World Academy of Science, Engineering and Technology
International Journal of Electrical and Information Engineering
Vol:9, No:10, 2015

Open Science Index, Electrical and Information Engineering Vol:9, No:10, 2015 publications.waset.org/abstracts/37402.pdf

Intrusion Detection System Using Linear Discriminant Analysis

Authors : Zyad Elkhadir, Khalid Chougdali, Mohammed Benattou

Abstract : Most of the existing intrusion detection systems works on quantitative network traffic data with many irrelevant and redundant features, which makes detection process more time’s consuming and inaccurate. A several feature extraction methods, such as linear discriminant analysis (LDA), have been proposed. However, LDA suffers from the small sample size (SSS) problem which occurs when the number of the training samples is small compared with the samples dimension. Hence, classical LDA cannot be applied directly for high dimensional data such as network traffic data. In this paper, we propose two solutions to solve SSS problem for LDA and apply them to a network IDS. The first method, reduce the original dimension data using principal component analysis (PCA) and then apply LDA. In the second solution, we propose to use the pseudo inverse to avoid singularity of within-class scatter matrix due to SSS problem. After that, the KNN algorithm is used for classification process. We have chosen two known datasets KDDcup99 and NSLKDD for testing the proposed approaches. Results showed that the classification accuracy of (PCA+LDA) method outperforms clearly the pseudo inverse LDA method when we have large training data.

Keywords : LDA, Pseudoinverse, PCA, IDS, NSL-KDD, KDDcup99
Conference Title : ICISS 2015 : International Conference on Information Systems Security
Conference Location : Paris, France
Conference Dates : October 29-30, 2015