Proceedings of the 5th WSEAS International Conference on Applied Computer Science, Hangzhou, China, April 16-18, 2006 (pp987-991)

A Fusion of ICA and SVM for Detection Computer Attacks

SURAT SRINOY[1], WITCHA CHIMPHLEE[2],SIRIPORN CHIMPHLEE[3],
YOOTHAPOOM POOPAIBOOL[4]
Faculty of Science and Technology
Suan Dusit Rajabhat University,
295 Ratchasima Road, Dusit, Bangkok, Tel: (662)-2445225, Fax: (662)-6687136
THAILAND.

http://www.dusit.ac.th

Abstract: - Intrusion detection is the art of detecting unauthorized, inappropriate, or anomalous activity on computer systems. Independent component analysis (ICA) aims at extracting unknown hidden factors/components from multivariate data using only the assumption that unknown factors are mutually independent. In this paper it discuss an intrusion detection method that proposes *independent component analysis* based feature selection heuristics and using *support vector machine* for classification data. The experimental results on Knowledge Discovery and Data Mining-(KDDCup 1999) dataset.

Key-Words: - Intrusion Detection System, Anomaly detection, Independent Component Analysis, Support Vector Machine

1 Introduction

Because of the attack space is dynamic and ever changing. Signature based IDS's are quickly becoming outdated and unmanageable. New attacks/network configurations cannot be constantly updated and hard-coded, and thus, a more efficient and robust method of differentiating normal behavior from anomalies is needed.

As defined in [1], intrusion detection is "the process of monitoring the events occurring in a computer system or network and analyzing them for signs of intrusions. It is also defined as attempts to compromise the confidentiality, integrity, availability, or to bypass the security mechanisms of a computer or network". Many approaches have been proposed which include statistical [2], machine learning [3], data mining [4] and immunological inspired techniques [5]. There are two main intrusion detection systems. Anomaly intrusion detection system is based on the profiles of normal behaviors of users or applications and checks whether the system is being used in a different manner [6]. The second one is called misuse intrusion detection system which collects attack signatures, compares a behavior with these attack signatures, and signals intrusion when there is a match. 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 standard support vector machine (SVM) is a classifier that finds a maximal margin separating two classes of data. Feature selection techniques aim at reducing the number of unnecessary features in classification rules. Feature selection is an optimization process in which one tries to find the best feature subset, from the fixed set of the original features, according to a given processing goal and a feature selection criterion. A pattern's features, from the point of view of processing goal and type, may be irrelevant (having no effect on processing performance) or relevant (having an impact on processing performance). Features can be redundant (correlated, dependent) [7].

An Intrusion Detection System (IDS) is a program that analyzes what happens or has happened during an execution and tries to find indications that the computer has been misused. An Intrusion detection system does not eliminate the use of preventive mechanism but it works as the last defensive mechanism in securing the system [8]

This paper suggests the use ICA as a dimensionality reduction technique to avoid this information loss. The rest of this paper is organized as follows. In section 2, it discuss the related works; Introduce independent component analysis in section 3; explains Support Vector Machines in section 4; Experimental Design and Setup show in section 5; and in section 6 ends the paper with a conclusion and some discussion.

2. Related Works

In a classification problem, the number of features can be quite large, many of which can be irrelevant or redundant. Since the amount of audit data that an IDS needs to examine is very large even for a small network, classification by hand is impossible. Feature reduction and feature selection improves classification by searching for the subset of features, which best classifies the training data. Some of the important features an intrusion detection system should possess include refer in Srilatha et al. [9].

Most intrusion occurs via network using the network protocols to attack their targets. Twycross [10] proposed a new paradigm in immunology, Danger Theory, to be applied in developing an intrusion detection system. Alves et al. [11] presents a classification-rule discovery algorithm integrating artificial immune systems (AIS) and fuzzy systems. For example, during a certain intrusion, a hacker follows fixed steps to achieve his intention, first sets up a connection between a source IP address to a target IP, and sends data to attack the target [6]. Generally, there are four categories of attacks [10]. They are: 1) DoS (denial-of-service), for example ping-of-death, teardrop, smurf, SYN flood, and the like. 2) R2L : unauthorized access from a remote machine, for example guessing password, 3) U2R : unauthorized access to local super user (root) privileges, for example, various “buffer overflow” attacks, 4) PROBING: surveillance and other probing, for example, port-scan, ping-sweep, etc. Some of the attacks (such as DoS, and PROBING) may use hundreds of network packets or connections, while on the other hand attacks like U2R and R2L typically use only one or a few connections.[11]

3 Independent Component Analysis (ICA)

ICA is a computational for separating a multivariate signal into additive subcomponents supposing the mutual statistical independence of the non-Gaussian source signals. A relevant feature is defined in [5] as one removal of which deteriorates the performance or accuracy of the classifier, and an irrelevant or redundant feature is not relevant. These irrelevant features could deteriorate the performance of a classifier that uses all features since irrelevant information is included inside the totality of the features. Thus the motivation of a feature selector is (i) simplifying the classifier by the selected features; (ii) improving or not significantly reducing the accuracy of the classifier; and (iii) reducing the dimensionality of the data so that a classifier can handle large values of data [6]. Many approaches as feature selectors have been proposed.

Independent component analysis (ICA) for dimension reduction is to separate these independent components (ICs) from the monitored variables. Introduction of ICA concepts in the early 1980s in the context of neural networks and array signal processing. ICA was originally developed to deal with problems that are closely related to the real world ‘cocktail-party’ problem. ICA is a method for automatically identifying the underlying factors in a given data set. Dimension reduction using ICA is based on the idea that these measured variables are the mixtures of some independent variables. When given such a mixture, ICA identifies those individual signal components of the mixture that are unrelated. Given that the only unrelated signal components within the signal mixture are the voices of different people. ICA is based on the assumption that source signals are not only uncorrelated, but are also ‘statistically independent’ [12].

ICA techniques provide statistical signal processing tools for optimal linear transformations in multivariate data and these methods are well-suited for feature extraction, noise reduction, density estimation and regression [13]. The ICA problem can be described as follows, each of h mixture signal x1(k), x2(k),…,xh(k) is a linear combination of q independent components s1(k),s 2(k),…,sh(k) , that is , X = AS where A is a mixing matrix. Now given X, to compute A and S. Based on the following two statistical assumptions, ICA successfully gains the results: 1) the components are mutual independent; 2) each component observes nongaussian distribution. By X = AS, it has S = A-1X=WX (where W = A-1). The take is to select an appropriate W which applied on X to maximize the nongaussianity of components. This can be done in an iteration procedure.

Given a set of n-dimensional data vectors [X(1),X(2),…,X(N)], the independent components are the directions (vectors) along which the statistics of projections of the data vectors are independent of each other. Formally, if A is a transformation from the given reference frame to the independent component reference from then

$$X = As$$

Such that

$$p(s) = \prod p_a(s_i),$$

where $p_a(.)$ is the marginal distribution and p(s) 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,

$$Y = Wx,$$

Such that each component of *y* becomes independent of each other. If the individual marginal distributions are non-Gaussian then the derived marginal densities become a scaled permutation of the original density functions if one such W can be obtained. One general learning technique [10; 11] for finding one W is

$$\Delta W = \eta(I - \phi(y)y^T)W,$$

Where $\phi(y)$ is a nonlinear function of the output vector y (such as a cubic polynomial or a polynomial of odd degree, or a sum of polynomials of odd degrees, or a sigmoidal function) [14].

4 Support Vector Machines (SVM)

Support Vector Machines have been proposed as a novel technique for intrusion detection. SVM maps input (real-valued) feature vectors into higher dimensional feature space through some nonlinear mapping. SVMs are powerful tools for providing solutions to classification problems. These are developed on the principle of structural risk minimization. Structural risk minimization seeks to find a hypothesis for which one can find the lowest probability of error. The structural risk minimization can be achieved by finding the hyper plane with maximum separable margin for the data [15].

To automatically separate IDS data into normal or anomalous distributions. The intrusion detection model based on SVM (support vector machine) is mainly classified into three types. The first type [16] divides data into normal data and attack data using characteristics of the binary classifier SVM, and the second type [17] implements an anomaly detection model using one-class SVM. Finally, the third type [18] establishes multi-class SVM at the form of combining many binary classifiers, namely, SVMs and divides data into normal data and four types of attack data [19].

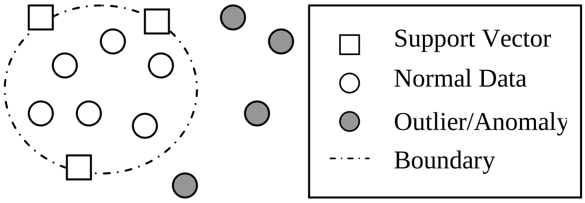

Figure 1. Sample SVM

In Fig. 1 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.

Computing the hyper plane to separate the data points, i.e. training a SVM, leads to a quadratic optimization problem. SVM uses a feature called a kernel to solve this problem. A kernel transforms linear algorithms into nonlinear ones via a map into feature spaces. SVMs classify data by using these support vectors, which are members of the set of training inputs that outline a hyper plane in feature space [20].

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

In [21] explained kinds of learning machines as follows.

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, it can find two parts representing the two classes with a hyper-plane with normal and distance from the origin as depicted in Figure 2.

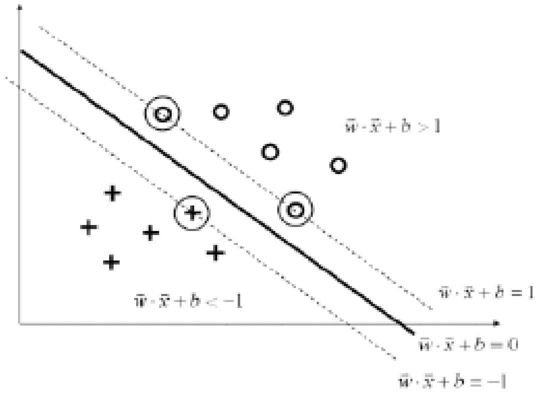
$\vec{w}\cdot\vec{x}+b>1$
$\vec{w}\cdot\vec{x}+b<-1$
$\vec{w}\cdot\vec{x}+b=1$
$\vec{w}\cdot\vec{x}+b=0$
$\vec{w}\cdot\vec{x}+b=-1$

Figure 2. Optimal separating hyperplane is the one that separates the data.

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

Support such separating hyper-planes exist. It define the margin of a separating hyper-plane as the minimum distance between all input vectors and the hyper-plane.

Multi-class Classification. SVM were originally designed for two-class classification, commonly called as binary classification. Currently there are two types of approaches for multi-class SV<, one-against-all [22] and one-against-one approaches [23]. One is by constructing and combining several binary classifiers while the other is by directly considering all data in one optimization formulation [24].

5. Experimental Design and Setup

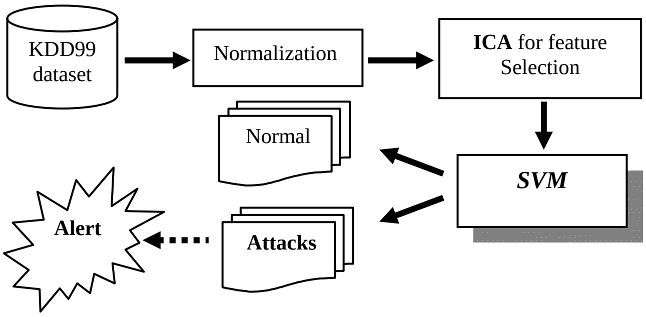

Figure 3. The architecture of integrating ICA and SVM

In our method have three steps (Figure.3). First step for cleaning and handle missing and incomplete data. Second step for select the best attribute or feature selection using ICA and the last step for classification group of data using SVM. Normalization step consisted of two steps.

The first step involved mapping symbolic-valued attributes to numeric-valued attributes and the second step implemented non-zero numerical features. In Table 2 describe variables for intrusion detection data set

Table 1. Dataset for attack distribution

Attack Type	Population Size
Normal	5,763
Probe	2,164
DoS	3,530
U2R	70
R2L	6,689
Summary	18,216

In this experiment, it use a standard dataset the raw data used by the KDD Cup 1999 intrusion detection contest [25]. This database includes a wide variety of intrusions simulated in a military network environment that is a common benchmark for evaluation of intrusion detection techniques. In general, the distribution of attacks is dominated by probes and denial-of-service attacks; the most interesting and dangerous attacks, such as compromises, are grossly under-represented [26]. The data set has 41 attributes for each connection record plus one class label. There are 24 attack types, but it treat all of them as an attack group. A data set of size N is processed. The nominal attributes are converted into linear discrete values (integers). After eliminating labels, the data set is described as a matrix X, which has N rows and m=41 columns (attributes). There are md=8 discrete-value attributes and mc = 33 continuous-value attributes.

It ran experiments on a system with a 1.5 GHz Pentium IV processor and 512 MB DDR RAM running Windows XP.

6 Conclusion

In this paper, it proposed an approach of integrating ICA and SVM for intrusion detection. In the first step, independent components are extracted from intrusion data, which included data about normal and anomalous patterns. The intrusion detection method can effectively get the essential features of intrusion action and possess the higher ability to identify new intrusion activities. Next, the obtained components were input into SVM for intrusion classification. It evaluated our approach on the benchmark data from KDD'99 data set.

Intrusion detection model is a composition model that needs various theories and techniques. One or two models can hardly offer satisfying results. In future work, we plan to apply other theories and techniques in intrusion detection in our future work.

Acknowledgements

This research was supported in part by grants from Suan Dusit Rajabhat University *www.dusit.ac.th* at Bangkok, Thailand.

References:

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

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

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

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

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

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

[7] 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.

[8] V. Ramos, A. Abraham, ANTIDS: Self-Organized Ant-based Clustering Model 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.

[9] S. Chebrolu, A. Abraham, J. P. Thomas, *Feature Deduction and Ensemble Design of Intrusion Detection Systems*, Computer & Security, 2004.

[10] J. Twycross , Immune Systems, Danger Theory and Intrusion Detection, *presented at the AISB 2004 Symposium on Immune System and Cognition*, Leeds, U.K., March 2004.

[11] R.T. Alves, M.R.B.S. Delgado, H.S. Lopes, A.A. Freitas, An artificial immune system for fuzzy-rule induction in data mining, *Lecture Notes in Computer Science, Berlin: Springer-Verlag,*Vol.3242, 2004, pp.1011-1020.

[12] D. Dagupta and F. Gonzalez, An Immunity-Based Technique to Characterize Intrusions in Computer Networks, *IEEE Transactions on Evolutionary Computation*, Vol. 6, June 2002, pp.28- 291,

[13] H. Jin, J. Sun, H. Chen, and Z. Han, A Fuzzy Data Mining Based Intrusion Detection System, *Proceedings of 10thInternational Workshop on future Trends in Distributed Computing Systems (FTDCS04) IEEE Computer Society*, Suzhou, China, May 26-28, 2004, pp. 191-197.

[14] Q. Shen and A., Chouchoulas. Rough Set-Based Dimensionality Reduction for Supervised and Unsupervised Learning, International Journal of Applied Mathematics and Computer Science,Vol.11, No. 3, 2001, pp.583–601.

[15] V.N.Vapnik, *The Nature of Statistical Learning Theory*, Springer, 1995.

[16] W.H. Chen, S.H. Hsu, and H.P. Shen, Application of SVM and ANN for intrusion, Computers & Operations Research, *ELSEVIER*, Vol. 32, No.10, 2005, pp. 2617-2634.

[17] K.L. Li, H.K. Huang, S.F. Tian, and W. Xu, Improving one-class SVM for anomaly detection, International Conference on Machine Learning and Cybernetics, Vol.5, 2003, pp. 3077-3081.

[18] T. Ambwani, Multi class support vector machine implementation to intrusion detection, *Proceedings of the International Joint Conference on Neural Networks*, Vol. 3, 2003, pp. 2300-2305.

[19] H. Lee, J. Song, D. Park, Intrusion Detection System Based on Multi-class SVM, RSFDGrC, Vol. 2, 2005, pp. 511-519

[20] A. Abraham, R.Jain, S*oft Computing Models for Network Intrusion Detection Systems* CoRRcs, CR/0405046, 2004.

[21] J. C.Christopher Burges, A Tutorial on Support Vector Machines for Pattern Recognition, *Data Mining and Knowledge Discovery*, 1998.

[22] B. Schoelkopf, C. Burges, and V. Vapnik., Extracting support data for a given task. In U.M. Fayyad, and R. Uthurusamy, editors, Proceedings, *First International Conference on Knowledge Discovery & Data Mining*, AAAI Press, MenloPark, CA ,1995.

[23] S. Knerrr, L. Personnaz, and G. Dreyfus, Single-layer Learning Revisited: a Stepwise Procedure for Building and Training a Neural Network, In J. Fogelman, editor, Neurocomputing: Algorithms, *Architectures and Applications, Springer-Verlag*, 1990.

[24] D. S. Kim, J. S. Park, *Network-Based Intrusion Detection with Support Vector Machines*, ICOIN, 2003, pp. 747-756

[25]KDD data set, 1999; http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

[26] P. Laskov, K. Rieck, C. Schäfer, K.R. Müller, Visualization of anomaly detection using prediction sensitivity, Proceedings of Sicherheit, April 2005, pp.197-208.

Table 2. Variables for intrusion detection data set

No.	Variable name	Type	Variable label
1	duration	continuous	A
2	protocol_type	discrete	B
3	service	discrete	C
4	flag	discrete	D
5	src_bytes	continuous	E
6	dst_bytes	continuous	F
7	land	discrete	G
8	wrong_fragment	continuous	H
9	urgent	continuous	I
10	hot	continuous	J
11	num_failed_logins	continuous	K
12	logged_in	discrete	L
13	num_compromised	continuous	M
14	root_shell	continuous	N
15	su_attempted	continuous	O
16	num_root	continuous	P
17	num_file_creations	continuous	Q
18	num_shells	continuous	R
19	num_access_files	continuous	S
20	num_outbound_cmds	continuous	T
21	is_host_login	discrete	U
22	is_guest_login	discrete	V
23	count	continuous	W
24	srv_count	continuous	X
25	serror_rate	continuous	Y
26	srv_serror_rate	continuous	Z
27	rerror_rate	continuous	AA
28	srv_rerror_rate	continuous	AB
29	same_srv_rate	continuous	AC
30	diff_srv_rate	continuous	AD
31	srv_diff_host_rate	continuous	AE
32	dst_host_count	continuous	AF
33	dst_host_srv_count	continuous	AG
34	dst_host_same_srv_rate	continuous	AH
35	dst_host_diff_srv_rate	continuous	AI
36	dst_host_same_src_port_rate	continuous	AJ
37	dst_host_srv_diff_host_rate	continuous	AK
38	dst_host_serror_rate	continuous	AL
39	dst_host_srv_serror_rate	continuous	AM
40	dst_host_rerror_rate	continuous	AN
41	dst_host_srv_rerror_rate	continuous	AO