Intrusion detection based on k-means clustering and OneR classification

ABSTRACT

Intrusion detection system (IDS) is used to detect various kinds of attacks in interconnected network. Many machine learning methods have also been introduced by researcher recently to obtain high accuracy and detection rate. Unfortunately, a potential drawback of all those methods is the rate of false alarm. However, our proposed approach shows better results, by combining clustering (to identify groups of similarly behaved samples, i.e. malicious and non-malicious activity) and classification techniques (to classify all data into correct class categories). The approach, KM+1R, combines the k-means clustering with the OneR classification technique. The KDD Cup '99 set is used as a simulation dataset. The result shows that our proposed approach achieve a better accuracy and detection rate, particularly in reducing the false alarm.

Keyword: Intrusion detection system; Clustering; Classification; Machine learning