Abstract

With the growth of networked computers and applications on top of it, network anomaly detection is an essential component in keeping network secure. The capability of network anomaly detection methods needed to update with inclusion of new attacks. A number of anomaly detection methods have been developed for protecting computers and networks using conventional statistical methods to new data mining methods in recent times. In these data mining methods supervised, unsupervised and outlier methods are usually found in misuse anomaly based intrusion detection. In this project, we use both supervised and unsupervised technique for increasing efficiency of detection of new and old attacks. In supervised technique, we used classification algorithm to detect known type of attacks. In unsupervised technique, we used outlier detection algorithm to separate the normal packet from unknown attacks and we used clustering algorithms to cluster the unknown attacks. We validated the clusters for getting the best result. Both supervised and unsupervised techniques are evaluated with the benchmark intrusion KDD Cup 1999 dataset and captured real-time flow and packet level dataset.

Keywords: network anomaly, supervised, unsupervised, outlier, multi-level, features, dataset.