MalFCS

Journal of Parallel and Distributed Computing(July 2020)

2020.01.21

김 정 우

MalFCS?

An effective malware classification framework (SVM)

with **automated feature extraction**

based on **deep convolutional neural networks**

Entropy graph generator

악성코드에서 추출한 structural entropy을 300 * 300 * 1 의 형태로 변환

논문에서 강조되야할 부분

- Automatic feature extraction

- CNN을 사용한 이유
  - code reuse

실험결과

- 성능이 1이 나오는 것은 매우 어려운 (논문에서는 10-fold 검증을 사용)
- Loss 값만이 믿을 수 있는 결과인 것

Table 5
Comparison of classification performance of different approaches for the Microsoft dataset.

Method	Accuracy	Macro-F1 score	Kappa	Test logloss
Nataraj [26]	0.9782	0.9579	0.9736	0.66735
Gibert [11]	0.9828	0.9636	0.9791	0.12443
Kalash [15]	0.9997	–	–	0.05710
Gibert [10]	0.9913	0.9830	0.9894	0.04190
Drew [9]	0.9741	–	–	0.22286
Our method	**1**	**1**	**1**	**0.03142**

malware samples belonging to Yuner.A, VB.AT, Malex.gen!J, Autorun.K, Rbot!gen are packed. Our method can process these samples directly without unpack, with corresponding accuracy of 1, 1, 0.99, 1, and 1, respectively.

For the Microsoft dataset, we use the training set to train the feature extractor and then conduct a 10-fold cross-validation with extracted features on the SVM classifier. The performance comparison over these methods is shown in Table 5. Our method achieves the best performance with accuracy of 100% and macro-averaged F1 score of 100%, while the accuracy of the winner of the Microsoft Malware Classification Challenge is 99.87%. For the