软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software, 2022,33(2):683−698 [doi: 10.13328/j.cnki.jos.006314]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

一种基于图模型的网络攻击溯源方法*

黄克振[1,2], 连一峰[1], 冯登国[1], 张海霞[1], 吴 迪[3], 马向亮[4]

[1](中国科学院 软件研究所 可信计算与信息保障实验室, 北京 100190)

[2](中国科学院大学, 北京 100049)

[3](中国网络安全审查技术与认证中心, 北京 100020)

[4](清华大学 集成电路学院, 北京 100084)

通信作者: 黄克振, E-mail: kezhen@iscas.ac.cn

摘 要: 随着信息技术的飞速发展, 网络攻击事件频发, 造成了日益严重的经济损失或社会影响. 为了减少损失或预防未来潜在的攻击, 需要对网络攻击事件进行溯源以实现对攻击者的挖掘追责. 当前的溯源过程主要依赖于人工完成, 效率低下. 面对日益增加的海量溯源数据和日趋全面的溯源建模分析维度, 亟需半自动化或自动化的网络攻击者挖掘方法. 提出一种基于图模型的网络攻击溯源方法, 建立网络攻击事件溯源本体模型, 融合网络攻击事件中提取的线索数据和威胁情报数据, 形成网络攻击事件溯源关系图; 引入图嵌入算法自动学习嵌有关联线索特征的网络攻击事件特征向量, 进而利用历史网络攻击事件特征向量训练 SVM(support vector machine)分类器, 并基于 SVM 分类器完成网络攻击者的挖掘溯源; 最后, 通过实验验证了该方法的可行性和有效性.

关键词: 网络攻击事件; 网络攻击者; 溯源; 网络攻击事件溯源; 关系图; 图嵌入

中图法分类号: TP309

中文引用格式: 黄克振, 连一峰, 冯登国, 张海霞, 吴迪, 马向亮. 一种基于图模型的网络攻击溯源方法. 软件学报, 2022, 33(2): 683–698. http://www.jos.org.cn/1000-9825/6314.htm

英文引用格式: Huang KZ, Lian YF, Feng DG, Zhang HX, Wu D, Ma XL. Method of Cyber Attack Attribution Based on Graph Model. Ruan Jian Xue Bao/Journal of Software, 2022, 33(2): 683–698 (in Chinese). http://www.jos.org.cn/1000-9825/6314.htm

Method of Cyber Attack Attribution Based on Graph Model

HUANG Ke-Zhen[1,2], LIAN Yi-Feng[1], FENG Deng-Guo[1], ZHANG Hai-Xia[1], WU Di[3], MA Xiang-Liang[4]

[1](Trusted Computing and Information Assurance Laboratory, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China)

[2](University of Chinese Academy of Sciences, Beijing 100049, China)

[3](China Cybersecurity Review Technology and Certification Center, Beijing 100020, China)

[4](School of Integrated Circuits, Tsinghua University, Beijing 100084, China)

Abstract: With the rapid development of technologies such as computers and smart devices, cyber attack incidents happen frequently, which cause increasingly serious economic losses or reputation losses. In order to reduce losses and prevent future potential attacks, it is necessary to trace the source of cyber attack incidents to achieve accountability for the attackers. The attribution of cyber attackers is mainly a manual process by forensic analyst. Faced with increasing analysis data and analysis dimensions, semi-automated or automated cyber attackers mining analysis methods are urgently needed. This study proposes a graph model-based attacker mining analysis method for cyber attack incidents. This method first establishes an ontology model for cyber attack incident attribution, and then fuses clue data extracted from cyber attack incidents with various threat intelligence data to construct a cyber attack incidents attribution relationship graph. The graph embedding algorithm automatically learns the representation vector of cyber attack incidents, which embedded clue characteristics of cyber attack incidents, from the attribution relationship graph of cyber attack incidents. And then a classifier is trained with the historical cyber attack incidents representation vector, which classifies the cyber attack incident to one cyber attacker. Finally, the

* 基金项目: 国家重点研发计划(2020YFB1806504, 2018YFC0824801)

收稿时间: 2020-06-23; 修改时间: 2020-09-27, 2020-11-24; 采用时间: 2021-01-10; jos 在线出版时间: 2021-08-03

feasibility and effectiveness of the method are verified by experiments.

Key words: cyber attack incident; cyber attacker; attribution; cyber attack incident attribution; relation graph; graph embedding

APT (advanced persistent threat)攻击多由具有国家背景的攻击组织发起, 通过向目标计算机系统投放特种木马, 以窃取国家机密信息、重要企业的商业信息、破坏基础设施等. 据不完全统计, 2019 年上半年与 2018 年上半年相比, 国内外公布的 APT 攻击事件数量增长近 5 成[1], 导致越来越多的经济损失或名誉损失[2]. 为了减少网络攻击带来的损失和阻止未来潜在的攻击行为, 需要进行网络攻击溯源, 以追究攻击者或攻击组织的罪责[3].

Wheeler 等人[4]将网络攻击溯源定义为“确定攻击者(或攻击者使用设备)的身份或位置的过程”. 根据溯源深度和粒度, 网络攻击溯源可分为攻击主机溯源、控制主机溯源、攻击者溯源、攻击组织溯源这 4 个级别[5]. 为了实现网络攻击溯源, 研究人员已从追踪回溯技术[6]、蜜罐技术[7]、数字取证技术[8]、网络取证技术[9]、恶意代码分析技术[10]、基于情报的溯源技术[11]等多方面开展了诸多研究. Allan 等人[12]针对已有研究工作的性能、可靠性、扩展性、关联性、攻击身份识别、攻击意图挖掘等指标进行综合评价, 得出基于情报的溯源技术和恶意代码分析技术的效果要明显优于网络取证技术、数字取证技术、蜜罐技术和追踪回溯技术. 为了实现已知攻击者或攻击组织的溯源, 典型的方法是通过融合威胁情报和网络攻击事件线索数据, 具体分为多源异构数据融合和攻击者挖掘两部分.

- 在多源异构数据融合方面, 基于本体的数据融合是一种典型的方法. 当前网络安全领域的本体多以支持网络安全威胁情报共享为主. Saad 等人[13]提出了一套适合网络取证调查的本体模型. Qamar 等人[14]提出了一套支持威胁情报分析和共享的本体模型, 该模型可以从攻击者画像的角度支持网络攻击溯源分析. 但是, 上述模型对网络威胁情报信息、攻击者与攻击目标间存在的地缘政治关系等信息的融合力度不够. 针对现有方法的局限性, 本文基于本体融合的方法, 提出一套较全面的网络攻击事件溯源本体;
- 在攻击者挖掘方面, 由于网络中的僵尸主机、匿名代理服务器、洋葱路由、注册隐私制度等隐藏了攻击者的真实身份, 增加了网络攻击事件溯源难度[15], 需要进一步增加溯源的分析维度[3](如攻击者与攻击目标间的国家关系、攻击目标的行业特征等等); 同时, IoT (Internet of Things)、智能设备等技术的发展也为攻击者提供了更多的攻击对象和利用跳板, 增加了网络攻击事件溯源过程中需要挖掘分析的数据[3]. 分析维度和数据量的增加, 进一步加大了网络攻击者挖掘分析的工作量, 亟需自动化辅助的分析方法[16], 以提高分析效率. 但是, 已有的研究工作存在分析特征或推理规则依赖专家经验[3,17]的问题. 针对该局限性, 本文提出通过挖掘网络攻击事件与攻击者使用的攻击工具、攻击方法、攻击模式、基础设施等特征间存在的隐含关系进行攻击溯源的思路.

综上所述, 本文提出一种基于图模型的网络攻击溯源方法.

- 首先构建网络攻击事件溯源本体模型, 融合事件中挖掘的线索数据与各种威胁情报数据形成溯源关系图;
- 然后引入图嵌入算法, 从溯源关系图中学习网络攻击事件的关联特征向量;
- 利用历史网络攻击事件的关联特征向量训练 SVM 分类器, 进而使用 SVM 分类器完成网络攻击者的挖掘分析.

本文的主要贡献有:

(1) 建立了面向网络攻击事件的溯源本体模型, 为线索数据和威胁情报数据的融合提供了基础框架;
(2) 引入图嵌入算法, 建立用于描述网络攻击事件隐含关系的关联特征向量, 克服分析特征和推理规则依赖专家经验的局限性;
(3) 利用机器学习算法自主学习生成攻击事件特征向量的分类判定模型, 实现自动化辅助的攻击溯源.

1 基于图模型的网络攻击溯源框架

网络攻击溯源需要安全专家首先收集攻击活动中遗留的线索数据, 与已知攻击者、历史攻击事件和各种地缘政治等相关数据进行关联分析, 挖掘多维数据间的关系, 从而判断可能的攻击者或攻击组织. 图数据结构适用于描述多维数据间的关系, 故本文将网络攻击者挖掘分析相关的多维数据融合形成网络攻击事件溯源关系图.

基于图的分析能够挖掘高价值的分析结果(如潜在的关系等), 但是已有的方法大多存在高计算资源和空间资源浪费的局限性[18], 而图嵌入算法能够在保留图信息的前提下将图转化为低维空间特征向量, 进而利用低维空间特征向量进行高效的图挖掘分析.

当前, 图嵌入算法主要分为基于因式分解的方法、基于随机游走的方法和基于深度学习的方法这三大类. 其中, 根据南加州大学的 Goyal 等人在参考文献[20]的分析结果: 在节点分类方面, 由于基于随机游走的 node2vec[19]方法能够较好地挖掘图节点间的同质性(即节点间存在边)和结构对等性(即节点间存在共同的连接节点), 故其与基于因式分解的方法和基于深度学习的方法相比具有明显的优势. 而网络攻击事件的溯源问题可以转化为网络攻击事件面向攻击者的分类问题: 同一攻击者发起的不同的网络攻击事件在攻击方法、攻击工具、攻击动机、攻击目标等方面具有相似性, 如果将网络攻击事件及其相关的攻击方法、攻击工具、攻击动机、攻击目标等转化为图模型, 那么表示某网络攻击事件的节点与表示攻击者在此网络攻击事件中使用的攻击方法、攻击工具、攻击动机、攻击目标等的节点间就具有同质性(即表示网络攻击事件的节点与表示攻击方法、攻击工具等的节点间存在边), 而同一攻击者发起的不同的网络攻击事件就存在结构对等性(即表示不同网络攻击事件的节点间存在共同的连接节点, 这些共同的连接节点表示不同攻击事件中使用的相同攻击方法、攻击工具、攻击动机等). 故本文引入基于随机游走的图嵌入算法学习网络攻击事件的关联特征向量, 进而将网络攻击事件面向攻击者进行分类, 辅助完成攻击事件的溯源分析.

如图 1 所示, 网络攻击溯源包含源数据获取、网络攻击事件溯源关系图生成和攻击者挖掘这 3 个阶段.

1) 在源数据获取阶段, 主要完成网络安全威胁情报和网络攻击事件线索数据两类数据的获取: 网络安全威胁情报数据主要是指从 Twitter 等社交网站、FireEye 等威胁情报源采集攻击者相关威胁情报(如已知攻击者、攻击者动机、攻击工具、基础设施、攻击方法和攻击模式等)和历史网络攻击事件相关的威胁情报(如历史攻击事件涉及的攻击目标、攻击者、攻击目标与攻击者所属区域间的地缘政治关系、恶意 IP 地址、恶意域名、恶意邮件地址、攻击工具、攻击工具利用的脆弱性、攻击方法等); 网络攻击事件线索数据主要是指从网络攻击目标的流量日志、告警日志、主机日志等数据源中利用恶意代码分析、数字取证和网络取证调查等手段分析提取的攻击者使用的攻击工具指纹、攻击 IP、攻击域名等线索数据;
2) 在网络攻击事件溯源关系图生成阶段, 首先对网络威胁情报和网络攻击事件线索数据进行数据清洗和标准化处理; 然后利用基于词向量的本体映射方法与基于词典的本体映射方法相结合完成本体映射; 最后利用字符串的编辑距离和字符串相似性对标准化后的数据进行实体对齐, 实现多源异构数据融合, 形成网络攻击事件溯源关系图;
3) 在攻击者挖掘阶段, 引入基于随机游走的图嵌入算法, 在网络攻击事件溯源关系图上随机游走, 生成网络攻击事件溯源实体序列(见定义 11), 基于该实体序列生成网络攻击事件的关联特征向量, 利用历史网络攻击事件的特征向量训练 SVM 分类器, 并使用 SVM 分类器实现对已知攻击者/组织的自动挖掘.

下文分别对网络攻击事件溯源本体模型、基于图嵌入的网络攻击事件自动特征提取算法和基于 SVM 分类器的攻击者判定算法进行详细阐述.

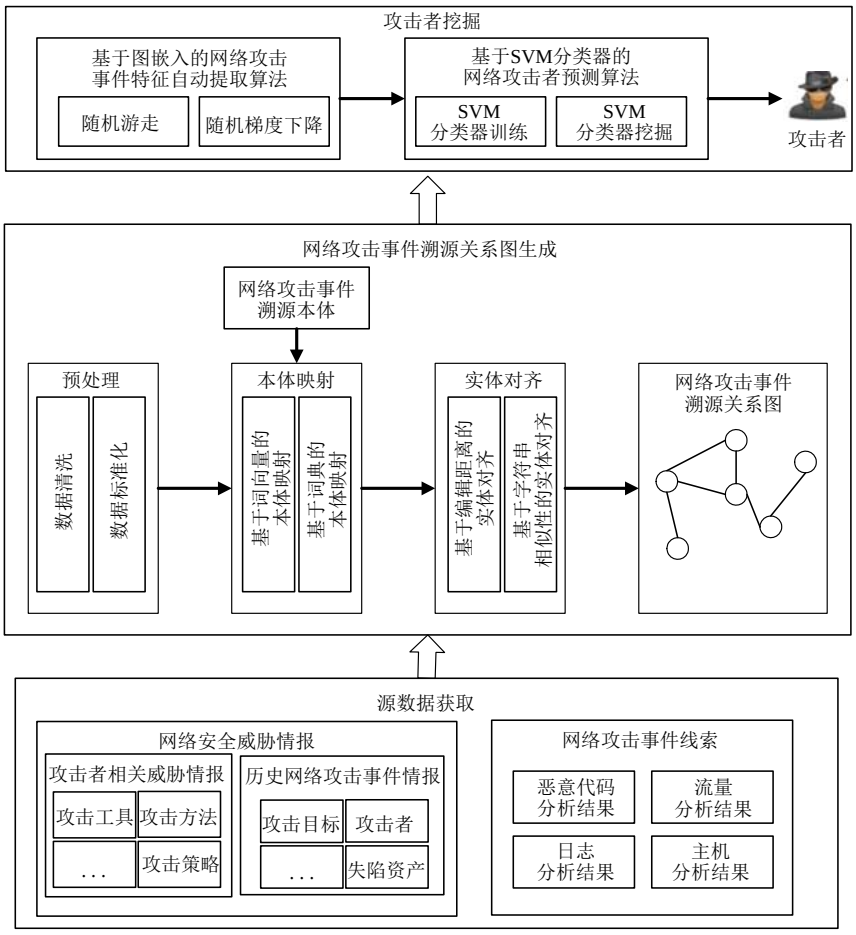


图 1　基于图模型的网络攻击事件溯源框架

2　网络攻击事件溯源本体模型

2.1　定　义

定义 1(网络攻击事件溯源局部本体(*LocalOntology*)). 网络攻击事件溯源分析过程中涉及网络安全威胁情报、网络攻击事件、地缘政治等领域, *LocalOntology* 是这些特定领域的概念及概念间关系的形式化表示. 即 $LocalOntology=\langle C,R\rangle$, 其中, C 表示概念, R 表示概念间的关系.

定义 2(网络攻击事件溯源本体(*CyberAttributionOntology*)). 描述网络攻击事件溯源相关的概念以及概念间关系的形式化表示, 即 $CyberAttributionOntology=\langle Classes,Relations\rangle$, 其中, *Classes* 表示概念, *Relations* 表示概念间的关系.

定义 3(网络攻击事件溯源实体(*CyberAttributionEntity*)). 这是指网络攻击事件溯源本体中概念的实例, 如实体 APT29 是概念 *Attacker* 的实例; 同理, 使用 *LocalOntologyEntity* 表示网络攻击事件溯源局部本体的实体.

定义 4(网络攻击事件溯源实体间关系(*CyberAttributionRelations*)). 这是指网络攻击事件溯源本体中概念间关系, 即 $CyberAttributionRelations\subseteq Relations$. 同理, 使用 *CyberAttributionRelations* 表示网络攻击事件溯源局部本体的实体间关系.

定义 5(网络攻击事件溯源元数据(*MetaData*)). 这是指用于攻击溯源的网络安全威胁情报和事件线索数据

的最小数据单元，使用六元组 $MetaData=\langle entity_1,r,entity_2,ontologyType,c_1,c_2\rangle$ 表示，其中，$entity_1,entity_2\in LocalOntologyEntity$, $r=(c_1,c_2)\in LocalOntologyRelations$, $OntologyType\in LocalOntology$, $c_1,c_2\in C$.

定义 6(网络攻击事件溯源关系图(*G*)). 使用无向图描述网络攻击事件溯源实体及实体间的关系，即 $G=(V,E)$，其中，V 是 *CyberAttributionEntity* 的集合，E 是 *CyberAttributionRelations* 的集合.

定义 7(网络攻击事件溯源本体映射(*OntologyMap*)). 如图 2 所示，描述网络攻击事件溯源局部本体 *LocalOntology* 向网络攻击事件溯源本体 *CyberAttributionOntology* 映射的方法，即 *OntologyMap*: *LocalOntology* $\rightarrow$*CyberAttributionOntology*. 具体来说，假设存在 $c_1,c_2\in C$, $(c_1,c_2)\in R$, $class_1,class_2\in Classes$, $(class_1,class_2)\in Relations$, $SimilarSemantic(c_1,class_1)$=True, $SimilarSemantic(c_2,class_2)$=True, 则 $c_1\rightarrow class_1$, $c_2\rightarrow class_2$, $(c_1,c_2)\in(class_1,class_2)$, 其中，$SimilarSemantic(c,class)=\begin{cases}\text{True, if } c,\ class \text{ 语义相似}\\ \text{False, else}\end{cases}$，概念间的语义是否相似根据词向量和词典的方法判断.

定义 8(网络攻击事件溯源实体对齐(*EntityAlignment*)). 如图 2 所示，描述网络攻击事件溯源元数据 *MetaData* 中的实体向网络攻击事件溯源关系图 *G* 中的实体转化的过程.

具体来说，如果$\exists v\in V$, $SimilarSemantic(v,MetaData.entity_i)$=True, 则 $MetaData.entity_i=v$, 其中, i=1,2.

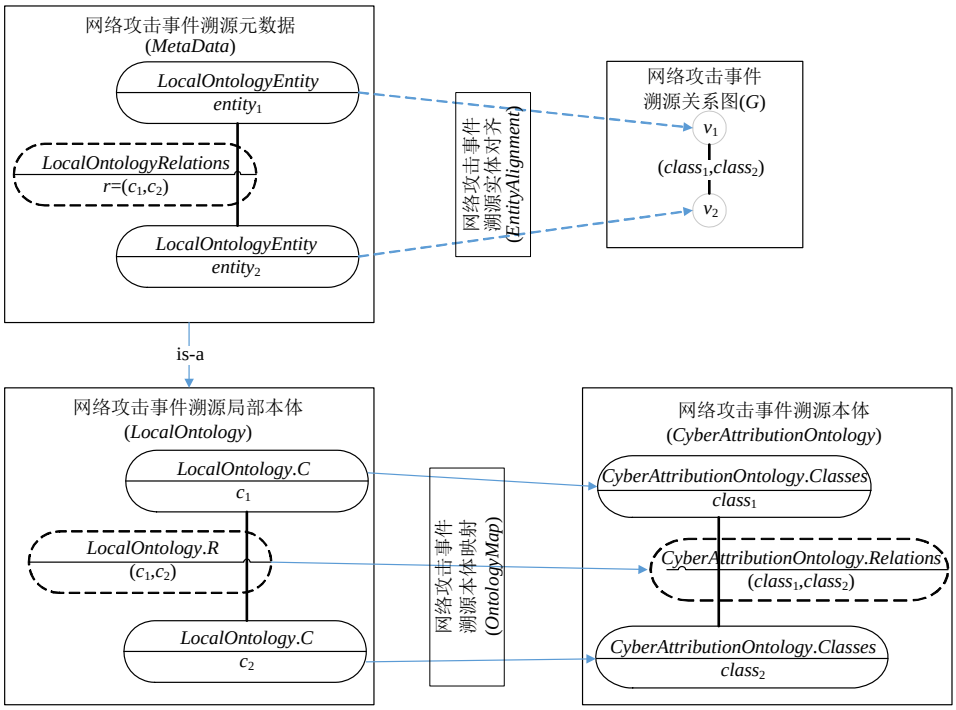


图 2　网络攻击事件溯源本体映射和网络攻击事件溯源实体对齐

2.2 本体模型

本文提出的网络攻击事件溯源本体模型如图 3 所示，图中节点标签表示概念，边的标签表示概念间的关系(见定义 2). 网络攻击事件溯源本体以网络攻击事件(*cyber incident*)为主要分析对象. 网络攻击事件是指在某个时间点或时间段(*time*)，有特定动机(*motivation*)的网络攻击者(*attacker*)，在某些政治事件(*GeoIncident*)的刺激下，为达成某种目的(*goal*)，利用一系列攻击工具(*tools*)、攻击方法(*means*)、基础设施(*IOC*)攻陷攻击目标(*target*)的信息资产(*asset*)，并产生一定后果(*consequences*)的安全事件，其中，*Tools* 针对 *Asset* 存在的漏洞或弱点(*exploit target*); *Attacker*、*GeoIncident*、*Target*、*Tools*、*Means* 中均可提取与地缘政治相关的本体(*GeoOntology*)辅助网络攻击事件溯源.

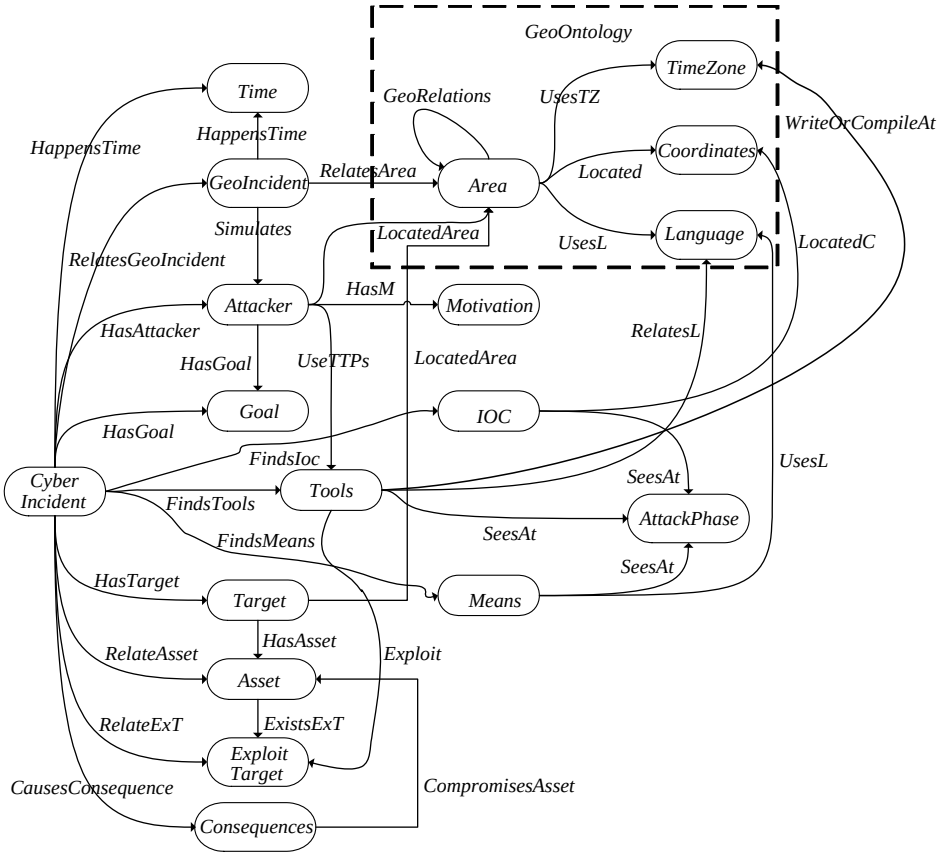


图 3 网络攻击事件溯源本体模型

网络攻击事件溯源本体使用二元组表示: *CyberAttributionOntology*=⟨*Classes*,*Relations*⟩表示, 其中,

- *Classes* 表示网络攻击事件溯源本体中的概念, *Classes*∈{*Cyber Incident*,*Time*,*Motivation*,*Attacker*, *GeoIncident*,*Goal*,*IOC*,*Means*,*Tools*,*Target*,*Asset*,*Exploit Target*,*Consequences*,*Area*,*TimeZone*,*Coordinates*, *Language*};
- *Relations* 表示网络攻击事件溯源本体中各个概念之间的关系, *Relations*∈{*HappensTime*, *RelatesGeoIncident*,*HasAttacker*,*HasGoal*,*FindTools*,*FindIoc*,*FindMeans*,*HasTarget*,*RelatesAsset*,*GausesConsequences*,*RelateExT*,…,*CompromisesAsset*}.

由于网络攻击事件溯源本体根据网络攻击事件的事前、事中、事后的关键关联因素进行构建, 故其对网络攻击事件事前的触发因素中暗含的攻击者与攻击目标间的地缘政治、事中攻击者使用的网络安全威胁情报、事后攻击目标发现的网络安全威胁情报等线索具有较好的融合力度.

3 网络攻击事件溯源算法

3.1 基于图嵌入的网络攻击事件自动特征提取算法(GECEFA)

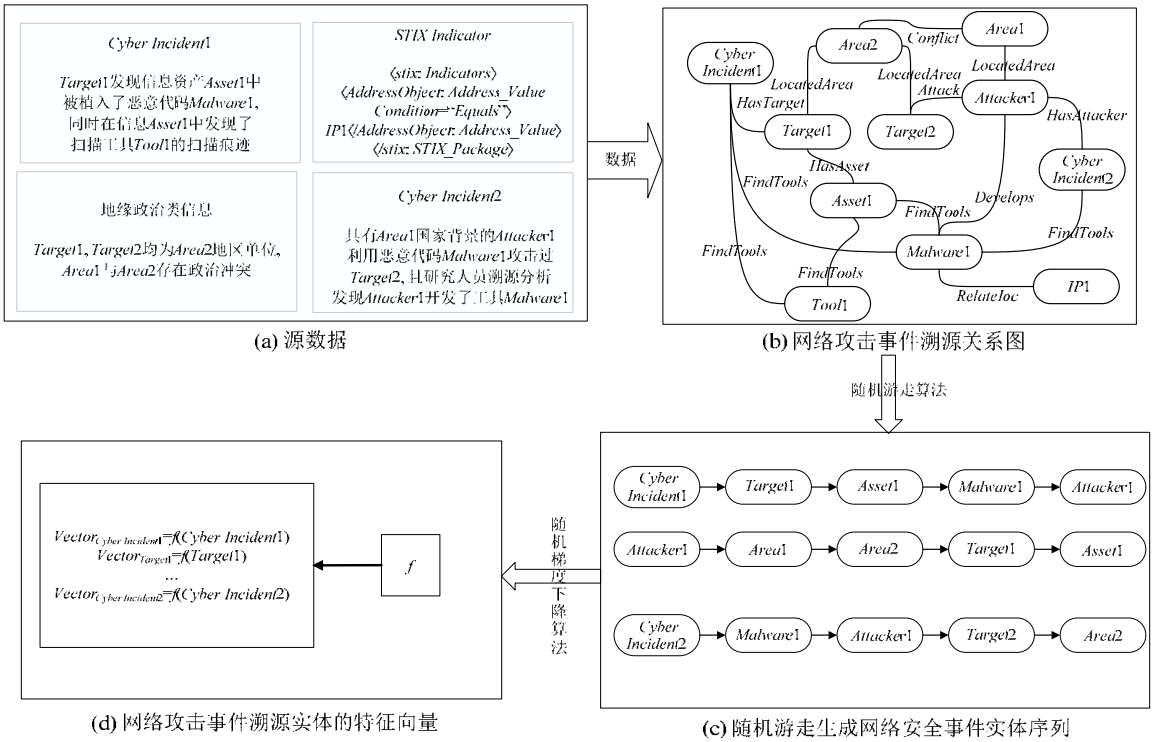
定义 9(1 阶关联实体集(*CyberAttributionEntity*$_v^1$)). 与网络攻击事件溯源实体 v 存在直接关联的网络攻击事件溯源实体的集合, 即:

$\exists(u,v)\in E$, $u\in CyberAttributionEntity_v^1$, 如图 4(b)所示, $Malware1\in CyberAttributionEntity^1_{Cyber\ Incident1}$, 即有: *Malware*1 是 *Cyber Incident*1 的 1 阶关联实体, 表示 *Malware*1 是 *Cyber Incident*1 的直接关联特征.

定义 10(*k* 阶关联实体集($CyberAttributionEntity_v^k$)). 与网络攻击事件溯源实体 v 存在间接关联的网络攻击事件溯源实体的集合，即: $\forall CyberAttributionEntity_v^{k-1} \cap CyberAttributionEntity_u^{k-1} \neq \varnothing$,

$$(CyberAttributionEntity_u^{k-1} - CyberAttributionEntity_v^{k-1}) \in CyberAttributionEntity_v^k,$$

其中, $1<k\in N$, 如图 4 所示, $IP1 \in CyberAttributionEntity^2_{Cyber\ Incident1}$, 即 *IP*1 为 *Cyber Incident*1 的 2 阶关联实体，表示 *IP*1 是 *Cyber Incident*1 的间接关联特征.



(a) 源数据　(b) 网络攻击事件溯源关系图

(d) 网络攻击事件溯源实体的特征向量　(c) 随机游走生成网络安全事件实体序列

图 4　网络攻击事件溯源实体特征向量生成流程

定义 11(网络攻击事件溯源实体序列(*AttributionEntityList*$_v$)). 表示以 v 为起点，在网络攻击事件溯源关系图中随机游走产生的实体集合. 具体来说，如果 G 中存在长度为 l 的路径 $walk=\langle v_0e_0v_1e_1\ldots e_{l-1}v_l\rangle$，则:

$$\langle v_0v_1...v_l\rangle \in AttributionEntityList_{v_0},$$

其中，对于所有的 $i<l$, 均有 $e_i=(v_i,v_{i+1})\in E$. 如图 4 中以 *Cyber Incident*1 为起点的长度为 5 的一组网络攻击事件溯源实体序列为〈*Cyber Incident*1,*Target*1,*Asset*1,*Malware*1,*Attacker*1〉，该实体序列包含了 *Cyber Incident*1 的 1 阶关联实体(*Target*1,*Malware*1)和 2 阶关联实体(*Asset*1,*Attacker*1)

定义 12(网络攻击事件溯源实体的特征向量(*Vector*$_v$)). 嵌入网络攻击事件溯源实体 v 的一阶关联实体集($CyberAttributionEntity_v^1$)或 k 阶关联实体集($CyberAttributionEntity_v^k$)信息的数学向量，即 $Vector_v=[x_1x_2x_3\ldots x_d]$,其中, $x_i\in R$, $0<i\leqslant d\leqslant|V|$, 而网络攻击溯源实体的特征向量提取过程即是寻找函数 $f:v\rightarrow Vector_v$ 的过程.

当前，网络攻击事件在分析过程中，需要依赖专家经验从线索数据中挖掘价值较高的直接特征和潜在特征，以备后续的溯源过程; 而网络攻击事件 v 发生时，与网络攻击事件相关的直接特征和潜在特征会以一定的概率同时存在(Pr(*AttributionList*$_v$|v)), 那么可将网络攻击事件 v 的特征提取过程和网络攻击事件 v 向量化过程同时进行，即转化为 $\max\limits_f \sum_{v\in V} \log \Pr(AttributionList_v \mid f(v))$. 即: 以 $f(v)$表示网络攻击事件 v 的特征向量时，其相关的特征能以极大的概率共存)的优化问题.

根据文献[19], 可将上述优化问题简化为 $\max_f \sum_{u\in V}[-\log(\sum_{v\in V}\exp(f(u)\cdot f(v)))+\sum_{\theta\in AttributionList_u} f(\theta)\cdot f(u)]$, 进而利用随机梯度下降求解 f.

基于上述分析, 本文设计了如算法 1 所示的基于图嵌入的网络攻击事件自动特征提取算法(GECEFA): 首先, 融合多源异构数据(如图 4(a)所示)形成网络攻击事件溯源关系图(如图 4(b)所示); 然后, 在溯源关系图上随机游走产生网络攻击事件溯源实体序列(如图 4(c)所示), 进而基于溯源实体序列, 利用随机梯度下降算法求解上述优化问题中的函数 f; 最后, 利用 f 计算网络攻击事件溯源实体的特征向量(如图 4(d)所示).

算法 1 的第 2 行将源数据获取阶段收集的源数据信息 *incidentInfo* 经过数据预处理, 转化为标准的 *MetaData* 形式; 第 3–8 行将元数据集中的数据经过本体映射和实体对齐融合入已有的网络攻击事件溯源关系图 g 中; 第 9–15 行在图 g 中随机游走, 形成网络攻击事件溯源实体序列集 *attributionEntityLists*; 第 16 行利用随机梯度下降算法求解网络攻击事件溯源实体的特征向量提取函数 f; 第 17–21 行将图 g 中各个网络攻击事件溯源实体的特征向量存入字典变量 *nodesVectors* 中, 并作为返回值返回. 该算法的时间复杂度为 O(|*V*|*d*), 其中, |*V*|表示网络攻击事件溯源关系图 g 中节点的个数, d 表示输出特征向量的维度 *dim*.

算法 1. 基于图嵌入的网络攻击事件自动特征抽取算法(GECEFA).

输入: 历史网络攻击事件溯源关系图 g; 网络攻击事件 *incident*; 源数据信息 *incidentInfo*; 特征向量的维度 *dim*; 每个实体的网络攻击事件溯源实体序列数量 *attributionEntityListNum*; 网络攻击事件溯源实体序列长度 *attributionEntityListLen*; 窗口大小 *winSize*;

输出: 网络攻击事件溯源关系图 g; 网络攻击事件溯源实体的特征向量 *incidentVec*.

```
1  gecefa(g,incident,incidentInfo,dim,attributionEntityListNum,attributionEntityListLen,winSize):
2  metaList=preProcess(incidentInfo)   /*数据预处理*/
3  for meta in metaList:   /*对每个元数据进行融合*/
4     class1,class2=OntologyMap(meta.ontologyType,meta.c1,meta.c2,CyberAttributionOntology)
5     entity1=EntityAlignment(entity1,g)
6     entity2=EntityAlignment(entity2,g)
7     g. add_edge(g.add_node(entity1),g.add_node(entity2),(class1,class2))
8  end for
9  attributionEntityLists=[]
10 for iter=1 to attributionEntityListNum:
11    for u in g.V:
12    attributionEntityList=RandomWalk(g,u,attributionEntityListLen)   /*随机游走产生溯源实体序列*/
13       attributionEntityLists.append(attributionEntityList)
14    end for
15 end for
16 f=StochasticGradientDescent(attributionEntityLists,dim,winSize)
17 nodesVectors={}
18 for v in g.V:
19    nodesVectors[v.value]=f(v)
20 end for
21 return g, nodesVectors
```

3.2 基于SVM分类器的网络攻击者判定算法(SVM-CADA)

网络攻击事件攻击者的挖掘过程可进一步转化为 k 分类问题, 即对网络攻击事件 *Cyber Incident*, 寻找函数 δ: $\delta(f(Cyber\ Incident))\rightarrow y$, $y\in(Attacker_1,Attacker_2,\ldots,Attacker_k)$, $Attacker_i$(其中, $1\leqslant i\leqslant k$)表示已知攻击者. SVM

分类的基本思想是: 构造一个决策超平面将数据点分开, 使数据点与平面距离最远. SVM 通过引入结构风险最小化原则、核函数思想, 可将非线性的问题转化为高维线性可分的问题, 使得 SVM 在处理有限样本、非线性高维模式中有广泛的应用. 单一的 SVM 分类器解决的是二分类问题, 基于一对多的原则可构建 k 个 SVM 分类器解决 k 分类问题. 本文设计了如算法 2 所示的基于 SVM 分类器的网络攻击者判定算法, 利用 GECEFA 获取欲溯源网络攻击事件及历史网络攻击事件的特征向量, 然后使用历史攻击事件的特征向量学习 SVM 分类器, 以挖掘网络攻击事件与网络攻击者间的分类关系δ, 最后使用学习完成的分类器自动判定欲溯源网络攻击事件的攻击者.

算法 2 的第 2 行调用算法 1(GECEFA 算法), 将网络攻击事件 *incident* 及已提取的攻击事件源数据(*incidentInfo*)融入已有的网络攻击事件溯源关系图 g 中, 并提取网络攻击事件溯源实体的特征向量, 存入字典 *nodesVectors*; 第 3–13 行从图 g 中搜寻网络攻击者列表 *attackerList*, 及每个攻击者发起的历史网络攻击事件列表 *historyIncidentList*; 第 14–16 行从网络攻击事件溯源实体的特征向量字段 *nodesVectors* 中提取历史网络攻击事件的特征向量, 存入变量 *historyIncidentVectorList* 中; 第 17–19 行训练 SVM 分类器模型, 以挖掘网络攻击事件间存在的潜在特征, 并将学习结果用于挖掘网络攻击事件 *incident* 的攻击者 *attacker*. 该算法的时间复杂度为 $O(|V|^2)$, 其中, $|V|$表示网络攻击事件溯源关系图 g 中节点的个数.

算法 2. 基于 SVM 分类器的网络攻击者判定算法(SVM-CADA).

输入: 已有网络攻击事件溯源关系图 g; 网络攻击事件 *incident*; 网络攻击事件源数据 *incidentInfo*; 输出特征向量的维度 *dim*; 每个节点的路径数量 *attributionEntityListNum*; 路径长度 *attributionEntityListLen*; 窗口大小 *winSize*;

输出: 攻击者或攻击组织 *attacker*.

```
1  svm-cada(g,incident,incidentInfo,dim,attributionEntityListNum,attributionEntityListLen,winSize):
2  g, nodesVectors=gecefa(g,incident,incidentInfo)
3  for v in g.V:
4     if v.type==“Cyber Incident”:
5        CyberAttributionEntity_v^1=getNeighborhoodNodes(v)
6        for u in  CyberAttributionEntity_v^1 :
7           if u.type==“Attacker”:
8              historyIncidentList.append(v.value)
9              attackerList.append(u.value)
10          end if
11       end for
12    end if
13 end for
14 for inc in historyIncidentList:
15    historyIncidentVectorList.append(nodesVectors[inc])
16 end for
17 svmModel=svmModelTrain(historyIncidentVectorList,attackerList)
18 attacker= svmModel.predict(nodesVectors[incident.name])
19 return attacker
```

4 攻击溯源实验验证

4.1 实验场景设计

为了验证基于图模型的网络攻击溯源方法的可行性和有效性, 本文设计了典型实验场景, 从 MITRE、

FireEye 和 Twitter 等数据源利用主体爬虫采集网络攻击者(*attacker*)、攻击方法(*means*)、攻击工具(*tools*)、历史网络攻击事件(*cyber incident*)、地缘政治事件(*GeoIncident*)数据. 利用如图 5 所示的实验拓扑环境, 其中,

- *Area*1、*Area*2 和 *Area*3 表示 3 个不同的地理区域: *Area*1 区域有攻击者 *Attacker*1、*Attacker*2; *Area*2 区域有攻击目标 *Target*1; *Area*3 区域有攻击目标 *Target*2;
- *IP*1 和 *IP*2 是不属于 3 个区域的 C2(command and control)服务器. 如表 1 所示, 模拟典型的两类攻击者, 其中, *Attacker*1 代表擅长基于钓鱼邮件和零日漏洞发起攻击的 APT28, *Attacker*2 代表擅长基于钓鱼邮件和历史漏洞发起攻击的 Lazarus.

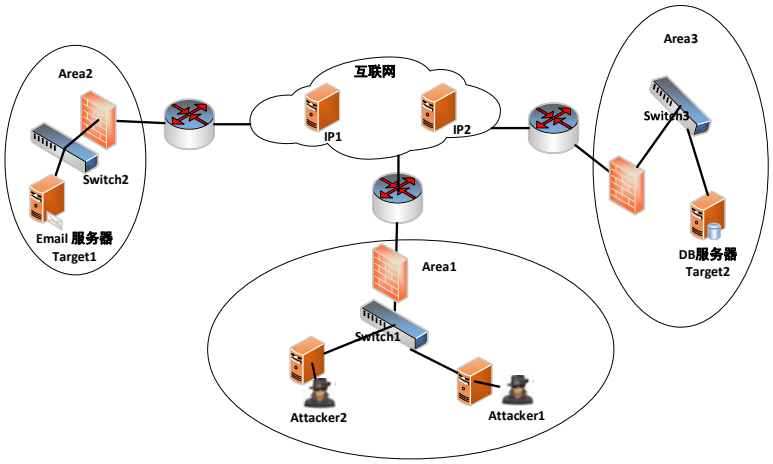


图 5 攻击溯源实验网络拓扑图

表 1 攻击溯源实验模拟攻击者

序号	攻击者	攻击方法和攻击工具	攻击目标	归属地区	使用语言	攻击动机
1	*Attacker*1	利用 Spearphishing Attachment 方法探测目标系统, 并利用基于零日漏洞(CVE-2017-2063)研制的工具(Seduploader)实施攻击	*Target*1	*Area*2	*Language*1	Spying
2	*Attacker*2	利用 Spearphishing Attachment 方法探测目标系统, 并利用基于历史漏洞(CVE-2010-2883)研制的工具(Asruex)实施攻击	*Target*2	*Area*3	*Language*1	Financial

4.2 网络攻击事件特征向量提取实验

*Attacker*1 和 *Attacker*2 分别针对攻击目标 *Target*1 和 *Target*2 发起攻击, 对应的网络攻击事件分别命名为 *Cyber Incident*1 和 *Cyber Incident*2, 攻击数据流如图 6(a)和图 6(b)所示.

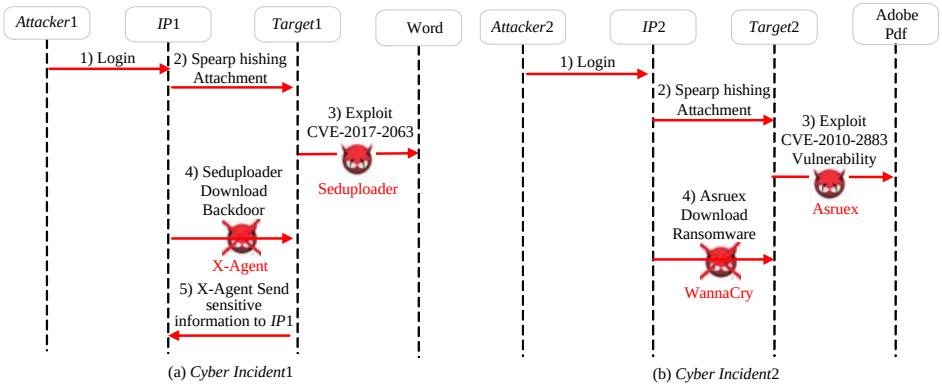


图 6 *Cyber Incident*1 和 *Cyber Incident*2 数据流

具体来说, *Attacker*1 利用 *IP*1 C2 服务器发送钓鱼邮件, *Target*1 打开钓鱼邮件附件触发基于 Microsoft Word 零日漏洞(CVE-2017-2063)实现的恶意代码 Seduploader 执行, Seduploader 从 *IP*1 服务器中下载后门工具 X-Agent, 进而 X-Agent 将 *Target*1 中的敏感信息发送至 *IP*1 的邮箱中; *Attacker*2 利用 *IP*2 C2 服务器发送钓鱼邮件, *Target*2 打开钓鱼邮件附件触发基于 Adobe Pdf 漏洞(CVE-2010-2883)实现的恶意代码 Asruex, Asruex 从 *IP*2 服务器中下载勒索病毒 WannaCry 并执行.

根据网络攻击事件(Cyber *Incident* 1 和 *Cyber Incident* 2)中分析提取的目标探测方法(Spearphishing Attachment)、攻击目标(*Target*1 和 *Target*2)、攻击工具(Seduploader、Asruex、X-Agent 和 WannaCry)、攻击目的(Steal Sensitive Information 和 Ransom)、利用漏洞信息(CVE-2017-2063 和 CVE-2010-2883)等攻击线索信息, 结合表 1 中 *Attacker*1 及 *Attacker*2 的攻击者威胁情报, 按照网络攻击事件溯源本体进行本体映射和实体对齐, 形成如图 7 所示的溯源关系图.

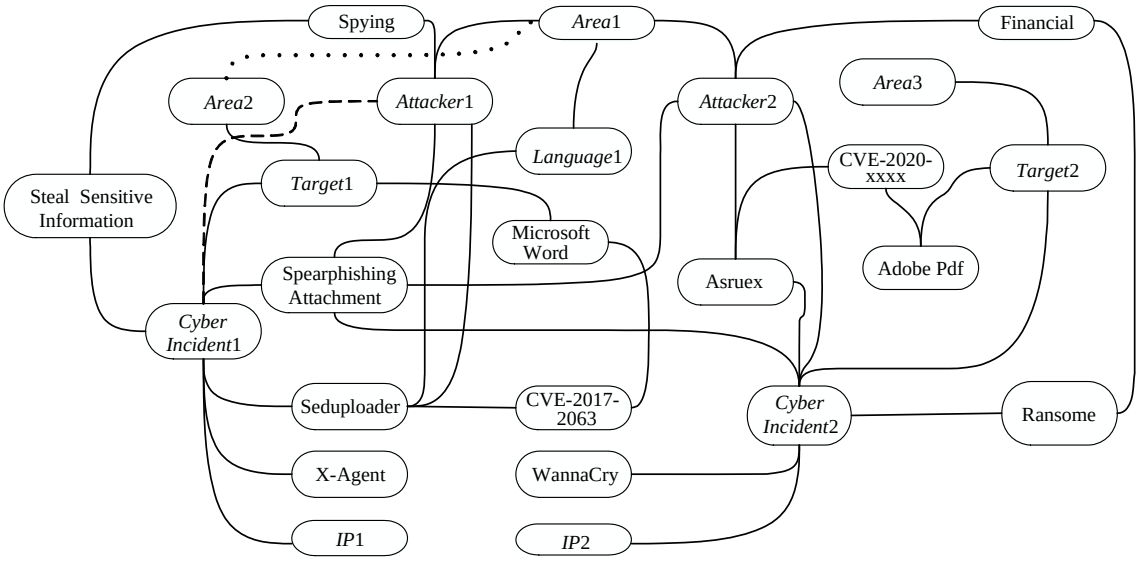


图 7 攻击溯源实验关系图

为了验证本文算法的特征提取能力, 我们首先将网络攻击事件与网络攻击者间的直接关联关系删除(如图 7 中"--"虚线所示), 尝试利用基于图嵌入的网络攻击事件自动特征提取算法生成网络攻击事件及攻击者的各个溯源实体特征向量(如表 2 所示, 其中, GECEFA 算法核心输入参数依据文献[19]设定为 *dim*=20, *attributionEntityListNum*=10, *attributionEntityListLen*=80, *winSize*=10), 验证其是否能够发现攻击事件与攻击者间的隐含关联关系.

表 2 *Cyber Incident*1 溯源实体特征向量示例

网络攻击事件溯源实体	特征向量
*Cyber Incident*1	[0.31503633 –0.2292631 –0.16837947 0.30400065 –0.2730783 –0.094090745 0.19904819 0.19169393 … 0.08717842 –0.2229294 0.049735274 –0.1393603]
Spying	[0.31179816 –0.21796714 –0.15583366 0.28965893 –0.30278617 –0.11816654 0.24400358 –0.073624246 … –0.23395094 0.01215893 –0.10738527]
*Area*2	[0.2812579 –0.35807425 –0.12953421 0.27463776 –0.32449752 –0.13647129 0.35081187 0.21411277 … 0.07754889 –0.45965984]
Seduploader	[0.2856931 -0.3336967 –0.14781223 0.28763297 –0.38636363 –0.17443292 0.41205558 0.281206 … 0.06979721 –0.31511995]
CVE-2017-2063	[0.33217767 –0.2864591 –0.17007424 0.33301264 –0.37664014 –0.17568526 0.33176097 0.21295169 … 0.065267056 –0.45379722]

计算攻击事件特征向量与攻击者间的皮尔森相关系数(*Cov* 表示协方差, σ表示标准差):

$$\rho_{X,Y}=\frac{Cov(X,Y)}{\sigma_X\sigma_Y} \tag{1}$$

计算攻击事件特征向量与攻击者间的距离相关系数(*dCov* 表示距离协方差, *dVar* 表示距离方差):

$$dCor(X,Y)=\frac{dCov(X,Y)}{\sqrt{dVar(X)dVar(Y)}} \tag{2}$$

利用公式(1)和公式(2)分别测试攻击事件特征向量与攻击者的不同画像维度相关性(见表 3), 可以看出: *Cyber Incident*1 与 *Attacker*1 的攻击动机、攻击目标区域、攻击工具、利用漏洞的皮尔森相关系数分别为 0.996、0.963、0.962、0.984, 均高于 *Cyber Incident*1 与 *Attacker*2 的皮尔森相关系数 0.762、0.582、0.585、0.672; *Cyber Incident*1 与 *Attacker*1 的攻击动机、攻击目标区域、攻击工具、利用漏洞的距离相关系数分别为 0.989、0.925、0.926、0.966, 均高于 *Cyber Incident*1 与 *Attacker*2 的距离相关系数的 0.497、0.299、0.304、0.391. 同理, *Cyber Incident*2 与 *Attacker*2 的攻击动机、攻击目标区域、攻击工具、利用漏洞的相关系数也均高于 *Cyber Incident*2 与 *Attacker*1 的各项相关系数.

表 3 网络攻击事件特征向量与攻击者的相关系数实验结果

相关性系数	网络攻击事件	*Attacker*1				*Attacker*2			
		攻击动机	目标区域	攻击工具	利用漏洞	攻击动机	目标区域	攻击工具	利用漏洞
皮尔森相关系数	*Cyber Incident*1	**0.996**	**0.963**	**0.962**	**0.984**	0.889	0.540	0.764	0.602
	*Cyber Incident*2	0.762	0.582	0.585	0.672	**0.971**	**0.946**	**0.996**	**0.968**
距离相关系数	*Cyber Incident*1	**0.989**	**0.925**	**0.926**	**0.966**	0.707	0.284	0.502	0.317
	*Cyber Incident*2	0.497	0.299	0.304	0.391	**0.922**	**0.909**	**0.990**	**0.935**

由上述实验结果可以得出, 基于图嵌入的网络攻击事件自动特征提取算法能够挖掘网络攻击事件与网络攻击者在攻击动机、攻击目标区域、攻击工具、利用漏洞等特征间的关联关系.

为了验证网络攻击事件溯源本体模型对地缘政治的融合能力, 首先假设 *Area*1 和 *Area*2 间存在地缘政治冲突; 然后利用网络攻击事件溯源本体模型进行数据融合, 在 *Area*1 和 *Area*2 间出现地缘政治冲突关系(如图 7 中"..."点线虚线所示); 最后, 与上述实验类似, 利用基于图嵌入的网络攻击事件自动特征提取算法生成网络攻击事件及攻击者的各个溯源实体特征向量, 并利用式(1)和式(2)计算网络攻击事件与目标区域的相关性(见表 4). 由表 3 和表 4 可以看出: 在融合了地缘政治冲突关系后, *Cyber Incident*1 与 *Area*2 的皮尔森相关系数 0.985 高于未考虑地缘政治冲突关系的皮尔森相关系数 0.963, 而 *Cyber Incident*1 与 *Area*3 的皮尔森相关系数 0.435 低于未考虑地缘政治冲突关系的皮尔森相关系数 0.540; 距离相关系数类似, 也出现了相应的增加和减少. 因 *Cyber Incident*2 的攻击者也属于 *Area*1 区域, 故其与 *Area*2 的相关度出现小幅度增加. 由此可以得出, 本文提出的网络攻击事件溯源本体模型在融合地缘政治关系和提取地缘政治隐含关系方面具有一定的优势.

表 4 网络攻击事件特征向量与目标区域的相关系数实验结果

相关性系数	网络攻击事件	*Area*2	*Area*3
皮尔森相关系数	*Cyber Incident*1	0.985	0.435
	*Cyber Incident*2	0.627	0.993
距离相关系数	*Cyber Incident*1	0.939	0.211
	*Cyber Incident*2	0.388	0.988

4.3 APT攻击事件溯源分析实验

为了进一步验证本文方法的有效性和准确性, 我们首先采集 2019 年上半年针对我国发起攻击较多的 APT32(海莲花)、APT37(Group123)和污水(MuddyWater)这 3 个攻击组织[1]的威胁情报数据和历史攻击事件(见表 5); 然后基于采集的数据集进行扩展, 将各个攻击者常用的攻击方法(*means*)、攻击工具(*tools*)、拥有基础设施(*IOC*)等按照杀伤链各个阶段进行分类; 从分类结果中按杀伤链各个阶段随机抽取攻击方法、攻击工具和基础设施构建模拟攻击杀伤链, 与已有的攻击目标、攻击动机等因素随机结合, 生成与已有攻击事件相同比例的模拟攻击事件, 由此得到的真实历史攻击事件和模拟攻击事件分布情况见表 5.

表 5　网络攻击数据集

攻击者	历史攻击事件数(件)	模拟攻击事件数(件)	攻击方法(种)	攻击工具(种)	基础设施(个)	地缘政治事件(件)
APT32	7	21	55	12	39	5
APT37	5	15	27	11	50	3
MuddyWater	3	9	31	3	167	0

针对上述数据集, 本文首先利用网络攻击事件溯源本体模型进行数据融合, 形成网络攻击溯源关系图(如图 8 所示), 并存储于 Neo4j 图形数据库, 利用基于图嵌入的网络攻击事件自动特征提取算法(GECEFA, 算法 1), 在图 8 所示的网络攻击溯源关系图中随机游走生成如表 6 所示的网络安全实体序列, 进而生成各个历史事件的特征向量(表 7 给出了其中 APT37 对应的特征向量示例, 其中, GECEFA 算法核心输入参数依据文献[19]设定为 *dim*=128, *attributionEntityListNum*=10, *attributionEntityListLen*=80, *winSize*=10).

然后基于交叉验证法[21], 分别使用支持向量机(support vector machines, SVM)、*k* 近邻(*k*-nearest neighbor, KNN)、决策树(decision tree)这 3 种分类器进行攻击者的判定, 并依据准确率[22]、精确率[22]、召回率[23]、*F*1 分数[24]及 ROC 曲线[25]等指标评价模型. 挖掘结果如表 8 和图 9 所示, 其中, SVM 分类器的准确率达到了 0.952, ROC 曲线中 AUC(area under curve)值达到 0.995, 优于文献[17]中提出的方法.

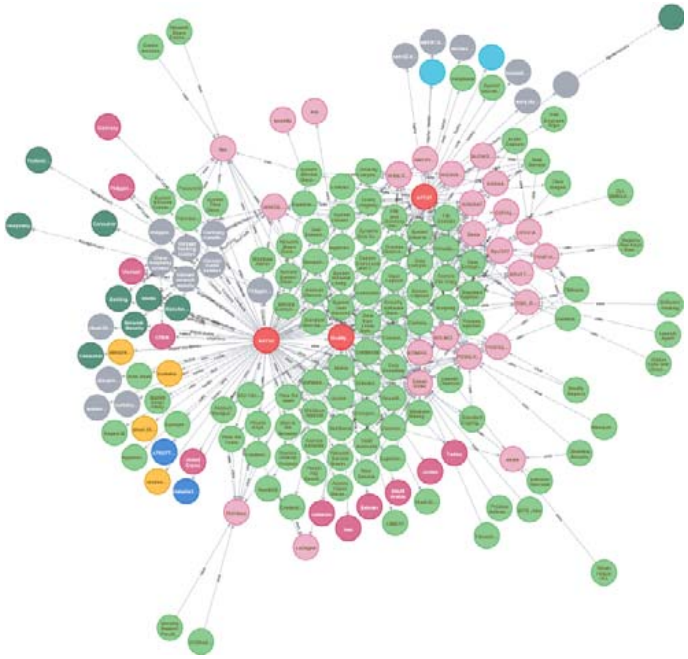


图 8　网络攻击溯源关系图示例

表 6　网络安全实体序列示例

序号	网络安全实体序列
1	[‘cloud.360cn.info’, ‘APT32’, ‘Process Discovery’, ‘Process Discovery’, ‘NavRAT’, ‘Command-Line Interface’, ‘Denis’, ‘Scripting’, ‘POWERSTATS’, …]
2	[‘Scripting’, ‘Cobalt Strike’, ‘Indicator Removal from Tools’, ‘Indicator Removal from Tools’, ‘Cobalt Strike’, ‘Windows Remote Management’, ‘APT32’, ‘Vietnam’, ‘Vietnam banking incident’, …]
3	[‘ourkekwiciver.comdieordaunt.comstraliaenollma.xyz’, ‘APT32’, ‘Exfiltration Over Command and Control Channel’, ‘APT37’, ‘Exploitation for Client Execution’, ‘APT32’, …]
4	[‘Standard Application Layer Protocol’, ‘APT37’, ‘Process Discovery’, ‘POORAIM’, ‘Web Service’, ‘DOGCALL’, ‘Audio Capture’, …]
5	[‘66.85.157.86’, ‘APT37’, ‘Audio Capture’, ‘DOGCALL’, ‘Obfuscated Files or Information’, ‘OSX_OCEANLOTUS.D’, ‘File Deletion’, ‘Denis’, …]

表 7 APT37 历史攻击事件特征向量示例

网络攻击事件溯源实体	特征向量
*Cyber Incident*1	[0.1818611 0.054629683 0.09002642 0.25070268 0.13314888 0.1568169 –0.17999335 0.2616101 –0.15407752 …]
*Cyber Incident*2	[0.1649639 0.2126497 0.0017947868 0.3686488 –0.21032447 –0.076248884 –0.10456581 0.20869191 –0.20489159 …]
*Cyber Incident*3	[0.3007822 0.00673637 –0.13540925 0.2864082 –0.23925436 –0.033850934 –0.079270884 0.23141465 –0.026851924 …]
*Cyber Incident*4	[0.16604747 –0.14231886 0.17420572 0.25907087 –0.16201456 0.1430352 0.061189238 0.3693804 0.0027026148 …]
*Cyber Incident*5	[0.1305695 0.22911757 –0.16194338 0.23060691 –0.36658522 0.023613885 0.087287396 0.2805204 –0.31468526 …]

由此可以看出：本文提出的算法可自动提取网络攻击事件的关联特征，充分利用了攻击事件的多维度关联信息，通过 SVM 分类器实现针对网络攻击者的判定，从而达到攻击溯源的目的.

表 8 攻击者挖掘分析结果

溯源方法	分类器	准确率	精确率	召回率	*F*1 分数
本文方法	SVM	0.952	0.961	0.941	0.949
	KNN	0.857	0.857	0.836	0.845
	Decision tree	0.523	0.488	0.467	0.470
文献[17]	Random forest	0.88	0.92	0.89	0.89
	DLNN	0.94	0.90	0.89	0.89

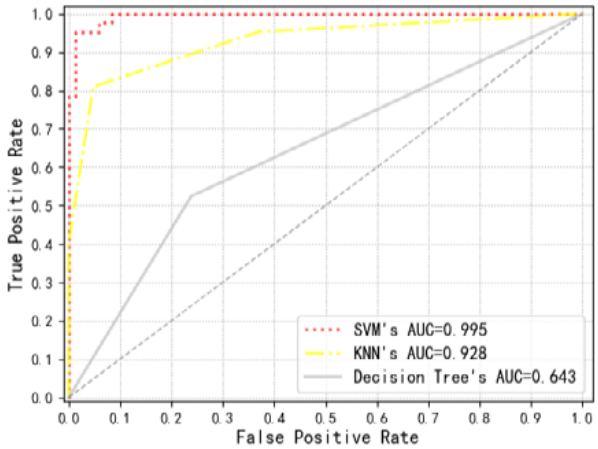


图 9 SVM、KNN、Decision Tree 的 ROC 曲线

5 结 语

本文针对当前网络攻击溯源工作过度依赖人工分析的局限性，提出了一种基于图模型的网络攻击溯源方法：建立网络攻击事件溯源本体模型，融合攻击事件线索数据与威胁情报，形成网络攻击事件溯源关系图；利用基于随机游走的图嵌入算法，从溯源关系图中自动提取网络攻击事件的关联特征，形成网络攻击事件特征向量；引入机器学习分类器，通过对网络攻击者的挖掘分析，判断攻击事件与攻击者之间的归属关系，从而实现网络攻击溯源. 本文根据实际的 APT 攻击组织数据，构造了测试数据和实验环境，对本文提出的本体模型、特征提取算法和攻击者判定算法的可行性及有效性进行了验证.

后续研究工作包括：进一步细化网络攻击链各个阶段的特点、网络攻击组织随着时间和技术积累攻击手段的演进过程等因素；并基于攻击链各个阶段的依赖性和时间性的考虑，可在图模型的基础上引入 LSTM 等能够提取依赖性因素和时间性因素的模型，以进一步优化模型.

References:

[1] Security T. Global advanced persistent threat research report for the first half of 2019. 2020 (in Chinese). https://s.tencent.com/research/report/762.html

[2] Cyber Security Observatory. Top 5 cybersecurity facts, figures and statistics for 2017. 2020. https://www.cybersecobservatory.com/2017/06/15/top-5-cybersecurity-facts-figures-statistics-2017/

[3] Karafili E, Wang L, Lupu EC. An argumentation-based approach to assist in the investigation and attribution of cyber-attacks. arXiv Preprint arXiv: 1904.13173, 2019.

[4] Wheeler DA, Larsen GN. Techniques for cyber attack attribution. Technical Report, Institute for Defense Analyses, 2003.

[5] Cohen D, Narayanaswamy K. Attack attribution in non-cooperative networks. In: Proc. of the 5th Annual IEEE SMC Information Assurance Workshop. IEEE, 2004. 436–437.

[6] Kuznetsov V, Sandström H, Simkin A. An evaluation of different ip traceback approaches. In: Proc. of the Int'l Conf. on Information and Communications Security. Berlin, Heidelberg: Springer, 2002. 37–48.

[7] Dacier M, Pham VH, Thonnard O. The WOMBAT attack attribution method: Some results. In: Proc. of the Int'l Conf. on Information Systems Security. Berlin, Heidelberg: Springer, 2009. 19–37.

[8] Ahmed I, Obermeier S, Naedele M, *et al*. Scada systems: Challenges for forensic investigators. Computer, 2012, 45(12): 44–51.

[9] Mahmood AN, Leckie C, Hu J, *et al*. Network traffic analysis and SCADA security. In: Handbook of Information and Communication Security. Berlin, Heidelberg: Springer, 2010. 383–405.

[10] Falliere N, Murchu LO, Chien E. W32.stuxnet dossier. White Paper, Symantec Corp., Security Response, 2011, 5(6): 29.

[11] Carr J. Inside Cyber Warfare: Mapping the Cyber Underworld. O'Reilly Media, Inc., 2011.

[12] Cook A, Nicholson A, Janicke H, *et al*. Attribution of cyber attacks on industrial control systems. Industrial Networks and Intelligent Systems, 2016, 3(7): 1–15.

[13] Saad S, Traore I. Ontology-based intelligent network-forensics investigation. In: Proc. of the SEDE. 2010. 313–319.

[14] Qamar S, Anwar Z, Rahman MA, *et al*. Data-driven analytics for cyber-threat intelligence and information sharing. Computers & Security, 2017, 67: 35–58.

[15] Boebert WE. A survey of challenges in attribution. In: Proc. of the Workshop on Deterring CyberAttacks. 2010. 41–54.

[16] Liu CG, Fang BX, Liu BX, *et al*. A hierarchical model of targeted cyber attacks attribution. Journal of Cyber Security, 2019, 4(4): 1–18 (in Chinese with English abstract).

[17] Noor U, Anwar Z, Amjad T, *et al*. A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise. Future Generation Computer Systems, 2019, 96: 227–242.

[18] Cai H, Zheng VW, Chang KCC. A comprehensive survey of graph embedding: Problems, techniques, and applications. IEEE Trans. on Knowledge and Data Engineering, 2018, 30(9): 1616–1637.

[19] Grover A, Leskovec J. node2vec: Scalable feature learning for networks. In: Proc. of the 22nd ACM SIGKDD Int'l Conf. on Knowledge Discovery and Data Mining. ACM, 2016. 855–864.

[20] Goyal P, Ferrara E. Graph embedding techniques, applications, and performance: A survey. Knowledge-based Systems, 2018, 151: 78–94.

[21] Wikipedia. Cross-validation (statistics). 2020. https://en.wikipedia.org/wiki/Cross-validation_(statistics)

[22] Wikipedia. Accuracy and precision. 2020. https://en.wikipedia.org/wiki/Accuracy_and_precision

[23] Wikipedia. Precision and recall. 2020. https://en.wikipedia.org/wiki/Precision_and_recall

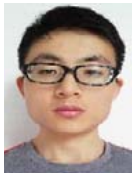
[24] Wikipedia. *F*1 score. 2020. https://en.wikipedia.org/wiki/F1_score

[25] Wikipedia. Receiver operating characteristic. 2020. https://en.wikipedia.org/wiki/Receiver_operating_characteristic

附中文参考文献:

[1] 腾讯安全. 全球高级持续性威胁(APT)2019 年上半年研究报告. 2020. https://s.tencent.com/research/report/762.html

[16] 刘潮歌, 方滨兴, 刘宝旭, 等. 定向网络攻击追踪溯源层次化模型研究. 信息安全学报, 2019, 4(4): 1–18.



黄克振(1988－), 男, 工程师, 主要研究领域为网络与系统安全测评.

连一峰(1974－), 男, 博士, 研究员, 博士生导师, 主要研究领域为网络与系统安全测评.

冯登国(1965－), 男, 博士, 研究员, 博士生导师, CCF 会士, 主要研究领域为信息安全.

张海霞(1981－), 女, 博士, 高级工程师, 主要研究领域为网络与系统安全测评.

吴迪(1977－), 女, 博士, 高级工程师, 主要研究领域为信息安全测评.

马向亮(1986－), 男, 博士, 主要研究领域为信息安全, 密码工程, 与侧信道攻防技术.