Abstract

Most existing network intrusion detection systems use signature-based methods which depend on labeled training data. This training data is usually expensive to produce due to cost of laboratory set up, experienced or knowledge person and non availability of ready software tool. Above all, these methods have difficulty in detecting new or unknown types of attacks. Using unsupervised anomaly detection techniques, however, the system is capable of detecting previously unknown attacks without labeled training data. In this paper, we have discussed anomaly based network intrusion detection and proposed two unsupervised clustering algorithms for anomaly detection. The algorithms are evaluated with our generated real life intrusion dataset. The dataset is created with extracted features of captured network packet as well as flow traffic. The algorithm is also tested and validated with standard KDD Cup 1999 dataset and NSL-KDD dataset. The results are compared with results of similar algorithms and have been found excellent.
Reference


**Index Terms**

Computer Science  
Security

**Key words**

Supervised  
Intrusion  
Unsupervised

Anomaly

Clustering

TPR

FPR