基于关联增强的网络威胁情报技战术分类

葛文翰[1]，王俊峰[1]，唐宾徽[2]，于忠坤[1]，陈柏翰[1]，余 坚[1]
(1. 四川大学计算机学院，成都 610065；2. 四川大学网络空间安全学院，成都 610065)

摘 要：网络威胁情报(Cyber Threat Intelligence，CTI)的技战术(Tactics，Techniques and Procedures，TTPs)分析能够为网络攻击事件提供全局视图，并揭示系统弱项，是网络攻击溯源的关键技术. 现有分类 TTPs 方案面向抽象语言环境效果较差且不平均. 本文提出一种基于关联增强的多标签深度学习模型 RENet，通过使用结合上下文信息和多词语义的多标签分类器对战术和技术进行分类，并通过技战术条件转移矩阵将原有战术的分类结果转移到技术中增强技术分类. 实验表明，RENet 比其他分类模型有更精确的技战术分类效果与更快的收敛速度. 在英文数据集上，RENet 对技术和战术分类的 F_1 分数比现有最好的模型分别提高 4.62%和 0.78%，在中文数据集上提高 3.95%和 3.77%.

关键词：网络威胁情报；技战术分析；多标签分类；关联增强；ATT&CK；IoC 识别
中图分类号：TP183 **文献标识码**：A DOI：10.19907/j.0490-6756.2022.023004

RENet：tactics and techniques classifications for cyber threat intelligence with relevance enhancement

GE Wen-Han[1], *WANG Jun-Feng*[1], *TANG Bin-Hui*[2], *YU Zhong-Kun*[1], *CHEN Bo-Han*[1], *YU Jian*[1]
(1. College of Computer Science, Sichuan University, Chengdu 610065, China;
2. School of Cyber Science and Engineering, Sichuan University, Chengdu 610065, China)

Abstract: Tactics, Techniques and Procedures (TTPs) analysis in Cyber Threat Intelligence (CTI), is a key technique for cyberattack traceability which providing a global view of cyberattack events and revealing system weaknesses. Existing TTPs classification schemes are poorly and unevenly oriented to abstract language environments. In this paper, we propose a multi-label deep learning model based on association enhancement: RENet, which classifies tactics and techniques by using a multi-label classifier that combines contextual information and multiple word meanings, and enhances technique classification by transferring the classification results of the original tactics through a conditional transfer matrix from tactics to techniques. Experiments show that RENet has more accurate classification results of tactics and techniques with faster convergence than other classification models. The F1 scores of RENet for techniques and tactics classification are 4.62% and 0.78% higher than the best existing models on the English dataset, and 3.95% and 3.77% higher on the Chinese dataset, respectively.

Keywords: Cyber Threat Intelligence (CTI); Tactics, Techniques and Procedures (TTPs) analysis; Multi-label classification; Relevance enhancement; ATT&CK; IoC recognition

收稿日期：2021-09-14
基金项目：国家重点研发计划(2019QY1400)；国家自然科学基金(U2133208)；四川省青年科技创新研究团队基金(2022JDTD0014)
作者简介：葛文翰(1997－)，四川成都人，硕士研究生，研究方向为网络空间安全. E-mail：gewenhan@stu.scu.edu.cn
通讯作者：王俊峰. E-mail：wangjf@scu.edu.cn

1 引　言

作为网络分析知识的重要信息来源渠道,网络威胁情报(Cyber Threat Intelligence, CTI)可以将零碎的信息组织成“基于证据的现有或新兴知识”[1].这些零碎的证据信息,也称妥协指标(Indicators of Compromise, IoCs)[2],可以帮助建立完整的网络攻击场景模型.目前比较认可的对 IoCs 信息的分级主要是由 David 提出的 IoCs 价值和成本测量系统:“痛苦金字塔模型”(Pyramid of Pain, PnP)[3].其中 IoCs 等级的增加标志着其价值和获取难度的同步增加.根据 PnP 的描述,直观的 IoCs 信息,比如 IP 地址或 Hash 值等,属于金字塔较低层次.这类信息通常具有相似结构或相似特征.而处在金字塔层级较高的是比较抽象的信息,比如恶意软件、工具、网络结构等.这类信息一般由多种描述方式,例如名称、行为、Hash 甚至作者,造成 CTI 描述的多样性.

经过多年发展,较为低级的 IoCs 信息已经能够被有效识别[2,4-6].部分较高等级的 IoCs 信息也能通过使用机器学习进行有效分析.Jang 等[7]使用卷积神经网络(Convolutional Neural Networks, CNN)通过代码特征图分类恶意软件.Deliu 等[8]通过支持向量机(Support Vector Machines, SVM)和潜在 Dirichlet 分解抽取恶意工具.

最高等级的 IoCs,战术、技术和过程(Tactics, Techniques and Procedures, TTPs)[9,10]不仅能对袭击事件提供全局预览,也能侧面反映现有系统的系统或防御策略的弱项或漏洞.TTPs 通常出现在网络威胁报告(Cyber Threat Reports, CTR)中,是对网络攻击事件过程的描述,通常包含代码、描述文本、图像等细节,因此 TTPs 的分析一般围绕非结构化文本开展[11].目前针对 TTPs 的 CTI 分析尚处在初期.TTPDrill [12]和 ActionMiner[13]虽然能够将 CTR 中的技术信息组织成为满足 STIX 框架[14]的结构体,但由于其过度依赖人工先验知识而无法分析战术并完成事件过程的合理推导.Legoy 等[11]通过开源数据和 Scikit-learn [15]实现了一个开源的工具集 rcATT 用于分类 TTPs.由于缺乏对文本依赖的处理,即便 rcATT 将技战术相关性作为数据后处理机制的方式,其实际分类效果也无法达到理想条件($F_{0.5}^{(\mathrm{tact})}=59.47\%$,$F_{0.5}^{(\mathrm{tech})}=27.52\%$).其原因一方面是其技战术相关性主要建立在战术分类结果上,必须等待战术训练完毕后方能进行技术的训练,具有滞后性和异步性且过程单向;另一方面是其关系的迭代存在人工定义的阈值,对人工依赖严重,且易导致其训练过程震荡或提升效果不明显.

针对当前 TTPs 分类效果差、不平均,人工关系不明确的问题,本文提出使用基于关联增强的技战术分类模型 RENet.该模型使用双向循环神经网络(Bidirectional Recurrent Neural Networks, BiRNN)和 CNN 作为基础分类器,并通过使用可自我学习和优化的技战术关联矩阵为引导的关联增强模块增强技术分类的效果.本文对 RENet 就中英文分别进行了工具化并开源到 Github 上(https:// github. com/MuscleFish/RENet),以供其他需求者使用.

2 相关工作

网络威胁报告(Cyber Treat Reports, CTR)是 CTI 中的一类情报.这类情报主要由人工撰写的安全文章、博客或其他文本组成[11].与之前的结构化数据相比,CTR 由于由多人撰写发布,不具备预定义且完整的描述规则或行文格式,因此被普遍认为是非结构化文本.随着网络安全事件的发生频率越来越高,大量的 CTR 和安全事件被各大安全公司和安全专家披露.在这种情况下,使用 CTR 作为安全知识信息库的情报来源,无疑是一种有效选择.

智能分析 CTR 的方法普遍分为两种:信息抽取(Information Extraction,IE)和分类方法.IE 的目标是通过筛选和查找具有特定语义的信息完成信息的检索工作[2].在传统的网络安全分析中,基于规则的方法擅长处理信息完整的结构化数据,如日志[16]和网络流量[17].基于规则的方法[18]可以在特定的结构或模式中优先识别特定的数据,同时保证其方法具有较好的通用性.IP 地址、Hash 和 URLs 是比较常见的结构化数据,围绕这部分数据的工作已有很多[2,4-6].命名实体识别(Named Entity Recognition,NER)[19]是目前较为主流的 IE 全监督学习方法.通过该方法,绝大多数的 IoCs 信息能够被结构化为特定的结构信息方便存取[14].但因为 IoCs 的高级信息的多描述、跨语句的特性,NER 并不能适用于此类信息抽取的场景.

分类方法是智能分析 CTR 的另一种方法,其特点在于对全局信息的把控而非对局部信息的抽

取. 因此现有分类方法对 CTR 的高级 IoCs 或全局信息的识别和定义能力明显强于 IE. Wang 等[20]使用 TextCNN 识别源代码. Zhao 等[21]使用全连接神经网络(Fully-Connected Neural Network，FC-NN)判别网络文章是否属于 CTI 情报. Grisham 等[22]使用 RNN 从 CTI 中识别恶意代码. Dang 等[23]使用 BiLSTM-CNN 的方式分类恶意软件.

作为 PnP 所定义的最高级的 IoCs，TTPs 在分析 CTI 的过程中扮演了串联事件、还原攻击的作用[9]. 当前针对 TTPs 的分析框架主要包括攻击链[24]、网络攻击生命周期[25]和 ATT&CK [26]. 由于 ATT&CK 较新且描述完整，目前大多数分析工作普遍围绕 ATT&CK 和其结构化描述框架 STIX[14]开展. ActionMiner[13]和 TTPDrill[12]作为从 CTR 分析 TTPs 的工具，采用的是结构化 STIX 信息作为抽取技术的关键. 其方法围绕抽取特定的关键细节为蓝本，构造对特殊词汇的技术描述. 虽然其出具结果比较优秀，但一方面这个过程过多依赖专家经验导致效果难以复现，另一方面此二者无法有效分析比技术更加抽象的战术信息. 正是由于发现了这个事实，Seifert 提出开源 TTPs 分析工具 rcATT[11]. 该工具使用以 SVM 为主的机器学习作为分类 TTPs 的核心，虽然能够有效解决人工分析的压力，但由于其在战术和技术上的分类效果较差且差距过大，导致其分析结果并不十分可信.

值得注意的是，ATT&CK 所制定的技战术具有严格的从属划分，对于特定的技术，一般只出现于 1～2 个战术中. 正是考虑到这点，rcATT 合理运用该关系修正了部分分类效果，但是该成果并不显著. 其原因可能是人工定义的关系和迭代阈值不能精确区分和划分技战术关系的重要性区间和迭代值，造成一定程度的无法进化. rcATT 选择的技术增强是典型的后处理，通过将战术分类结果输入 SVM 分类器作为特征进行技术分类，其假设的条件是战术分类结果正确且关系正确. 虽然提高了技术的部分准确性但效果不可逆，即技术的分类推导无法提高战术分类效果.

因此本文考虑使用多任务分类模型作为抽取技战术信息的模型. 该模型将同时训练技战术分类，并在分类过程中对技术分类的效果产生指导，合理优化技战术关系，提高技战术分类准确性.

3　方法原理

作为多标签深度学习模型，RENet 主要包含两个任务：一个是多标签分类任务；另一个是使用关联增强修正技术的分类结果. 本章节将就上述两个目标做数学推导和模型结构说明.

3.1　模型结构

图 1 展示了 RENet 的网络模型结构. RENet 主体分为两个相互独立分类器，一个管理战术分类，另一个管理技术分类. 其独立性体现在两个模型的权重和层的不共享. 在分类器尾部 RENet 使用关联增强的方式将战术的分类效果迁移至技术分类器上共同维护技术的分类效果.

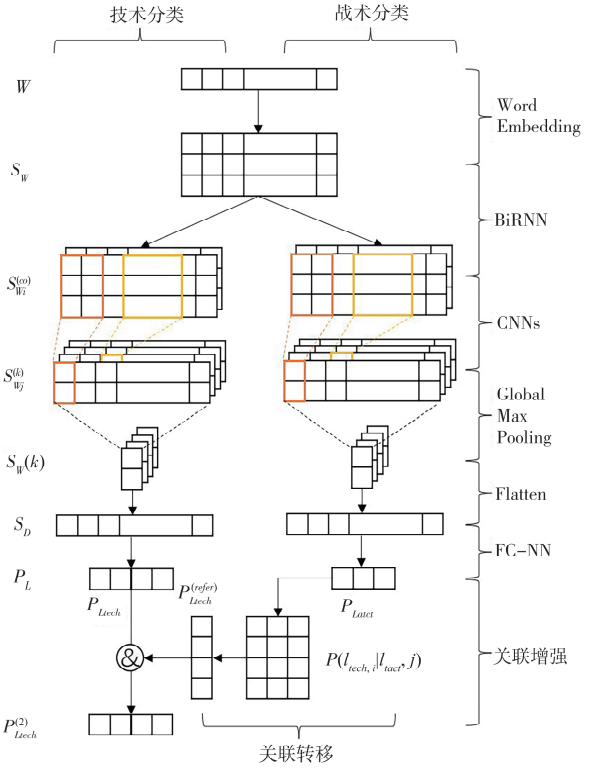

图 1　RENet 网络结构与数学表达对应关系

Fig. 1　RENet network structure and mathematical expression correspondence

3.2　技战术分类器

RENet 的分类器是由 BiRNN [27]和 CNN 共同组成的 TextRCNN 模型[28]. 分类器通过式(1)完成分类任务. 该任务要求分类器 Cls 根据文档 D 推导其标签列表 L. 因此 Cls 的方法实际上是一个由 D 到 L 的映射.

$$Cls: D \rightarrow L \tag{1}$$

事实上，通常文档 D 是由单词词汇 W 组成的，通过合理表征 W 就能够合理表示 D 的特征. 而单词 W 的表征，一般通过词嵌入学习的方式获取其词向量 S_W. 同时对标签 L 列表的表示也可以通过其概率模型 P_L 表示. 因此式(1)也可以被表示

成式(2).

$$Cls: S_W \rightarrow P_L \tag{2}$$

BiRNN 为原始的S_W提供上下文信息,通过该上下文,$S_{w_i} \in S_W$可被表示成为式(3)中的$S_{w_i}^{(co)}$. 其中W_f为前序 RNN 的权重;b_f为其偏移量;W_b为后序 RNN 的权重;b_b为其偏移量.

$$S_{w_i}^{(co)} = [W_f S_{w_{i-1}}^{(co)} + b_f; S_{w_i}; W_b S_{w_{i+1}}^{(co)} + b_b] \tag{3}$$

CNN 负责针对由 RNN 产生的上下文向量$S_{w_i}^{(co)}$进行 k-gram 合并. k-gram 是指连续 k 个向量$S_{w_i}^{(co)}$合并为一个向量$S_{w_j^{(k)}}$. 这个过程参考式(4). 针对第 j 位的 k-gram 向量$S_{w_j^{(k)}}$,其数值满足 k-gram CNN 对该位连续 k 个上下文向量$S_{w_i}^{(co)}$的加权求和. 其中$W_{i-j,k}$为 k-gram CNN 的共享权重,$b_j^{(k)}$为其偏移量.

$$S_{w_j^{(k)}} = \sum_{i=j}^{j+k-1} W_{i-j,k} \cdot S_{w_i}^{(co)} + b_j^{(k)} \tag{4}$$

在 CNN 获取 k-gram 词向量后,最大池化层将从所有$S_{w_j^{(k)}}$中,按照 k-gram 划分求取最大的 k-gram 特征$S_{W^{(k)}}$. 该特征可以表示为式(5).

$$S_{W^{(k)}} = \max(S_{w_j^{(k)}}) \tag{5}$$

式(6)负责将所有的 k-gram 特征$S_{W^{(k)}}$合并为一个特征S_D,该特征将表示原本文档 D 的特征.

$$S_D = [S_{W^{(1)}}; S_{W^{(2)}}; \cdots; S_{W^{(k)}}] \tag{6}$$

通过使用式(7),文档特征向量S_D将转化为标签概率P_L. 其中W_L和b_L分别是其权重和偏移量. σ是 sigmoid 激活函数.

$$P_L = \sigma(W_L S_D + b_L) \tag{7}$$

通过实现式(3)~(7),式(2)得以实现. 由于 RENet 存在独立的技战术分类器,因此技术和战术的分类将被分别描述为式(8)和式(9).

$$Cls_{\text{tech}}: S_W \rightarrow P_{L_{\text{tech}}} \tag{8}$$

$$Cls_{\text{tact}}: S_W \rightarrow P_{L_{\text{tact}}} \tag{9}$$

3.3　关联增强

RENet 的关联增强目的在于使用战术的分类结果和技战术相关性限制技术分类所产生的误差. 由于技战术在 Mitre 所定义的 ATT&CK 框架中存在从属的特点(战术$\xrightarrow{1:n}$技术). 当确定没有相关战术出现的时候,能够很大意义上排除一部分与该战术相关技术. 对于剩下的技术而言,模型能够较好地进行分类,同时确保技术分类的梯度不会过早消失.

战术分类结果$P_{L_{\text{tact}}}$将通过关联转移矩阵 $P(l_{\text{tech},i} | l_{\text{tact},j})$,$l_{\text{tech},i} \in L_{\text{tech}}$,$l_{\text{tact},j} \in L_{\text{tact}}$将自己的影响传递给技术分类. 这种影响可以被表示成式(10).

其中$P_{l_{\text{tact},j}} \in P_{L_{\text{tact}}}$. 由于分类器是多标签分类器,因此$\sum_j P_{l_{\text{tact},j}}$并不总是为 1,为了完成归一化,影响的计算将除以$\sum_j P_{l_{\text{tact},j}}$.

$$P_{l_{\text{tech},i}}^{(\text{refer})} = \frac{\sum_j P(l_{\text{tech},i} | l_{\text{tact},j}) \cdot P_{l_{\text{tact},j}}}{\sum_j P_{l_{\text{tact},j}}} \tag{10}$$

在获取到影响$P_{l_{\text{tech},i}}^{(\text{refer})}$后,需要将该影响整合到原有技术的分类结果中. 用于使用关联增强的初衷是限制技术标签的出现范围,因此该影响的发挥将主要依赖于使用“与”操作,如式(11). 只有当影响$P_{l_{\text{tech},i}}^{(\text{refer})}$未限制标签$l_{\text{tech},i}$的出现,且文本有该标签出没的语义时,该标签才能被正常表达,否则将不予显示.

$$P_{l_{\text{tech},i}}^{(2)} = AND(P_{l_{\text{tech},i}}^{(\text{refer})}, P_{l_{\text{tech},i}}) \tag{11}$$

事实上,标签$l_{\text{tech},i}$的概率并不是非 0 即 1 的. 在深度模型中无论是$P_{l_{\text{tech},i}}^{(\text{refer})}$还是$P_{l_{\text{tech},i}}$都长期处于 0 到 1 之间. 这将导致无法正常使用“与”操作. 因此 RENet 使用 min 函数作为替代方案,min 同样能达到“与”操作的目的,如式(12).

$$P_{l_{\text{tech},i}}^{(2)} = \min(P_{l_{\text{tech},i}}^{(\text{refer})}, P_{l_{\text{tech},i}}) \tag{12}$$

4　算法仿真与实验结果

本文基于 ATT&CK 知识库数据,我们将使用 ATT&CK 技战术数据就 RENet 和其他常用 CTI 分析模型作比较,以验证 RENet 在分类 TTPs 上的效果.

4.1　实验准备

本文使用的数据源为 MITRE 公司官方网站提供的针对 ATT&CK V8 语句公开标注. 表 1 展示了 Mitre 官网[26]针对技术 T1548.002 的描述实例参考. 通过数据清洗和去重后形成对 14 个战术和 184 个主要技术的 6504 条描述语句. 并通过翻译和校对的方式形成了带有技战术标签的中英文数据集. 各数据集将按照 6∶4 的比例被分割为训练集和测试集. 由于技战术分类是多标签分类,本文将使用 Precision-Recall 和 F_β 分数为评价指标[29]. 针对该数据集文本,使用 Bert [30]作为其预训练词嵌入模型.

为有效分析 RENet 的分类效果,如下模型将被作为横向对比实验. 所有对比模型均被设计为和 RENet 类似的多任务模型.

(1) rcATT: rcATT [11]作为目前全监督技战术分类的模型,在使用以线性 SVM 为分类器时能够达到其最好的结果.

表 1　ATT&CK 官网对技术 T1548.002 的语句标注

Tab. 1　An instance of some examples to explain T1548.002 given by the website of Mitre ATT&CK framework

技术名称	绕过用户账户控制
技术 ID	T1548.002
技术网址	https://attack.mitre.org/versions/v8/techniques/T1548/002/
描述实例	
攻击组织	描述
APT29	APT29 has bypassed UAC.
APT37	APT37 has a function in the initial dropper to bypass Windows UAC in order to execute the next payload with higher privileges
AutoIt backdoor	AutoIt backdoor attempts to escalate privileges by bypassing User Access Control.
BlackEnergy	BlackEnergy attempts to bypass default User Access Control (UAC) settings by exploiting a backward-compatibility setting found in Windows 7 and later.
BRONZE BUTLER	BRONZE BUTLER has used a Windows 10 specific tool andxxmm to bypass UAC for privilege escalation.

(2) FC-NN：FC-NN 作为 Zhao [25] 判别网络文章是否属于 CTI 的分类器的核心，在本文的实验中将被重构为多标签技战术分类模型.

(3) TextCNN：在 Wang [24] 的实验中，TextCNN 被用于识别源代码的分类，并取得了不错的效果. 因此本文选择使用经过技战术分类的 TextCNN 作为对比模型.

(4) BiRNN：Grisham[26] 使用 RNN 模型作为从 CTI 中分类恶意代码的方式. BiRNN [31] 在 RNN 的基础上使用双向机制讲古抽取上下文信息. 在本文中将使用 BiRNN 作为对比模型之一.

(5) BiRNN-CNN：作为 BiRNN 和 CNN 的混合模型，该模型兼顾了 RNN 在上下文记忆和 CNN 在高维抽象上的优势，因此，在 Dang [27] 的实验中表现良好.

(6) TextRCNN：TextRCNN[28] 是 RENet 分类器的核心. 设计目标是验证在没有使用关联增强的前提下，TextRCNN 的分类结果能否与 RENet 相同. 以此验证关联增强的有效性和必要性.

4.2　RENet 变种

RENet 的关联分析矩阵 $P(l_{\text{tech},i}|l_{\text{tact},j})$ 同时具备人工初始化和自我训练优化的优点，因此本文将设计如下变种用来验证不同关系初始化和优化方式对技战术分类效果的影响. 这些变种主要包括：

(1) 0-RENet：该模型使用未经过人工初始化的关联转移矩阵，其所有 $P(l_{\text{tech},i}|l_{\text{tact},j})$ 均初始化为 0. 其设计目的在于检验模型能否更具自身需要设计技战术关系实现分类

(2) a-RENet：该模型使用经过人工初始化的技战术关联关系. 人工初始化关系我们参考 ATT&CK 官网，对每个有从属关系的技战术 $P(l_{\text{tech},i}|l_{\text{tact},j})$ 赋值 0.1.

(3) la-RENet：该模型同样适用人工初始化的技战术关系为关联转移条件. 与 a-RENet 不同的是，其关系是锁定的. 这意味着关系不会随着训练的进行改变. 该模型的设计是目标是检测从属关系是否为技战术主要关系.

4.3　结果与讨论

表 2～表 5 分别展示了 RENet 变种与对比模型在中英文数据集上对技战术分类测试集的结果.

表 2　中文数据集战术分类结果

Tab. 2　Chinese dataset tactics classification results

模型	Recall/%	Precision/%	F_1/%	$F_{0.5}$/%
rcATT	72.64	88.85	79.93	85.05
FC-NN	69.19	82.65	75.33	79.56
TextCNN	77.27	87.93	82.26	85.57
BiRNN	77.27	85.83	81.33	83.97
BiRNN-CNN	73.23	87.48	79.73	84.20
TextRCNN	79.17	87.57	83.16	85.75
0-RENet	84.97	87.86	86.39	87.27
a-RENet	83.46	87.32	85.35	86.52
la-RENet	84.34	89.78	86.98	88.64

表 3　中文数据集技术分类结果

Tab. 3　Chinese dataset techniques classification results

模型	Recall/%	Precision/%	F_1/%	$F_{0.5}$/%
rcATT	52.99	88.25	66.22	77.89
FC-NN	43.05	87.16	57.63	72.34
TextCNN	59.97	90.02	71.99	81.82
BiRNN	62.99	89.29	73.87	82.41
BiRNN-CNN	65.11	86.55	74.31	81.20
TextRCNN	66.77	87.01	75.56	82.03
0-RENet	72.36	87.09	79.04	83.68
a-RENet	72.36	87.73	79.30	84.15
la-RENet	73.26	86.92	79.51	83.70

表 4　英文数据集战术分类结果

Tab. 4　English dataset tactics classification results

模型	Recall/%	Precision/%	F_1/%	$F_{0.5}$/%
rcATT	75.18	90.12	81.98	86.68
FC-NN	66.75	83.59	74.23	79.58
TextCNN	75.02	86.65	80.42	84.04
BiRNN	73.34	85.61	79.00	82.84
BiRNN-CNN	75.66	83.89	79.57	82.11
TextRCNN	72.89	84.76	78.38	82.09
0-RENet	79.73	83.90	81.76	83.03
a-RENet	80.57	85.07	82.76	84.13
la-RENet	79.21	85.45	82.21	84.12

表 5　英文数据集技术分类结果

Tab. 5　English dataset techniques classification results

模型	Recall/%	Precision/%	F_1/%	$F_{0.5}$/%
rcATT	44.31	88.25	58.99	73.64
FC-NN	42.01	83.63	55.92	69.80
TextCNN	48.60	87.34	62.45	75.33
BiRNN	48.51	86.75	62.22	74.94
BiRNN-CNN	52.94	85.55	65.40	76.16
TextRCNN	53.75	86.86	66.41	77.33
0-RENet	62.06	80.16	69.96	75.74
a-RENet	61.97	81.47	70.40	76.65
la-RENet	61.70	83.70	71.03	78.13

根据表 2～表 5 结果可以产生如下推论.

(1) RENet、BiRNN-CNN 和 TextRCNN 在总体分析结果上优于单独使用 TextCNN 或 BiRNN. 这说明 RENet、BiRNN-CNN 和 TextRCNN 能够有效兼顾 RNN 和 CNN 的优势.

(2) 使用关联增强的 RENet 无论是在战术的分类还是技术的分类上都优于不用关联增强的 TextRCNN. 这说明关联增强起到了一定的作用.

(3) 经过人工关系初始化的 a-RENet 和 la-RENet 比未经过初始化的 0-RENet 表现效果好. 其原因可能是在训练的初期引入了较少的误差使得模型能够获得并学习更加有效且准确的参数.

(4) la-RENet 比 a-RENet 的效果好. 可能是由于技战术的关系主要以 ATT&CK 所定义的从属关系为主,同时锁定的关系能够进一步降低训练误差.

(5) 中文数据集的效果优于英文数据. 其可能原因是中文描述的多样性低于英文描述,导致词汇的分布较为集中,引起效果的提升.

此外,图 2 和图 3 分别反映了在中英文数据集中测试集技术分类效果随训练次数的变化. 可以发现使用了关联增强的 RENet 在拟合能力上快于其他没有使用关联增强的对比模型. 其可能的原因在于,RENet 的关联增强模块能够优先将战术的限制传递到技术的训练上,造成技术的训练从原本的随机梯度下降转变为半随机梯度下降,即有指向性的迭代分类参数,迫使技术分类器能够快速获取进化的方向,完成拟合.

图 4～图 8 分别反映了经过训练后不同 RENet 变种的关联转移模块权重 $P(l_{\text{tech},i}\,|\,l_{\text{tact},j})$ 的邻接矩阵热力图. 通过对比图 4～图 6,可以发现虽然存在噪声但 3 种 RENet 的技战术关联信息大致接近,同时模型对技战术的关联和联想存在优先级.

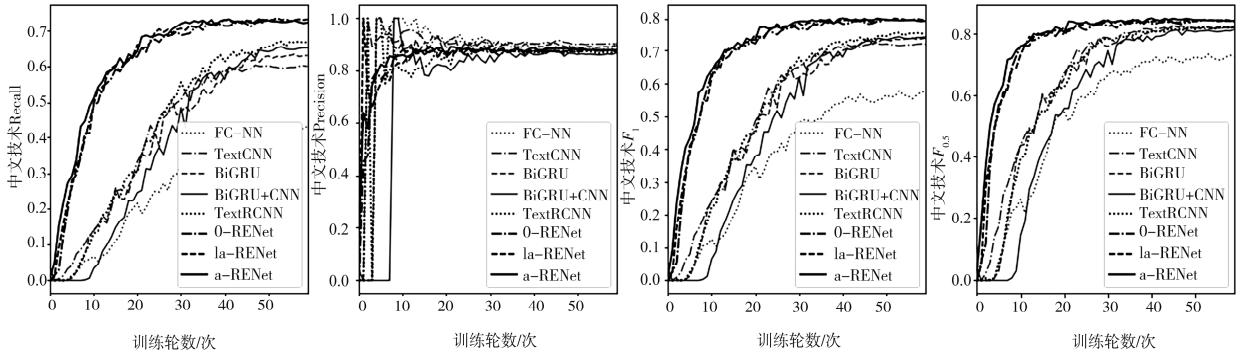

图 2　中文数据集技术测试集效果随训练变化

Fig. 2　Chinese dataset techniques test set effect within training

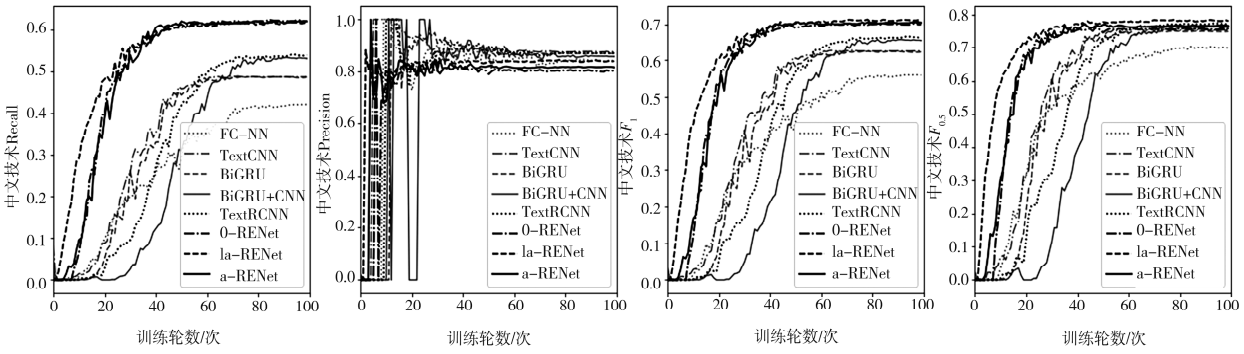

图 3　英文数据集技术测试集效果随训练变化

Fig. 3　English dataset techniques test set effect within training

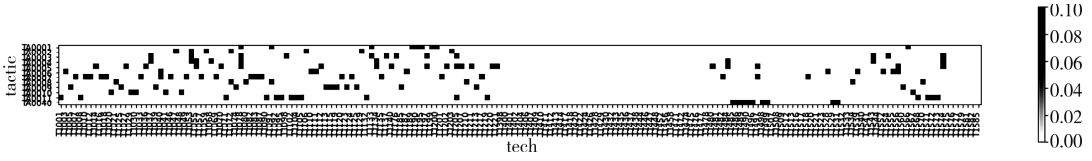

图 4　la-RENet 技战术关联转移邻接矩阵

Fig. 4　la-RENet tactics-techniques correlation transfer adjacency matrix

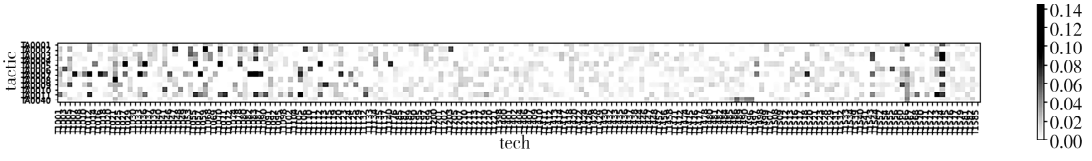

图 5　0-RENet 技战术关联转移邻接矩阵(正值)

Fig. 5　0-RENet tactics-techniques correlation transfer adjacency matrix (positive)

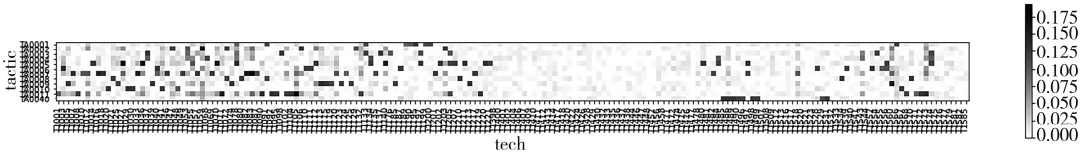

图 6　a-RENet 技战术关联转移邻接矩阵(正值)

Fig. 6　a-RENet tactics-techniques correlation transfer adjacency matrix (positive)

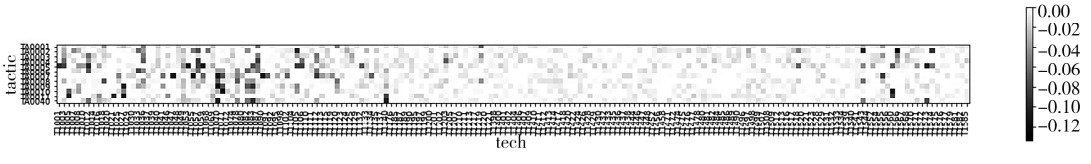

图 7　0-RENet 技战术关联转移邻接矩阵(负值)

Fig. 7　0-RENet tactics-techniques correlation transfer adjacency matrix (negative)

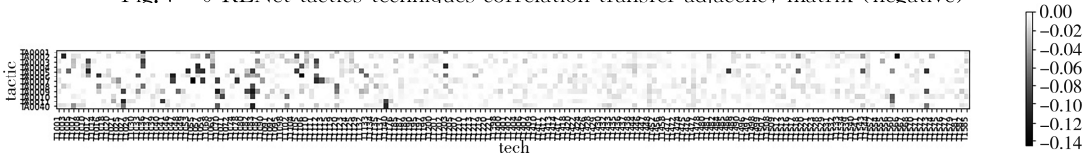

图 8　a-RENet 技战术关联转移邻接矩阵(负值)

Fig. 8　a-RENet tactics-techniques correlation transfer adjacency matrix (negative)

同时，图 7 和图 8 也反映出 RENet 在正支持相关性外也学习到了负支持的相关性. 即出现在负支持中的技战术对很难同时出现，这是人工定义所不具备的条件. 说明 RENet 能够利用但不依赖人工关系的特点.

5 结　论

针对现有工具在 TTPs 分类上的不足,本文提出使用关联增强的多标签分类模型 RENet 用于技战术分析. RENet 通过形成较为完整的技战术分布依赖,锁定技战术标签的范围,提高技战术分类的准确性. 实验表明,RENet 较现有方法在中英文的技战术分类上均有良好表现,同时具备快速训练和自动关系优化的特点.

参考文献:

[1] Gartner. Threat intelligence definition [EB/OL]. (2013-05-16)[2021-09-01]. https://www.gartner.com/en/documents/2487216.

[2] Liao X J, Yuan K, Wang X F, *et al*. Acing the ioc game: toward automatic discovery and analysis of open-source cyber threat intelligence[C]// Proceedings of the Acm Sigsac Conference on Computer & Communications Security. Vienna, Austria: ACM, 2016.

[3] David B. The pyramid of pain [EB/OL]. (2014-01-17) [2021-09-01]. https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html.

[4] Usman N, Usma S, Khan F, *et al*. Intelligent dynamic malware detection using machine learning in IP reputation for forensics data analytics [J]. Future Gener Comp Sy, 2021, 118: 124.

[5] Kim G, Lee C, Jo J, *et al*. Automatic extraction of named entities of cyber threats using a deep Bi-LSTM-CRF network [J]. Int J Mach Learn Cyb, 2020, 11: 2341.

[6] Sun X Q, Wang Z L, Yang J H, *et al*. Deepdom: malicious domain detection with scalable and heterogeneous graph convolutional networks [J]. Comput Secur, 2020, 99: 102057.

[7] Jang S, Li S, Sung Y. FastText-Based local feature visualization algorithm for merged image-based malware classification framework for cyber security and cyber defense [J]. Mathematics-Basel, 2020, 8: 460.

[8] Deliu I, Leichter C, Franke K. Collecting cyber threat intelligence from hacker forums via a two-stage, hybrid process using support vector machines and latent dirichlet allocation [C]//Proceedings of the 2018 IEEE International Conference on Big Data (Big Data). Seattle, WA, USA: IEEE, 2018.

[9] Carvery H. Follow up on TTPs post [EB/OL]. (2014-04-16) [2021-09-05]. http://windowsir.blogspot.com/2014/04/follow-up-on-ttps-post.html.

[10] Carvery H. TTPs [EB/OL]. (2014-04-13)[2021-09-05]. http://windowsir.blogspot.com/2014/04/ttps.html.

[11] Legoy V, Caselli M, Seifert C, *et al*. Automated retrieval of ATT&CK tactics and techniques for cyber threat reports [EB/OL]. (2020-04-29)[2021-09-06]. https://arxiv.org/abs/2004.14322.

[12] Husari G, Al-share E, Ahmed M, *et al*. TTPDrill: automatic and accurate extraction of threat actions from unstructured text of CTI sources[C]// Proceedings of the 33rd Annual Computer Security Applications Conference. Orlando, FL, USA: ACM, 2017.

[13] Husair G, Xi N, Chu B, *et al*. Using entropy and mutual information to extract threat actions from cyber threat intelligence [C]// Proceedings of the 2018 IEEE International Conference on Intelligence and Security Informatics (ISI). Florida, USA: IEEE, 2018.

[14] Barnum S. Standardizing cyber threat intelligence information with the structured threat information expression (stix™) [EB/OL]. (2013-07-08)[2021-09-05]. http://www.mitre.org/sites/default/files/publications/stix.pdf.

[15] Scikit-learn. API reference Scikit-learn 1.0.0 documentation [EB/OL]. (2021-09-01)[2021-09-10]. https://scikit-learn.org/stable/modules/classes.html.

[16] Munk M, Kapusta J, Švec P, *et al*. Data advance preparation factors affecting results of sequence rule analysis in web log mining [J]. EAM Ekon Manag, 2010, 13: 143.

[17] Abedin M, Nessa S, Khan L, *et al*. Analysis of firewall policy rules using data mining techniques [C]//Proceedings of the 2006 IEEE/IFIP Network Operations and Management Symposium (NOMS 2006). Vancouver, BC, Canada: IEEE, 2006.

[18] Li L L, Li J Z, Gao H. Rule-Based method for entity resolution [J]. IEEE T Knowl Data En, 2015, 27: 250.

[19] Kim G, Lee C, Jo J, *et al*. Automatic extraction of named entities of cyber threats using a deep Bi-LSTM-CRF network[J]. Int J Mach Learn Cyb, 2020, 11: 2341.

[20] Wang X, Guan Z, Xin W, *et al*. Multi-type source code defect detection based on TextCNN [C]//

Proceedings of the Frontiers in Cyber Security (FCS 2020). Tianjin, China: Springer, 2020.

[21] Zhao L, Shang Z, Zhao L, *et al*. Software defect prediction via cost-sensitive siamese parallel fully-connected neural networks[J]. Neurocomputing, 2019, 352: 64.

[22] Grisham J, Samtani S, Patton M, *et al*. Identifying mobile malware and key threat actors in online hacker forums for proactive cyber threat intelligence [C]// Proceedings of the 2017 IEEE International Conference on Intelligence and Security Informatics (ISI). Beijing, China: IEEE, 2017.

[23] Dang D, Troia F D, Sta M M. Malware classification using long short-term memory models [EB/OL]. (2021-05-03)[2021-09-10]. https://arxiv.org/abs/2103.02746.

[24] Ghaith H, Ehab A S, Bill C, *et al*. Learning APT chains from cyber threat intelligence [C]// Proceedings of the 6th Annual Symposium on Hot Topics in the Science of Security. Nashville, TN, USA: ACM, 2019.

[25] Mandiant. Cyber attack lifecycle [EB/OL]. (2021-09-10)[2021-09-10]. https://www.iacpcybercenter.org/resource-center/what-is-cyber-crime/cyber-attack-lifecycle/.

[26] Mitre. ATT&CK framework [EB/OL]. (2021-04-28)[2021-08-01]. https://attack.mitre.org/versions/v8/.

[27] Mike S, Kuldip K P. Bidirectional recurrent neural networks [J]. IEEE T Signal Proces, 1997, 45: 2673.

[28] Ruishuang W, Zhao L, Jian C, *et al*. Convolutional recurrent neural networks for text classification [C]//Proceedings of the 2019 International Joint Conference on Neural Networks (IJCNN). Budapest, Hungary: IEEE, 2019.

[29] Jesse D, Mark G. The relationship between precision-recall and ROC Curves [C]// Proceedings of the 23th International Conference on Machine Learning. Pittsburgh Pennsylvania, USA: ACM, 2006.

[30] Devlin J, Chang M W, Lee K, *et al*. BERT: pre-training of deep bidirectional transformers for Language understanding [EB/OL]. (2019-05-24)[2021-09-10]. https://arxiv.org/abs/1810.04805.

引用本文格式：

中　文：葛文翰，王俊峰，唐宾徽，等. 基于关联增强的网络威胁情报技战术分类[J]. 四川大学学报：自然科学版，2022，59：023004.

英　文：Ge W H, Wang J F, Tang B H, *et al*. RENet: tactics and techniques classifications for cyber threat intelligence with relevance enhancement [J]. J Sichuan Univ: Nat Sci Ed, 2022, 59: 023004.