Malware Classification Using Ensemble Classifiers

Abstract

Antimalware offers detection mechanism to detect and take appropriate action against malware detected. To evade detection, malware authors had introduced polymorphism to malware. In order to be effectively analyzing and classifying large amount of malware, it is necessary to group and identify them into their corresponding families. Hence, malware classification has appeared as a need in securing our computer systems. Algorithms and classifiers such as k-Nearest Neighbor, Artificial Neural Network, Support Vector Machine, Naïve Bayes, and Decision Tree had shown their effectiveness towards malware classification in various recent researches. This paper proposed the concept of ensemble classifications to classify malwares, in which three individual classifiers, k-Nearest Neighbor, Decision Tree and Naïve Bayes classifiers are ensemble by using the bagging approach.