# IMPLEMENTATION OF VARIETY ASSOCIATION ANALYSIS FOR DENIALOF-SERVICE ATTACK DETECTION

Mr. Sachin Jalindar Runwal[1], Prof. Vidya Jagtap[2]

[1] *M.E. Computer Engineering Department Student, G.H. Raisoni College of Engineering & Management Ahmednagar.*
[2]*Assistant Professor, G.H. Raisoni College of Engineering & Management, Ahmednagar.*

**ABSTRACT**

*Net servers, data servers, cloud computing servers and so forth, are inter- connected techniques and they're currently beneath threads from network attackers. Collectively of commonest and aggressive means that, Denial-of-carrier (DoS) attack reason severe impact on these computing methods. Throughout this paper, we tend to gift a DoS assault detection approach that uses Variety Association Analysis for right community site visitors characterization via extracting the geometrical correlations between network visitors choices. Those DoS attack detection procedure employs the precept of anomaly- situated detection in attack cognizance. This makes our answer ready of detective work satisfactory-known and unknown DoS attacks easily through finding out the patterns of official network site visitors completely .What is extra, a triangle-area-based procedure is projected to give a boost to and to hurry up the procedure of evaluation. And for that reason the influences of each non-normalized expertise and normalized skills on the efficiency of the projected detection process are examined. On this paper we use a naïve-bayes classifier for attack detection which finely become aware of attacker percent . Also our experimental outcome taken on real dataset and hence the influences of every non-normalized expertise and normalized advantage on the performance of the projected detection method are examine.*

**Keyword**: - *Denial of Service Attack, Network traffic, Triangle area, Variety Association Analysis*

## 1. INTRODUCTION

DENIAL-OF-SERVICE attacks are one form of menacing intrusive habits aggressive and for online servers. DoS attacks severely reduce the provision of a sufferer, which could be a node, a router, a host, or an whole community. They inflict intensive calculation duties to the victim by way of flooding it with colossal amount of vain packets or exploiting its method vulnerability. The sufferer will also be compelled out of the service from a several days to even couple of minutes. It motives severe damages to a offerings walking on the sufferer. Thus, mighty finding of DoS attacks is principal to a safeguard of online offerings. Work on DoS attack detection the important makes a specialty of the development of community head quartered detection strategies. Detection programs situated on these strategies monitor transmitting visitors over blanketed networks. These mechanisms release the covered on-line servers from the monitoring assaults and make certain that the servers can devote themselves to furnish first-rate services with minimum delay in response. Distributed opportunistic scheduling(DOS) is inherently more complicated than conventional opportunistic scheduling due to the absence of a central entity that knows the channel

state of all stations [6].Interconnected systems, such as cloud computing servers database servers and web servers etc., are now under threads from network attackers. As one of most common attack is Denial of Service (DoS) these attacks cause serious impact on the computing system [8].Denial Of Service(DOS) attacks are limitless chance to web sites and among the many hardest protection issues in at presents web. The difficulty of DoS attacks has turn out to be well identified, but it has been intricate to discover the Denial of service in the web. Disbursed Denial of provider (DDoS) attacks is a significant-scale, coordinated attack on an availability of offerings of a victim approach or network useful resource, launched not directly by means of many compromised computers on the net. Researchers have provide you with increasingly specified solutions to a DDoS trouble. With DOS, stations [9] use random access to dispute for the channel and upon winning a competition, they measure the stipulations of channel. After measuring a channel stipulations it offers up the transmission possibility if channel first-rate is just not good; in any other case, the station best transmits if the channel first-class is just right. For egocentric customers the allotted nature of DOS makes it prone. A selfish user can acquire a better share of wireless assets at expenditures of good-behaved users by making use of more transmission possibilities and deviating from.

## 2. OVERVIEW OF DOS ATTACKS

### 2.1 Denial of Service Type

A Denial of Service attack is characterized by the attackers to prevent legitimate users of a service by an explicit attempt from using that service. Examples include, attempts to disrupt connections between two machines thereby preventing access to the service, attempts to flood a network, thereby preventing legitimate network traffic. Attempts to prevent the particular individual from accessing a service, Attempts to disrupt service to the specific system or person. Maintaining Integrity of the Specifications [10]. The following figure shows the basic structure of Denial of Service Attack. The DoS structure consists of three components as Attacker, Internet and the target on which the attacker can attack for prevention of user from its service access.

**DoS Attacks**

DoS attacks a single machine can sent a huge number of malicious packets, with the purpose of exhausting a targets networking resources and computational, or crashing the target. The aim of such attacks is to despoil appropriate access of users to the targets services**.** In a DoS attack, one internet connection and one computer is used to flood a server with packets, with the purpose of overloading the targeted servers bandwidth and resources [10].Following are the different DoS Attack classification.

- **Network Device Level**: DOS attacks in the Network Device Level include attacks that might be caused either by taking the advantage of bugs in software or by trying to exhaust the hardware resources of network devices [10].
- **Operating System Level**: In an OS Level DOS attacks take advantage of the ways operating systems implement protocols [10].
- **Application based attacks**: A great number of attacks try to settle a machine or a service out of the order either by taking advantage of specific bugs in network applications that are running on the target host or by using such applications to dram a resources of their victim [10].
- **Data Flooding**: An attacker may attempt to use a bandwidth available to a network, host or device at its greatest extent, by sending massive quantities of data and so causing it to the process extremely large amounts of data [10].
- **Attacks based on protocol features**: DOS may take advantage of certain standard protocol features, for example the several attacks exploit a fact that source addresses can be spoofed [10].

## 3. RELATED WORK

There are different Denial Of service Attack detection ways proposed by various researchers which have some advantages over and vice-versa. There are various way used like K-map, combination of stateful and stateless signature with trace back technique,game-theoretic, Variety Association Analysis.

Qiuming A. Zhu ,Suseela T. Sarasamma ,and Julie Huff[2] put a diffrent K-Map multilevel hierarchical structure for an intrusion detection each step of the hierarchical map is organized as the simple winner takes all K-Map. One most important competencies of this K-Map multilevel hierarchical is its calculation ability. Apart from different statistical inconsistency detection methods comparable to okay-method clustering or probabilistic evaluation, nearest neighbor technique that interact distance size in a characteristic interval to respect the outlines our request does not raise luxurious factor to factor calculations in organizing an information into clusters. A different competencies is community size diminished. It uses the grouping efficiency of the K-Map for detecting anomalies on selected dimensions of information set. Randomly selected data subsets that include both the assaults and average documents from a KDD Cup knowledge are used to instruct the hierarchical net.

The paper [2] illustrate the multilevel hierarchical Kohonen self-ordering map (K-Map) to implement an inconsistency based intrusion detection system they did our testing and training using the pre -processed KDD Cup data set. The experiment was done in two levels. Firstly we used a single level winner takes all K-Map to do a development of IDS.

John Haggerty, Madjid Merabti and Qi Shi [3], can combines both stateless and stateful signature to furnish early discovering of the DoS attack due to this corporation network is guard. This paper is as a rule focuses on how area centered way response to an assaults is utilized by mechanism to block visitors attack. This new resolution is allows for the blockage of the attack to be regularly propagated handiest by way of affected domains towards the attack sources.

Joerg Widmer, Andres Garcia Saavedra ,Albert Banchs and Pablo Serrano [6], derive game theory We tackle the situation of selfishness from a game-theoretic standpoint in DoS . They recommend algorithm that satisfies the following homes: a) wireless network is driven to the most suitable factor of operation when all the stations put in force the algorithm and b) a number of selfish stations are not able to obtain any achieve by using deviating from an algorithm.

Randolph Marchany, Jung-Min Park and Ruiliang Chen[4], think on mitigation of attack plan actively strangle traffic attack produced attacks in Distributed Denial of Service(DDoS). In such paper presents Attack Diagnosis (AD), a mitigation of attack scheme that adopts a divide and conquer method.Packet marking and pushing standards are mixed in advert, and its architecture is in chain with the ideal DDoS attack countermeasure sample for finding attack is performed near the packet filtering and sufferer node is finished just about the attack of sources.

Gautam Thatte, and John Heidemann ,Urbashi Mitra, Fellow [7] , introduce parametric way to find network anomalies using contrast to other works requiring flow
separation in only aggregate traffic statistics, even if anomaly of total traffic is a small unit.Through adopting easy statistical items for heritage traffic and anomalous in the area of time.You can actually forecast standard parameters in the actual time, hence to preclude the need for handbook parameter
tuning or long training segment. Additionally, it uses each traffic-expense yielding a bivariate requirements and packet size information that ignore most false positives.

## 4. PROPOSED WORK

The main aim is DoS attack detection system that uses Variety Association Analysis for accurate network traffic characterization by extracting the geometrical correlations between network traffic features. My VAA-based DoS attack detection system is the type of anomaly based detection in attack recognition. Which detects known as well as unknown attacks without any prior knowledge of attacks? Specifically,
the following problems have been addressed:

A. Variety Association Analysis.
B. Common Profile Generation.
C. Detecting Attack.

**Task A** is Variety Association Analysis, in which it generate Triangle Area Map(TAM) this module is applied to extract the association between two different features within each network traffic records getting by Normalization.
**Task B** represent all the extracted association which is stored by Triangle Area Maps, it used to exchange the basic original features present in network traffic. This gives information to shows the differences between legitimate networks traffic records and illegitimate networks traffic records.

**Task C** is used Decision Making. It uses the detection of any kind of DoS attacks without requiring knowledge of attack. Furthermore, gives attack analysis and the time to time update of the attacks signature for avoiding misuse detection.

A. Algorithm For Normal Profile Generation

In this algorithm the ordinary profile pro is built via the density estimation of the MDs between all authentic training traffic records (TAM common, r, lower) and the expectation (TAM common, lower) of the g traffic records

Step 1: Network traffic records as Input.
Step 2: Every records Original Features extraction.
Step 3: Triangle area concept is apply to extracting the geometrical association with the pth and qth record in the vector zi.
Step 4: Normal and simple profile generation with the VAA.

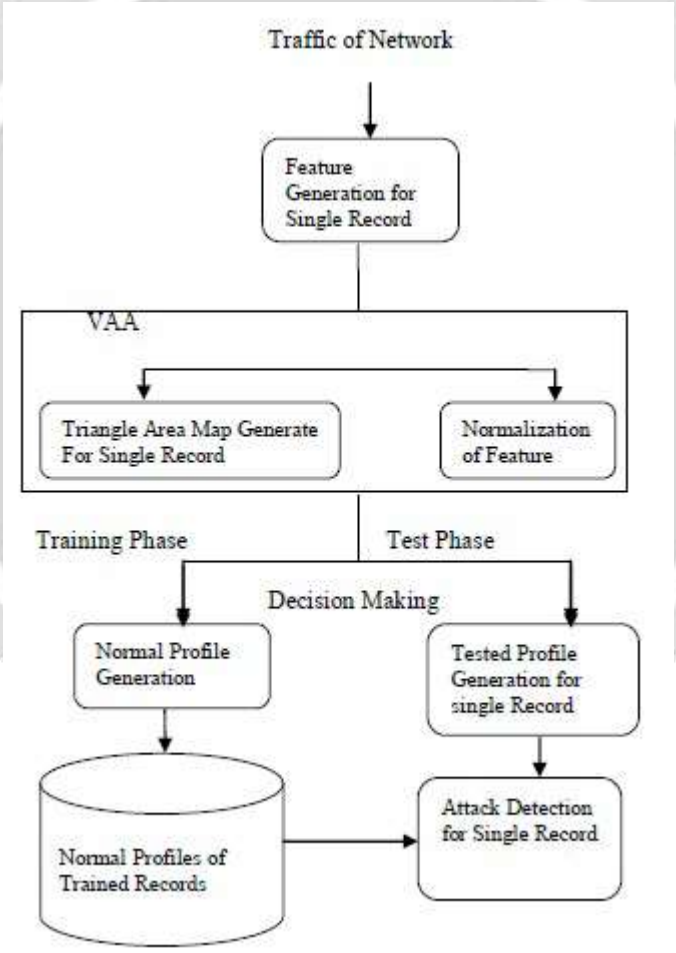


Fig 1 System Architecture

1. For every records it generate triangle area map.
2. Matrix (covariance) generates.
3. MD Calculation between input traffic records TAM and

TAM record.
4. Calculate mean
5. Calculate deviation.
6. Value (Pro) return.
Step 5: Attack Detection
1. Input: Given network traffic, alpha and actual profile.
2. Calculate TAM for input network traffic records.
3. Calculate MD's between actual profile generated and
Input network traffic records.
4. If MD < Thr(Threshold)
Detect Simple Normal
Else
Detect Attack.

B. Naive Bayes Algorithm Attack detection
This algorithm is used for different purpose.
Step 1: This task is used to classify arriving packets, it will decide different class label for packets, depends on the existing networks traffic records.
Step 2: Calculate probability (Prior), new Packet classification completed.
Step 3: Calculate among all network traffic records the number of points in the packet.
Step 4: To form the posterior probability for the final classification it combines two information sources.

C. Mathematical Modeling
Let S be the system which we use to find the DoS attack detection system presented in this paper employs the principles of VAA and anomaly-based detection. They equip our detection system with capabilities of accurate characterization for traffic behaviors and detection of known and unknown attacks respectively.

Input: Number of Packets arrive at Network
S= {DT, VAA, NPG, ATD, DP}
Output: Detection of packet as Attack or not.
Where,
S= System.
DT= Dataset.
VAA = Variety Association Analysis
NPG = Normal profile generation.
ATD =Attack detection.
DP= Detected packets.

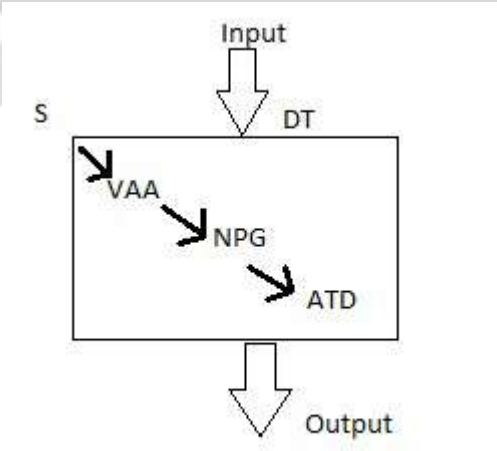


Fig 2. Process of Detection of Denial of Service Attack

## 5. EVALUATION AND ANALYSIS

We can see in fig.3 , it shows the graph of accuracy achieved while DDoS attack detection in distributed networks. There are 2 methods use for detection. First is VAA based attack detection method and second is our proposed work method which shows that our proposed method achieves highest accuracy of 99 % and existing method achieves accuracy of 80%.

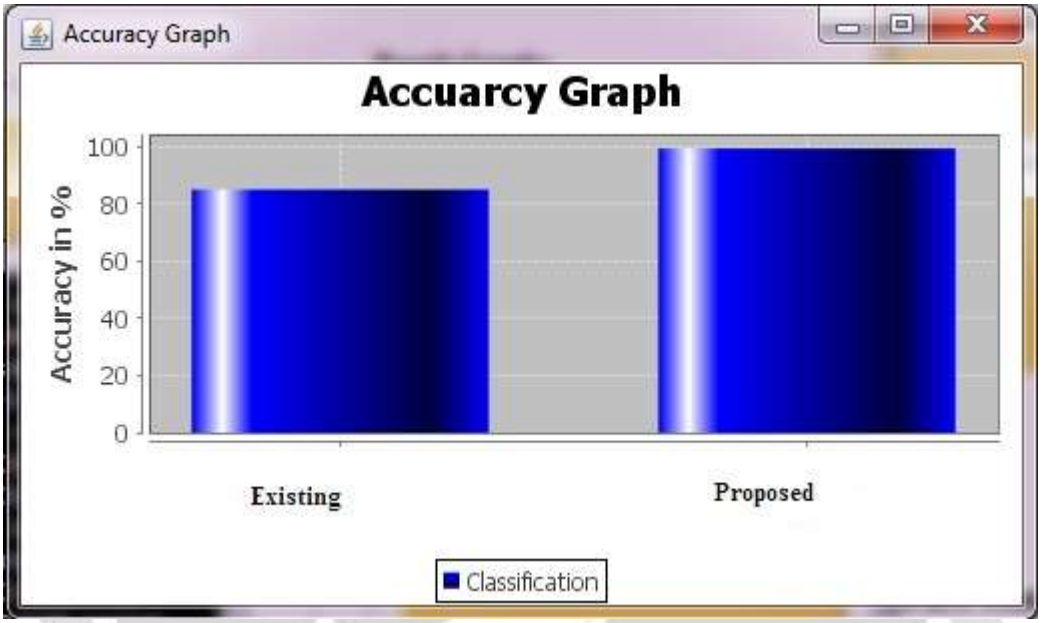


Fig 3. Accuracy Graph

As we can see in fig.4, it shows the graph of detection rate achieved while DoS attack detection in distributed networks. The following graph shows that proposed method i.e. naïve bayes classifier has highest detection rate of 95% as compared to previous method i.e. VAA method it achieves 81% detection rate.

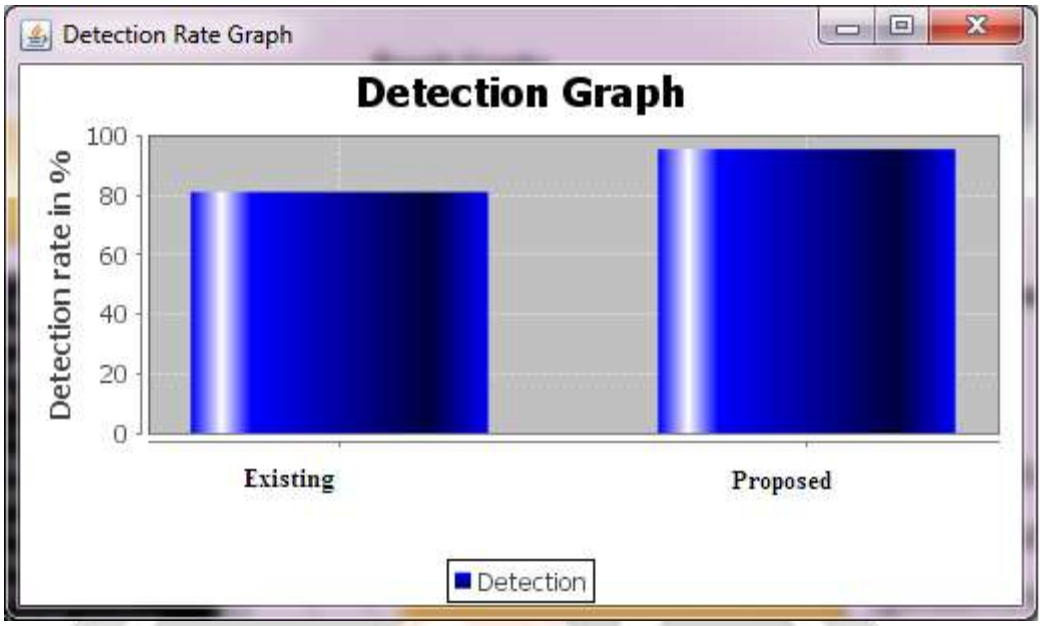


Fig 4. Attack Detection Rate Graph

As we can see in fig.5, it shows the graph of false alarm rate achieved while DoS attack detection in distributed networks. The below given graph shows that proposed has lowest false alarm rate as compared to existing VAA based method.

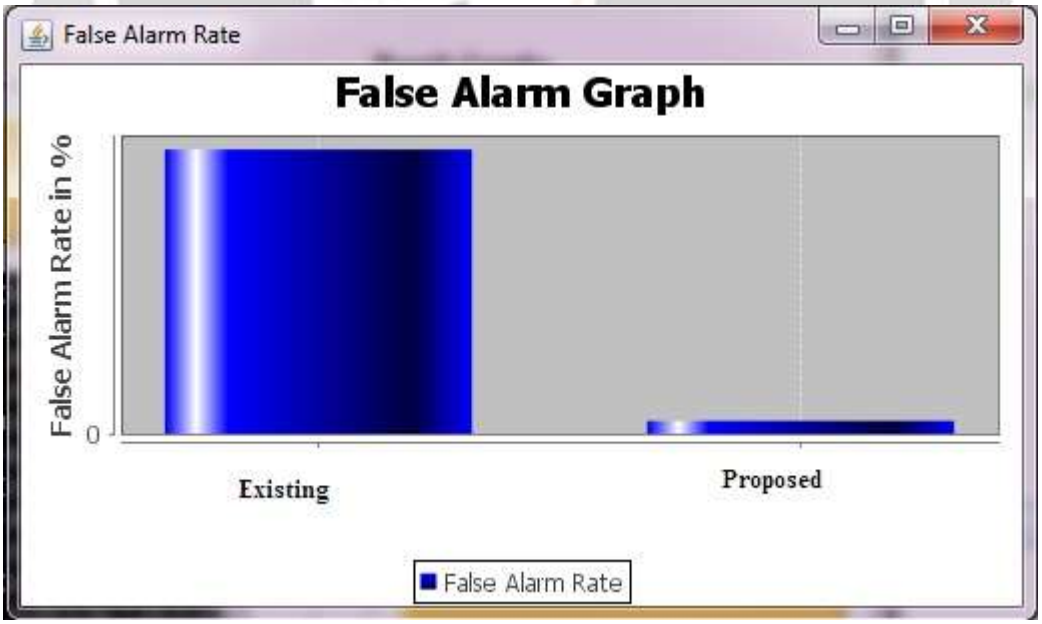


Fig 5. False Alarm Rate Graph

**PERFORMANCE ANALYSIS**

- **Detection Rate:** The detection rate is defined as the number of intrusion instances detected by the system (True Positive) divided by the total number of intrusion instances present in the test set.
- **False Alarm Rate:** Defined as the number of 'normal' patterns classified as attacks (False Positive) divided by the total number of 'normal' patterns.

**ALERT TYPE:**

- **True Positive:** : Attack - Alert
- **False Positive:** : No attack - Alert
- **False Negative:** : Attack - No Alert
- **True Negative:** : No attack - No Alert

**Terms:**

- **True Positive:** A legitimate attack which triggers IDS to produce an alarm.
- **False Positive:** An event signalling IDS to produce an alarm when no attack has taken place.
- **False Negative:** When no alarm is raised when an attack has taken place.
- **True Negative:** An event when no attack has taken place and no detection is made.

## 6. CONCLUSION

This paper has presented a Variety Association Analysis DoS attack detection system which is used b a triangle-area based VAA technique and an normal anomaly-based detection techniques. This technique extracts geometrical Association hidden in each pairs of two unique features within the every network traffic records, and offers more correct classification for network traffic behaviors.

## 7. REFERENCES

[1] Zhiyuan Tan, Aruna Jamdagni, Xiangjian He, Senior Member, Priyadarsi Nanda, and Ren Ping Liu, "A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, 2013

[2] S. T. Sarasamma, Q. A. Zhu, and J. Huff, "Hierarchical Kohonenen Net for Anomaly Detection in Network Security," Systems, Man and Cybernetics, Part B: Cybernetics, IEEE Transactions on, vol. 35, pp. 302-312, 2005.

[3] J. Haggerty, Qi Shi, "Early Detection and Prevention of Denial-of-Service Attacks: A Novel Mechanism with Propagated Traced-Back Attack Blocking" IEEE Transaction on, Vol. 23, 2005.

[4] R. Chen, Jung-Min Park, R. Marchany, "A Divide-and-Conquer Strategy for Thwarting Distributed Denial-of-Service Attacks", IEEE Transactions, Vol. 18, 2007

[5] R Nagadevi, P Nageswara Rao, Rameswara Anand, "A New Way of Identifying DOS Attack Using Multivariate Correlation Analysis", International Journal of Computational Engineering Research (IJCER), Vol.04, 2014.

[6] A. G. Saavedra, P. Serrano, J. Widmer, "A Game-Theoretic Approach to Distributed Opportunistic Scheduling Banch", IEEE Transactions on, vol. 21, 2013.

[7] G. Thatte, U. Mitra, and J. Heidemann, "Parametric Methods for Anomaly Detection in Aggregate Traffic," Networking, IEEE/ACM Transactions on, vol. 19, no. 2, pp. 512-525, 2011.

[8] S. Gomathi, "An Efficient Way of Detecting Denial-Of-Service Attack Using Multivariate Correlation Analysis", International Journal of Innovative Research in Computer and Communication Engineering (IJRCCE) Vol.2, 2014.

[9] S. Yu, W. Zhou, W. Jia, S. Guo, Y. Xiang, and F. Tang, "Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient," Parallel and Distributed Systems", IEEE Transactions on, vol. 23, pp. 1073 - 1080, 2012.

[10] Darshan Lal Meena Dr. R.S.Jadon , "A Survey on Different Solutions to DDoS Attacks", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, 2014.
[11] V. Jyothsna, V. V. Rama Prasad, " A Review of Anomaly based Intrusion Detection Systems", International Journal of Computer Applications, Vol.28, 2011.