International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

A Hybrid Intrusion Detection System Based on C5.0 Decision Tree and One-Class SVM

Meesala Shobha Rani†* and S. Basil Xavier†

†Department of Computer Science & Engineering, Karunya University, Tamil Nadu, India

Accepted 10 May 2015, Available online 15 May 2015, **Vol.5, No.3 (June 2015)**

Abstract

Cyber security threats have become increasingly sophisticated and complex. Intrusion detection which is one of the main problems in computer security has the main goal to detect infrequent access or attacks and to protect internal networks. A new hybrid intrusion detection method combining multiple classifiers for classifying anomalous and normal activities in the computer network is presented. The misuse detection model is built based on the C5.0 Decision tree algorithm and using the information collected anomaly detection model is built which is implemented by one-class Support Vector Machine (SVM). Integration of multiple algorithms helps to get better performance. The Experimental results are performed on NSL-KDD Dataset, and it is shown that overall performance of the proposed approach is improved in terms of detection rate and low false alarms rate in comparison to the existing techniques.

Keywords: *Intrusion detection system, Misuse detection, Anomaly detection, hybrid approach, C5.0 Decision tree, One Class SVM.*

1. Introduction

The survey on 'Information Security' in India (2015) reveals that security breaches are increasing year by year. The security attack incidents is in the range of 1 million attacks every year which is in turn about 2800 attacks every day. The global estimated financial loss is about 2.7 million USD, which 34% more than in 2013.

Cyber Security is one of the major business risks. The awareness about cyber security has created a greater impact among customers, so more concentration is on the analysis of which the organization may face. The US Federal Bureau of Investigation (FBI) has notified 3000 companies who have been victims of cyber security breach. The survey of stock exchanges conducted by International Organization of Securities Commissions (IOSCO) and World Federations of Exchange Office have found that 53% of the exchanges have been affected by cyber attacks (The Global State of Information Security survey 2015).

Interconnected devices are more vulnerable to attacks. HP viewed commonly used connected devices and found 70% of serious vulnerability. Google has launched Project Zero initiative, in identifying and stopping threats (unknown code) before any of hackers can exploit by using the attacks.

A proper intrusion detection system when deployed in an organization can avoid threats and vulnerabilities. Intrusion detection is the art of detecting inappropriate, incorrect, or anomalous activity both internally and externally. Generally intrusion detection algorithms are categorized as misuse detection and anomaly detection (Gisung Kim *et al*, 2014). The misuse detection algorithm detects attacks based on the known attack signature. It is effective in detecting known attack with low errors. It cannot detect newly created attacks that do not have similar behavior to the known attacks. In contrast anomaly detection algorithm confirms the normal behavior profiles. It analyzes the current activities with the normal profiles and reporting significant deviations as intrusions. Anomaly detection algorithms can be useful for identifying new attack patterns; it is not effective as compared to the misuse detection model in terms of detection rate and low false alarm rate.

In order to solve the limitations of these two conventional intrusion detection methods, hybrid intrusion detection method that combines misuse detection method and anomaly detection method has been proposed. The hybrid intrusion detection system uses both combination of misuse detection and anomaly detection in order to achieve high detection rate and low false alarm. Both known attacks and unknown attacks can be detected by using these two models.

The paper is organized as follows: Section 2 presents the related hybrid intrusion detection methods are studied. Section 3 describes the detailed description of proposed hybrid intrusion detection and

*Corresponding author **Meesala Shobha Rani** is a Post Graduate Scholar and **S.Basil Xavier** is working as Assistant Professor

section 4 describes experimental setup and result analysis finally conclusion of the paper is given in section 5.

2. Related Work

Extensive research is being carried out for detection of misuse and anomaly model. Some of the relevant algorithms and their limitations are discussed in this section.

(Gisung Kim *et al*, 2014) presents a new hybrid intrusion detection method hierarchically integrates a misuse detection and anomaly detection in a decomposed structure. The misuse detection model is built based on C4.5 decision tree algorithm and is used to decompose the normal training data into smaller subsets. The one-class SVM is used to create anomaly detection for the decomposed region.C4.5 decision tree does not form a cluster, which can degrade the profiling ability

(Amuthan Prabakar Muniyandi *et al*, 2012) presents an anomaly detection method using K-Means+C4.5 , a method to cascade k-means clustering and the C4.5 decision tree methods. This method achieves better performance in comparison to the K-Means, ID3, Naïve Bayes, K-NN, and SVM.

(Basant Agarwal *et al*, 2012) proposed an anomaly traffic detection system based on the Entropy of network features and Support Vector Machine (SVM) are compared, then hybrid method is a combination of both Entropy and SVM is compared with individual methods. The Hybrid method outperforms the single method in terms of accuracy but it is not dynamic to decide whether it has attack or not it causes high false alarms.

(Cheng Xiang *et al*, 2008) proposed a multiple-level hybrid classifier, a novel intrusion detection system, which combines the supervised tree classifiers and unsupervised Bayesian clustering to detect intrusion. This approach provides the high detection rate and false alarm rate in comparison of Kernel miner, Three-level tree classifier, Bagged boosted C5.0 trees.

(Gang Wang *et al*, 2010) proposed a new approach called FC-ANN, based on ANN (Artificial Neural Network) and fuzzy clustering, to solve the problems in the IDS. This approach achieves better detection precision rate and detection stability in comparison to the back propagation neural network, Decision tree and Naïve Bayes.

(Hyun Joon Shin *et al* , 2005) proposed a novel test technique for machine fault detection and classification in electro-mechanical machinery from vibrating measurements using one-class Support Vector Machines (SVM).This method gives better performance in detecting outliers in comparison of multi-layered perception it is one of the artificial neural technique.

(Levent Koc *et al*, 2012) proposed an Hidden Naïve Bayes (HNB) model for the intrusion detection problems that suffers from dimensionality, high correlated features and high network data stream volumes. This method achieves overall performance in terms of accuracy, error rate and misclassification cost in comparison to the traditional Naïve Bayes model, leading extended Naïve Bayes model and the knowledge Discovery and Data mining Cup 1999 winner.

(M. Ali Aydm *et al*, 2009) proposed a hybrid IDS by integrating two approaches in one system. The hybrid IDS used combination of Packet Header Anomaly Detection (PHAD) and Network Traffic Anomaly Detection (NETAD) are added one after the other to signature based IDS namely Snort as a pre-processor. The hybrid IDS is much powerful then the signature based IDS.

(Mahsa Khoronejad *et al*, 2013) proposed a hybrid method of Hidden Markov Models and C5.0 are combined to achieve better accuracy in comparison to the HMM. The hybrid method reduce the limitations of HMM algorithm.

(Ming-yang Su. 2011) proposed a genetic weighted KNN (K-Nearest-neighbor) classifier for anomaly detection on flooding attacks and an unsupervised clustering algorithm, MLBG is applied to reducing the time expense and increasing the performance in terms of accuracy in comparison to the un-weighted KNN classifier, using a genetic algorithm.

(Mrutyunjaya Panda *et al*, 2012) proposed hybrid intelligent decision technologies using data filtering by adding supervised or unsupervised methods along with a classifier to make intelligent decisions in order to detect network attacks. This approach provides high detection rate and low false alarms.

(Neelam Sharma *et al*, 2012) proposed a novel layered approach with multi-classifier by combining Naïve Bayes classifier (NBC) and Naïve Bayes tree (NB Tree). NBC for major attack detection and NB Tree for minor attack detection. NB Tree provides better recall and precision for all four attacks, but fails to increase the detection performance of minority attacks. Single classifier is not effective in detecting minority attacks, combing of multi classifier gives better results.

(Sankar Mahadevan *et al*, 2012) proposed a new approach for fault detection and diagnosis using 1-class SVM and SVM-recursive feature elimination. This approach is based on non-linear distance metric distance metric measured in feature space. This method achieves better performances in terms of false alarm rates, detection latency and fault detection rates in comparison to the conventional techniques such as PCA and DPCA.

(Shih-Wei Lin *et al*, 2012) proposed an intelligent algorithm with feature selection and decision rules applied to anomaly intrusion detection using Support Vector Machine (SVM), Decision Tree (DT) and Simulated annealing (SA).This method achieves better accuracy in comparison to the hybrid processes of DT, SA, and feature selection, the hybrid process of particle swarm optimization (PSO), SVM and feature selection, only DT, only SVM are used to simulate the results.

(Shi-Jinn Horng *et al*, 2011) proposed an SVM-based intrusion detection system, which combines a hierarchical clustering algorithm, a simple feature

selection procedure, and the SVM technique. This approach provides better performance in terms of accuracy in comparison to the other NIDS. It only detects Dos and Probe attacks not U2L and R2L attacks.

(Siva S. Sivatha Sindhu *et al*, 2012) proposed a light weight Intrusion Detection System to detect anomalies in the network using a wrapper based feature selection algorithm that maximizes the specificity and sensitivity, adding neural ensemble decision tree to evolve better optimal features. This method increases the detection rate in comparison various six decision tree classifiers are Decision Stump, C4.5, Naïve Bayes Tree, Random Forest, Random Tree and Respective tree model.

(T. Shon *et al*, 2007) proposed a new approach called Enhanced SVM approach for detection and classification of novel attacks in networks in network traffic. This method improve better performance it uses packet profiling using SOFM, packet filtering using PTF, field selection using GA , and packet-flow based data pre-processing

(Tamer F. Ghanem *et al*, 2014) proposed a hybrid approach for anomaly detection in large scale datasets using detectors generated based on multi-start meta-heuristic method and genetic algorithm. It has taken inspiration of negative selection based detector generation. This approach shows a better accuracy in generating a suitable number of detectors compared to the other machine learning algorithms like NB (Naïve Bayes) , J48 (Decision tree), FBNN (Multilayer Feedback Neural Network), Bayes Network (BN), Bayesian Logistic Regression (BLR), Radial Basis Function Network (RBFN).

(Vahid Golmah. 2014) proposed an efficient hybrid intrusion detection method based on C5.0 and SVM. This method achieves a better performance compared to the individual SVM. Evaluate the proposed method using DARPA dataset.

(Yinhui Li *et al*, 2012) proposed an efficient feature removal method for Intrusion detection system using gradually feature removal method, combination of clustering method, ant colony algorithm and support vector machine.

3. Proposed Methodology

In this section C5.0 decision tree algorithm and one-class SVM algorithms are change to build the misuse detection and anomaly detection model respectively, are briefly discussed. Then the integration of models can be explained

3.1 C5.0 Algorithm for building misuse detection in proposed scheme

The C5.0 algorithm is the latest version of machine learning algorithms (MLAs) developed by Quinlan, based on decision tree (Information on See5/C5.0-Rule quest Research Data.see5/Mining Tools, 2011). The decision trees are built based on list of possible attributes and set of training instances, and then the tree can be classified by using subsequent set of test instances. It is a modified version of well-known and widely used C4.5 Classifier and it has several important advantages over its ancestors [Is See5/C5.0 Better Than C4.5, 2009). C5.0 supports boosting of decision trees. Boosting is a technique for generating and combining multiple classifiers to give improved final predictive accuracy. C5.0 incorporates variable misclassification costs. It allows separate cost for each predicted / actual class pairs.

C5.0 constructs classifiers to minimize estimated misclassification costs rather than the error rates. New attributes are dates, times, timestamps, ordered discrete attributes. The values can be marked as missing or not applicable for particular cases. It supports sampling and cross-validation.C5.0 models are quite robust in thepresence of problems such as missing data and large numbers of input fields. It does not require long training times to estimate. In addition, it is easier to understand than some other model types, since the rules derived from the model have a very straightforward interpretation. C5.0 have option to convert the tree to rules C5.0 tree or rule sets are usually smaller than C4.5.

Some other features of C5.0 are, the soft or fuzzy thresholding can also be specified .The Asymmetric cost can be assigned to specific types of error. The confidence factor for pruning can also be changed. An option global pruning algorithm can be turned on/off. The minimum number of nodes in the terminal node can also be adjusted (See5/C5.0 Updated Record).

3.1.1 Information Gain and Entropy

Information gain is used to decide how well an attribute separates the training data according to the target model. It is based on a measure commonly used in information theory known as entropy. The units of entropy are bits. (Neelam Sharma *et al*, 2012), (Ms Rashmi R. Tundalware *et al*, 2013)

Let T is the training sample set.
C_i is Class I; i= 1,2,…….n
$I(T_1, T_2 \ldots, Tn) = -\sum pi\ log2(pi)$
T_i is the number of samples in class i
$Pi=T_i/T$
$Log_{2\ is}$ the binary Logarithm
Let attribute F have v distinct values
Entropy= E(F) is

$$\sum\{(T1j + T2j + \cdots + Tnj)/T\} * I(T1j \ldots . Tn) \quad j=1$$

Where T_{ij} is Samples in Class i and subset j of attribute F

$$I(T1j, T2j, \ldots . Tnj) = -\sum pijlog2(pij)$$
$$Gain(F) = I(T1, T2, \ldots Tn) - E(F) \quad \text{Eq. (3.1)}$$

3.1.2 Decision Tree Based On C5.0 Classification Algorithm

Step 1- The C5.0 node generates either decision tree or a rule set.
Step 2- A C5.0 works by splitting the sample into subsample based on the field that provides maximum information gain by using Eq. (3.1)
Step 3 - The target field must be categorical .Multiple Splits into more than two subgroups are allowed.
Step 4 - Each subsample defined by the first split is then split again, based on a different field, and the process Iterated until the subsamples cannot be split any more or the partitioning tree has reached the threshold.
Step 5- Finally, the lowest-level splits are re-examined, and those that do not contribute significantly to the value of the model are removed or pruned.

Fig.1 Building Decision tree based on C5.0 Algorithm

3.2 One Class SVM for anomaly detection in proposed scheme

The One-class SVM was proposed by Scholkopf *et al*. was inspired by general SVM. One-class SVM is a famous outlier (or) novelty (or) anomaly detection algorithm in various application like machine fault detection and document classification (Hyun joon Shin *et al*, 2005). It identifies outliers among positive instances and uses them as negative instances. It is used to classify anomalous packets as outliers.

Let $x1, x2 \ldots \ldots xl \pounds X$ be the training data instances belonging to original space X *and* l be the number of instances. The 1-classSVM may be viewed as a regular binary SVM where all training data lies in the first class and the origin belongs to the second class. It discovers the maximal margin hyper plane that best separates the training data from the origin (Scholkopf *et al*., 2001). It is difficult to locate a hyper plane that creates training data patterns separable from the origin in the original space X, the SVM uses a feature map ($\phi: X \rightarrow F$) , which non-linearly transforms the data from the original space to the feature space in order to locate the hyper plane in the feature space. The 1-class SVM is formulated as the following quadratic programming.

$$\min_{w,\varepsilon,\rho} \frac{1}{2}||w||^2 + \frac{1}{vl}\sum_{i=1}^{l} \varepsilon_i - \rho \text{ Subject to } (\mathrm{w}.\phi(\mathrm{xi})) \geq \rho - \xi\mathrm{i}$$

$$\xi\mathrm{i} \geq 0, \mathrm{i} = 1, \ldots \mathrm{l} \quad \text{Eq. (3.2)}$$

Where w is the weight vector orthogonal to the hyperplane,$\varepsilon = (\varepsilon 1, \ldots, \varepsilon l)$ is the vector of slack variableused to panalize the rejected instances,and ρ represents the margin (the distance of hyperplane from the origin), v is the parameter that controls the trade-off between maximizing the distance of hyperplane from the origin and fraction data containing in the separate region.

Due to curse of dimenstionality(Manevitz & Yousef *et al*, 2002; Shin *et al*, 2005), the SVM utilizes the kernal theory,the inner dot product in the feature space is calculated using a simple kernal function $k(x, y) = \phi(x).\phi(y)$, such as Gaussian kernal, $k(x, y) = e^{-\gamma||x-y||^2}$.Using the kernal function and Lagrangian multiplie to the original quadratic programing ,the solution of Eq.(3.2) creates a decision function. The generic test instance (x) is

$$\mathrm{f(x)} = \mathrm{sgn}((\mathrm{w}.\phi(\mathrm{x}) + \mathrm{b}) - \rho) \quad \text{Eq.(3.3)}$$

The test instance (x) is accepted when f(x) is possitive and it is rejected when f(x) is negative.Positive instances indicates that test instance (x) is similar to the training training data and the Nedgitive instances indicates that it departs from the training data and is considerred as anomaly.

3.3. Proposed System Model

The proposed hybrid intrusion detection system approach is shown in fig 2 below. C5.0 is used to train the misuse detection model in the hybrid intrusion detection system. The Misuse detection model can detect known attacks with a low false alarm rate. One-class SVM was applied to the anomaly detection (trained using normal training traffic).During the training procedure decision boundaries are located normal data from the origin. The outliers are detected as using decision function and the model classify outlier as attack connection.

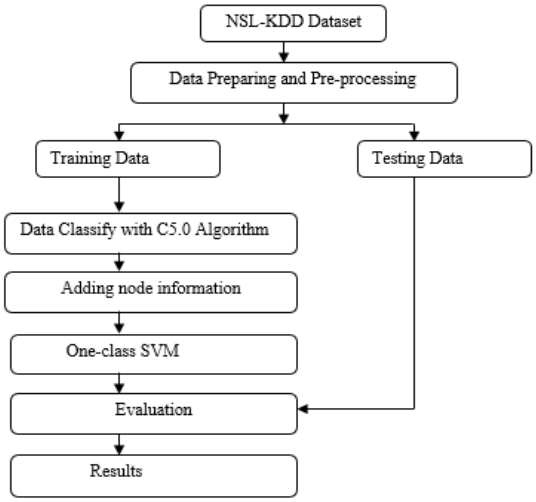

Fig. 2 Frame work of Proposed Methodology

4. Experimental Setup

The NSL-KDD dataset are taken to evaluate the proposed the proposed C5.0 and One-class SVM. The experiment have been performed using Intel core 5 Processor with 4 GB of RAM and LIBSVM (MATLAB). The proposed method is compared with C4.5 and one-class SVM

4.1 Intrusion detection dataset

NSL-KDD dataset, developed by (M. Tavallaee *et al* 2009) an advanced version of KDD Cup 1999 benchmark intrusion detection dataset because of the inherent problems Statistical analysis conducted on KDD data set found important issues that greatly affected the performance of anomaly evaluated systems, and results is very poor for anomaly detection.

In our experiment, LIBSVM software is used. It is an integrated software tool for support vector classification, regression and distribution estimation, which can handle One-class SVMs.

4.2 Result Analysis

To evaluate the performance of proposed technique Confusion matrix is used, it contains data about actual and predicted classifications (Kohavi *et al*, 1998)

Table.1 Confusion Matrix

Confusion Matrix		Predicted Class	
		Negative	Positive
Actual Class	Negative	A	B
	Positive	C	D

4.2.1 Recall

The recall or true positive rate (TP) is defined as the proportion of positive cases that were correctly identified, as calculated using the equation:

$$TP=\frac{d}{c+d} \qquad \text{Eq. (4.1)}$$

4.2.2 False Positive

The false positive rate (FP) is defined as the proportion of negatives cases that were incorrectly classified as positive, as calculated using the equation

$$FP=\frac{b}{a+b} \qquad \text{Eq. (4.2)}$$

4.2.3 False Negative

The false negative rate FN) is defined as the proportion of positives cases that were incorrectly classified as negative, as calculated using the equation.

$$FN=\frac{c}{c+d} \qquad \text{Eq. (4.3)}$$

4.2.4 True Negative

The true negative rate (TN) is defined as the proportion of negatives cases that were classified correctly, as calculated using the equation

$$TN=\frac{a}{a+b} \qquad \text{Eq. (4.4)}$$

4.2.5 Precision

Precision (P) is defined as the proportion of the predicted positive cases that were correct, as Calculated using the equation

$$P=\frac{d}{b+d} \qquad \text{Eq. (4.5)}$$

4.2.6 F-Measure/F-Value/F-Score

The F-Score consider both precision and recall of the procedure to compute the score.

$$F = 2\left(\frac{P*R}{P+R}\right) \qquad \text{Eq. (4.6)}$$

Table 2 Confusion metrics of existing method C4.5 & 1-Class SVM

Confusion matrix		Predicted Class	
		0	1
Actual Class	0	347	47
	1	530	4076

Table 3 Overall Comparison of existing method C4.5 & 1-Class SVM

Parameters	value	Percentage (%)
Correctly Classified Instance	4423	88.5%
Incorrectly classified Instance	577	11.5%
Total number of Instance	5000	

Table 3 shows that, out of 5000 instances of attacks (Normal and anomaly attacks) , 4423 instances are detected and the detection rate is 88.5% and the false alarm ratio is 11.5%. The confusion metric is tested on proposed method i.e., C4.5 & 1-Class SVM.

Table 4 Confusion metric proposed method C5.0 & 1-Class SVM

Confusion metric		Predicted Class	
		0	1
Actual Class	0	372	22
	1	246	4360

Table 5 Overall Comparison proposed method C5.0 & 1-Class SVM

Parameter	Values	Percentage (%)
Correctly Classified Instance	4732	95%
Incorrectly Classified Instance	268	5%
Total Number of Instance	5000	

Table 5 shows that, out of 5000 instances of attacks (Normal and anomaly attacks) , 4732 instances are detected and the detection rate is 95% and the false alarm ratio is 5%.The confusion metric is tested on proposed method i.e., C5.0 & 1- Class SVM.

Table 6 Comparison results of Normal and Anomaly (attack)

Alg.	Class	Parameters						
		TP	FP	FN	TN	P	R	S
C5.0 & 1- Class SVM	0	372	22	246	4360	94	60	90
	1	4360	246	22	372	95	99	60
C4.5 & 1- Class SVM	0	347	47	530	4076	80	40	99
	1	4076	30	47	347	88	99	40

4.2.7 Accuracy

The accuracy (AC) is defined as the proportion of the total number of predictions that were correct. It is determined using the equation

$$AC = \frac{a+d}{a+b+c+d} \qquad \text{Eq. (4.7)}$$

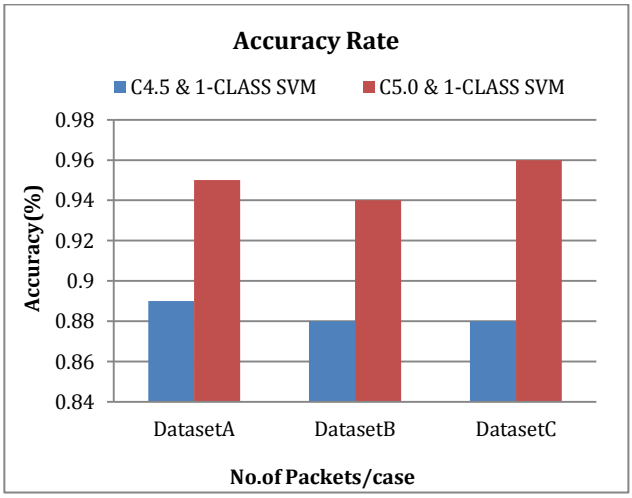

Chart 1 Accuracy rate on different datasets

Chart 1 shows that ,The experiment is iterated multiple times using different sets of training and testing cases (depending on number of inputs used to create the case). Dataset A contains 10000 training and 10000 testing cases. Date set B contains 5000 and 5000 testing cases. Whereas Dataset C contains 15000 training and 15000 testing cases. The result shows that the proposed C5.0 & 1-Class SVM has high accuracy rate compared to the existing algorithm.

Chart 2 shows that Error rate on different datasets are evaluated. The results shows that the proposed C5.0 & 1-Class SVM has less Error rate compared to the existing algorithm.

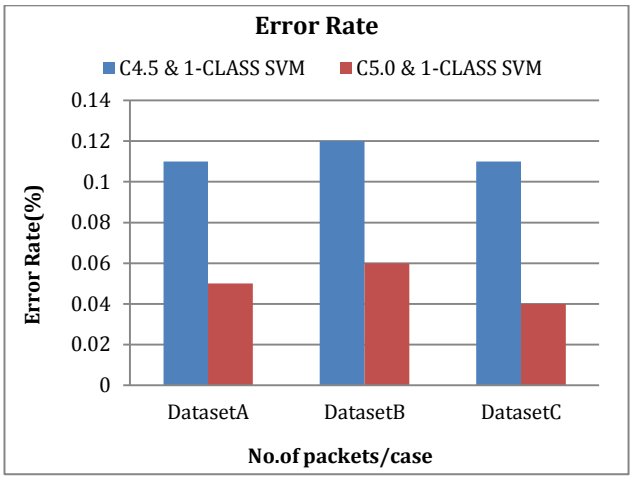

Chart-2: Error Rate on different datasets.

4.2.8 Roc Curve

ROC graphs are another way of confusion matrices to examine the performance of classifiers (Swets, 1988). Receiver Operating Characteristic's (ROC), or ROC curve, is a graphical plot that shows the performance of a binary classifier system as its discrimination threshold is varied. The curve is created by plotting the true positive rate against the false positive rate.

4.2.8 Error rate

The Error Rate (ER) is defined as the proportion of the total number of predictions that were incorrectly classified, as calculated using the equation

$$ER = 1 - AC \qquad \text{Eq. (4.8)}$$

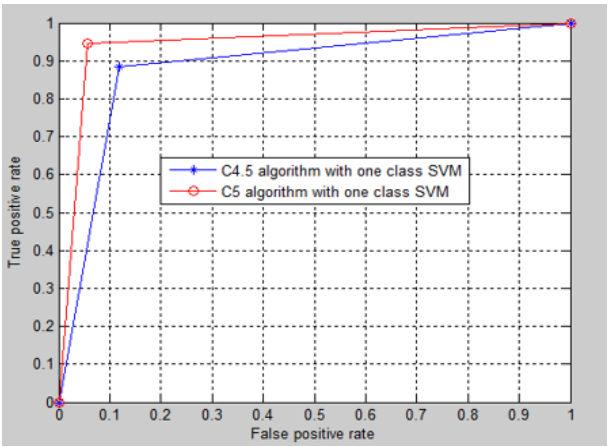

Chart 3 ROC curve

The probability distributions for both detection and false alarm are known, the ROC curve can be generated by plotting the detection probability in the y-axis versus the false-alarm probability in x-axis.

5. Conclusion

Intrusion detection is one of the main research problems in computer security. The main goal is to detect infrequent access or attacks to protect internal networks from attacks. A hybrid intrusion detection system using C5.0 & one class SVM is proposed to give better performance when compared to the existing algorithm in terms of accuracy , true positive , true negative , false positive, false negative, recall, precision, specificity, F-Measure, error rate, ROC graph. Compared to the single algorithms, combining with multiple algorithms has given much better results. The proposed algorithm outperforms other existing approaches. Simulation results demonstrate that the proposed algorithm is successful in detecting misuse and anomaly intrusion detection system.

References

Gisung Kim and Seungmin Lee (2014), A Novel Hybrid Intrusion Detection Method Integrating Anomaly Detection With Misuse Detection, *ELSEVIER, Expert Systems with Applications* vol. 41 pp. 1690 – 1700.

Amuthan Prabakar Muniyandi., R.Rajeswari and R. Rajaram (2012), Network Anomaly Detection By Cascading K-Means Clustering And C4.5 Decision Tree Algorithm," In Procedia Engineering vol. 30 pp.174 – 182.

Basant Agarwal and Namita Mittal, Hybrid Approach For Detection Of Anomaly Network Traffic Using Data Mining Techniques*, Elsevier, In Procedia Engineering* vol. 6 pp. 996 – 1003.

Cheng Xiang., Ping Chin Yong and Lim Swee Meng (2008), Design Of Multiple-Level Hybrid Classifier For Intrusion Detection System Using Bayesian Clustering And Decision Trees,*ELSEVIER ,Pattern Recognition Letters* vol.29 pp. 918 – 9

Gang Wang., Jinxing Hao., Jian Ma and Lihua Huang (2010),A New Approach To Intrusion Detection Using Artificial Neural Networks And Fuzzy Clustering, *Elsevier, Expert System with Applications* 37 6225 – 623

Hyun Joon Shin, Dong-Hwan Eom and Sung-Shick Kim (2005), One-class support vector machine-an application in machine fault detection and classification, *Elsevier, Computer & industrial engineering 48 395-408.*

Levent Koc and Thomos A.Mzzuchi (2012) A Network Intrusion Detection System Based On Hidden Naïve Bayes Multiclass Classifier, *ELSEVIER, Expert Systems with Applications* vol. 39, pp. 13492-13500.

M. Ali Aydin and A. Halim Zaim (2009), A Hybrid Intrusion Detection System Design For Computer Network Security," *ELSEVIER ,Computers and Electrical Engineering* 35517 – 526.

Mahsa Khosronejad and Elham Sharififar, "Developing a Hybrid Method of Hidden Markov Models and C5.0, *International Journal of Database Theory and Application* vol.6 No.5 (2013), pp.165 – 174. http:// dx.dot.org10.14257 /ijdta. 2013.6.5.15

Ming-Yang Su(2011) ,Using Clustering To Improve The KNN-Based Classifier For Online Anomaly Network Traffic Identification, *ELSEVIER Journal of Network and Computer application 3*4 722 – 730.

Mrutyunjaya Panda, Ajith Abraham and Manas Ranjan Patra (2012), A Hybrid Intelligent Approach For Network Intrusion Detection, *ELSEVIER ,In Procedia Engineering* 30 1 – 9.

Neelam Sharma and Saurabh Mukherjee (2011), A Novel Multi-Classifier Layered Approach To Improve Minority Attack Detection In IDS, *ELSEVIER, In Procedia Technology* 6 913-921.

Sankar Mahadevan and Sirish L. Shah (2009), Fault detection and diagnosis in process data using one-class support vector machines, *ELSEVIER ,Journal of Process Control* 19 1627-1639

Shih-Wei Lin, Kuo-Ching Ying, Chou-Yuan Lee and Zne-Jung Lee(2012), An Intelligent Algorithm With Feature Selection And Decision Rules Applied To Anomaly Intrusion Detection, *ELSEVIER, Applied Soft Computing* 12 3285-3290.

Shi-Jinn Horng and Ming-Yang Su (2011), Novel Intrusion Detection System Based On Hierarchical Clustering And Support Vector Machines, *ELSEVIER, Expert Systems with Applications* 38 306-313

Siva S. Sivatha Sindhu, S. Geetha and A. Kannan (2012), Decision Tree Based Light Weight Intrusion Detection Using A Wrapper Approach, *ELSEVIER, Expert Systems with Applications* 39 129-141.

Taeshik Shon and Jonsub Moon (2007) , A Hybrid machine learning approach to network anomaly detection, *ELSEVIER, Information Sciences* 177 3799-3821.

Tamer F. Ghanem, Wali S. Elkilani and Hatem M. Abdul-Kader (2014), A Hybrid approach for efficient anomaly detection using meta heuristic methods*, Journal of Advanced Research.* 2090-1232 © 2014 Production and hosting by *Elsevier* B.V on half of Cairo University. http://dx.doi.org/ 10.1016/jare.2014.02.009.

Vahid Golmah (2014), An Efficient Hybrid Intrusion Detection System Based On C5.0 And SVM*, International Journal of Database Theory and Applications* vol.7 No.2 , pp.59 – 70. http://dx.doi.org/10.14257/ijdta.2014.7.2.06

Yinhui Li and Jingbo Xia (2012), An Efficient Intrusion Detection System Based On Support Vector Machines And Gradually Feature Removal Method, *ELSEVIER, Expert Systems with Applications* 39 424-430.

Information on See5/C5.0-RuleQuest Research Data.See5/ MiningTools, 2011 .[Online]. Available: http://www.rulequest.com/see5-info.htm

Is See5/C5.0 Better Than C4.5?, 2009. [Online].Available: http://www.rulequest.com/see5 -comparison.html

See/C5.0 updated record [Online]. Available:

Prof Manasi Kulkarni and Ms Rashmi R. Tundalwar (2013), Web Spam Detection Using C5.0 Classification Algorithm, . *IJARCSSE* ,volume 3 issues

Manevitz and Yousef, M (2002), One-class SVMs for document classification, *ELSEVIER, Journal of Machine Learning Research* 2 139-154.

M. Tavallaee, E. Bagheri, W. Lu, and A. Ghorbani (2009), A Detailed Analysis of the KDD CUP 99 Data Set, Submitted to Second IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA).

LIBSVM 2.5 is available at http:/ /www.csie .ntu.tw/~cjlin/libsvm

Kohavi and Provost (1998), "Confusion Matrix". [Online].Available:http://www2.cs.uregina.ca/~dbd/cs83 1/notes/confusion_matrix/confusion_matrix.htm

Swets (1988) ROC Graph is Available: http://www2.cs. uregina.ca/~dbd/cs831/notes/ROC/ROC.html

Managing cyber risks in interconnected world Key findings from The Global State of Information Security® Survey 2015 is Available at http:// www.pwc.com/gsiss2015