# DDoS Attack Detection and Attacker Identification

Brajesh Kashyap
Department of Computer Science and Engineering
National Institute of Technology
Rourkela- 769008

S.K.Jena
Department of Computer Science and Engineering
National Institute of Technology
Rourkela- 769008

## ABSTRACT
DDoS attack is a form of DoS attack in which attacker uses authorized user IP address to attack on a particular victim. Of the two types of attack it falls in the active category. The main aim of the attacker is to jam the resources in order to deny services to the recipient. The attacker can use several strategies to achieve this goal, one of which is by flooding the network with bogus requests. The attack is distributed because the attacker is using multiple computers to launch the denial of service attack. In this paper we have first identified the types of DoS and DDoS attack. Then we have provided the solution for those attacks on the basis of attacker's identification. Main focus of this paper is to identify the actual attacker, who has performed attack by sitting behind a forged System. For that purpose first we prevent IP forgery by using sender authentication process, then calculate TCP flow rate and from it we identify whether packets are nor- mal packet or malicious packet. We detect attack on receiver proxy server by using entropy and normalize entropy calculation on receiver proxy server. If attack is detected then we drop packets, get their mark value and trace them back to the source. Finally we use the concept of ISP and IANA to identify the actual attacker. NS2 has been used to simulate the proposed methods.

## General Terms
Normal packet: packets that are sand by authentic user, Attack packet: packets that are sand by attacker to perform attack on particular victim.

## Keywords:
Denial of Service (DoS), Distributed Denial of Service (DDoS), Internet Assign Number Authority (IANA), Internet Service Provider (ISP)

## INTRODUCTION
The Internet was initially designed for openness and scalability. The infrastructure is certainly working as envisioned by that yardstick. However, the price of this success has been poor security. On the Internet, anyone can send any packet to anyone without being authenticated, while the receiver has to process any packet that arrives to a provided service. The lack of authentication means that attackers can create a fake identity, and send malicious traffic with impunity. All systems connected to the Inter- net are potential targets for attacks since the openness of the Internet makes them accessible to attack traffic.[3]

## 1.1 Denial of service (DoS) attack:
A Denial of Service (DoS) attack aims to stop the service provided by a target. It can be launched in two forms. The first form is to exploit software vulnerabilities of a target by sending malformed packets and crash the system. The second form is to use massive volumes of useless traffic to occupy all the resources that could service legitimate traffic. While it is possible to protect the first form of attack by patching known vulnerabilities, the second form of attack cannot be so easily prevented. The targets can be attacked simply because they are connected to the public Internet.[3]

A DoS attack is a malicious attempt by a single person or a group of people to disrupt an online service. DoS attacks can be launched against both services, e.g., a web server, and networks, e.g., the network connection to a server.[3]

**Types of DoS attack:**
TCP Syn Flood Attack
UDP flood attack
Ping of death attack
Teardrop attack

## 1.2 Distributed Denial of service (DDoS) attack:
In the distributed form of DoS attacks (called DDoS), the attacker first takes control of a large number of vulnerable hosts on the internet, and then uses them to simultaneously send a huge flood of packets to the victim, exhausting all of its resources. There are a large number of exploitable machines on the internet, which have weak security measures, for attackers to launch DDoS at- tacks, so that such attacks can be executed by an attacker with limited resources against the large, sophisticated sites.[2]

**Types of DDoS attack:**

A) Bandwidth Attacks:

The bandwidth attack can be defined as any activity that aims to disable the services provided by the victim by sending an excessive volume of useless traffic

A.1) IP Spoofed Attack: In this type of attack The attackers in DDoS attacks always modify the source addresses in the attack packets to hide their identity, and making it difficult to distinguish such pack- ets from those sent by legitimate users.[2]

A.2) Distributed Reflector Attacks: In these attacks, the attacker (also referred to as a slave from now on; many slaves carry out an attack on behalf of the real attacker: a human) does not flood the victim directly, but uses innocent servers as reflectors to achieve its goal. A reflector may be any IP host that will return a reply packet when sent a request packet. For example, all web servers, DNS servers and routers can be reflectors since they would reply with SYN ACK or RST packets in response to SYN packets. A slave spoofs the source address of the request packets with the address of the victim and sends them to the reflectors. The reflectors then send reply packets to the victim (apparent source of the request packets).

A.3) Forged Source Attack: In this type of DDoS attack attacker first sent the agent software and gathers command and control server and with the help of command and control server they have gather zombie pc's in the network and perform DDoS attack with the help of that systems. Systems those perform DDoS attack in this type of attack are not actual system these are the system that is controlled by the command and control server and perform attack.

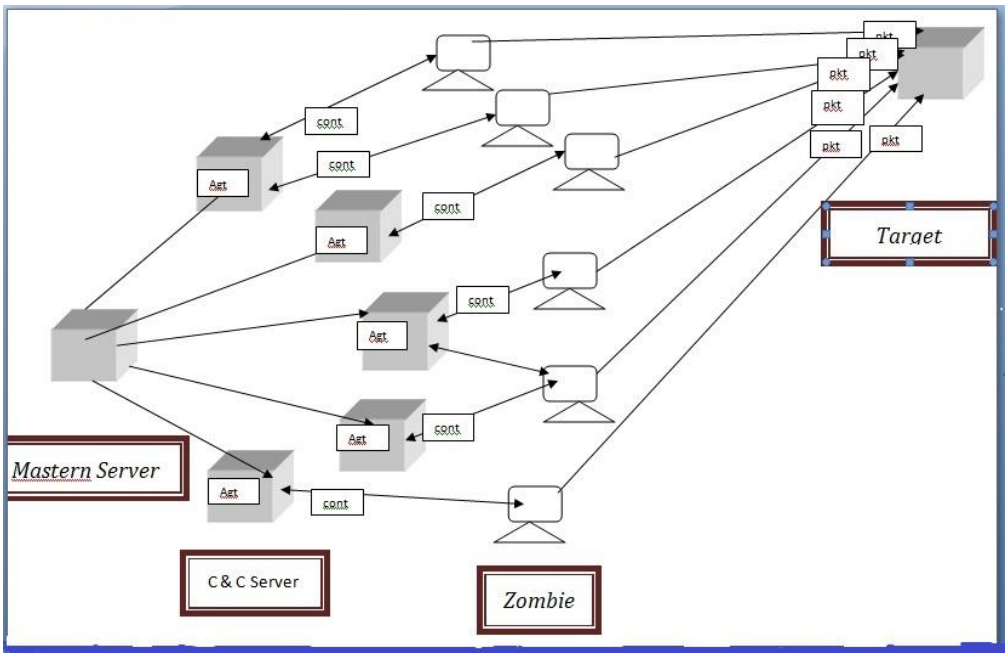


**Fig 1: DDoS Attack Process**

## 2. DDoS ATTACK DETECTION AND PREVENTION:

To detect the DDoS attack on victim proxy server, we use the concept of entropy calculation on victim proxy server. As we know that attacker doesn't play any role in Network path determination it is totally done by the router dynamically. To detect DDoS attack we use the concept of symmetric shared key. We assume that each router is having common shared secret key. Router used that key to encrypt and decrypt marking value with the help of this shared symmetric key. Man in middle attack performed by the attacker by treating himself as a router because it is easy to forge router ip address in a network .This attack can be very well removed by this

### 2.1 Entropy:

Entropy is an important concept of information theory, which is a measure of the uncertainty or randomness. associated with a random variable or in this case data coming over the network. The more random it is, the more entropy it contains. The value of sample entropy lies in range [0, logn]. The entropy value is smaller when the class distribution is pure i.e. belongs to one class. The entropy value is larger when the class distribution is impure i.e. class distribution is more even. Hence comparing the value of entropy of some sample of packet header fields to that of another sample of packet header fields provides a mechanism for detecting changes in the randomness.

The entropy H (X) of a random variable X with possible values x1, x2,...., xn and distribution of probabilities P = $p_1$, $p_2$, . . . , $p_n$ with n elements, where $0 \le p_i \le 1$ and $\sum pi = 1$ can be calculated as.

$$H(X) = -\sum_{i=1}^{n} P(x_i) \log P(x_i)$$

### 2.2 Sender Authentication:

With the help of given approach, we are able to protect IP Spoofed DDoS Attack. For that, we follow the following

**steps:**

**1)**. Sender will send Marking M to the receiver proxy server. Marking value M is a 24 bit Random number generated by the source.

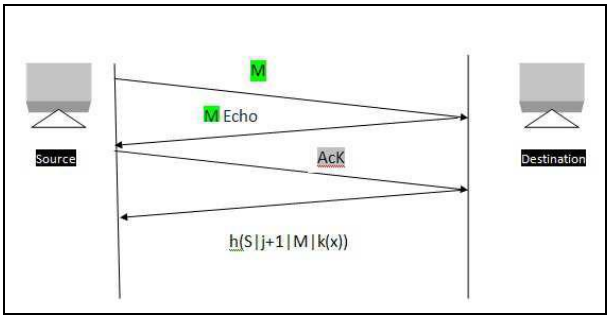


**Fig 2: Sender Authentication Process**

**2).** Receiver Proxy server will receive that Marking value M and send Echo message to verify that marking value.

**3).** If marking value is correct and if it is sanded by a source then they will provide positive acknowledgement else negative acknowledgement.

**4).** If Receiver receive Positive acknowledgement, then they will sent new marking digest to source associated with new higher sequence number (S,j+1,h(S | j+1 | M | k(x))) to sender otherwise discard the request.

**5).** sender will put that 24 bit digest(h(S | j+1 | M | k(x))) value to the option field of the packet and then send packet.

## 2.3 Packet Transmission:

**1).** Suppose any sender wants to send a packet to a receiver firstly they will send packet to edge Router without putting any marking value in an Identification field.

**2).** When edge router receive packet first they examine the packet and then check the identification field.

If packets come without any mark then they will calculate the mark: Mark calculation is done in following way:

Suppose IP is a ip of edge router

Then

h(e)= H(16Sip) ʘ T(16Sip) ʘ H(16Dip) ʘ T(16Dip)

M = E (h(e)|K(x))

Put it to the digest table associated with source IP. Else if already Mark in a packet, then router first decrypt the packet using formula:

P = D (M|K(x))

Then router will calculate h(e) by using the Ip of source where the packet was arrived

h (e)= H(16Sip) ʘ T(16Sip) ʘ H(16Dip) ʘ T(16Dip) Then

Check if (P==h (e))

Calculate h(e)by using their own IP address and their neighbor IP address through which they want to send packet to particular destination.

Repeat above Steps until Final Destination reach.

We are able to solve the problem that when attacker has already filled the mark value and by using above strategy if we decrypt it, we will never get their neighbor IP addresses (those addresses attacker forged and treat himself as a neighbor).

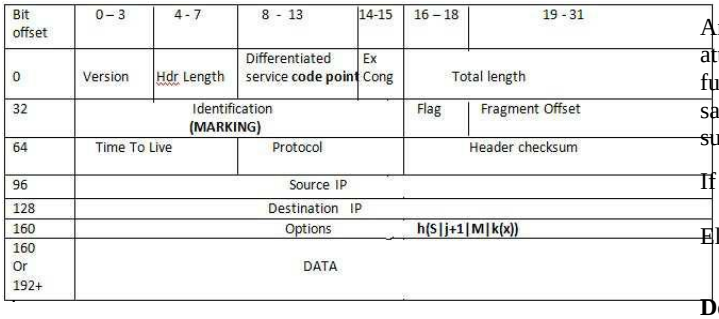


**Fig 3: IP Packet format**

**Table 1: Digest Table**

| S.No. | Source IP | Digest | Timestamp |
|---|---|---|---|
| 1 | X.X.X.X | Dig 1 | 1 min |
| 2 | ---- | Dig 2 | 1 min |
| 3 | ---- | Dig 3 | 1 min |
| 4 | ---- | Dig 4 | 1 min |
| 5 | ---- | Dig 5 | 1 min |
| 6 | ---- | Dig 6 | 1 min |
| 7 | ---- | Dig 7 | 1 min |
| 8 | ---- | Dig 8 | 1 min |
| 9 | ---- | Dig 9 | 1 min |
| 10 | ---- | Dig 10 | 1 min |

## 2.4 DDoS Detection:

Identify the normal packet and attack packet. For the purpose of identification, we calculate TCP flow rate for each packet.

**TCP Flow Rate Calculation**:

We know that normal user send either 3 or 4 packet successively. After that they wait for some time for receiver reply and then start sending packet. But attacker's behavior is different and they won't wait for such amount of time. They send packets continuously without any delay because if they don't do so then are not able to perform attack. If they wanted to perform like normal user then they need to acquire lakh of systems which is very tough for attacker as most of the systems in a network are secure. Systems check agent software registration information and easily know that it is an attack. So on the basis of above assumption, we derive the formula for tcp flow rate:

Suppose $t_p$ is a propagation time and B is Channel Bandwidth. Normal user sent maximum 3 or 4 packet consecutively. After that he waits for $t_p$ time to get the reply from receiver. So

Normal flow rate= $(t_p + t_p)/4 = t_p/2$.

And we know that total capacity of channel is = $B*t_p$. So attacker try to send this much of packet to utilize bandwidth fully. If S1, S2, S3, S4... are successive packets containing same marking value. Calculate time duration (TD) between successive packets

If $((t_p/2) < TD)$

Then packets are normal packets:

Else

Packets are attack packets:

**Detection Procedure**:

**1).** Calculate entropy on receiver proxy server:

$$H(X) = -\sum_{i=1}^{n} P(x_i) \log P(x_i)$$

Where

$P(x_i)$ = (Number of attack or normal packet)/ Total No of packet.

3) Normalized Entropy NE = H/log $n_0$

Where

$n_0$ = no of source node in particular Time Interval

4) If NE < threshold (Δ) identify suspected attack.

## 2.5 Simulation and Results:

The simulation was done using NS-2 simulator to evaluate the performance of our DDoS detection algorithm with results obtained from the experiment. We tested our anomaly detection algorithm in linux (Ubuntu 10) environment. This section introduces the experimental setup and reports performance results.

1) **Experimental setup:** Our simulation includes 3 source, 2 intermediate routers and 1 destination nodes as shown in figure . The bandwidth of legitimate traffic is set constant and the simulation of attack traffic is achieved by randomly generating many pairs of Constant Bit Rate (CBR) UDP flows in NS2. The legitimate user send packets in an interval of 0.20 second and the attacker starts sending attack traffic after 0.0 second frequently. The experiment lasts for 2 seconds. We traced number of packets received in every 0.5 second interval. The traced data is shown below:

2) **Entropy:**

$$H(X) = -\sum_{i=1}^{n} P(x_i) \log P(x_i)$$

Where P (*xi*) = (Number of attack or normal packet)/ Total No of packet.

**Calculation:**

**0 - 0.5:**

$$P(M1) = -\sum_{i=1}^{n} (25/116)\log(25/116) + (91/116)\log(91/116)$$

= 0.225

P(M2) = 0.273

P(M3) = 0.238

NE = (0.225+0.273+0.238)/log3 = 1.54

**0.5 - 1:**

P(M1) = 0.230

P(M2) = 0.192

P(M3) = 0.048

NE = 0.98

**Table 2. Traced Data**

| Time Interval | Normal Packet | | | Attack Packet | | | Normalize Entropy |
|---|---|---|---|---|---|---|---|
| | M1 | M2 | M3 | M1 | M2 | M3 | |
| 0 - 0.5 | 25 | 38 | 32 | 91 | 78 | 101 | 1.54 |
| 0.5 - 1.0 | 38 | 29 | 4 | 131 | 148 | 431 | 0.98 |
| 1.0 – 1.5 | 39 | 31 | 8 | 104 | 126 | 396 | 1.03 |
| 1.5 – 2.0 | 27 | 32 | 29 | 132 | 112 | 142 | 1.32 |

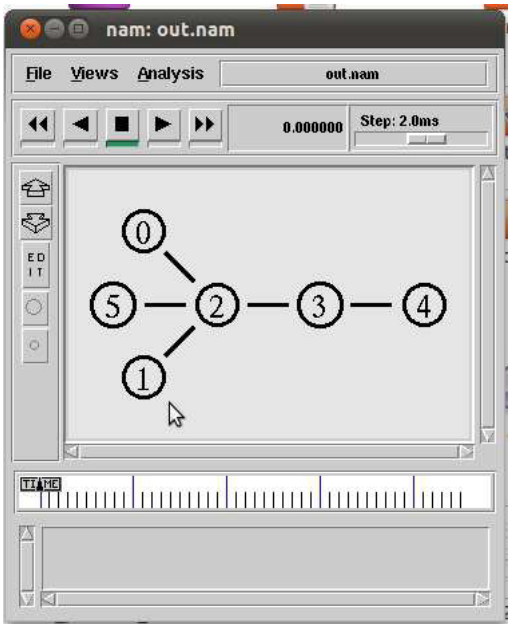


**Fig 4: Screen shot of Setup**

We assume here our threshold value 1.1 because if some packets are reaching destination slowly due to network delay then we are also able to identify attacker.

**Performance Evaluation:**

To evaluate the performance of our algorithm, we plot the evaluation graph which contains time value in X-axis and normalize entropy value in Y-axis. With the help of graph shown below, we are easily able to conclude that if we take threshold value1.1, it can easily detect the attack.

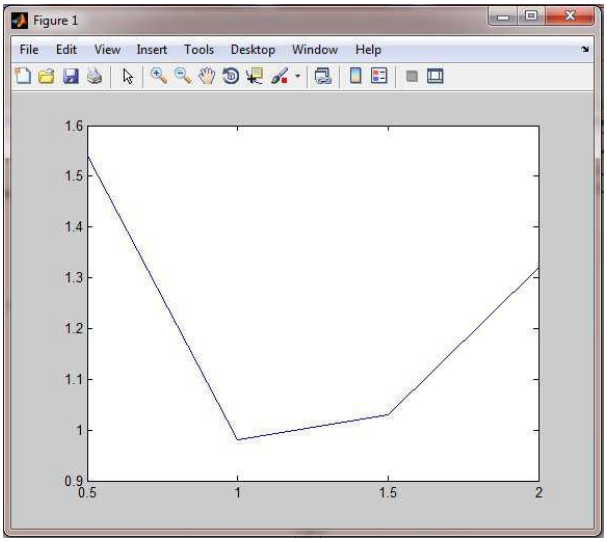


**Fig 5: Effect of DDoS Attack**

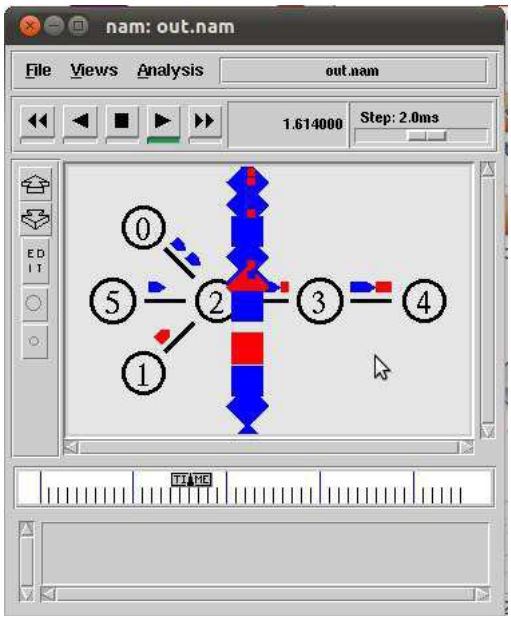


**Fig 6: Screen shot of packet drop**

## 2.5 DDoS prevention:

To prevent DDoS attack if NE value is less then threshold (1.1), then simply drops all packets containing the same path for particular time interval.

# 3. ATTACKER IDENTIFICATION:

## 3.1 Spoofed Attacker Identification

In our approach, there are two ways to identify the attacker.

**A. Router Entropy:**

1) If attack is there in receiver proxy server, it means NE < threshold ( Δ) Then calculate entropy for each downstream router to identify suspected attack flow.

2) Those routers whose NE rate is less than threshold we suspect it as attack router.

3) Further, calculate the NE rate for each Neighbor router of that attack router until we reach the source of attack .

**B. IP Trackback:**

1) If attack is there then first identify the packets, get there source IP address and mark value and contact to that sender who is sending those packets to receiver.

2) Intermediate router matches those digest value to their digest table eateries and get the IP address of particular sender router.

3) These process will continue until we reach the source of attack.

## 3.2 Actual Attacker Identification:

The attackers that we have identified earlier are not actual attackers but they are simple hosts who are occupied by the attacker in distributed environment by sending and executing agent software on their systems: To identify the actual attacker, we use the IANA and ISP.

## IANA*:*

The Internet Assigned Numbers Authority (IANA) is a department of ICANN responsible for coordinating some of the key elements that keep the Internet running smoothly. Whilst the Internet is renowned for being a worldwide network free from central coordination, there is a technical need for some key parts of the Internet to be globally coordinated - and this coordination role is undertaken by IANA.Specifically, IANA allocates and maintains unique codes and numbering systems that are used in the technical standards ("protocols") that drive the Internet. IANA's various activities can be broadly grouped in to three categories:

1) **Domain Names:** IANA manages the DNS root, the .int and .arpa domains, and an IDN practices resource.

2) **Number Recourses:** IANA coordinates the global pool of IP and AS numbers, providing them to Regional Internet Registries.

3) **Protocol Assignment:** Internet protocols' numbering systems are managed by IANA in conjunction with standards bodies.**Table 3. IANA Table**

| ISP | Domain Name | Number Resources | | Protocol |
|---|---|---|---|---|
| | | IP | AS | |
| ISP 1 | A<br>B<br>C<br>…… | x.x.x.x<br>y.y.y.y<br>z.z.z.z<br>…….. | w<br>l<br>t<br>…….. | S<br>T<br>U<br>…… |
| ISP 2 | ---------- | ---------- | ---------- | ---------- |
| ISP 3 | ---------- | ---------- | --------- | ---------- |

## ISP:

It refers to a company that provides Internet services, including personal and business access to the Internet. For a monthly fee, the service provider usually provides a software package, username, password and access phone number. Equipped with a modem, you can then log on to the Internet and browse the World Wide Web and USENET, and send and receive e-mail . For broadband access you typically receive the broadband modem hardware or pay a monthly fee for this equipment that is added to your ISP account billing.

**Table 4. ISP Table**

| IP Address | User name | pass | Login time/date | Software package | |
|---|---|---|---|---|---|
| | | | | PAC | IP |
| X.X.X.X | ABC | 123 | 2:23AM/1/1/12 | P1 | X.Y.Z.A |
| Y.Y.Y.Y | DEF | 321 | 5:22AM/2/1/12 | P2 | Y.X.Y.A |
| Z.Z.Z.Z | GHI | 136 | 3:40PM/2/1/12 | P3 | X.Z.T.A |
| ------ | ----- | ----- | ---------- | ---------- | |
| ------ | ----- | ----- | ---------- | ---------- | |

To identify the actual attacker, we follow the following steps:

**1).** Get the Information from spoofed attacker related to agent software such as that software's installing date and time.

**2).** Contact to spoofed attacker's ISP and ask him about that software's installation date and time and they will provide information about who is sending that software.

**3).** Also through spoofed attacker's ISP we go to the IANA and enquiry them about that particular attacker's IP address.

**4).** IANA provide Information related on which ISP that IP belongs.

**5).** Finally we reach attacker's ISP and identify the original attacker.

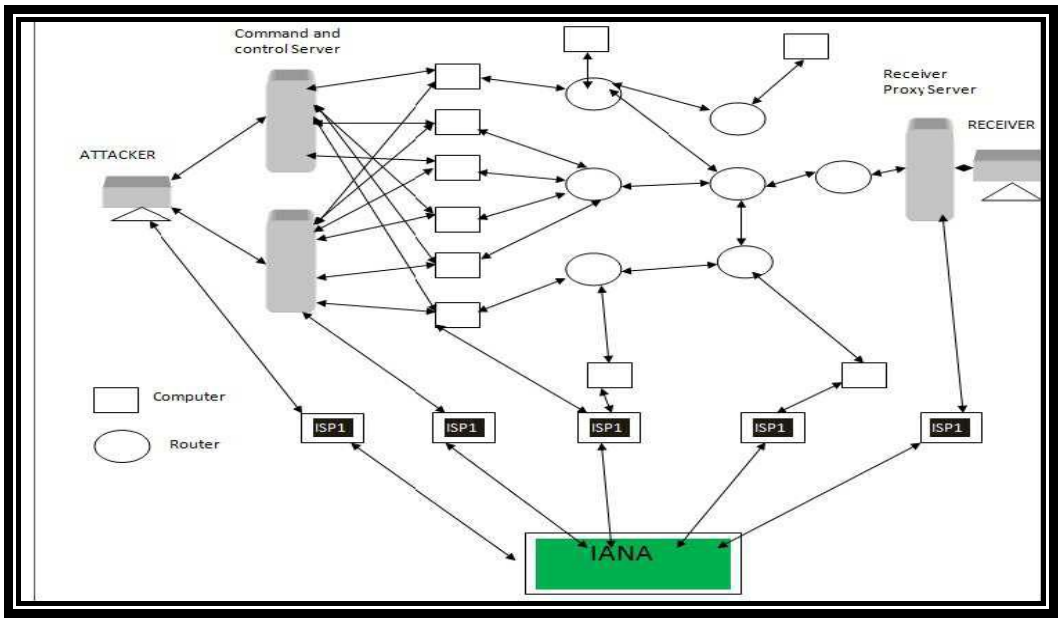


**Fig 7: DDoS Attacker Identification Proces**

## 4. CONCLUSION

In this paper we have proposed and simulated a new Marking and entropy based approach for sender authentication and DDoS detection . We have also used the concept of IANA and ISP to identify the actual attacker who is sitting behind forged systems . In fact, all the mentioned requirements have to be developed and applied to current information technology environment. Otherwise, DDoS attack will remain a perennial threat to information technology.

## 5. REFERENCES

[1] Yang-Seo Choi, Jin-Tae Oh, Jong-Soo Jang,Jae-Cheol Ryou. Integrated DDoS Attack Defense Infrastructure for Effective Attack Prevention. Information Technology Convergence and Services (ITCS), 2010 2nd International Conference, pages 1 - 6, 23 September 2010.

[2] Yao Chen, Shantanu Da, Pulak Dhar, Abdulmotaleb El Saddik, and Amiya Nayak Detecting and Preventing IP-spoofed Distributed DoS Attacks International Journal of Network Security,Vol.7, No.1,, pages 70 - 81, July 2008.

[3] Tao Peng, Defending Against Distributed Denial of Service Attacks IEEE 2002.

[4] Mopari, I.B. ; Pukale, S.G. ; Dhore, M.L. . Detection and defence against DDoS attack with IP spoofing. Computing, Communication and Networking, 2008. ICCCn 2008. International Conference, pages 1 – 5 , 24 February 2009.

[5] Wei-Tsung Su ; Tzu-Chieh Lin ; Chun-Yi Wu ; Jang-Pong Hsu ; Yau-Hwang Kuo . An On-line DDoS Attack Trace back and Mitigation System Based on Network Performance Monitoring. Advanced Communication Technology, 2008. ICACT 2008. 10th International Conference, pages 1467 - 1472, 22 April 2008.

[6] Arun Raj Kumar, P. and S. Selvakumar Distributed Denial-of-Service (DDoS) Threat in Collaborative Environment - A Survey on DDoS Attack Tools and Trace back Mechanisms 2009 IEEE International Advance Computing Conference (IACC 2009), pages 1275 - 1280 ,Patiala, India, 6-7 March 2009.

[7] Jie Wang ; Phan, R.C.-W. ; Whitley, J.N. ; Parish, D.J. DDoS attacks traffic and Flash Crowds traffic simulation with a hardware test center platform . Internet Security (WorldCIS), 2011 *World Congress on,* pages 15 - 20, 21-23 Feb. 2011.

[8] Jieren Cheng; Jianping Yin ; Yun Liu ; Zhiping Cai ; Chengkun Wu. DDoS Attack Detection Using IP Address Feature Interaction. 2009 International Conference on Intelligent Networking and Collaborative Systems , pages 113 - 118 ,4-6 Nov. 2009 .

[9] El Defrawy, K. ; Markopoulou, A. ; Argyraki, K. Optimal Allocation of Filters against DDoS Attacks . Information Theory and Applications Workshop, 2007, pages 140 - 149 , Jan. 29 2007 Feb. 2 2007 .

[10] Xiang,, Yang ; Li, Zhongwen . An Analytical Model for DDoS Attacks and Defense. International Multi-Conference on Computing in the Global Information Technology ., page 66,Aug. 2006

[11] Wanlei Zhou . Keynote III: Detection and Traceback of DDoS attacks . 8th IEEE International Conference on Computer and Information Technology, page 3,8-11 July 2008.

[12] Thing, V. ; Sloman, M. ; Dulay, N. Network domain entry point /path determination for DDoS attacks . Network Operations and Management Symposium, 2008. NOMS 2008. IEEE, pages 57 - 64, 7-11 April 2008.

[13] Shui Yu and Wanlei Zhou. Entropy-Based Collaborative Detection of DDOS Attacks on Community Networks Sixth Annual IEEE International Conference on Pervasive Computing and Communications, pages 566 - 571 ,17-21 March 2008 .

**ABOUT AUTHOR: S. K. Jena:** was born in 28April , 1954. He received his Ph.D. from Indian Institute of Technology , Bombay and M.tech from Indian Institute of Technology , Kharagpur . He has joined National Institute of Technology as Professor in the Department of Computer Science and Engineering in 2002.He has more than 70 publications in International Journals and conferences. His research areas of Interest are Database Engineering , Distributed Computing , Parallel algorithm, Information Security and Data Compression.

**Brajesh Kashyap:** was born in 15 Jan 1988. He is pursuing his M. Tech in Information Security(CSE) from National Institute of Technology , Rourkela and B.E. in Computer Science & Engineering from Govt Engg College Bilaspur in 2010 .He is selected as a Software Engineer in IBM Pvt.Ltd.