A K-Means and Naive Bayes learning approach for better intrusion detection

ABSTRACT

Intrusion Detection Systems (IDS) have become an important building block of any sound defense network infrastructure. Malicious attacks have brought more adverse impacts on the networks than before, increasing the need for an effective approach to detect and identify such attacks more effectively. In this study two learning approaches, K-Means Clustering and Naïve Bayes classifier (KMNB) are used to perform intrusion detection. K-Means is used to identify groups of samples that behave similarly and dissimilarly such as malicious and non-malicious activity in the first stage while Naive Bayes is used in the second stage to classify all data into correct class category. Experiments were performed with KDD Cup '99 data sets. The experimental results show that KMNB significantly improved and increased the accuracy, detection rate and false alarm of single Naïve Bayes classifier up to 99.6, 99.8 and 0.5%.

Keyword: Intrusion detection system; K-Means clustering; Naive Bayes classifier; Accuracy; Detection rate; False alarm