Random Projection Method for Scalable Malware Classification

József Hegedüs, Yoan Miche, Alexander Ilin and Amaury Lendasse

Aalto University School of Science,
Department of Information and Computer Science,
FI-00076 Aalto, Finland

Abstract. In this poster a new approach for scalable behavioral based malware classification is presented. It is based on the random projection method which is an efficient, effective yet simple dimensionality reduction method. Interestingly, however, the random projection method has not – to the authors' best knowledge – ever been investigated for its possible usefulness for the malware classification problem. Here, we – for the first time – demonstrate its ability to reduce the dimensionality and to retain the properties of the data important for malware classification; it speeds up the distance calculations by an order of magnitude and yet it does not sacrifice much of the accuracy.

1 Introduction

Antivirus companies receive tens of thousands of samples on a daily basis. Each one needs to be analyzed in order to determine whether it is malicious or not. Part of the samples are analysed by being executed in a sandbox environment. This allows to extract behavioral properties (such as system calls made, ports opened etc.) which are then used as features for classification. The number of samples received daily is ever increasing, therefore methods need to be developed for scaling up this process. Even though previous attempts have been made to do so [3,1] – to the authors' best knowledge – no work has been done yet on determining the suitability of a powerful dimensionality reduction technique, random projections [2], for speeding up the malware classification process.

The random projection method has the advantage over hash based methods [3,1] that the resulting random projected vectors (which are representing the samples) are real valued vectors and they can be fed directly to most machine learning software packages whilst still achieving a considerable speedup due to the reduced dimensionality. In this work we demonstrated that the random projection method performs well in the malware classification task compared to the non-approximated case.

2 Random projection approximation and its accuracy

For each executable sample the sandbox generates a set of hashes that describe the behavior of the sample. The meaning of these hashes is not disclosed here

due to confidentiality. According to the anti-virus experts at F-Secure it is reasonable to assume that the more hashes two samples have in common the more similar they are. Based on this, we measure the similarity by the cosine distance between two binary vectors, each describing a sample. In order to get the random projected approximation for these binary vectors, one has to multiply them with a random matrix having entries drawn independently from the standard normal distribution.

In Figure 1 the accuracy of two k nearest neighbor classifications are compared. The speedup due to the approximation is tenfold for the distance calculations while the detection rate only decreases by a few percent in the approximated case.

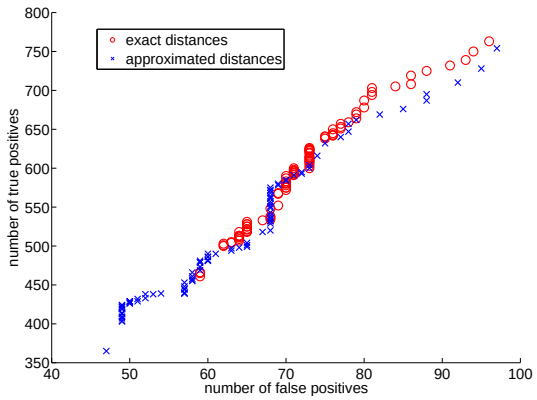

Fig. 1. In this figure the number of false and true positives are shown for the case of 1000 classified samples. We applied a k nearest neighbor classifier using either exact or approximated cosine distances. Different points in the figure correspond to different k values. We predicted a sample to be malicious if all k neighboring samples were malicious, benign if all k neighbors were benign and undeterminable otherwise.

References

1. Ulrich Bayer, Paolo Milani Comparetti, Clemens Hlauschek, Christopher Krügel, and Engin Kirda. Scalable, behavior-based malware clustering. In *NDSS*. The Internet Society, 2009.
2. S. Dasgupta. Experiments with random projection. In *Proceedings of the 16th Conference on Uncertainty in Artificial Intelligence*, UAI '00, pages 143–151, San Francisco, CA, USA, 2000. Morgan Kaufmann Publishers Inc.
3. J. Jang, D. Brumley, and S. Venkataraman. Bitshred: Fast, scalable malware triage. Technical report, CyLab, 2010.