Abstract

Intrusions pose a serious threat in a network environment and so the intrusion detection problem has been frequently studied. Modern computer networks are subjected to various malicious attacks. Since attacks are becoming more sophisticated and networks are becoming larger, there is need for an efficient intrusion detection system that can distinguish illegitimate traffic and be able to signal attacks with a high detection rate and a low false alarm rate. We propose an intrusion detection method which can detect attacks based on a clustering algorithm. The dataset is divided into clusters and a labeling method is used which label the clusters based on their sizes and an outlier detection algorithm. Our algorithm is to able to detect both single and multi-connection attacks. The algorithm is evaluated over KDD cup 1999 dataset and encouraging results are obtained.