Abstract

Anomaly detection has emerged as an important technique in many application areas mainly for network security. Anomaly detection based on machine learning algorithms considered as the classification problem on the network data has been presented here. Dimensionality reduction and classification algorithms are explored and evaluated using KDD99 dataset for network IDS. Principal Component Analysis for dimensionality reduction and Support Vector Machine for classification have been considered for the application on network data and the results are analysed. The result shows the decrease in execution time for the classification as we reduce the dimension of the input data and also the precision and recall parameter values of the classification algorithm shows that the SVM with PCA method is more accurate as the number of misclassification decreases.

References

- Lindsay I Smith, "A tutorial on Principal Components Analysis."
- Chin-Jen Lin, "Formulations of Support Vector Machines: A Note from an Optimization Point of View," Department of Computer Science and Information Engineering, National Taiwan University, Neural Computation 13, 2001.

**Index Terms**

Computer Science  
Network Security

**Keywords**

Intrusion Detection  
Anomaly Detection  
Principal Component Analysis  
Support Vector Machine