http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 6 (8): 1139-1145, 2007
ISSN 1812-5638

A Distributed Framework with less False Positive Ratio Against Distributed Denial of Service Attack

[1]S. Meenakshi and [2]S.K. Srivatsa
[1]Department of Information Technology,
Sathyabama University, Chennai, India
[2]St. Josephs' College of Engineering, Chennai, India

Abstract: Distributed denial of service is a major threat to the availability of Internet services. The distributed, large scale nature of the Internet, makes DDoS 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. In order to cope with the increase, many ISP (Internet Service Provider) customers introduced IDSs (Intrusion Detection System). However, the IDSs cannot always detect the network attacks due to dropping the packets when DDoS packets are aggregated to the customer's link. 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. Therefore more effective countermeasures are required to counter the threat. This requirement has motivated us to propose a novel mechanism against DDoS attack. This study presents the design details of a distributed defense mechanism against DDoS attack. The DDoS attack cannot be addressed through isolated actions of defense nodes. The effectiveness of attack detection increases near the victim and the effectiveness of packet filtering increases near the attack source. So we choose the detection system in the intermediate location to get benefits in both ways. 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. In our distributed IDS system, there is a corresponding true positive ratio. In this Distributed frame work, the information and services are exchanged between systems through which they act together against the threat.

Key words: DDoS attack, sequential test method, anomaly detection

INTRODUCTION

About DDoS: Denial of service attacks are a major cause of incorrect operation in the Internet and are arguably the most serious threat that the Internet community faces today. A Distributed Denial of Service (DDoS) attack is a large-scale, coordinated attack on the availability of services at a victim system or network resource as shown in Fig. 1. The DDoS attack is launched by sending an extremely large volume of packets to a target machine through the simultaneous cooperation of a large number of hosts that are distributed throughout the Internet. The attack traffic consumes the bandwidth resources of the network or the computing resource at the target host, so that legitimate requests will be discarded. The impact of these attacks can vary from minor inconvenience to the users of a web site, to serious financial losses to companies that rely on their on-line availability to do business.

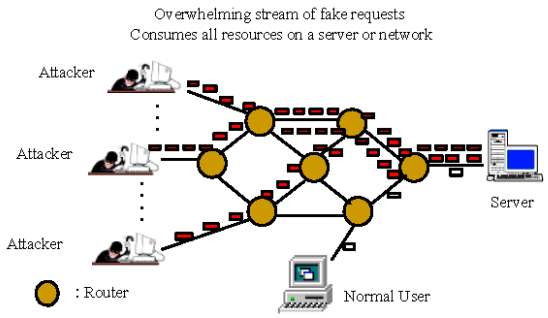

Fig. 1: Distributed denial of service attack

In February 2000, one of the first major DDoS attacks was waged against Yahoo.com (Zhang and Parashar, 2006). This attack kept Yahoo off the Internet for about 2 h and cost Yahoo a significant loss in advertising revenue. Another recent DDoS attack occurred on

Corresponding Author: S. Meenakshi, Department of Information Technology, Sathyabama University, Chennai, India

October 20, 2002 against the 13 root servers that provide the Domain Name System (DNS) service to Internet users around the world. They translate logical addresses such as www.yahoo.edu into a corresponding physical IP address, so that users can connect to websites through more easily remembered names rather than numbers. If all 13 servers were to go down, there would be disastrous problems accessing the World Wide Web. Although the attack only lasted for an hour and the effects were hardly noticeable to the average Internet user, it caused 7 of the 13 root servers to shut down, demonstrating the vulnerability of the Internet to DDoS attacks. If unchecked, more powerful DDoS attacks could potentially cripple or disable essential Internet services in minutes.

Flooding based distributed denial of service (DDoS) attack presents a very serious threat to the stability of the Internet. SYN Flooding: Although this type of attack benefits from TCP protocol features (TCP three-way handshake), we consider it as a flood attack, since its impact is due to flood principles. Due to the importance of this DDOS attack type, we present a detailed explanation of how it works.

TCP connection establishment (3 way handshake): When a system (called the client) attempts to establish a TCP connection to a system providing a service (the server), the client and server exchange a set sequence of messages (Fig. 2).

- The client system begins by sending a SYN message to the server.
- When the server receives the SYN message, it reserves some of its resources for the expected connection and sends a SYN-ACK message back to the client.
- The client then finishes establishing the connection by responding with an ACK message.
- After reception of the last message ACK from the server, the connection is successfully established and the two peers are able to start exchanging their data.

Attack description: The attacking system sends SYN messages with spoofed source IP address to the victim server system.

These appear to be legitimate but in fact reference a client system that does not exist or that will not respond to the SYN-ACK messages (Fig. 3). This means that the final ACK message will never sent to the victim server system. The allocated resources of the half-open TCP connections will only be released after time-out. Since system resources are finite and limited, the system will soon be unable to accept any new incoming connections.

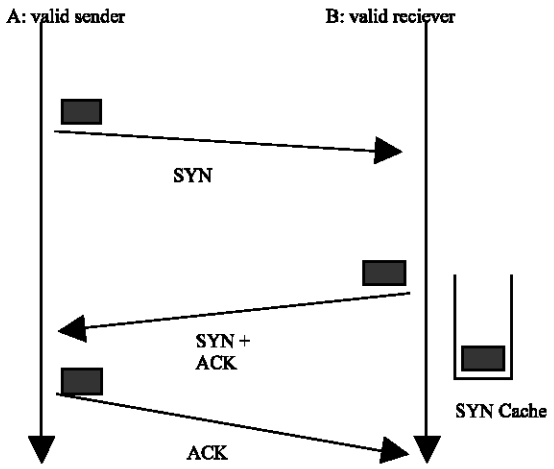

Fig. 2: TCP three way handshake

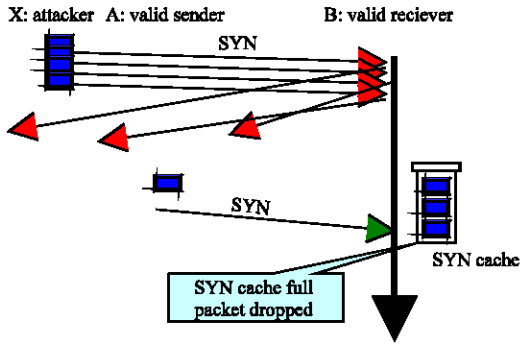

Fig. 3: TCP SYN flooding

The magnitude of the combined traffic is significant enough to exhaust system resources. The DDOS attacks against yahoo (Zhang and Parashar, 2006; Chen and Song, 2005) eBay, Amazon.com shows the vulnerability of even well equipped networks. There are more number of user friendly attack tools available. So DDoS attack launching becomes very easy. But, there is still a lack of effective solutions to defend against them in terms of aborting an ongoing attack in a timely fashion (Chen and Song, 2005; Specht, 2004).

This study presents the design details of a distributed defense mechanism against DDoS attack. The DDoS attack cannot be addressed through isolated actions of defense nodes. We used a comprehensive detection mechanism in the edge routers of each network. They act as local detection system for that network. Each local detection system communicate with other detection system to take global decision against the DDoS attack. The true positive ratio considerably increased in this system.

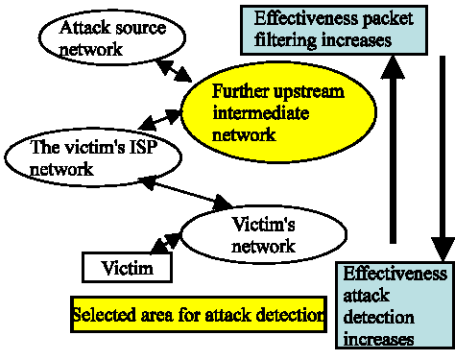

Fig. 4: DDoS attack detection location

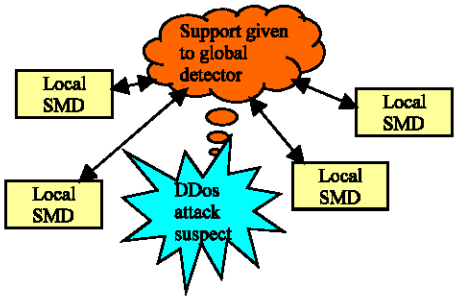

Fig. 5: Two level architecture

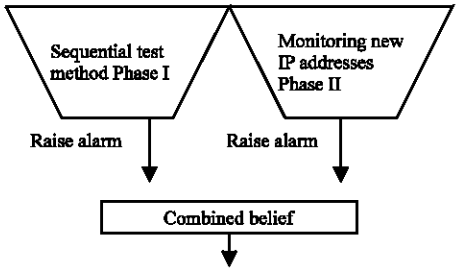

Fig. 6: Two phases of SMD

A Distributed Denial of Service (DDoS) attack is a large-scale, coordinated attack on the availability of services at a victim system or network resource. The DDoS attack is launched by sending an extremely large volume of packets to a target machine through the simultaneous cooperation of a large number of hosts that are distributed throughout the Internet. The attack traffic consumes the bandwidth resources of the network or the computing resource at the target host, so that legitimate requests will be discarded.

Due to the readily available tools, Flooding attack becomes most common DDoS attack. They intend to overflow and consume resources available to the victim. When the number of attackers is very large, the flows from each attacker can be very small to detect. So, detection based on instantaneous deviation will be useless. Because, the deviation will be very small in small flow (Mirkovic *et al*., 2002; Haggerty *et al*., 2005; Gil and Poleto, 2001). Most of the DDoS detection system models are based on traffic flow rates. As many new applications are coming up and End user's behavior also varies, it is difficult to get a general efficient model based on traffic flow alone.

So, we need a DDoS detection system which is not only based on traffic flow. We propose 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 we choose the detection system in the intermediate location to get benefits in both ways (Fig. 4).

Proposed work: One major challenge in detection system design is to process packets at very high speeds, especially when placed in backbone 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 detection process with two levels: Local detection and Global detection (Fig. 5).

The combined belief of all local Sequential Method Detection (SMD) systems is considered to detect the DDoS attack globally. The sequential analysis test is very much useful to reduce detection time and to reduce misdetection rates. It is possible to balance the trade of between the three quantities namely detection time, false alarm and misdetection rate.

IMPLEMENTATION

The proposed method consists of two levels (Fig. 5).

System architecture: The system consists of two levels namely

- Local Detection system-SMD (Sequential Test Method Detector).
- Global Detector.

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 (Fig. 6).

Phase 1 sequential test method: 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 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'.

$\sum_{t=1}^{n} Xi$ = Total number of requests-corresponding replies for one sampling period

This value is normalized by R' as follows

$$\Delta n = \sum_{t=1}^{n} Xi / R'$$

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

- H = 0 (Null hypothesis) ---Normal situation
  H = 1 (Alternative hypothesis) --- abnormal situation.
- Sequence of observed data
  X1,X2,X3,...Xn
- Decision consists of
  -Stopping time N(stop taking samples)
  -Make a hypothesis – H=0 (or) H=1 ?

Now (Fig. 7) the alarm is raised if the Δn value exceeds the threshold value N.

Phase. 2 monitoring new IP addresses: Monitoring the percentage of new IP addresses is effective in detecting

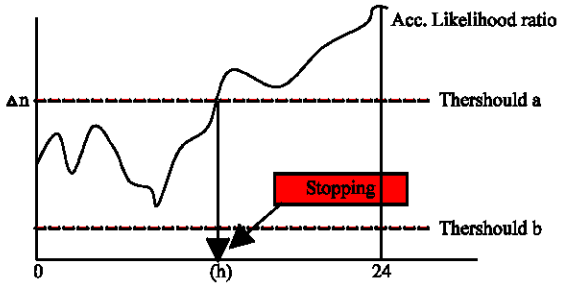

Fig. 7: SMD Detection method

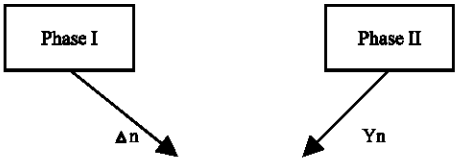

Fig. 8: Decision making based on Combined belief

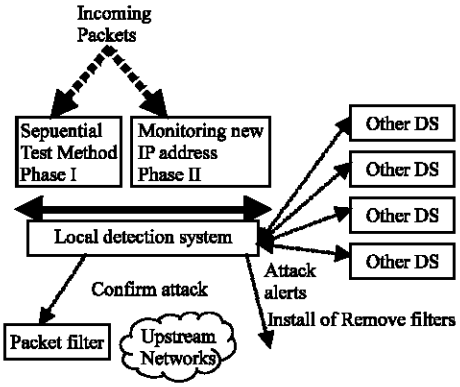

Fig. 9: Two-level attack detection in the distributed detection approach

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.

$$Yn = \frac{|M| - |M \cup F|}{|F|},$$

Where:

Yn = The percentage of new IP addresses in time interval T. When this value Yn exceeds the threshold value say N, then alarm is raised.

DDoS detection: When both phase I and phase II raise alarms, based on the combined belief DDoS attack is

confirmed (Fig. 8). Based on the values of Δn and Yn the hypothesis is decided and DDoS attack is confirmed.

$$P(H/\Delta n, Yn)$$

Where:

P = Decision function which is deciding over DDoS attack confirmation
H = 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 supports 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 (Fig. 9).

SIMULATION RESULTS

The simulation Model is implemented in Network Simulator software (NS2). In the Simulation Model we set up three networks Configured with 16 nodes (3 networks) and 2 edge routers. Script is written using Tool Command Language (TCL). The output of this topology construction (Fig. 10). Egress routers are represented as red nodes and normal nodes are represented as black nodes. Egress router is the one through which all nodes sends the traffic(flow of packet).

The Fig. 11 shows how data packets are transferred from one node to other. In this topology, there are 3 different networks. They are 2 source network and 1, destination network. The source network 1 composed of node 5, 6, 7, 8 and Detection system node 9. The source

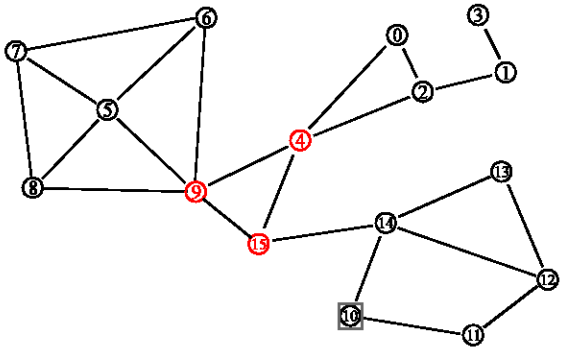

Fig. 10: Constructing a model with three networks

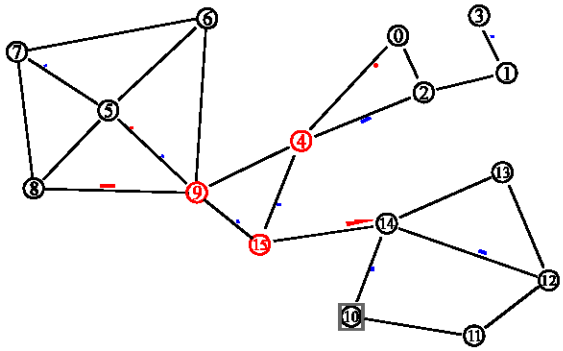

Fig. 11: Traffic flow through the networks

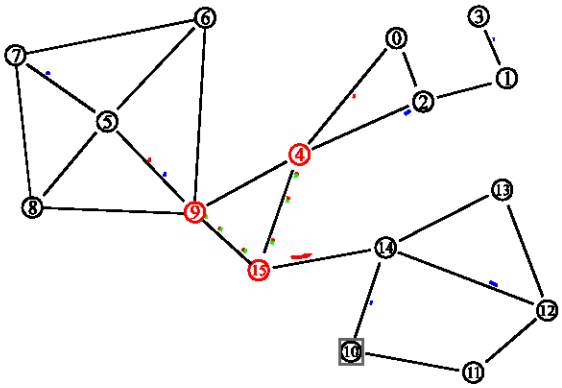

Fig. 12: Local detection system share attack alerts with other DS

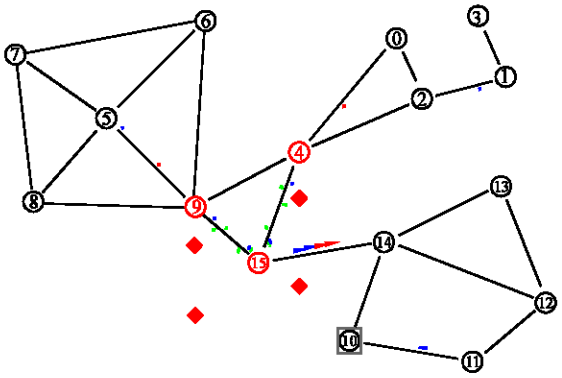

Fig. 13: Detecting and blocking attack traffic

network 2 composed of node 0, 1, 2, 3 and detection system node 4. The destination network composed of node 10, 11, 12, 13, 14 and detection system node 15.

The detection systems 4, 9 and 15 share their knowledge and take global decision. The detection system node 15 installs filter based on this decision (Fig. 12) and also instructs the other upstream routers to install filters (Fig. 13).

PERFORMANCE

Even though anomaly based IDSs are widespread and successful in most environments, they possess various disadvantages, too. The main drawback with anamoly 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 (Specht, 2004) raised by the IDS and the actual intrusion scenario, the following types of detection results are possible (Fig. 14).

True Positive: Occur When the actual attack occurs.
True negative: Normal activity of IDS.
False Positive: Typically known as false alarms. These occur when IDS reads legirimate activity as being an attack.
False Negative: When a potential attack is missed.

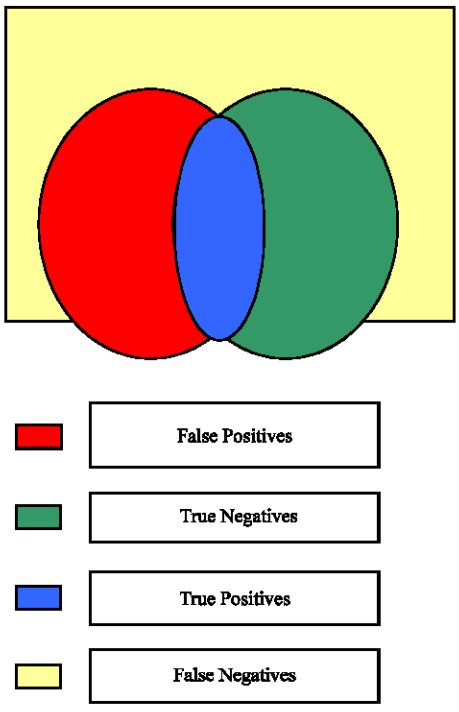

Fig. 14: Detection issues in IDSs

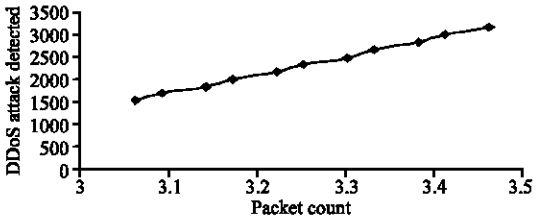

Fig. 15: True positive ratio

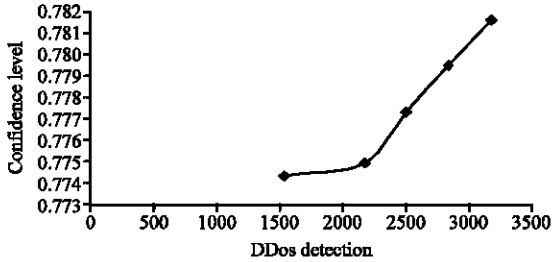

Fig. 16: Confidence level (Based on DDoS detection)

DDoS attacks generate a large volume flow to overwhelm the target host. 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. In our distributed IDS system, there is a corresponding true positive ratio (Fig. 15). More over, the global decision is made based on the confidence level generated at each individual defense node. So, False positive is also reduced. Fig. 16 shows the confidence level generated based on DDoS attack detected.

CONCLUSION AND FUTURE ENHANCEMENT

Traditional Intrusion Detection Systems (IDS) result in high false alarms when used to detect DDoS attacks. By cooperation, we can improve the accuracy of DDoS detection. However, given the large number of nodes in the Internet, we need a scalable and efficient self organizing architecture to share the information among the individual detection systems. The primary contribution of this paper is to propose a global detection infrastructure by sharing attack information between the local detection systems. Unlike the traditional IDSs this method has the potential to achieve high true positive ratio. This work can further be explored by using consensus algorithms for exchanging the information

between the detection systems. So the overall time consumption will be reduced for global decision making.

REFERENCES

Chen, S. and Q. Song, 2005. Perimeter-based defense against bandwidth DDoS attacks. IEEE Trans. Parallel and Distributed Syst., 16: 6.

Gil, T.M. and M. Poleto, 2001. MULTOPS: A data-structure for bandwidth attack detection. In: Proceedings of 10th Usenix Security Symposium, Washington, DC., pp: 23-38.

Haggerty, J., Q.I. SHI and M. Merabti, 2005. Early detection and prevention of denial-of-service attacks: A novel mechanism with propagated traced-back attack blocking. IEEE J. Selected Areasin Commun., 23: 10.

Mirkovic, J., G. Prier and P. Reiher, 2002. Attacking DDoS at the Source, Presented at ICNP.

Specht, S.M., 2004. Electrical engineering, princeton university, ruby b lee, electrical engineering, princeton university, distributed denial of service: Taxonomies of attacks, tools and countermeasures. Proceedings 17th International Conference on parallel and distributed computing system, International Workshop on Security in Parallel and Distributed System, pp: 543-550.

Zhang, G. and M. Parashar, 2006. Department of electrical and computer engineering, RUTGERS. The State University of New Jersey, Cooperative defense against DDoS attacks. J. Res. Practice Inform. Technol., 38: 1.