*IOSR Journal of Computer Engineering (IOSRJCE)*
*ISSN: 2278-0661, ISBN: 2278-8727 Volume 7, Issue 1 (Nov-Dec. 2012), PP 13-18*
*www.iosrjournals.org*

# Efficient Detection of Ddos Attacks by Entropy Variation

[1]V.Sushma Reddy, [2]K.Damodar Rao, [3]P.Sowmya Lakshmi
*1, 2, 3(M Tech(Software Engineering) Dept .of Computer Science & Technology,(Student) Sreenidhi Institute of Science & Technology/An Autonomous Institution ,Hyderabad,AP, India)*

***Abstract**: Distributed Denial- of- Service (DDoS) attacks are a critical threat to the Internet. It is extremely hard to trace back the attackers because of memory less feature of the internet routing mechanisms. As a result, there is no effective and efficient method to deal with this issue .In this paper, traces back of the attackers are efficiently identified and also to protect the data from the attackers using entropy variations. In the existing system, some approaches have been suggested to identify the attackers such as probabilistic Packet Marking (PPM), Deterministic Packet Marking (DPM). These two approaches are not efficient because it requires injecting marks into individual packets in order to trace back the attackers. In PPM; it can only operate in a local range of internet. In DPM, it requires all the internet routers to be updated for packet marking. Scalability is also a big problem in both PPM and DPM. In order to overcome the above drawbacks, a method based on Entropy Variation is used which is a measure changes of randomness of flows at a router for a given interval. We propose a novel trace back method for DDoS attacks that is based on entropy variations between normal and DDoS attack traffic, which is fundamentally different from commonly used packet marking techniques. This method is used to identify the attackers efficiently and supports a large scalability. In the proposing system, this method is applied to block the attackers in a wide area of network which was much efficient and protect the data from the attackers.*

***Keywords:** DDOS, IPtraceback, Entropy Variation, Flows.*

## I. Introduction

To trace back the source of the DDOS attacks in the internet is extremely hard. It is one of the extraordinary challenge to trackback the DDOS attacks, that attackers generate huge amount of requests to victims through compromised computers(zombies), in order to denying normal services or degrading the quality of services. Recent survey shows that than 70 internet operators in the world demonstrated that DDOS attack are increasing dramatically and individual attacks are more strong and sophisticated. IP trace back means the capability of identifying the actual source of any packet across the internet; with the help of IP trace back schemes identify the zombies from which the DDOS attack packets entered the internet. A number of IP trace back approaches have been suggested to identify attackers. Among them two major methods for IP trace back, Probabilistic packet marking (PPM) and deterministic (DDPM). Both of these require routers to inject marks into individual packets. And also provides some limitations such as scalability, huge demands on storage space and vulnerability to packet pollution. Both PPM and DPM also require duplicate on the existing routing software which is extremely hard.

IP traceback using information theoretical parameters, and there is no packet marking in the proposed strategy; we, therefore, can avoid the inherited shortcomings of the packet marking mechanisms. We categorize packets that are passing through a router into flows, which are defined by the upstream router where a packet came from, and the destination address of the packet. During nonattack periods, routers are required to observe and record entropy variations of local flows. In this paper, we use flow entropy variation or entropy variation interchangeably. Once a DDoS attack has been identified, the victim initiates the following pushback process to identify the locations of zombies: the victim first identifies which of its upstream routers are in the attack tree based on the flow entropy variations it has accumulated, and then submits requests to the related immediate upstream routers. The upstream routers identify where the attack flows came from based on their local entropy variations that they have monitored. Once the immediate upstream routers have identified the attack flows, they will forward the requests to their immediate upstream routers, respectively, to identify the attacker sources further; this procedure is repeated in a parallel and distributed fashion until it reaches the attack source(s) or the discrimination limit between attack flows and legitimate flows is satisfied.

## II. Steps To Launch The Ddos Attack

1) Attacker first establishes a network which is responsible for huge volume of traffic to deny the series of normal users.
2) Attackers then discover vulnerable hosts of the network. Vulnerable host in the sense that the system running no anti viruses or out of date anti viruses software.

3) Attackers The now install new programs known as attack tools on the compromised hosts.
4) It can be shown by the growth of entropy rate from the point of attack.


Fig1.DOS Attack

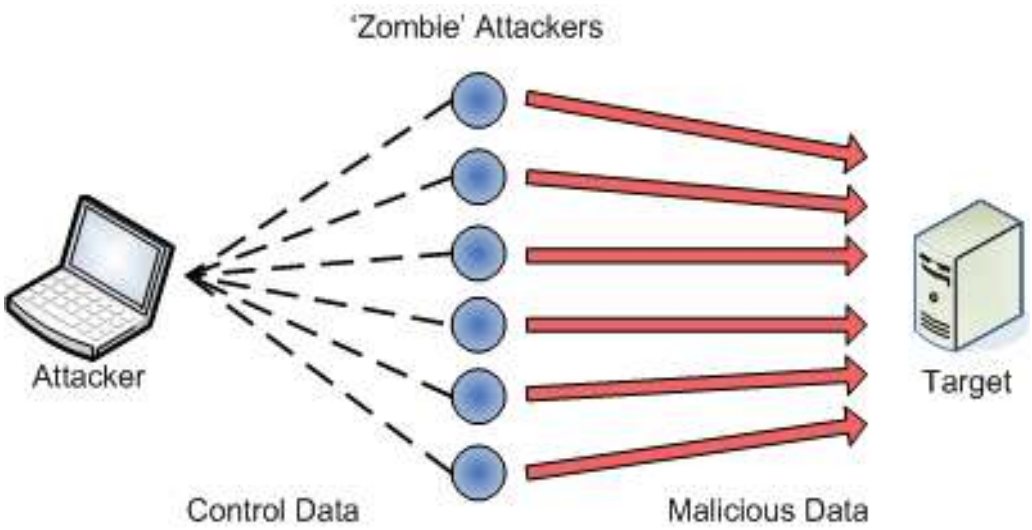
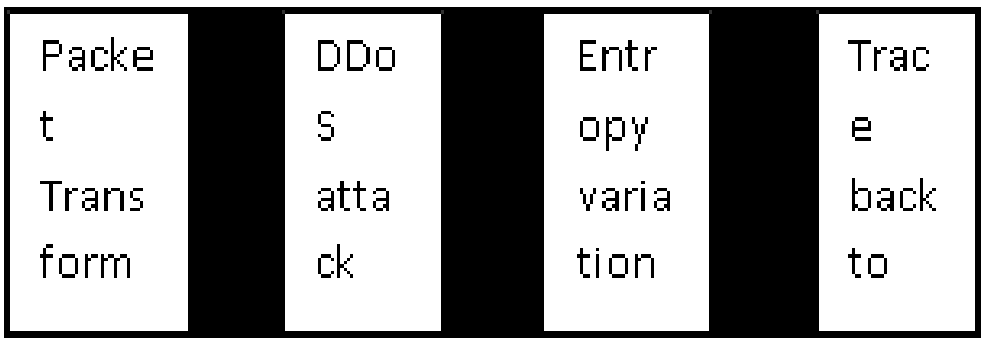



Fig2.DDOS Attack

The fig.2 explain that DDOS is "Distributed-Denial-of-Service" meaning, many "zombie" computers ganging up on one computer (or more), usually directed by one "master", which is controlled by the attacker.

**METHODS**

There are four methods used for DDOS Attacks, as shown in fig.




1) Packet Transformation: Networks and routers are created.
2) DDoS detection method: Local flow monitoring and IP traceback algorithms are used in DDoS detection.
3) Entropy Variation measurement: Entropy is a randomness measurement of flow of routers which is measured by using standard variation of flow of routers (number of packets transferred via a particular router).
4) Traceback to low rate attacks: Initialization of IP traceback algorithm (low-rate detection) through Upstream routers and Downstream routers. Low-rate DDoS attacks can detect by individual packet analyzing through some algorithm implementation

## III. System Modeling For Ip Traceback On Entropy Variations

With DDOS Attacks In order to clearly describe our traceback mechanism, we use Fig.3 as a sample network with DDoS attacks to demonstrate our traceback strategy.

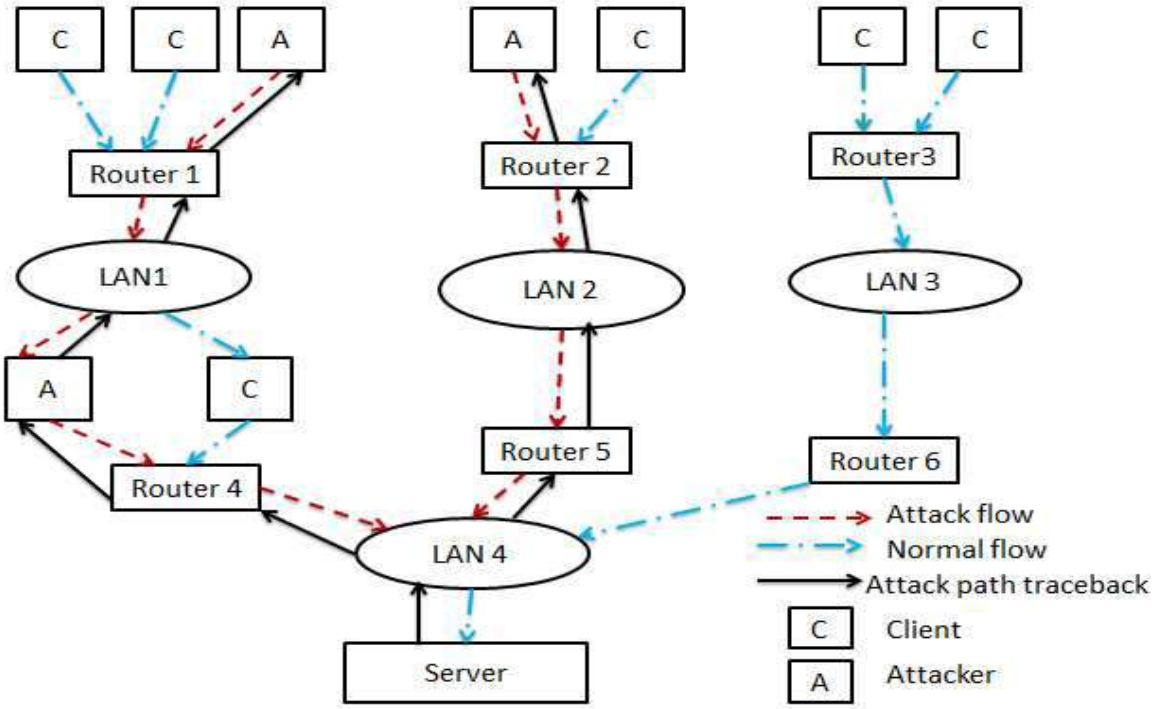



Fig3.A sample network with DDoS attacks.

In a DDoS attack scenario, as shown in Fig.3, the flows with destination as the victim include legitimate flows, such as f3, and a combination of attack flows and legitimate flows, such as f1 and f2. Compared with nonattack cases, the volumes of some flows increase significantly in a very short time period in DDoS attack cases. Observers at routers R1, R4, R5, and V will notice the dramatic changes; however, the routers who are not in the attack paths, such as R2 and R3, will not be able to sense the variations. Therefore, once the victim realizes an ongoing attack, it can push back to the LANs, which caused the changes based on the information of flow entropy variations, and therefore, we can identify the locations of attackers.

The traceback can be done in a parallel and distributed fashion in our proposed scheme. In Fig.3, based on its knowledge of entropy variations, the victim knows that attackers are somewhere behind router R1, and no attackers are behind router R2. Then the traceback request is delivered to router R1. Similar to the victim, router R1 knows that there are two groups of attackers, one group is behind the link to LAN0 and another group is behind the link to LAN1. Then the traceback requests are further delivered to the edge routers of LAN0 and LAN1, respectively. Based on entropy variation information of router R3, the edge router of LAN0 can infer that the attackers are located in the local area network, LAN0. Similarly, the edge router of LAN1 finds that there are attackers in LAN1; furthermore, there are attackers behind router R4. The traceback request is then further passed to the upstream routers, until we locate the attackers in LAN5.

## IV. Topology Creation

We categorize the packets that are passing through a router into flows. A flow is defined by a pair—the upstream router where the packet came from and the destination address of the packet. Entropy is an information theoretic concept, which is a measure of randomness. We employ entropy variation in this paper to measure changes of randomness of flows at a router for a given time interval. We notice that entropy variation is only one of the possible metrics.

First, let us have a close investigation on the flows of a router, as shown in Fig. 2. Generally, a router knows its local topology , e.g., its upstream routers, the local area network attached to the router, and the downstream routers. We name the router that weare investigating now as a local router. In the rest of the paper, we use I as the set of positive integers, and R as the set of real numbers.Wedenote a flow on a local router by <ui; dj; t>; i; j 2 I; t 2 R, where ui is an

Upstream router of a local router Ri, dj is the destination address of a group of packets that are passing through the local router Ri, and t is the current time stamp. For example, the local router Ri in Fig. 2 has two

different incoming flows—the ones from the upstream routers Rj and Rk, respectively. We name this kind of flows as transit flows. Another type of incoming flows of the local router Ri is generated at the local area network; we call these local flows, and we use L to represent the local flows.

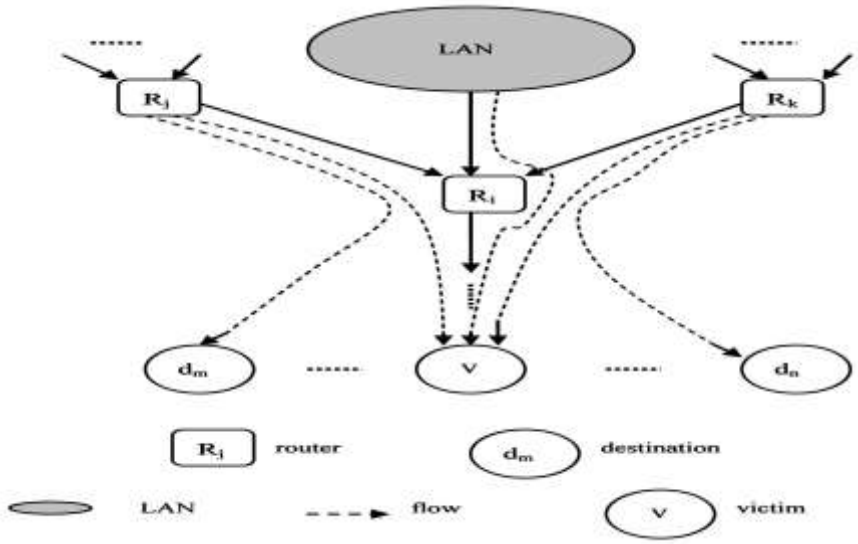



Fig.4 Traffic flows at a router on an attack path.

All the incoming flows as input flows and all the flows that are leaving from router Ri as named as output flows. D represent the destinations of the packets that are passing through the local router Ri, Attacker is responsible for traffic flow at a router.

## V. Ddos Attack Detection And Prevention

**A.DDoS Detection**

Identify the normal packet and attack packet. For the purpose of identification, we calculate Entropy variation.

**Detection Procedure**:

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

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

Where

P (*xi*) = (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.

**B.DDoS prevention**

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

## VI. Attacker Identification

**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.

## VII. Algorithm For Traceback Model

**The local flow monitoring algorithm**

1. initialize the local threshold parameter, $C, \delta$, and sampling interval $\Delta T$ ;
2. identify flows, $f_1, f_2, \ldots, f_n$ ,and set count number of each flow to zero, $x_1 = x_2 = \ldots = x_n = 0$ ;
3. when $\Delta T$ is over, calculate the probability distribution and the entropy variation as follows.

$$p_i = x_i \cdot \left( \sum_{i=1}^{n} x \right)^{-1}, \quad H(F) = -\sum_{i=1}^{n} p_i \log p_i ;$$

4. save $x_1, x_2, \ldots, x_n$ and $H(F)$ ;
5. if there is no dramatic change of the entropy variation $H(F)$ , namely, $| H(F) - C | \leq \delta$ , progress the mean $C[t] = \sum_{i=1}^{n} \alpha_i \cdot C[t-i]$ , $\sum_{i=1}^{n} \alpha_i = 1$ , and the standard variation $\delta[t] = \sum_{i=1}^{n} \beta_i \cdot \delta[t-i]$ , $\sum_{i=1}^{n} \beta_i = 1$
6. go to step 2.

Fig.5 Algorithm for local flow traffic monitoring

**The IP traceback algorithm**

1. initialize a set $A = \phi$ , and obtain the local parameter of $C$ and $\delta$ ;
2. Let $U = \{u_i\}, i \in I$ be a set of the upstream routers, $D = \{d_i\}, i \in I$ be a set of the destinations of the packets, and $\mathcal{V}$ be the victim.
3. define attack flows, $f_i = <u_j, v>, i = 1,2,\ldots,n, u_j \in U$ , and sort the attack flows in the descent order, and we have $f_1', f_2', \ldots, f_n'$ ,
4. for $i$=1 to $n$
   {
   calculate $H(F \setminus f_i')$
   if ($| H(F) - C | > \delta$) then append the responding upstream router of $f_i'$ to set A
   else break;
   end if;
   end for;
5. submit traceback requests to the routers in set A respectively, and deliver the confirmed zombies information, set A, to the victim.

Fig.6 IP Trace back algorithm on a router.

In this section, the related algorithms according to our previous modeling and analysis. There are two algorithms in the proposed traceback suite, the local flow monitoring algorithm and the IP traceback algorithm. The local flow monitoring algorithm is running at the nonattack period, accumulating information from normal network flows, and progressing the mean and the standard variation of flows. The progressing suspends when a DDoS attack is ongoing. The local flow monitoring algorithm is shown as Fig.5. Once a DDoS attack has been

confirmed by any of the existing DDoS detection algorithms, then the victim starts the IP traceback algorithm, which is shown as Fig.6. The IP traceback algorithm is installed at routers. It is initiated by the victim, and at the upstream routers, it is triggered by the IP traceback requests from the victim or the downstream routers which are on the attack path. The proposed algorithms are independent from the current routing software; they can work as independent modules at routers.

## VIII. Conclusion

I proposed an effective and efficient IP Traceback scheme against DDOS attacks based on entropy variations. Here the packet marking strategies is avoided, because it suffers a number of drawbacks. This paper employs by storing the information of flow entropy variations at routers. Once the DDOS attack has been identified it performs pushback tracing procedure. The Traceback algorithm first identifies its upstream router where the attack flows comes from and then submits the Traceback request to the related upstream router.

This procedure continues until the most far away zombies are identified. But in my existing case I used the static value to determine to determine the entropy rate. But in my proposed strategies I used dynamic value to determine the entropy rate which is based upon the packet size of the client's behavior.

## References

[1] K. Park and H. Lee, "On the Effectiveness of Probabilistic Packet Marking for IP Traceback under Denial of Service Attack," Proc.IEEE INFOCOM.
[2] S.Yu and W.Zhou, "Entropy-Based Collaborative Detection of DDoS Attacks on Community Networks," Proc. Sixth Ann. IEEEInt'l Conf. Pervasive Computing and Comm., pp. 566-571, 2008.
[3] Hoai-Vu Nguyen and Yongsun Choi," Proactive Detection of DDoS Attacks Utilizing k-NN Classifier in an Anti-DDos Framework"proc. IEEEINFOCOM 2010.
[4] Anusha. J,"Entropy Based Detection of DDOS Attacks"IJSEC-2011.
[5] G. Jin and J. Yang, "Deterministic Packet Marking Based on Redundant Decomposition for IP raceback," IEEE Comm. Letters,vol. 10, no. 3, pp. 204-206, Mar. 2006.
[6] K. Lu et al., "Robust and Efficient Detection of DDoS Attacks for Large-Scale Internet," Computer Networks, vol. 51, no. 9, pp. 5036-5056, 2007.
[7] R. Chen, J. Park, and R. Marchany, "A Divide-and-Conquer Strategy for Thwarting Distributed Denial-of-Service Attacks,"IEEE Trans. Parallel and Distributed Systems, vol. 18, no. 5, pp. 577-588, May 2007.
[8] "IP Flow-Based Technology," ArborNetworks, http://www.arbornetworks.com, 2010.
[9] A. Belenky and N. Ansari, "IP Traceback with Deterministic Packet Marking," IEEE Comm. Letters, vol. 7, no. 4, pp. 162-164.
[10] M.T. Goodrich, "Probabilistic Packet Marking for Large-Scale IP Traceback," IEEE/ACM Trans. Networking.