Threat Intelligence Relationship Extraction Based on Distant Supervision and Reinforcement Learning

Xuren Wang, Jie Yang
Information Engineering College
Capital Normal University
Beijing, China
wangxuren@cnu.edu.cn

Qiuyun Wang, Changxin Su
Key Laboratory of Network Assessment Technology
Institute of Information Engineering
Chinese Academy of Sciences
Beijing, China

Abstract—**In recent years, threat intelligence has become a new hotspot in cybersecurity. It analyzes and predicts attacks that have occurred and have not occurred, and plays an important role in building an efficient defense system. Traditional threat intelligence relies on a manual collection and its efficiency is relatively low. Therefore, the efficient sharing of threat intelligence has important research value. For the information extraction technology of threat intelligence, we focus on the construction of threat intelligence labeling data sets and the extraction technology of threat intelligence relationship. The specific content and research results include two aspects: (1) Research on the construction of threat intelligence information extraction data set. The threat intelligence extraction data set is constructed by a distantly supervised labeling method. In this paper, more than 900 threat intelligence reports are used as a corpus. We finally obtain a relation extraction data set containing 10,000 sentence instances of 30 relationships. (2) Research on the extraction of threat intelligence relationships. To mitigate noise labeling data in the relation extraction data, we propose a distant supervision relationship extraction method based on DRL-ET-PCNN-ATT (Deep Reinforcement Learning Entity Type Piecewise Convolution Neural Network-Attention) based on the PCNN-ATT (Piecewise Convolution Neural Network-Attention) model. The experimental results show that compared with the CNN (Convolution Neural Network), PCNN (Piecewise Convolution Neural Network), RL-CNN (Reinforcement Learning Convolution Neural Network) models, the accuracy of the extraction model used in this paper has increased by 16.77%, 5.88%, and 4.97%, and the recall rate has increased by 16.39%, 2.83%, and 4.49%.**

Keywords-threat intelligence; relationship extraction; distant supervision; reinforcement learning

I. INTRODUCTION

Threat intelligence sharing research faces two major challenges: First, when there is a large amount of threat intelligence report, it is very inefficient to rely solely on manual analysis and sharing of critical information. It is impossible to synchronize and share real-time threat intelligence on time, resulting in Threat information lags. Second, unlike the natural language processing corpus in the general domain, the tagging corpus in the field of threat intelligence is scarce, which makes research on threat intelligence extraction very difficult. Therefore, information extraction on threat intelligence has important practical significance and application value.

In summary, we make contributions in this work include: (1) Constructing a threat intelligence extraction data set through a distantly supervised labeling method; (2) We evaluate our model and achieve the best result compared with several state-of-the-art relation extraction models.

II. RELATED WORK

In recent years, there has been an increasing amount of literature on threat intelligence data, and the dataset for threat intelligence is increasing. Varish Mulwad et al. proposed a framework to extract vulnerability and attack information from web text, and generate machine-understandable languages. The data set was from 107 vulnerability description documents and was not publicly available [1]; Nikki McNeil et al. proposed a new entity extraction guidance algorithm PACE is used to extract valuable network security concepts. The data set is manually annotated 10 documents from online open source websites with a total of seven entity types [2]; Corinne L. Jones and others proposed a bootstrapping algorithm to extract security entities and their relationships from the text. The dataset is a corpus of 62 documents made from various security-related websites. The dataset is not open source [3]; Arnav Joshi et al. The research of linked data completed an experimental data set through professional annotations. The training set consists of 3800 entities and 38,000 instances. The test set consists of 1200 entities and 9,000 instances. The dataset is not public [4]; Ravendar Lal et al. Researched extracting secure entities and concepts from unstructured text, and they built datasets from more than 100 select reports After screening and the fact that sampling CVE eventually got 60, 12 and 12 Dobe Microsoft bulletin announcement of the composition of the data set, it is not open to the public [5]. In summary, threat intelligence related datasets are very rare and most of them are not public. Hence, we propose an annotation method based on distant supervision to help security analysts to label OSINT data more quickly and efficiently. Then we propose the relationship extraction method combined with reinforcement learning to research threat intelligence information extraction on this data set.

III. DATASET

After distant supervision labeling and manual verification, the label definition and quantity distribution for each relationship are shown in Table 1.

The final threat intelligence relationship extraction data set contains 10,000 sentence examples of 30 types of relationships.

DOI reference number：10.18293/SEKE2020-149

TABLE I RELATIONSHIP LABEL DEFINITION AND QUANTITY DISTRIBUTION

Head entity	Relation	Tail entity	Relation number
Hacker group	Background	Region	386
Hacker group	Target	Region	1155
Hacker group	Target	Industry	1218
Hacker group	Target	Organization	257
Hacker group	Target	User	179
Hacker group	Attack	Way	759
Hacker group	Use	Tool	1227
Hacker group	Use	Loophole	97
Hacker group	Oldest active	Time	167
Hacker group	First found	Time	103
Hacker group	Attack	Time	458
Hacker group	Attack	Purpose	325
Hacker group	Have	Alias	153
Hacker group	Launch	Attack action	238
Hacker group	Use	Tool	146
Hacker group	Attack	Purpose	91
Sample file	Generate	Time	109
Sample file	Use	Loophole	96
Sample file	Have	File type	85
Sample file	Propagation	Way	444
Sample file	Have	Features	238
Sample file	Target	Region	91
Sample file	Target	Industry	295
Sample file	Related	Sample file	111
Sample file	Have	Alias	222
Security Team	Found	Sample file	112
Security Team	Found	Attack activity	248
Security Team	Release	Time	123
Security Team	Found	Hacker group	115
Offensive action	Attack	Time	752

IV. THREAT INTELLIGENCE RELATIONSHIP EXTRACTION FRAMEWORK

Aiming at the complicated threat data in a large number of threat intelligence reports, as shown in section III, the entity-relationship is marked based on the method of distant supervision, which solves the problem of marking threat intelligence data. However, this method generally classifies sentences at the sentence set level, and cannot map relationships to sentences one by one. The main reason for this problem is the noisy data in the distantly supervised labeled data set, which has a great effect on relationship extraction great influence. To solve this problem, based on the distant supervised model PCNN, we propose a distant supervised extraction model based on DRL-ET-PCNN-ATT. The model is shown in Fig. 1, which is mainly composed of the input vector layer and piecewise convolution neural network and sentence instance selector. The model first inputs three layers of feature vectors, including pre-trained word vectors, the vector of the relative position between each word and the entity, and the entity type vector; the next step is the piecewise convolutional neural network to extract the context information related to the entity, and add the attention mechanism to the sentence vector, and get the classification result of the relationship label. To alleviate the problem of noisy sentences, we introduce a sentence selector based on reinforcement learning.

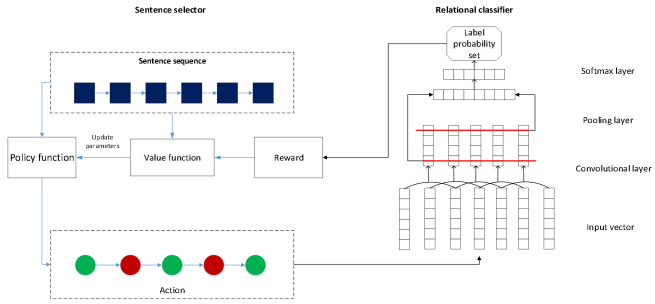


Figure 1. DRL-ET-PCNN-ATT relationship extraction model diagram

A. *Input Vector Layer*

- In this paper, before inputting into the neural network layer, it is necessary to characterize the word vector and obtain the context relationship between words. Here, the word2vec word vector language model is used to convert each word in the corpus into a d-dimensional vector. Thus, we get a single vector representation of each word.

- In the input vector feature, to highlight the relative position of the entity in the sentence and make full use of the position information in the sentence, this article adds the vector feature of the entity position and uses the relative position of each word and the entity position in the sentence as an important feature input. Here, position embedding proposed by Zeng [6] are used. As shown in Fig. 2, the relative distance between each word and the entities E_1 and E_2 in the sentence is stitched together as the position vector feature.

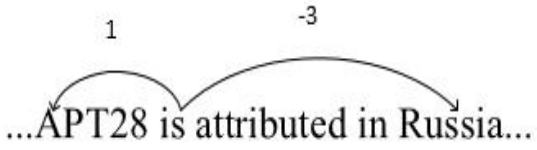


Figure 2. Example of the position feature vector

- Due to the difference in the order of magnitude of each entity type in the threat intelligence data set, consider adding entity type features based on a common model. First label the text with a BIO labeling scheme, that is, label each element as "BX", "IX" or "O". Among them, "BX" indicates that the fragment in which this element is located belongs to type X and this element is at the beginning of this fragment, "IX" indicates that the fragment in which this element exists belongs to type X and that the element is in the middle position of this fragment, and "O" indicates that it does not belong to any type, and then quantify the labeled entities and words to give them corresponding features, and then stitch them together with word features and location features as input features of the convolutional neural network. That is, if the dimension of the word vector is, the dimension of the position vector is, the dimension of the entity type feature vector is, and the dimension of the input vector layer is d:

$$d = d_w + 2*d_p + d_e \quad (1)$$

B. Convolutional neural network layer And Attention layer

The construction process of the convolutional neural network layer and attention layer uses the baseline model proposed by Lin et al. [7].

C. Sentence selector based on reinforcement learning

Reinforcement learning is an area in machine learning that emphasizes how to act based on the environment to achieve the maximum expected benefits. The problem that reinforcement learning solves is to get an optimal action for a specific problem so that the reward obtained under this strategy is the largest.

Definition of the problem to be solved by the instance selector: given a set [sentences, relationship labels], expressed as X $=\{(x_1,r_1), (x_2,r_2),\ldots, (x_n,r_n)\}$, X include the noise annotation generated by the distant supervision method, and the task of the selector is to determine which sentence correctly describes the relationship, then select the sentence and hand it to the convolutional neural network classifier.

According to the task requirements of this problem, we construct a reinforcement learning selector for relation extraction tasks. As shown in Fig. 1, the state, action, and reward are defined as follows:

- The state contains the current sentence, selected sentences, and entities. The author uses a continuous function $\emptyset(s_i)$ to represent the state, which will output a vector. Among them, the vector representation of the current sentence is obtained from the non-linear layer of the PCNN used for relation classification; the vector representation of the selected sentence set is the average of each sentence vector; the vector representation of a pair of entities is pre-trained word vector.
- The value of action is {0, 1}, indicating whether to select the current sentence. The a_i obtained according to the policy function $\pi_\theta(s_i,a_i)$ where θ is the parameter to be learned. The following logical function is used here as the policy function definition, where $\emptyset(s_i)$ is the state feature mentioned earlier.

$$\pi_\theta(s_i,a_i) = P_\theta(a_i,s_i) = a_i\sigma(W * \emptyset(s_i) + b) + (1 - a_i)(1 - \sigma(W * \emptyset(s_i) + b)) \quad (2)$$

- The reward is a quality representation of the selected sentence. When a round of sentences is selected, there will be final feedback, that is, final feedback is set at the final state. The definition of the feedback function is as follows, where Q is the selected sentence set, which is a subset of state, r represents the relationship label of the current sentence, and $p(r|s_j)$ is the label probability output by the relationship classifier.

$$r(s_i|Q) = \begin{cases} 0, & i < |Q+1| \\ \frac{1}{Q}\sum_{S_j \in Q} logp(r|s_j), & i = |Q+1| \end{cases} \quad (3)$$

- The optimization function of sentence selector for maximizing feedback is defined as:

$$J(\theta) = V_\theta(s_0|Q) = E_{s_0,a_0,s_1,a_1\ldots s_i,a_i,\ldots}[\sum_{i=0}^{|Q|+1} r(si|Q)] \quad (4)$$

- According to Actor-critic algorithms [8], we add value function Q_ω after state and reward calculations to reduce the error of the policy function. The value function is defined as follows:

$$Q_\omega(s,a) = \emptyset(s_i)^T\omega \quad (5)$$

- Where $\emptyset(s_i)$ is the initial state vector, $\emptyset(s_i')$ is the state vector after the sentence is selected, input these two vectors to the value function to get the Q value output $Q_\omega(s_i)$ and $Q_\omega(s_i')$, the TD error δ is used as the parameter update error of the policy function and value function, γ is the decay.

$$\delta = r + \gamma Q_\omega(s_i') - Q_\omega(s_i) \quad (6)$$

- The parameter ω of the value function is updated as follows, β is the training step.

$$\omega = \omega + \beta\delta\emptyset(s_i) \quad (7)$$

- The parameter θ of the policy function is updated as follows, α is the training step.

$$\theta = \theta + \alpha\sum_{i=1}^{|Q|} \nabla_\theta log\pi_\theta(s_i,a_i)\,\delta \quad (8)$$

V. EXPERIMENTS

In this section, we evaluated the model on the threat intelligence data set constructed in part III. We first introduce the experiment dataset and parameter settings. To verify the advantages of this model, we conducted experiments on CNN, PCNN, and RL-CNN separately. The experimental results show that the model used in this paper has a higher accuracy of extracting threat intelligence relationships than other models, and gives this comparison of experimental results and PR (precision-recall) curves of these four models.

A. Dataset

As shown in the third part, 10000 sentence instances containing 30 relationships are established, and the data set is randomly divided into a training set of 90% and a test set of 10%, that is, the training data contains 9,000 sentence examples, and the test data contains 1000 sentence examples. Relationship extraction usually has three types of evaluation indicators: precision, recall, and F1 measure. We will use

these three indicators to compare the performance of our model with the baseline extraction model.

B. *Parameter Settings*

Some key parameters need to be set during model training. For the parameter settings of the relational classifier part, the word vector dimension is set to 50, the position vector dimension is set to 5, and the entity type feature vector dimension is set to 3. In the convolutional neural network layer, the size of the convolution window is set to 3. The number of neurons in the hidden layer of the convolutional layer is set to 230. In the instance selector section, set batch size 40 and learning rate 0.1. To alleviate the problem of overfitting the model, we add a dropout unit.

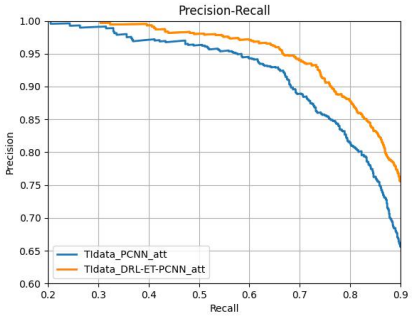
C. *Experiment Results*

To verify the effectiveness of the DRL-ET-PCNN-ATT based relationship extraction model used in the extraction of threat intelligence relationships, this paper compares this with general models CNN [9], PCNN [6], and RL-CNN [10]. Second, we also compare the processing of sentence information in the package. There are 4 ways, namely ATT, AVE, ONE, CROSS_MAX, and AVE. All the sentence weights in a package are regarded as the same, that is, the vector is taken. The average value; ONE takes the sentence instance vector with the highest confidence in the bag as the input calculation; CROSS_MAX [11] performs an instance-max-pooling operation on all sentence vectors inside the bag. The triples and sentences are converted into a dictionary format and input to the above model for training and testing. The accuracy, recall, and F1 values are shown in Table 2. By analyzing the experimental results in Table 2, we can see the advantages of the model used in this article. The DRL-ET-PCNN-ATT model has the highest accuracy rate, reaching 92.31%, and the recall rate is 83.24%. The ATT method is also used in the package example. Compared with the CNN / PCNN / RL-CNN model in the field of relation extraction, the accuracy rate has increased by 16.77%, 5.88%, and 4.97%, and the recall rate has increased by 16.39%, 2.83%, and 4.49%.

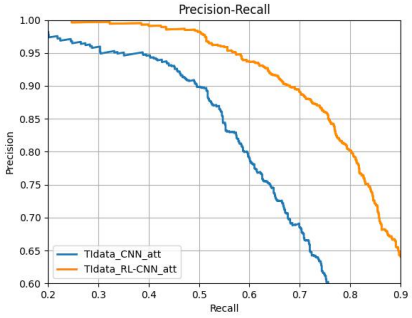
The precision/recall curves for each method are shown in Fig. 3. By analyzing the PR curve of Fig. 3 (a)(b), the extraction effect of DRL-ET-PCNN-ATT is significantly better than PCNN-ATT, and the extraction effect of RL-CNN-ATT is significantly better than CNN-ATT. The processor eliminates some noise data and improves the accuracy of relation extraction. From Fig. 3 (c), the extraction effect of PCNN is better than the CNN model, and we can see the advantage of the segmented pooling method in the extraction effect. From Fig. 3 (d), it can be seen that the advantages of DRL-ET-PCNN-ATT for the other three models reflect the advantages of adding entity type features and combining the PCNN model with reinforcement learning, making full use of the distribution characteristics of entity type threat intelligence data and the advantages of joint training. The combination of the two greatly improves the accuracy of relation extraction, as shown in Fig. 3 (e), the extraction performance comparison of the four bag instance processing methods on the DRL-ET-PCNN model shows that the ATT method is the most suitable for the model used in this paper, maximizing the extraction accuracy.

TABLE II. EXPERIMENTAL RESULTS OF EACH MODEL ON FOUR BAG PROCESSING METHODS

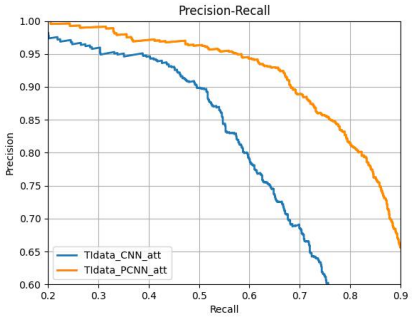
Model	Bag Way	ACCURACY	AUC	F1
CNN	ATT	0.7554	0.6685	0.7092
	AVE	0.7585	0.6745	0.7140
	ONE	0.7773	0.6723	0.7210
	CROSS_MAX	0.7626	0.6854	0.7219
PCNN	ATT	0.8643	0.8041	0.8331
	AVE	0.8639	0.7843	0.8222
	ONE	0.8723	0.7587	0.8115
	CROSS_MAX	0.8745	0.7743	0.8213
RL-CNN	ATT	0.8734	0.7875	0.8282
	AVE	0.8830	0.8047	0.8420
	ONE	0.8942	0.8102	0.8501
	CROSS_MAX	0.8864	0.7957	0.8386
DRL-ET-PCNN	ATT	**0.9231**	**0.8324**	**0.8754**
	AVE	0.8943	0.8075	0.8487
	ONE	0.9018	0.8186	0.8582
	CROSS_MAX	0.9113	0.8265	0.8679



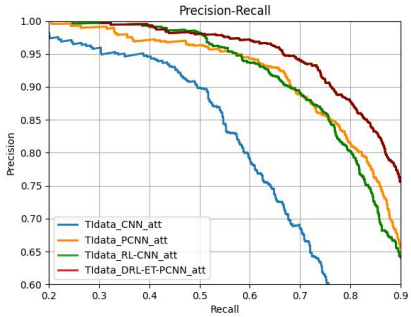
(a)



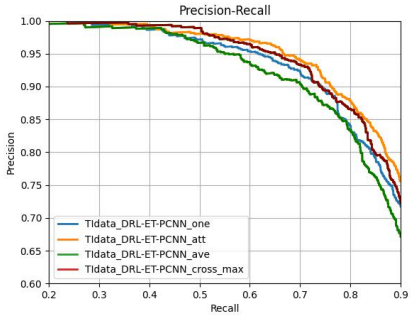
(b)



(c)



(d)



(e)

Figure 3. Comparison of Experimental P-R Curves of Threat Intelligence Relation Extraction Data Sets on Different Models

VI. Conclusion and Future Work

In this paper, we use the knowledge base to distantly supervise structured threat intelligence data to construct a relationship extraction dataset and compare the number of sentences and relationship types with the classic data set in the field of relationship extraction. In the research of the construction of the threat intelligence relationship extraction model, based on the PCNN-ATT model, we propose a distant supervision relationship extraction method based on DRL-ET-PCNN-ATT, The extraction accuracy is significantly improved.

In the future, we will explore the following directions:

The dataset used in this paper is extracted from unstructured text. It is limited to text corpora such as hacker organizations, security teams, and sample files. It ignores charts in threat intelligence reports, threat information in pictures. In future research, we can consider building a set of report pre-processing process and image recognition model, which can extract this non-text information and enrich the shared information of threat intelligence.

In relation extraction, the assumption in distant supervision is too positive, and it is inevitable to introduce a lot of noise data. To alleviate the problem of mislabeling, at present, the typical model of entity-relationship extraction is PCNN-ATT, but it mainly uses the semantic information of the sentence and does not involve grammatical information. Therefore, how to effectively fuse the semantic and sentence grammatical information to extract entity relationships is also one of the main directions to optimize the extraction model in future work.

Acknowledgment

This work is supported by the National Key Research and Development Program of China (Grant No.2018YFB0805005).

References

[1] Mulwad V, Li W, Joshi A, et al, “Extracting information about security vulnerabilities from web text”. 2011 IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology. USA: IEEE, 2011, pp. 257-260.

[2] McNeil N, Bridges R A, Iannacone M D, et al, “Pace: Pattern accurate computationally efficient bootstrapping for timely discovery of cyber-security concepts”. 2013 12th International Conference on Machine Learning and Applications. USA: IEEE, 2013, pp. 60-65.

[3] Jones C L, Bridges R A, Huffer K M T, et al, “Towards a relation extraction framework for cyber-security concepts”. Proceedings of the 10th Annual Cyber and Information Security Research Conference. USA: ACM, 2015, pp. 1-4.

[4] Joshi A, Lal R, Finin T, et al, “Extracting cybersecurity related linked data from text”. 2013 IEEE Seventh International Conference on Semantic Computing. USA: IEEE, 2013, pp. 252-259.

[5] Lal R, “Information Extraction of Security related entities and concepts from unstructured text”. 44(3), pp. 127-131, 2013.

[6] Zeng D, Liu K, Chen Y, et al, “Distant supervision for relation extraction via piecewise convolutional neural networks”. Proceedings of the 2015 conference on empirical methods in natural language processing. Portugal: Association for Computational Linguistics, 2015, pp. 1753-1762.

[7] Lin Y, Shen S, Liu Z, et al, “Neural relation extraction with selective attention over instances”. Proceedings of the 54th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers). Germany: Association for Computational Linguistics, 2016, pp. 2124-2133.

[8] Konda V R, Tsitsiklis J N, “Actor-critic algorithms”. Advances in neural information processing systems. USA: NIPS, 2000, pp. 1008-1014.

[9] Zeng D, Liu K, Lai S, et al, “Relation classification via convolutional deep neural network”. Ireland: ACL 2014, 2014, pp. 2335-2344.

[10] Feng J, Huang M, Zhao L, et al, “Reinforcement learning for relation classification from noisy data”. Thirty-Second AAAI Conference on Artificial Intelligence. USA: AAAI, 2018.

[11] Jiang X, Wang Q, Li P, et al, “Relation extraction with multi-instance multi-label convolutional neural networks”. Proceedings of COLING 2016, the 26th International Conference on Computational Linguistics: Technical Papers. Japan: The COLING 2016 Organizing Committee 2016, pp. 1471-1480.