Defense of DDoS Attacks using Traffic Analysis at Router Level

Sirisala Sreenivasulu,
St.Johns College of Engg & Tech.,Yemmiganur, A.P, India,

S. S.Raja Kumari
M.Tech (Ph.D),
Asso Prof, CSE Dept.
St.Johns College of Engg & Tech.,Yemmiganur, A.P, India

V.Chandra Sekhar
M.Tech (Ph.D),
Prof & HOD, CSE Dept
St.Johns College of Engg & Tech.,Yemmiganur, A.P, India

ABSTRACT
Efficient Distributed denial-of-service (DDoS) is a rapidly growing problem. The multitude and variety of both the attacks and the defense approaches is overwhelming. This paper presents taxonomies for classifying attacks and defenses, and thus provides researchers with a better understanding of the problem and the current solution space. The attack classification criteria were selected to highlight commonalities and important features of attack strategies, that defines challenges and dictate the design of countermeasures. 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, results are graphically represented, the proposed model out performs the existing models in a significant way.

General Terms
This paper exposes the work on IP Trace Back of DDoS attacker based on entropy(Traffic) variations at Router level.

Keywords: DDoS attacks, IP trace back, Entropy variation.

1. INTRODUCTION
Distributed denial-of-service (DDoS) attacks pose an immense threat to the Internet, and many defense mechanisms have been proposed to combat the problem. Attackers constantly modify their tools to bypass these security systems, and researchers in turn modify their approaches to handle new attacks[11],[12]. The DDoS field is quickly becoming more and more complex, The variety of known attacks creates the impression that the problem space is vast, and hard to explore and addres.

It is an extraordinary challenge to traceback the source of Distributed Denial-of-Service (DDoS) attacks in the Internet. In DDoS attacks, attackers generate a huge amount of requests to victims through compromised computers (zombies), with the aim of denying normal service or degrading of the quality of services. It has been a major threat to the Internet for several years,even the literature does not have effective and efficient existing trace back methods to locate attackers, it is easy for attackers to disguise themselves by taking advantages of the vulnerabilities of the World Wide Web, such as the dynamic, stateless, and anonymous nature of the Internet In fact, IP traceback schemes are considered successful if they can 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 [1], [2], and there are two major methods for IP trace back, the probabilistic packet marking (PPM) [6], and the deterministic packet marking (DPM) [4]. Both of these strategies require routers to inject marks into individual packets. Moreover, the PPM strategy can only operate in a local range of the Internet (ISP network), where the defender has the authority to manage. However, this kind of ISP networks is generally quite small, and we cannot trace back to the attack sources located out of the ISP network. The DPM strategy requires all the Internet routers to be updated for packet marking further, both PPM and DPM are vulnerable to hacking [5], which is referred to as packet pollution. IP trace back methods should be independent of packet pollution and various attack patterns. In existing methods on DDoS attack detection, comparison done on the packet number distributions of packet flows, which are out of the control of attackers once the attack is launched, and we found that the similarity of attack flows is much higher than the similarity among legitimate flows,

2. RELATED WORK

2.1 DDoS Attack
The DDoS attacks are targeted at exhausting the victim's resources, such as network bandwidth, computing power, and operating system data structures. To launch a DDoS attack, the attacker(s) first establishes a network of computers that will be used to generate the huge volume of traffic needed to deny services to legitimate users of the victim. To create this attack network, attackers discover vulnerable hosts on the network. Vulnerable hosts are those that are either running no antivirus or out-of-date antivirus software, or those that have not been properly patched. These are exploited by the attackers who use the vulnerability to gain access to these hosts. The next step for the attacker is to install new programs (known as attack tools) on the compromised hosts of the attack network. The hosts running these attack tools are known as zombies, and they can be used to carry out any attack under the control of the attacker. Numerous zombies together form an army or botnet [6].

.

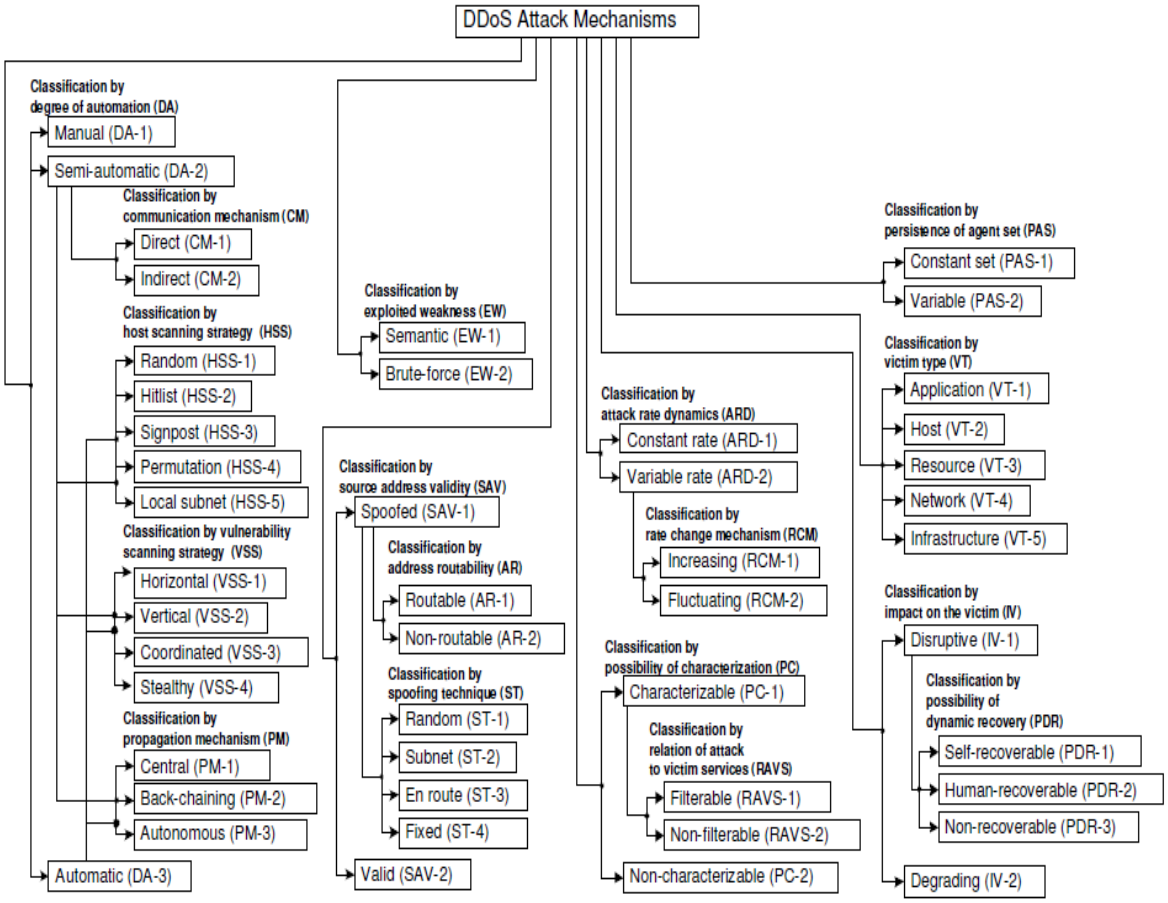

Figure 1: Toxonomy of DDoS Attack Mechanism

2.2 Toxonomy of DDoS Attack

In order to devise a taxonomy of DDoS attacks, we observe the means used to prepare and perform the attack (recruit, exploit and infect phases), the characteristics of the attackitself (use phase) and the effect it has on the victim. Figure 1 summarizes the taxonomy.

In Figure1, DA: Degree of Automation Each of the recruit, exploit, infect and use phases can be performed manually or can be automated. Based on the degree of automation, we differentiate between manual, semiautomatic and automatic DDoS attacks.

2.3 IP Trace Back

It is obvious that hunting down the attackers (zombies), and further to the hackers, is essential in solving the DDoS attack challenge. The summary of the existing DDoS traceback methods can be found in [7] and [8]. In general, the traceback strategies are based on packet marking. Packet marking methods include the PPM[3] and the DPM[4].

The PPM mechanism tries to mark packets with the router's IP address information by probability on the local router, and the victim can reconstruct the paths that the attack packets went through. The PPM method is vulnerable to attackers, as pointed out in [5], as attackers can send spoofed marking information to the victim to mislead the victim. The accuracy of PPM is another problem because the marked messages by the routers who are closer to the leaves (which means far away from the victim) could be overwritten by the downstream routers on the attack tree. At the same time, most of the PPM algorithms [9] suffer from the storage space problem to store large amount of marked packets for reconstructing the attack tree Moreover, PPM requires all the Internet routers to be involved in marking.

The deterministic packet marking mechanism tries to mark the spare space of a packet with the packet's initial router's information, e.g., IP address. Therefore, the receiver can identify the source location of the packets once it has sufficient information of the marks[10]. The major problem of DPM is that it involves modifications of the current routing software, and it may require very large amount of marks for packet reconstruction. Moreover, similar to PPM, the DPM mechanism cannot avoid pollution from attackers.

3. PROPOSED WORK

3.1 IP Trace Back based on Traffic variations

In order to clearly describe our trace back mechanism, we use Fig. 3 as a sample network with DDoS attacks to demonstrate our trace back strategy. 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 non attack 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. 1, 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 LAN_0 and another group is behind the link to LAN_1

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.

In Fig.2. The IP traceback algorithm is installed at routers. It is triggered by the IP traceback requests from the victim or the downstream routers which are on the attack path. And H(F) reefers entropy variation at the router

3.2 IP Trace Back Algorithm

Step1: Take a empty set A,consider parameters C and δ

Step2: Let $U=\{u_i\}$, $i\varepsilon I$, be a set of upstream routers, $D=\{d_i\}$, $i\varepsilon I$, be a set of destination of the packets, v is the victim

Step3: Define attack flows $f_i=(u_j,v)\ i=1,2,---n,$ and $u_j\varepsilon U$ And sort the flows in their decreasing order, and it is $f_1^{'}, f_2^{'},....f_n^{'}$

Step4: for i=1 to n

{ calculate $H\left(\frac{F}{f_i^{'}}\right)$

$if\ (|H(F)-C|>\delta)$ then

append the responding upstream router $f_i^{'}$ to set A

Else break; End if; }

Step5: Submit trace back request to router in set A sequentially and deliver the confirmed zombies information i.e set A to the victim.

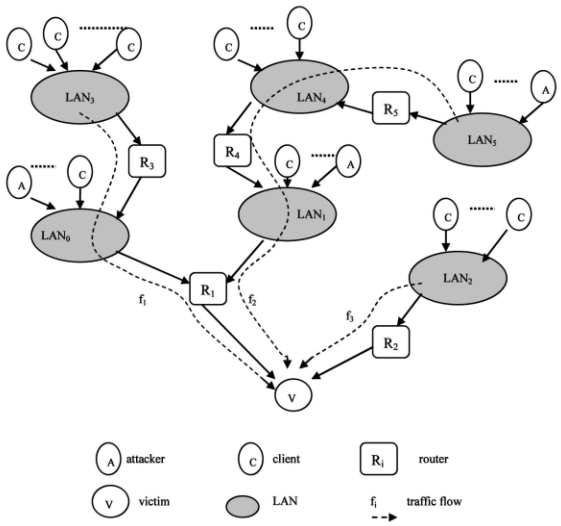

Figure 3: A Sample Network with DDoS Attacks

4. EXPERIMENTAL RESULTS

In the pursuit of establishing the claimed improvement due to the proposed method, DPE model was taken as the base for comparisons. This is due to the fact of the superiority of DPE model is already well established in the literature. The proposed model will henceforth referred as IPE model

We use the essential DDoS attack parameters in our simulations, such as, 5-10 minutes attack duration, 10,000 packets per second of attack flows

The experiments were conducted with increasing number of flows and we measure the entropy variations, as shown in Fig 4, it is clearly observed our proposed method (IPE) is out performing the existing method (DPM) for all the levels of number of flows

5. CONCLUSION

This paper is a first attempt to cut through the obscurity and structure the knowledge in the field of DDoS attacks. The taxonomies of DDOS attacks are intended to help the community think about the threats and the possible countermeasures. we proposed an effective and efficient IP traceback scheme against DDoS attacks based on entropy variations. It is a fundamentally different traceback mechanism from the currently adopted packet marking strategies, results obtained are graphically presented and show a significant improvement over the previous models.

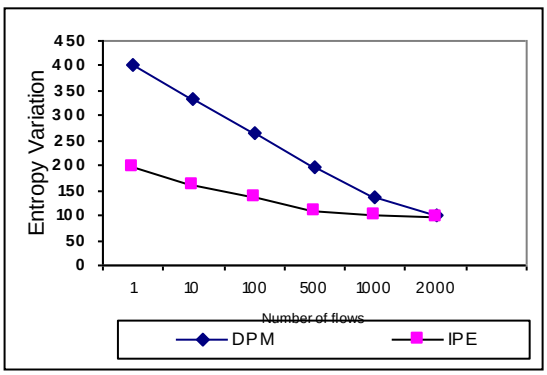

Figure.4 Comparison for IPE and DPE

6. REFERENCES

[1] T. Baba and S. Matsuda, "Tracing Network Attacks to TheirSources," IEEE Internet Computing, vol. 6, no. 2, pp. 20-26, Mar. 2002.

[2] Belenky and N. Ansari, "On IP Traceback," IEEE Comm.Magazine, pp. 142-153, July 2003.

[3] M.T. Goodrich, "Probabilistic Packet Marking for Large-Scale IP Traceback," IEEE/ACM Trans. Networking, vol. 16, no. 1, pp. 15-24, Feb. 2008.

[4] G. Jin and J. Yang, "Deterministic Packet Marking Based on Redundant Decomposition for IP Traceback," IEEE Comm.Letters, vol. 10, no. 3, pp. 204-206, Mar. 2006.

[5] K. Park and H. Lee, "On the Effectiveness of Probabilistic Packet Marking for IP Traceback under Denial of Service Attack," Proc. IEEE INFOCOM, 2001.

[6] T. Peng, C. Leckie, and K. Ramamohana rao, "Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems," ACM Computing Surveys, vol. 39, no. 1, p. 3, 2007.

[7] H. Aljifri, "IP Traceback: A New Denial-of-Service Deterrent?" IEEE Security & Privacy, vol. 1, no. 3, pp. 24-31, May/June 2003.

[8] Z. Gao and N. Ansari, "Tracing Cyber Attacks from the Practical Perspective," IEEE Comm. Letters, vol. 43, no. 5, pp. 123-131, May 2005.

[9] B. Al-Duwairi and M. Govindarasu, "Novel Hybrid Schemes Employing Packet Marking and Logging for IP Traceback,"

[10] .Saurabh, S.; Sairam, A.S "Linear and Remainder Packet Marking for fast IP traceback", Communication Systems and Networks (COMSNETS), 2012 Fourth International Conference

[11] M.; Mercy Shalinie, S.; Arun Pragash, A."IP traceback system for network and application layer attacks," Recent Trends In Information Technology (ICRTIT), 2012 International Conference

[12] Wen-Chung Kuo; Yi-Lin Chen; Shuen-Chih Tsai;,Single-Packet IP Traceback with Less Logging Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2011 Seventh International Conference