Denial-of-Service Attack Detection using multivariate Correlation Information Based SVM Method

Prajakta P. Solankar*, Jaymala K. Hipparkar

[1] Department of Computer Science, Karmayogi engineering college, Shelve, Pandharpur, India

*Corresponding author

doi: https://doi.org/10.21467/proceedings.118.44

ABSTRACT

Now day's network technology is developing rapidly and the network security is important issue. DoS attack is serious threat in network. Denial of service attack forces victim machine out of service several days or few minutes. DoS attack degrades the system performance. This paper constitutes detecting denial of service attack using Multivariate correlation analysis technique. This approach is used to characterize the features of network traffic.This MCA method consists of Triangular area determination methodology for correlation analysis. Normalization is used before this process to remove the bias from data .Normalization technique has greater impact on the performance.

Keywords: Denial of service attack,Multivariate correlation analysis, Triangular area

1 Introduction

In this paper method based on triangular area map (TAM) is used for correlation analysis to well characterize the network traffic features. Various types of attacks are presents in literature which affects on network or host. There is necessity of detecting dos attack and this detection problem is called as Intrusion detection method. There are two types of intrusion detection systems (IDS) are presents. These are host based IDS and Network based IDS.Network based IDS is used in this paper for detecting dos attack. Network based intrusion detection system is divided into two categories i.e Misuse based IDS and Anomaly based IDS. Anomaly based method is better than Misuse based method because Misuse based technique need to store attack signatures manually and in Anomaly based technique there is not necessary to keep signature database instead it is based on profiles generation. The profile of various types of features are generated and deviation from this profile database is treated as attack. The following fig. shows distributed denial of service attack. the fig.1 dot line represents control messages and without dot line represents attack traffic. [1,2,3].The below fig1.shows Distributed DoS attack architecture

2 Related work

Yu Chen, Kai Hwang et.al. detected ddos attack. They used distributed change point detection mechanism by the use of change aggregation trees [4].In paper[5] traffic flooding attack detection is performed by SNMP MIB using SVM.The SNMP MIB statistical data is taken from SNMP agents. For classification of attack, support vector machine is used. The author Arman Tajbakhsh et. al. used data mining methods for detecting intrusion. They used Association rule based classification which is the core part of Intrusion detection system. They used Fuzzy rules for building classifiers.Kddcup99 dataset is used to evaluate the performance of the system [6]. In paper [7] real time intrusion detection system is developed. In this paper principle component analysis(PCA) method is used for preprocessing of the data. To find the hidden correlation MDM is used. Dimitris Gavrilis described Distributed Dos attack behavior using the statistical descriptors. They used Radial Basis function Neural Network(RBFNN) for classification purpose. In this paper[8] trained RBF-NN and evaluated in two experiments. In the first experiment they set up 100 Mpps network and DDoS attack was launched in the University of Patras central library on the main web server

Proceedings DOI: 10.21467/proceedings.118; Series: AIJR Proceedings; ISSN: 2582-3922; ISBN: 978-81-947843-6-4

in the second experiment. Christos Douligeris et. al. described DDos attack , architecture of DDos attack and also various mechanisms and classification methods. They showed various defense mechanism for the DDos attack problem. Various DDos attack tools are also described in this paper[9].

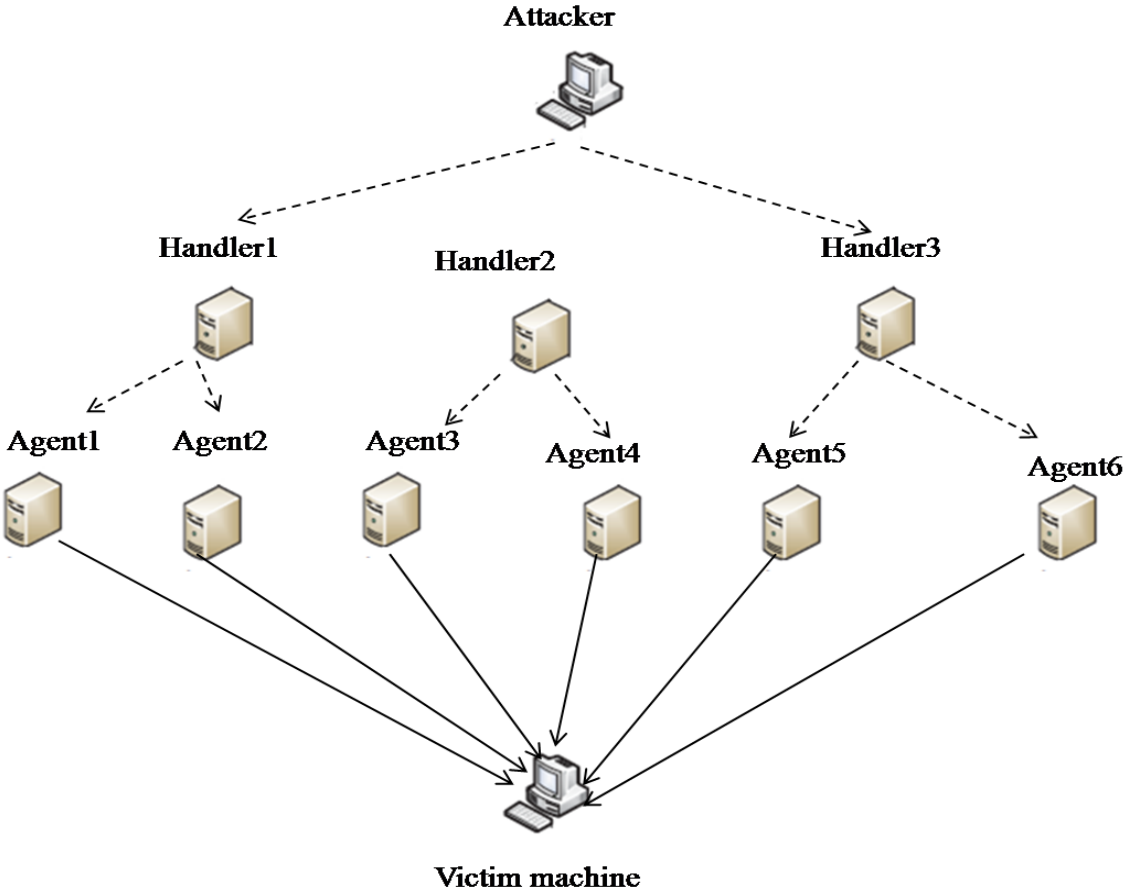


Figure 1: Dos attack architecture

In paper [10] intrusion detection system is developed and used 19 critical features by using the gradually feature removal method. They developed efficient classifier using the combination of support vector machine, ant colony technique and clustering algorithm.They performed experiment using the kddcup99 dataset. They used k-means to reduce the dataset and which is the powerful method in the literature. Shuyuan jin,Danial so Yeung and Xizhao Wang [11] designed covariance matrix based method for mining multivariate correlation of sequential sample. They performed experiments using decision tree and threshold method. S.Yu et. al.[12] discriminated DDos attack from the flash crowd by using the flow correlation coefficient. In this paper[13] computer attacks are detected using the Support vector machine and Independent component analysis (ICA). They used ICA for extracting the features from the multivariate data. Support vector machine classifies data in two categories. part should contain sufficient detail to reproduce the reported data. It can be divided into subsections if several methods are described.

3 Proposed System

The proposed system consists of two main phases i.e. train phase and testing phase, as shown in fig.2. In the train phase profiles are determined and testing phase consists of classification of attack.Kddcup99 dataset is used as input to the proposed system which consists of different types of records: normal, smurf, teardrop, Neptune etc.

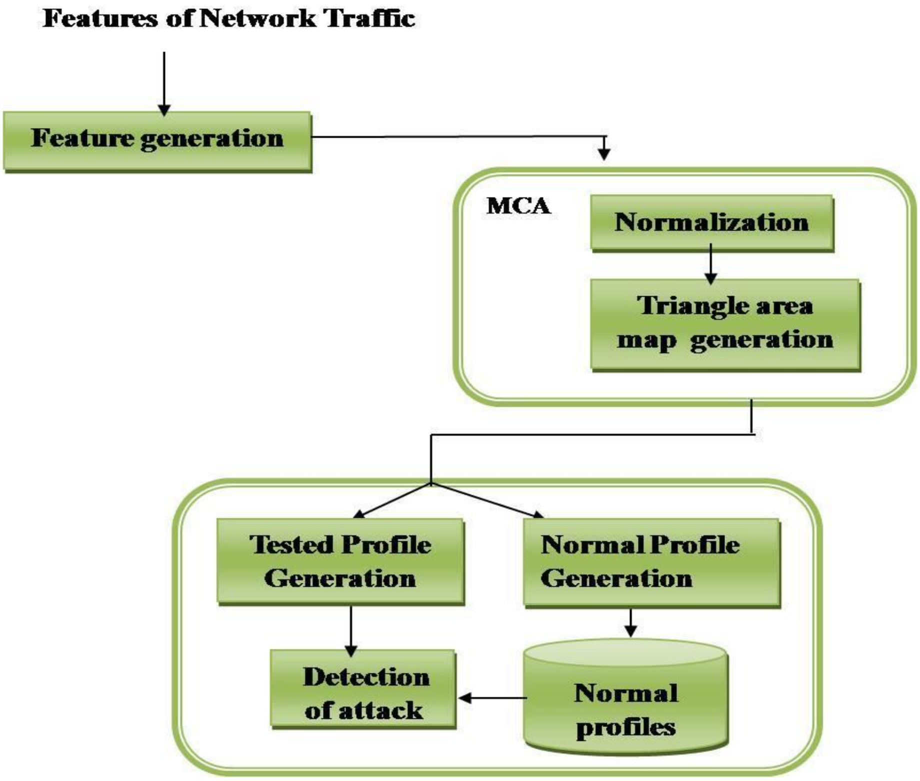

Features of Network Traffic
Feature generation
MCA
Normalization
Triangle area map generation
Tested Profile Generation
Normal Profile Generation
Detection of attack
Normal profiles

Figure 2: System architecture

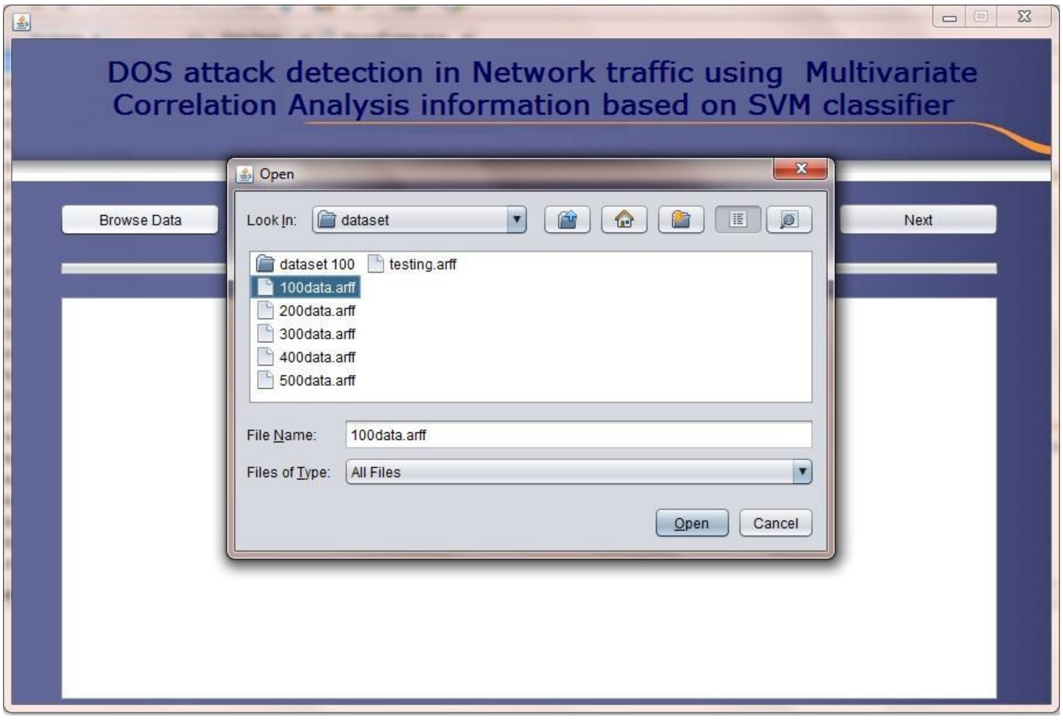
There are 41 features in the dataset. The duration, source bytes, protocol etc are features of dataset. Only useful features of kddcup99 dataset are used in the proposed system. In normalization step the features coming from the network or the features of kddcup99 dataset are normalized to remove bias from the data. The advantage of this is accuracy increases. From literature review, we analyzed that detection rate increases. So normalization of data is used before features are extracted.

3.1 SMO SVM

SMO SVM:

SMO algorithm is used with SVM because of its high speed. It gives high accuracy results. SMO algorithm solves the problem by breaking problem into sub problems and solves the problem analytically. SMO uses Lagrange multiplier for this purpose. Algorithm consists of threshold determination, Lagrange multipliers and heuristic to select the multiplier for optimization.

Results



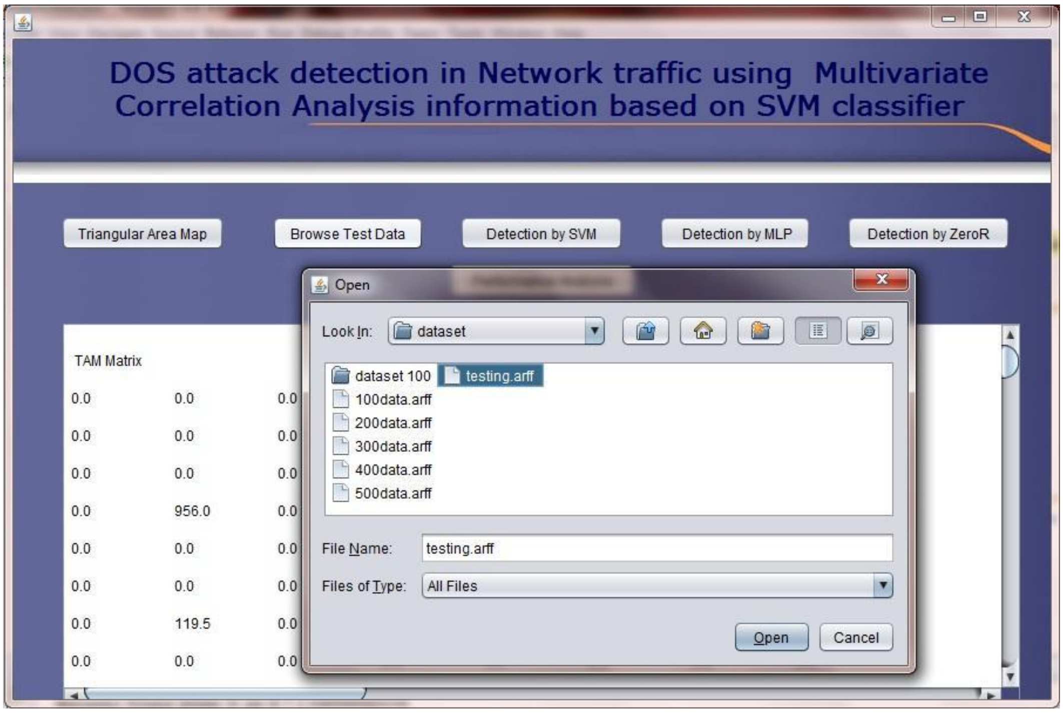
DOS attack detection in Network traffic using Multivariate Correlation Analysis information based on SVM classifier

Look In: dataset

File Name: 100data.arff

Files of Type: All Files

Figure 3: Input dataset instance



DOS attack detection in Network traffic using Multivariate Correlation Analysis information based on SVM classifier

TAM Matrix

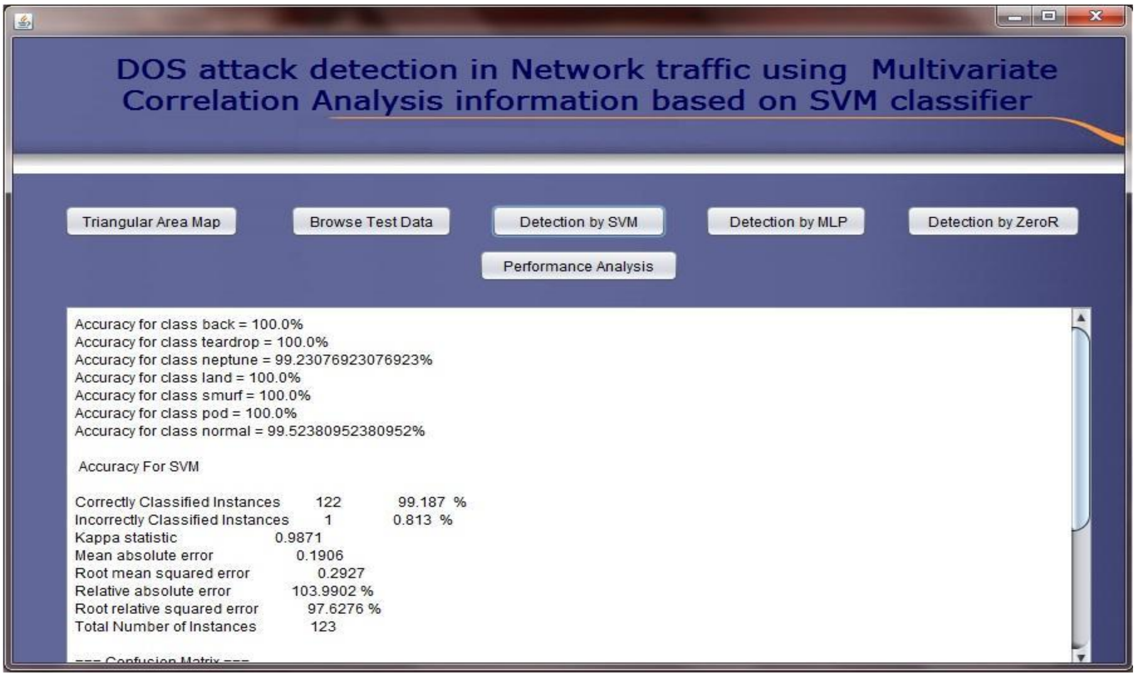
```
0.0    0.0     0.0
0.0    0.0     0.0
0.0    0.0     0.0
0.0    956.0   0.0
0.0    0.0     0.0
0.0    0.0     0.0
0.0    119.5   0.0
0.0    0.0     0.0
```

Look In: dataset

File Name: testing.arff

Files of Type: All Files

Figure 4: testing dataset



DOS attack detection in Network traffic using Multivariate Correlation Analysis information based on SVM classifier

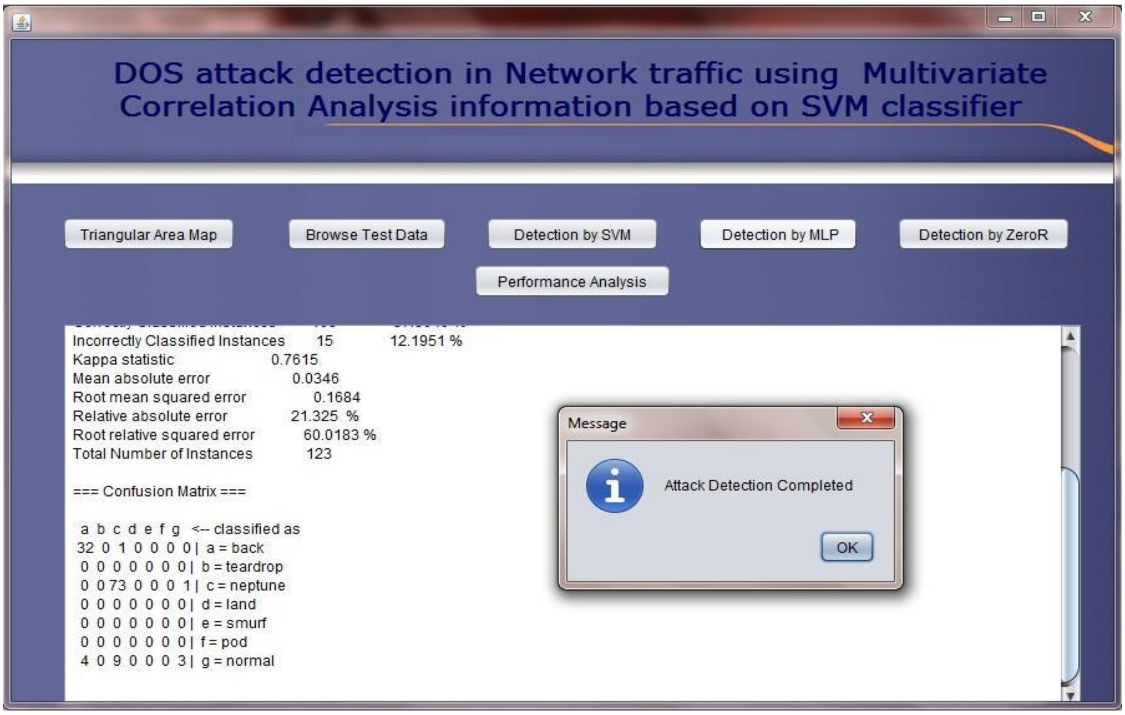
```
Accuracy for class back = 100.0%
Accuracy for class teardrop = 100.0%
Accuracy for class neptune = 99.23076923076923%
Accuracy for class land = 100.0%
Accuracy for class smurf = 100.0%
Accuracy for class pod = 100.0%
Accuracy for class normal = 99.52380952380952%

 Accuracy For SVM

Correctly Classified Instances       122           99.187  %
Incorrectly Classified Instances       1            0.813  %
Kappa statistic                   0.9871
Mean absolute error                  0.1906
Root mean squared error               0.2927
Relative absolute error            103.9902 %
Root relative squared error          97.6276 %
Total Number of Instances            123

=== Confusion Matrix ===
```

Figure 5: Accuracy of attack classification using SVM



DOS attack detection in Network traffic using Multivariate Correlation Analysis information based on SVM classifier

```
Incorrectly Classified Instances      15           12.1951 %
Kappa statistic                   0.7615
Mean absolute error                  0.0346
Root mean squared error               0.1684
Relative absolute error             21.325  %
Root relative squared error          60.0183 %
Total Number of Instances            123

=== Confusion Matrix ===

  a  b  c  d  e  f  g   <-- classified as
 32  0  1  0  0  0  0 |  a = back
  0  0  0  0  0  0  0 |  b = teardrop
  0  0 73  0  0  0  1 |  c = neptune
  0  0  0  0  0  0  0 |  d = land
  0  0  0  0  0  0  0 |  e = smurf
  0  0  0  0  0  0  0 |  f = pod
  4  0  9  0  0  0  3 |  g = normal
```

Message

Attack Detection Completed

Figure 6: Attack detection

Table 1: *Dataset instance analysisummary*

Instances	SMO	MLP	ZeroR
100 instance dataset	99.18%	87.80%	50.40%
200 instance dataset	98.37%	85.36%	53.65%
300 instance dataset	99.18%	86.17%	50.40%
400 instance dataset	99.18%	99.18%	50.40%
500 instance dataset	99.18%	78.04%	50.40%

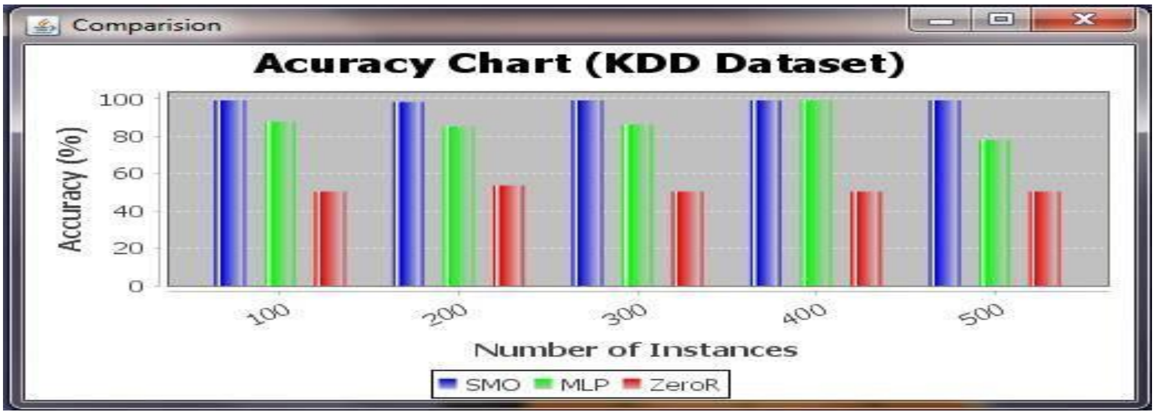


Figure 7: Accuracy of different Methods

4 Conclusion

The proposed system classifies dos attack from normal traffic data by using support vector machine (SVM) algorithm and also uses triangular area based MCA methodology. Our method SMO SVM gives better results than MLP and zeroR methodology. zeroR technique gives very low results.In the proposed system Kddcup99 dataset is used as input data to algorithm. Kddcup99 dataset is well known dataset, many researchers uses this dataset for research purpose.In future work we will use real time data for the evaluation.

References

[1] Dorothy E. Denning “An Intrusion – Detection Model”

[2] Zhiyuan Tan “Detection of Denial-of-Service Attacks Based on Computer Vision Techniques” Thesis Copyright by Zhiyuan Tan, 2013

[3] Zhiyuan Tan, Aruna Jamdagni, Xiangjian He, Priyadarsi Nanda and Ren Ping Liu,“A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis” IEEE transaction on parallel and distributed systems, vol. 25, no. 2, February 2014.

[4] Yu Chen, Kai Hwang, and Wei-Shinn Ku “Collaborative Detection of DDoS Attacks over Multiple Network Domains” IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, vol.18,no.12,pp.1649-1662.

[5] Jaehak Yu, Hansung Lee, Myung-Sup Kim , Daihee Park “Traffic flooding attack detection with SNMP MIB using SVM” Computer Communications,vol. 31,no.17 ,pp.4212–4219, 2008.

[6] Arman Tajbakhsh, Mohammad Rahmati, Abdolreza Mirzaei “Intrusion detection using fuzzy association rules” Applied Soft Computing ,vol. 9 ,pp.462–469, 2009.

[7] Aruna Jamdagni , Zhiyuan Tan , Xiangjian He , Priyadarsi Nanda , Ren Ping Liu “RePIDS: A multi tier Real-time Payload-based Intrusion Detection System”Computer Networks,vol. 57,pp.811–824, 2013.

[8] Dimitris Gavrilis, Evangelos Dermatas “Real-time detection of distributed denial-of-service attacks using RBF networks and statistical features” Computer Networks,vol. 48 ,pp.235–245, 2005.

[9] Christos Douligeris and Aikaterini Mitrokotsa “DDoS attacks and defense mechanisms: classification and state-of-the-art”Computer Networks , vol.44, pp.643–666, 2004.

[10] Yinhui Li , Jingbo Xia, Silan Zhang , Jiakai Yan, Xiaochuan Ai , Kuobin Dai “An efficient intrusion detection system based on support vector machines and gradually feature removal method” science direct Expert Systems with Applications,vol. 39,pp. 424–430, 2012.

[11] Shuyuan Jin,Danial So Yeung and Xizhao “Network intrusion detection in covariance feature space”sciencedirect Pattern Recognition,vol. 40 ,pp.2185-2197, 2007.

[12] S. Yu, W. Zhou, W. Jia, S. Guo, Y. Xiang, and F. Tang, “Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient,” IEEE Trans. Parallel and Distributed Systems, vol. 23, no. 6, pp. 1073-1080, June 2012.

[13] Surat Srinoy,Witcha Chimphlee and Siriporn Chimphlee “A Fusion of ICA and SVM for Detection Computer Attacks” Proceeding of the 5th WSEAS International Conference on Applied Computer Science,Hangzhou,china, (pp987991), April 16-18, 2006.

[14] Fatin Norsyafawati Mohd Sabri and Norita Md.Norwawi et.al “Identifying False Alarm Rates for Intrusion Detection System with Data Mining” IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.4, April 2011

[15] A. M. Riad and Ibrahim Elhenawy “VISUALIZE NETWORK ANOMALY DETECTION BY USING K-MEANS CLUSTERING ALGORITHM” International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.5, September 2013