ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 8, August 2013

Analytical approach for Mitigation and Prevention of DDoS Attack using Binomial theorem with Bloom filter an Overlay Network Traffic

V.ShyamalaDevi[1], Dr. R. Umarani [2]

Associate Professor, Department of MCA, KSRCT, Tiruchengode, Tamilnadu[1]

Professor, Department of MCA, Saradha Womens College, Salem, Tamilnadu[2]

Abstract: A distributed denial of service attack (DDoS) occurs when multiple systems flood the bandwidth or resources of a targeted system. These systems are compromised by attackers using various methods. IP address spoofing occurs when an attacker assumes the source Internet Protocol (IP) address of IP packets to make it appear as though the packet originated from a valid IP address. Most IP networks utilize the user's IP address to verify identities and routers also typically ignore source IP addresses when routing packets. Routers use the destination IP addresses to forward packets to the intended destination network. It could enable an attacker to bypass a router and to launch a number of subsequent attacks. Mitigation Threat Management System (MTMS) is a vital component of sophisticated and adaptive DDoS countermeasures which surgically mitigate and remove attack traffic while enabling the flow of legitimate traffic. It offers a mechanism for attack mitigates and detection the attack traffic route using Binomial distribution with Bloom filters. It protects both IPv4 and IPv6 infrastructure from DDoS attacks. This threat management functionality can be improving profitability by providing the foundation for new, revenue-generating, managed DDoS protection services.

Keywords: DDoS, Mitigation Threat Management System, IP spoofing, Binomial Distribution, Bloom filter

I. INTRODUCTION

Denial of Service (DoS) attack is aimed at preventing authorized, legitimate users from accessing services on the network. Automated or user-initiated network-aware attacks which targets files and data often causing loss of machine control, productivity and time. Malicious system misuse which targets shared resources and protected data. Symptoms of denial-of-service attacks include unusually slow network performance (opening files or accessing web sites), unavailability of a particular web site and inability to access any web site. Such attacks can be perpetrated in a number of ways. The five basic types of attack are the Consumption of computational resources, such as bandwidth, disk space, or processor time, causing resource starvation and preventing any useful work from occurring etc. A Distributed Denial of Service occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. The five major components of a Distributed Denial of Service attack are: (1) Client is an application that can be used to initiate attacks by sending commands to other components, also called the attacker or intruder. (2) Daemon is a process running on an agent, responsible for receiving and carrying out commands issued by a client. (3) Handler is a host running a Client also called master. (4) Agent is a host running a daemon also called zombie. (4) Victim is the target (a host or network) of a distributed attack. Figure 1.1 clearly depicts the phases of attack. The attacker uses a single source machine to scan for vulnerable machines which will be capable of acting as handlers. Once identified and compromised the handlers each will in turn search for large number of vulnerable machines which will be used to carry out the actual attack. These machines are called Agents or Daemons. The handlers are used to trigger the attack on the victim via the agents. In the early Distributed Denial of Service days, the IP addresses of handlers were hard coded in the attack code, and handlers stored the encrypted information about available agents in the

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 8, August 2013

file. Recently this drawback was overcome with the use of the Internet Relay Chat (IRC) channels for communication. The IRC server tracks the addresses of connected agents and handlers and facilitates communication between them. The discovery of the single participant leads to discovery of the communication channel, but other participants' identities are protected.

II. RELATED WORKS

The concept of Probabilistic Packet marking was first proposed by Stefan Savage et al. PPM is a technique for tracing anonymous packet flooding attacks in the Internet back toward their source. It is a general purpose Traceback mechanism which allows a victim to identify the network path(s) traversed by attack traffic without requiring interactive operational support from Internet Service Providers (ISPs). Huang et al [2][4] proposed a DDoS Traceback scheme based on real-time consideration by dividing the tracing process into two steps. In the first step, Probabilistic Packet Marking Based on Autonomous System (ASPPM) is adopted to determine the attack-originating Autonomous System (AS). In the second step, Random Number Packet Marking is used to identify the exact origin of the attacks in the specific AS.

Yaar et al [7][8] proposed a Path Identification Mechanism Pi (Path Identifier) a packet marking approach in which a path fingerprint is embedded in each packet, enabling a victim to identify

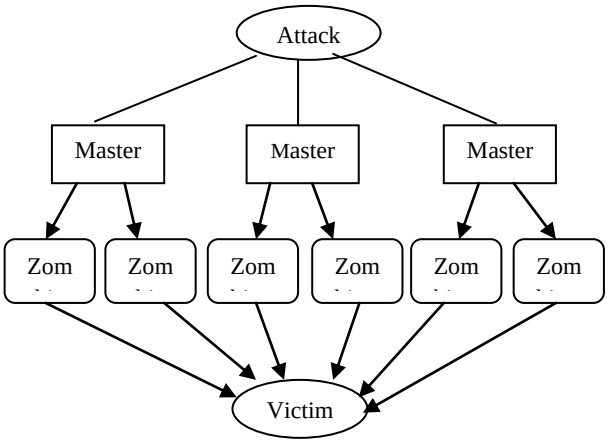


Figure 1.1 Architecture of DDoS Attack

Packets traversing the same paths through the Internet on a per packet basis, regardless of source IP address spoofing.

In this approach an identifier is embedded in each packet, based on the router path that a packet traverses. The victim need only classify a single packet as malicious to be able to filter out all subsequent packets with the same marking. [4] Ren et al proposed a dynamic Possibility based packets marking Traceback scheme, by which packets were marked with different source information such as AS number and IP address. If the passing router is an internal or external transit router, it's AS number will be marked in the identification field. If the router is a stub router the last three segments of the IP address will be marked in the identification and fragment offset field. The first 8 bits in the IP address is ignored in the expectation of the AS number, will be marked by the afterward routers. Marking the information according to the logical location of the routers allows faster and easier path reconstruction.

Lee et al [5] proposed a Fast Two Phrases (FTP) PPM for IP Traceback scheme, which depends on the division of Autonomous System (AS) and two algorithms are used to reconstruct the attacking paths. The scheme can reconstruct the exactly attacking paths between AS when it has received tens of packets, and also reconstruct the attacking paths within AS after receiving more packets. This method can reduce the number of packets that are needed to reconstruct the attacking paths to the lowest, while reducing the complexity of packet marking and reconstructing. Yang et al proposed an AMS Based Reconstruction Algorithm with Two-dimensional Threshold for IP Traceback, a new reconstruction algorithm based on the Advanced Marking Scheme (AMS) which works with a two-dimensional threshold to decide if a node is on the attack path by judging the situation of the edge of the packet and the Hash value match. To reconstruct the attack paths, the victim uses the upstream router map as a road-map and performs a breadth-first search from the root. This consequently reduces the time of reconstruction and overhead and improves the accuracy.

Sung et al [9] proposed a IP Traceback technique that focuses on tracking the location of the attackers and mitigating the effect of an attack while it is raging on

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 8, August 2013

by effectively filtering out the majority of DDoS traffic, thus improving the overall throughput of the legitimate traffic. Whitaker et al proposed that for the experimental setting, each packet keep a Bloom Filter of where it's come from. As it passes through the router, the router can check if it is likely that a loop occurred. It's made very efficient if each router predetermines its hash and just ORs them into the packets.

III. METHODOLOGY AND IMPLEMENTATION

A. Mitigation

Mitigation Threat Management System (MTMS) is a vital component of sophisticated and adaptive DDoS countermeasures which surgically remove attack traffic while enabling the flow of legitimate traffic. MTMS is proven effective in the most demanding networks for detecting and removing high volume flood attacks, stealthy application level attacks and blended attacks. It protects both IPv4 and IPv6 infrastructure from DDoS attacks. Mitigation threat management Solution allows network elements to work together to identify suspicious traffic, confirm whether or not the traffic is malicious and then take action to block that traffic from the network. Service providers now have the ability to cost effectively identify attacks on per user or per application basis and to quickly mitigate these attacks. The solution combines the power of advanced in-line detection and prevention with dynamic service policy creation and configuration.

B. Performance efficiency

MTMS removes DDoS attack traffic, provides visibility into application performance and generates flow for enhanced network wide visibility. Service Visibility: Gain complete visibility into the applications that are traversing critical segments to network. MTMS automatically identifies over 90 IP-based applications and defines custom applications based upon network attributes such as IP address or range, router interfaces and Active Threat Feed fingerprints. Protection: The size and complexity of application-layer attacks continues to rise. MTMS automatically detects and surgically mitigates these threats. Building on the core technology to deliver carrier-class protection for zero-day threats, MTMS stops Denial of Service/DDoS attacks and protect critical revenue-generating service recognizing such anomalies and rate-limiting traffic to keep the service up and running.

C. Attack detection using Binomial Distribution

The basic step to carry out is to identify the source of the attack and to check whether the attack is happening in the network or not. It is identified with the help of information packets and their rate of arrival to destination machine. These packets are classified into two basic categories such as the valid packets from the legitimate user and the attack packets from the source of the attacker as shown figure 3.2.1. The process of identifying the attack packets, carried out with the help of Binomial distribution. When the victim machine feels congestion in traffic, the reason for this may be, over flow of information packets and some other factors. Dilemma over the congestion may be due to more number of packets sent by the hackers. In this situation, a proper rescue mechanism has to take up and deal with the traffic congestion in order to make a smooth flow of packets in the network. The information flow in the network should be monitored frequently in order to achieve high efficiency. For finding out the attack, it has to be identified whether the packet received by the receiver is legitimate or illegitimate packets deliberately sent by hackers. To achieve this,

Mitigation threat management system along with Binomial distribution is applied in order to rescue from the problem.

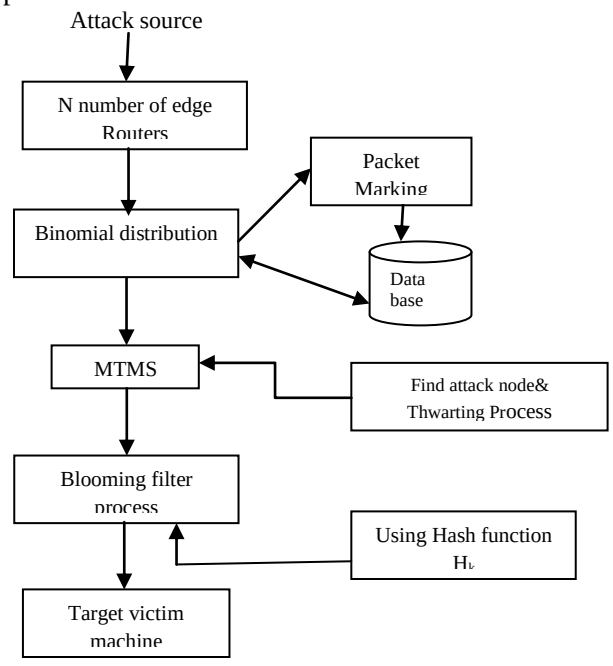


Figure 3.2.1 Process for thwarting a DDoS attack

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 8, August 2013

The binomial distribution is the discrete probability distribution of the number of successes in a sequence of *n* independent experiments, each of which yields success with probability *p*. when *n* = 1, the binomial distribution is a Bernoulli distribution. The binomial distribution is frequently used to model the number of successes in a sample of size *n* drawn with replacement from a population of size *N*. However, for *N* much larger than *n*, the binomial distribution is a good approximation, and widely used.It gives the discrete probability distribution $p_p(n/N)$ of obtaining exactly 'n' successes out of 'N' Bernoulli trials where the result of each Bernoulli trial is true with probability 'P' and false with probability 'q = 1-p'. The binomial distribution is therefore given by

$$p_p(n/N) = \left(\frac{N}{n}\right) p^n q^{N-n} \quad \text{---------- (1)}$$

$$= \frac{N!}{n!(\mathrm{N}-\mathrm{n})} p^n (1-n)^{\mathrm{N-n}} \quad \text{----------(2)}$$

Where $\binom{N}{n}$ is a binomial coefficient. The above plot shows the distribution of n successes out of N = 20 trials with $p = q = 1/2$ also it define the distribution of [n, p]. It describes the possible number of times that a particular event will occur in a sequence of observations. It's specified by the number of observations, n, and the probability of occurrence, which is denoted by p. The BD can be used for the mitigation of DDoS to find the probability of maximum number of samples that are invalid is the probability of the number of samples greater than half of total number of samples taken. It is calculated using binomial distribution which is given by the equation (1) & (2),

$P(x>n/2) = nCx\ p^x\ q^{n-x}$ Where,

p=probability of success (invalid packets)

q= probability of failure (valid packets)

n=total number of samples taken

Algorithm:

```
fact(int x)
{
int temp;
while((x-1)!=0)
{
temp=x*x-1;
x--;
}
return temp;
}
for(i=n/2+1;n/2<=n;i++)
t= fact(n) / fact(n-i)* fact(i) *p^i *q^(n-i);
}
```

D. Process in Bloom filter

Find a malicious packet in the server log to find out where it came from. The figure 3.3.1 represents the functions for bloom filter, hence a bit array of size **q**, initializing all bits to 0. Create **k** different hash functions h1, h2… hk. Hash to values between **0** and **q-1.** Assume negligible storage requirements for the hash functions. When we want to add an element, hash it **k** times and set the corresponding bits to 1. DDoS attack Bit Vector Source address

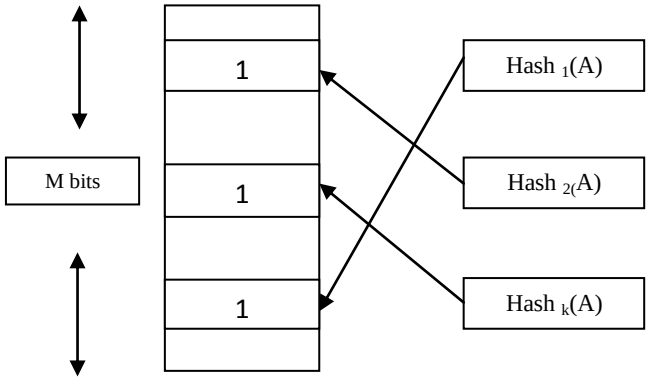


Fig 3.3.1 Bloom Filter

with K function

```
add<T>(T item)
{
for(int i = 0; i < k; i++)
array[hi(item)] = 1;
}
```

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 8, August 2013

When we want to check for containment, hash k times and see if all k bits are set to 1 contains<T>
(T item)
{
for(int i = 0; i < k; i++)
if(!array[hi(item)]) return false;
return true;
}

IV. SIMULATION ENVIRONMENT

A. Experimental Procedure

The experimentation is conducted with two networks containing maximum number of nodes interconnected with one another. This experimentation comprises of two networks. The deployment of the admission control scheme of the DDoS mechanism based on bandwidth threshold the admission of unnecessary packets will be controlled to improve the resistance of DDoS attack generated by the source attacker. Bandwidth threshold is applied on the Scrupulous packet examination is shown in Fig 4.1.1 This made the control scheme of the bandwidth mode to drop some unwanted packets. The dropped packet size is 1000 bytes and the dropped time is 2.695. Packets with different sizes varying from 400 to 1600 bytes with the interval gap of 400 are simulated for the admission control scheme of the DDoS resistance. Figure 4.1.2 the systematic flow of the simulation is set in a way that packets with greater than limited sizes are dropped and bandwidth with greater than 20MB is send to destination port.

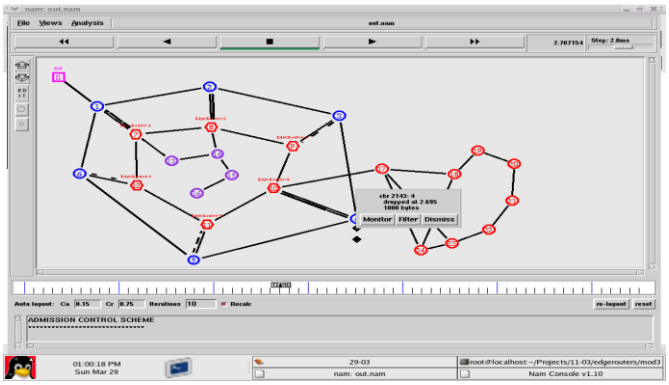


Fig 4.1.1 Bandwidth threshold on scrupulous packet examination

B. Results and Discussions

The graph 1 shows the result of the DDoS resistive mechanism function with number of nodes Vs Bandwidth. As the number of nodes in the network of the source or intermediate junction increases, consumption of bandwidth decreases. When compared to existing method (without bandwidth threshold), the bandwidth is high in the proposed method. Graph 2 depicts the output of the simulation by varying the nodes there is an appreciable change in the throughput of the data communication. As the number of nodes increases, throughput decreases. By comparing it with non bandwidth threshold model, the throughput is high in the admission control bandwidth threshold model.

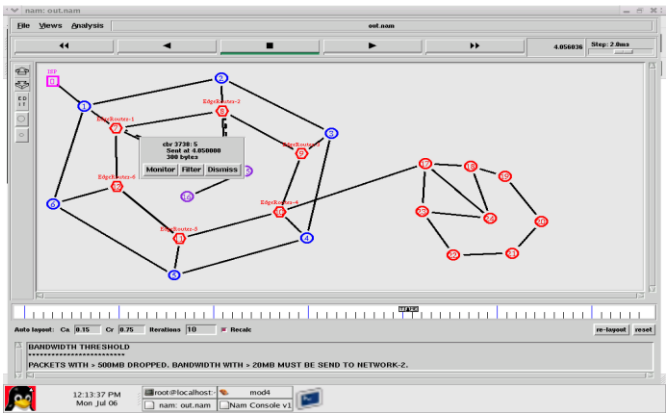
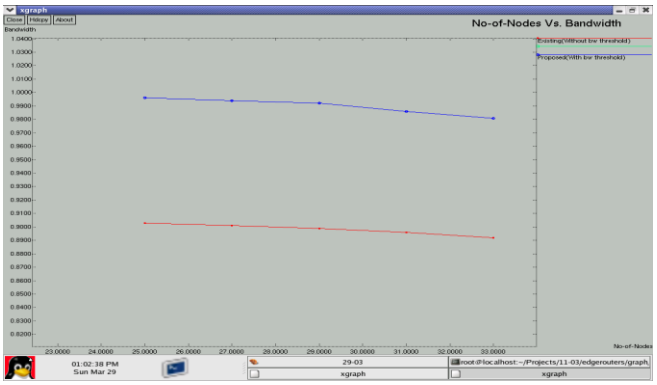


Fig 4.1.2 Packet restriction of sizes more than 500MB

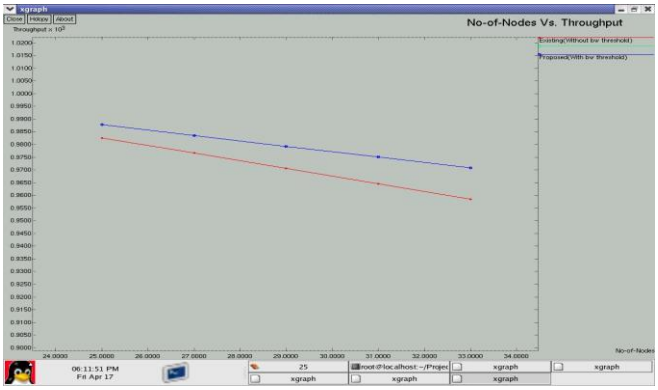


Graph 1 Number of nodes Vs Bandwidth

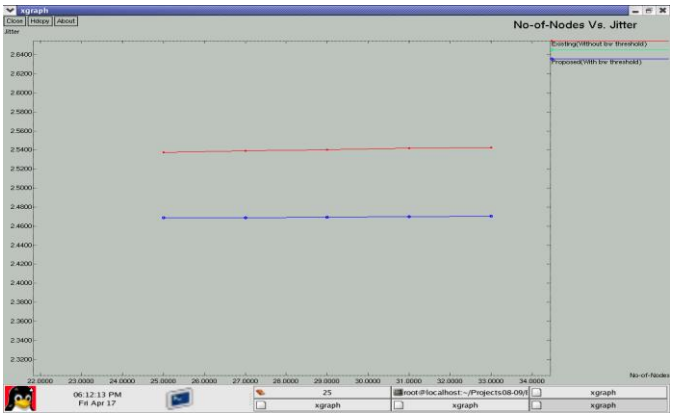
The simulation result based on the node variation affecting the jitter is depicted in the graph3. The jitter value increases as the number of nodes increased in the network communication path of edge and link routers. As for comparison made on existing method (without bandwidth threshold), the jitter is low in the proposed method.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 8, August 2013



Graph 2 Throughput Vs Number of Nodes



Graph 3 Nodes Vs Jitter

V. CONCLUSION

DDoS attacks are posing a vital threat to the emerging global environment, become it's focused to provide an effective mitigate mechanism for these attacks. Many existing solutions need to track and maintain per-flow state information; hence the aggregate flows by using one or more hash functions (Bloom filters) to avoid maintaining per-flow information and thus are not scalable at high-speed networks. In this paper we proposed an analytical approach to address the DDoS attacks problem and simulation results shows that our proposed algorithm saves on potential computation time while provide an impressive detection rate. A mathematical model is designed to estimate the packet delivery ratio in the network which is estimated using the probability of binomial distribution. NS-2 simulation results shows proposed algorithm, that it not only effectively decreases the flow of malicious packets from DDoS attacks, but also provides smooth and constant flows sent by normal users and increase the throughput of the normal packets.

REFERENCES

[1] Andersen D. (2003) 'Distributed filtering for internet services', In USITS, Seattle, WA.
[2] Huang, Changlai, Li, Ming et al. *"*A Real-Time Traceback Scheme For DDoS Attacks*"*. WCNM 2005 International Conference on Wireless *Communications, Networking and Mobile Computing, pg.* **...** October *16*, 2006
[3] Argyraki K. and Cheriton D.R. (2005), 'Active internet traffic filtering: Real-time response to denial-of-service attacks', In USENIX Annual Technical Conference, pp. 135-148.
[4] Collins M. and Reiter M.K. Ren.G (2004), 'An Empirical Analysis of Target Resident DoS Filters (Extended Abstract)', In Proceedings of the 2004 IEEE Symposium on Security and Privacy, pp. 103-114.
[5] Ioannidis J. and Bellovin M. (2002), 'Implementing Pushback: Router- Based Defense against DDoS Attacks', In Proceedings of the Symposium on Network and Distributed Systems Security (NDSS 2002), San Diego, CA, pp. 312-321.
[6] Lee H. and Park K. (2001), 'On the Effectiveness of Probabilistic Packet Marking for IP Traceback under Denial of Service Attack', In Proceedings of the IEEE Info comm 2001.
[7] Park K. and Lee H. (2001), 'On the Effectiveness of Route-Based Packet Filtering for Distributed DoS Attack Prevention in Power-Law Internets', In ACM SIGCOMM'01, pp. 15-26.
[8] Yaar A., Perrig A. and Song D. (2003), 'Pi: A path identification mechanism to defend against DDoS attacks', In Proceedings of IEEE Symposium on Security and Privacy, pp. 93-109.
[9] Sung, Jun (Jim) Xu, Li (Erran) Li , Jun Li, Minho IEEE Trans. on Parallel and Distributed Systems ,Large-Scale IP Traceback in High-Speed Internet: Practical Techniques and Theoretical Foundation., 2004.
[10] Yang, Pei Changxing, Yan Li. AMS Based Reconstruction Algorithm with Two-dimensional Threshold for IP Traceback .Sixth International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT 2005), 5-8 December 2005, Dalian, China. pages 781-783, IEEE Computer Society, 2005.
[11] Simpson, S., Lindsay, A.T., Hutchison, D.: Identifying Legitimate Clients under Distributed Denial-of-Service Attacks. In Network and System Security (NSS). IEEE, 2010.
[12] B.B. Gupta, R.C. Joshi and M. Misra, Distributed Denial of Service prevention techniques, international Journal of Computer and Electrical Engineering, Vol. 2, No. 2, April 2010, 1793-8163.
[13] K. Kumar, R.C. Joshi, K. Singh, An Integrated Approach for Defending against Distributed Denial of Service (DDoS) attacks, in: IRISS, 2006, IIT Madras.