Abstract

Intrusion detection systems (IDS) is a system that can detect any intrusion or attack on a network or information systems. Anomaly detection is one of the method in IDS. In anomaly detection, network traffic data is detected as intrusion if it has different characteristics from most of data. There are clustering based approach in anomaly detection where data will be grouped into several clusters. Intrusion cluster is the cluster with a small number of members. One of well-known clustering algorithm is K-Means because it is easy to implement and has low complexity. However there are some shortcoming in that algorithm. Y-Means is a clustering algorithm that is built to solve the shortcoming of K-Means. Network traffic data will be grouped into several clusters, and there will be intrusion cluster which can be seen by the threshold. Test carried out with several scenarios to determine the accuracy of the system based on the value of detection rate and false positive rate, the influence of the merging variable on the number of final cluster and also the influence of merging variable and threshold value on accuracy. Y-Means can detect intrusions with fairly good accuracy based on detection rate (92.46%). From false alarm value, Y-Means accuracy is not too bad (9.69%).

Keywords: *intrusion, clustering, anomaly detection, Y-Means*