ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 2, February 2015

Intrusion Detection System Using Multiclass Batch Algorithm

V. Jaiganesh[1] Dr. P. Sumathi[2] A.Vinitha[3]

Doctoral Research Scholar, Department of Computer Science, Manonmaniam Sundaranar University, Tirunelveli Tamil Nadu, India[1]

Doctoral Research Supervisor, Assistant Professor, PG & Research Department of Computer Science, Government Arts College and Science College, Coimbatore, Tamil Nadu, India[2]

M.Phil Scholar, Department of Computer Science, Dr. N.G.P Arts and Science College, Assistant Professor, Sasurie Arts &Science College, Erode, Tamil Nadu, India[3]

Abstract: An intrusion detection system is used to find the malicious activities in the network and reports to the management. It can be done in two ways. One is host based intrusion detection system and another one is network based intrusion detection system. There are two types of detection methods one is anomaly detection and another one is misuse detection. In this paper classification algorithm is used to detect the malicious activities in the network. Support vector machine concept is used to find the optimal hyper plane. Initially classification is done to classify the data whether it is normal or an attack. Then clustering concept is applied to group the similar attacks. After grouping multiple class batch processing is done.

Keywords: Intrusion detection system, Detection types, data mining, classification, Support vector machine, Multiclass batch algorithm.

1 INTRODUCTION

Using internet is wide nowadays. Day by day the usage of searching information and hacking information through net is increased. Many persons try to hack information which is unauthorized to them. Many people's search some technique to secure their information. The only solution is to find that whether any malicious activity is entering the network or not. If it occurred there should be an alert to the system administrator to take safety measures.

2 INTRUSION DETECTION SYSTEMS

An intrusion detection system checks the malicious activities that enter the network or not. It can be done at two ways. One is host based intrusion detection system and another one is network based intrusion detection system [22]. There are two types of detection.

- Signature based detection
- Anomaly based detection

Signature based detection

It compares the normal activities with seriously known attack patterns that are stored in a database.

Anomaly based detection

It defines the normal baseline activities of system. If there is any change in normal activity it informs the administrator.

Different types of attacks

- Denial of service
- User to root attack
- Probing
- Remote to local attack

Different types of protocol attacks

- Internet control message protocol attack
- Transmission control protocol attack
- User datagram protocol attack
-

3 DATA MINING

It is used to find the useful information in the large databases. It finds the relationship between data and summarizes it into useful information. There are two modeling techniques. One is predictive and another one is descriptive. The predictive models tell the future with the help of past information. The descriptive model finds the relationship between data items and gives useful information.

4 CLASSIFICATION

It is a supervised learning technique which categorizes the data according to the predefined labels.

Some techniques of classification

- Decision tree
- Naïve bayes
- Support vector machine
- Neural networks

5 LITERATURE SURVEY

- Many research techniques have developed to detect the attacks. In the paper network intrusion detection system using reduced dimensionality they have said that the ID3 algorithm provides the better accuracy and efficiency.
- In the paper expert system with application two algorithms are compared to find the accuracy. C4.5 and

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

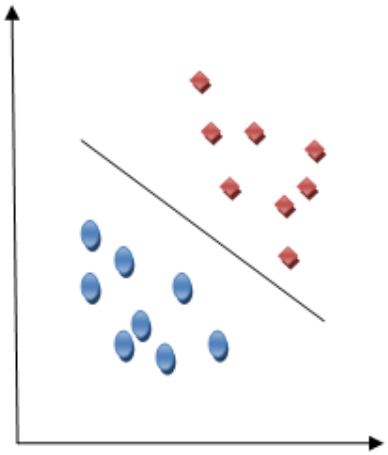
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 2, February 2015

support vector machine are compared to find accuracy. They find that SVM is better to find false alarm when compared to c4.5

- In this paper the new algorithm is proposed to find the better accuracy. Based on the SVM the new technique called multi class batch support vector machine is introduced to find the accuracy.

6 SUPPORT VECTOR MACHINE

It is a classification technique which separates the classes by using a hyper plane. It supports both linear and non linear data. The support vector machine finds the optimal linear hyper plane in the feature space. It avoids the model to be over fitting. The objects are rearranged using a set of mathematical functions known as kernels.



(Figure 6.1) (SVM)

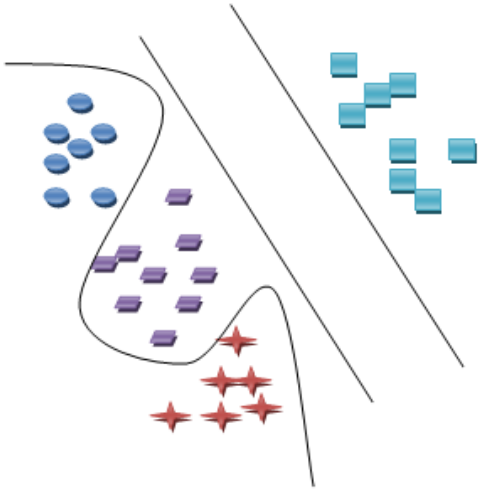
7 MULTICLASS BATCH SUPPORT VECTOR MACHINE

It is a technique which separates the hyper plane into multiple classes. It makes the linear into non linear sub space. It is performed after the clustering process. Support vector machine is to find out the multi kernel hyper plane which is the most distant away from any data, this can minimize error rate.

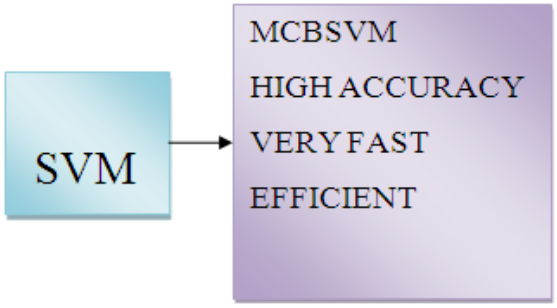
MCBSVM steps:

Step 1: collect training data samples and test samples.
Step 2: According to gathered data, constructs training sample set and test sample set.
Step 3: Set up parameters, initializes the initial support vector object position, every position
corresponding a set of attributes (*a1, a2...an*) in MCBSVM model, builds up SVM prediction model by parameters and samples.
Step 4: From the parameters calculate every class threshold value, and then analyze the hyper plane value.
Step 5: Randomly select *P* objects from initial cluster, find out the optimal object position *best X* based on the hyper plane. Set it up as individual target *obj X*.
Step 6: The non-optimal objects in the initial cluster moving to target class position and make the overall search.
Step 7: The optimal object make overall search according to its neighborhood.
Step 8: Update every objects class
Step 9: Apply the optimal parameter (*a1, a2…an*) and training sample to build up MCBSVM classification model.

The improved MCBSVM makes separating hyper plane quickly find the right class position basis optimized hyper plane function, makes the algorithm substantially higher than the previous methods for intrusion class detection.



(Figure 7.1) MCBSVM Classifications



(Figure 7.2) Research Methodology

Detection and identification of attack and non-attack behaviors can be generalized as the following table.

- True positive (TP): the amount of attack detected when it is actually attack.
- True negative (TN): the amount of normal detected when it is actually normal.
- False positive (FP): The amount of attack detected when it is actually normal, namely false alarm.
- False negative (FN): The amount of normal detected when it is actually attack, namely the attacks which can be detected by intrusion detection system.

8 RESULTS AND DISCUSSIONS

In the experiments, the system use benchmark data set from UCI repository (KDD Cup 99 dataset).The data applied in the research comes from KDD Cup 99 dataset,

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 2, February 2015

which was initially used for The Third International Knowledge Discovery and Data Mining Tools Competition. It was intended to assess the efficiency of intrusion detection algorithm. Therefore, the research also applies the dataset.

Dataset Description

Benchmark UCI data sets:
Dataset Name: KDD cup 99
URL: http:\\www.UCIrepostory.org\kddcup 99
Total Attributes:38
Total Instances:65000

Table: 8.1 Performance Comparison Table

Type	**Neighbourhood Based Method**	**MCBSVM**
Precision (%)	90.7	99.5
Training Time(ms)	5.6	2.3
Testing Time (ms)	3.4	2.1
Efficiency	Ordinary	Better

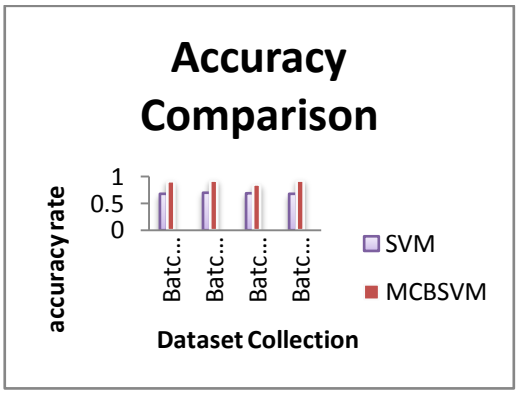


Figure 8.2Accuracy comparison - Batch by Batch

9 CONCLUSION

The proposed MCBSVM has been applied KDD cup 99 dataset. The system expands the existing SVM by applying Multi class and batch based process to achieve two goals. The first goal is improving the efficiency of the intrusion classification. Another one is the optimized hyper plane for multi class SVM which is the trial of satisfying the research and improving the sub type detection accuracy. Further the study compares accuracy, detection rate, false alarm rate and accuracy of other attacks under different proportion of normal information.

10 FUTURE WORK

The optimized MCBSVM algorithm has been expanded with the new optimal classification algorithms, which can handle large category dataset more rapidly, accurately and effectively, and keep the good scalability at the same time. The algorithm mainly created to perform active learning process in the given data, but this should disperse the value data in the dealing process. So, this should do further improvement to the algorithm to adapt the mixed data directly.

REFERENCES

[1] Ahmed Youssef and Ahmed Emam"Network Intrusion Detection using Data Mining and Network Behavior Analysis" International Journal of Computer Science &Information Technology (IJCSIT) Vol 3, No 6, Dec 2011

[2] Ahmed, Tarem, Boris Oreshkin, and Mark Coates. "Machine learning approaches to network anomaly detection." Proc. SysML (2007).

[3] Amoroso EG (1999) Intrusion detection: an introduction to internet surveillance, correlation, trace back, traps, and response. Intrusion.Net Books, NJ

[4] AnazidaZainal, MohdAizainiMaarof and SitiMariyamShamsuddin "Data Reduction and Ensemble Classifiers in Intrusion Detection" in 2008 IEEE.

[5] Cannady.J. Artificial Neural Networks for isuse Detection. National Information Systems Security Conference, 1998.

[6] Chandolikar N.S, V.D.Nandavadekar Comparative analysis of two algorithm for Intrusion attack classification using dataset" in International Journal of Computer Science and Engineering (IJCSE) in 2012 .

[7] Devaraju .S, S .Ramakrishnan "Detection of Accuracy for Intrusion Detection System using Neural Network Classifier" International Journal of Emerging Technology and Advanced Engineering(ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013)

[8] Devendrakailashiya, Dr. R.C. Jain "Improve Intrusion Detection Using Decision Tree with Sampling" in IJCTA | MAY-JUNE 2012.

[9] DuinR.P.W , "The Combining Classifier: To Train or Not to Train?" Proc. 16th Int'l Conf.Pattern Recognition, vol. 2, pp. 765-770, 2002.

[10] GuangqunZhai, ChunyanLiu "Research and Improvement on ID3 Algorithm in IntrusionDetection System" in 2010 IEEE.

[11] Jorge Blasco, Agustin Orfila, Arturo Ribagorda "Improving Network Intrusion Detection by Means of Domain-Aware Genetic Programming" DOI10.1109/ARES.2010.53 in IEEE 2010.

[12] Joshi S A, VarshaS.Pimprale "Network Intrusion Detection System (NIDS) based on Data 2, Mining" International Journal of Engineering Science and Innovative Technology (IJESIT) Volume Issue 1, January 2013

[13] V.Jaiganesh "A Survey on Building Intrusion Detection System Using Data Mining Framework",ISSN: 1947-5500, Vol. 10 No. 3 March2012.

[14] V.Jaiganesh "An Efficient Algorithm for NetworkIntrusion Detection System", ISSN: 0975 â€" 8887, Volume No: 90, Issue No: 12-3,March 2014.

[15] Kong.Q, H. Zhao, and B.L. Lu, "Adaptive Ensemble Learning Strategy Using an Assistant Classifier for Large-Scale Imbalanced Patent Categorization," Proc. 17th Int'l Conf. Neural InformationProcessing: Theory and Algorithms, pp. 601-608, 2010.

[16] Lin R. Jin, and A. Hauptmann, "Meta- Classification of Multimedia Classifiers," Proc.Int'l Workshop Knowledge Discovery in Multimedia and Complex Data, 2002.

[17] LiuC.L,"Classifier Combination Based on Confidence Transformation," Pattern Recognition, vol. 38, no. 1, pp. 11-28, 2005.

[18] LiuC.L,H. Hao, and H. Sako, "Confidence Transformation for Combining Classifiers,"Pattern Analysis and Applications, vol. 7, no. 1, pp. 2-17, 2004.

[19] Lunt, T.F. (1989). Real -Time Intrusion Detection. Proceedings from IEEE COMPCON.

[20] Mohd.JunedulHaque, Khalid.W. Magld, NisarHundewale "An Intelligent Approach for Intrusion Detection Based on Data Mining Techniques" in 2012 IEEE.