International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 3 (2015) pp. 7109-7124

http://www.ripublication.com

Democracy Inspired Computer Network Intrusion Detection System Using Ensemble of Decision Tree Classifiers

Chandrashekhar Azad [1], Vijay Kumar Jha [2]

[1, 2]Department of Computer Science and Engineering, Birla Institute of Technology Mesra, Ranchi-835215(India)
[1] csazad@bitmesra.ac.in, [2] vkjha@ bitmesra.ac.in

Abstract

The purpose of this research paper is to develop a classification model for classification of intrusion in computer network, which is inspired from the concept of democracy. In this paper for measuring the effectiveness of the proposed model we used NSL KDDCUP dataset. In proposed prediction model, five decision tree classifiers are used to trained advanced system. In experiment, we applied K –fold cross validation technique for true prediction so that each record is used for training as well as testing. The main reason behind using K–fold cross validation in this model is, for unbiased classification. This proposed democracy inspired intrusion detection model provides a better result in comparison to the standalone classifier and the existing systems. The different performance parameters are used for evaluation are classification accuracy, classification error, Kappa, root relative squared error, mean absolute error, root mean squared error and relative absolute error.

Keyword: Data mining, Anomaly Detection, Misuse detection, Decision Stump, Random Forest, LAD Tree, LMT, AD Tree.

I. INTRODUCTION

Today in the era of development of smart devices in various fields like communication, transportation, retailing, manufacturing and finance etc. the usual expenditure of the Internet is not a big issue for users. It's because today the people fulfilling their need

and wants through Internet. Today the World Wide Web became the main stream for the people to do work or being socialized as a human being and due to effect of these lifestyle people became the technology dependent and it increases the transfer of private data through Internet exponentially. Due to this, Computer Network security is the important matter for every individual who connected through it either they are public organization or private organization or individuals. Computer security is devoted to the protection of computing devices and services that violate the integrity, reliability, availability and confidentiality of the data and resources in it. Intrusion detection is the way to provide security to computing resources, today there exists some methods such as firewall, antivirus etc. for Intrusion detection and prevention but they have high false alarm rate or they are not 100% secured, so there is a requirement of system which have the low false alarm rate. In other words, we can say that there is a need to improve the performance of the system or development of the new system which is better in comparison to the existing system. Today Data mining methods such as classification, clustering, association mining, outlier detection etc. [1, 2] moving towards to Intrusion detection and prevention. Data mining has the capability to identify the hidden pattern in the large volume of data which are previously unknown. Traditional computer security systems are cope with the large volume of data and the manual analysis of the large volume of the network data, is impossible it's because today the size of the data increases exponentially and the approx. 40% of the total population of the world using the Internet for fulfilling their need and wants [3]. Data mining also has the capability to learn from the experience, that is the learning from the previous data which is labeled or unlabeled. Here in the 21st century when the digital data increases exponentially in this concerned data mining in the network security are the solution to the all the inherent problem in the security. The data mining based application may give the best alternative in the intrusion detection and prevention. The data mining based Intrusion detection and prevention may serve as an alternative to protect network resources in the World Wide Web. The aim of the data mining based intrusion detection system is to do protection, detection, prevention and action to malicious activities on computer network. Several solutions are emerged for computer network security day by day which provides security at both host and network level. The traditional solutions like firewall, antivirus, spyware and other authentication system provide security to some extends but they are still facing the challenges of network attacks. Some interesting solutions are emerged like Intrusion Detection and Prevention Systems, but these too have so many problems like detecting and responding in real time & discovering novel attacks that's why Intrusion detection field attracted for research and development [4]. Machine learning[2] techniques like Neural Network[5], Fuzzy Logic [6], Rough Set[7] and Support Vector Machine[8] etc. based techniques are proposed for making intelligent intrusion detection System. Recent development in the field of IDS and development in the field of information and communication technology shows, securing the network with the help of a single technique is insufficient, as it is difficult to cope

with different kind of network vulnerabilities, there is a demand, to combine different security technologies under a full secure system that combines the strength of many theoretical and technological domains under a fully secured system, they combines the strength or power of these technologies domain & thus eventually provide a solid multifaceted system well against intrusion attempt. Data mining is the computational process of discovering hidden patterns in large data sets. It is the intersection of machine learning, artificial intelligence, database systems statistics etc. The main goal of the data mining process is to extract previously unknown useful facts from the data set and then transform found information into a well understandable structure for further use. Data mining involves data pre-processing, cleaning, integration, selection, transformation, pattern mining, evaluation and presentation.

2. RELATED WORK

In [9] authors proposed an algorithm with feature selection and decision rules based anomaly intrusion detection. In [10] hybrid intelligent system is proposed which is based on the concept of multi classifiers. In [11] an intrusion detection system is designed to classify by the incorporation of enhanced rules as learnt from the network behavior. In [12] A Novel Multi-classifier layered Approach is used to improve the minority attack detection in IDS. In [13] Decision tree based lightweight intrusion detection using a wrapper approach is proposed. In [14] authors Designed a multiple-level hybrid classifier for intrusion detection system using Bayesian clustering and decision trees is proposed. In [15] A Novel Intrusion Detection Method Based on Principle Component Analysis is proposed. In [16] an efficient intrusion detection system based on support vector machines and gradually feature removal method has proposed. In [17] swarm optimization (SSO) based a hybrid network intrusion detection system is proposed. In [18] An Intrusion-Detection Model Based on Fuzzy Class-Association-Rule Mining Using Genetic Network Programming. In [19] Intrusion Detection using Naive Bayes Classifier with Feature Reduction is proposed. An improved network intrusion detection technique based on k-Means clustering via naive Bayes classification [20].In most of the literature the intrusion detection systems are based on the single classifier and the classifier predict network traffic as a normal or attack then the system will alarm to the administrator. In the societal environment the decision on which majority of the people are agreed are acceptable and the decisions are always true that is the democracy. So, decision on the network traffic is whether normal or attack by the multi classifiers is given preferences against the single classifiers system. In this paper democracy inspired intrusion detection system is proposed.

3. INTRUSION DETECTION SYSTEM

Intrusion is a set of actions that attempt to break the integrity, availability or confidentiality of data on a technological platform. An intrusion detection system is the software, hardware or both that detects intrusions on the network. Intrusion detection system can monitor all the network activities and hence can detect the signs of known or unknown attacks depend on the type of intrusion detection system has been used. The main objective of IDS is to alarm the system administrator, if any suspicious activity is happening. Intrusion detection techniques are classified under two categories: anomaly detection and Signature detection. Anomaly detection refers to detecting patterns in a given network dataset that do not confirm to an established normal behavior and the pattern that are detected are called anomalies and are often translated into an actionable information in several domains. Anomalies are also referred to as outliers, change, deviation, surprise intrusion etc. In misuse detection, the IDS analyzes the information gathered and compare it to large network traffic attack signatures, IDS look for a particular attack that already been documented as an attack signature, Like detection system. So we can say that the misuse detection software is a database of attack signatures that IDS uses to attack in World Wide Web [4, 21].

4. DATA MINING AND CLASSIFICATION

4.1. Alternating decision tree (ADT)

An alternating decision tree is a machine learning method for classification. It generalizes decision trees and has connections to boosting. An alternating decision tree consists of decision nodes and prediction nodes. Decision nodes specify a predicate condition. Prediction nodes contain a single number. ADTrees always have prediction nodes as both root and leaves. An instance is classified by an AD Tree by following all paths for which all decision nodes are true and summing any prediction nodes that are traversed. This is different from binary classification trees such as CART (classification and regression tree) or C4.5 in which an instance follows only one path through the tree [22].

4.2. LAD Tree(LADT)

Class for generating a multi-class alternating decision tree using the LogitBoost strategy. The alternating decision tree (AD tree) is a successful classification technique that combines decision trees with the predictive accuracy of boosting into a set of interpretable classification rules. The original formulation of the tree induction algorithm restricted attention to binary classification problems, LAD tree overcomes this drawback. Seeking a more natural solution authors then adapt the multi class LogitBoost and AdaBoost [23].

4.3. Decision Stumps(DS)

A decision stump is a machine learning model consisting of a one-level decision tree. That is, it is a decision tree with one internal node (the root) which is immediately connected to the terminal nodes (its leaves). Decision stump makes a prediction based on the value of just a single input feature. Sometimes they are known as 1-rules.Depending on the type of the input feature, several variations are possible. For nominal features, one may build a decision stump which contains a leaf for eachpossiblefeature valueora decision stump with the two leaves, oneof whichcorresponds to some chosen category, and the other leaf to all the other categories. For binary features, these two schemes are identical. A missing value may be regarded as a yet another category [24].

4.4. Logistic model tree (LMT)

Logistic model tree (LMT) is a classification model with an associated supervised training algorithm that combines logistic regression (LR) and decision tree learning. Logistic model trees are based on the earlier idea of a model tree: a decision tree that has linear regression models at its leaves to provide a piecewise linear regression model (where ordinary decision trees with constants at their leaves would produce a piecewise constant model). In the logistic variant, the LogitBoost algorithm is used to produce an LR model at every node in the tree; the node is then split using the C4.5 criterion. Each LogitBoost invocation is warm-started from its results in the parent node. Finally, the tree is pruned [25].

4.5. Random Forest(RF)

Random forests are an ensemble learning method for classification (and regression) that operate by constructing a multitude of decision trees at training time and outputting the class that is the mode of the classes output by individual trees. Random Forests grows many classification trees. To classify a new object from an input vector, put the input vector down each of the trees in the forest. Each tree gives a classification, and we say the tree "votes" for that class. The forest chooses the classification having the most votes (over all the trees in the forest) [26].

5. Proposed Prediction Model:

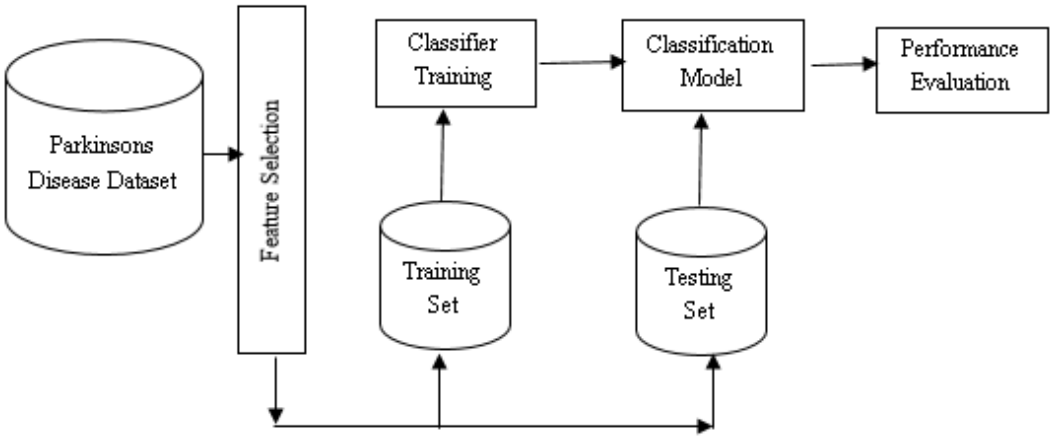

Figure 1. Base architecture of the proposed intrusion detection system

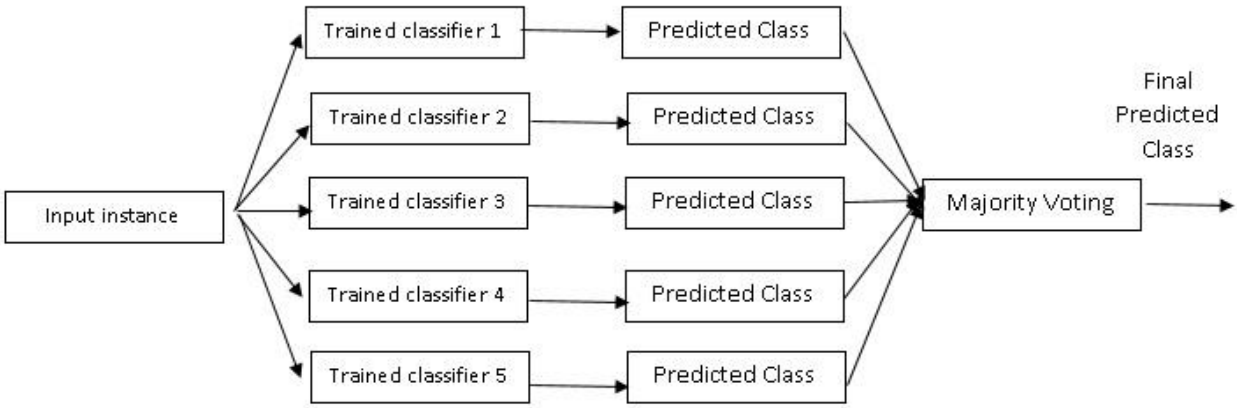

Figure 2. Detailed systemarchitecture of the democracy inspiration

The proposed intrusion detection model is inspired from the concept of democracy system. In this the n number of voters cast vote to the m numbers of the candidates. Candidate who got the highest numbers of vote in the election process is selected as the winner. In the democracy based system each and every voters have the equal weight to cast the vote. In other words we can say that the democracy best system have the majority voting system. This concept is here we applied for intrusion detection system. In today's era security of the data and services in the World Wide Web is very important

task because a lot of finance is being invested in this area and the data and services are important assets for individuals and or the organizations.So there is a requirement of the robust security system which provide the high detection rate and the low false alarm rate. So in this paper we proposed a democracy inspired intrusion detection system to protect the data and services in the computer network environment. Main motivation for this research work is the most famous proverb "Two heads are better than one". Because in the societal environment things those who support majority of the people are always true, so we think about this real world concept for the security of data and services in the computer network. In this democracy based system the traffic is considered normal or attack who have the highest number of vote cast by the different classifiers. Here the classifiers are voters and the network attack type are the candidates. Figure 1 shows the base architecture of the proposed system and the figure 2 shows the detailed architecture of the democracy inspiration.

5.1. Steps in Prediction Process:

Step 1: Start
Step 2: Load data set
Step 3: Model Creation using Training set
Step 4: Testing Model using validation set
Step 5: Performance analysis
Step 6: Selection of best Model
Step 7: Stop

In machine learning or data mining, an ensemble methods uses multiple learning algorithms to obtain better predictive performance than could be obtained from any of the constituent learning algorithms.An ensemble-based system, also known as multiple-classifier system (MCS), predicts by combining several diverse classifiers [27, 28] . Diversity may be achieved by using entirely different set of classifiers and also by using a different training data set for each classifier. The idea is that each ensemble member will generate a different decision boundary and make a different error, and suitable combination of classifiers will reduce the total error. Class labels generated by individual classifiers are combined using majority voting, and the class label chosen by most classifiers is the final ensemble decision. Our ensemble based prediction model for intrusion detection is constructed with the help of Random Forest, LAD Tree, LMT, Decision Stump, and AD Tree classifiers.

6. DATASET

KDD'99 is the mostly used data set for the anomaly detection methods, in contains around 2 million records in test data and approximately 4,900,000 records in training dataset, each of which contains 41 features and one decision attribute or class attribute. In NSL-KDD data set some of the inherent problems of the KDD'99 data set are resolved.

NSL KDD cup dataset does not contain duplicate records in the train set and test set. To test our IDS system we used the NSL KDD Intrusion Detection Evaluation dataset, in our experiments we used the 24999 randomly chosen records from NSL KDD dataset [29].

Attribute	**Description**	**Type**
duration	duration (number of seconds) of the connection	numeric
protocol_type	type of the protocol, e.g. tcp, udp, etc.	Nominal
service	Network service on the destination, e.g. http, telnet, etc.	Numeric
src_bytes	number of data bytes from source to destination	Numeric
dst_bytes	number of data bytes from destination to source	Numeric
flag	Normal or error flag status of the connection	Nominal
land	1 if connection is from/to the same host/port; 0 otherwise	Numeric
wrong_fragment	number of ``wrong'' fragments	Numeric
urgent	number of urgent packets	Numeric
hot	number of ``hot'' indicators	Numeric
num_failed_logins	number of failed login attempts	Numeric
logged_in	1 if successfully logged in; 0 otherwise	Numeric
num_compromised	number of ``compromised'' conditions	Numeric
root_shell	1 if root shell is obtained; 0 otherwise	Numeric
su_attempted	1 if ``su root'' command attempted; 0 otherwise	Numeric
num_root	number of ``root'' accesses	Numeric
num_file_creations	number of file creation operations	Numeric
num_shells	number of logins of normal users	Numeric
num_access_files	number of operations on access control files	Numeric
num_outbound_cmds	number of outbound commands in an ftp session	Numeric
is_host_login	1 if the login belongs to the ``hot'' list; 0 otherwise	Numeric
is_guest_login	1 if the login is a ``guest''login; 0 otherwise	Numeric
count	number of connections to the same host as the current connection in the past two seconds	Numeric
srv_count	sum of connections to the same destination	Numeric

	port number	
serror_rate	% of connections that have ``SYN'' errors	Numeric
rerror_rate	% of connections that have ``REJ'' errors	Numeric
same_srv_rate	% of connections to the same service	Numeric
diff_srv_rate	% of connections to different services	Numeric
srv_serror_rate	% of connections that have ``SYN'' errors	Numeric
srv_rerror_rate	% of connections that have ``REJ'' errors	Numeric
srv_diff_host_rate	% of connections to different hosts	Numeric
dst_host_count	sum of connections to the same destination IP address	Numeric
dst_host_srv_count	sum of connections to the same destination port number	Numeric
dst_host_same_srv_rate	% of connections that were to the same service, amongthe connections aggregated in dst_host_count	Numeric
dst_host_diff_srv_rate	% of connections that were to different services, amongthe connections aggregated in dst_host_count	Numeric
dst_host_same_src_port_rate	% of connections that were to the same source port,among the connections aggregated in dst_host_srv_count	Numeric
dst_host_srv_diff_host_rate	% of connections that were to different destination machines, among the connections aggregated in dst_host_srv_count	Numeric
dst_host_serror_rate	% of connections that have activated the flag s0, s1, s2or s3, among the connections aggregated in dst_host_count	Numeric
dst_host_srv_serror_rate	% of connections that have activated the flag s0, s1, s2 ors3, among the connections aggregated in dst_host_srv_count	Numeric
dst_host_rerror_rate	% of connections that have activated the flag REJ,among the connections aggregated in dst_host_count	Numeric
dst_host_srv_rerror_rate	% of connections that have activated the flag REJ,among the connections aggregated in dst_host_srv_count	Numeric
class	Type of attacks	Nominal

Table 1: Dataset Description

7. RESULTS AND DISCUSSION

This section we describe our experimental result, Experiment is carried out using rapid miner on environment of Intel i5 3rd generation processor, 4 GB RAM, 500 GB hard disk, Windows 7 ultimate operating system. In our study, ensembles of decision tree classifiers based system is used to classify the network traffic iswhether normal or attack. In the process of classification or prediction of normal or attack we took NSL KDD dataset, which is improved version of KDD CUP 99 dataset. Here we used 10 – Fold cross validation technique to complete our experiment, reason behind choosing 10 fold cross validation for training & testing the effectiveness of proposed intrusion detection model is for unbiased predication. In k – fold(Here 10-fold) cross validation technique entire dataset is divided into k parts and K-1 parts are used for training and K^{th} part is taken as testing set , this process is repeating k times so that each part is taken as testing set.

7.1. Performance measures

- Mean Absolute Error (MAE): It can define as statistical measure of how far an estimate from actual values i.e. the average of the absolute magnitude of the individual errors. It is usually similar in magnitude but slightly smaller than the root mean squared error.
- Root Mean-Squared Error (RMSE): The root mean square error (RMSE)) calculates the differences between values predicted by a model / an estimator and the values actually observed from the thing being modeled/ estimated. RMSE is used to measure the accuracy. It is ideal if it is small.
- Correctly Classified Instances(Accuracy): Total Number of instance correctly classified by the model**.**
- Incorrectly Classified Instances(CE): Total Number of instance incorrectly classified by the model.
- Kappa Statistic: Kappa statistic defined as measure agreement of predication with true class. It can be defined as :

$$K = (P(A) - P(E))/ (1 - P(E))$$

Where P (A) is the percentage agreement i.e. between classifier and ground truth, P (E) is the chance agreement. K=1 indicates perfect agreement, K=0 indicates chance agreement. The value greater than 0 means classifier is doing better. Higher the kappa statistic value betters the classifier result.

7.2. K folds Cross validation:

K-fold cross validation technique divide the whole dataset into k subsets and training and testing method is repeat k times. In each iteration training and testing one of the subset out of the k subset is used as a testing set and the remaining k-1 subsets are used as a training set. After the K iteration the average accuracy and error across all k iteration is calculated. Advantage of using this method is, in this instance gets once in test set and k-1 times in training set.

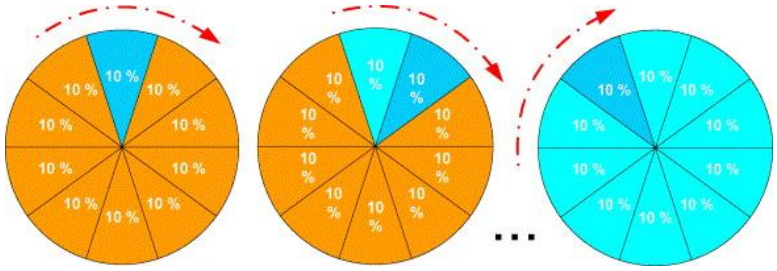

Figure. 3. K-fold Cross Validation

7.3. Results

Parameters	Result
Accuracy	99.9016
Classification error	0.09840
Kappa statistic	0.99750
Mean absolute error	0.00100
Root mean squared error	0.03140
Relative absolute error	0.24580
Root relative squared error	7.0116 0

Table 2: Classification Result of DIIDS

Model	Class	TP Rate	FP Rate	Precision	Recall	F-Measure
Proposed	**normal**	0.999	0.001	0.997	0.999	0.998
	anomaly	0.999	0.001	1.000	0.999	0.999
	Average	0.999	0.001	0.999	0.999	0.999
DS	**normal**	0.931	0.088	0.924	0.931	0.927
	anomaly	0.912	0.069	0.92	0.912	0.916
	Average	0.922	0.079	0.922	0.922	0.922
LAD	**normal**	0.987	0.035	0.97	0.987	0.979
	anomaly	0.965	0.013	0.985	0.965	0.975
	Average	0.977	0.024	0.977	0.977	0.977

RF	**normal**	0.999	0.006	0.995	0.999	0.997
	anomaly	0.994	0.001	0.999	0.994	0.997
	Average	0.997	0.003	0.997	0.997	0.997
LMT	**normal**	0.997	0.004	0.997	0.997	0.997
	anomaly	0.996	0.003	0.997	0.996	0.997
	Average	0.997	0.003	0.997	0.997	0.997
ADT	**normal**	0.992	0.031	0.974	0.992	0.983
	anomaly	0.969	0.008	0.99	0.969	0.98
	Average	0.981	0.02	0.982	0.981	0.981

Table 3: Comparison of proposed model with base classifiers by class

Fold	**Accuracy**	**Error**	**Kappa**	**MAE**	**RMSE**	**RAE**	**RRSE**
1	99.8907	0.1093	0.9973	0.0011	0.0331	0.2731	7.3913
2	100.0000	0.0000	1.0000	0.0000	0.0000	0.0000	0.0000
3	100.0000	0.0000	1.0000	0.0000	0.0000	0.0000	0.0000
4	99.8907	0.1093	0.9973	0.0011	0.0331	0.2731	7.3913
5	99.8907	0.1093	0.9973	0.0011	0.0331	0.2731	7.3913
6	99.6721	0.3279	0.9918	0.0033	0.0573	0.8192	12.8021
7	100.0000	0.0000	1.0000	0.0000	0.0000	0.0000	0.0000
8	100.0000	0.0000	1.0000	0.0000	0.0000	0.0000	0.0000
9	99.7812	0.2188	0.9945	0.0022	0.0468	0.5466	10.4551
10	99.8906	0.1094	0.9973	0.0011	0.0331	0.2733	7.3929

Table 4: Fold Wise Classification result of the proposed model

Parameters	**Proposed (DIIDS)**	**DS**	**LAD**	**RF**	**LMT**	**ADT**
Accuracy	99.9016	92.2078	97.7096	99.6983	99.6745	98.1343
Classification error	00.0984	07.7922	02.2906	00.3017	00.3255	01.8657
Kappa statistic	00.9975	00.8434	00.9539	00.9939	00.9935	00.9625
MAE	00.0010	00.1437	00.0444	00.0067	00.0040	00.0627
RMSE	00.0314	00.2681	00.1319	00.0493	00.0547	00.1351
RAE	00.2458	28.8717	08.9254	01.3427	00.8046	12.5930
RRSE	07.0116	53.7352	26.4378	09.8911	10.9673	27.0843

RRSE: Root relative squared errorMAE:Mean absolute error,
RMSE: Root mean squared error, RAE: Relative absolute error

Table 5: Comparison of the DIIDS with other systems

7.4. Discussion

In our experiment for training the proposed model using the democracy inspired IDS (DIIDS) model,we first load the dataset and apply feature selection algorithm to find useful features for classification. Splitter module of the proposed model divide the whole dataset into K (here K=10 used) sets. In k-fold (here 10 fold) cross validation, the IDS dataset is partitioned into K (here K=10) equal size subsamples and a subsample is used as a testing set and the remaining K − 1 sub samples are used as training set. This process is repeated K (here K=10) times as shown in figure 3, with each of the k sub samples used exactly once as the testing data after that the mean of the K results from the k folds are combined to produce a single estimation. Table 2 shows the classification result of the proposed model. Figure 1 and the figure 2 shows the architecture of the proposed democracy inspired intrusion detection system and the figure 3 shows the concept of the k fold cross validation technique. In the K fold cross validation method each and every sample are used for training and testing. This is the very good methodology for testing the effectiveness of the any of the classification system. Table 1 shows the details of the attribute in the dataset and the type of the attribute. The dataset are the most important component for any of the prediction system. The whole systems effectiveness is depends on the quality of the training set. Here we use the NSLKDD dataset, this data set is derived from the DARPA intrusion detection dataset. Table 2 shows the classification result of the proposed intrusion detection system. Table 3 gives the detailed comparison of the proposed model with the base classifiers Random Forest, LAD Tree, LMT, Decision Stump, and AD Tree, the comparison is based on the class by class . Table 4 shows the fold wise classification result of the proposed system and finally the table 5 shows the comparative study of the proposed system with the Random Forest, LAD Tree, LMT, Decision Stump, and ADT classifiers based system. From Table 5 we can conclude that the democracy based intrusion system provide the best result. The classification accuracy of the proposed DIIDS is 99.9016 and classification error 00.0984. Results are expressed in terms of percentage. The second best model is the random forest and it have the classification accuracy 99.6983 and classification error 00.3017. The result shows that the proposed system provide approximately 100 percent detection rate.

8. CONCLUSION

In this paper we proposed a democracy inspired intrusion detection model using data mining methods, for predictions we used concept of democracy. NSL KDD dataset is used in this for training and testing the effectiveness of the proposed tree based intrusion detection system. For experiment randomly selected 24999 records are sampled from the original NSL KDD dataset, we selected 13442 normal data and 11557 anomalous records. Anamolous records are categorized in 20 different categories like normal,portsweep,Neptune,satan,ipsweep,guess_passwd,back,land, imap, nmap, pod,

smurf, ftp_write, rootkit, warezmaster, buffer_overflow, loadmodule, multihop, phf, teardrop. To test the effectiveness of the proposed model K cross fold validation method is used to for training and testing the proposed model. The mean results indicate that in terms of accuracy and classification error, Proposed model performed very well, it gave 99.9016 % accuracy and 00.0984classification error whereas the second best is the random forest and it have the classification accuracy 99.6983 and classification error 00.3017.

REFERENCES

1. Han, Jiawei, Micheline Kamber, and Jian Pei. "Data Mining: Concepts and Techniques, (The Morgan Kaufmann Series in Data Management Systems)." (2006).
2. Witten, Ian H., and Eibe Frank. Data Mining: Practical machine learning tools and techniques. Morgan Kaufmann, 2005.
3. http://www.internetworldstats.com/stats.htm
4. Azad, Chandrashekhar, and Vijay Kumar Jha. "Data Mining in Intrusion Detection: A Comparative Study of Methods, Types and Data Sets."International Journal of Information Technology and Computer Science (IJITCS) 5.8 (2013): 75.
5. Sivanandam, S. N., and S. N. Deepa. Introduction to neural networks using Matlab 6.0. Tata McGraw-Hill Education, 2006.
6. Sivanandam, S. N., Sai Sumathi, and S. N. Deepa. Introduction to fuzzy logic using MATLAB. Vol. 1. Berlin: Springer, 2007.
7. Bazan, Jan G., et al. "Rough set algorithms in classification problem." Rough set methods and applications. Physica-Verlag HD, 2000. 49-88.
8. Hsu, Chih-Wei, Chih-Chung Chang, and Chih-Jen Lin. "A practical guide to support vector classification." (2003).
9. Shih-Wei Lin, Kuo-Ching Ying, Chou-Yuan Lee, Zne-Jung Lee, An intelligent algorithm with feature selection and decision rules applied to anomaly intrusion detection, Applied Soft Computing, Volume 12, Issue 10, October 2012, Pages 3285-3290.
10. Mrutyunjaya Panda, Ajith Abraham, Manas Ranjan Patra, A Hybrid Intelligent Approach for Network Intrusion Detection, Procedia Engineering, Volume 30, 2012, Pages 1-9,
11. G. Gowrison, K. Ramar, K. Muneeswaran, T. Revathi, Minimal complexity attack classification intrusion detection system, Applied Soft Computing, Volume 13, Issue 2, February 2013, Pages 921-927.
12. Neelam Sharma, Saurabh Mukherjee, A Novel Multi-Classifier Layered Approach to Improve Minority Attack Detection in IDS, Procedia Technology, Volume 6, 2012, Pages 913-921.

13. Sindhu S. S. S., Geetha S., Kannan A., Decision tree based light weight intrusion detection using a wrapper approach, Expert Systems with Applications. 39 (2012) 129–141.
14. Xiang C., Yong P. C., Meng L. S., Design of multiple-level hybrid classifier for intrusion detection system using Bayesian clustering and decision trees, Pattern Recognition Letters .29 (2008) 918–924.
15. Wang W., Guan X., Zhang X., A Novel Intrusion Detection Method Based on Principle Component Analysis in Computer Security, Springer-Verlag Berlin Heidelberg (2004) 657–662.
16. Li Y. , Xia J., Zhang S., Yan J., Ai X., Dai K., An efficient intrusion detection system based on support vector machines and gradually feature removal method, Expert Systems with Applications .39 (2012) 424–430.
17. Chung Y. Y., Wahid N., A hybrid network intrusion detection system using simplified swarm optimization (SSO), Applied Soft Computing 12 (2012) 3014–3022.
18. Mabu S., Chen C., Lu N., Shimada K., Hirasawa K., An Intrusion-Detection Model Based on Fuzzy Class-Association-Rule Mining Using Genetic Network Programming, IEEE Transactions on systems, MAN, and Cybernetics—Part C: Applications and Reviews. 41(2011).
19. Mukherjee D. S., Sharma N. , Intrusion Detection using Naive Bayes Classifier with Feature Reduction , Procedia Technology. 4 (2012) 119 – 128.
20. Sharma S. K., Pande P., Tiwari S. K., Sisodiai M. S., An Improved Network Intrusion Detection Technique based on k-Means Clustering via Naive Bayes Classification. IEEE-International Conference on Advances in Engineering, Science and Management. (2012).
21. Azad, Chandrashekar, and Vijay Kumar Jha. "Data Mining Based Hybrid Intrusion Detection System." Indian Journal of Science and Technology 7.6 (2014): 781-789.
22. Freund, Y., Mason, L.: The alternating decision tree learning algorithm. In: Proceeding of the Sixteenth International Conference on Machine Learning, Bled, Slovenia, 124-133, 1999.
23. Geoffrey Holmes, Bernhard Pfahringer, Richard Kirkby, Eibe Frank, Mark Hall: Multiclass alternating decision trees. In: ECML, 161-172, 2001.
24. Iba, Wayne; and Langley, Pat (1992); Induction of One-Level Decision Trees, in ML92: Proceedings of the Ninth International Conference on Machine Learning, Aberdeen, Scotland, 1–3 July 1992, San Francisco, CA: Morgan Kaufmann, pp. 233–240.
25. Niels Landwehr, Mark Hall, Eibe Frank (2005). Logistic Model Trees. Machine Learning. 95(1-2):161-205.
26. Leo Breiman (2001). Random Forests. Machine Learning. 45(1):5-32.

27. Dietterich, Thomas G. "Ensemble methods in machine learning." Multiple classifier systems. Springer Berlin Heidelberg, 2000. 1-15.
28. Valentini, Giorgio, and Francesco Masulli. "Ensembles of learning machines."Neural Nets. Springer Berlin Heidelberg, 2002. 3-20.
29. http://nsl.cs.unb.ca/NSL-KDD/

Mr. Chandrashekhar Azad received his B.Sc. (Honours) in Computer Application form Ranchi University in 2007 and MCA from Ranchi University, Ranchi, Jharkhand (India) in 2011. His research interests include data mining, swarm intelligence, medical mining and web mining. At present, he is research scholar at Department of Computer Science and Engineering, Birla Institute of Technology, Mesra, Ranchi, Jharkhand (India).

Dr. Vijay Kumar Jha received his BE in Electronics from SIT Tumkur in the year 1996, M.Sc. Engineering in Electronics from MIT Muzaffarpur in the year 2007 and PhD in Information Technology in the Area of Data Mining from MIT Muzaffarpur, in the year 2011. He has been associated with Birla Institute of Technology, Mesra,and Ranchi, India since 2001, and currently, he is working as an Associate Professor in the Department of Computer Science and Engineering, Birla Institute of Technology, Mesra, Ranchi, Jharkhand (India). His research interest includes Data mining, ERP.