Abstract

Intrusion Detection System (IDS) is an effective security tool that helps to prevent unauthorized access to network resources by analysing the network traffic and classifying the records as either normal or anomalous. In this paper, a new classification method using Fisher Linear Discriminant Analysis (FLDA) is proposed. The features of KDD Cup attack dataset are reduced for each class of attacks using correlation based feature selection method. Then with the reduced feature set, discriminant analysis is done for the classification of records. Comparison with other approaches reveals that our approach achieves good classification rate for R2L (Remote-to-Local) and U2R (User-to-Root) attacks.

References

- R. Agarwal and M. V. Joshi, "PNrule: A new framework for learning classifier


- H. Moayedi and M. Masnadi-Shirazi, &quot;Arima model for network traffic prediction and anomaly detection&quot;; in Proc. ITSIm 2008, pp. 1-6, August 2008.


- SPSS Inc., &quot;SPSS 13.0 Base User's Guide&quot;


**Index Terms**

Computer Science Security
Keywords
Intrusion Detection System  R2L  U2R  Fisher Linear Discriminant Analysis  Feature Reduction  Spss  Weka  Kdd Cup ‘99