Volume 2, No. 7, July 2011
Journal of Global Research in Computer Science
ISSN-2229-371X
RESEARCH PAPER
Available Online at www.jgrcs.info

ANALYSIS OF DDoS ATTACKS IN DISTRIBUTED PEER TO PEER NETWORKS

Vooka Pavan Kumar[1*], Abhinava Sundaram.P[2], Munnaluri Bharath Kumar[3], N.Ch.S.N.Iyengar[4]

[1234]School of Computing Science and Engineering, VIT University, Vellore, Tamil Nadu, India
[1]vookapavankumar@gmail.com
[4]nchsniyengar48@gmail.com

Abstract: The term 'peer-to-peer' generally describes a class of systems that employ distributed resources to perform a specific function in a decentralized manner. Distributed P2P networks are widely used for file sharing and in such a scenario, a Distributed P2P network could be easily exploited by an attacker to establish a DDoS attack against any arbitrary host on the internet. Distributed denials of service (DDoS) attacks are very hard to detect and regarded as a major threat to the Internet. Though a number of techniques have been proposed to defeat DDoS attacks in Distributed P2P networks, it is still very hard to respond to flooding- based DDoS attacks due to a large number of attacking machines and the use of source- address spoofing. An efficient framework has been designed to detect and defend against DDoS attacks in Distributed Peer-to-Peer networks. It defends against attacks by considering the distance between the source ends and the victim end and also the Time-to-Live (TTL) value in IP header. The proposed system has three major components: DDoS detection, agent-based trace back, and traffic control. The agent based mechanism is used to keep track of all the node details (e.g. bandwidth, node capacity, etc). The proposed system can be evaluated on a network simulation platform called NS2. The results demonstrate that the detection techniques are capable of detecting DDoS attacks accurately, and the defence mechanism can efficiently control attack traffic in order to maintain the quality of service for legitimate traffic. Also, the framework shows better performance in defeating the DDoS attacks in Distributed P2P networks compared to the other existing techniques.

***Keywords*:** Distributed Peer-to-Peer Networks, Distributed Denial of Service Attack, Time-to-Live, Internet Protocol

INTRODUCTION

Distributed denials of service (DDoS) attacks are widely regarded as a major threat to the Internet. A flooding-based DDoS attack is a very common way to attack a victim machine by sending a large amount of malicious traffic. The distributed nature of DDoS problem requires a distributed solution in Distributed P2P networks. DDoS is a serious problem that has not been solved completely yet and is still an active area of research. In a nutshell, DDoS attacks target the availability of resources, infrastructure and hosts on the Internet and prevent them from performing their legitimate functionality. DDoS attacks can be classified into one of the following categories:

1. Resource Exhaustion (Bandwidth, CPU, Memory..)
2. Vulnerability Attacks
3. Protocol Attacks

A Distributed Denial of Service (DDoS) occurs when users or hosts are prevented from utilizing a legitimate service provided by a system. The most widespread method of creating a DDoS in a Distributed P2P network is by artificial exhaustion of a resource, such as bandwidth, processor cycles, or memory. A Distributed Denial of Service (DDoS) attack is one in which an attacker uses the combined power of many hosts to exhaust the resources of a server system. The separation of traffic into aggregates will make it easier for an attacker to target a specific subset of traffic flowing in the network.

MOTIVATION

All Internet Service Providers (ISPs) face the consequence of increasing amounts of un- wanted and malicious traffic. A DDoS attack is difficult to be stopped quickly and effectively. Hence, a powerful mechanism is required to detect and mitigate the DDoS attacks in Distributed Peer to Peer networks.

The primary goal is to analyze and mitigate the effects of Distributed Denial of Service attacks in distributed P2P networks. It includes the following:

1. A strong detection technique should detect a DDoS attack with high reliability and at an early stage of the attack.
2. A good response technique should drop most of the attack packets without sacrificing the QoS in a network (using the agent-based technique).
3. The defense framework should work effectively in distributed P2P networks.
4. Analyze the performance of distributed P2P network subjected to DDoS attack.

An agent-based distributed DDoS defense framework is proposed which defends against attacks by coordinating the distance between the source ends and the victim end using the agents which keep track of the node details like bandwidth, node capacity, etc along with the time-to-live value. Also, the Quality of Service (QoS) can be provided using the differentiated services (diffserv). The proposed agent-based defence system has three major components: detection, agent-based trace back, and traffic control. Developing strong mechanisms against these attacks can effectively minimize their effect on saturating Internet links and preventing legitimate traffic from reaching its destination. The performance of this technique is verified and compared to the results obtained by simulation.

RELATED WORK

Distributed Denial of service attacks are a lower level attack that are used against P2P systems and these have a great impact on legitimate traffic. Lower level attacks focus

on the communication aspect (TCP/IP) of P2P systems. Generally, a DDoS attack is an attempt to make a computer resource unavailable to those who intend to use it. [6] The most common form of DDoS attack is flood of packets that are invalid.

Compromised hosts are gathered to send useless service requests at the same time. The burst of generated traffic crashes the victim or disables it. Threats of DDoS attacks include:

- Hard to detect and stop.
- Can spread within few minutes
- Usually period of flooding lasts for a few hours and is sporadic
- IP spoofing makes it harder to identify the attackers.

There are two approaches [2] that can be used to launch a DDoS attack in Overnet, which is one of the largest P2P file sharing network. The first one involves poisoning the distributed file indexes, which leads to TCP Connection DDoS attack, and the second one involves poisoning the routing table of the peers, leading to Bandwidth Flooding DDoS attack.

Distributed packet filtering [6] technique to detect and filter out TCP packets with spoofed source IP address used for Distributed Reflection Denial of Service (DRDoS) attacks. But the proposed models have not focused on the physical attacks that are possible on P2P systems. These kinds of attacks need an efficient and effective algorithm to protect the network resources.

The Path Identification mechanism [9] features many unique properties. It is a per-packet deterministic mechanism: each packet traveling along the same path carries the same identifier. This allows the victim to take a proactive role in defending against a DDoS attack by using the Pi mark to filter out packets matching the attackers' identifiers on a per packet basis. The Pi scheme performs well under large-scale DDoS attacks consisting of thousands of attackers, and is effective even when only half the routers in the Internet participate in packet marking.

Pi marking and filtering models fail to detect IP spoofing attacks with just a single attack packet. Finally, there is a need to propose an effective mechanism where the victim needs to identify only a single attack packet in order to block all subsequent packets arriving from the same path, and from the same attacker. The results can be shown through simulations in ns2 (Network Simulator).

APPROACH

DDoS attacks continue to grow not only in size and frequency but also in variety. The fluidity and span of today's DDoS problem demands specialized, systematic attention in order to effectively mitigate such attacks. An efficient algorithm is required which can reduce the impact of DDoS on distributed Peer to Peer networks and also provide a complete study and analysis of possible network attacks.

Distributed Cooperative Architecture of DDoS

The main objective is to control unwanted traffic by mitigating flooding-based DDoS attacks in IP-based networks. This concentrates especially on the following objectives:

A detection technique should detect a DDoS attack

1. with high reliability and at an early stage of the attack in a distributed P2P network.
2. A response technique should drop most of the attack packets without sacrificing the QoS for legitimate traffic.
3. The defence framework k should work effectively in distributed P2P network environments.

Before real attack traffic reaches the victim, the attacker must cooperate with all its DDoS agents. Therefore, there must be control channels between the agents and the attacker. This cooperation requires all agents send traffic based on commands received from the attacker. The network which consists of the attacker, agents, and control channels is called the attack networks. Attack networks [10] are divided into three types: the agent-handle model, the Internet Relay Chat (IRC)-based model, and the reflector model.

IP Spoofing

IP spoofing is used in all DDoS attacks as a basic mechanism to hide the real address of agents or the attacker. In a classical DDoS attack, the agents randomly spoof the source addresses in the IP header. In a reflector-based DDoS attack, agents must put the victim's address in the source address field. The spoofed addresses can be addresses of either existing or non-existing hosts. To avoid ingress filtering, the attacker can use addresses that are valid in the internal network because non-existing addresses have a high possibility of being filtered out.

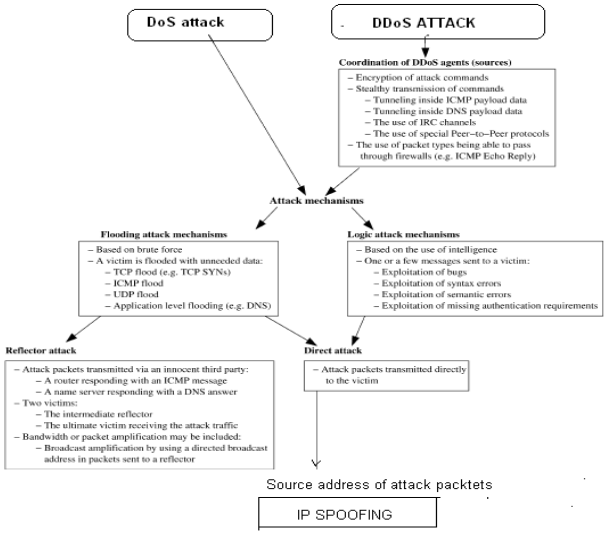


Figure 1: Major attack mechanisms used by DDoS ATTACKS

In the real-world, it is possible to launch an attack without IP spoofing if the attacker can compromise enough hosts. For this situation, the attacker would consider how to avoid to be traced out. Usually, the attacker will use a chain of compromised hosts. Tracing a chain which extends across multiple countries is very hard to be achieved. Furthermore, to compromise poorly monitored hosts in a network will make tracing more difficult due to a lack of information. In these situations, IP spoofing is not a necessary step for hiding the attacker.

Flooding DDoS Attack Mechanisms

Flooding-based DDoS attacks involve agents or reflectors sending a large volume of unwanted traffic to the victim. The victim will be out of service for legitimate traffic because its connection resources are used up. Common connection resources include bandwidth and connection control in the

victim system. Generally, flooding-based DDoS attacks consist of two types: direct and reflector attacks.

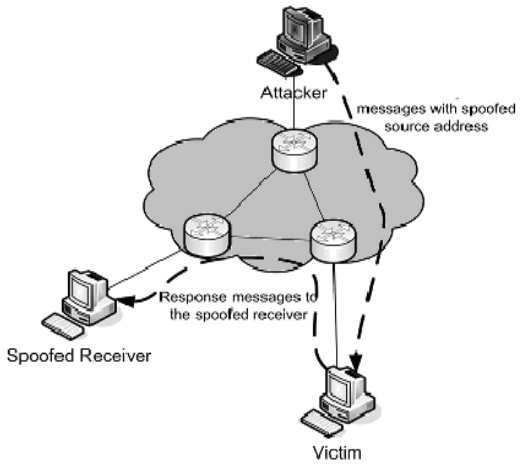


Figure 2: A direct flooding-based DDoS attack

The agents send the Transmission Control Protocol/Internet Protocol (TCP/IP), the Internet Control Message Protocol (ICMP), the User Datagram Protocol (UDP), and other packets to the victim directly. The response packets from the victim will reach the spoofed receivers due to IP spoofing. In a reflector attack, the response packets from reflectors truly attack the victim. No response packets need be sent back to reflectors from the victim. The key factors to accomplishing a reflector attack include: setting the victim address in the source field of the IP header and finding enough reflectors.

Direct attacks usually choose three mechanisms: TCP SYN flooding, ICMP echo flooding, and UDP data flooding. The TCP SYN flooding mechanism is different from the other two mechanisms. It causes the victim to run out of all available TCP connection control resources by sending a large number of TCP SYN packets. The victim cannot accept a new connection from a legitimate user without new available control resources. ICMP echo flooding-based attacks will consume all available bandwidth as a large number of ICMP ECHO REPLY packets arrive at the victim. UDP data flooding-based attacks achieve the same result as ICMP echo attacks by sending a large number of UDP packets to either random or specified ports on the victim.

ARCHITECTURE OF PROPOSED FRAMEWORK

The current network systems can simply be classified into two domains. The first domain is the core routing network. This network usually consists of high-speed routers. It is the basic network which is in charge of transferring traffic among multiple edge networks. The edge network is another domain which connects to a core network through edge routers. An edge network usually represents a single customer network. Usually, there does not exist a huge volume of traffic which needs to be forwarded by edge routers.

While distributed denial of service (DDoS) attack traffic is being transmitted across the network towards the victim, the defence system in the victim-end edge network can easily detect the attack because attack traffic creates a larger set of anomalies at the victim end than at the source ends. However, it is impossible for the defence system to react to the attacks in the victim-end edge network when the attacks are heavy. The agent-based DDoS detection technique detect DDoS attacks in the victim-end edge network by recognizing anomalous variations in TTL values of spoofed address and the victim node. The agents keep track of all the necessary node details which enable the detection of DDoS attacks in Distributed P2P networks more effectively.

To drop attack packets effectively, an attack traffic rate limit control will be triggered in the source-end edge network after receiving an alert message from the defence system of the victim-end edge network. To find all source-end edge networks, we can use the existing Fast Internet Traceback (FIT) technique[11]. In the distributed framework, all edge routers should mark the distance from the victim and their IP address into the 16 bit IP identification field of the IP header. The agent-based detection and response techniques will use this information.

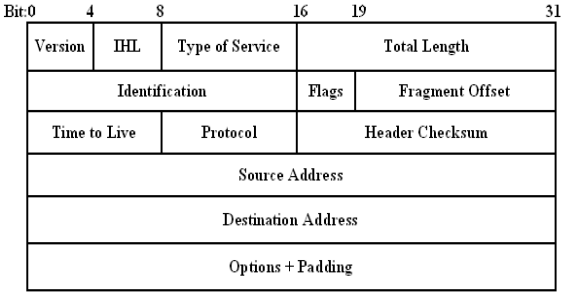


Figure 3: IP Header

A TTL (Time to Live) is an 8-bit field to specify the maximum lifetime of an IP packet. During transit, each router decrements the TTL value of an IP packet by one. When an IP datagram (each contains an 8 bit header field called TTL) is constructed for transmission, the source assigns a constant integer (in the range of 0-255) as the initial TTL value. As the datagram moves from the source to the destination through intermediate routers (inter-connecting devices), each router along the path decrements the TTL value by one, and the datagram is forwarded to the next router only if the TTL is greater than zero. As per the IP standard, the router should discard a datagram with TTL value zero. The primary objective of the TTL is to ensure that the datagram should not wander the Internet for ever due to problems like routing loops.

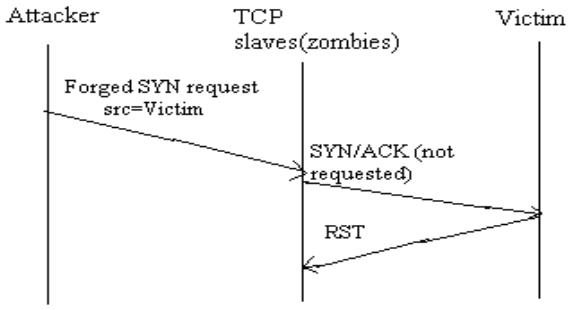


Figure 4: Three- way handshake during attack

In the above diagram, both SYN and RST packets will contain the same source IP address. In the case of SYN packet, the IP addressed is spoofed, where as in the case of RST, it is the actual IP address of the victim. Thus, the TCP filter has two packets claiming to be originating from the same machine. Assuming that there is no route change in the network path, these two packets are supposed to have the

same TTL value. If the TTL values are different, it is likely that the SYN packet has a spoofed source IP address. It is significant that the RST packet is generated by the victim in response to SYN/ACK packet and the attacker has no control on it. Hence the IP address seen in the RST packet can be trusted.

Fig. 5 illustrates the whole operation of defending in the event of a DDoS attack. Alert messages between a victim end and a source end include three types: Request messages, Update messages, and Cancel messages. These messages are used in different phases of defeating a DDoS attack. At the beginning of an attack, a request message from a victim end will provide a suggested rate limit value to a source end. If the volume of attack traffic still increases aggressively, an update message will be sent to the source end again. This might slightly increase the burden on victim, however this message is necessary to keep the rate limit under control and monitor the source-end. Based on the requirements in the message, the source-end defence system will decrease the rate limit value exponentially. After the traffic at the victim end has returned to normal for a while, an update message sent to the source end asks it to increase the rate limit value linearly. Finally, if the defence system has not found any anomalous changes in the victim end since the update message, a cancel message to remove the rate limit at the source end is sent. Due to the unwanted flooded traffic, there is a possibility that the message sent by victim to source end may not even reach the source node. To overcome this problem, the request and update messages are sent repeatedly by victim to source end until proper acknowledgement is received from the source.

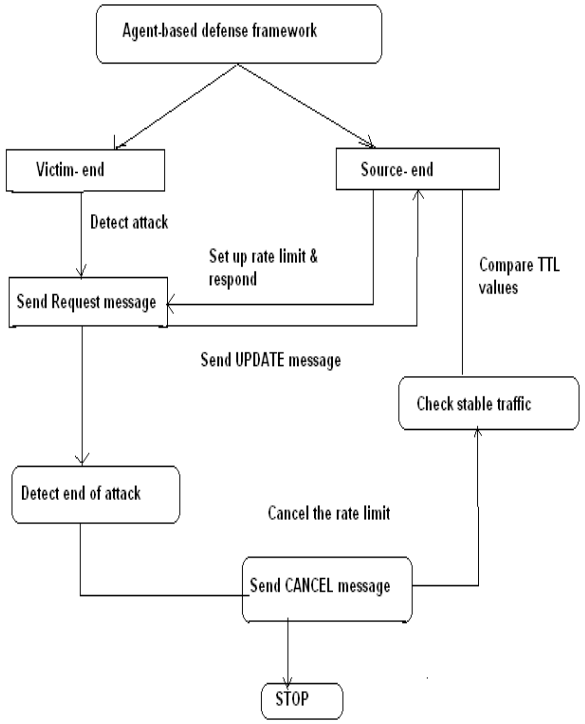


Figure 5: Flow chart depicting the defence framework and architecture

The problems in the existing detection techniques are as follows:

1. The weak connections between selected attributes and DDoS attacks make the detection schemes ineffective.

2. The time to reveal the anomalous conditions is too long due to complex computations.

Existing DDoS detection techniques are mainly categorized into two types: DDoS detection based on analysis of IP attributes and DDoS detection based on traffic volume. To respond to a DDoS attack, packet filtering tries to filter out attack traffic based on DDoS attack signatures. However, it is hard to get attack signatures for current DDoS attacks because attack traffic is similar to normal traffic. Another problem with packet filtering techniques is collateral damage for legitimate traffic. In contrast, recent studies show that rate limit techniques can mitigate an attack effectively by setting up fitting rate limits on attack traffic. At the same time, it will not lead to serious collateral damage for legitimate traffic. Finally, correlation analysis can be made between the RTT values and the router buffer occupancy at the bottleneck links and the results can be compared to that of an attack scenario and without the DDoS attack. In Agent based defence mechanism, agents need not be monitored always to know about the nodes, because it might increase the overhead of the network. Hence it can be monitored at fixed regular intervals.

To demonstrate the improvements of the framework in defeating DDoS attacks, we compare results in three situations. In the first situation, start the attack on NS2 simulation network without enabling any DDoS defence mechanisms. The edge router at the victim end just drops all packets which it cannot handle. In the second situation, deploy the framework in the NS2 simulation network. Each router will detect the aggregate of its local traffic and attempt to lower traffic in cooperation with upstream routers. In the final situation, deploy the agent-based DDoS defence framework in the same NS2 simulation network. The following code snippet describes few changes made to the header files in ns2 which differentiates the spoofed IP address and the actual address of victim using the TTL value. The changes are made in diffserv folder which is responsible for providing Quality of Service(QoS). Various files like the queue.h, dsred.h, icmp.h, dsredq.h have been inherited in the c++ file and their functionalities are utilised.

```
TTL_SOURCE=iph->ttl();
TTL_INCOMING=iph->inc();
ns_address src = iph->src();
ns_address dst = iph->dst();
bool accept=true;
bool drop = false;
  //if TTL_VALUE is invalid, drop without any other processing
          if (codePt == dsFeedback::INVALID_CP){
        cout << "Dropped due to invalid TTL" << endl;
                    stats.drops_FB++;
//increment count of feedback drops
                      stats.drops++;
                        drop(pkt);
                      dropped = true;
    } #endif
 if (!dropped) {
        //allow transfer of packet to the destined node.
          if(TTL_SOURCE == TTL_INCOMING){
          lookupPHBTable(codePt, &queue, &prec);

            hdr_flags* hf = hdr_flags::access(pkt);
              if (ecn_ && hf->ect()) ecn = 1;
                stats.pkts_CP[codePt]++;
```

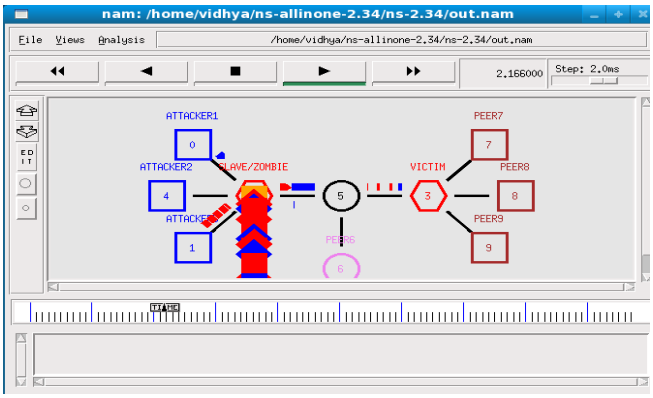
```
//intimate the packet drop to source node by peer node
        cout << "Dropped by peer node." << endl;
  if
(!Feedback::isFeedbackRunning(src,dst))
{
          Feedback::dropNotify(src, dst,
       now, icmpAgent);        }
#endif
cout << "Early dropped." << endl;
#ifdef ds_feedback_h
//notify sender of packet dropped by the domain router
if (!dsFeedback::isFeedbackRunning(src,dst)) {
dsFeedback::dropNotify(src, dst, now, icmpAgent);
} #endif
```

OBSERVATION AND RESULTS

The snapshots are provided for the DDoS attack simulations in distributed Peer to Peer networks. Graphs are plotted for the purpose of comparison and performance analysis. Also, the correlation coefficients between the RTT values and router buffer occupancy at the bottleneck links are calculated using MATLAB.

Correlation(r) = NΣXY - (ΣX)(ΣY) / Sqrt([NΣX^2 - (ΣX)^2][NΣY^2 - (ΣY)^2])

These snapshots given below depict the Distributed Denial of Service attacks in wired and wireless P2P networks. It includes the ultra-peers, the attackers, slaves/zombies (controlled by the attacker) and the victim.



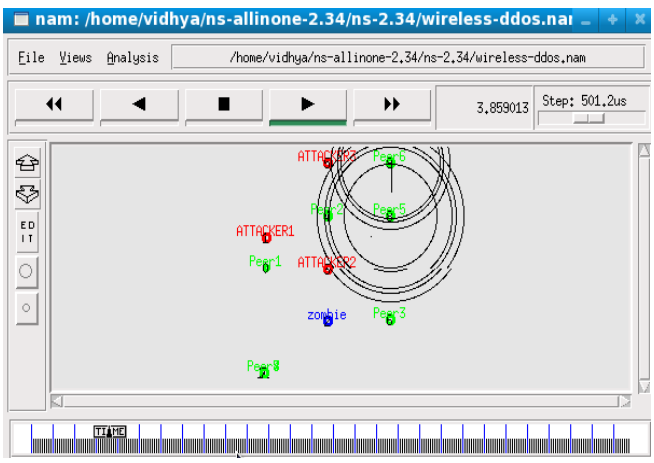


Table.I Correlation Coefficients without Attack

RTT vs Qsize	Qsizen2n	Qsizen3n	Qsizen5n
RTT 1	0.4074	0.7287	0.7663
RTT 2	0.471	0.8852	0.7717
RTT 3	0.4620	0.5674	0.6448

Table.II Correlation Coefficients with Attack

RTT vs Qsize	Qsizen2n	Qsizen3n	Qsizen5n
RTT1	-0.2208	0.1099	0.1134
RTT2	-0.2326	0.5532	0.5482
RTT3	-0.1764	0.5701	0.5973
RTT4	-0.6216	0.1880	0.2606
RTT5	-0.6468	0.1335	0.1848

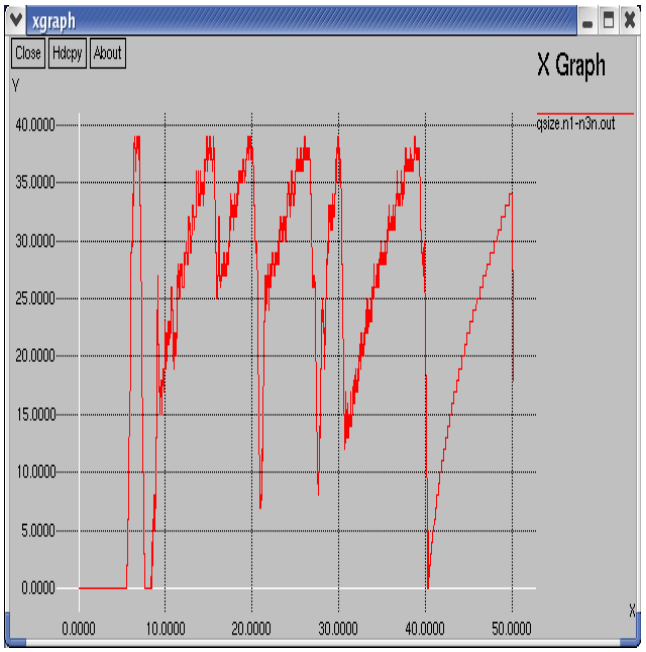
Table .III Replacing FIFO by RED

RTT vs Qsize	Qsizen2n	Qsizen3n	Qsizen5n
RTT1	0.2105	0.4595	-0.1579
RTT2	0.1228	0.2362	-0.0556
RTT3	0.0210	0.0791	-0.0394
RTT4	0.0491	0.0547	-0.0139
RTT5	-0.0058	0.0340	0.0175

GRAPHS OBTAINED

Queue-size Graphs

Time Vs Queue-size (no attack)

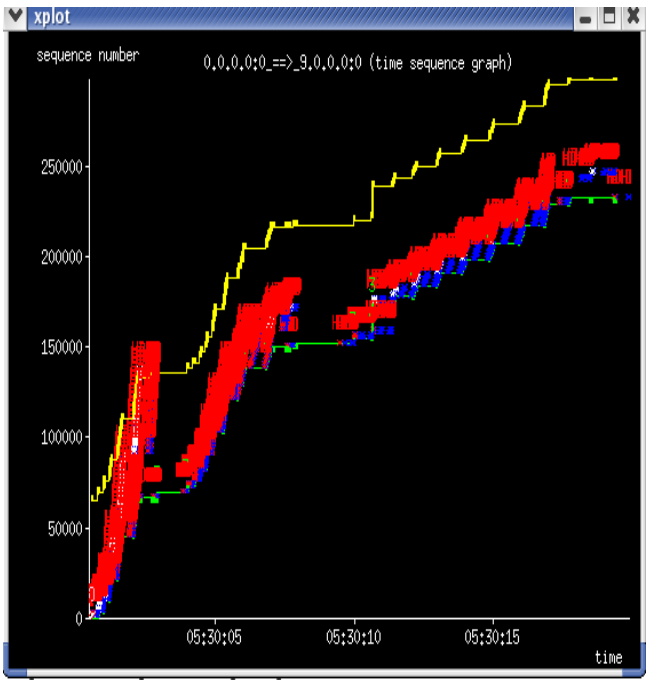


Time Vs Queuesize (under attack)

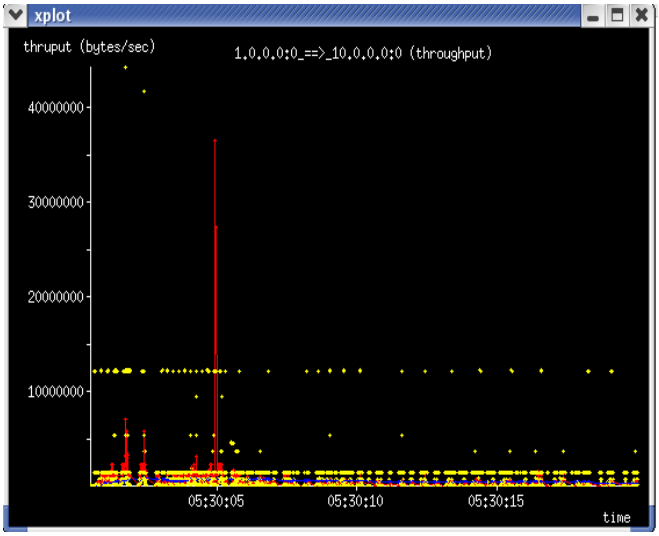
Time Sequence Graph

The calculated throughput and correlation coefficients decrease rapidly when subjected to Distributed Denial of Service Attack. The graphs given above clearly indicate that the proposed agent-based mechanism has reduced the effect of DDoS attack on distributed Peer-to-Peer networks. It has also increased the throughput of packet transmission and hence we can observe minimum packet loss in the network.

We can conclude from the above mechanism that with little effort in optimizing the attack, a significant amount of packet loss can be minimized and packets can be properly directed to the destination host.



3. Throughput Graph



CONCLUSIONS

After analyzing many existing DDoS detection and response techniques along with defence frameworks, it is clear that the major challenges of DDoS defence are to detect attacks quickly and with high effectiveness and to control attack traffic so as to sustain QoS for legitimate traffic. To address these challenges, an efficient DDoS attack detection technique has been analysed which works with very little communication overhead.

Basically, the process of defence can be divided into three phases. At the beginning of an attack, an agent-based detection technique can detect the attack if there are anomalous variations of average distance values and traffic rates at different distances at the victim end. Then the defence system at the victim end attempts to find all edge routers that are forwarding attack traffic aggressively. Finally, a series of alert messages will be sent to the source-end defence systems, which set up rate limits on each edge router based on the received information and its own drop rate.

The recovery process will be triggered if traffic at the victim end has returned to normal. DiffServ is used to provide the Quality of Service. It is not always possible to completely prevent these attacks, because there will always be vulnerable hosts in the internet to be compromised for attack purposes and also many DDoS attack mechanisms are available. But, the proposed method of detecting and mitigating attacks has proved to be more effective than the existing methods showing a better performance.

REFERENCES

[1] S. Gokhale and P. Dasgupta, "Distributed Authentication for Peer-to-Peer Networks," in Proceedings *IEEE Workshop on Security and Assurance in Ad hoc Networks*, 2003.

[2]Pankaj Kohli and Umadevi Ganugula, "DDoS attacks using P2P networks",2 007

[3]William Stallings, "Data and computer communications", Pearson Education, 7th Ed, 2003.

[4]G. Steve, "Distributed reflection denial of service," http://grc.com/ dos/drdos.htm.

[5]J. Postel, "Transmission Control Protocol," RFC 793, September 1981.

[6] S. Sivapooranam, V. Anil Kumar, G. K. Patra, Dr.N.Ch.S.N.Iyengar, "Analysis of Reflector based Distributed Denial of Service Attacks", *ICSCIS*-2007

[7] Ruichuan Chen, Eng Keong Lua, Jon Crowcroft, Wenjia Guo, Liyong Tang, Zhong Chen1, "Securing Peer-to-Peer Content Sharing Service from Poisoning Attacks", *Eighth International Conference on Peer-to-Peer Computing* (P2P'08)

[8] D. Dumitriu, E. W. Knightly, A. Kuzmanovic, I. Stoica, and W. Zwaenepoel. *Denial of-service resilience in peer-to-peer file sharing systems.*

[9]Abraham Yaar, Adrian Perrig, Dawn Song, "Pi: A Path Identification Mechanism to defend against DDoS attacks", *Proceedings of the 2003 IEEE Symposium on Security and Privacy* (SP.03)1081-6011/03

[10] S. M. Specht and R. B. Lee, \Distributed denial of service: taxonomies of attacks, tools and countermeasures." in *Proceedings of the 17th International Conference on Parallel and Distributed Computing Systems*, September 2004, pp. 543-550.

[11] A. Yaar, A. Perrig, and D. Song, \FIT: fast internet traceback," in *Proceedings of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, 2005, pp. 1395- 1406.

[12]V. Shyamaladevi, Dr.R.S.D.WahidaBanu, "Detection of Spoofing Attacks Using Intrusive Filters For DDoS", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.10, October 2008

[13]Kemal Bicakci , Bulent Tavli , "Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks", Computer Standards & Interfaces 31 (2009) 931–941. journal homepage: www.elsevier.com/locate/csi.

[14]Qijun Gu , Peng Liu, Chao-Hsien Chu, "Analysis of area-congestion-based DDoS attacks in ad hoc Networks", Ad Hoc Networks 5 (2007

[15] Benjamin Armbruster , J. Cole Smith , Kihong Park, "A packet filter placement problem with Application to defense against spoofed denial of service attacks", European Journal of Operational Research 176 (2007) 1283–1292

