OPEN ACCESS

*International*
*Journal*
*Of Modern Engineering Research (IJMER)*

# Detection and Mitigation of Denial of Service Attack In Interconnected Systems

[1]Mr.V.Elaiyaraja [2]Mrs.R.Kalaiselvi
[1,2]*Asst.Prof,Department Of Information Technology Arasu Engineering College, Kumbakonam*

***ABSTRACT:*** *Denial of service is one of the most important and severe attack in the interconnected systems.In this paper, we present a DoS attack detection and mitigation.the detection system that uses Multivariate Correlation Analysis (MCA) for accurate network traffic characterization by extracting the geometrical correlations between network traffic features. Our MCA-based DoS attack detection system employs the principle of anomaly-based detection in attack recognition and the mitigation system uses the IP-trace back algorithm. The effectiveness of our proposed detection system is evaluated using KDD Cup 99 dataset, and the influences of both non-normalized data and normalized data on the performance of the proposed detection system are examined.*

***Keywords:*** *Denial-of-Service attack, network traffic characterization, multivariate correlations, triangle area map,Ip-trace back algorithm.*

## I. INTRODUCTION:

DENIAL-OF-SERVICE (DoS) attacks are one type of aggressive attack. DoS attacks severely degrade the availabil- ity of a victim, which can be a host, a router, or an entire network.They impose intensive computation tasks to the victim by exploiting its system vulnerability or flooding it with huge amount of useless packets. The victim can be forced out of service from a few minutes to even several days..This causes serious damages to the services. Therefore, effective detection and mitigation of DoS attacks is essential to the protection of online services.

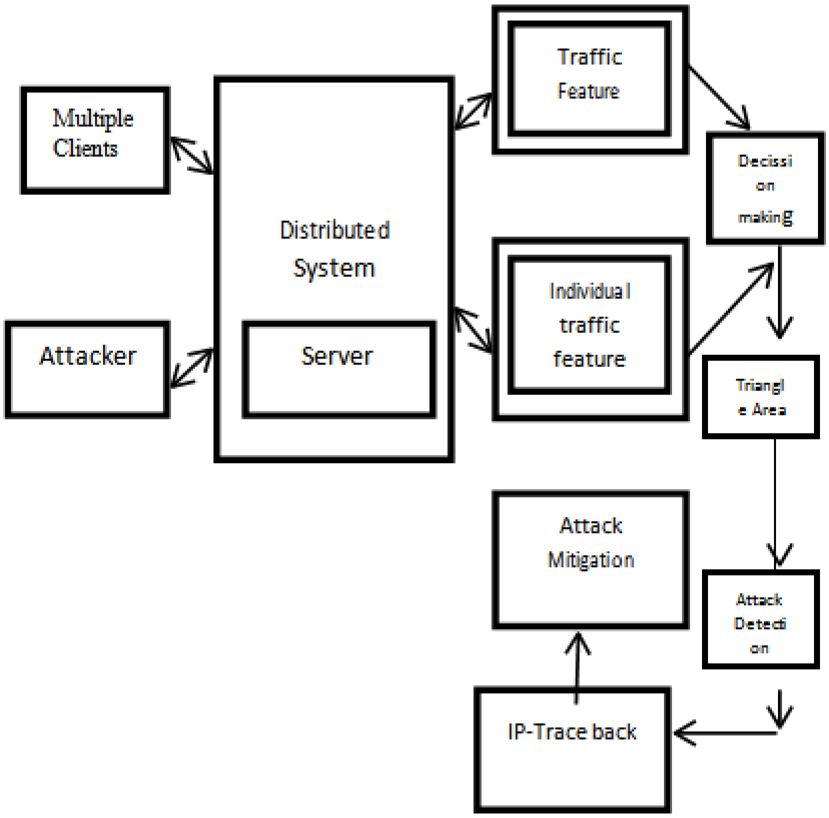
DoS attack detection mainly focuses on the development of network-based detection mech- anisms. Detection systems based on these mechanisms monitor traffic transmitting over the protected networks. Moreover, network-based detection systems are loosely coupled with operating systems running on the host machines which they are protecting. As a result, the configurations of network- based detection systems are less complicated than that of host- based detection systems.Generally, network- based detection systems can be classified intotwo main categories, namely misuse- based detection systems and anomaly-based detection systems . Misuse-based detection systems. In spite of having high detection rates to known attacks and low false positive rates, misuse- based detection systems are easily evaded by

features. non-payload- based DoS detection approach using Multivariate Correlation Analysis(MCA).Following this emerging idea,we present a new MCA-based detection system to protect online services against DoS attacks in this paper, which is built upon our previous work . In addition to the work shown, we present the following contributions in this paper. First, we develop a complete framework for our proposed DoS attack detection system . Second, we propose an algorithm for normal profile generation and an algorithm for attack detection. Third, we proceed a detailed andfeatures.addition, this approach can only label an entireattacks that linearly change all monitored In group of observed samples as legitimate or attack traffic but not the individuals in the group.improves detection ac- curacy, it is vulnerable to To deal with the above problems, an approach based on triangle area was presented in todesigned in to mine the multivariate correlation for sequential samples. Although the approach generate bet- ter discriminative complete mathematical analysis of the proposed system and investigate further on time cost. As resources of interconnected systems (such as Web servers, database servers, cloud computing servers etc.) are located in service providers'detection, which monitors and flags any network activities pre- senting significant deviation from legitimate traffic pro- files as suspicious objects.security expertise. Owing to the principle of a covariance matrix based approach was Localmanual process and heavily involves network Area Networks that are commonly constructed using the same or alike network underlyinglabor intensive task to keep signature database updated because signature generation is a infrastructure and are any new attacks and even variants of the existing attacks. Furthermore, it is a complicated and detection system can provide effective protection to all of these systems by considering their commonality.Then for mitigation,in this paper we are using the Ip-tracback algorithm com- pliant with the underlying network model, our proposed.

## II. RELATED STUDY

In this paper,the author(P.Garca-Teodora et. Al.) discussed about Anomaly-based approaches are efficient, signature-based detection is preferred for mainstream implementation of intrusion detection systems and the issues in this paper the reason why industries don□t favor the anomaly-based intrusion detection methods can be well understood by validating the efficiencies of the all the methods [1].Then in this paper the author(Keunsoo Lee et. Al) discussed a method for proactive detection of DDoS attack by exploiting its architecture which consists of the selection of handlers and agents, the communication and compromise, and attack was proposed.It having ability to detect the attack only proactive detection[2].In the next paper ,the author(LifangZi et. al.) discussed about the novel adaptive clustering method combined with feature ranking for DDoSattacks detection.Recalculating the cluster and feature identification makes morecomplex.[3].In this paper the author(C.F.Tsai and C.Y.Lin) discussed about the A hybrid learning model based on the triangle area based nearest neighbors (TANN) has proposed in order to detect attacks more effectively.Traditional detection approaches neglect the correlationinformation contained in groups of network traffic samples which leads to their failure to improve the detection effectiveness.[4].In the next paper the author(V.Paxson) discussed about the stand- alone system.

## III. SYSTEM ARCHITECTURE



### 3.1 System Study

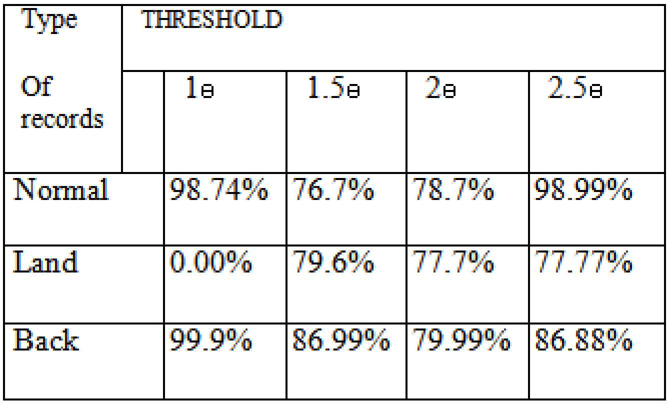
Concentrating only on relevant inbound traffic. This also enables our detector to provide protection which is the best fit for the targeted internal network because legitimate traffic profiles used by the detectorsared eveloped for a smaller numberof network services. The detailed process can be found in Step 2 is Multivariate Correlation Analysis, in which the “Triangle Area Map Generation” module is applied to extract the correlations between two distinct features within each traffic record coming from the first step or the traffic record normalized by the “Feature Normal-ization” the destination network reduce the over head of detecting malicious activities by concentrating only on relevant inbound traffic. This also enables our detector to provide protection which is the best fit for the targeted internal network because The whole detection and mitigation process consists of three major steps as shown in Fig. 1. The sample-by-sample detection mechanism is involved in the whole detection phase( i.e., Steps 1, 2,3 and 4) . In Step 1, basic features are generated from ingress network traffic to the internal network where protected servers reside in and are used to form traffic records for a well-defined time interval. Monitoring and analyzing at module in this step (Step 2). The occurrence of network in trusions cause changes to these correlation so that the changes can be used as indicators to identify the intrusive activities. All the extracted correlations, namely triangle areas stored in Triangle Area Maps (TAMs), are then used to replace the original basic features or the normalized features to represent the traffic records. This provides higher discriminative information to differentiate between legitimate and illegitimate traffic records.Our MCA method and the feature normalization tech- nique are explained . In Step 3, the anomaly-based detection mechanism is adopted in Decision Making. It facilitates the detec- tion of any DoS attacks without requiring any attack relevant knowledge. Furthermore, the legitimate traffic profiles used by the detectorsare developed for a smaller number of network services. The detailed process can be found inStep 2 is Multivariate Correlation Analysis, in which the “Triangle Area Map Generation” module is applied to extract the correlations between two distinct features within each traffic record coming from the first step or the traffic record normalized by the “Feature Normal- ization labor-intensive attack analysis and the frequent update of the attack signature database in the case of misuse-based detec- tion are avoided. Meanwhile, the mechanism enhances the robustness of the proposed detectors and makes them harder to be evaded because attackers need to generate attacks that match the normal traffic profiles built by a specific detection algorithm. This, however, is a labor-intensive task and requires expertise in the targeted detection algorithm. Specifically, two phases (i.e., the “Training Phase” and the “Test Phase”) areinvolved in Decision Making.

The effectiveness of our proposed detection system is evaluated using KDD Cup 99 dataset, and the influences of both non- normalized data and normalized data on the performance of the proposed detection to be examined.

classifier is employed in the “Attack Detection”module is used in the “Test Phase” to build profiles for individual observed traffic records. Then, the tested profiles are handed over to the “Attack Detection” module, which compares thegenerated normal profiles are

The “NormalProfile Generation” module is operated stored normal profiles.A threshold individual tested profiles stored in a database. The “Tested Profile Generation”with the respective module to distinguish DoS attacks from legitimate traffic.Formitigation,we are using the Iptracebackalgorithm,here the IP addresses are tracked and the attacker can be found.In(step 4)Attack mitigation is performed using the Ip-trace back algorithm.

**TABLE-1 Computational Analysis**



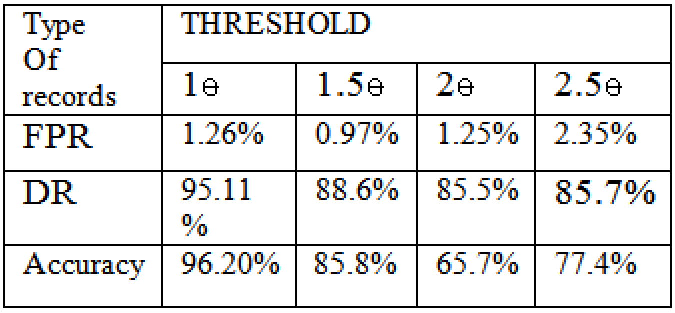
| Type Of records | THRESHOLD | | | |
|---|---|---|---|---|
| | 1θ | 1.5θ | 2θ | 2.5θ |
| Normal | 98.74% | 76.7% | 78.7% | 98.99% |
| Land | 0.00% | 79.6% | 77.7% | 77.77% |
| Back | 99.9% | 86.99% | 79.99% | 86.88% |

## IV. Implimentation Results:

In this paper,we have implemented the detection and mitigation of denial of service attack.Here,we have several users and each user can access the system by giving their login credentials such as user name,IP address of the system and the IP address of the Server.After that if the user is an legitimate user then the server will give an authorized code and the user by entering the authorized code can access the files and datas.then we introduce the attacker there bycan be detected and after the detection of denial of service attackgiving request from the same system again and again and there occurs the network traffic and that must be analysed using the muti-variatecoorelation analysis and by triangle area map generation. Mitigation done by IP-Traceback algorithm.

The system which senda request from the same Ip address is traced by traffic analysis and that will be the attacker.mitigation and detection can be implemented.

**TABLE-2 Computational Analysis by various records**



| Type Of records | THRESHOLD | | | |
|---|---|---|---|---|
| | 1θ | 1.5θ | 2θ | 2.5θ |
| FPR | 1.26% | 0.97% | 1.25% | 2.35% |
| DR | 95.11 % | 88.6% | 85.5% | 85.7% |
| Accuracy | 96.20% | 85.8% | 65.7% | 77.4% |

## V. CONCLUSION

This paper has presented a MCA-based DoS attack de- tection and attack mitigation system which is powered by the triangle-area- based MCA technique and the anomaly-based detection technique The former technique extracts the geometrical correlations hidden in individual pairs of two distinct features within each network traffic record, and offers more accurate characterization for network traffic behaviors. The latter technique facilitates our system to be able to distinguish both known and unknown DoS attacks from legitimate network traffic. Evaluation has been conducted using KDD Cup 99 dataset to verify the effectiveness and performance of the proposedDoS attack detection system. The in fluence of original (non- normalized) and normalized data has been studied in the paper. The results have revealed that when working with non-normalized data,our detection system achieves maximum 95.20% The problem, however, can be solved by utilizing statistical normalization technique to eliminate the bias from the data. The results of evaluating with the normalized data have shown a more encouraging detection accuracy of 99.95% and nearly 100.00% DRs for the various DoS attacks. Besides, the comparison result has proven that our detection system outperforms two state-of-the-art approaches in terms of detection accuracy. Moreover, the computational com- plexity and the time cost of the proposed detection system have been analyzed. The proposed system achieves equal or better performance in comparison with the two state- of-the-art approaches. To be part of the future work, we will further test our DoS attack detection system using real world data and employ more sophisticated classification techniques to further alleviate the false positive rate it does not work.

## REFERENCES

[1]. V.Paxson,“Bro:ASystemforDetectingNetwok IntrudersinReal- time,” Computer Networks, vol. 31, pp. 2435-2463, 1999

[2]. P. Garca-Teodoro, J. Daz-Verdejo, G. Maci- Fernndez, and E. Vzquez, “Anomaly-based Network Intrusion Detection: Tech- niques, Systems and Challenges,” Computers & Security, vol. 28, pp. 18-28, 2009

[3]. D. E. Denning, “An Intrusion-detection Model,” IEEE Transactions on Software Engineering, pp. 222-232, 1987

[4]. K. Lee, J. Kim, K. H. Kwon, Y. Han, and S. Kim, “DDoS attack detection method using cluster analysis,” Expert Systems withApplications, vol. 34, no. 3, pp. 1659-1665, 2008.

[5]. S. Jin, D. S. Yeung, and X. Wang, “Network Intrusion Detection in Covariance Feature Space,” Pattern Recognition, vol. 40, pp. 2185- 2197, 2007.

[6]. C.F.TsaiandC.Y.Lin,“ATriangle Area Based Nearest Neighbors Approach to Intrusion Detection,” Pattern Recognition, vol. 43, pp. 222-229, 2010.

[7]. A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis,Zhiyuan Tan, ArunaJamdagni,Xiangjian He‡, Senior Member, IEEE, Priyadarsi Nanda, Member, IEEE, and Ren Ping Liu, Member, IEEE,