How to aggregate scores in a multi-heuristic detection system: a comparison between WOWA and Neural Networks

A. Croix, W. Mees, T. Debatty
cylab.be

24 apr 2020

Cyber-attacks are becoming increasingly complex and therefore require more sophisticated response systems. A lot of them are multi-agents systems and MASFAD is a typical example.

A crucial step in the development of these types of systems is to aggregate all agents results correctly in order to classify an event as a threat or no. There are various ways to do that. We studied two approaches and performed an efficiency comparison. The first classifier is an aggregation function in which parameters are learned by a genetic algorithm. The second is a neural network classifier trained by a backpropagation algorithm.

We compared the performance of the two systems on the same task: the training of the classifiers whose objective is to distinguish if a PHP file, previously analyzed by a 5-agents system, is a webshell or an harmless PHP file.

Aggregation function and genetic algorithm

The aggregation function used is the WOWA (Weighted Ordered Weighted Averaging) function. It is the generalization of the Weighted Mean and the Ordered Weighted Averaging and uses two parameters by data source (agent).

The parameters are learned by a genetic algorithm. This algorithm reflects the process of natural selection where the fittest individuals (solutions) are selected for reproduction in order to produce offspring of the next generation.

Artificial Neural Network

An artificial neural network is a computing system inspired by the biological neural networks that constitute animal brains. The algorithm tries to find a set of internal parameters that perform wells against a performance measure or a cost function.

The algorithm is iterative, the convergence occurs over discrete steps that improved internal parameters.

Evaluation and conclusions

The efficiency is evaluated with two classical criteria in statistics: the AUC of a ROC curve and the AUC of a Precision-Recall curve. The ROC AUC illustrates the diagnostic ability of a binary classifier. It is he Area Under the Curve of a ROC that is created by plotting the true positive rate against the false positive rate.

The second is very informative for imbalanced datasets. As for first criteria, we measure the AUC of a curve obtained by plotting the Recall against the Precision.

We observed better results with the neural network classifier on all our tests. However, for a reasonable training time, it is best to do it on GPUs that are quite more expensive than CPUs.

Another advantage of the classifier based on aggregation function is the possible results interpretation. The function parameters obtained after the training can gives information about efficiency of the different agents. It is not possible with the trained neural network.

The complete code used to run the tests is available online at

- https://gitlab.cylab.be/cylab/java-neural-network
- and https://gitlab.cylab.be/cylab/java-wowa-training