Abstract

The role of Intrusion Detection System (IDS) is having a very essential role in network Security. As the need of internet is increasing day by day, the importance of security is also increasing. A traditional intrusion detection technology indicates the limitations like low detection rate, high false alarm rate and so on. Performance of the classifier is a necessary concern in terms of its effectiveness; also number of feature to be examined by the IDS should be improved. In this, hybrid IDS is applied using Snort with J48 Graft Decision tree algorithm, J48 Graft Decision tree with Pruning using feature selection and Naïve Bayes algorithm. In J48 Graft Decision tree with pruning, only discrete value attributes for classification are considered and for Naïve Bayes redundant records are removed with feature selection. KDDCup’99 dataset is used to train and test the classifier. The performance of the classifiers is also tested on dataset created by capturing online packets which classifies packet as either normal or anomaly. Results and analyses show that, J48 Graft decision tree with pruning and Naïve Bayes approach is giving better results with enhanced accuracy than existing classification techniques.
Performance Evaluation of Attack Detection Algorithms using Improved Hybrid IDS with Online Captured Data

References


Index Terms

Computer Science

Algorithms

Keywords

Classification Algorithms, Pruning, Anomaly Detection, Accuracy, KDD, Hybrid, Snort.