# A Secure Lightweight Algorithm for protecting Network from DoS Attack

Meenakshi Choudhary
M Tech Scholar CSE IV Sem
OIST Bhopal, India

Sanjay Kumar Sharma
Asst. Professor CSE
OIST Bhopal, India

## ABSTRACT
Protecting private networks from various attacks is the primary goal of Network managers of a company or office. The attack can be launched either from an insider or outsider. Among these attacks, Denial of service (DoS) attack is most important and has been attracting the interest of researchers. We are providing a lightweight Intrusion Detection and prevention system based on simple modified algorithm which protects the private networks from various DoS attacks. We have used a proper synchronization of IDS and Firewall for intrusion detection and blocking. We have implemented the system as a software application and also analyzed result and performance of the system.

## 1. INTRODUCTION
LAN comprises local networks like a company or an organization, where much sensitive information and private data are usually kept in server systems. Having access to this data requires proper authorization and privilege. If someone attempts access without privilege and without getting authorization, this is also an intrusion activity. And if somebody attempts to harm this data, by attacking on corresponding system, it is even worst. The attacker may be an outsider or an insider. If attacker is an insider he can attempt to get access to someone else's account and also can steal password. Even he can take over someone else's identity to commit a fraud.

Local networks are also attacked by a masquerader, who attempts to stand between two communicating parties and intercepts the information being exchanged. It is passive attack because attacker does not interfere with the communication. In active attack, he changes the information and then passes over to the end systems.

Finally, the most important and today's common attack is DoS attack, which may be carried out by outsider to destroy the company's server system by heavily loaded it through continuous fake requests. These goes beyond the handling capability of the system after some time. As a result, system stops working.

### 1.1 Denial of Service Attack
The DoS attack is having the aim to prevent legitimate and valid users from accessing network resources, services and information. A DoS attack occurs when an attacker has engaged most of the network resources or consumes the network bandwidth by imposing excessive traffic to the network. A huge amount of requests are continuously sent to the victim computer for its resources and services and system remains busy in serving those requests. As a result, the victim system cannot serve the legitimate users requests and after some time it goes down. Even its components may be destroyed. More specifically, this sort of attack targets the availability of the network i.e. by blocking network access, causing excessive delays, consuming valuable network resources, etc

### 1.2 Defense Mechanisms against DoS attack
There are three main defense mechanisms against DoS attack-

*1.2.1 Victim end defense-* The DoS attack can be detected at the victim end by measuring the traffic, bandwidth consumption and no of incoming packets in certain time interval etc. Detection at victim end is much easy task but this approach cannot stop the traffic flow i.e. it cannot prevent the attack even it detects the attack only when it reaches to the victim.

*1.2.2 Source end defense-* At source end a traffic controller module is configured which controls the traffic rate on ongoing connections. It also compares the incoming and outgoing traffic statistics. A big difficulty with these systems is that generally the sources are distributed in this huge internet than how can this system are deployed at source end.

*1.2.3 Intermediate Network Defense-* It is deployed at the routers through which traffic is passed. Router continuously observes the amount and rate of traffic and also shares their observations with other routers in the network. When abnormal traffic is observed they can limit the traffic rate by dropping some packets. This scheme also has an issue of deploy ability, because for this to work all routers on the internet will have to employ this scheme.

We have worked on the victim end defense mechanism with a prevention mechanism, which does not let the victim to be overwhelmed with the traffic and also block the attack.

## 2. SURVEY OF EXISTING APPROACHES USED FOR INTRUSION DETECTION

### 2.1 Intrusion Detection System (A Layered Based Approach for Finding Attacks)

The proposed system [1] is a combination of HIDS and NIDS. An IDS sensor is located inside individual systems to monitor system level behavior to look at all network packets, connection attempts, or login attempts to the monitored machine. The NIDS system also works together with the HIDS and detects intrusion layer wise. The NIDS and HIDS both systems invokes the detection engine to detect attacks, which uses a Network database and host database containing signatures of known attacks to match the features. If match is found an alarm is generated.

## 2.2 An Intrusion Detection System Alert Reduction and Assessment Framework Based on Data Mining

The proposed system [2] is aimed to reduce the false alerts and redundant alerts by the IDS system. It has three components: Traffic data retrieval and collection mechanism system, reduction IDS alert processes system and threat score process of IDS alert system. The first systems develops a mechanism to save IDS alerts, extract the standard features as intrusion detection message exchange format and save them in DB file. The main function of reduction IDS alert processes system is to remove duplicate IDS alerts and reduces the amount of false alerts based on a new aggregation algorithm.

## 2.3 NIDS using Learning process

Gaidhane[4] et al, To overcome the problem of large amount of training time, they proposed a new approach. The system works in three stages: data preprocessing, training and testing. Whole process is done as following-Network data monitoring module captures data packets to be used as the data source of NIDS. In data preprocessing the network traffic is processed to be used as the system input. The feature extraction module extracts feature vectors from the network packets and submits them to the classifier module. Classifier module analyses the network traffic and draw a conclusion whether intrusion happens or not. For classification it uses neural networks.

## 2.4 NIDS using Misuse Detection

[5] The proposed system is a Network Intrusion Detection System. It works as lower level of firewall. This system not only detects intrusion based on the IP address but by the content also. It is based on misuse detection in which a database model is prepared containing the known intrusion patterns. Currently arrived data patterns are matched against these patterns by using suitable matching algorithm. If intrusion is found, it is forwarded to firewall for blocking.

## 2.5 SNORT Intrusion Detection System

SNORT [5] is a signature-based NIDS. It works in a sequence of stages using various modules. The first module is packet decoder that decodes the data packets arrived in the network. The decoded packet header values are stored in a data structure for later use by detection engine. The preprocessor performs a variety of preprocessing. The detection engine carried out actual detection by matching values in previous steps against a set of rules that encodes patterns of known attacks. If match is found, alarm is generated.

## 2.6 Flow-based Abnormal Traffic Detection Algorithm

Kim[6] et al. propose a method to detect abnormal network traffic. The detection module receives flow information from monitoring systems or routers. After detecting abnormal traffic, an alarm is emitted if an attack is detected. The overall process consists of two parts: the flow header detection and the traffic. pattern detection. The flow header detection takes part in checking the fields of the flow headers.

## 2.7 MULTOPS

Gil and Poletto[7] propose a scheme called MULTOPS to detect denial of service attacks by monitoring the packet rate in both the up and down links. MULTOPS assumes that packet rates between two hosts are proportional during normal operation. A significant, disproportional difference between the packet rate going to and from a host or subnet is strong indication of a DoS attack. MULTOPS assumes that the incoming packet rate is proportional to outgoing packet rate, which is not always the case. For example, real audio/video streams.

## 2.8 SYN and Batch Detection

Wang et al. [8] proposed SYN detection to detect SYN floods, and Blazek et al. [25] proposed batch detection to detect DoS attacks. Both methods detect DoS attacks by monitoring statistical changes. The first step for these methods is to choose a parameter for incoming traffic and model it to be a random sequence during normal operation. In [27], the ratio of SYN packets to FIN and RST packets is used, while in [25] a variety of parameters, such as TCP and UDP traffic volume, are used. The attack detection is based on the following assumptions. First, the random sequence is statistically homogeneous. Second, there will be a statistical change when an attack happens.

## 2.9 Using Source IP Address Monitoring

Peng[9] proposed a new detection scheme called Source IP address Monitoring (SIM) which monitors the increase in new IP addresses over a certain period. By detecting an abnormal increase in the new IP addresses, distributed denial of service attack can be identified. The system works as follows- A learning engine adds legitimate IP addresses into an IP address database (IAD). A hash table is used to record the IP address that appeared in the current time interval. By comparing the current count of hash table with the IAD, we can conclude how many new IP addresses have appeared in this time slot. If the no of packets per IP address is larger than a certain threshold, an alarm is generated to indicate bandwidth attack.

## 2.10 Agent Based Intrusion Detection

[10] In this approach the workload will be divided between the individual processors. Servers can communicate with one another and can alarm each other. In order to respond to an attack, sometimes it can be sufficient enough to disconnect a subnet. In this type of system in order to contain a threat, the distributed IDS can order severs, routers or network switches to disconnect a host or a subnet.

# 3. PROBLEM IDENTIFICATION

We have surveyed various existing systems designed to detect and/or prevent intrusions in different networking environments. They have many advantages but also have some problems as follows-

1. HIDS requires the IDS sensor or agent to be installed in each and every system in the network which is not suitable for large networks. Also they create network latency because huge information flows in the network for the synchronization between sensors and detection engine.

2. Signature based systems can detect only those attacks whose signatures are available in the signature base. Other attacks are beyond its handling capability. They can easily made fool by attacker if he launches attack by changing the signature.

3. If attack is detected some systems forward it to firewall for blocking but if the detection is false the legitimate users will be denied access.

We have solved most of the above problems in our system but the proposed system is limited to the detection of DoS attack

only. Other attacks are beyond the scope of this system. We have more focused on making the detection accurate. The system is lightweight and can detect attack in much less time. The system is also free from false detection.

## 4. PROPOSED IDS SOLUTION

The figure 4.1 shows the design of proposed system, in which IDS system is collaborated with firewall.

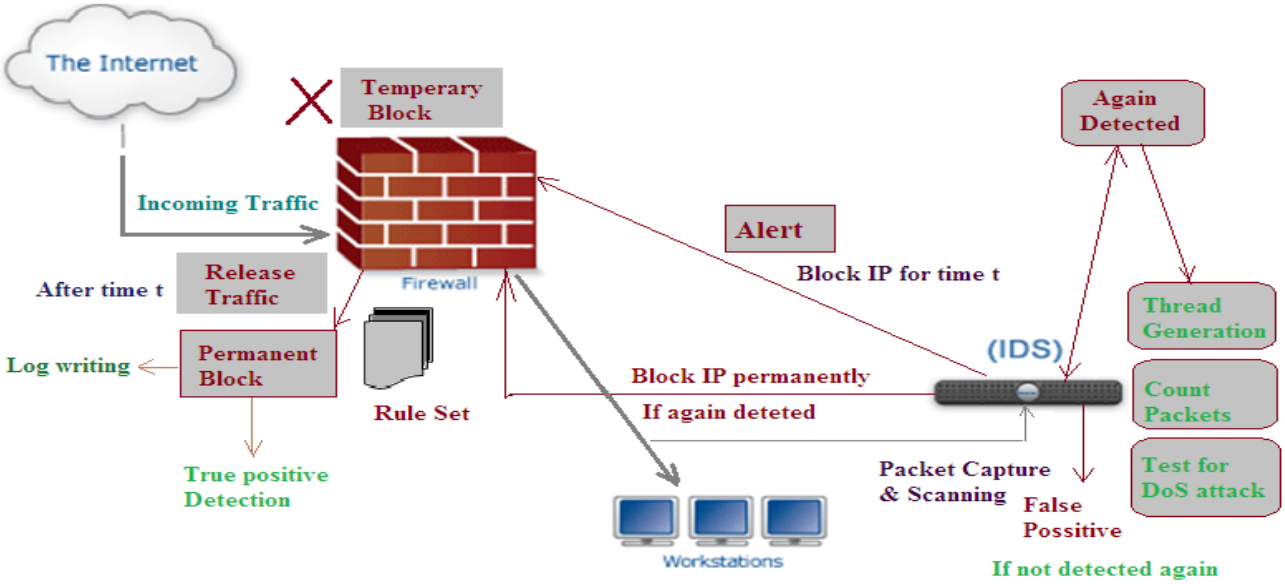


**Fig. 4.1 Proposed System Design**

Our aim is to protect through DOS attack in LAN. We have implemented the system as a software application, which can be deployed on any host machine in the network. As the application starts it captures and analyses all At the same time it analyses the traffic intended for a particular host machine by computing the no of incoming packets from the same source. For this we have used thread which handles the incoming packets. A threshold value is decided which equivalent to the no of packets, allowed to arrive on a particular computer. System starts analyzing packets by generating threads with a sleep time (time for which the thread is alive) and starts counting the packet by increasing the packet_count value on each request packet with same source and intended for a particular host. If the count doesn't touch the threshold value within the sleep time, then thread is destroyed and packet_count value becomes zero. Now a new thread is generated again with same sleep time and the whole process repeated.

If at any pass the packet_count value goes beyond the threshold then it shows a popup indicating DOS detected together with the IP address of attacker. This situation can occur only if the attacker sends huge no of packets continuously. If detected it sends a command to the underlying system to block the traffic from that IP for some time. This time also specified by IDS system, because if the detection is false positive then the traffic will not be blocked for long and can again be started. Hence the communication will be continued.

## 5. PROPOSED ALGORITHM

Algo DOS_Detection

Create unbounded buffer as Buffer;

Initialize Buffer = null;

Set Threshold = T;

//capture the incoming IP packets to the network.

For each incoming IP packet

Get the destination IP address;

Store the corresponding source IP address as Current_IP in Buffer;

Create a thread with sleep time S.

Initialize Packet_Count = 0;

While(S!=0) //as long as the thread is alive

{

a. Get the following IP packets with same destination IP address

//For other packets

b. Call Algo DOS_Detection

c. Retrieve their source IP address as Next_IP;

//compare Next_IP with Current_IP in Buffer

d. If (Next_IP == Current_IP)

{

Packet_Count++;

}

Else

{

For Next_IP go to step ii

}

vi.Thread sleep;

//Thread destroyed

// check condition for DOS attack (If packet count goes beyond the threshold value)

5. For each DOS Detected

//Request the server to block this IP permanently;

vii If (Packet_Count < T)

{

Then goto step 3

}

Else

{

Show message("DOS detected from Current_IP");

Call log writer

}

//False Positive Detection

b. Block Current_IP;

c. Call log writer;

Send command to the server system to block the traffic from Current_IP with block time B;

//Block time is the duration for which the traffic is blocked and become allowed again after its completion.

6. Repeat step 1 for Current_IP;
7. If DOS attack again detected then

{

a. Show message ("DOS detected");

// accurate detection

}

Else

{

a. Report this detection as false positive;

b. Call log writer;

}

## 6. RESULTS

In this section, we present a set of experiments to understand the working of the proposed system and also test the performance metrics. The interface of the system is shown in figure 2. It shows the DoS attack as continuous IP packets incoming from same source IP address. We tasted the system in a LAN network by launching attacks from a system in the same as well as from different network. Then we analyze our system for this attack detection.

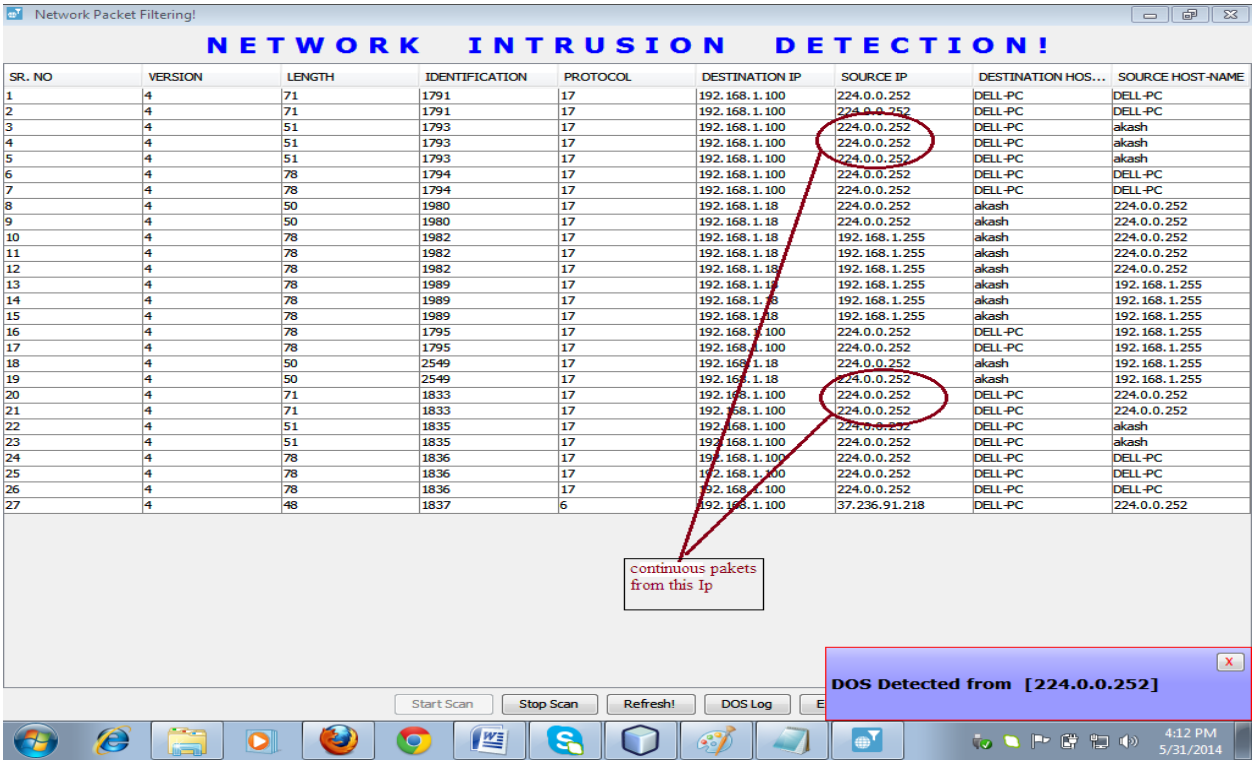


**Figure 2 DoS Detection**

## 7. RESULTS ANALYSIS

In Result analysis we consider the two cases and try to analyze the system. In first case we take output of the system when there is normal packet flow i.e. there no attack is present. This output contains the packet_count in individual threads. Then we launch attack in second case from somewhere and again analyze packet_count value in each thread and based on these values we plot different graphs for each case.

### *Case 1: When there is no attack (Normal packet flow)*

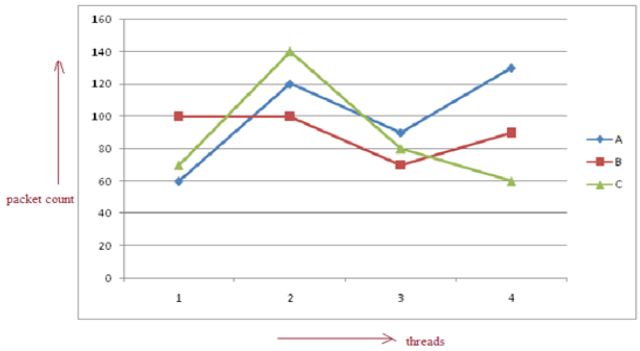


**Fig 7.1 DoS is launched from single source**

The graphs shows three different lines for packet count in three different threads for individual source. Each line is below the threshold point above which a packet count is considered as an indication of DoS attack. Hence there is no attack launched.

### *Case 2: When DoS is launched from multiple sources*

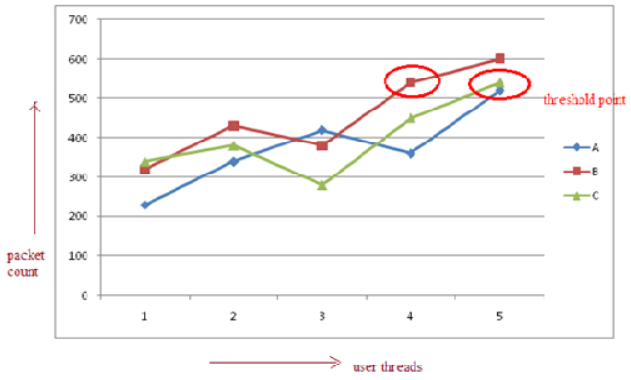


**Fig 7.2 DoS is launched from multiple sources**

In this graph the packet count of three different sources reached above threshold value hence it is an indication of DoD attack.

## 8. PERFORMANCE ANALYSIS

Performance analysis describes how much time the system takes to detect an attack. Here we are taking different cases and analyzing the performance of system in each case.

### *Case 1: When attack is detected from single host*

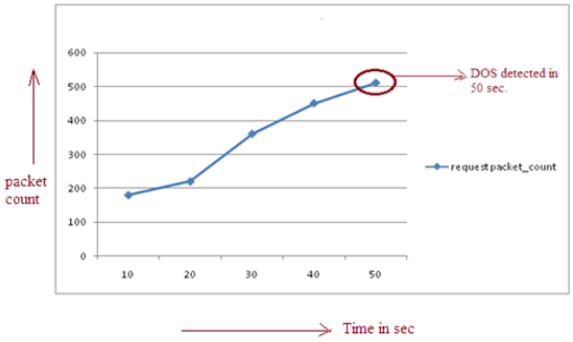


**Fig 8.1 Performance analysis for single attack**

Here the attack is launched from the single host at time 0sec. We start counting the time until attack is detected. And we see in result that system takes less than 50 sec to detect the attack. It shows improved performance of system.

### *Case 2: When attack is detected from multiple hosts*

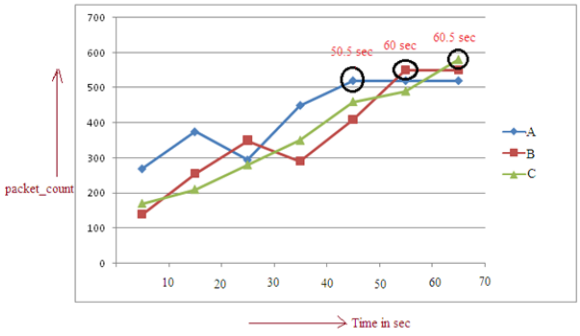


**Fig 8.2 Performance analysis for multiple DoS attacks**

Here the graph is plotted for the time taken to detect DOS attack from 3 different hosts or attackers. The lines showing the packet count from each attacker. As the graph shows the system takes much less time to detect such attacks which is considerable improvement in system performance.

### *True/False positive detection*

We have used additional mechanism to detect whether the detection is false/true positive. When system detects DoS attack from a particular IP, the firewall is invoked to block the IP for a particular duration. After that duration, the IP become unblocked. Now system again checks the traffic from that IP. If again the attack is detected, it is true positive and firewall permanently block the traffic from that IP or may apply some other protection based on rules and a log is generated for it otherwise, the detection is false positive.

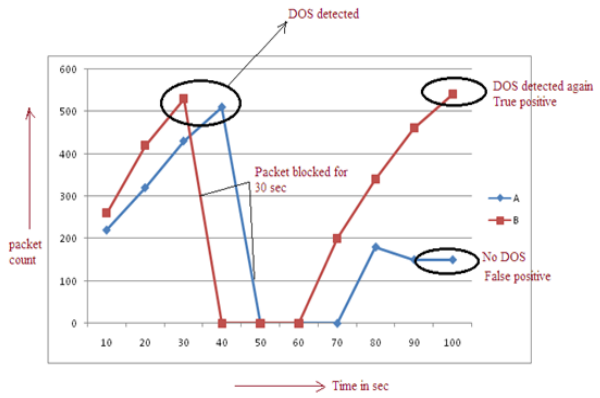


**Fig 8.2 Performance analysis for multiple DoS attacks**

We have shown another graph for true/ false positive detection by system. If the system detects attack then the alert report is sent to firewall to block the traffic from the corresponding source for some time t. In our experiment we have taken t= 30sec. Now packet count goes to zero. After time t, the traffic is unblocked and again system starts counting packets. If the Dos attack is detected again then the detection was true positive otherwise false positive as shown in the graph.

We can conclude from this experiment that the proposed system is detecting attacks accurately and very fast which shows great performance of the system. Also it uses the concept of thread which is light weight and hence causes less overhead on processor and requires less system memory.

## 9. CONCLUSION

The proposed system can be used to identify Denial of Service attack in private networks and also attempt to prevent it. The algorithm used, is much simple and light weight takes less time to execute and hence the attack can be detected immediately. Also it is free from wrong detection and guarantees that legitimate users will not be blocked. The performance analysis shows that it performs well when DoS attack is launched and the system is tested to detect and prevent it.

It is an approach to keep the network secure itself by providing a defending system which alerts for intrusion in the whole network and uses the services of firewall to block it. It also prepares the log report for network analyzer.

## 10. REFERENCES

[1] Kiran Dhangar, Prof. Deepak Kulhare Arif Khan Intrusion Detection System (A Layered Based Approach for Finding Attacks) International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 5, May 2013 ISSN: 2277 128X.

[2] Karim Al-Saedi Selvakumar Manickam Sureswaran Ramadass, Wafaa Al-Salihy Ammar ALmomani Journal of Computer Science, 9 (4): 421-426, 2013 ISSN 1549-3636 2013.

[3] K.Santhi, "A Defense Mechanism to Protect Cloud Comuputing Against Distributed Denial of Service Attacks", International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 5, May 2013 ISSN: 2277 128X.

[4] Roshani Gaidhane, Prof. C. Vaidya, Dr. M. Ranghuswami, "Survey: Learning Techniques for Intrusion Detection System (IDS) International Journal of Advance Foundation and Research in Computer (IJAFRC) Volume 1, Issue 2, Feb 2014. ISSN 2348 – 4853.

[5] Munish Sharma and Anuradha "Network Intrusion Detection System for Denial of Service Attack based on Misuse Detection." IJCEM International Journal of Computational Engineering & Management, Vol. 12, April 2011 ISSN (Online): 2230-7893.

[6] Saman Taghavi Zargar, James Joshi and David Tipper A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks Feb. 2013.

[7] Nilotpal Chakraborty, "Intrusion Detection System and Intrusion Prevention System: A Comparative Study" International Journal of Computing and Business Research (IJCBR) ISSN (Online) : 2229-6166 Volume 4 Issue 2 May 2013.

[8] Dong Lin Network Intrusion Detection and Mitigation against Denial of Service Attack April 15, 2013.

[9] Suchita Patil, Dr. B.B.Meshram, "Network Intrusion Detection and Prevention techniques for DoS attacks", International Journal of Scientific and Research Publicat ions, Volume 2, Issue 7, July 2012 ISSN 2250-3153.

[10] Ms. Parag K. Shelke, Ms. Sneha Sontakke, Dr. A. D. Gawande Intrusion Detection System for Cloud Computing International Journal of Scientific & Technology Research Volume 1, Issue 4, May 2012 ISSN 2277-8616.

[11] T. Gil and M. Poletto. MULTOPS: a data-structure for bandwidth attack detection. 2001.

[12] Amirreza Zarrabi, Alireza Zarrabi Internet Intrusion Detection System Service in a Cloud IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 5, No 2, September 2012 ISSN (Online): 1694-0814.

[13] Amrita Anand Brajesh Patel "An Overview on Intrusion Detection System and Types of Attacks It Can Detect Considering Different Protocols", International Journal of Advanced Research in Computer Science and Software EngineeringVolume 2, Issue 8, August 2012 ISSN: 2277 128X.

[14] Monowar H. Bhuyan H. J. Kashyap D. K. Bhattacharyya J. K. Kalita Detecting Distributed Denial of Service Attacks: Methods, Tools and Future Directions December 2012.

[15] Qijun Gu, Peng Liu Denial of Service Attacks 2007.