I.J.Computer Network and Information Security, 2014, 2, 45-53
Published Online January 2014 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2014.02.07

Hybrid Intrusion Detection Using Ensemble of Classification Methods

M.Govindarajan
Assistant Professor, Department of Computer Science and Engineering, Annamalai University
Annamalai Nagar – 608002, Tamil Nadu, India
Email: govind_aucse@yahoo.com

Abstract **—** One of the major developments in machine learning in the past decade is the ensemble method, which finds highly accurate classifier by combining many moderately accurate component classifiers. In this research work, new ensemble classification methods are proposed for homogeneous ensemble classifiers using bagging and heterogeneous ensemble classifiers using arcing classifier and their performances are analyzed in terms of accuracy. A Classifier ensemble is designed using Radial Basis Function (RBF) and Support Vector Machine (SVM) as base classifiers. The feasibility and the benefits of the proposed approaches are demonstrated by the means of real and benchmark data sets of intrusion detection. The main originality of the proposed approach is based on three main parts: preprocessing phase, classification phase and combining phase. A wide range of comparative experiments are conducted for real and benchmark data sets of intrusion detection. The accuracy of base classifiers is compared with homogeneous and heterogeneous models for data mining problem. The proposed ensemble methods provide significant improvement of accuracy compared to individual classifiers and also heterogeneous models exhibit better results than homogeneous models for real and benchmark data sets of intrusion detection.

Index Terms **—** Data Mining, Ensemble, Radial Basis Function, Support Vector Machine, Accuracy.

I. INTRODUCTION

Traditional protection techniques such as user authentication, data encryption, avoiding programming errors and firewalls are used as the first line of defense for computer security. If a password is weak and is compromised, user authentication cannot prevent unauthorized use; firewalls are vulnerable to errors in configuration and suspect to ambiguous or undefined security policies (Summers, 1997). They are generally unable to protect against malicious mobile code, insider attacks and unsecured modems. Programming errors cannot be avoided as the complexity of the system and application software is evolving rapidly leaving behind some exploitable weaknesses. Consequently, computer systems are likely to remain unsecured for the foreseeable future. Therefore, intrusion detection is required as an additional wall for protecting systems despite the prevention techniques. Intrusion detection is useful not only in detecting successful intrusions, but also in monitoring attempts to break security, which provides important information for timely countermeasures (Heady et al., 1990; Sundaram, 1996). Intrusion detection is classified into two types: misuse intrusion detection and anomaly intrusion detection. Several machine-learning paradigms including neural networks (Mukkamala et al.,2003), linear genetic programming (LGP) (Mukkamala et al., 2004a), support vector machines (SVM), Bayesian networks, multivariate adaptive regression splines (MARS) (Mukkamala et al., 2004b) fuzzy inference systems (FISs) (Shah et al., 2004), etc. have been investigated for the design of IDS. The primary objective of this paper is ensemble of radial basis function and Support Vector Machine is superior to individual approach for intrusion detection in terms of classification accuracy.

Data mining methods may be distinguished by either supervised or unsupervised learning methods. One of the most active areas of research in supervised learning has been to study methods for constructing good ensembles of classifiers. It has been observed that when certain classifiers are ensembled, the performance of the individual classifiers.

Recently, advances in knowledge extraction techniques have made it possible to transform various kinds of raw data into high level knowledge. However, the classification results of these techniques are affected by the limitations associated with individual techniques. Hence, hybrid approach is widely recognized by the data mining research community.

Hybrid models have been suggested to overcome the defects of using a single supervised learning method, such as radial basis function and support vector machine techniques. Hybrid models combine different methods to improve classification accuracy. The term combined model is usually used to refer to a concept similar to a hybrid model. Combined models apply the same algorithm repeatedly through partitioning and weighting of a training data set. Combined models also have been called Ensembles. Ensemble improves classification performance by the combined use of two effects: reduction of errors due to bias and variance (Haykin, 1999).

This paper proposes new ensemble classification methods to improve the classification accuracy. The main purpose of this paper is to apply homogeneous and heterogeneous ensemble classifiers for real and benchmark dataset of intrusion detection to improve classification accuracy. Organization of this paper is as follows. Section 2 describes the related work. Section 3 presents proposed methodology and Section 4 explains the performance evaluation measures. Section 5 focuses on the experimental results and discussion. Finally, results are summarized and concluded in section 6.

II. RELATED WORKS

The Internet and online procedures is an essential tool of our daily life today. They have been used as an important component of business operation (T. Shon and J. Moon, 2007). Therefore, network security needs to be carefully concerned to provide secure information channels. Intrusion detection (ID) is a major research problem in network security, where the concept of ID was proposed by Anderson in 1980 (J.P. Anderson, 1980). ID is based on the assumption that the behavior of intruders is different from a legal user (W. Stallings, 2006). The goal of intrusion detection systems (IDS) is to identify unusual access or attacks to secure internal networks (C. Tsai, et al., 2009) Network-based IDS is a valuable tool for the defense-in-depth of computer networks. It looks for known or potential malicious activities in network traffic and raises an alarm whenever a suspicious activity is detected. In general, IDSs can be divided into two techniques: misuse detection and anomaly detection (E. Biermannet al.2001; T. Verwoerd, et al., 2002).

Misuse intrusion detection (signature-based detection) uses well-defined patterns of the malicious activity to identify intrusions (K. Ilgun et al., 1995; D. Marchette, 1999) However, it may not be able to alert the system administrator in case of a new attack. Anomaly detection attempts to model normal behavior profile. It identifies malicious traffic based on the deviations from the normal patterns, where the normal patterns are constructed from the statistical measures of the system features (S. Mukkamala, et al., 2002). The anomaly detection techniques have the advantage of detecting unknown attacks over the misuse detection technique (E. Lundin and E. Jonsson, 2002). Several machine learning techniques including neural networks, fuzzy logic (S. Wu and W. Banzhaf, 2010), support vector machines (SVM) (S. Mukkamala, et al., 2002; S. Wu and W. Banzhaf, 2010) have been studied for the design of IDS. In particular, these techniques are developed as classifiers, which are used to classify whether the incoming network traffics are normal or an attack. This paper focuses on the Support Vector Machine (SVM) and Radial Basis Function (RBF) among various machine learning algorithms.

The most significant reason for the choice of SVM is because it can be used for either supervised or unsupervised learning. Another positive aspect of SVM is that it is useful for finding a global minimum of the actual risk using structural risk minimization, since it can generalize well with kernel tricks even in high-dimensional spaces under little training sample conditions.

In Ghosh and Schwartzbard (1999), it is shown how neural networks can be employed for the anomaly and misuse detection. The works present an application of neural network to learn previous behavior since it can be utilized to detection of the future intrusions against systems. Experimental results indicate that neural networks are "suited to perform intrusion state of art detection and can generalize from previously observed behavior" according to the authors.

Chen et al. (2005a) Suggested Application of SVM an ANN for intrusion detection. Chen et al. (2005b) used flexible neural network trees for feature deduction and intrusion detection. Katar, (2006) combined multiple techniques for intrusion detection.

Freund and Schapire (1995,1996) proposed an algorithm the basis of which is to **a**daptively **r**esample and **c**ombine (hence the acronym--arcing) so that the weights in the resampling are increased for those cases most often misclassified and the combining is done by weighted voting.

Previous work has demonstrated that arcing classifiers is very effective for RBF-SVM hybrid system. (M.Govindarajan et al, 2012). A hybrid model can improve the performance of basic classifier (Tsai 2009).

In this paper, a hybrid intrusion detection system is proposed using radial basis function and support vector machine and the effectiveness of the proposed bagged RBF, bagged SVM and RBF-SVM hybrid system is evaluated by conducting several experiments on real and benchmark datasets of intrusion detection. The performance of the proposed bagged RBF, bagged SVM and RBF-SVM hybrid classifiers are examined in comparison with standalone RBF and standalone SVM classifier and also heterogeneous models exhibits better results than homogeneous models for real and benchmark data sets of intrusion detection.

III. PROPOSED METHODOLOGY

A. Pre-processing of real and benchmark datasets

The real data is related with Acer07 dataset, being released for the first time is a real world data set collected from one of the sensors in Acer eDC (Acer e-Enabling Data Center) and the benchmark data used in classification is NSL-KDD, which is a new dataset for the evaluation of researches in network intrusion detection system. Before performing any classification method the data has to be pre-processed. In the data pre-processing stage it has been observed that the datasets consist of many missing value attributes. By eliminating the missing attribute records may lead to misclassification because the dropped records may contain some useful pattern for Classification. The dataset is pre-processed by removing missing values

using supervised filters.

B. Existing Classification Methods

1) Radial Basis Function Neural Network

Radial basis function (RBF) networks (Oliver Buchtala et al, 2005) combine a number of different concepts from approximation theory, clustering, and neural network theory. A key advantage of RBF networks for practitioners is the clear and understandable interpretation of the functionality of basis functions. Also, fuzzy rules may be extracted from RBF networks for deployment in an expert system.

The RBF networks used here may be defined as follows.

1. RBF networks have three layers of nodes: input layer u_I, hidden layer u_H and output layer u_0.
2. Feed-forward connections exist between input and hidden layers, between input and output layers (shortcut connections), and between hidden and output layers. Additionally, there are connections between a bias node and each output node. A scalar weight $w_{i,j}$ is associated with the connection between nodes i and j.
3. The activation of each input node (fanout) $i \in u_I$ is equal to its external input

$$a_i(k) \overset{def}{=} x_i(k) \tag{3.1}$$

where $x_i(k)$ is the element of the external input vector (pattern) $X(k)$ of the network ($k = 1,2,\ldots$ denotes the number of the pattern).

4. Each hidden node (neuron) $j \in u_H$ determines the Euclidean distance between "its own" weight vector $W_j \overset{def}{=} (w_{(1,j)}, \ldots, w_{(n,j)})$ and the activations of the input nodes, i.e., the external input vector

$$s_j(k) \overset{def}{=} \|W_j - X(k)\| \tag{3.2}$$

The distance $s_j(k)$ is used as an input of a radial basis function in order to determine the activation $a_j(k)$ of node j. Here, Gaussian functions are employed

$$g(s_j) = e^{-s_j^2/r_j^2} \tag{3.3}$$

The parameter r_j of node j is the radius of the basis function; the vector W_j is its center.

Localized basis functions such as the *Gaussian* or the *inverse multiquadric* are usually preferred.

5. Each output node (neuron) $l \in u_0$ computes its activation as a weighted sum

$$a_l(k) \overset{def}{=} \sum_{j=1}^{|u_H|} w_{(j,l)}.a_j(k) + \sum_{i=1}^{|u_I|} w_{(i,l)}.a_i(k) + w_{(B,l)} \tag{3.4}$$

The external output vector of the network, $y(k)$ consists of the activations of output nodes, i.e., $y_l(k) \overset{def}{=} a_l(k)$. The activation of a hidden node is high if the current input vector of the network is "similar" (depending on the value of the radius) to the center of its basis function. The center of a basis function can, therefore, be regarded as a prototype of a hyperspherical cluster in the input space of the network. The radius of the cluster is given by the value of the radius parameter. In the literature, some variants of this network structure can be found, some of which do not contain shortcut connections or bias neurons.

2) Support Vector Machine

Support vector machines (Cherkassky *et al.*, 1998; Burges, 1998) are powerful tools for data classification. Classification is achieved by a linear or nonlinear separating surface in the input space of the dataset. The separating surface depends only on a subset of the original data. This subset of data, which is all that is needed to generate the separating surface, constitutes the set of support vectors. In this study, a method is given for selecting as small a set of support vectors as possible which completely determines a separating plane classifier. In nonlinear classification problems, SVM tries to place a linear boundary between two different classes and adjust it in such a way that the margin is maximized (Vanajakshi and Rilett, 2004). Moreover, in the case of linearly separable data, the method is to find the most suitable one among the hyperplanes that minimize the training error. After that, the boundary is adjusted such that the distance between the boundary and the nearest data points in each class is maximal.

In a binary classification problem, its data points are given as:

$$D = \{(x^1, y^1), \ldots (x^l, y^l)\}, \ldots x \in \Re^n, y \in \{-1, 1\}, \tag{3.5}$$

where

y = a binary value representing the two classes and,

x = the input vector.

As mentioned above, there are numbers of hyperplanes that can separate these two sets of data and

the problem is to find the hyperplane with the largest margin. Suppose that all training data satisfy the following constraints:

$$w.x + b \geq +1 \text{ for } y_i = +1 \quad (3.6)$$

$$w.x + b \leq -1 \text{ for } y_i = -1 \quad (3.7)$$

where

w = the boundary
x = the input vector
b = the scalar threshold (bias).

Therefore, the decision function that can classify the data is:

$$f(y) = \text{sgn}((w.x) + b) \quad (3.8)$$

Thus, the separating hyperplane must satisfy the following constraints:

$$y_i[(w.x_i) + b] \geq 1 \quad (3.9)$$

where l = the number of training sets

The optimal hyperplane is the unique one that not only separates the data without error but also maximizes the margin. It means that it should maximize the distance between closest vectors in both classes to the hyperplane. Therefore the hyperplane that optimally separate the data into two classes can be shown to be the one that minimize the functional:

$$\varphi(w) = \frac{|w|^2}{2} \quad (3.10)$$

Therefore, the optimization problem can be formulated into an equivalent non-constraint optimization problem by introducing the Lagrange multipliers ($\alpha_I >= 0$) and a Lagrangian:

$$L(w,b,\alpha) = \frac{1}{2}\|w\|^{2-} \sum_{t=1..l} \alpha_t (y_t((w.x_t) + b) - 1) \quad (3.11)$$

The Lagrangian has to be minimized with respect to w and b by the given expressions:

$$w_0 = \sum y\alpha x \quad (3.12)$$

This expressions for w_0 is then substitute into equation (3.11) which will result in dual form of the function which has to be maximized with respect to the constraints $\alpha_I > 0$.

Maximize $w.x + b \geq +1$ (3.13)

Subject to $\alpha_I \geq 0, i = 1..l$ and $\sum \alpha_I y_i$

The hyperplane decision function can therefore be written as:

$$f(x) = sign(w_0 x + b_0) = sign(\sum y_i \alpha_i^0 (x_i.x) + b_0) \quad (3.14)$$

However, the equation (3.14) is meant for linearly separable data in SVM. In a non-linearly separable data, SVM is used to learn the decision functions by first mapping the data to some higher dimensional feature space and constructing a separating hyperplane in this space.

C. Homogeneous Ensemble Classifiers using Bagging

1) Proposed Bagged RBF and SVM Classifiers

Given a set D, of d tuples, bagging (Breiman, L. 1996a) works as follows. For iteration i (i =1, 2,…..k), a training set, D_i, of d tuples is sampled with replacement from the original set of tuples, D. The bootstrap sample, D_i, created by sampling D with replacement, from the given training data set D repeatedly. Each example in the given training set D may appear repeated times or not at all in any particular replicate training data set D_i. A classifier model, M_i, is learned for each training set, D_i. To classify an unknown tuple, X, each classifier, M_i, returns its class prediction, which counts as one vote. The bagged RBF and SVM, M^*, counts the votes and assigns the class with the most votes to X.

Algorithm: RBF and SVM ensemble classifiers using bagging

Input:

- D, a set of d tuples.
- k = 1, the number of models in the ensemble.
- Base Classifiers (Radial Basis Function, Support Vector Machine)

Output: Bagged RBF and SVM, M^*

Method:

1. for i = 1 to k do // create k models
2. Create a bootstrap sample, D_i, by sampling D with replacement, from the given training data set D repeatedly. Each example in the given training set D may appear repeated times or not at all in any particular replicate training data set D_i
3. Use D_i to derive a model, M_i;
4. Classify each example d in training data D_i and initialized the weight, W_i for the model, M_i, based on the accuracies of percentage of correctly classified example in training data D_i.
5. endfor

To use the bagged RBF and SVM models on a tuple, X:

1. if classification then
2. let each of the k models classify X and return the majority vote;
3. if prediction then
4. let each of the k models predict a value for X and return the average predicted value.

D. Heterogeneous Ensemble Classifiers using Arcing

1) Proposed RBF-SVM Hybrid System

Given a set D, of d tuples, arcing (Breiman. L, 1996) works as follows; For iteration i (i =1, 2,…..k), a training set, D_i, of d tuples is sampled with replacement from the original set of tuples, D. some of the examples from the dataset *D* will occur more than once in the training dataset D_i. The examples that did not make it into the training dataset end up forming the test dataset. Then a classifier model, M_i, is learned for each training examples *d* from training dataset D_i. A classifier model, M_i, is learned for each training set, D_i. To classify an unknown tuple, X, each classifier, M_i, returns its class prediction, which counts as one vote. The hybrid classifier (RBF-SVM), M^*, counts the votes and assigns the class with the most votes to X.

Algorithm: Hybrid RBF-SVM using Arcing Classifier

Input:

- D, a set of d tuples.
- k = 2, the number of models in the ensemble.
- Base Classifiers (Radial Basis Function, Support Vector Machine)

Output: Hybrid RBF-SVM model, M^*.

Procedure:

1. For i = 1 to k do // Create k models
2. Create a new training dataset, D_i, by sampling D with replacement. Same example from given dataset *D* may occur more than once in the training dataset D_i.
3. Use D_i to derive a model, M_i
4. Classify each example d in training data D_i and initialized the weight, W_i for the model, M_i, based on the accuracies of percentage of correctly classified example in training data D_i.
5. endfor

To use the hybrid model on a tuple, X:

1. if classification then
2. let each of the k models classify X and return the majority vote;
3. if prediction then
4. let each of the k models predict a value for X and return the average predicted value;

The basic idea in Arcing is like bagging, but some of the original tuples of D may not be included in Di, where as others may occur more than once.

IV PERFORMANCE EVALUATION MEASURES

A. Cross Validation Technique

Cross-validation (Jiawei Han and Micheline Kamber**,** 2003) sometimes called rotation estimation, is a technique for assessing how the results of a statistical analysis will generalize to an independent data set. It is mainly used in settings where the goal is prediction, and one wants to estimate how accurately a predictive model will perform in practice. 10-fold cross validation is commonly used. In stratified K-fold cross-validation, the folds are selected so that the mean response value is approximately equal in all the folds.

B. Criteria for Evaluation

The primary metric for evaluating classifier performance is classification Accuracy: the percentage of test samples that the ability of a given classifier to correctly predict the label of new or previously unseen data (i.e. tuples without class label information). Similarly, the accuracy of a predictor refers to how well a given predictor can guess the value of the predicted attribute for new or previously unseen data.

V EXPERIMRNTAL RESULTS AND DISCUSSION

A. Real dataset Description

The Acer07 dataset, being released for the first time is a real world data set collected from one of the sensors in Acer eDC (Acer e-Enabling Data Center). The data used for evaluation is the inside packets from August 31, 2007 to September 7, 2007.

B. Benchmark dataset Description

The data used in classification is NSL-KDD, which is a new dataset for the evaluation of researches in network intrusion detection system. NSL-KDD consists of selected records of the complete KDD'99 dataset (Ira Cohen, et al., 2007). NSL-KDD dataset solve the issues of KDD'99 benchmark [KDD'99 dataset]. Each NSL-KDD connection record contains 41 features (e.g., protocol type, service, and ag) and is labeled as either normal or an attack, with one specific attack type.

C. Experiments and Analysis

In this section, new ensemble classification methods are proposed for homogeneous ensemble classifiers using bagging and heterogeneous ensemble classifiers using arcing classifier and their performances are analyzed in terms of accuracy.

1) Homogeneous Ensemble Classifiers using Bagging

The Acer07 and NSL-KDD datasets are taken to evaluate the proposed Bagged RBF and bagged SVM classifiers.

a) Proposed Bagged RBF and Bagged SVM

TABLE 1. THE PERFORMANCE OF BASE AND PROPOSED BAGGED CLASSIFIERS FOR REAL DATASET

Real Dataset	Classifiers	Classification Accuracy
Acer07 dataset	RBF	99.53%
	Proposed Bagged RBF	99.86%
	SVM	99.80%
	Proposed Bagged SVM	99.93%

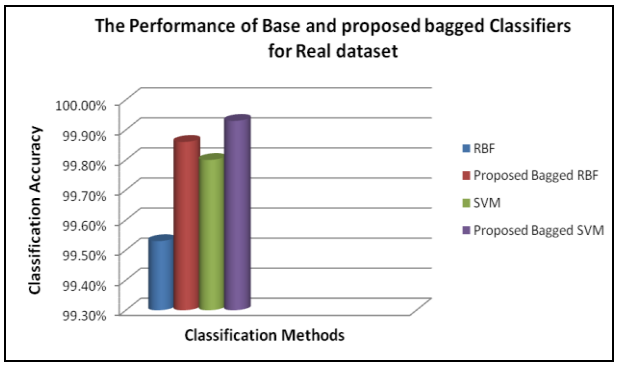

Figure 1. Classification Accuracy of Base and Proposed Bagged Classifiers Using Real dataset

TABLE 2. THE PERFORMANCE OF BASE AND PROPOSED BAGGED CLASSIFIERS FOR BENCHMARK DATASET

Benchmark Dataset	Classifiers	Classification Accuracy
NSL-KDD dataset	RBF	84.74%
	Proposed Bagged RBF	86.40%
	SVM	91.81%
	Proposed Bagged SVM	93.92%

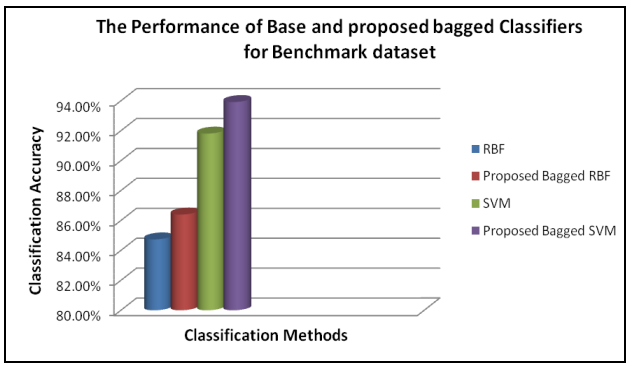

Figure 2. Classification Accuracy of Base and Proposed Bagged Classifiers Using Benchmark Dataset

In this research work, new ensemble classification methods are proposed for homogeneous ensemble classifiers using bagging and their performances are analyzed in terms of accuracy. Here, the base classifiers are constructed using radial basis function and Support Vector Machine. 10-fold cross validation (Kohavi, R, 1995) technique is applied to the base classifiers and evaluated Classification accuracy. Bagging is performed with radial basis function classifier and support vector machine to obtain a very good classification performance. Table 1 and 2 show classification performance for real and benchmark datasets of intrusion detection using existing and proposed bagged radial basis function neural network and support vector machine. The analysis of results shows that the proposed bagged radial basis function and bagged support vector machine classifies are shown to be superior to individual approaches for real and benchmark datasets of intrusion detection problem in terms of classification accuracy. According to figure 1 and 2 proposed combined models show significantly larger improvement of Classification accuracy than the base classifiers. This means that the combined methods are more accurate than the individual methods in the field of intrusion detection.

2) Heterogeneous Ensemble Classifiers using Arcing

The Acer07 and NSL-KDD datasets are taken to evaluate the proposed hybrid RBF-SVM classifiers.

a) Proposed Hybrid RBF-SVM System

TABLE 3. THE PERFORMANCE OF BASE AND PROPOSED HYBRID RBF-SVM CLASSIFIERS FOR REAL DATASET

Real Dataset	Classifiers	Classification Accuracy
Acer07 dataset	RBF	99.40%
	SVM	99.60%
	Proposed Hybrid RBF-SVM	99.90%

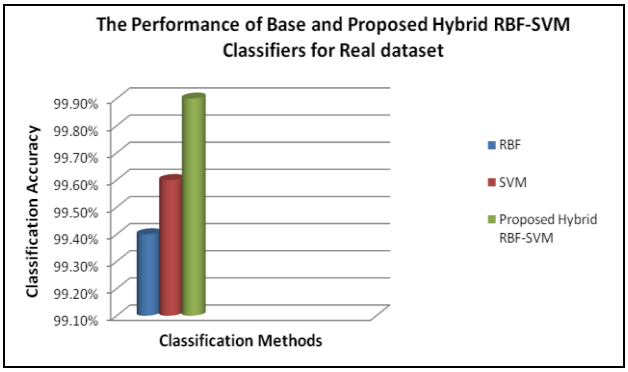

Figure 3. Classification Accuracy of Base and Proposed Hybrid RBF-SVM Classifiers Using Real Dataset

TABLE 4. THE PERFORMANCE OF BASE AND PROPOSED HYBRID RBF-SVM CLASSIFIER FOR BENCHMARK DATASET

Benchmark Dataset	Classifiers	Classification Accuracy
NSL-KDD dataset	RBF	84.74%
	SVM	91.81%
	Proposed Hybrid RBF-SVM	98.46%

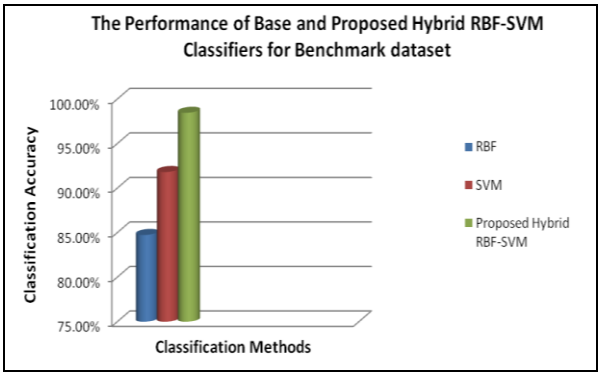

Figure 4. Classification Accuracy of Base and Proposed Hybrid RBF-SVM Classifiers Using Benchmark Dataset

In this research work, new hybrid classification methods are proposed for heterogeneous ensemble classifiers using arcing classifier and their performances are analyzed in terms of accuracy. The data set described in section 5 is being used to test the performance of base classifiers and hybrid classifier. Classification accuracy was evaluated using 10-fold cross validation. In the proposed approach, first the base classifiers RBF and SVM are constructed individually to obtain a very good generalization performance. Secondly, the ensemble of RBF and SVM is designed. In the ensemble approach, the final output is decided as follows: base classifier's output is given a weight (0–1 scale) depending on the generalization performance as given in Table 3 and 4. According to figure 3 and 4, the proposed hybrid models show significantly larger improvement of classification accuracy than the base classifiers and the results are found to be statistically significant.

The experimental results show that proposed hybrid RBF-SVM is superior to individual approaches for intrusion detection problem in terms of classification accuracy.

VI CONCLUSIONS

In this research work, new combined classification methods are proposed for homogeneous ensemble classifiers using bagging and the performance comparisons have been demonstrated using real and benchmark dataset of intrusion detection in terms of accuracy. Here, the proposed bagged radial basis function and bagged support vector machine combines the complementary features of the base classifiers. Similarly, new hybrid RBF-SVM models are designed in heterogeneous ensemble classifiers involving RBF and SVM models as base classifiers and their performances are analyzed in terms of accuracy.

The experiment results lead to the following observations.

- SVM exhibits better performance than RBF in the important respects of accuracy.
- The proposed bagged methods are shown to be significantly higher improvement of classification accuracy than the base classifiers.
- The hybrid RBF-SVM shows higher percentage of classification accuracy than the base classifiers.
- The χ^2 statistic is determined for all the above approaches and their critical value is found to be less than 0.455. Hence corresponding probability is $p < 0.5$. This is smaller than the conventionally accepted significance level of 0.05 or 5%. Thus examining a χ^2 significance table, it is found that this value is significant with a degree of freedom of 1. In general, the result of χ^2 statistic analysis shows that the proposed classifiers are significant at $p < 0.05$ than the existing classifiers.
- The accuracy of base classifiers is compared with homogeneous and heterogeneous models for data mining problems and heterogeneous models exhibit better results than homogeneous models for real and benchmark data sets of intrusion detection.
- The intrusion detection dataset could be detected with high accuracy for homogeneous and heterogeneous models.

The future research will be directed towards developing more accurate base classifiers particularly for the intrusion detection problem.

ACKNOWLEDGMENT

Author gratefully acknowledges the authorities of Annamalai University for the facilities offered and encouragement to carry out this work.

REFERENCES

[1] P. Anderson, "Computer security threat monitoring and surveillance", Technical Report, James P. Anderson Co., Fort Washington, PA, 1980.

[2] E. Biermann, E. Cloete and L.M. Venter, "A comparison of intrusion detection Systems", Computer and Security, vol. 20, pp. 676-683, 2001.

[3] Breiman. L, "Bias, Variance, and Arcing Classifiers", Technical Report 460, Department of Statistics, University of California, Berkeley, CA, 1996.

[4] Breiman, L. "Bagging predictors", Machine Learning, vol.24, no. 2, pp. 123– 140, 1996a

[5] Burges, C. J. C, "A tutorial on support vector machines for pattern recognition", Data Mining and Knowledge Discovery, vol. 2, no. 2, pp. 121-167, 1998.

[6] W. H. Chen, S. H. Hsu, H.P Shen, "Application of SVM and ANN for intrusion detection", Comput OperRes Vol-ume 32, Issue 10, pp. 2617–2634, 2005a.

[7] Chen Y, Abraham A, and Yang J, "Feature deduction and intrusion detection using flexible neural trees", In: Second IEEE International Symposium on Neural Networks, 2005b, pp. 2617-2634.

[8] C. Katar, "Combining multiple techniques for intrusion detection", Int J Comput Sci Network Security, pp. 208–218, 2006.

[9] Cherkassky, V. and Mulier, F, "Learning from Data - Concepts, Theory and Methods", John Wiley & Sons, New York, 1998.

[10] Freund, Y. and Schapire, R, "A decision-theoretic generalization of on-line learning and an application to boosting", In proceedings of the Second European Conference on Computational Learning Theory, 1995, pp 23-37.

[11] Freund, Y. and Schapire, R, "Experiments with a new boosting algorithm", In Proceedings of the

Thirteenth International Conference on Machine Learning, 1996, pp. 148-156 Bari, Italy.

[12] Ghosh AK, Schwartzbard A, "A study in using neural networks for anomaly and misuse detection", In: The proceeding on the 8th USENIX security symposium, <http://citeseer.ist.psu.edu/context/1170861/0>; [accessed August 2006], 1999.

[13] M.Govindarajan, RM.Chandrasekaran, "Intrusion Detection using an Ensemble of Classification Methods", In Proceedings of International Conference on Machine Learning and Data Analysis, San Francisco, U.S.A, 2012, pp. 459-464.

[14] Haykin, S, "Neural networks: a comprehensive foundation" (second ed.), New Jersey: Prentice Hall, 1999.

[15] Heady R, Luger G, Maccabe A, Servilla M, "The architecture of a network level intrusion detection system", Technical Report, Department of Computer Science, University of New Mexico, 1990.

[16] K. Ilgun, R.A. Kemmerer and P.A. Porras, "State transition analysis:A rule-based intrusion detection approach", IEEE Trans. Software Eng. vol. 21, pp. 181-199, 1995.

[17] Ira Cohen, Qi Tian, Xiang Sean Zhou and Thoms S.Huang, "Feature Selection Using Principal Feature Analysis", In Proceedings of the 15th international conference on Multimedia, Augsburg, Germany, September, 2007, pp. 25-29.

[18] Jiawei Han , Micheline Kamber, " Data Mining – Concepts and Techniques" Elsevier Publications, 2003.

[19] Kohavi, R, "A study of cross-validation and bootstrap for accuracy estimation and model selection", Proceedings of International Joint Conference on Artificial Intelligence, 1995, pp. 1137–1143.

[20] KDD'99 dataset, http://kdd.ics.uci.edu/databases, Irvine, CA, USA, 2010.

[21] E. Lundin and E. Jonsson, "Anomaly-based intrusion detection: privacy concerns and other problems", Computer Networks, vol. 34, pp. 623-640, 2002.

[22] D. Marchette, "A statistical method for profiling network traffic", In proceedings of the First USENIX Workshop on Intrusion Detection and Network Monitoring (Santa Clara), CA.1999, pp. 119-128.

[23] Mukkamala S, Sung AH, Abraham A, "Intrusion detection using ensemble of soft computing paradigms", third international conference on intelligent systems design and applications, intelligent systems design and applications, advances in soft computing. Germany: Springer, 2003, pp. 239–48.

[24] Mukkamala S, Sung AH, Abraham A, "Modeling intrusion detection systems using linear genetic programming approach", The 17th international conference on industrial & engineering applications of artificial intelligence and expert systems, innovations in applied artificial intelligence. In: Robert O., Chunsheng Y., Moonis A., editors. Lecture Notes in Computer Science, vol. 3029. Germany: Springer, 2004a, pp. 633–42.

[25] Mukkamala S, Sung AH, Abraham A, Ramos V, "Intrusion detection systems using adaptive regression splines", In: Seruca I, Filipe J, Hammoudi S, Cordeiro J, editors, Proceedings of the 6th international conference on enterprise information systems, ICEIS'04, vol. 3, Portugal, 2004b, pp. 26–33.

[26] S. Mukkamala, G. Janoski and A.Sung, "Intrusion detection: support vector machines and neural networks", In proceedings of the IEEE International Joint Conference on Neural Networks (ANNIE), St. Louis, MO, 2002, pp. 1702-1707.

[27] Oliver Buchtala, Manuel Klimek, and Bernhard Sick, Member, IEEE, "Evolutionary Optimization of Radial Basis Function Classifiers for Data Mining Applications", IEEE Transactions on systems, man, and cybernetics—part b: cybernetics, vol. 35, no. 5, 2005.

[28] Shah K, Dave N, Chavan S, Mukherjee S, Abraham A, Sanyal S, "Adaptive neuro-fuzzy intrusion detection system", IEEE International Conference on Information Technology: Coding and Computing (ITCC'04), vol. 1. USA: IEEE Computer Society, 2004, pp. 70–74.

[29] T. Shon and J. Moon, "A hybrid machine learning approach to network anomaly detection", Information Sciences, vol.177, pp. 3799-3821, 2007.

[30] Summers RC, "Secure computing: threats and safeguards", New York: McGraw-Hill, 1997.

[31] Sundaram A, "An introduction to intrusion detection", ACM Cross Roads, vol.2, no.4, 1996.

[32] W. Stallings, "Cryptography and network security principles and practices", USA: Prentice Hall, 2006.

[33] C. Tsai, Y. Hsu, C. Lin and W. Lin, "Intrusion detection by machine learning: A review", Expert Systems with Applications, vol. 36, pp.11994-12000, 2009.

[34] Vanajakshi, L. and Rilett, L.R, "A Comparison of the Performance of Artificial Neural Network and Support Vector Machines for the Prediction of Traffic Speed", IEEE Intelligent Vehicles Symposium, University of Parma, Parma, Italy: IEEE, 2004, pp.194-199.

[35] T. Verwoerd and R. Hunt, "Intrusion detection techniques and approaches", Computer Communications, vol. 25, pp.1356-1365, 2002.

[36] S. Wu and W. Banzhaf, "The use of computational intelligence in intrusion detection systems: A review", Applied Soft Computing, vol.10, pp. 1-35, 2010.

M.Govindarajan received the B.E and M.E and Ph.D Degree in Computer Science and Engineering from Annamalai University, Tamil Nadu, India in 2001 and 2005 and 2010 respectively. He did his post-doctoral research in the Department of Computing, Faculty of Engineering and Physical Sciences, University of Surrey, Guildford, Surrey, United Kingdom in 2011 and pursuing Doctor of Science at Utkal University, orissa, India. He is currently an Assistant Professor at the Department of Computer Science and Engineering, Annamalai University, Tamil Nadu, India. He has presented and published more than 75 papers at Conferences and Journals and also received best paper awards. He has delivered invited talks at various national and international conferences. His current Research Interests include Data Mining and its applications, Web Mining, Text Mining, and Sentiment Mining. He was the recipient of the Achievement Award for the field and to the Conference Bio-Engineering, Computer science, Knowledge Mining (2006), Prague, Czech Republic, Career Award for Young Teachers (2006), All India Council for Technical Education, New Delhi, India and Young Scientist International Travel Award (2012), Department of Science and Technology, Government of India New Delhi. He is Young Scientists awardee under Fast Track Scheme (2013), Department of Science and Technology, Government of India, New Delhi and also granted Young Scientist Fellowship (2013)**,** Tamil Nadu State Council for Science and Technology, Government of Tamil Nadu, Chennai. He has visited countries like Czech Republic, Austria, Thailand, United Kingdom, Malaysia, U.S.A, and Singapore. He is an active Member of various professional bodies and Editorial Board Member of various conferences and journals.

How to cite this paper: M.Govindarajan,"Hybrid Intrusion Detection Using Ensemble of Classification Methods", IJCNIS, vol.6, no.2, pp.45-53, 2014. DOI: 10.5815/ijcnis.2014.02.07

