International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

# Detection of Denial of Service Attack Based on EMD Embedded with 3D Reduction Method

**Swathy Mohan[1], Niyas N.[2]**

Department of Computer Science and Engineering, KMCT College of Engineering and Technology, Calicut, Kerala, India

**Abstract:** ***Denial-of-Service attack is an attempt to make network resources or machine unavailable to its intended users. It can temporarily or indefinitely interrupt or suspend the services of a host connected to the Internet. For the Detection of denial of service attack (DoS) various detection systems are developed. The existing system is based on sophisticated anomaly based system for detecting DoS attacks. But there is a problems occurs in this paper is that it reduces the performance of detecting the denial of service attack also it requires more time for the execution. This proposed system is developed to overcome these problems. To extract the features use SIFT it reduces the time when compared to the existing feature extraction method. The traffic records are trained as attack and non attack or the network traffic records changes the records into the respective images using Multivariate correlation analysis. Network traffic records images are used for the proposed denial of service attack detection system that is developed based on a dissimilarity measure Earth Movers Distance embedded with three dimensional reduction method. By using this method it can also detect the unknown Denial of Service attack. It efficiently measure the distance between trained records and new records. It increases the performance of detection of Denial of service attack and also requires only less time for the computation.***

**Keywords:** Denial of service attack (DoS), Earth mover's distance, Machine learning, Statistical learning

## 1. Introduction

Network attack is an attempt to destroy, expose, alter disable, steal or gain unauthorized access. Denial of service attack is active attacks which attack the services of the system also gain the information from the system. Denial of service attacks is used for exploiting system vulnerabilities of a victim or flooding a victim with a large volume of useless network traffic to occupy the designated resources. The attack detection mechanisms can be divided into two namely misuse-based detection and anomaly-based detection. The misuse detection mechanism can achieve high detection rates in known attacks .But they are incapable of detecting any unknown attacks or even variants of existing attacks. Anomaly-based detection mechanism uses a different detection methodology that monitors and labels any network activities presenting significant deviation from the legitimate traffic profiles as suspicious objects. Thus anomaly-based detection mechanism is able to identify previously unknown attacks.

In the existing systems are based on traditional statistical correlation analysis techniques, capable of studying the correlations between the features in a given sample set. The traditional statistical correlation analysis techniques make these anomaly-based detection systems which is incapable of recognizing individual attack records hidden in a sample set. Various classifiers are used to help improve detection accuracy for classifying normal and attack traffic. In computer vision tasks the technique used are the potential candidates. Image retrieval and object shape recognition are some of the commonalities in attack detection and computer vision task. The queries to image retrieval tasks or object shape recognition tasks are equivalent to normal traffic to attack detection. Object shapes or the images that do not match the queries interpreted the detection of DoS attack. To determine or characterize the traffic records first the basic features are generated from the network traffic packets captured at the destination .Then dimensionality Reduction Based on PCA performs dimensionality reduction using PCA for the training normal traffic records. It does not cause loss of information by the use of PCA which seeks the optimal subspace for the best representation of the data. Subspace selected are used for training and the test phase it can reduces the computational overhead for finding the attack and normal traffic records. It consists of a training phase and a test phase, in the training phase it consist of both attack and normal traffic records. In the test phase new records are comparing with the trained records. When compared with the previous method by using this method it can efficiently distinguish both known and unknown DoS attacks. Thus for detecting the attacks to improve the detection accuracy use the principle of object shape recognition and Earth Movers Distance (EMD) for testing the traffic records. EMD will find the distance between normal and new records and determining whether the record is attack or non attack. But it will decreases the performance also requires high time. Both the performance and time are important factors in the detection of denial of service attack.

To overcome the problems of existing system new project is proposed .Finding similar images to a given query image can be computed by different distance measures. For dimensionality reduction SIFT is used thus it decreases the execution time. To find the distance between normal and attack traffic using EMD embedded with three dimension reduction methods: sampling, sketching, Sampling is a method that picks a small fraction of the image features. Sketching is a distance estimation method that is based on specific summary statistics. Sampling, reduces execution time and sketching method increases the performance of recognition. Thus it can increases the performance and reduces the execution time.

## 2. Detection of Denial of Service Attack

Network traffic records are given as input. Then the image is generated based on traffic records with packet counts also with the number of flow. Then find the subspace using the method SIFTS. It extracted the dominant features from the image. After that the records are It arrange the records into legitimate and illegitimate. After training phase the test phase is occurred the new records are matching with distance measure method. Thus it can identify the denial of service attack and normal traffic records.

The various Earth movers distance techniques for the distance measure.EMd,EMDl1 are the some of the earth movers distance method. EMD has proven its ability to retrieve similar images in an average precision, it requires high execution time .It is one of the major drawback of EMD. The another drawback of EMD is that if any previously unknown attack is occurred it cannot detect the attack. Embedding EMD into L1 is a solution that solves this problem by sacrificing performance. It can also useful in the case of previously unknown attack. Thus it decreases the execution time but the performance will be low. To reduce the execution time of embedded EMD and increase its performance using three dimension reduction methods are proposed in this paper. Thus it satisfy both the execution time and performance.

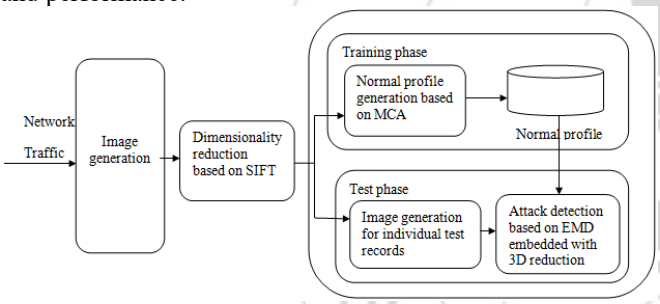



**Figure 1:** Denial of service attack detection system

The proposed project EMD embedded with three dimensional reduction method which can reduces the execution time and increases the performance. In this project SIFT is employed in the new detection system to reduce the dimensionality (noise) of data it also extract the features from the image. When compared with the existing method this method reduces the time complexity.

The distance measure EMD-l1 reduces performance also it requires more time .The proposed record method EMD embedded with 3D reduction method which categorizes the normal and attack traffic records.It consists of a method sketching. Sketching that used for finding the distance between selected samples. Thus it can differentiate attack traffic and normal traffic. It can increases the performance and reduces the time complexity. The proposed project consist of following steps:

- Image generation
- Feature extraction
- Training records
- Testing

### 2.1 Image Generation

In this step, basic features or image are generated from network traffic packets captured at the destination network. Then, they are applied to construct records describing statistics for a well defined time interval. Image is generated based on the network traffic record Kdd cup 99 dataset. The image is generated for each individual data's with the 32 attributes in the dataset. The image size is 4*8 matrix

### 2.2 Optimal subspace generation

This step performs dimensionality reduction using SIFT for the training normal traffic records. The feature reduction techniques, our dimensionality reduction algorithm do not cause loss of information by the use of SIFT which seeks the optimal subspace for the best representation of the data. It reduce the computational overhead. The key points is extracted from the image. The selected key points are mapped to a new subspace. Thus it reduces the dimensionality and it does not cause any loss of data.

### 2.3 Training Phase

In this stage the normal records are trained using multivariate correlation analysis. It consist of both normal and attack traffic for the training. Select two distinct features and obtain triangle for each two different features. This method can efficiently sort out the legitimate and illegitimate traffic records.

### 2.4 Test Phase

In the test phase the new records are tested with the trained records. The distance is measured using EMD embedded with 3D reduction method sketching. Sketching which find the distance between the trained and test records, It can efficiently differentiate denial of service attack and normal records.

## 3. Implementation and Analysis

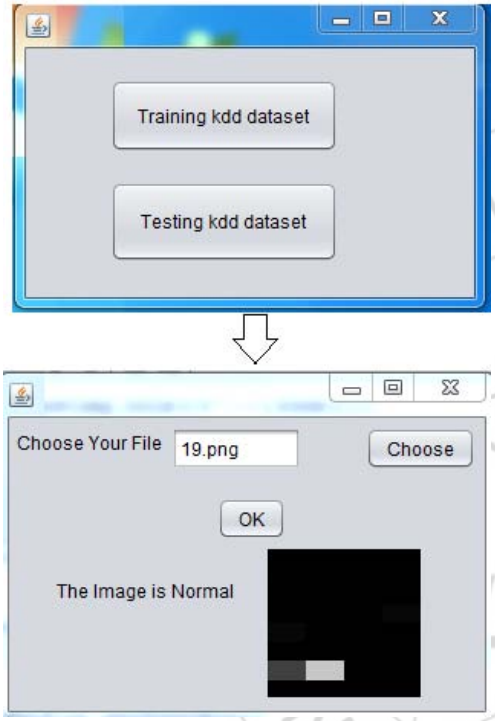
To determine real time denial of service attack is one of the main problem occurs. There are several existing methodologies to find out the denial of service attack. But every method has its own drawbacks. Based on the existing drawbacks, detection of denial of service attack based on EMD embedded with 3D reduction method is proposed to recognize the denial of service attack. By using these method it can effectively and efficiently identify the denial of service attack. Existing method cannot classify normal traffic and attack traffic it can only classify when it is previously known attack. Thus it reduces the performance of detecting the denial of service attack. Also requires high execution time for the computation.

To solve these problem EMD embedded with three dimensional reduction method is used .This method can efficiently distinguish normal traffic and attack traffic .In the proposed method first image is constructed,then the feature is extracted using SIFT. After that in the training phase the

records are trained using multivariate correlation analysis .It consist of both attack traffic and normal traffic. The distance measure EMD embedded with three dimension reduction method is used for finding the distance measure between normal and new records. The distance is find using method sketching. These methods are more efficient than previous method. It is able to detect the attack even it is not previously occurred. It increases the performance of detection of denial of service attack.

### 3.1 Integrated Result

The given figure shows the initial input and final result. First the dataset is trained and at last testing the records with the trained records.



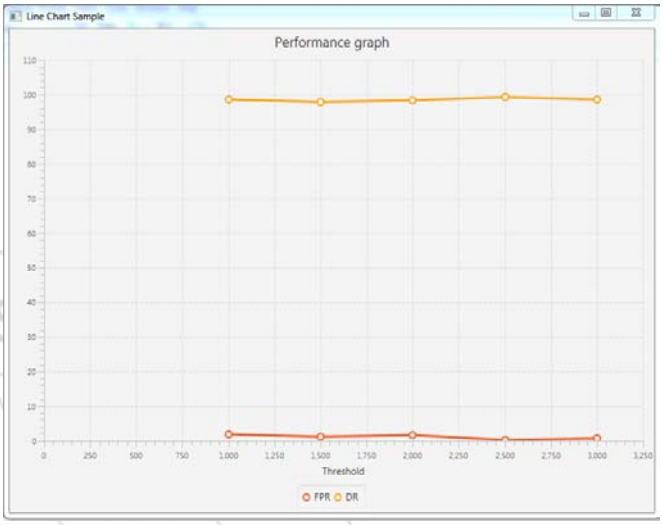

First the image is generated from the dataset. The image is generated for each individual data's with the 32 attributes in the dataset. The image size is 4*8 matrix .Then the constructed image use for the testing the record using the method Multivariate correlation analysis. In MCA Select two distinct feature and Obtain triangle with the selected feature. The selected points are mapped into a Cartesian coordinate system. Then obtain a triangle with an origin and selected points. Find the area of the triangle. In testing records choose the image then using the method sketching it shows the image is denial of service attack or normal record.

### 3.2 Performance Graph

In the proposed method the false positive rate is low and the detection rate is high

## 4. Conclusion

The problem occurs in the previous paper is that it requires high execution time for the computation also it is difficult to differentiate the denial of service attack and normal traffic. To solve these problems proposed method EMD embedded with 3D reduction method was developed. In this method it can efficiently determine real time denial of service attack. It also requires only less time for the computation when compared with the previous method. In the EMD embedded with three dimensional reduction method Initially the image is constructed. Then find the optimal subspace. Trained the network traffic records. Testing records with the trained records. When compared with the previous method the proposed system can efficiently detect denial of service attack also it requires only less time for the computation.




## 5. Future Scope

As the future scope, a new distance measure method DREAT will be invented based on the detection approach proposed in this paper. The new method DREAT will efficiently differentiate the denial of service attack and normal traffic.

## References

[1] M. Bando, N. S. Artan, and H. J. Chao, "Scalable Lookahead Regular Expression Detection System for Deep Packet Inspection," Networking, IEEE/ACM Transactions on, vol. 20, no. 3, pp. 699-714, 2012.
[2] M. Thottan, and C. Ji, "Anomaly detection in IP networks," Signal Processing, IEEE Transactions on, vol.51, no. 8, pp. 2191-2204.
[3] A. Patcha and J. M. Park, "An Overview of the Anomaly Detection Techniques: Existing Solutions and Latest Technological Trends ,"Computer Networks, vol. 51, pp. 3448-3470, 2007.
[4] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R. Liu, "A System for Denial of Service Attack Detection Based on Multivariate Correlation Analysis"Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 2,pp.447-456, 2014.
[5] Y. Rubner, C. Tomasi, and L. Guibas, "The Earth Mover's Distance as a Metric for the Image Retrieval,"International Journal of Computer Vision, vol. 40, no. 2, pp. 99-121, 2000/11/01, 2000.
[6] J.Xu, Z. Zhang, A. K. H. Tung, and G. Yu, "Efficient and effective of similarity search over probabilistic data based Earthmover's distance " The VLDB Journal, vol. 21, no. 4, pp. 535–559, 2012.

[7] R. Batra and L. Hesselink, "Feature comparisons of the 3-D vector fields using Earth mover's distance," in Proceedings of the IEEE Visualization '99, pp. 105–114, IEEE Computer Society Press, October 1999.
[8] Hindawi Publishing Corporation" Image Matching Using Dimensionally Reduced Embedded Earth Mover's Distance "Journal of Applied Mathema Volume 2013, Article ID 749429, 11 pages .
[9] H.H. Crokell, "Specialization and International Competitiveness," in Managing the Multinational Subsidiary, H. Etemad and L. S, Sulude (eds.), Croom-Helm, London, 1986. (book chapter style)
[10] K. Grauman and T. Darrell, "Fast contour matching using approximate Earth mover's distance," inProceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR '04), vol. 1, pp. I220–I227, July 2004
[11] S. J. Stolfo, W. Fan, W. Lee, A. Prodromidis, and P. K. Chan, "Costbased modeling for fraud and intrusion detection: results from JAM project"in DARPA Information Survivability Conference and Exposition2000 DISCEX '00. Proceedings, 2000, pp. 130-144 vol.2.

## Author Profile

**Swathy Mohan** completed her bachelor of engineering in computer science and engineering in 2014, from Paavai College of engineering Salem. She currently doing master degree in computer science and engineering in Kmct college of engineering Calicut university.

**Niyas N** He completed master degree in computer science and engineering from KMCT College of Engineering in year 2014.Now he is an Assistant Professor, Department of Computer Science and Engineering, in KMCT College of Engineering, Calicut University.