ISSN: 2229-6948 (ONLINE)
DOI: 10.21917/ijct.2010.0013

A TWO LEVEL ARCHITECTURE USING CONSENSUS METHOD FOR GLOBAL DECISION MAKING AGAINST DDoS ATTACKS

S.Seetha[1] and P.Raviraj[2]
Department of Information Technology, Karunya University, Coimbatore, Tamil Nadu, India
Email: seetha_mismin@yahoo.com[1], raviraj_it@yahoo.co.in[2]

Abstract
Distributed Denial of service is a major threat to the availability of internet services. Due to the distributed, large scale nature of the Internet makes DDoS (Distributed Denial-of-Service) attacks stealthy and difficult to counter. Defense against Distributed Denial- of - Service attacks is one of the hardest security problems on the Internet. Recently these network attacks have been increasing. Therefore more effective countermeasures are required to counter the threat. This requirement has motivated us to propose a novel mechanism against DDoS attack. This paper presents the design details of a distributed defense mechanism against DDoS attack. In our approach, the egress routers of the intermediate network coordinate with each other to provide the information necessary to detect and respond to the attack. Thus, a detection system based on single site will have either high positive or high negative rates. Unlike the traditional IDSs (Intrusion Detection System) this method has the potential to achieve high true positive ratio. This work has been done by using consensus algorithms for exchanging the information between the detection systems. So the overall detection time would be reduced for global decision making.

Keywords:
DDoS Attack, IDSs, Consensus Algorithm

1. INTRODUCTION

Denial of service attack is a major cause of incorrect operation in the Internet and is arguably the most serious threat that the Internet community faces today. DDoS attacks generate a large volume flow to overwhelm the target host. The victim cannot protect itself even if it detects this event. So the detection and defense of DDoS should ideally be near the source of the attack or somewhere in the network. It is difficult to distinguish attack packets from legitimate packets. Attack packets can be identical to legitimate packets, since the attacker only needs volume, not content, to inflict damage. Furthermore, the volume of packets from individual sources can be low enough to escape notice by local administrators. Thus, a detection system based on single site will have either high positive or high negative rates [1][2]. Due to the readily available tools, "Flooding" attack becomes most common DDoS attack. They intend to overflow and consume resources available to the victim [3]. When the number of attackers is very large, the flows from each attacker can be very small to detect. So, the detection based on instantaneous deviation is useless, because of the deviation is very small in flow [4] [5]. Most of the DDoS detection system models are based on traffic flow rates [6]. As many new applications are coming up and End user's behavior also varies, that is difficult to get a general efficient model based on traffic flow alone.

Hence, we need a DDoS detection system which is not only based on traffic flow. For that, in this paper we proposed a sequential method to detect DDoS attack quickly, which captures cumulative deviations from a normal behavior over time. The effectiveness of attack detection increases near the victim and the effectiveness of packet filtering increases near the attack source. So that we have chosen the detection system in the intermediate location to get benefits in both ways as shown in Fig.1

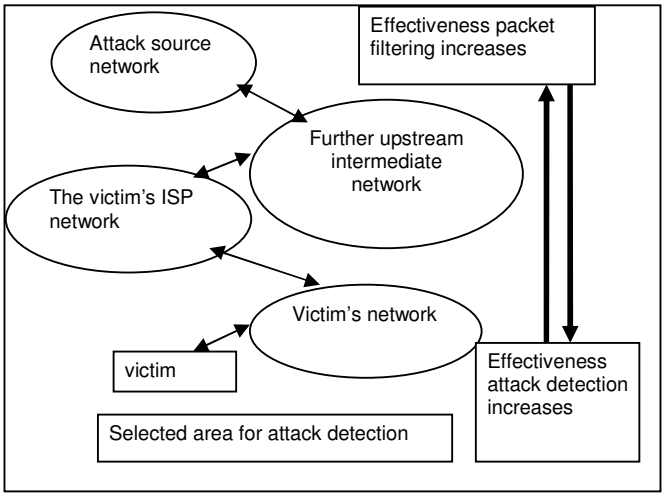

Fig.1. DDoS attack detection location.

2. PROPOSED METHODOLOGY

One of the major challenges in detection system design is to process packets at very high speeds, essentially when placed in back bone networks. The algorithms for high-speed packet processing continue to be very important and active research area. So, we used a comprehensive test method in the local detection systems (in the edge routers). Due to the distributed nature of a typical DDoS attack, each local detection system observes only partial traffic anomalies. Due to this nature we designed the entire process with two levels: Local detection and Global detectionas shown in Fig.2. The combined belief of all local sequential method detection system (SMD) is considered to detect the DDoS attack globally. This is achieved by the consensus algorithm. It is very much useful to reduce detection time and to reduce misdetection rates.

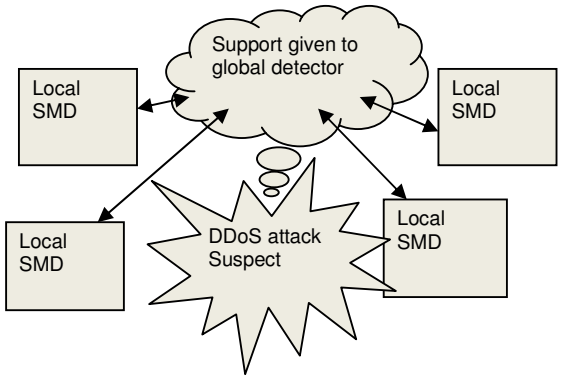

Fig.2. Two level architecture

2.1 LOCAL DETECTION OF ATTACKS USING SEQUENTIAL TEST METHOD

The Sequential Test Method has been implemented in each Egress router (DS). The Egress router is the one through which all nodes sends the traffic (flow of packet). Each Detection system perform the sequential test and based on the confidence level of an attack, it Will send attack alert to the Leader Detection System. The Leader Detection System consolidates and analyzes its local detection result with attack alerts received from other detection systems to make a global detection decision. If a DDoS attack is confirmed, the DS notifies the packet filtering component to install packet filters for the corresponding packet stream

2.2 SEQUENTIAL TEST METHOD

In each SMD we have two phases for detecting the anomaly namely

Phase-1: Sequential test method

Phase-2: Monitoring new IP addresses.

The two phases raise alarms when they find the observed statistical ratio crosses some threshold. Based on the combined belief of the two alarms DDoS attack is confirmed as shown in Fig.3

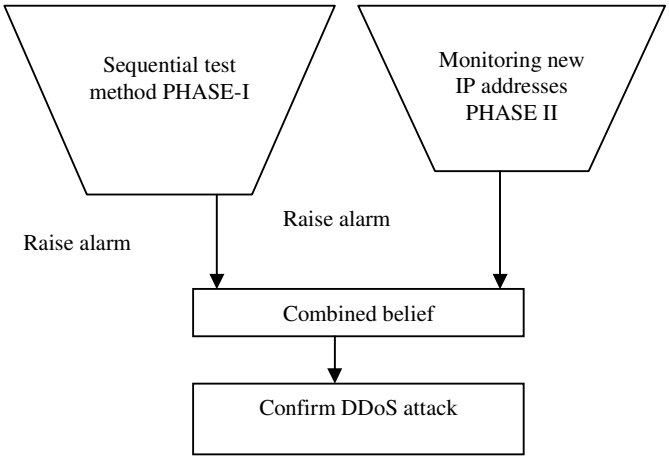

Fig.3. Two phases of SMD

2.2.1 Phase-1:

This is based on inherent request vs reply protocol behavior. We have taken TCP-SYN flooding attack. Here, a large number of TCP SYN packets is sent to victim's server port. If the port is actively listening for connection requests, the victim would respond by sending back SYN-ACK packets. However, since the source addresses in these packets are spoofed addresses, these response packets are sent elsewhere in the Internet. Thus the victim retransmits the SYN-ACK packets several times before giving up. However, these half open connections will quickly consume all the memories allocated for pending connections, thus preventing the victim from accepting new request.

In the Fig.3, phase 1, the number of requests and number of replies are calculated. We consider a time series {T1, T2, T3,…Tn}. We find the number of SYN (opening connections) and FIN (RST) (closing connections) packets. For each sampling period we calculate the average number of replies R'.

$\sum_{t=1}^{n} X_i$ = Total number of requests – corresponding replies for one sampling period (1)

Where Xi is the collection of observed data.

This value is normalized by R' as follows

$$\Delta n = \sum_{t=1}^{n} Xi / R' \qquad (2)$$

Now we consider this ratio for deciding hypothesis and raise alarm when it crosses the threshold value.

i) H = 0 (Null hypothesis) ---Normal situation
H = 1 (Alternative hypothesis) – abnormal situation

ii) Sequence of observed data
X1,X2,X3,…Xn

iii) Decision consists of
- Stopping time N(stop taking samples)
- Make a hypothesis – H=0 (or) H=1 ?

Now as shown in Fig.4 the alarm is raised if the Δn value exceeds the threshold value N.

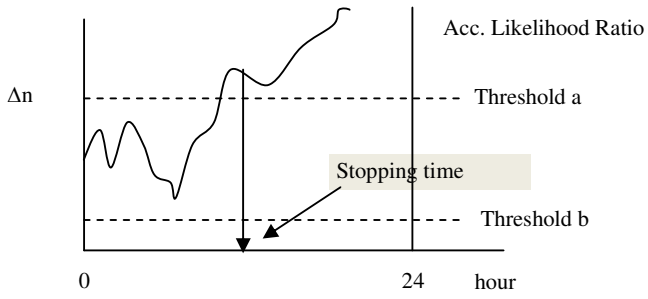

Fig.4. SMD Detection method

2.2.2 Phase-2:

Monitoring the percentage of new IP addresses is effective in detecting the attacks. Over the same time series T1,T2, T3,…Tn, the incoming IP addresses are collected. Let F be the collection

of frequent IP addresses, and M be the collection of incoming IP addresses in time interval T.

$$Yn = \frac{|M| - |M \cup F|}{|F|} \quad (3)$$

where Yn is the percentage of new IP addresses to be calculated in the time interval T. When this value Yn exceeds the threshold value say N, then alarm is raised. Normally Yn is calculated for the confirmation of DDoS attack.

2.2.3 DDoS Detection:

When both Phase.1 and Phase.2 raise alarms, based on the combined belief DDoS attack is confirmed as shown in Fig.5. Based on the values of Δn and Yn the hypothesis is decided, and DDoS attack is confirmed.

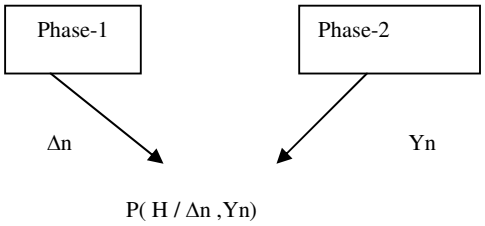

Fig.5. Decision making based on combined belief

where P is decision function which is deciding over DDoS attack confirmation and H is the Hypothesis.

There are two hypothesis to test on both levels: H1 for the presence of a DDoS attack and H0, a null hypothesis. The binary hypothesis is tested on the two phases of SMDs. As soon as the local SMDs support H1, the detection system involved passes attack information to all other detection systems signaling a possible DDoS attack.

Each Detection system then independently consolidates and analyzes its local detection result with attack alerts received from other detection systems to make a global detection decision. For this purpose, each attack alert is attached with a confidence level that quantifies the amount of evidence supporting the suspected attack. If a DDoS attack is confirmed, the DS notifies the packet filtering component to install packet filters for the corresponding packet stream. It also notifies the upstream networks to filter the attack packets as shown in Fig.6.

2.2.4 Implementation of Consensus Algorithm:

In consensus algorithm, the leader detection system receives attack suspect ion from other DS's. Based on the combined belief of majority of the detection system (DS) it will make filtering action and sent filtering rate to the majority of the system who suspect the attack.

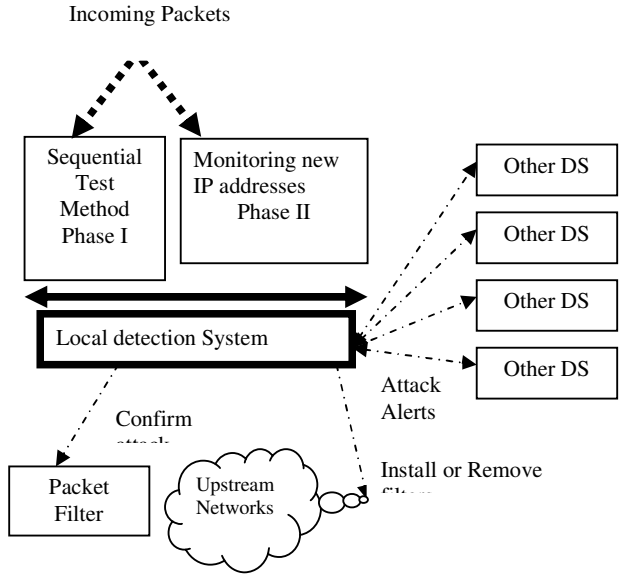

Fig.6. Two-level attack detection in the distributed detection approach.

Consensus Algorithm:

A group of processes cooperating to provide a highly available service need to agree on which processes are currently functioning as members of the group. The consensus algorithm is explained in Table.1.

Processes: Detection systems

Service: Suspect and prevent DDoS

Currently functioning members: Only few detection systems are selected among many to do the service

Table.1. Implementation of Consensus Algorithm

Algorithm:

1. The server (victim) keeps track of no of half open connections. There are two threshold value are considered.

   Threshold value first - HC_f

   Threshold value second - HC_s

2. There is a leader detection system. It

   gets all the allowed actions

   Chooses the outcome(filtering value)

   Tells everyone

3. When the number of half open connections reaches HC_f , then it passes the suspection to the consensus leader. The leader alerts all detection systems.

4. In each detection system the sequential test is performed and based on that test, they raise alarm as follows.

Each detection system passes the following information to the leader.

   (i) actual incoming rate

   (ii) actual exit rate

   (iii) actual acceptance rate

Cont…

Cont…

(iv) Deviations

- Percentage of unmatched request vs reply
- Destined to the victim- DV_{um}
- Percentage of excess amount of packets coming through the detection system than the actual acceptance rat -DV_e

5. The leader detection system receives the above information from many detection systems that suspect and raise alarm.

6. The leader now applies the consensus among these values and decides the outcome which is the filtering value to be applied in selected detection systems at the end. The leader has the predefined threshold value TV_{dev} for the deviation DV_{um}.

7. Now among the many detection systems involved, the majority group is selected by the following method. For the detection systems DS1, DS2, DS3,…DSn , who raised alarm, the following check is done.

8. The DV_{um} of detection systems DS1, DS2, DS3, DSn are checked with this threshold value TV_{dev}. The particular detection system DSi is included in the majority group if and only if the following condition satisfies.

DV_{um} of detection system DSi > TV_{dev}

Let the no of DS wins this check be 'm

9. Now to check the majority the leader has to decide the outcome only if (n-m) is greater than or equal to n/2.

10. Deciding the outcome (filtering value)

The Outcome (filtering value) =Max DV_{um} among the majority group/2

11. This outcome is passed only to the members of majority group. The relative value is then calculated by the individual DS and filtering is done.

12. Periodically the leader checks the no of half open connections at the victim server. If it below $HC_{s,}$ then the leader instructs the DS of majority group with the same filtering value. (Here the it checks whether the actual packet rate converges to acceptance rate or not).If the no of half open connections is greater than or equal to $HC_{s,}$ then the filtering value is decided as Max DV_{um} among the majority group

The process stops when all of the DS in majority group DS incoming converges or tphe no of half open connections at victim converges below HC_f

2.2.5 Detecting and Filtering the Global traffic:

If the confidence level value exceeds confidence threshold, then it confirms the attack and sends the response to corresponding Egress router. Now the egress router (DS) will drop the packets from the corresponding destination node.

3. RESULTS AND DISCUSSIONS

The Fig.7 shows the setting up of a network topology. Configure 25 nodes. The Script is written using Tool Command Language (TCL) for front end to design GUI and C++ is used to design the back end for processing. Source nodes are represented as blue nodes and destination nodes are represented as green nodes. Then the data packets are transferred from one node to other. In this topology, there are 24 nodes. They are 3 source nodes and 1, destination node. Packets are sending at a particular rate. This rate is evaluated by timer by extending the Timer Handler. Normal data packets are represented by Blue color and acknowledgment packets are represented by Red color.

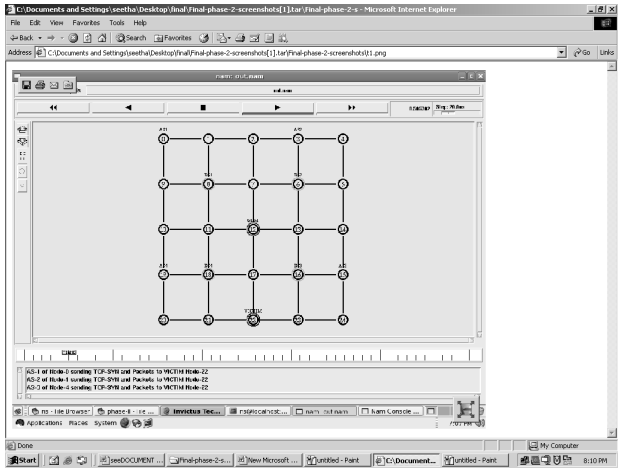

Fig.7. Topology Construction with 25 nodes

In Fig.8, there are four detection system (DS) marked as green color node and one leader detection system marked as blue color node. Now the victim system sends the attack suspection to leader DS (node 12).

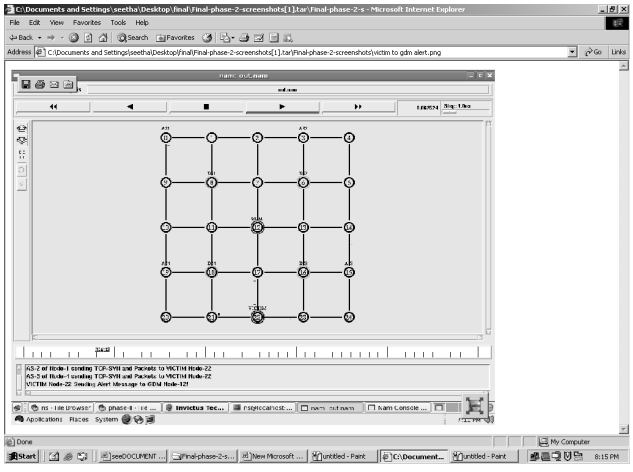

Fig.8. The victim (node 22) sends the attack alert to leader DS (node 12)

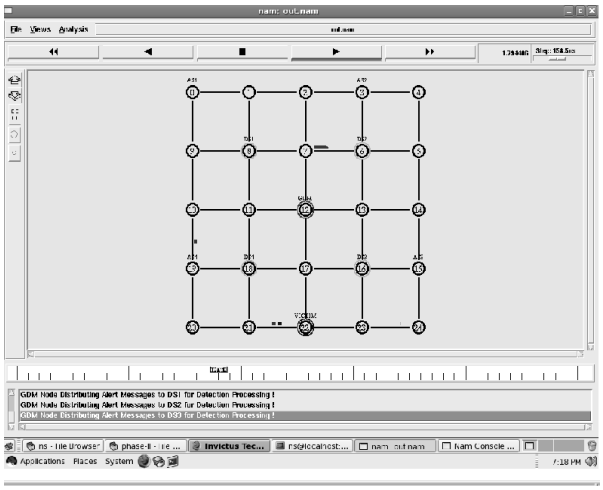

Fig.9. The leader node 12(leader DS) is sending the attack alert to node 6 (DS 2).

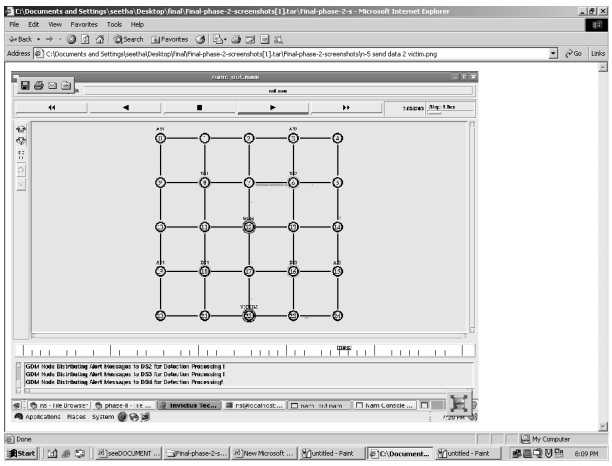

Fig.10. DS 6 now suspects the attack.

In this Fig.10, DS 6 now suspect the attack; it will perform the sequential test and send the result (threshold value) to leader Ds.

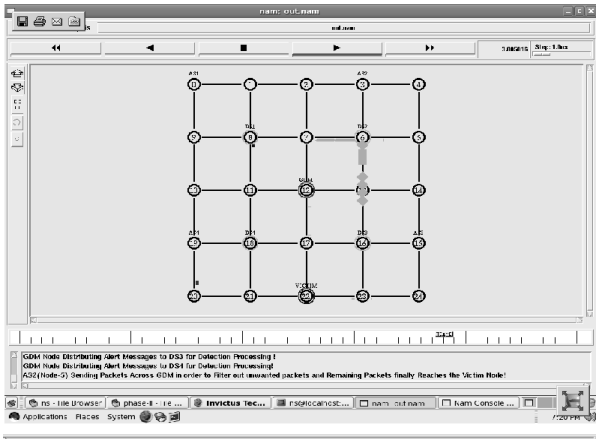

Fig.11. Detecting & filtering Traffic

Thus the traffic is detected and filtered using Consensus algorithm. If the confidence level value exceeds threshold, then it confirms the attack and now the egress router (DS) will drop the packets.

4. PERFORMANCE ANALYSIS

Even though anomaly based IDSs are widespread and successful in most environments, they possess various disadvantages, too. The main drawback with anomaly based systems is that they can raise a high proportion of false alarms. IDSs often have both accurate detections and missed attacks. Depending on the type of alarm 2004] raised by the IDS and the actual intrusion scenario, following types of detection results are possible. The false Positive ratio, typically known as false alarms, these occur when IDS reads legitimate activity as being an attack. The following figures show performance measure of existing with the proposed algorithm. Let P represents the probability that each detection node in the detection overlay network sends local traffic information to its neighbor nodes. We vary the probability of consensus between 0.2, 0.4, 0.6, 0.8, 1.0. The performance of this approach with different probability P used are shown in Fig.12. As we can see from the simulation results, with p=0.4 we have high false positive ratio. This is because we adopt high initial drop rate. When the local detection system detects an attack as a result legitimate packets will be dropped dramatically.

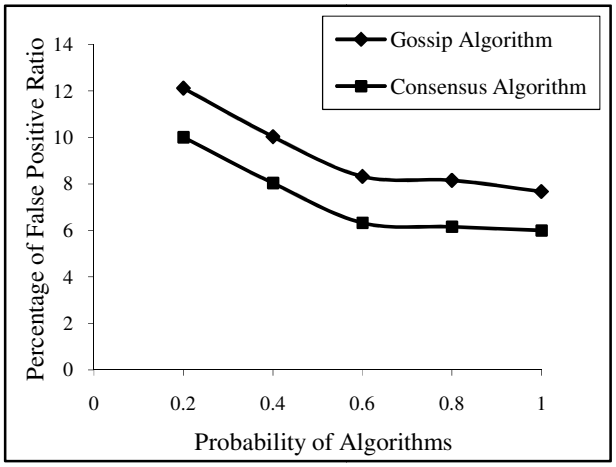

Fig.12. Performance analysis of consensus algorithm and Gossip algorithm

5. CONCLUSION AND FUTURE ENHANCEMENTS

Distributed denial o f service is a major threat that cannot be addressed through isolated actions of sparsely deployed defense nodes. Instead, various defense systems must organize into a framework and inter-operate, exchanging information and service, and acting together, against the threat. In this paper we proposed a global detection infrastructure by building an overlay network on top of the internet. The consensus algorithm is used to detect distributed denial of service attacks by information sharing. Compared to the existing solutions, this method has the

potential to achieve high true positive ratio. This work has been done by using consensus algorithms for exchanging the information between the detection systems. So the overall time consumption will be reduced for global decision making. This work can further be explored for locating the Zombies (compromised system) and for other types of attack.

REFERENCES

[1] Guangsen Zhang and Manish Parashar, "Cooperative Defense against DDoS attacks",Journal of Research and Practice in InformationTechnology, Vol .38, No.1, February 2006, pp. 69-74.

[2] Haining Wang, Danlu Zhang and Kang G.Shin," Change Point Monitoring for the Detection of DoS Attacks", IEEE Transactions On Dependable and Secure Computing, Vol.1, No.4, 2004.

[3] Wang, D. Zhang, and K. G. Shin, "Detecting SYN flooding attacks," In Proceeding of IEEE Infocom'2002, June 2002.

[4] Rocky.K.C.Chang,"Defending against Flooding–based, DDoS attacks", IEEE Communication magazine, Vol 40, No.10, 2002.

[5] Mirkovic, G. Prier, and P. Reiher, "Attacking DDoS at the Source," presented at ICNP 2002.

[6] John Haggerty, Qi Shi and Majid Merabti," Early Detection and Prevention of Denial-Of-service Attacks: A Novel Mechanism with Propogated Traced-Back Attack Blocking", IEEE Journal On selected Areasin Communication, Vol 23, No.10, October, 2005.