Australian Journal of Basic and Applied Sciences, 7(8): 940-944, 2013
ISSN 1991-8178

An Accurate Method for Detection of Cyber Attacks

[1]Uma Murugesan, [2]Dr. G.Padmavathi

[1]Ph.D Research scholar Department of Computer Science Avinashilingam Institute for Home Science and Higher Education for Women Coimbatore, India
[2]Professor and Head Department of Computer Science Avinashilingam Institute for Home Science and Higher Education for Women Coimbatore, India

Abstract: Due to the rapid growth of wireless local area networks in day-to-day applications detection of cyber attacks have been increasing. In 2012, a survey stated that an organization experiences with an average of 102 attacks every week, whereas 72 attacks and 50 attacks were detected during 2011 and 2010, approximately 42% of attacks have increased in a year. In this paper, the dimensionality reduction techniques are used to detect the cyber attacks. The objective of this research work is to extract the meaningful class labels in the data set using linear dimensionality reduction techniques like Principal Components Analysis (PCA), Independent Component Analysis (ICA) and Linear Discriminant analysis (LDA). The experimental study shows that PCA performs better than LDA and ICA. To improve the obtained results the PCA is combined with SVM, where an accuracy rate increases in the detection of cyber attacks.

Key words: PCA, LDA, ICA, SVM, Cyber attacks

INTRODUCTION

Increased usage of internet in wireless local area networks lead to the major growth of cyber attacks and produce a lot of damage to an entire society. Cyber attacks not only compromise the confidentiality, integrity and availability of data, it also creates some key impacts on the economic status of the country. Nowadays attacking moves from the network layer to the application layer. The motivation behind these attacks is to gain financially, so that the attackers are targeting business and web applications (http://gulfnews.com).

It is obvious that the computers and cyber world are exposed to the outside world which comforts the attackers to accord those computers and networks. In this case, the unauthorized users will be identified from the authorized users of the pertinent techniques. The booming area of network security in a wireless local area network is to identify the attacks using various techniques to avoid the issues. High dimensionality reduction is a technique that helps to identify the cyber attacks in network traffic. The high dimensionality reduction techniques like PCA, ICA and LDA play a vital role in detecting attacks in present days.

The paper is organized as follows. Section 2 discusses the dimensionality reduction techniques.In Section 3, process of PCA with SVM is explained. Section 4 elucidates the results and discussions and Section 5 concludes the work.

Dimensionality Reduction Techniques:

Dimensionality reduction techniques are used to transform the original high dimensional data into consequential description of reduced data. The process of assuming that the data will be placed on or near a linear subspace of higher dimensional space is termed as linear technique (George, E. Noel, *et al.*,). The dimensionality technique is mainly classified as linear and non-linear technique with various types and it is depicted in figure 1.

Principal Component Analysis (PCA):

PCA (Wei Wang, Roberto Battiti, 2009) can be used to analyze the density of data. It is otherwise known as Karhunen-Loeve transform. It is considered as a competent scheme of identifying any type of attacks. It helps to check the similarities and differences between the data. The basic process of PCA is fully dependent on reconstructing comparatively huge numeral variables into the lesser of uncorrelated variables where the data will be retained as it is. PCA produces a set of principal components, which are orthonormal eigenvalue/ eigenvector pairs. It is considered as a more efficient analysis tool as it helps to reduce the data in certain outline being without losing the data.

The principal component produces the results in a number of component values according to the number of original variables. The first linear variable will be calculated by replacing the original variable with the new principal component. Principle component values can be calculated using the following equation

Corresponding Author: Uma Murugesan, Ph.D Research scholar Department of Computer Science Avinashilingam

$$X_{nxm} = \begin{bmatrix} x_{11}.....x_{1m} \\ x_{21}.....x_{2m} \\ ..... \\ xn1.....x_{nm} \end{bmatrix} = [x_1,...,x_n]$$

x1, x2 are the observations which will be exhibited as a vector of length m and the entire dataset will be reproduced Xnxm as a matrix.

The average observation and deviation can be calculated using the following formulas respectively

$\mu = \frac{1}{n}\sum_{i=1}^{n} x_i$ and $\Phi^i = xi - \mu$

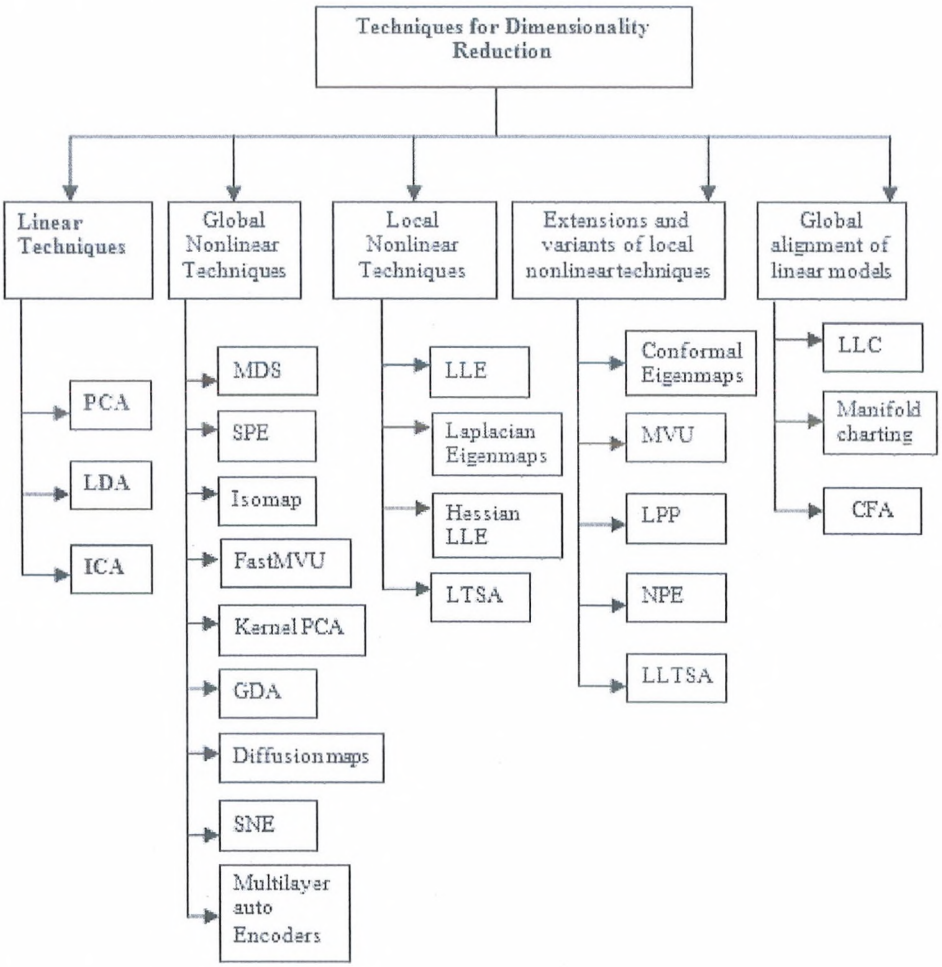


Fig. 1: Dimensionality Reduction Techniques

Linear Discriminant Analysis (LDA):

One of the traditional statistical techniques for dimensionality reduction is Linear Discriminant Analysis (Laurens van der Maaten,). It is otherwise known as Fisher Mapping. It enables to sort out the group of biased information to the maximum when executing dimensionality reduction and aims to locate the directions [3]. It is a promising strategy developed recently to detect attacks from network traffic and it also helps to detect new, unknown and pattern of attacks (Aapo Hyvärinen and Erkki Oja, 2000).

$$S_w = \sum_c Pc \underset{X^c - X^c}{\text{cov}}$$

$$S_b = \sum_c \text{cov}_{x^c} = \text{cov}_{X-\bar{X}} - S_w$$

Independent Component Analysis:

A linear transformation is performed in order to split the multivariate signal into subcomponents and it is the basic process of Independent Component Analysis (ICA). ICA has a wide area of applications like data analysis and compression, audio and image processing, feature extraction, signal separation, detecting the hidden components, Noise is diminishing from Images, telecommunications (Venkatachalam, V., S. Selvan,). It relates the process of method called blind source separation (Aapo Hyvärinen, 1999). It helps for redundancy reduction.

Xj=aj1s1+ aj2s2+.... +ajnsn, for all j.

Proposed System:

In this research work, PCA and SVM are integrated and used to detect outliers in a simulated data set. The algorithm can accurately detect anomalies in non-Gaussian data. Class training stage in which the negative class data are generated based on outlying positive class data. The method for selection of both the size and actual data points for the negative class. It specifies the size of the negative class and the actual data points that represent it are chosen based on the sum of the second norm distances of each data point to their neighbors.

To figure out the joint class probability, a consequence of cross space detection is done. The joint class probabilities can be used to predict the future system performance of the SVM classifier, which constructs two predictor models D1 (y1) and D2 (y2) for each distribution respectively. Predictor models are constructed using the given PCA where the output is ascertained from two subspaces and a distribution of negative class data. One class classifiers would be more appropriate in this situation where negative class data (representing the faulty behavior) are not available. A soft decision boundary can be constructed with the training data with a likelihood function that maps SVM with posterior probabilities.

In the evaluation stage, a new observation is processed through the same algorithmic steps; it is projected against the model and residual subspace. Then it is classified by the SVM predictor model. The joint class probability from the two subspaces will be used for the decision classification. PCA reduces the calculated cost of NIDS (Network Intrusion Detection System) and improves the efficiency of the analysis. Principal component analysis reduces forty two dimensions and its output provides a set of features that are the linear combination of the original set of features. It also minimizes the error that is incurred during the reconstruction of data.

The input for the SVM becomes more efficient as it represents the principal components that are with maximum variance and that are orthogonal. The new subspace consisting of features is clustered according to the variance, so that the classification done by discriminating plane which considers minimum variance becomes more accurate. Thus, it calculates the margin, the support vectors the alpha values and the weights. For the connection of records, class labels are represented as 0 for normal and 1 for anomaly class. Figure 2 depicts the flow of the proposed system.

RESULTS AND DISCUSSIONS

Principal component Analysis, Linear Discriminant Analysis and Independent Component Analysis are compared in detecting the attacks with the given dataset. Among the three, Principal Component Analysis is found to be the best dimensionality reduction techniques. It detects the 87% of the attacks whereas LDA and ICA finds only 82% and 74% respectively. In order to increase its efficiency the most popular optimization technique SVM is combined with PCA. Usually the optimization techniques will be used to classify the detected attacks. But in this research work the dataset is given as input in SVM to make data as an optimized one and the output of it is given as input to PCA for detection. While combining the SVM with PCA it increases the accuracy rate at 94%. The percentage of detection rate is increased to 7%.

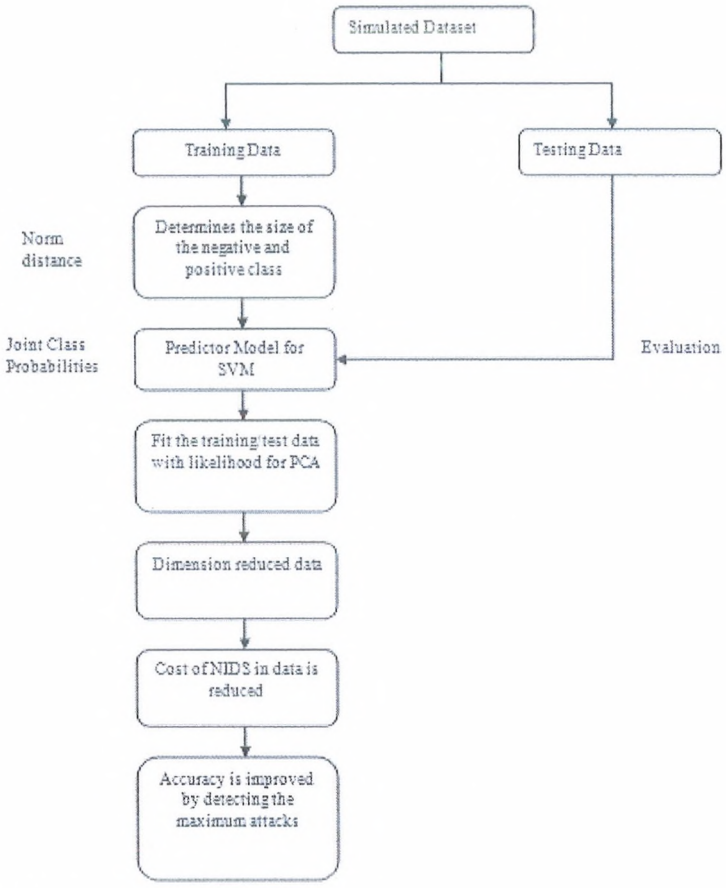
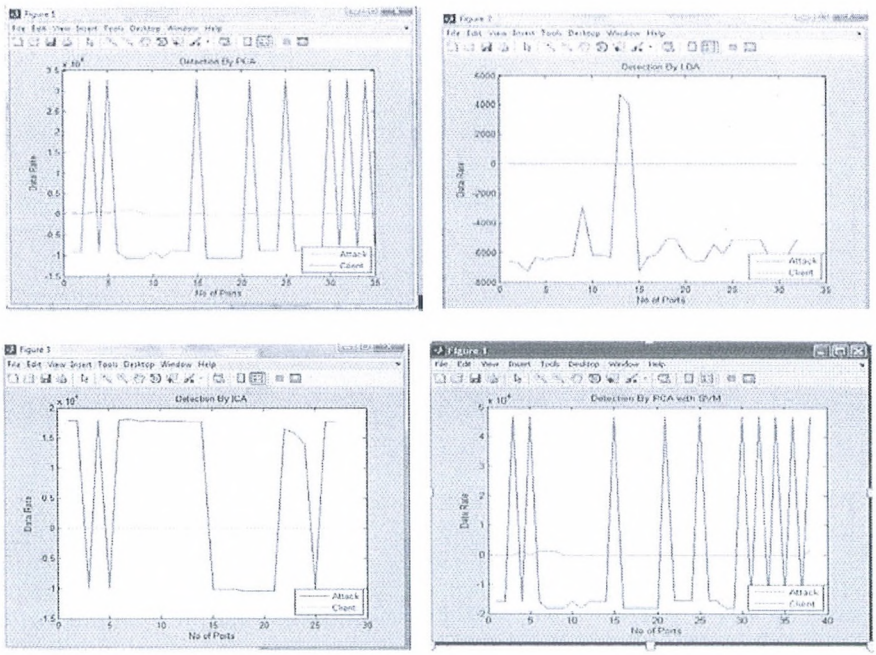


Fig. 2: Proposed Framework



Conclusion:

This study helps to find out an efficient method to detect attacks using dimensionality reduction techniques such as Principal Component Analysis, Linear Discriminant Analysis and Independent Component Analysis. The performance of the three techniques is compared with each other to find out the best technique. In future the real time traffic data can be used to study the capability of the techniques used in this research work and the accuracy level can be improved.

REFERENCES

Aapo Hyvärinen and Erkki Oja, 2000. "Independent Component Analysis: Algorithms and applications", Neural Networks Research Centre, Helsinki University of Technology, Neural Networks, 13(4-5): 411-430.

Aapo Hyvärinen, 1999. "Survey on Independent Component Analysis", Neural Computing Surveys, 2: 94-128.

George, E. Noel, Steven C. Gustafson, Gregg H. Gunsch, "Network-Based Anomaly Detection Using Discriminant Analysis", Air Force Institute of Technology, USA.

http://gulfnews.com/business/technology/cyber-attacks-on-atm-and-internet-banking-applications-on-the-rise.

http://svr-www.eng.cam.ac.uk/~kkc21/thesis_main/node25.html

Laurens van der Maaten, "An Introduction to Dimensionality Reduction Using Matlab" MICC, Maastricht University, The Netherlands, pp: 1-6.

Rupali Datti and Bhupendra verma, 2010. "Feature Reduction for Intrusion Detection Using Linear Discriminant Analysis", International Journal on Computer Science and Engineering, 02(04): 1072-1078.

van der Maate, L.J.P., E.O. Postma and H.J. van den Herik, "Dimensionality Reduction: A Comparative Review", Preprint submitted to Elsevier.

Venkatachalam, V., S. Selvan, "Performance Comparison of Intrusion Detection System Classifiers using various Features Reduction Techniques", I.J. of SIMULATION, 9(1): 30-39.

Wei Wang, Roberto Battiti, 2009. "Identifying Intrusions in Computer Networks with Principal Component Analysis", Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06) IEEE.