ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Intrusion Detection System Using SVM Classification

Sandeep Ranode

Dept. of Computer Engineering, G.H. Raisoni College of Engineering, Ahmednagar, India

ABSTRACT: Intrusion detection systems(IDS) has plays a very important role to defend the characteristics of computer mainly into two categories: malicious and irrelevant activities. Intrusion detection can be achieve by Categorization. A new machine learning based algorithm for classification of data is implemented to network intrusion detection is introduced in this paper. The most simple job is to differentiate activities of network are as normal or irrelevant while reducing the misclassification. The objective of Intrusion detection system (IDS) are to apply all the available information in order to identify the attacks by outsider hackers and misuse of insiders. For Network intrusion detection there are different classification models have been developed, the most commonly applied methods are Support Vector Machine(SVM) and Clustering based on Self-Organized Ant Colony Network(CSOACN) both consider their strengths and weaknesses individually. To reduces the weakness, combination of the SVM method with CSOACN to take the advantages of both . A standard benchmark of data set KDD99 is evaluated and implemented as a new algorithm. Although to increase both the classification rate and runtime effectiveness it is necessary to implement the Combining Support Vectors with Ant Colony (CSVAC) which outplay SVM alone or CSOACN. An individual real time network dataset and a well-known dataset i.e. KDD99 CUP has been implemented as proposed system. All attack types, detection rate, detection speed, false alarm rate can be measured by implementation of intrusion detection system IDS.

KEYWORDS: IDS; SVM;ACO;KDDD99 CUP;CSVAC.

I. INTRODUCTION

Information technology of today's generation have become very challenging as well as crucial for handling the classification and clustering of big scale data. For real time application in computer system,where different kind of powerful tools are used to secure the computing resources such as exponential increase-in-size and large-scale data inputs. In this paper ,intrusion detection system term implement as a responding process to identify and manage the malicious activities targeted by networking resources and computational resources. An intrusion detection system IDS finds to reveal or expose configuration or characteristics that could lead detection system is formulation of hardware and software elements, this combination implemented to search unexpected events in all three tenses; that shows an attack will happen, is happening or has already happened.

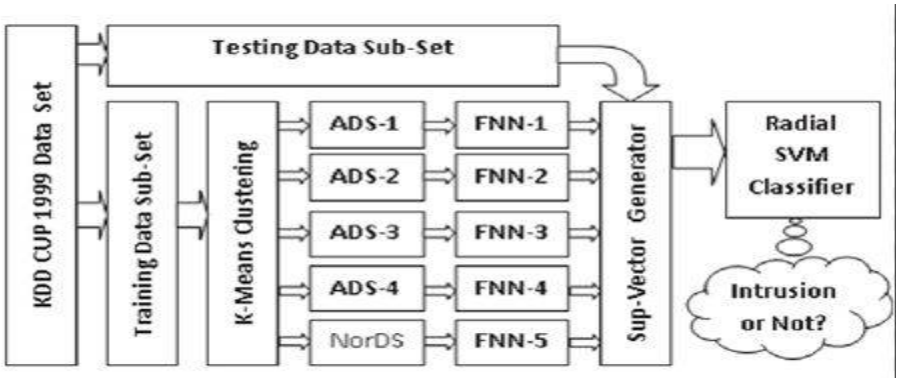

Fig1:System Architecture

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

II. RELATED WORK

Issues related to intrusion detection can be categorized into two broad areas: (1) network security and intrusion detection models, and (2) intrusion detection methods and algorithms based on artificial intelligence (mostly machine learning) techniques. In this section we shall briefly review some related work in the second area, and leave area (1) to the next section, when we discuss the background of IDSs. Intrusion detection as a classification problem has been studied for decades using machine learning techniques, including traditional classification methods (single classifier) such as KNearest Neighbor (K-NN), Support Vector Machines (SVMs), Decision Trees (DTs), Bayesian,Self-Organized Maps (SOMs), Artificial Neural Networks(ANNs), Generic Algorithms (GAs), and Fuzzy Logic, as wellas hybrid classifiers that combine multiple machine learning techniquesto improve the performance of the classifier. A review of using these approaches was given , which also included statistics of the use of these techniques reported in 55 research articles during the period 20002007. The review indicates that SVM and K-NN were the most commonly used techniques while the use of a hybrid increased significantly after 2004 and became mainstream. Another more recent review provided a thorough survey of intrusion detection using computational intelligence. It presented the details of the classification algorithms and swarm intelligence methods to solve problems using the decentralized agents. Most recently, IDS was introduced by integrating On Line Analytical Processing (OLAP) tools and data mining techniques. It is shown that the association of the two fields produces a good solution to deal with defects of IDSs such as low detection accuracy and high false alarm rate. As stated, as one of the swarm intelligence approaches, Ant Colony Optimization (ACO),has been applied in many fields to solve optimization problems, but its application to the intrusion detection domain is limited. Several methods were reported using ACO for intrusion detection. For example, an ant classifier was proposed that used more than one colony of ants to find solutions in.
multiclass classification problem. Another antbased clustering algorithm applied to detect intrusions in a network presented in showed that the performance was comparable to some traditional classification methods like SVM, DT, and GA the authors evaluated the basic antbased clustering algorithms and proposed several improvement strategies to overcome the limitations of these clustering algorithms that would not perform well on clustering large and high-dimensional network data. The work presented also used ACO for intrusion detection in a distributed network. The basic ingredient oftheir ACO algorithm was a heuristic for probabilistically constructing solutions. All these ACO-based intrusion detection approaches are single classifiers as categorized. Hybrid intrusion detection approaches involving SVM have been studied in the past, such as the one reported that uses the Dynamically Growing Self-Organizing Tree (DGSOT) algorithm for clustering to help in finding the most qualified points to train the SVM classifier. It starts with an initial training set and expands the set gradually so that the training time for the SVM classifier is significantly reduced. Another hybrid intrusion detection approach was recently reported that combines hierarchical clustering and SVM.

III. PROPOSED ALGORITHM

Algorithm 1:
(1) SUPPORT VECTOR MACHINES (SVM):
Algorithm Steps:
Input: A training set with each data point labeled as positive or negative (class labels).
Output: A classifier.
1) Begin
2) Randomly select data points from each class.
3) Generate a SVM classifier.
4) While more points to add to training set do
5) Find support vectors among the selected points;
6) Apply CSOACN clustering around the support vectors;
7) Add the points in the clusters to the training set;
8) Retrain the SVM classifier using the updated training set;
9) End
Algotithm 2:-
Input: A training data set.
Input: N number of training iterations.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Input: RR detection rate threshold.
Output: SVM and CSOACN Classifiers.
1) Begin
2) Normalize the data;
3) Let r be the detection rate, initially 0;
4) While r ¡RR do
5) for k = 1, , N do
6) SVM training phase;
7) Ant clustering phase;
8) End
9) Construct classifiers;
10) do testing to update r;

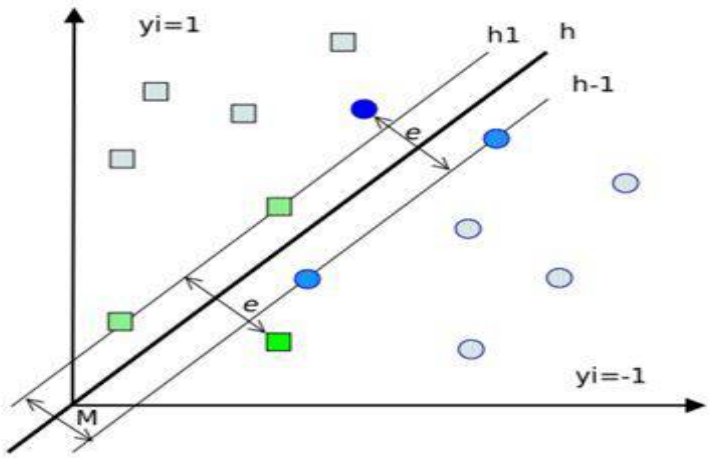

Fig2:General Linear Binary Classification Case

IV. RESULT ANALYSIS

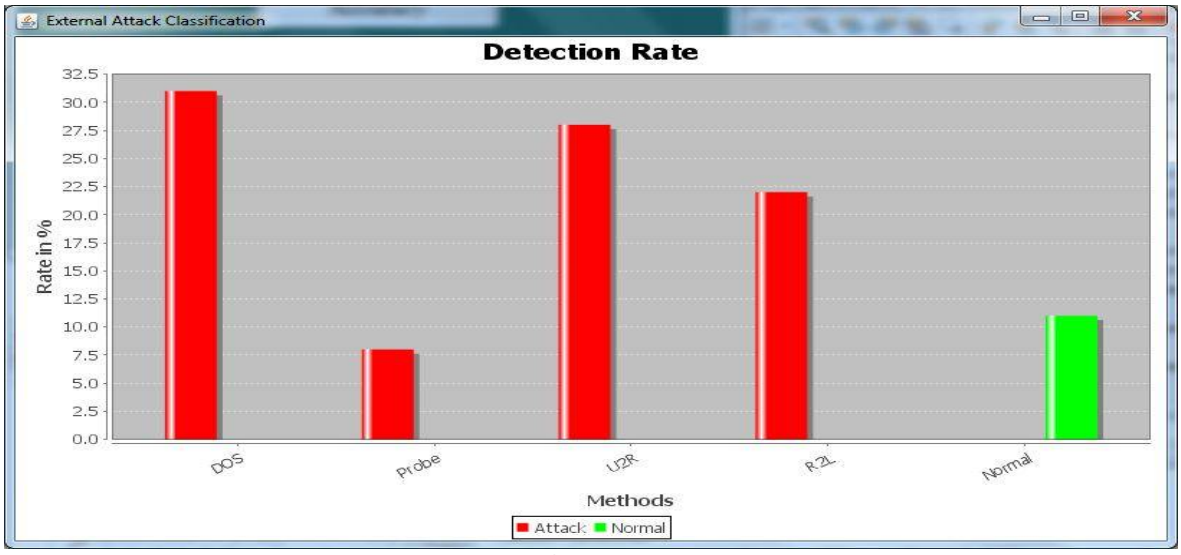

Fig3: Detection Rate

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

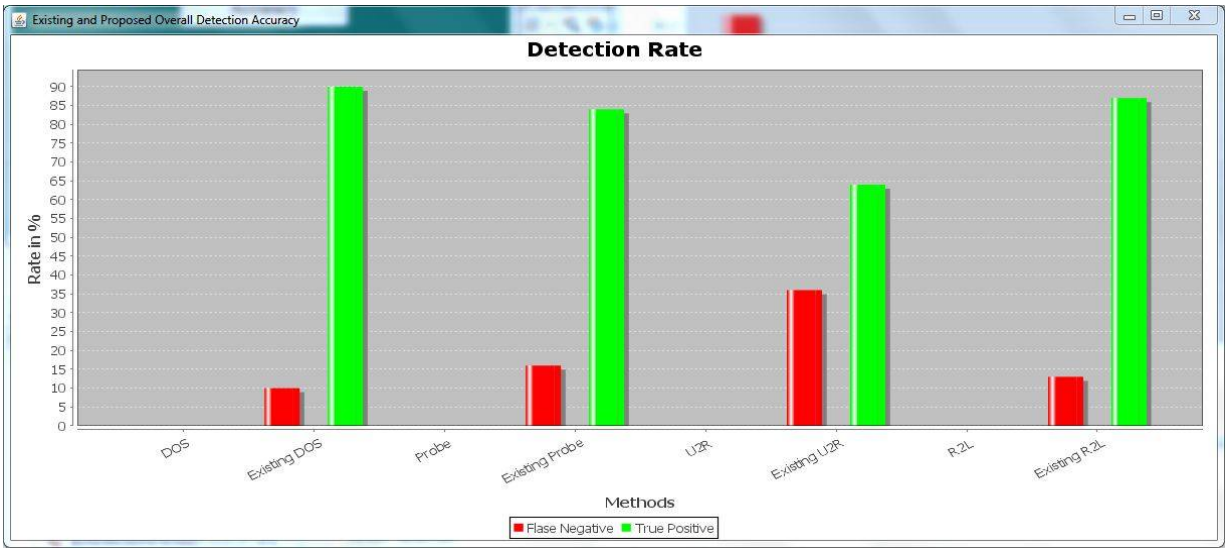

Fig4: Overall Existing System Dection accuracy

To evaluate the performance of decision tree intrusion detection model we compared it with SVM in terms of accuracy, training time and testing times and we summarize the results in table 2. Decision tree gives better accuracy for Probe, R2L and U2R classes compared to SVM and it gives worse accuracy for DoS class of attacks. For normal class both give the same performance. There is a small difference in the accuracy for Normal, Probe and DoS classes for decision trees and SVM but there is a significant difference for U2R and R2L classes. These two classes have small training data compared to other classes, so we can conclude that decision tree gives good accuracy with small training data sets. The results also show that testing time and training time of the classifiers are slightly better than SVM. Moreover, decision tree is capable of multi-class classification which is not possible with SVM. Multi-class classification is a very useful feature for intrusion detection models. The training time and testing times are also less for decision tree compared to the SVM (Support Vector machine).

IV. Conclusion and Future Work

As this paper describe the research in NIDS as well as HIDS. The proposed Algorithms and methods are design to grow the detection rate of NIDS with distinct attacks and HIDS are also implemented for existing work.In Order to boost the efficiency and reliability of IDS system in future ,consideration the morality of privacy preserving OLAP with the proposed structure. As a future work ,intensify the CSVAC algorithm to produce multiple SVM classifiers to handle multi-class cases as well as find the different ways to change a problem of nonlinear classification to linear by implementing the latest proposed Maximum Information Coefficient. For a detailed examination of performance and the comparisons with other existing algorithms, applying the KDD99 data set will be distributed differently and also implementing other standard benchmark datasets.

ACKNOWLEDGMENTS

I would like to take this opportunity to express my sincere gratitude to my Project Guide Ramesh G. Patole (Assistant Professor, Computer Engineering Department) for his encouragement, guidance, and insight throughout the research and in the preparation of this dissertation. He truly exemplifies the merit of technical excellence and academic wisdom.

References

[1].W. Lee, S.J. Stolfo, K.W. Mok, Mining audit data to build intrusion detection models, in: Proceedings of the 4thInternational Conference on Knowledge Discovery and Data Mining, AAAI Press, 1998, pp. 6672.
[2] .T. Zhang, R. Ramakrishnan, M. Livny BIRCH: an efficient data clustering method for very large databasesProceedings of SIGMOD, ACM, 1996, pp. 103114.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

[3] .L. Khan, M. Awad, B. Thuraisingham A new intrusion detection system using support vector machines and hierarchical clustering The VLDB Journal 16 (2007) 507521.
[4] . X. XuAdaptive intrusion detection based on machine learning: feature extraction, classifier construction and sequential pattern prediction Information Assurance and Security 4 (2006) 237246.
[5] ..X. Huang, J. Miao, Ben He High performance query expansion using adaptive co-training Information Processing Management 49 (2) (2013) 441453.
[6] .Y. Liu, X. Yu, J.X. Huang An, Combining integrated sampling with SVM ensembles for learning from imbalanced datasets Information Processing Management 47 (4) (2011) 617631.
[7] .V. Vapnik The Nature of Statistical Learning Theory Springer, 1999