Poster: Mobile Malware Detection using Multiple Detector Set Artificial Immune System

James Brown, Mohd Anwar*, Gerry Dozier
Department of Computer Science
North Carolina Agricultural and Technical State University
Greensboro, NC, USA
manwar@ncat.edu

***Abstract*—As mobile devices become increasingly more powerful and important in everyday life, the need for efficient and effective detection of mobile malware has become pressing. We developed a multi-detector set Artificial Immune System (mAIS) to classify apps into benign and malicious categories based upon information flows within the app. The performance of mAIS has been compared with the performance of a variety of conventional Artificial Immune Systems (AISs) using a feature-set of information flows captured from malicious and benign Android applications. Our preliminary results show that the mAIS outperforms the conventional AISs in terms of accuracy and false positive rate as well as the computational complexity of the negative selection process. We plan to replicate the study on a large set of mobile applications.**

Keywords— Mobile Malware Detection; Artificial Immune System; Multiple Detector Set; Evolutionary Computing

I. Introduction

The mobile industry has grown exponentially since the introduction of iOS and Android. Mobile devices have become a staple in everyday life for users around the world. There are an estimated 11 billion mobile devices currently in use [3]. Currently, Android constitutes roughly 82.8% of the market share for mobile operating systems [2]. This dominance by Android in the mobile OS landscape has conversely affected mobile malware production. Ninety-seven (97) percent [4] of all mobile malware is specifically designed to target the Android OS. Therefore, sophisticated, robust and self-healing solutions are needed to address this increasingly pressing threat.

The Artificial Immune System (AIS) is a self-healing, self-contained, and adaptive solution modeled after the biological immune system. The biological immune system first recognizes and identifies 'self'. By doing this, the biological immune system is able to detect non-self pathogens, which enter the body and respond with the appropriate antibodies. The major drawback of the AIS is its inability to react and evolve in a dynamic environment. This can result in high false positives when 'self' is no longer static. Therefore, we applied a multi-detector set Artificial Immune System (mAIS), which evolves two independent AISs: one identifies "self"/detects "non-self", and the other identifies "non-self"/detects "self". The mAIS uses the two detector sets in a proportional based classifier, similar to a committee machine. This technique significantly reduces false positives while retaining a high detection rate.

II. Model Overview

False Positives (FPs), Type I errors, create confusion in and hassle for users because a benign app was misclassified as malicious which throws unnecessary warnings. Although False Negatives (FN), Type II errors, pose a larger threat to users' security and privacy, the standard AIS has shown the ability to detect malicious apps with a True Positive Rate (TPR) of 80.00%. Unfortunately, the standard AIS results in a False Positive Rate (FPR) of 73.33%. As evidenced in Idris & Muhammed [6], the mAIS is proficient at detecting non-self instances and significantly reducing FPs. Therefore, we applied the mAIS to the Android malware detection problem. When used with Split Detector Method (SDM) [5] and GEFeS [7], the mAIS outperformed the standard AIS with a TPR of 86.67% and a false positive rate (FPR) of 0.00%.

A. Detector Set Generation

To develop the mAIS, two independent detector sets are generated: one detects "non-self" app instances and the other detects "self" app instances. The "non-self" mature detector set is trained in a similar way as a standard AIS. During Negative Selection, if an immature detector matches a "self" app instance, it is discarded or split depending on the variants of mAIS used. Theoretically, this results in a detector set which only detects "non-self". For 'self' mature detector set generation, if an immature detector matches a "non-self" instance, it is either discarded or spilt.

B. Proportion Based Classification

The two detector sets are used in a proportion based classification method to detect unknown instances. If the proportion of "non-self" mature detectors that match an instance is greater than the proportion of "self" mature detectors that match the instance, the instance is classified as "non-self". Likewise, if the proportion of "self" mature detectors that match are greater than the proportion of "non-self" mature detectors, the instance is classified as self. Since, FNs have the potential to cause significantly more damage than those of FPs, in the rare case that the proportions of the two independent detector sets are equal, the instance is classified as "non-self".

C. *Any-r Interval Matching Rule*

The any-r interval matching rule is used to determine if a detector matches an instance (app). Each detector is composed of 590 intervals, where each interval corresponds to a specific feature from the dataset feature vectors. To determine if a detector matches an instance, first, an r-value is selected. If he number of features from an instance that are contained within the detectors intervals is $\geq$ r, the detector matches the instance.

III. Results

We tested GEFeS, the AIS and mAIS variants on a dataset of 30 benign apps and 28 malicious apps. The benign apps were gathered from the Google Play Store. The malicious apps were obtained from the Android Malware Genome Project [1], which is a repository of over 1,200 malicious Android apps organized into various families. These families are created based on similar behaviors and exploits targeted.

For the standard AISs and mAISs, six fold cross-validation was used where the training set consisted of 38 feature vectors associated with 20 benign and 18 malicious apps, the tuning set consisted of 10 feature vectors associated with 5 benign and 5 malicious apps and the test set also consisted of 10 feature vectors associated with 5 benign and 5 malicious apps.

The cross-validation training was as follows. For the first fold, the training, tuning, and test sets were created as explained earlier. On a particular run, a sweep of the r-values, for the 'self' and 'non-self' detector sets, was used to discover the best r-value, for the any-r intervals matching rule (where the self and non-self detector sets have their own independent r-value). For a particular r-value, the two detector sets were randomly generated and exposed to the 'self' and 'non-self' training instances. Those detectors that failed to match an instance were promoted to mature detectors. The mature detectors of each detector set were exposed to their respective instances of the tuning set. The best performing 'self' r-value / detector set pairing and the best performing 'non-self' r-value / detector set pairing on the tuning set were retained. They were retained to be exposed to the test set on a proportion basis. After being exposed to the test set, the statistics, such as accuracy, TPR, FPR, TNR, and FNR were recorded.

After the recording of the statistics for the first fold, the 10 instances from the test set were removed and appended to the training set. The 10 instances from the tuning set became the new test set. The first 5 self and 5 non-self instances (5 benign, 5 malicious apps) were removed from the training set and appended to the tuning set. After the sets have been modified/rotated, the second fold begins using the same training method explained earlier. This process is completed for the third, fourth, fifth, and sixth folds, where the standard AISs and mAISs were a total of 30 times for each fold, resulting in a total of 180 runs.

The results for the different algorithms are shown below in Table I. The mAIS with SDM and with GEFeS performed the best, with an overall accuracy of 93.33%. The standard AIS with SDM and GEFeS outperformed the other algorithms in True Positive Rate (TPR) with a rate of 93.33% but the four mAIS variants all achieved False Positive Rates (FPR) of 0.00%.

Table I: The Results of Comparing the 9 Methods on the 30-28 Dataset

Method	Accuracy	TPR	TNR	FPR	FNR
GEFeS	70% (53.67)	40% (14.00%)	**100.0% (93.33%)**	**0.00% (6.67%)**	60.00% (86.00%)
AIS$_{-SDM,-GEFeS}$	53.33% (35.39%)	80.00% (49.00%)	26.67% (21.78%)	73.33% (78.22%)	20.00% (51.00%)
AIS$_{+SDM,-GEFeS}$	50.00% (33.50%)	80.00% (46.11%)	20.00% (20.89%)	80.00% (79.11%)	20.00% (53.89%)
AIS$_{-SDM,+GEFeS}$	51.67% (32.11%)	83.33% (42.44%)	20.00% (21.78%)	80.00% (78.22%)	16.67% (57.56%)
AIS$_{+SDM,+GEFeS}$	56.67% (32.82%)	**93.33%** (43.56%)	20.00% (22.07%)	80.00% (77.93%)	**6.67%** (56.44%)
mAIS$_{-SDM,-GEFeS}$	88.33% (66.72%)	76.67% (46.00%)	100.00% (87.44%)	0.00% (12.56%)	23.33% (54.00%)
mAIS$_{+SDM,-GEFeS}$	86.67% (64.39%)	73.33% (44.22%)	100.00% (84.56%)	0.00% (15.44%)	26.67% (55.78%)
mAIS$_{-SDM,+GEFeS}$	86.67% (60.72%)	73.33% (41.11%)	100.00% (80.33%)	0.00% (19.67%)	26.67% (58.89%)
mAIS$_{+SDM,+GEFeS}$	**93.33%** (60.29%)	86.67% (42.86%)	100.00% (77.71%)	0.00% (22.29%)	13.33% (57.14%)

References

[1] Zhou, Y., & Jiang, X. (2012). Android malware genome project. Available at http://www.malgenomeproject.org

[2] IDC: Smartphone OS Market Share. (n.d.). Retrieved March 24, 2016, from http://www.idc.com/prodserv/smartphone-os-market-share.jsp

[3] Radicati, S. (Ed.). (2016, January). Mobile Statistics Report, 2016-2020. Retrieved March 24, 2016, from http://www.radicati.com/wp/wp-content/uploads/2016/01/Mobile-Growth-Forecast-2016-2020-Executive-Summary.pdf

[4] Kelly, G. (2014, March 24). Report: 97% Of Mobile Malware Is On Android. This Is The Easy Way You Stay Safe. Retrieved June 19, 2015, from http://www.forbes.com/sites/gordonkelly/2014/03/24/report-97-of-mobile-malware-is-on-android-this-is-the-easy-way-you-stay-safe/

[5] Dozier, Gerry, et al. "Vulnerability analysis of AIS-based intrusion detection systems via genetic and particle swarm red teams." Evolutionary Computation, 2004. CEC2004. Congress on. Vol. 1. IEEE, 2004.

[6] Idris, I., & Abdulhamid, S. M. (2014). An Improved AIS Based E-mail Classification Technique for Spam Detection. arXiv preprint arXiv:1402.1242.

[7] Dozier, Gerry, et al. "GEFeS." Symposium Series on Computational Intelligence, IEEE SSCI 2011-2011 IEEE Workshop on Computational Intelligence in Biometrics and Identity Management, CIBIM 2011. 2011.