International Journal of Engineering Research and Application www.ijera.com ISSN : 2248-9622, Vol. 8, Issue 2, (Part -3) February 2018, pp.76-78

RESEARCH ARTICLE OPEN ACCESS

Soft Computing Applications for Intrusion Detection on Computer Network Security

Kshitish Kumar Dash[1], Jagdish Pradhan[2], Prasant Kumar Sahu[3]

[1,3]Assistant Professor, Department of Mechanical Engineering, Gandhi Institute For Technology (GIFT), Bhubaneswar

[2] Assistant Professor, Department of Mechanical Engineering, Gandhi Engineering College, Bhubaneswar

ABSTRACT---In today's competitive world, computer security is at a boom due to tremendous amount of intruders. To prevent such intruders, detection is required at all levels of a network security. Computer hackers have destroyed voluminous data for which computer security uses a secured tool that helps in detecting attacks in order to harm the computer. These intrusion detections are programmed to detect malicious attacks by anomalous activity. This paper presents new technique of detecting network intrusions using soft computing techniques.

Keywords- Soft Computing, Network intrusions, web semantics, fuzzy rules.

I. INTRODUCTION

Intrusion have been applied in various areas of education. Specifically Web Semantics have been used in teaching and learning using fuzzy rules. Fuzzy rules being one of the applications of Soft Computing techniques.[1] Intrusion detection is an important problem of computer network security. Based on the observed findings, the Signature based attacks have become obsolete. Due to this reason new methodologies are required for finding out the anomalies in the attacks

Intrusion detection is the process of monitoring the events occurring in a computer network system and analyzing them for signs of intrusions [3]. On different situations intrusions have been defined as a hazardous entry into a network that will destroy the valuable data in a authorised network. An Intrusion Detection System does not eliminate the use of preventive mechanism but it works as the defensive mechanism in securing the system [4].

Many required data collected and analysis engine processes of IDS to identify intrusive activities which include statistical [5], machine learning [6], data mining [7] and immunological inspired techniques [8]. There are two main Intrusion Detection Systems. There are two types of intrusions:

- Anomaly Based
- Signature Based

This paper we provide the new technique for solved problem, Independent Component Analysis (ICA) aims at extracting unknown hidden factors/components from multivariate data using only the assumption that the unknown factors are mutually independent. The SVM is one of the techniques of soft computing that would also facilitate the process of detecting the intrusions in a network.

The rest of this paper is organized as follows: In Section 2, we discuss the related works and introduction to Independent Component Analysis, an explanation on Support Vector Machines. The experimental design and setup are shown in section 3. An Experimental Result is shown in Section 4.

II.RELATED WORK

There are some important features that an Intrusion Detection System should possess/include.

Most attacks make their way by network protocolas which are the major loop holes of attacking a network.Twycross [10] proposed a new paradigm in immunology, Danger Theory, to be applied in developing an intrusion detection system.

A. Independent Component Analysis (ICA) ICA is a computation for separating a multivariate signal into additive subcomponents supposing the mutual statistical independence of the non-Gaussian source signals. Thus the motivation of a feature selector

is first, simplifying the classifier by the selected features.

But many SC techniques have produced the following results: 1) the components are mutual independent; 2) each component observes nongaussian distribution. By X = AS, we have S □□A^{-1}X □WX (where W □□$A^{□□}$).

X □□As

(1)

Such that

$P(s) = \prod P_a(S_i)$, (2)

Where $P_a(.)$ the marginal distribution and p is the joint distribution over the n-dimensional vectors. Usually, the technique for performing Independent Component Analysis is expressed as the technique for deriving one particular W,

Y □Wx, (3)

Such that each component of y becomes independent of each other. One general learning technique [12] for finding one W is

$\Delta W = \eta(I – Ø(y) y^T) W$, (4)

B. Support Vector Machine (SVM)

Support Vector Machines have been proposed as a novel technique for intrusion detection.

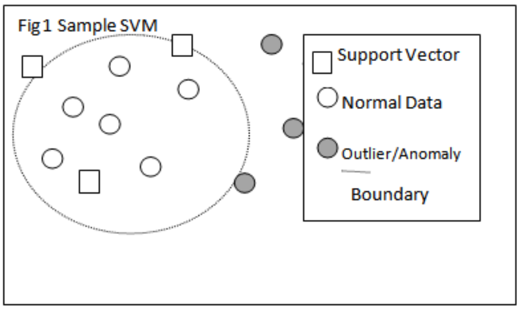


Fig1 Sample SVM

In Figure1, Normal (within bounds) and Anomalous (outliers): Those data points that define the boundary between the normal and the anomalous are called Support Vectors, thus Support Vector Machines. These “define” normalcy.

The kernels are very useful in finding and generalizing the principles that distinguish normal data from attacks. It is in this flexibility that the use of SVM and kernels can greatly increase the IDS success rate at detecting new attacks.

- Two-class classification. SVM learn linear decision rules described by a weighted vector and a threshold. The idea of Structural Risk Minimization is to find a hypothesis for which one can guarantee the lowest probability of error. Geometrically, we can find two parts representing the two classes with a hyper-plane with normal distance from the origin as depicted in Figure 2.

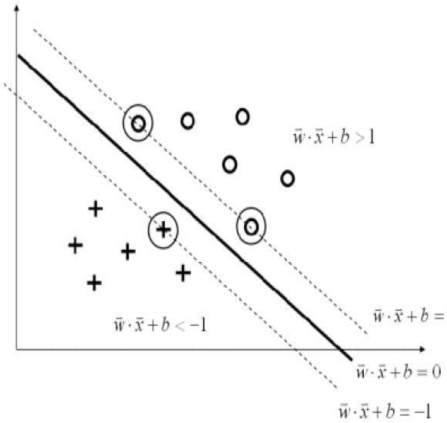

$\vec{w}\cdot\vec{x}+b>1$
$\vec{w}\cdot\vec{x}+b<-1$
$\vec{w}\cdot\vec{x}+b=1$
$\vec{w}\cdot\vec{x}+b=0$
$\vec{w}\cdot\vec{x}+b=-1$

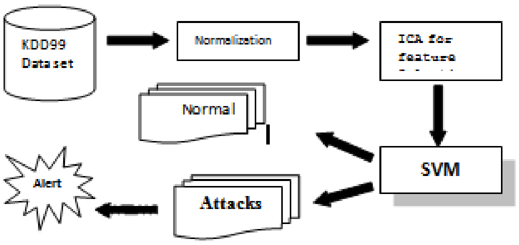
Figure 2 Optimal separating hyper-plane is the one that separates the data

$$D(x) = \text{sign}\{w.x + b\} = = \begin{cases} +1, & \text{if } w.x + b > 0 \\ -1, & \text{else} \end{cases} \quad (5)$$

The vector w is perpendicular, b is to find the widest margin, what is the distance expression for a point x to a line, supports that separating hyper-planes exist. We define the margin of a separating hyper-plane as the minimum distance between all input vectors and the hyper-plane.

III. EXPERIMENTAL DESIGN AND SETUP

In our method [26], we have three steps (Figure.3). First step is for cleaning and handling missing and incomplete data. Second step is for selecting the best attribute or feature selection step using ICA. And the finally is for classifying different groups of data using SVM. Normalization step consist of two steps.



IV. EXPERIMENTAL RESULT

A. Data Manipulation

A lot of data had to be manipulated for considering our experimental challenges. For this reason, the derived data set was considered as the original set and numerous amount of data was categorized based on severe attacks.

B. Performance Measurement

Standard measures for evaluating IDS include detection rate, false alarm rate, trade-off between detection rate and false alarm rate [29], performance (Processing Speed + Propagation + Reaction), and Fault Tolerance (resistance to attacks, recovery, and subversion).

V. CONCLUSION

The data vectors are apparently been discussed as having affectors higher in the Independent Componenet Analysis.

Intrusion detection techniques have demanded more attention and observation due to its frequent attacks on networks in all corporations. Our future work shall investigate more into different types of networks using various other soft computing techniques.

REFERENCES

[1]. Huda Fatima, Sateesh Pradhan, G.N.Dash, Web Semantics in improving teaching and learning using fuzzy rules,Volume 3, Issue ICRASE13, May 2013, ISSN Online: 2277-2677.

[2]. D.S Bauer, M.E Koblentz, NIDX- An Expert System for Real-Time Network Intrusion Detection, Proceedings of the Computer NetworkingSymposium, 1988, pp. 98-106.

[3]. Sandhya Peddabachigari, Ajith Abraham, and J. Thomas, IntrusionDetection Systems Using Decision Trees and Support Vector Machines.VECTOR MACHINES, INTERNATIONAL JOURNAL OF APPLIED SCIENCE AND COMPUTATIONS 2004: p. 118--134.

[4]. V. Ramos, A. Abraham, ANTIDS: Self-Organized Ant-based ClusteringModel for Intrusion Detection System, In Swarm Intelligence and Patterns special session at WSTST-05 - 4th IEEE International Conference on Soft Computing as Trans disciplinary Science and Technology - Japan, LNCS series, Springer-Verlag, Germany, May 2005, pp. 977-986.

[5]. R. Bace and P. Mell, Intrusion Detection Systems, NIST Special Publication on Intrusion Detection System, 31 November 2001.

[6]. A. Sundaram, An Introduction to Intrusion Detection, Crossroads: The ACM student magazine, Vol. 2, No. 4, April 1996.

[7]. D. Denning, An Intrusion-Detection Model, In IEEE computer society symposium on research in security and privacy, 1986, pp. 118-131.

[8]. T. Lane, Machine Learning Techniques for The Computer Security, PhD thesis, Purdue University, 2000.

[9]. W. Lee and S. Stolfo, Data Mining Approaches for Intrusion Detection, Proceedings of the 7th USENIX security symposium, 1998.

[10]. Roman W. Swiniarski , Andrzej Skowron, Rough set methods in feature selection and recognition, Pattern Recognition Letters, v.24 n.6, p.833-849, March 2003.

Kshitish Kumar Dash “ Soft Computing Applications for Intrusion Detection on Computer Network Security” *International Journal Of Engineering Research And Applications (IJERA*), VOL.8(2), 2018, PP 76-78.