基于注意力机制和特征融合的网络威胁情报技战术分类研究

于忠坤[1]，王俊峰[1]，唐宾徽[2]，葛文翰[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：在威胁情报包含的信息中，与网络攻击相关的战术、技术、程序(TTPs)是最能刻画组织行为的关键信息. 但是 TTPs 信息抽象层次高，并且通常存在于语法结构不规则的网络威胁情报文本中. 这导致传统的人工分析方法以及基于特征工程的机器学习方法难以快速有效地从中分类出 TTPs. 使用单一的深度学习特征提取器则因无法提取文本语意中完整的邻域特征和序列特征，导致技战术分类精度低. 针对上述问题，本文提出一种基于注意力机制和特征融合的深度学习模型：ACRCNN，用于网络威胁情报中的战术与技术的分类. 该模型通过卷积与循环神经网络同时提取网络威胁情报文本中的邻域与序列信息，再由卷积层与池化层进行深层次的特征抽取与降维，完成特征融合. 然后，通过注意力层完成特征加权，最终经由全连接层完成战术与技术的分类. 实验结果表明，ACRCNN 在战术、技术分类任务中表现优异，分别在 F_1 指标上达到了 91.91%和 83.86%，对比现有模型，分别提高了 2.46%和 4.94%.

关键词：网络威胁情报；技战术分类；深度学习；多标签分类；注意力机制；特征融合
中图分类号：TP301.6 **文献标识码**：A DOI：10.19907/j.0490-6756.2022.053003

Research on the classification of cyber threat intelligence techniques and tactics based on attention mechanism and feature fusion

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

Abstract: Among the information contained in cyber threat intelligence, the tactics, techniques, and procedures (TTPs) associated with cyber attacks are the key information that best portrays organisational behaviour. However, TTPs information has a high level of abstraction and is often found in cyber threat intelligence texts with irregular grammatical structures, which makes it difficult for traditional manual analysis methods and feature engineering-based machine learning methods to quickly and effectively classify TTPs, while the use of a single deep learning feature extractor leads to low accuracy in TTP classification because it cannot extract the complete neighbourhood features and sequence features in the text semantics. To address these problems, this paper proposes a deep learning model based on attention mechanism and feature fusion: ACRCNN, for the classification of TTPs and techniques in cyber

收稿日期：2021-09-14
基金项目：国家重点研发计划项目(2018YFB0804503，2019QY1400)；国家自然科学基金(U20A20161，U1836103)；基础加强计划项目(2019-JCJQ-ZD-113)
作者简介：于忠坤(1995－)，四川成都人，硕士研究生，研究方向为网络空间安全. E-mail：yuzhongkun@stu.scu.edu.cn
通讯作者：王俊峰. E-mail：wangjf@scu.edu.cn

threat intelligence. The model extracts the neighbourhood and sequence information from the cyber threat intelligence text by convolutional and recurrent neural networks simultaneously, and then completes deep feature extraction and dimensionality reduction by convolutional and pooling layers to complete feature fusion. Then, feature weighting is completed by the attention layer, and finally the classification of tactics and techniques is completed by the fully connected layer. The experimental results show that ACRCNN performs well in tactical and technical classification tasks, reaching 91.91% and 83.86% in F_1 metrics, which are 2.46% and 4.94% higher than the existing models.

Keywords: Cyber Threat Intelligence (CTI); Techniques and tactics classification; Deep learning; Multi-label classification; Attentional mechanism; Feature fusion

1 引　言

随着网络技术的不断发展，网络攻击行为日益频繁，对个人与社会的影响日益严重. 据 Hackmageddon 统计[1]，仅 2021 年第一季度就发生了 713 例网络攻击事件，并且攻击频率仍有上升趋势. 然而，面对日益频繁的网络攻击，当前的网络防御手段却越来越难以抵抗其威胁[2]. 因此，如何有效应对与处置各类网络攻击，已成为事关国计民生、国家和区域稳定与发展的重要因素[3]. 而及时掌握网络攻击态势并及时发现自身系统面临的潜在威胁，是有效应对与处置各类网络攻击的前置条件[4]. 但是，网络攻击事件体量逐渐增大、事件信息逐渐碎片化以及要素关联的错综复杂导致孤立地分析单个攻击行为已经无法刻画网络攻击全貌，更别提掌握目前的网络攻击态势了. 不过，网络威胁情报共享机制的不断完善，为全面建模威胁行为，掌握网络攻击态势提供了可能.

网络威胁情报是对发生的网络威胁行为进行专业分析后形成的报告，是针对攻击者及其动机、目的和手段分析后整理归纳的专业知识[5]. 这类专业知识的主要实体表现形式是失陷指标 IoCs (Indicator of Compromises)，内容包括 Hash、IP、域名、网络或主机特征、攻击工具以及 TTPs(Tactics、Techniques & Procedures) 信息. 其中，TTPs 是对攻击者的攻击方法、意图、过程的描述，是建模威胁行为的重要指标[6]. 这是因为文献[6]提出的“痛苦金字塔”模型认为位于金字塔顶端的 TTPs 是攻击者最难改变的高级行为特征，通过分析 TTPs 能够定性地刻画网络攻击行为，掌握攻击者的目的与手段，这对于应对网络攻击具有重要意义.

随着网络攻击复杂度的提高以及对抗性的增强，为更好地刻画网络攻击行为，TTPs 指标的定义也在不断调整与改进. 从最初的 KillChain[7] 模型，再到如今 MITRE 提出的 ATT&CK(Adversarial Tactics, Techniques, and Common Knowledge)[8]，TTPs 已经被细分为 14 个战术以及几百种技术. 目前，由 ATT&CK 定义的 TTPs 站在攻击者的视角上，对整个攻击生命周期的敌方行为进行了战术与技术的划分. 其中，战术类别代表攻击者攻击行为的意图，技术类别代表攻击者执行战术目标的方式，或者发动攻击后获得的内容. 通过这种划分，ATT&CK 框架能够以战术-战术、战术-技术的攻击链方式有效地刻画威胁行为，辅助安全人员掌握攻击者在每个攻击生命周期的攻击意图、使用手法以及威胁行为所导致的后果. 文献[9]基于 ATT&CK 框架提出一种企业安全威胁建模语言. 它使用元攻击语言框架设计，专注于描述系统资产，攻击步骤，防御和资产关联. 通过模拟攻击的方式找出企业系统防御的薄弱点，从而提出改进措施. 文献[10]扩展了 Ward 连接凝聚层次聚类算法，生成了威胁行为技术关联模型. 模型包含 97 类威胁行为技术关联簇，每一类簇可直观地看到不同组织所对应的威胁行为模式，可为组织溯源提供有力支撑.

虽然 TTPs 对应对网络威胁行为具有重要价值，但是从 CTI 中抽取 TTPs 却非易事. 随着网络威胁情报共享机制的不断完善，CTI 报告数量迅速增长，传统的人工分析方法因不能及时有效地从非结构化的威胁情报中分析出 TTPs，变得愈发难以应对如今的网络攻击态势. 另一方面，由于特征工程的限制，用于提取底层 IoC 信息的传统机器学习方法在提取抽象层次更高的 TTPs 任务中表现也不好[11]. 而使用单一的深度学习特征提取器则因无法提取文本语意中完整的邻域特征和序列特征，导致技战术分类精度低[12].

所以，本文针对上述问题，以 ATT&CK 知识

库中定义的 TTPs 为标准，提出了一种基于注意力机制和特征融合的深度学习模型 ACRCNN(Recurrent and Convolutional Neural Networks based on Attention and Convergence)用于网络威胁情报中的战术与技术的分类. 该模型通过卷积与循环神经网络同时提取网络威胁情报文本中的邻域与序列信息，再通过卷积层与池化层完成深层次的特征抽取与降维形成融合特征，然后通过注意力层完成特征加权，最终经由全连接层完成战术与技术的分类. 实验结果表明，本文提出的方法能够有效地从网络威胁情报 CTI(Cyber Threat Intelligence)中分类出 TTPs，并且在 F_1 度量指标上优于现有模型.

2　相关工作

根据 Gartner 的定义，网络威胁情报(CTI)是“基于证据的知识，包括背景、机制、指标、影响和可采取行动的建议，这些知识与现有或新出现的威胁或资产危害有关，可用于告知有关主体对该威胁或危害的反应的决策.”[13]CTI 中最核心的信息无疑是 IoCs，而 IoCs 信息中最核心的是 TTPs 信息[11,14]. 通过分析与共享网络威胁情报中蕴含的 IoCs 信息，安全团队能够及时了解他们的安全态势，发现早期的安全迹象，并不断改进其安全控制.

得益于自然语言处理技术的发展，从威胁情报文本中快速有效地抽取安全实体、TTPs 等高价值 IoC 信息成为了可能. 在自然语言处理领域，威胁情报的抽取工作实质上是为对威胁情报文本集合进行的分类任务. 目前，网络威胁情报抽取的方法主要分为基于特征工程的机器学习方法和深度学习方法.

在威胁情报信息分类任务中，机器学习方法首先构建特征工程来完成数据到信息的转换与识别，再通过分类器完成信息的分类. Liao 等[14]使用一组规则表达式从 IoCTerms 中提取的公共上下文术语来查找包含假定 IoC-tokens 的句子，例如 IP、MD5 等字符串. 在每个这样的句子中，该方法在 IoC 令牌和上下文术语之间建立描述语法结构的依赖图，并用图挖掘技术分析这些令牌之间的关系，从而完成对 IoCs 的抽取. 文献[11]提出一种基于支持向量机和置信度评分的机器学习模型 RCATT，用于网络威胁情报中的 TTPs 抽取. 该模型使用词频统计的方式表示了网络威胁情报文本，使用支持向量机进行分类；并利用 TTPs 战术与技术的层级关系，通过投票计算置信度的方式提高了技术的分类效果. 但该方法受限于特征工程，无法挖掘出非结构化的威胁情报更深层次的隐含特征，导致准确率低，假阳性高. 因此，越来越多的学者开始使用深度学习的方式进行威胁情报的抽取.

区别于传统的机器学习，深度学习通过不同的特征器，挖掘文本的深层次特征[15]. 并且，深度学习还能够从异质的文本数据中发现其内在联系，提取隐含特征，用于下游的安全实体识别、文本分类等任务.

作为自然语言处理的常用算法，卷积神经网络[16]和循环神经网络[17]常用于文本的特征提取. 卷积神经网络是通过对文本进行卷积，从而捕捉文本的局部邻域信息，完成高维特征的提取，用于文本分类. 例如，文献[18]提出，通过一种基于 TextCNN[19]的高效率领域标签识别器来识别威胁情报的所属目标域，然后使用基于词嵌入和句法依赖的折衷抽取方法来识别不可见的 IoCs 类型. 但是，TextCNN 使用固定词窗口捕捉上下文语意信息，实验结果受窗口大小的影响. 而循环神经网络则是通过特殊的隐藏层网络结果对文本进行循环递归处理，从而能够捕捉更长的上下文语义信息. 例如，文献[20]提出一种基于软字典映射和 RNN 变体 LSTM[21]的 IoCs 抽取模型. 该模型通过 LSTM 进行网络威胁情报上下文语意编码，然后条件随机场进行 IoC 序列的生成，并通过软字典映射的方式提高准确度. 在文本分类领域，基于 CNN 和 RNN，诞生了许多优秀的分类模型，例如 RCNN[22]和 CRNN[23]. 但是，文献[12]指出，网络威胁文本中通常包含大量具有不同语法和不规则结构的威胁对象，这对网络威胁情报文本的特征提出了更高的要求. 如果仍然使用使用单一的 CNN 或 RNN 特征提取器，是无法有效且完整地提取威胁对象特征的，这将直接影响模型性能. 因此，该文献在网络威胁情报中抽取 IoC 信息时，使用的是多粒度的双向 LSTM，用于挖掘威胁情报中的邻域信息和上下文信息，从而极大地提升了模型的性能. 但是该模型在提取领域信息时仍然使用的是 RNN，而未结合对邻域信息提取能力更强的 CNN.

另一方面，Attention 机制因其能强化网络挖掘文本特征信息的能力而逐渐在自然语言处理中得到应用[24]. 例如，文献[25]在 RNN 网络中引入

attention 机制以提高关键词的权重,从而提升了模型的文本分类能力. 文献[26]在 TextCNN 的基础上,引入异构注意力机制. 通过 CNN 提取文本特征,注意力层对特征图进行多粒度加权,从而提升了模型的文本分类能力.

3　本文的方法

为从网络威胁情报文本中分类出 TTPs, 本文以 ATT&CK 知识库中定义的 TTPs 为标准,提出了一种基于注意力机制和特征融合的深度学习模型:ACRCNN. 本章将描述具体的模型结构及原理.

3.1　模型结构

ACRCNN 模型结果如图 1 所示,包含词嵌入层、双向 RNN 编码层、CNN 编码层、CNN 特征融合层、最大池化层、注意力层以及全连接层. 词嵌入层是对一条标注语句完成从单词到词向量的转换过程. 双向 RNN 编码层和 CNN 编码层则是用于序列特征提取以及邻域信息提取,通过该过程会形成三个编码向量. CNN 特征融合层则首先将三个编码向量拼接成一个编码向量,再通过卷积的操作将序列信息和邻域信息进行融合,形成抽象层次更高的特征向量. 然后,经过池化降维以及注意力层的加权,形成了最终的特征向量.

ACRCNN 最后完成技战术分类任务的是全连接层,通过全连接层展开特征向量, 送入多层前馈神经网络单元,最后 sigmoid 函数计算每个技战术类别的概率,完成技战术分类.

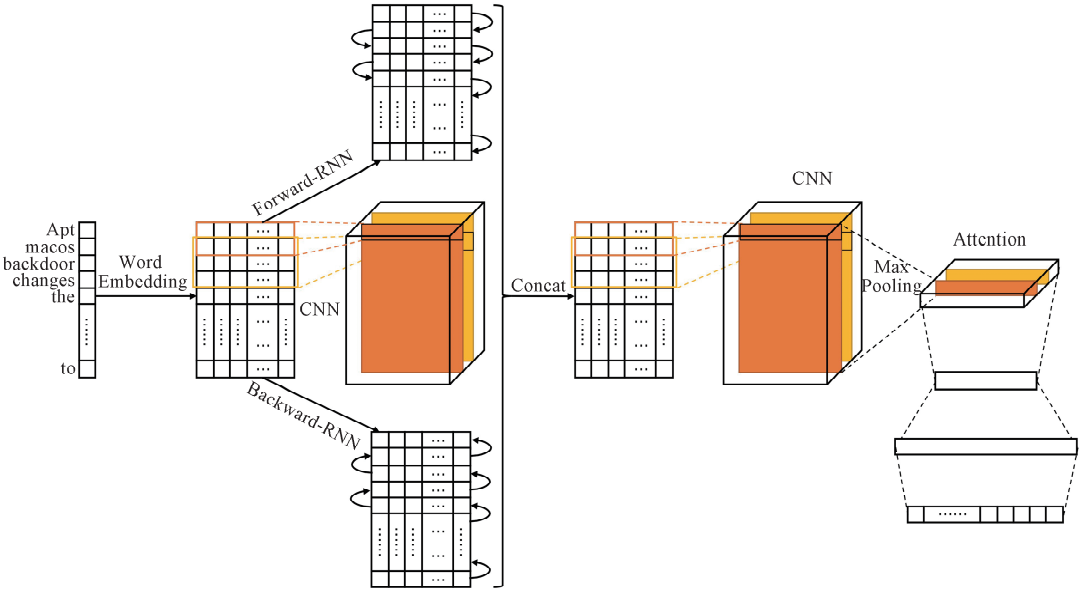

图 1　ACRCNN 模型网络结构图

Fig. 1　ACRCNN model network structure diagram

3.2　技战术分类原理

3.2.1　词嵌入表达　模型开始训练之前,首先要对威胁情报文本数据进行处理,将字词转换成特征向量. 本文采用的是 BERT[27] 词嵌方法,通过 Google 开源的 BERT 预训练模型来完成词到词向量的转换. 对于每条标注文本, 设输入文本为 W, n 是其词汇长度, 则一条标注文本可表达为

$$W=[w_1,w_2,\cdots,w_n] \tag{1}$$

通过 BERT 对每条标注文本进行词向量编码.

$$E=WordEmbedding(W)\in R^{n\times v_e} \tag{2}$$

得到词向量表示 E. 其中, v_e 是其词嵌向量维度; $e_i\in E$ 是其第 i 位向量($i=1,2,\ldots,n$).

3.2.2　特征融合机制　将得到的词向量表达分别通过双向 RNN 和 CNN 进行特征编码, 得到新的特征向量. 过程如下.

$$\overrightarrow{R_E}=\overrightarrow{RNN}(E) \tag{3}$$

$\overrightarrow{R_E}$ 为 RNN 前向编码得到的特征向量.

$$\overleftarrow{R_E}=\overleftarrow{RNN}(E) \tag{4}$$

$\overleftarrow{R_E}$ 为 RNN 后向编码得到的特征向量.

$$C_E=[Conv1\ D_1(E),\ldots,Conv1\ D_k(E)] \tag{5}$$

C_E 为通过不同大小的 CNN 卷积核卷积编码后得到的特征向量, $Conv1D$ 表示一维卷积操作.

然后,连接双向 RNN 和 CNN 编码后的特征向量,形成新的文本表示向量:

$$V_W=[\overrightarrow{R_E},C_E,\overleftarrow{R_E}] \tag{6}$$

其中，V_W为拼接编码后得到的特征向量.

将得到的拼接编码向量V_W送入新的 CNN 特征提取器进行特征融合.

$$C_V=Conv1\ D_1(V_W),\ldots,Conv1\ D_k(V_W)] \tag{7}$$

得到融合后的特征为C_V. C_V经过新的卷积操作后，将邻域信息和序列信息进行了融合，形成了抽象层次更高且语义信息更加丰富的特征向量. 然后，经过池化层，将信息进行降维：

$$M_{C_V}=\mathrm{Max}(C_V) \tag{8}$$

得到高度抽象的特征向量M_{C_V}.

3.2.3　注意力机制　将M_{C_V}送入注意力层，通过注意力层的不断学习，在特征通道维度上得到加权向量. 假设特征通道维度为 K，设第 i 个特征向量为T_i. 随机初始化一个与 K 具有相同维度的向量$\bar{T}$，使用相关性公式计算其与当前特征向量的相关程度.

$$A_i=Score(\bar{T}^T,T_i) \tag{9}$$

然后，通过注意力权重计算公式计算A_i绝对值与整个特征向量的匹配得分占总得分的百分比.

$$\alpha_i=\frac{\exp(Score(\bar{T}^T,T_i))}{\sum_j\exp(Score(\bar{T}^T,T_j))} \tag{10}$$

最后，通过加权求和的方式得到最终的特征向量 A 的表示.

$$A=\sum_i\alpha_iA_i \tag{11}$$

对于最终的特征向量 A 通过全连接层进行非线性变换后，使用 Sigmoid 函数计算每个技战术类别的概率，若超过阈值则表示属于该战术或技术类别.

4　实验与分析

4.1　数据准备与评估指标

本文收集了 MITRE 公司在 GitHub 上开源的 STIX 事件语料，并对其进行关联整理与标注，共形成了 6500 条标注数据. 其中，战术类别共 12 个，技术类别共 36 个. 标注过程中，对一条语料中包含的战术与技术类别赋值为 1，未包含的战术与技术类别赋值为 0. 实验过程中，本文将数据集按照 8∶1∶1 的比例分割成了训练集、验证集和测试集.

在度量神经网络模型性能指标的选取方面，本文认为识别率 Recall 和精确度 Precision 对于网络威胁情报战术与技术分类而言都很重要. 因此，为综合衡量两个指标，避免单一指标分数高和数据分布不均造成的评价不准确的问题，本文选择了 F_1 指标中的 Micro-F_1指标作为最终的评估指标. F_1 指标越高，表明模型在 Recall 和 Precision 两个方面的综合表现越好，反之则越差. 计算公式如下.

$$F_1=\frac{2*Recall*Precision}{Recall+Precision} \tag{12}$$

4.2　实验设计

为验证 ACRCNN 能够有效地完成网络威胁情报的技战术分类任务以及特征融合机制对模型性能的提升，本文选择了对 BiLSTM、BiGRU、RCNN、CRNN、TextCNN 等模型进行了对比试验，通过对比 F_1值的大小来评估模型的表现.

同时，在实际工业生产环境下，模型的收敛速度与稳定性也十分重要. 因此，本文还绘制了 tactics 和 techniques 训练过程中测试集上 F_1 值随 epoch 的变化，对模型收敛情况和稳定性进行了讨论与分析.

此外，本文还进行了消融实验，通过对比加入与不加入注意力机制的 ACRCNN 模型的实验结果，来验证引入注意力机制的正确性.

4.3　实验结果与分析

4.3.1　总体比较与分析　因战术与技术在 ATT&CK 中属于不同层级，本文的实验结果分为了战术与技术两个方面进行分析. 表 1 和表 2 分别是战术与技术的实验结果. 总体对比而言，本文的 ACRCNN 相较于其他深度学习模型在 F_1 指标上表现更好. 在战术与技术分类任务中，本文模型比其他模型中的最优模型分别提高了 2.46%和 4.94%.

战术分类实验结果如表 1 所示. 对比 RNN（BiLSTM、BiGRU）与 TextCNN 的实验结果可知，在网络威胁情报战术分类任务中，单一的邻域信息特征要比单一的序列信息特征更重要. 对比 RCNN、CRNN 和 RNN 的实验结果也验证了这一结论. 另一方面，对比 ACRCNN 和其他模型可知，本文提出的 ACRNN 同时使用了 CNN 和 RNN 作为特征提取器，并将提取到的邻域信息和序列信息再通过卷积融合，得到的融合信息要比单一的邻域和序列信息更重要，对 F_1的指标提升幅度很大. 这一结果也验证了本文方法对于网络威胁情报战术分类的有效性.

技术分类实验结果如表 2 所示. 由于技术类

别数远多于战术类别数，平均每一类技术类别的标注数据要远少于战术类别. 因此，技术分类的结果普遍要低于战术分类的结果. 但是，对比实验结果，本文的 ACRCNN 模型在 F_1 指标上仍要优于其他深度模型. 对比 RNN(BiLSTM、BiGRU)与 TextCNN 的实验结果可知，在网络威胁情报技术分类任务中，单一的邻域信息特征仍然要比单一的序列信息特征更重要. 同时，对比 ACRCNN 和其他模型可知，特征融合信息仍然要比单一的邻域和序列信息更重要. 结合战术与技术分类结果可知，本文方法提出的特征融合机制能够有效提升模型对技战术分类的效果.

表 1　战术分类的实验结果

Tab. 1　Experimental results for tactics classification

模型	Recall/%	Precision/%	F_1/%
BiLSTM	80.47	85.27	82.80
BiGRU	79.86	84.77	82.24
RCNN	81.29	86.84	83.40
CRNN	87.68	90.12	88.88
TextCNN	86.93	92.12	89.45
ACRCNN	**91.36**	**92.47**	**91.91**

表 2　技术分类的实验结果

Tab. 2　Experimental results for techniques classification

模型	Recall/%	Precision/%	F_1/%
BiLSTM	59.33	82.33	68.96
BiGRU	59.55	81.62	68.86
RCNN	61.79	**88.48**	83.40
CRNN	66.03	87.56	75.29
TextCNN	71.73	87.70	78.92
ACRCNN	**81.01**	86.93	**83.86**

4.3.2　模型收敛性和稳定性讨论　为讨论模型的收敛性与稳定性，本文记录了模型训练过程中 F_1 指数的变化，并绘制成了曲线图. 图 2 和图 3 分别展示了各模型在训练过程中预测标签的 F_1 值随着训练次数增加而产生的变化.

通过对比分析可知，基于 CNN 的深度模型收敛速度要快于基于 RNN 的深度模型. 其中，ACRCNN 不仅收敛速度最快，F_1 峰值最高，并且相比于其他模型收敛更加平稳. 这一结论也证明了本文方法的先进性.

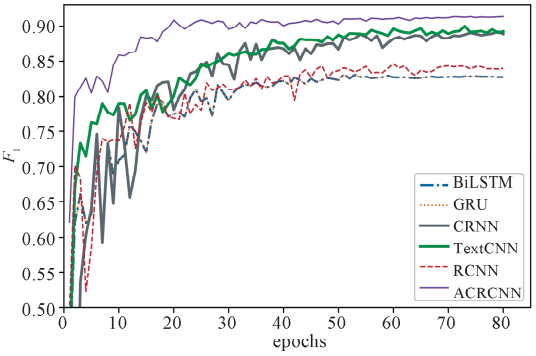

图 2　战术分类训练过程中，F_1 值随训练次数的变化趋势

Fig. 2　The change trend of F_1 with training epochs in tactics classification

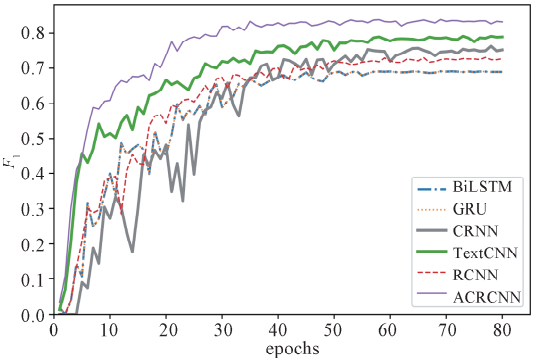

图 3　技术分类训练过程中，F_1 值随训练次数的变化趋势

Fig. 3　The change trend of F_1 with training epochs in techniques classification

4.3.3　消融实验结果分析　为验证注意力机制根据重要程度对融合特征进行加权求和得到的最终特征是否能够提升模型在网络威胁情报技战术分类的性能，本文进行了消融实验，实验结果如表 3 所示.

表 3　消融实验结果

Tab. 3　Ablation results

模型	战术			技术		
	Recall/%	Precision/%	F_1/%	Recall/%	Precision/%	F_1/%
ACRCNN(无注意力机制)	90.16	90.29	90.23	78.21	88.83	83.18
ACRCNN	91.36	92.47	91.91	81.01	86.93	83.86

对比有无注意力机制的 ACRCNN 模型实验结果可知，不论是战术分类还是技术分类，有注意力机制的 ACRCNN 在 F_1 指标上都表现得更好，最高的提升达到了 1.68%. 这一结果证明，注意力机制通过学习特征重要性后，对融合特征的加权求和得到的最终特征相比与没有加权的融合特征特征更加突出，并且能有效提升模型的分类效果.

5　结　论

受限于特征工程，传统的机器学习方法难以从多源异质的威胁情报中抽象出 TTPs 信息，而单一的深度学习特征提取器因无法提取文本语意中完整的邻域信息和序列信息，导致技战术分类精度低. 针对上述问题，本文以 ATT&CK 知识库中定义的 TTPs 为标准，提出一种基于注意力机制和特征融合的深度学习模型：ACRCNN，用于网络威胁情报中的战术与技术的分类. 相比于 BiLstm、CRNN 等深度学习方法，本文的方法在 F_1 指标上表现更优，特别是技术的分类提升上，不仅收敛速度更快，Recall 值提升也很大.

参考文献：

[1] Passeri P. Q1 2021 cyber attack statistics, 2021. [EB/OL]. (2021-01-13) [2022-01-01]. https://www.hackmageddon.com/2021/04/13/q1-2021-cyber-attack-statistics/.

[2] Siddiqui M Z, Yadav S, Husain M S. Application of artificial intelligence in fighting against cyber crimes: a review [J]. Int J Adv Res Comput Sci, 2018, 9: 118.

[3] Chowdhury A . Recent cyber security attacks and their mitigation approaches-an overview [C]//International Conference on Applications and Techniques in Information Security. Singapore: Springer, 2016.

[4] Dutt V, Ahn Y S, Gonzalez C. Cyber situation awareness: modeling detection of cyber attacks with instance-based learning theory [J]. Hum Factors, 2013, 55: 605.

[5] Barnum S. Standardizing cyber threat intelligence information with the structured threat information expression (stix)[J]. Mitre Corpor, 2012, 11: 1.

[6] Iqbal Z, Anwar Z. Ontology generation of advanced persistent threats and their automated analysis [J]. NUST J Eng S, 2016, 9: 68.

[7] Kim H, Kwon H J, Kim K K. Modified cyber kill chain model for multimedia service environments [J]. Multimedia Tools Appl, 2019, 78: 3153.

[8] Xiong W, Legrand E, Åberg O, *et al*. Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix[J]. Softw Syst Model, 2022, 21: 157.

[9] Xiong W, Legrand E, Åberg O, *et al*. Cyber security threat modeling based on the MITRE enterprise ATT&CK matrix [J]. Softw Syst Model, 2021 (2): 1.

[10] 陈柏翰，王俊峰，唐宾徽，等. 面向组织溯源的威胁行为技术关联研究[J]. 四川大学学报：自然科学版，2022，59：012006.

[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)[2022-01-01]. https://arxiv.org/abs/2004.14322.

[12] Zhao J, Yan Q, Liu X, *et al*. Cyber threat intelligence modeling based on heterogeneous graph convolutional network [C]//Proceedings of the 23rd International Symposium on Research in Attacks, Intrusions and Defenses. San Sebastia: USENIX, 2020.

[13] Noor U, Anwar Z, Altmann J, *et al*. Customer-oriented ranking of cyber threat intelligence service providers [J]. Electron Commer R A, 2020, 41: 100976.

[14] Liao X, 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 2016 ACM SIGSAC Conference on Computer and Communications Security. Vienna Austri: Association for Computing Machinery, 2016.

[15] Bengio Y, Courville A, Vincent P. Representation learning: A review and new perspectives [J]. IEEE T Pattern Anal, 2013, 35: 1798.

[16] Shin H C, Roth H R, Gao M, *et al*. Deep convolutional neural networks for computer-aided detection: CNN architectures, dataset characteristics and transfer learning [J]. IEEE T Med Imaging, 2016, 35: 1285.

[17] Yu W, Kim I Y, Mechefske C. Analysis of different RNN autoencoder variants for time series classification and machine prognostics [J]. Mech Syst Signal Pr, 2021, 149: 107322.

[18] Zhao J, Yan Q, Li J, *et al*. TIMiner: automatically extracting and analyzing categorized cyber threat intelligence from social data [J]. Comput Secur,

2020, 95: 101867.

[19] Chen Y. Convolutional neural network for sentence classification [D]. Waterloo: University of Waterloo, 2015.

[20] Ameri K, Hempel M, Sharif H, *et al*. CyBERT: cybersecurity claim classification by fine-tuning the BERT language model [J]. J Cybersecur Priv, 2021, 1: 615.

[21] Chen T, Xu R, He Y, *et al*. Improving sentiment analysis via sentence type classification using BiLSTM-CRF and CNN [J]. Expert Syst Appl, 2017, 72: 221.

[22] Jiang D, Li G, Tan C, *et al*. Semantic segmentation for multiscale target based on object recognition using the improved Faster-RCNN model [J]. Future Gener Comp Sy, 2021, 123: 94.

[23] Tong G, Li Y, Gao H, *et al*. MA-CRNN: a multi-scale attention CRNN for Chinese text line recognition in natural scenes [J]. Int J Doc Anal Recog, 2020, 23: 103.

[24] Liu G, Guo J. Bidirectional LSTM with attention mechanism and convolutional layer for text classification [J]. Neurocomputing, 2019, 337: 325.

[25] Du C, Huang L. Text classification research with attention-based recurrent neural networks [J]. Int J Comput Commun, 2018, 13: 50.

[26] Liang Y, Li H, Guo B, *et al*. Fusion of heterogeneous attention mechanisms in multi-view convolutional neural network for text classification [J]. Inform Sci, 2021, 548: 295.

[27] Lu Z, Du P, Nie J Y. VGCN-BERT: augmenting BERT with graph embedding for text classification [J]. Adv Inf Ret, 2020, 12035: 369.

引用本文格式:

中　文: 于忠坤, 王俊峰, 唐宾徽, 等. 基于注意力机制和特征融合的网络威胁情报技战术分类研究[J]. 四川大学学报: 自然科学版, 2022, 59: 053003.

英　文: Yu Z K, Wang J F, Tang B H, *et al*. Research on the classification of cyber threat intelligence techniques and tactics based on attention mechanism and feature fusion [J]. J Sichuan Univ: Nat Sci Ed, 2022, 59: 053003.