter 和统计方法提取的与 21 种攻击类型有较高相关性的 69 种流量特征。作为 DDoS 攻击类型和特征的映射图，它能够直观地展示不同流量特征的重要性和不同 DDoS 攻击类型的特征对应情况，并能通过特征筛选或中心度算法提取不同 DDoS 攻击类型中影响力更大的流量特征，将这些特征反馈给检测模块以调整 DDoS 攻击检测策略，协助检测模块提升检测能力。

（3）实体行为感知图

该图用于感知整个网络的拓扑环境。海量设备的接入导致了网络拓扑的复杂化，也为网络攻击分析提供了更多的信息。该图存储了网络拓扑中连接到接入网关的各个主机的五元组信息。针对使用广泛分布主机发起的 DDoS 攻击，实体行为感知图基于检测模块的反馈能够快速定位攻击主机的位置和该攻击发起的方式、路径等信息，从而指导恶意行为溯源等功能。

（4）恶意行为溯源图

该图主要负责攻击的溯源工作。基于前 3 张图谱中的反馈和检测模块的流量信息对攻击进行溯源，该图谱能够发掘攻击的完整路径以及攻击所使用的恶意操作和漏洞等信息。该图谱包含了攻击发起到结束时间段中攻击主机和被攻击主机的五元组信息和使用的攻击类型等信息，使用这些信息模拟一次攻击的全过程，然后对输入的流量进行检测，从而识别攻击并溯源到攻击发起的主机。通过检测攻击发起到结束的完整路径，能够指导攻击防御软件对攻击路径中的薄弱环节进行针对性打击并采取相应的缓解措施降低后续的恶意流量强度。

上述 4 张知识图谱都设计了专门的数据导入和导出接口实现图谱间的数据交互。数据导入接口基于本知识图谱特定的数据模型构建导入规则，将导入数据处理为结构化数据，使得导入的数据能正确地匹配知识图谱的数据模型；数据导

出接口基于本知识图谱功能以及其他知识图谱所需信息构建导出模型，与其他知识图谱的数据导入接口对接，进而实现知识图谱数据交互。

恶意行为知识库的主体为上述 4 张知识图谱及其接口构成的恶意行为知识图谱。在数据层面上，4 张图谱包含了各自定义的数据结构以及基于数据结构存储的结构化流量数据；在知识层面上，4 张图谱包含了 DDoS 攻击在时间维度、空间维度和特征维度的多元信息。因此，基于上述知识图谱构建的 DDoS 攻击恶意行为知识库能够对 DDoS 攻击进行全面的描述，进而防御和缓解 DDoS 攻击产生的恶意流量。

3.3.1　流量行为知识图

该图谱基于恶意行为本体收集各类知识库信息（ATT&CK、CAPEC、CNNVD、CWE 等）作为恶意行为基础知识的补充。其图谱的三元组构成见表 2。

表 2　流量行为知识图谱三元组构成

实体	属性	关系
CAPEC 节点	攻击名称、攻击 ID、攻击危害、攻击后果、缓解措施、严重程度	攻击间级别 弱点利用
CWE 节点	弱点名称、弱点描述、弱点危害、缓解措施	弱点间级别 攻击关联
CNNVD 节点	漏洞名称、漏洞描述、漏洞危害、缓解措施	漏洞间级别

流量行为知识图主要是第三方数据库中的知识数据，包含各类攻击库，如 ATT&CK、CAPEC 以及各类枚举库，如 CWE、CVE、国家信息安全漏洞库（china national vulnerability database of information security，CNNVD）等。这些知识库的构建依赖专家经验、威胁情报的收集、验证，所抽象的概念和关系是通用的建模基础。

流量行为知识图的构建能够提供特定环境和场景（如 DDoS 攻击）下恶意行为的关联知识，评估恶意行为的影响范围和深度，对这些恶意行为做出预警，并给出相应的缓解措施。这些第三方数据库中也包含了很多相互关联的信息，通过将第三方数据库的知识数据抽取，导入数据库中并构建知识图谱，并通过关系推理的方式对知识图进行扩展，从而构建成一个包含各种关联的攻击、漏洞的知识图谱。

流量行为知识图的数据导入接口从第三方数据库获取数据并修改数据结构以满足该图谱的导入规则；数据导出接口根据查询对象输出对应的攻击、漏洞和弱点等信息。

3.3.2　恶意行为特征图

该图谱基于 DDoS 攻击和恶意行为，通过流量特征提取工具 CICFlowMeter 转换成的数据特征集，基于阈值或统计方法归纳影响各类攻击的重要特征并存储，是攻击类型识别与攻击路径检测的重要依据。其图谱的三元组构成见表 3。

表 3　恶意行为特征图谱三元组构成

实体	属性	关系
DDoS 攻击	DDoS 攻击描述	关联攻击方式
攻击方式	5 类攻击方式描述	关联攻击类型
攻击类型	21 种攻击类型描述	关联流量特征
流量特征	69 种流量特征描述	对应攻击类型

恶意行为特征图采用分级的方案将 DDoS 攻击类型细分成五大类，总计 21 种 DDoS 攻击类型，并通过统计方法确定 DDoS 攻击与流量特征的对应关系，从而建立恶意行为特征图。一方面展示了每种攻击与具体流量特征种类之间存在关联，另一方面体现了多种攻击类型受一种流量特征的影响，简化了流量特征的处理难度。此外，以 ID 为索引，在流量特征实体中存储了每条流量的具体特征值，以用于基于特征的攻击检测等方案。

恶意行为特征图的主要作用是统计 21 种 DDoS 攻击类型所对应的流量特征，这些对应关系来自于恶意流量检测库，是使用机器学习阈值和多分类方法的结果。将这些对应关系作为先验知

识，运用统计方法检测未标签流量的攻击类型。恶意行为特征图是知识库对 DDoS 攻击恶意流量识别、归类、响应和溯源的前提，应用已知的行为特征对输入流量进行检测识别，并调用流量行为知识图中的攻击和漏洞等信息，对检测出的 DDoS 攻击类型给出相应的缓解措施。检测结果也能作为恶意行为溯源图的推理依据，用于攻击路径的提取等。

恶意行为特征图与检测模块直接相连，其数据导入接口用于导入 DDoS 攻击类型与流量特征的对应关系；数据导出接口用于导出图算法更新后的对应关系。

3.3.3 恶意行为溯源图

该图谱以知识图谱的形式记录一次攻击发起到结束的过程，包含了攻击者主机、被攻击者主机、攻击方式以及时间戳等实体。其图谱的三元组构成见表 4。

表 4 恶意行为溯源图谱三元组构成

实体	属性	关系
攻击时间点	开始时间、结束时间	指向攻击主机
攻击类型	攻击类型描述	指向攻击主机
攻击主机	IP 地址、端口号、协议	指向被攻击主机
被攻击主机	IP 地址、端口号、协议	连接攻击时间

恶意行为溯源图主要作用是对引起恶意流量的攻击行为进行追溯，追踪攻击数据的来源，定位攻击者。恶意行为溯源图中的 IP 地址、端口号、传输协议类型和时间段等信息作为溯源的样本可以用来分析、挖掘攻击源头。恶意行为特征图所提供的不同 DDoS 攻击的流量特征和恶意流量检测库所提供的第三方知识数据也能作为恶意行为溯源图的样本，分析 DDoS 攻击链利用的恶意操作和漏洞，从而更好地指导溯源图进行攻击行为的溯源。

恶意行为溯源图的数据导入接口基于其他图谱提供的攻击方和被攻击方具体信息，构建攻击时序图作为知识信息；数据导出接口根据需求选择性导出攻击方或被攻击方的五元组信息。

3.3.4 实体行为感知图

该图谱基于实验系统的拓扑环境构建，收集所有流经部署了行为知识库的接入路由器的流量信息，提取实时网络拓扑结构并存储。其图谱的三元组构成见表 5。

表 5 实体行为感知图谱三元组构成

实体	属性	关系
用户	用户名、群组、角色，权限	拥有设备
设备	设备名、IP 地址、端口号	属于用户、利用资源、访问结果
资源	资源名、IP 地址、端口号	使用协议

实体行为感知图记录与网络拓扑相关的信息，并对拓扑环境中的设备和用户添加多种属性和属性值来对设备和用户进行管理，进而控制设备和用户的接入。在收集到足够信息之后，实体行为感知图能够发掘攻击者使用设备的信息，并将攻击信息输出，进行 DDoS 攻击检测。

实体行为感知图的数据导入接口导入的数据为网络拓扑结构以及网络中用户和设备的属性；数据导出接口根据特定需求导出攻击者设备的属性信息。

3.4 知识库分布式构建方法

分布式拒绝服务开放威胁信号（DOTS）是用来承载有关受到 DDoS 攻击的网络资源或网络信息的协议。这些信息由多个 DOTS 客户端发送到一个或者多个 DOTS 服务器，对被识别为恶意流量的网络行为给出一个相应的缓解措施，因此作为分布式知识库间的安全传输协议。

DOTS 本体由服务器、客户端和客户端控制器 3 部分组成，服务器包含缓解措施数据库和数据收发模块，负责处理客户端请求并提供相应的缓解措施；客户端包含数据收、发模块，向服务器发送不同的请求；客户端控制器主要负责请求内容的编译，如请求保护的地址段，请求目标服

务器的地址等内容。DOTS 拥有信令和数据两种传输数据的信道，信令信道用于请求保护信息的传输，为 DOTS 客户端向服务器发送请求以及服务器相应请求时使用的信道；数据信道传递知识库数据和配置信息，是客户端发送知识库配置更新命令以及知识库之间数据交互时使用的信道。

基于 DOTS 构建的分布式知识库架构如图 4 所示，DOTS 客户端控制器为主要控制部分，DOTS 客户端为主要请求发送部分，DOTS 服务器为反馈提供部分并连接知识库。基于 yang-data 和 json 文件格式构建知识库数据传输模型，作为 DOTS 数据信道的标准数据传输格式，客户端传输知识库配置更新文件到服务器端，服务器解析配置更新文件并对知识库进行知识更新以及数据传输等操作。

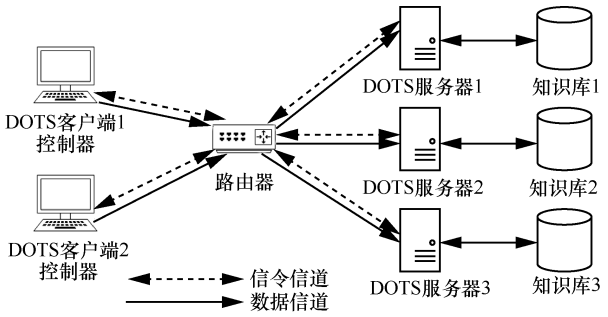

图 4　基于 DOTS 构建的分布式知识库架构

4　实验结果

本节进行了分布式 DDoS 攻击恶意行为知识库构建的实验，使用 Neo4j 图形数据库作为知识图谱构建工具和可视化工具，通过编写 Cypher 语句将知识信息插入知识图谱中；基于 DOTS 协议构建分布式知识库，进行知识库之间数据交互实验；探讨分布式知识库在 DDoS 攻击检测方面的应用场景。实验环境部署在 ESXi 配置的集群中，软件环境为 Ubuntu18.04。

4.1　知识图谱构建

知识图谱构建实验主要对恶意流量检测知识图谱和网络安全知识库中的 4 张知识图谱进行构建，编写基于 Cypher 语言的代码构建知识图谱的数据模型，导入部分数据构建知识图谱可视化节点和关系进行展示。

基于 Neo4j 图形数据库构建的知识图谱将数据模型进行可视化，以节点链接图的形式展示数据的结构和链接关系。Neo4j 包含的搜索引擎能根据需求针对性地查询相关数据并对选中的数据实体进行扩展，从而显示出所有关联数据。

基于 Neo4j Cypher API 和 JAVA 开发语言编写知识图谱数据导入接口和数据导出接口的脚本文件，实现知识图谱间的关键数据交互与关联查询。实验结果表明知识图谱能够正常进行数据导入和数据导出。

恶意流量检测图如图 5 所示，该图谱包含以下 3 部分的内容。

（1）DDoS 攻击流量节点

图 5 中显示为深灰色节点，每一个深灰色节点表示从检测模块中收集到的一条流信息，节点的属性包括 CICFlowMeter 输出的 84 种流特征、多分类器输出的预测该流量攻击类型的标签 Pre_label 和表示该流量真实攻击类型的标签 Real_label。

（2）攻击类型节点和正常流量节点

图 5 中显示为浅灰色的攻击类型节点和白色的正常流量节点，这两种节点包含了检测模块检测出的 19 种细分类的 DDoS 攻击类型和 1 种正常流量类型。这两种节点用来给深灰色的攻击流量节点分类。

（3）真实标签关系和预测标签关系

真实标签关系在图 5 中表示为 real 线，预测标签关系在图 5 中表示为 predict 线。这两种关系均由深灰色的 DDoS 攻击流节点指向浅灰色的攻击类型节点或白色的正常流量节点，用来指示存储的 DDoS 攻击流节点的预测类型和真实类型。恶意流量检测图的可视化显示能快速查询不同 DDoS 攻击类型在检测精确率和误判倾向上的信息。

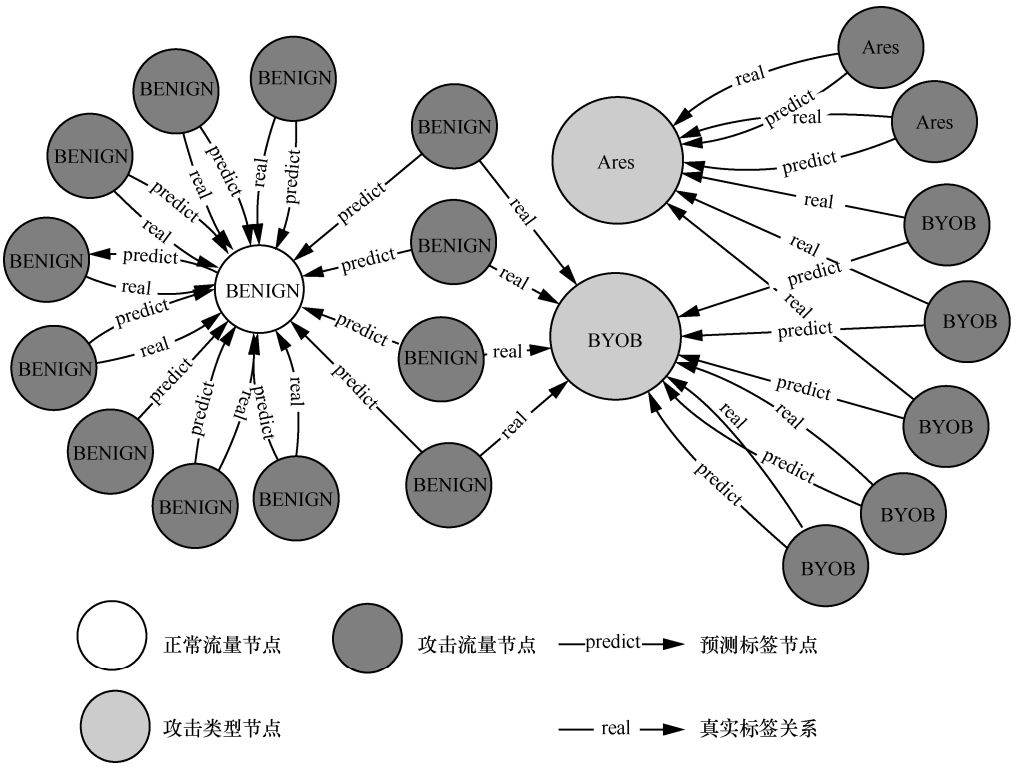

图 5　恶意流量检测图

流量行为知识图如图 6 所示，浅灰色节点表示 CAPEC 攻击类型，深灰色节点表示 CWE 弱点类型，并通过 Related_weakness 的关系链接在一起；每个实体都包含了名称、ID、描述、造成危害、缓解措施 5 种属性和属性值。在保留原有相关关系的基础上，基于攻击节点描述中关联的弱点名称创建关系来连接攻击节点和弱点节点，构建起攻击和弱点关联的知识图谱。在查询攻击和弱点时，都能关联查询到所有的连接关系。

恶意行为特征图存储了检测的 21 种 DDoS 攻击以及 69 种流量特征，以及实体之间的关系，如图 7 所示。图 7 中白色节点表示 DDoS 攻击，黑色节点表示 DDoS 攻击的 5 类攻击种类，浅灰色节点表示 5 类攻击种类各自包含的攻击方式总计 21 种，深灰色节点表示与攻击方式对应的重要流量特征。

恶意行为溯源图如图 8 所示，包含 4 种实体类型，分别为恶意节点、被攻击节点、恶意攻击类型以及时间段。恶意源节点包含其 IP 地址以及源端口号，它既指向恶意攻击类型，又指向被攻击节点，其关系属性中定义了传输协议的类型；被攻击节点同样包含其 IP 地址及其端口号。此外，所有主机节点均通过指向对应时间段，以便梳理攻击与时间的关系，展示攻击随时间的变化规律。

图 8 中深灰色节点表示攻击节点，白色节点表示被攻击节点，黑色节点表示深灰色攻击节点所使用的攻击方式，两个浅灰色节点分别表示攻击开始时间和攻击结束时间。整幅图描绘了攻击开始时间点，所用攻击节点调用 ACK Flooding 攻击方式对被攻击节点发起攻击，最后结束攻击的全过程。

4.2　数据收集与导入

知识库有两部分数据来源，一部分是基于系统生成攻击流量和正常流量，另一部分是第三方网络安全数据库导入的信息。

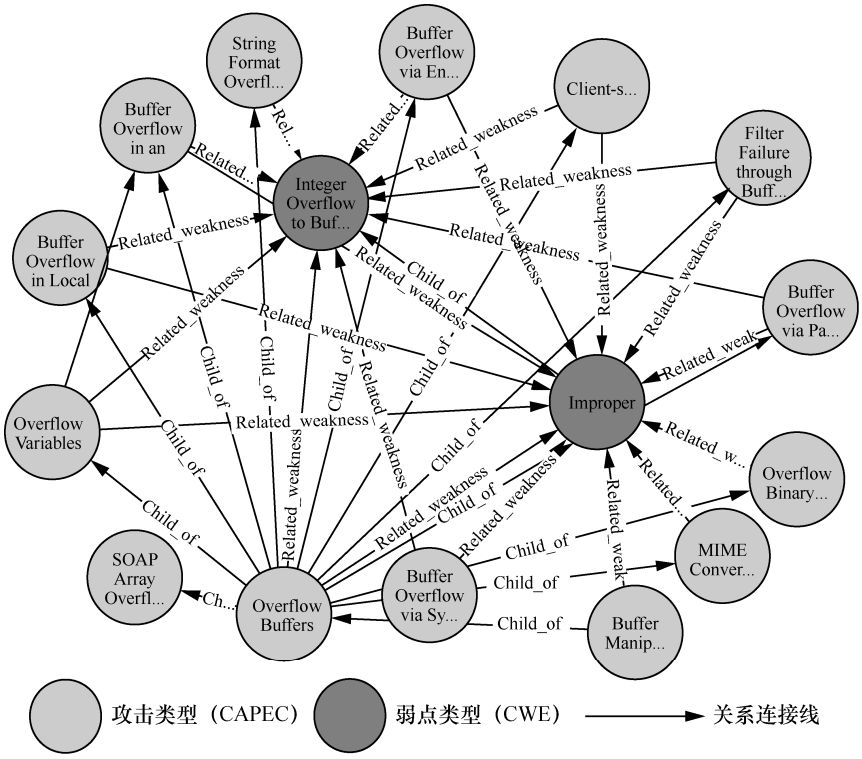

图 6　流量行为知识图

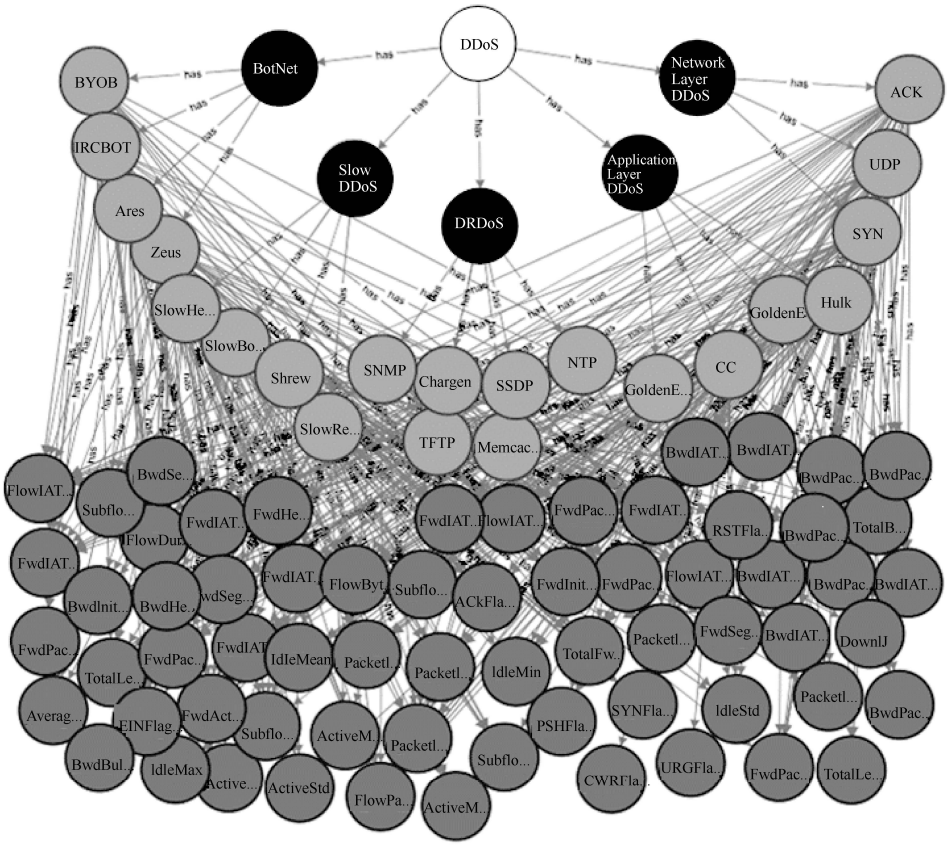

图 7　恶意行为特征图

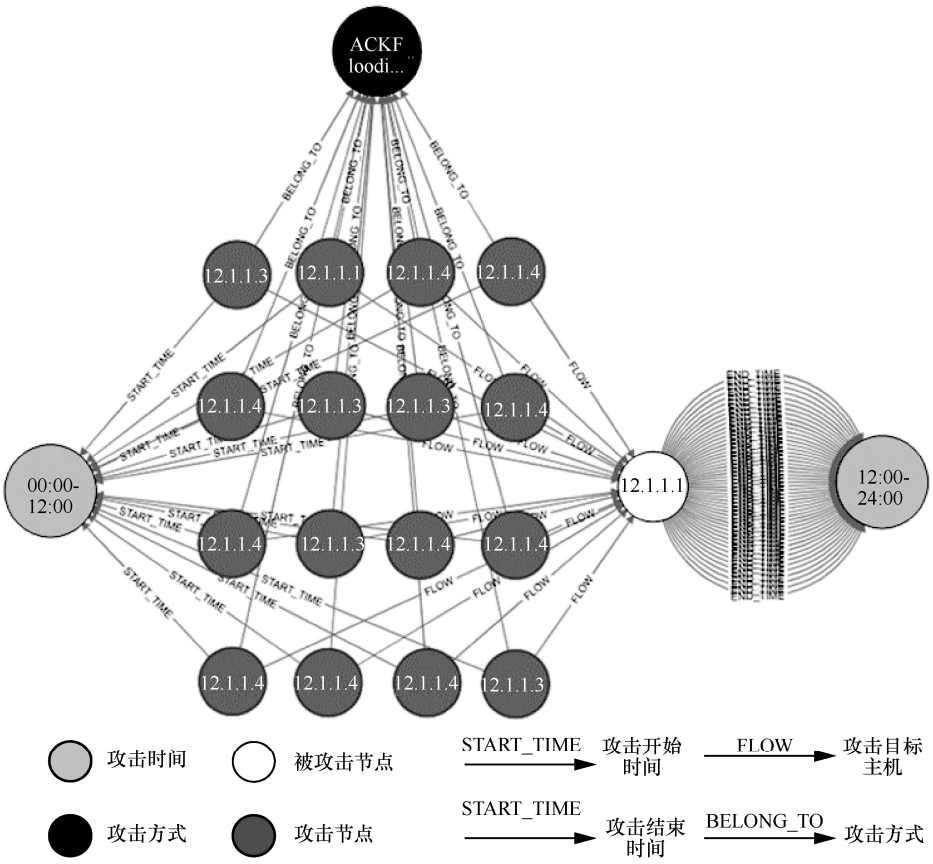

图 8　恶意行为溯源图

原型系统基于区块链技术构建了 5G 海量设备接入的场景[14]并收集了这些模拟设备发送的攻击流量数据和正常流量数据，共计 327 万条数据。其中攻击流量数据由僵尸网络、反射放大 DDoS、慢速 DDoS、应用层 DDoS 和网络层 DDoS 攻击共同组成并存入知识库中，恶意流量检测库不同类型流量及其比例见表 6。

表 6　恶意流量检测库不同类型流量及其比例

类型	数量	比例
正常流量	903 076	27.58%
僵尸网络	715 294	21.85%
反射放大 DDoS	129 164	3.94%
慢速 DDoS	324 300	9.91%
应用层 DDoS	425 403	12.99%
网络层 DDoS	776 662	23.73%

知识库导入第三方网络安全数据库共计 3 个：CNNVD 漏洞库、CAPEC 攻击库、CWE 弱点库。对数据库中数据进行结构化并添加关联关系后导入知识库中，导入数据库类型及其数据量见表 7。

表 7　第三方数据库类型及其数据量

类型	数量
CNNVD 漏洞记录	81 090
CAPEC 攻击类型	541
CWE 弱点类型	918

数据收集完成后，基于不同的数据需求与数据模型，通过数据导入接口导入结构化数据，构成完整的 DDoS 攻击恶意行为知识并实现可视化输出。

4.3　分布式知识库构造

本节对基于 DOTS 协议构造的分布式知识库

进行性能测试。分布式知识库的实验拓扑如图 9 所示。在 1 台物理服务器上搭建 8 台虚拟机，并在每台主机上安装适配知识库传输的 DOTS 协议。其中，3 台主机启动 DOTS 服务器并搭载网络安全知识库作为服务器的后台数据库，3 台主机启动 DOTS 客户端和客户端控制器并搭载恶意流量检测库用于检测 DDoS 攻击，2 台主机启动 DOTS 的 GOBGP 路由器作为被攻击地址段和正常地址段的网关路由器。

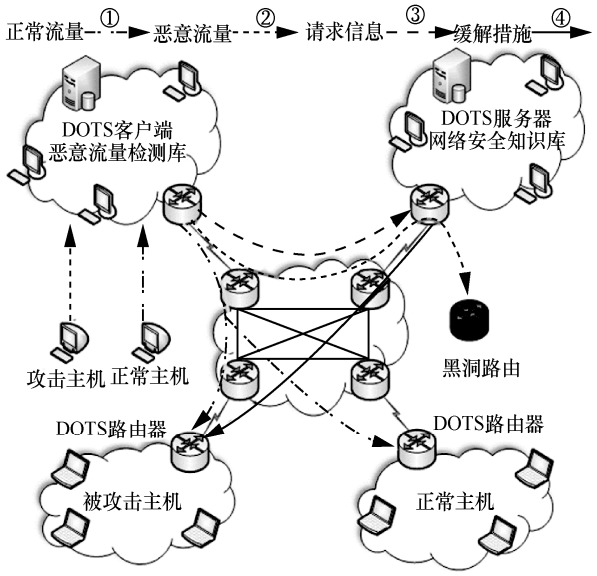

图 9　分布式知识库实验拓扑

实验一首先验证 DDoS 攻击恶意行为知识库的恶意流量检测性能。正常流量①和恶意流量②首先流经 DOTS 客户端主机所在域的接入网关，客户端主机调用恶意流量检测库对输入流量进行检测，检测为正常流量的数据正常转发，检测为恶意流量的数据则解析其攻击的目的地址段，客户端主机通过 DOTS 信令信道向服务器发送保护请求③，并将恶意流量导向 DOTS 服务器。DOTS 服务器接收并处理客户端发送的请求，通过数据信道将恶意流量解析后的相关信息传输到网络安全知识库中并根据恶意流量的攻击类型向被攻击地址段的 DOTS 路由器发送缓解措施④，以指导 DOTS 路由器进行 DDoS 攻击防御。

调用恶意流量检测库选用检测率高的检测模块对原型系统在 1 h 内生成的正常流量和 3 种 DDoS 攻击流量进行检测并存储结果，检测结果见表 8。

表 8　恶意流量检测结果

DDoS 攻击种类	数量	精确率
正常流量	33 206	95%
僵尸网络	28 070	92%
反射放大 DDoS	19 621	96%
应用层 DDoS	20 342	97%

僵尸网络攻击与正常流量的相似程度较高，因此在检测时误判为正常流量的次数较多，其检测精确率为 92%，其他流量类型的检测精确率均在 95%及以上。其中，检测为恶意 DDoS 攻击的流量目的地址被更改为黑洞路由以实现攻击缓解。

实验二验证了分布式知识库的知识数据更新效率。如图 10 所示，在 1 h 内对单个知识库节点提交了 4 次数据更新请求，柱状图为每次更新后的知识库数据总量，折线图为 DOTS 客户端发送知识更新请求命令到知识库更新完成所消耗的时间。Neo4j 数据库会对导入的数据添加唯一性约束，更新耗时会随着知识库已有数据量的增加而增加，因此图 10 中更新耗时随着更新次数而增加。

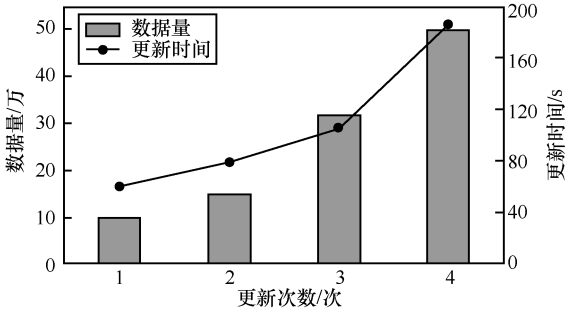

图 10　分布式知识库知识数据更新

图 11 以实体行为感知图为例展示了分布式知识库更新前后知识图谱可视化图形的变化。更新

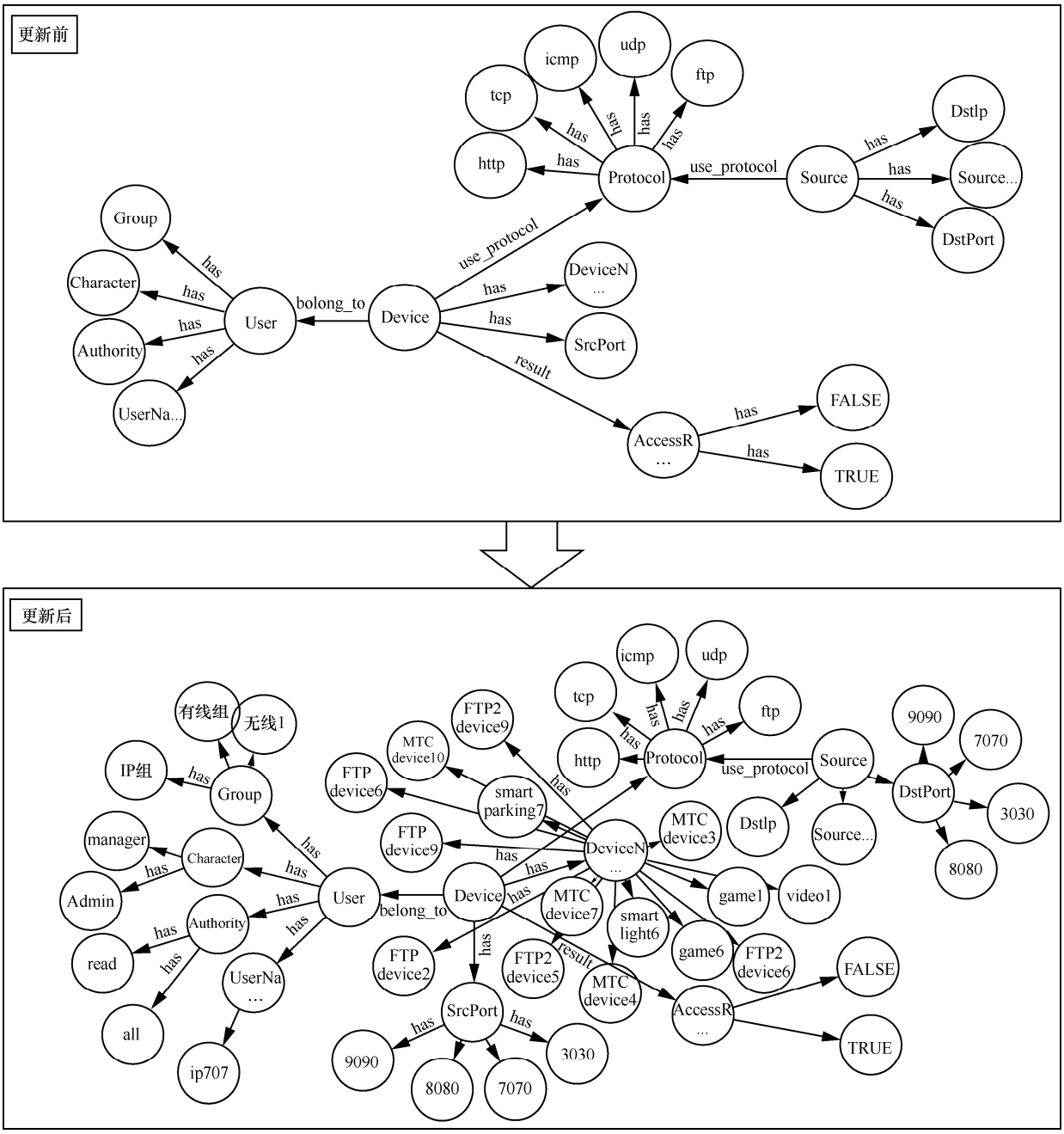

图 11　分布式知识库数据更新可视化

前的知识图谱仅包含实体行为感知图的数据实体结构和属性，在一次更新之后，新导入的实体节点根据属性匹配自动与已有实体相互关联，形成包含更多实体和关系的新实体行为感知图。

实验结果表明，对于信令信道，DOTS 服务器能够正确响应 DOTS 客户端的请求并对申请保护的地址段执行恶意流量缓解措施；对于数据信道，DOTS 服务器能接受 DOTS 客户端自定义的数据模型，提取传输文件中的知识库更新资源，并对分布式知识库进行知识更新操作。

实验三验证了知识库检测 DDoS 攻击的能效。利用知识库对 DDoS 攻击流量进行在线检测，在一定时

间内收集网络入口处的流量，然后输入到知识库进行检测。对僵尸网络、反射放大 DDoS、应用层 DDoS 和慢速 DDoS 攻击进行在线检测，分析检测精确率、召回率和识别攻击的响应时间，其结果见表 9。

表 9　知识库在线检测与响应时间结果

DDoS 种类	精确率	召回率	响应时间/s
僵尸网络	0.87	0.92	145
反射放大 DDoS	0.94	0.94	86
应用层 DDoS	0.92	0.93	114
慢速 DDoS	0.91	0.93	98

实验结果表明除僵尸网络外，知识库对其他 3 种 DDoS 攻击在线检测的精确率和召回率参数均在 90%以上，且对攻击的响应时间少于 2 min。僵尸网络攻击与正常流量特征较为相似，导致知识库对僵尸网络攻击存在较多的误判，使得僵尸网络攻击在线检测参数比其他 DDoS 攻击略低。

4.4　知识库应用场景

分布式 DDoS 攻击恶意行为知识库除了具有恶意流量检测与知识更新功能，还能够在查询展示、推理反馈等多种应用场景中发挥作用。

在查询展示和关联分析的应用场景中，知识库能对查询对象进行可视化展示，并提供查询对象的关联实体和关系。以恶意流量检测图为例，能够关联到应用层 DDoS 攻击流量的 84 种特征属性、属性值及目前检测模块的精确率和误判倾向等信息；以恶意行为特征图为例，当查询到应用层 DDoS 攻击时，能够关联到其 3 种攻击方式及与这 3 种攻击方式相关性较高的流量特征；以恶意行为溯源图为例，能够查询并关联到应用层 DDoS 攻击时序图等攻击过程信息。随着分布式 DDoS 攻击恶意行为知识库的不断更新，在 DDoS 攻击查询展示和关联分析的应用场景中能基于最新的数据和模型给出查询和分析的结果以及与之关联的其他信息。

在推理反馈的应用场景中，知识库能基于先验知识推理出新的实体或关系信息。以恶意行为特征图为例，基于图算法或聚类算法推理出最具影响力的特征并反馈给检测模块，指导检测模型修改以提升检测能力。随着知识库不断积累检测模块反馈的特征知识，能够进一步优化特征推理和反馈过程，以应对 5G 网络中不断提升的 DDoS 攻击威胁。

5　结束语

本文提出了一种分布式 DDoS 攻击恶意行为知识库构建方案，首先，基于知识图谱构建了恶意流量检测库和网络安全知识库中的知识图谱来全面描绘 DDoS 攻击；然后，在原型系统中收集 DDoS 攻击正常、异常流量及第三方网络安全知识库中攻击、漏洞和弱点信息，基于预设的数据结构导入知识库中，构建 DDoS 攻击恶意行为知识库；最后，基于 DOTS 协议构建了分布式知识库，实现知识库之间的数据传输。通过实验，验证了 DDoS 攻击恶意行为知识库在数据传输、指导检测 DDoS 攻击、缓解恶意流量方面的性能，弥补了传统 DDoS 攻击检测方法与知识库构建的劣势，同时探讨了分布式 DDoS 攻击恶意行为知识库的各类应用场景。下一步将在优化知识库数据传输性能、完善知识库服务安全检测机制和实现知识库智能化网络控制方面进行研究。

参考文献：

[1] BONGUET A, BELLAICHE M. A survey of denial-of-service and distributed denial of service attacks and defenses in cloud computing[J]. Future Internet, 2017, 9(3): 43.

[2] ARSHI M, NASREEN M D, MADHAVI K. A survey of DDOS attacks using machine learning techniques[J]. E3S Web of Conferences, 2020(184): 01052.

[3] XIE X, LI J P, HU X Y, et al. High performance DDoS attack detection system based on distribution statistics[M]//Lecture Notes in Computer Science. Cham: Springer International Publishing, 2019: 132-142.

[4] 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): 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): 56-76.

[5] MITRE. Common attack pattern enumeration and classification[EB].2009.

[6] BERMAN D, BUCZAK A, CHAVIS J, et al. A survey of deep learning methods for cyber security[J]. Information, 2019, 10(4): 122.

[7] OBRST L, CHASE P, MARKELOFF R. Developing an ontology of the cyber security domain[C]//STIDS. [S.l.:s.n.], 2012: 49-56.

[8] CHEN X J, JIA S B, XIANG Y. A review: knowledge reasoning over knowledge graph[J]. Expert Systems With Applications, 2020(141): 112948.

[9] 王勇超, 罗胜文, 杨英宝, 等. 知识图谱可视化综述[J]. 计算机辅助设计与图形学学报, 2019, 31(10): 1666-1676.
WANG Y C, LUO S W, YANG Y B, et al. A survey on knowledge graph visualization[J]. Journal of Computer-Aided Design & Computer Graphics, 2019, 31(10): 1666-1676.

[10] 陈佳. 基于知识图谱的 DDoS 攻击源检测研究[J]. 信息安全研究, 2020, 6(1): 91-96.
CHEN J. DDoS attack detection based on knowledge graph[J]. Journal of Information Security Research, 2020, 6(1): 91-96.

[11] ZHANG Z J. Graph databases for knowledge management[J]. IT Professional, 2017, 19(6): 26-32.

[12] MISAKI M, TSUDA T, INOUE S, et al. Distributed database and application architecture for big data solutions[C]// Proceedings of IEEE Transactions on Semiconductor Manufacturing. Piscataway: IEEE Press, 2016: 328-332.

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

[14] 王子恒. 基于区块链的海量连接管理架构设计与实现[D]. 北京: 北京交通大学, 2021.
WANG Z H. Design and implementation of mass connection management architecture based on blockchain[D]. Beijing: Beijing Jiaotong University, 2021.

[作者简介]

刘飞扬（1997− ），男，北京交通大学电子信息工程学院硕士生，主要研究方向为网络安全。

李坤（1997− ），男，北京交通大学电子信息工程学院博士生，主要研究方向为网络安全、智能通信。

宋飞（1983− ），男，北京交通大学电子信息工程学院教授，主要研究方向为信息网络理论及关键技术、信息处理与人工智能。

周华春（1965− ），男，博士，北京交通大学电子信息工程学院教授，主要研究方向为智能通信、移动互联网、网络安全与卫星网络。