Abstract

At Present, it is very essential to establish a high level network security to make sure the more trusted and secure communication between various organizations. Network Security provides a platform to secure information channels from the huge amount of network attacks. Intrusion Detection System (IDS) is an estimable tool for the defense mechanism in computer networks. IDS focus on detecting of harmful network traffic that would exploit vulnerability in network system. Feature selection performs a necessary role in intrusion detection process. The
dataset extracted in IDS contain a large number of features, in which some of the irrelevant, redundant and noisy. These unnecessary features degrades the performance of the IDS. In order to discard irrelevant, redundant & noisy features in the experiment, have need to analyzed different feature selection approaches with various search methods. The pre-processed NSL-KDD dataset is used in experiments for evaluation purpose at WEKA 3. 6. 9 environment tool. By using Bayes Net and Naive Bayes Classifier classify the selected feature dataset. The comparison of all empirical results are done by using different performance metrics. The ultimate goal of work is to increase the overall accuracy of the detection process with minimal number of selected feature dataset and reduced training time.

References

- G. Stoneburner, Underlying technical models for information technology security, NIST Special Publication 800-33, National Institute of Standards and Technology.
- K. Kumar, G. Kumar, Y. Kumar, Feature selection approach for intrusion detection system, International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE) 2 (5).

Index Terms

Computer Science

Computer Networks
Keywords

Intrusion Detection System (ids)  Feature Selection (fs) Approaches  Pre-processing
Dataset
Net
Naive Bayes

Nsl-kdd