International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 3 Issue: 11
ISSN: 2454-4248
583 – 588

A Review on Distributed Denial of Service Attack On Network Traffic

Aakash Tiwari
Rungta College of Engineering and Technology, Bhilai
Dept. of Computer Science and Engineering
Bhilai, Chhattisgarh, India
aakashtiwari91@gmail.com

Asst. Prof. Toran Verma
Rungta College of Engineering and Technology, Bhilai
Dept. of Computer Science and Engineering
Bhilai, Chhattisgarh, India
Vermatoran24@gmail.com

***Abstract*—** Distributed Denial of Service (DDoS) attacks is the most difficult issues for network security. The attacker utilizes vast number of traded off hosts to dispatch attack on victim. Different DDoS defense components go for distinguishing and keeping the attack traffic. The adequacy relies upon the purpose of sending. The reason for this paper is to examine different detection and defense mechanism, their execution and deployment attributes. This helps in understanding which barrier ought to be sent under what conditions and at what areas.

***Keywords*—** *DDoS attacks, defense, deployment, Types of DDoS Attack.*

*****

I. INTRODUCTION

Distributed Denial of Service (DDoS) is the organized endeavor to bargain the accessibility of system resources or servers as appeared in figure 1. These attacks make money related misfortunes by hindering true blue access servers and online administrations. To moderate the effect of these attacks solid safeguard components are required that can identify and prevent progressing attacks. Numerous resistance instruments have been proposed and sent at different areas in current web. The viability of these systems relies upon the execution exchange offs and cost acquired in deployment.

DDoS recognition systems recognize the deviation of movement from typical conduct. This activity is named attack movement and afterward obstructed by proper resistance instrument. For exactness the recognition system should bring about low false positive and false negative rate.

In view of the arrangement areas, barrier components are named source based, goal based, organize based and cross breed (disseminated) systems. Source based instruments are conveyed shut to the sources forestalling them making attack traffic proactively.

II. DEFENCE MECHANISM

In the destination based defense location and reaction is normally performed at the casualty site. System based resistances are primarily conveyed in the systems inside the switches of the frameworks. Hybrid protection instruments are disseminated in nature also, are conveyed at different areas, for example, sources, goals and middle of the road systems. The circulated barrier includes participation of different deployment areas.

Contingent upon the point in time when protection happens the components are named before the attack, amid the attack and after the attack. Protecting before the attack is keeping the attack at introductory stages in which attack counteractive action frameworks are sent at sources, goals, middle of the road systems or blend of above spots. Amid the attack barrier includes recognition of progressing attack by the discovery frameworks utilized at different areas when movement blockage comes to a specific predefined threshold level. This attack movement is the dropped by fitting sifting component. Safeguarding after the attack includes attack source recognizable proof and trace back in which once the attack source is distinguished all the activity from that source is blocked.

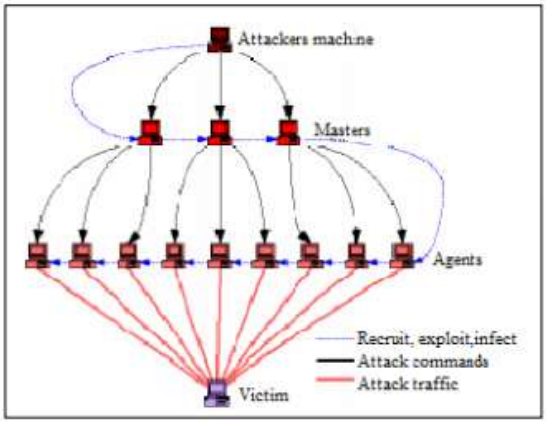

Fig. 1: DDoS attack model.

III. TYPES OF DDOS ATTACKS

A. Denial of sleep attack

Denial of sleep attack goes for nodes power utilization. In this sort of attack the enemies know about the MAC layer protocol and it have a capacity to bypass confirmation and encryption protocols. MAC layer protocol is particularly intended for remote sensor nodes to save battery energy of the hub by setting radio in low power modes. At the point when the hub isn't dynamic MAC protocol can conquer radios essential wellsprings of vitality misfortune, for example, impact and control packet overhead.

 ISSN: 2454-4248
583 – 588

B. *UDP flood attack*

User Datagram Protocol (UDP) is a misleading protocol since data packets or demand may touch base out of request, may appear of being copy or might be postponed. So the UDP enables the data and demand to be sent to a server without requiring a reaction or affirmation that the demand was gotten. UDP protocols produce a bigger data transmission DDoS attack since they are connectionless and is anything but difficult to create as it doesn't require any authorization to transfer packets. This comprise of messages bigger than the ordinary size sent by the pernicious hub to target, devouring system data transmission.

C. *ICMP (Ping) flood*

Internet Control Message Protocol (ICMP) is like UDP. ICMP Ping ask for persistently sends packets as quick as conceivable without expecting any answers. So both approaching and the active data transmission will be expanded prompting attack on the line size of the ports

D. *SYN flood*

Here the attacker tries to send packets consistently to the server so as to keep the association being closed. During the association time frame different frameworks won't have the capacity to get to the server this is one kind of DDoS attack. In a spoofed SYN flood the attacker tries to send an enormous measure of TCP SYN packets with a false IP address.

E. *Ping Of Death (POD)*

POD is an extremely old attack which isn't a danger to the framework any longer. The IP protocol comprise of most extreme recompenses for packets sent between two machines. The most extreme stipend under IPv4 is 65,535 bytes. At the point when a bigger sum is sent surpassing the number

Then it will make the getting server crash as it searches for the parcel information bigger than the most extreme buffer size.

IV. Literature Survey

In this segment, we survey the existing literature on Distributed Denial of Service attacks.

S. Yu, et al. [1], proposed a dynamic resource allocation method for securing singular clients of cloud amid DDoS attack guaranteeing quality of service during attack. The cloud condition is fit for controlling the resource allotment since it has vast number of resources to dispense to individual client. The resource allocation system utilized as a part of mists assumes key part in relieving the effect of attack by offering access to resources. In cloud condition the accomplishment of attack or defends relies on who is holding more resources, attacker or cloud client. The dynamic additional resource allocation counteracts starvation, along these lines protecting against DDoS attack. They additionally exhibited line based model of resource portion under different attack situations.

V. A. Foroushani, et al. [2], proposed protection against DDoS attacks containing attack packets with spoofed IP addresses called Trace back based safe defense against DDoS loading attacks. The component is executed shut to attack source, rate-constraining measure of movement sent towards casualty. The execution assessment of the system utilizing true CAIDA DDoS attack datasets showed increment in throughput of real activity forcing less overhead on participating routers.

B. Liu, et al. [3], proposed shared departure filtering for giving insurance against IP spoofing based flooding attacks. They have utilized genuine web dataset for acquiring reenactment comes about. The instrument utilizes the entrance control rundown of autonomous (AS) that contains rundown of tenets for applying entrance/departure separating and unicast reserve path forwarding. This strategy ensures the frameworks which send the component while keeping non-deployers from openly utilizing it.

In [4], A. Compagno, et al. introduced barrier against interest flooding conveyed dissent of administration attacks in Named Data organizing. Interest flooding requires restricted resources to dispatch attack. Pending interest table is kept up at switches for maintaining a strategic distance from copy interests. Poseidon structure is presented for identification and relief of interest flooding attacks. The assessment of the system over system reenactment condition utilizing NS3 demonstrated that it is conceivable to use up to 80% accessible data transfer capacity amid attack utilizing this framework.

C. Chung, et al. [5], proposed distributed intrusion recognition and countermeasure choice component in cloud frameworks. The NICE framework utilizes interruption recognition conspire at each cloud server for distinguishing and dissecting approaching traffic. The strategy works for virtual cloud framework and makes situation attack diagram for ascertaining helplessness to communitarian attacks. The defenseless frameworks are the exchanged to review state where profound bundle assessment is utilized to stamp potential attack practices.

In [6], S. Rastegari, et al. displayed a quantitative structure for understanding DDoS attack systems and gave defense answers for these attacks. The collaboration amongst aggressor and safe defense is exhibited utilizing Red group Blue group practice where Red group speaks to adversaries and Blue group recognizes conceivable vulnerabilities endeavoring to shield them. The framework was tried utilizing OMNeT++ arrange test system. The reproduction comes about show that one defense technique isn't generally an ideal arrangement; rather it ought to powerfully adjust and enhance as indicated by changing attack strategies.

In [7], L. Jingna has portrayed different Denial of Service attack standards, strategies for recognizing the DoS and DDoS attacks, and safe defense instruments against DDoS attacks. Different attack propelling techniques, for example, SYN Flood, IP mocking DoS attack, UDP flood attack, the PING flood attack, Teardrop attack, Land attack, Smurf attack, Fraggle attacks, and so on are clarified. Discovery techniques

 ISSN: 2454-4248
583 – 588

for above attacks are recorded with their organization area. Certain methodologies are recommended for improving barrier techniques.

S. Yu, et al. [8], proposed a strategy for recognizing flash crowds from DDoS attacks in view of stream connection coefficient. The attackers utilize the movement design fundamentally the same as blaze swarm which cripples the recognition of attack. This poses a test for the individuals who endeavor to safe defense the DDoS attacks. By distinguishing genuine DDoS attack utilizing this technique applies fitting resistance component to protect against DDoS attacks. They made overlay organize on switches that was under their control. The approaching stream was observed and number of packets in each stream was recorded. This recorded data helps in isolating glimmer swarm from real movement. They assessed the created component utilizing 1998 FIFA World CUP genuine informational indexes of blaze group and genuine attack tools, Mstream.

B. S. K. Devi, et al. [9] proposed Interface Based Rate Limiting (IBRL) algorithm for moderating recognized DDoS attacks in the system. It ensures that enough data transmission is accessible for honest to goodness activity amid attack. System checking framework sent in exploratory testbed gather the movement follows in organizes. This movement is investigated for measuring its effect amid attack utilizing host and system based measurements, for example, packet loss, latency, connect use and throughput took after by rate-restricting on the attack movement in order to permit genuine clients. Trial comes about show increment in throughput of honest to goodness traffic.

In [10], A. Mishra, et al. nearly portrayed different defense systems, diverse attacking instruments and preferences impediments of these strategies. The procedures for interruption location and moderation are grouped on the premise of blame resistance and nature of administrations gave.

In [11], Z. Chao-yang, et al. given a definite investigation of existing refusal of administration attack counteractive action standards. Four sorts of barrier procedures are clarified. In the first place strategy is protecting utilizing switch utilizing reverse way sending. Second strategy includes utilizing TCP catch for TCP obstructing for constraining SYN attack. Third technique is creating trusted stage in which a chain of trust and validation is shaped in view of confided in root. Fourth strategy utilizes confirmation framework for giving validation.

In [12], J. Mirkovic, et al. displayed examination between resistance instruments that channel parodied attack movement in light of some execution measurements. The accessible resistances are either conveyed at end organize or require joint effort of center switch for sifting or parcel checking. Every resistance is assessed in its controlled condition; henceforth, they played out a near examination to discover the execution of every component as a rule organize setting with no topology changes.

In [13], X. Bi, et al. proposed an idea to fabricate and ensure security declaration framework for avoiding DDoS attacks. This strategy depends on a Service Oriented Architecture (SOA). Servers and different supplies shape overlay arrange concealing the genuine area of server. The overlay network has two arrangement of nodes, steering nodes that allots distinctive transfer speed to various streams and serving nodes. Customer needs to first get to direct declaration toward access the server, however it requires parcel of CPU time. As cost of propelling effective attack is high it is valuable in anticipating attacks.

M. S. Fallah [14], proposed amusement theoretic approach for controlling customer baffle based resource utilization. Four protection strategies were created, two for single source attack and two for appropriated attacks. In customer bewilder based technique for safe defending the flooding attacks, asked for resources of the server are dispensed if the customer gives amend answer for the baffle sent by server. Confuse explaining expends the resources of assailant; henceforth, the aggressor is debilitated from making attack more than once. The amusement hypothesis approach keeps up ideal level of riddles in order to serve effectively to honest to goodness customers.

B. Krishna Kumar, et al. [15] proposed a bounce tally based parcel handling approach for recognizing aggressors utilizing mock source IP address. In this technique the bundles from the frameworks at a similar jump tally going through a similar switch are set apart with a similar recognizable proof number which is the mix of 32 bits IP address of the switch way and the scrambled estimation of the bounce check. This esteem is coordinated with as of now put away an incentive at getting switch. In this way, attack packets are recognized early and caricaturing dangers are diminished.

J. Atoum, et al. [16], introduced two methodologies of defense systems for upgrading the productivity of resistance against DDoS. The principal procedure called Distributed discovery/parcel Reflector utilizes bundle reflecting system and the second Graveyard methodology drops malignant packets in the wake of playing out a few levels of testing on them. This strategy joins information mining, learning sharing and is sent at numerous areas in the system.

Z. Xiao-hui, et al. [17] displayed safe defense calculation against TCP SYN flood attack. SYN flood attack is identified when number of half-open associations surpasses 95% of the line limit. In view of this condition arrange is checked for the nearness of attack indications. In the event that attack is identified then the SYN bundles living for over one moment are deserted. The trial was performed in genuine system condition utilizing Tribe Flood Network attack programming. CPU and memory usage were utilized for execution assessment amid attack by applying created system.

G. Jin, et al. [18] proposed a parcel checking plan called hash based way distinguishing proof for shielding against DDoS attack with mocking of IP addresses. 16-bit IP Identification field in every parcel is utilized to produce special identifier relating to a way through which bundle

 ISSN: 2454-4248
583 – 588

navigates. Hashing of last 16 bits is performed by switches along the way empowering the casualty to separate amongst honest to goodness and attack bundles. HPi2HC channel is exhibited giving sifting abilities to casualty to drop vindictive packets.

In [19], J. Mirkovic, et al. proposed a few Denial-of-Service affect measurements for measuring nature of-benefit experienced by clients amid an attack. They assessed the measurements by testing in Emulab testbed and NS2 recreations. They built up the metrics percentage of failed transaction (pft) per application, DoS-hist that gives histogram of pft to every application, DoS-level which is normal estimation of pft level for all exchanges, QoS, QoS-debase, life graph which demonstrates life of exchange in an application and disappointment proportion that shows number of exchange that are as of now dynamic however will flop in future. They quantified the adequacy of DoS barrier utilizing these measurements against TCP SYN flood attack, UDP flood attack at high and low rate.

R. Kumar et al. [20] introduced a goal based alleviation technique. A table of dynamic clients with their opportunity out esteem is kept up. Time-out esteem is reset when parcel land from dynamic client. On the off chance that parcel is from new client at that point if transfer speed is accessible it is held generally dropped. The table of dynamic clients is checked for including new client. On the off chance that the table is full new client is added to hold up line and included when dynamic client is timeout. Number of clients permitted relies upon table length.

Y. Xie, et al. [21], proposed DDoS attack location and separating against application based attacks. For portraying perusing conduct of web clients and location of electronic attacks a model is presented in light of concealed semi-Markov demonstrate. They utilized the re-estimation calculation for portraying a model that characterizes ordinary conduct of web clients. The deviation from this ordinary access of site pages is considered as variation from the norm. In light of this conduct display, they built up a recognition and channel technique.

X. Wang [22] exhibited a general alleviation strategy through pushback and resource direction. Enhance total based clog control (IACC) calculation is utilized for actualizing pushback and resource direction is connected at casualty. On the off chance that an approaching bundle matches attack signature it is passed to rate limiter which chooses whether to drop or forward it in light of clog level. Generally bundle is sent to molecule swarm advancement corresponding indispensable differential calculation that chooses whether to drop it or add to FIFO yield line. Results indicated viability against attacks expending intemperate transmission capacity and resources.

P. Jayashree, et al. [23] exhibited protection system in light of Packet Score plot actualized at switches. Defective pail is utilized for activity checking and blockage control. Parcel score is figured utilizing bundle traits and bundles having score over certain limit are sifted through. Permitted packets are then gone through second channel where bundle payload is utilized to coordinate with information mark of beforehand distinguished attack bundles. Twofold sifting diminished false positive proportion.

M. Muthuprasanna, et al. [24] proposed circulated separate and overcome approach for tending to three issues, viz. attack tree development, attack way recurrence location, and bundle to way relationship, in any protection instrument. Singular issue is taken care of through repeat connection. Genuine web topologies were utilized for execution assessment. Results demonstrated that this technique permits single bundle trace back for vast number of casualties, with less false positive and negative rate.

S. Malliga, et al. [25] introduced deterministic parcel checking plan called modulo method for interface denoting that permits single bundle trace back. ID field of IP parcel is utilized for bundle stamping. Switch denotes the parcel utilizing its interface number as opposed to IP address related with it in this way lessening time and substance required for checking. Execution is assessed utilizing parameters, for example, joining time, stockpiling and correspondence overhead.

C. Chae, et al. [26] proposed IP trace back strategy which contains operator framework that report any irregular movement marvel, make IP Trace message and send it to server framework. Goal framework identifies attack by investigating IP Trace message and gather significant data which is utilized for IP trace back. The strategy is adaptable and requires no basic changes to existing system.

R. Kompella et al. [27], proposed an adaptable recognition system. In the majority of interruption recognition and avoidance frameworks location depends on per-stream investigation. Such recognition plans don't perform well in rapid systems. The location plans for rapid systems utilize the conglomeration strategy that characterizes a bundle in view of total movement gathered. The collection can at times dishonestly order honest to goodness movement as attack activity and vice versa.

V. PROPOSED METHODOLOGY

In this section the proposed system architecture with detailed explanation are discussed. Fig. 2. Shows the proposed system architecture.

 ISSN: 2454-4248
583 – 588

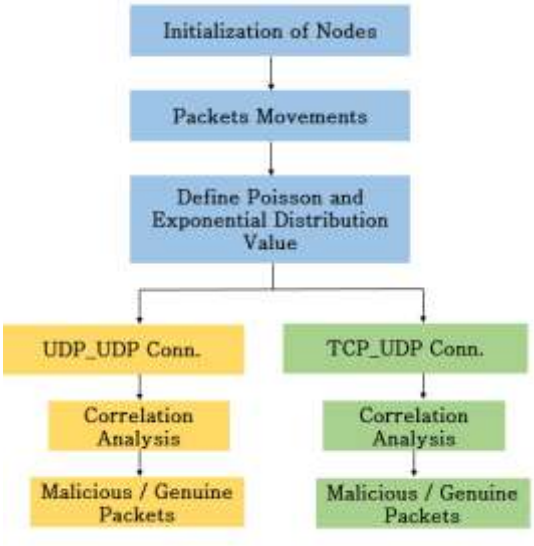

Fig. 2. Proposed system work flow

Firstly the nodes and packets are created. These packets are sent to different server via client or hacker in sence of flooding.

The Poisson distribution is used to control and manage the arrival rate of the packets over networks. The exponential distribution are used to define the service time of the packets in the network.

When packets arrived at server end, the server checks the packet constantly for any viruses or malicious packets. It calculates the malicious packets via correlation analysis shown in fig. 2.

VI. Expected Outcome

We will perform our experiments using the NS2 simulator. The simulator is responsible for creating and sending of packets to nodes. The packets sends via two protocol.

1. UDP
2. TCP

Using these two protocols the UDP and TCP, the packets are delivered to the client or server.

Finally we will compare the throughput of the system by applying correlation analysis.

VII. Conclusion

In this paper, we have exhibited a review of DDoS discovery and resistance plans grew up until now. By and by, outlining and executing DDoS guard systems for continuous systems is very lumbering. It isn't conceivable to totally stop the attack; consequently DDoS tolerant systems must be created and actualized to enhance nature of administration gave to authentic customers during attack. Collaboration of a few barrier mechanisms can be utilized to overcome huge scale attacks.

The above literature review papers has used some packet-level defense methods. Filtering all incoming response packets, which is of low cost, will result in no general access to the remote server. Inspecting packet content and tracking protocol status maybe helpful, but need a lot of computation which is also vulnerable to attacks. Along with more protocols being exploited to launch DRDoS, countermeasures must consider a list of possible protocols with each one treated specifically, and the list needs to be updated in time. So we urgently expect some protocol independent methods to help detecting most kinds of DRDoS. These problems can be solved usig packet correlation and ranking method.

References

[1] S. Yu, Y. Tian, S. Guo, D. Wu, "Can We Beat DDoS Attacks in Clouds?", *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 9, pp. 2245-2254, Sept. 2014.

[2] V. A. Foroushani, A. N. Zincir-Heywood, "TDFA: Trace back based Defense against DDoS Flooding Attacks", *IEEE 28th International Conference on Advanced Information Networking and Applications*, pp. 597-604, May 2014.

[3] B. Liu, J. Bi, A. V. Vasilakos, "Toward Incentivizing Anti Spoofing Deployment", *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 3, pp. 436-450, March 2014.

[4] A. Compagno, M. Conti, P. Gasti, G. Tsudik, "Poseidon: Mitigating Interest Flooding DDoS Attacks in Named Data Networking", *IEEE 38th Conference on Local Computer Networks*, pp. 630-638, Oct. 2013.

[5] C. Chung, P. Khatkar, T. Xing, J. Lee, D. Huang, "NICE: Network Intrusion Detection and Countermeasure Selection in Virtual Network Systems", *IEEE Transactions on Dependable and Secure Computing*, vol. 10, no. 4, pp. 198-211, July/Aug. 2013.

[6] S. Rastegari, P. Hingston, C. Lam, M. Brand, "Testing A Distributed Denial of Service Defense Mechanism Using Red Teaming", *IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA)*, pp. 23-29, April 2013.

[7] L. Jingna, "An Analysis on DOS Attack and Defense Technology", *IEEE 7th International Conference on Computer Science & Education (ICCSE)*, pp. 1102-1105, July 2012.

[8] S. Yu, W. Zhou, W. Jia, S. Guo, Y. Xiang, F. Tang, "Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient", *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 6, pp. 1073-1080, June 2012.

[9] B. S. K. Devi, G. Preetha, S. M. Shalinie, "DDoS Detection using Host-Network based Metrics and Mitigation in Experimental Testbed", *IEEE International Conference on Recent Trends In Information Technology (ICRTIT)*, pp. 423-427, April 2012.

[10] A. Mishra, B. B. Gupta, R. C. Joshi, "A Comparative study of Distributed Denial of Service Attacks, Intrusion Tolerance and mitigation Techniques", *European Intelligence and Security Informatics Conference (EISIC)*, pp. 286-289, Sept. 2011.

[11] Z. Chao-yang, "DOS attack analysis and study of new measures to prevent", *IEEE International Conference on Intelligence Science and Information Engineering*, pp. 426-429, Aug. 2011.

 ISSN: 2454-4248
583 – 588

[12] J. Mirkovic, E. Kissel, "Comparative Evaluation of Spoofing Defenses", *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 2, pp. 218-232, March-April 2011.

[13] X. Bi, Q. Zheng, "Study on Network Safety Strategy against DDoS Attack", *IEEE International Conference on Advanced Management Science (ICAMS)*, pp. 623-627, July 2010.

[14] M. S. Fallah, "A Puzzle-Based Defense Strategy Against Flooding Attacks Using Game Theory", *IEEE Transactions on Dependable and Secure Computing*, vol. 7, no. 1, pp. 5-19, Jan.-March 2010.

[15] B. Krishna Kumar, P. K. Kumar, R. Sukanesh, "Hop Count Based Packet Processing Approach to Counter DDoS Attacks", *IEEE International Conference on Recent Trends in Information, Telecommunication and Computing*, pp. 271-273, March 2010.

[16] J. Atoum, O. Faisal, "Distributed Black Box and Graveyards Defense Strategies against Distributed Denial of Services", *2nd International Conference on Computer Engineering and Applications*, pp. 87-91, March 2010.

[17] Z. Xiao-hui, P. Xuan-ge, L. Man-hua, X. Hong-qi, J. Shi-yao, "Research on An Effective Approach against DDoS Attacks", *IEEE International Conference on Research Challenges in Computer Science*, pp. 21-23, Dec. 2009.

[18] G. Jin, F. Zhang, Y. Li, H. Zhang, J. Qian, "A Hash-based Path Identification Scheme for DDoS Attacks Defense", *IEEE 9th International Conference on Computer and Information Technology*, pp. 219-224, Oct. 2009.

[19] J. Mirkovic, A. Hussain, S. Fahmy, P. Reiher, R. K. Thomas, "Accurately Measuring Denial of Service in Simulation and Testbed Experiments", *IEEE Transactions on Dependable and Secure Computing*, vol. 6, no. 2, pp. 81-95, April-June 2009.

[20] R. Kumar, R. Karanam, R. C. Bobba, Raghunath S., "DDoS Defense Mechanism", *IEEE International Conference on Future Networks*, pp.254-257, March 2009.

[21] Y. Xie, Shun-Zheng Yu, "A Large-Scale Hidden Semi-Markov Model for Anomaly Detection on User Browsing Behaviours", *IEEE/ACM Transactions on Networking*, vol. 17, no. 1, pp. 54-65, Feb. 2009.

[22] X. Wang, "Mitigation of DDoS Attacks through Pushback and Resource Regulation", *IEEE International Conference on Multimedia and Information Technology*, pp. 225-228, Dec. 2008.

[23] P. Jayashree, K. S. Easwarakumar, Anandharaman V., Aswin K., Raja Vijay S, "A Proactive Statistical Defense Solution for DDOS Attacks in Active Networks", *IEEE 1st International Conference on Emerging Trends in Engineering and Technology*, pp. 878- 881, July 2008.

[24] M. Muthuprasanna, G. Manimaran, "Distributed divide-and conquer techniques for effective DDoS attack defenses", *IEEE 28th International Conference on Distributed Computing Systems*, pp. 93-102, June 2008.

[25] S. Malliga, A. Tamilarasi, "A defensive mechanism to defend against DoS/DDoS attacks by IP trace back with DPM", *IEEE International Conference on Computational Intelligence and Multimedia Applications*, pp. 115-119, Dec. 2007.

[26] C. Chae, S-H. Lee, J-S. Lee, J-K. Lee, "A Study of Defense DDoS Attacks using IP Trace back", *IEEE International Conference on Intelligent Pervasive Computing*, pp. 402-408, Oct. 2007.