IP Traceback Techniques Review for DOS/DDOS Attacks

[1]Chirag D Patel, [2]Chirag A. Patel
[1]ME Scholar, [2]Asso. Professor
Department of Computer Engineering
Government Engineering College, Modasa, Gujarat, India

***Abstract* - Today, Internet has become the primary source of communication in networks. Distributed denial of service attacks is major source of attacks over the past decade. The source of attacks sometimes comes from a single source or multiple sources that makes harder to an investigator to trace attacks back to their original computer. DDOS attack is difficult to identify at the source since the attackers to spoofed IP address. In this paper we discuss various IP Trackback scheme to find out attacker or source of attack.**

***Keywords* - Denial of Service Attacks, IP Traceback System, IP Spoofing**

I. INTRODUCTION

DDOS Attacks are major source of cyber attacks now days. The attacker tries to hide its identification by spoofing the IP address. Current IP traceback mechanism use to solve such type of attacks. Recent IP traceback mechanism can be mainly classified into four categories. These are packet marking, debugging, link testing and Messaging.

Even though, many security devices such as firewall and intrusion detection system (IDS) are used in the network for preventing such attacks. But they are failed to identify the source of attack. Generally IP Traceback is used to find source of attacks. This IP traceback are classified into two categories: Proactive and Reactive techniques. The proactive techniques prepare information for tracing when packets are in communication while the reactive techniques start tracing after DOS attacks are detected [1].

DDos attacker is one of the most common attack in cloud computing. Attacker sends a huge amount of packets to a certain service. Each of these requests has to be processed by the server. This increases workload per attack request. This usually causes denial of service to the legitimate users also the performance of network reduces. This attack is also known as flooding attack. Denial of service does not modify data instead it crashes server and networks, making service unavailable to the legal users.DOS can be launched from either a single source or multiple sources. Multiple sources DOS attacks are Distributed denial of service (DDOS) [2]. DDOS is distributed, large scale coordinated attempt of flooding the network with large amount of packets which becomes difficult for victim network to handle and hence the victim sever becomes unable to provide the services to its legitimate user [2]. Various resources such as bandwidth, memory, computing power get wasted in serving flooding packets. It makes services or resources unavailable for indefinite amount of time. The attacker usually spoofs IP address section of a packet header in order to hide their identity from their victim.

II. TRACEBACK TECHNIQUES

A. Probabilistic Packet Marking Mechanism (PPM)

The PPM mechanism [3] utilizes 16 bit identification field and one bit reserve flag (RF) for the marking. This mechanism encodes the path by encoding bits in the IP packets. This mechanism uses three fields: start, end and distance field to encode the marking in the IP Packet. Router marks the starting address in the start field. Distance field is marked as zero by this router. When the packet reaches to the neighboring router, if it decides to mark the IP addresses, it marks its IP address into end field. Otherwise, the distance field is incremented. Here router is using probability and randomness for marking the packets. Hence, by using this technique, the edges between the routers are encoded which will be used for path reconstruction during IP traceback mechanism. The victim uses edge samples to create the graph. In PPM, there is less probability of marking of packets by farthest routers. The expectancy to receive the packet in time is bounded by the equation 1/(1-p)d-1 where ‘p’ is the probability and ‘d’ is the hops away from the victim.

B. Deterministic Packet Marking Scheme

Deterministic Packet Marking (DPM) [4][5] consider 17 bit of IP Packet (16 bit Identification field and 1 bit RF) for marking. The marks remain unchanged for as long as the packet traverse the network. The marking is done by ingress router closer to the source of attack. Hence it ensures that egress router does not overwrite the mark. Hence, the scheme makes a distinction between inbound and outbound packets. The marking of the packets is done deterministically. The 16 bits of identification fields are used for storing IP Address and one bit flag will indicate whether the segment is first or second.

C. mproved Deterministic Packet Marking

In Improved Deterministic Packet Marking algorithm [4], the packets are marked by the ingress routers. The IP packets have two fields, Identification field (16 bits) and Reserve Flag (1 bit) that can be used for marking. DPM uses two packets for marking

the IP Address of the routers [5]. IDPM uses four packets for marking the IP address of the router. In DPM, it was assumed that the Routers cannot be compromised. But in IDPM, it is assumed that the Routers can also be compromised to a certain extent.

Routers can spoof the marking code to thwart the identification of the marking process. 8 bits will be used for marking the IP Address. 7 bits will be used for storing the hash of its IP address. Two bits left will be used for storing the four segment number of the IP packet from 0 to 3. Once the packet is marked by the ingress router, intermediate routers will calculate the hash digest for the IP Address stored in ID field of IP packet from bits 0-7.

If the calculated hash of IP Address matches with the hash digest stored in Identification field of the IP packet, the packet will be passed to the next router, otherwise the packet will be dropped by the router. Hence, the next packet will be passed only if the marked IP address is not spoofed by the upstream routers. This is an improved over DPM in which victim identifies the malicious packet and after reconstructing IP address, informs the ingress router to block the packet containing that source IP address. The probability of the spoofed packet reaching the victim will be very negligible by using IDPM. The non uniform probability distribution will bring randomness to the marking of flag bit and hence will improve reconstruction.

D. Ingress/Egress Filtering

In the ingress / egress filtering [6], the edge routers are programmed by network administrators to filter the packets coming inside the network (ingress filtering) and going outside (egress filtering). The packet filtering is commonly based on the source IP addresses beyond the allocated address space to a network from which the packet is received at router's interface. The source address beyond the allocated space is deemed to be spoofed and hence the packet is discarded.

However, the filtering can also be based on some other criteria such as port number, protocol type etc. This method is a source-end, proactive technique capable of protecting against both direct and reflector types of DDoS attacks [7].

The ingress / egress filtering is easy to deploy as ISPs and network administrators have the knowledge of assigned IP address spaces allocated to different customer networks.

E. D-WARD

Ideally, DDoS attacks should be stopped as close to the sources as possible. DDoS defense system called D-WARD [8] that is deployed at the source end networks (stub networks or ISP networks) and prevents the machines from participating in DDoS attacks. DWARD is configured with a set of addresses whose outgoing traffic should be policed (its *police address set*), and monitors two-way traffic between the police address set and the rest of the Internet. Online traffic statistics are compared to predefined models of normal traffic, and non-complying flows are rate-limited. The imposed rate limit is dynamically adjusted as flow behavior changes, facilitating fast recovery of misclassified legitimate flows while severely limiting ill-behaved aggressive flows that are likely part of an attack. D-WARD strives to guarantee good service to legitimate ttraffics by profiling individual connections and serving those that are classified as good, regardless of the imposed rate limit.

F. Hope Count Filtering (HCF)

DDoS attacks are difficult to identify at the source since the attackers use spoofed IP addresses. But it is not possible for the attackers to spoof the Hop Count value in the IPV6 header. all the systems in the current Internet architecture are located within a maximum hop count value of 255. In Hope Count Filtering [9] approach the packets from the systems at the same hop count and traversing through the same router are marked with the same identification number. This number is derived by the concatenation of the 32 bits of the IP address of the router path and the encrypted value of the hop count. At the receiving side of the router interface the hop count value of the incoming packet is checked with the already stored value.

Hop Count Filtering (HCF) [10] is a packet filtering technique at victim-end which observes the TTL (Time-To- Live) values of incoming packets. The TTL value of a packet is observed and a guess is made about the same which should be inserted in the packet at sender. The difference between the initial and observed values provides the hop count. In fact, the victim-end server maintains a table of frequently communicating legitimate clients with their source IP addresses and corresponding hop counts. In a DDoS attack scenario, packets with spoofed source addresses are dropped having no entry in the table or their source addresses do not match with relevant hop counts. For such requests, the victim does not offer its resources such as TCP buffer etc. This method is a victim-end, reactive technique capable of protecting against direct DDoS attacks [11].

G. ICMP Traceback Scheme

In ICMP Traceback scheme [12], each router that suspicious packets pass through generates an ICMP traceback message or iTrace. Typically, the iTrace message consists of the next and previous hop information, and a timestamp. These information will be used as a path recovery to identify the routing path back to an originated source.

Similarly to a packet marking scheme, the disadvantages of this scheme are a requirement of a large number of packets to reconstruct attacking paths, as well as a modification of routers in which they can support a feature of routing information addition. Also, the ability to prevent major DoS and DDoS attacks is bad because this technique cannot deal with a large number of reflectors.

H. Deterministic Flow Marking

DFM [13] is a promising IP traceback approach. Unlike DPM, DFM marks every flow1, (i.e. K first packets of each flow), instead of every packet, to have both advantages of "high traceback accuracy of DPM" and "marking only some packets" of probabilistic packet marking approaches like PPM. Moreover, DFM aims to trace the attack up to the source node(s) located on a LAN behind the edge routers. To this end, DFM uses three identifiers to mark a flow: (i) the IP address of the egress interface of the edge router; (ii) the NI-ID, which is an identifier assigned to each interface of either the MAC address of a network interface

on the edge router or the VLAN ID of a virtual interface if the edge router uses VLAN interfaces; and (iii) Node-ID, which is an identifier assigned to each source MAC address observed on incoming traffic from local networks.

I. Hash-based IP Traceback Scheme

The hash-based IP traceback technique or Source Path Isolation Engine (SPIE) was introduced by Snoeren et al. [14] in 2002. The router, called Data Generation Agents (DGAs), records packet information from packets passing through it. The other components in this technique consist of; 1) SPIE Collection and Reduction Agents (SCARs) which are used for query necessary information from connected DGAs, 2) SPIE traceback manager (STM) which is used as a central management unit that communicates to IDSs of the victims and SCARs. This scheme reduces the size of storage space to store path information by using hash functions.

The negative side of this scheme is investigated by Bhaskaran et al. [15]. They found that when we use SPIE to trace attacks on high-rate interface, we must perform the action within a very short period of time. This situation gets worse if the victim does not realize he/she is under attacks, or he/she is unable to contact STM.

J. Packet Logging Traceback Scheme

In the packet logging scheme [16], which is also referred as Source Path Isolation Engine (SPIE), the information of each packet is stored or logged at routers through which the packet is passed. The routers under this scheme are termed as Data Generation Agents (DGAs). The stored information of the packet contains constant header fields and first 8 bytes of the payload which are hashed through many hash functions to produce digests. These digests are stored by DGAs using bloom filter, a space-efficient data structure. This structure is capable of reducing storage requirements by large magnitude. When about 70% of a bloom filter is filled, it is archived for later information processing and the new bloom filter is used. The duration of using a single bloom filter is called time period. Hash functions are changed during different time periods and the data necessary to reconstruct the attack path is stored in a table called Transform Lookup Table (TLT).

When an attack is detected under packet logging scheme, the central management unit called SPIE Traceback Manager (STM) sends requests to the units allocated for region wise management of DGAs known as SPIE Collection and Reduction Agent (SCARs). Each SCAR obtains copies of digests and TLTs from DGAs of its own region for the appropriate time period. It can identify which packets were forwarded by which router and reconstruct the path based on the obtained information. All SCARs report the calculated information to the STM. The STM is finally able to reconstruct the attack path through the whole network based on the information provided by SCARs. The main drawback of this scheme has been identified as the requirements of enormous computational power and storage capacity due to hash processing and bloom filter usage.

K. Pushback Traceback Scheme

In the pushback scheme [17], the router under congestion sends the rate-limit request to upstream routers. In fact, it determines from which routes the stream of packets is arrived and devises an attack signature for such traffic. The signature belongs to the aggregate traffic having some common property such as the same destination address [18]. A local mechanism called Aggregate Congestion Control (ACC) is responsible to determine the congestion on the router and create the attack signature. Based on this signature, the router sends requests to adjacent neighbors (upstream routers) to rate-limit such aggregate traffic. The neighbors, then recursively send requests (propagate pushback) to further upstream routers. However, congested router sends rate-limit requests only to those upstream routers from which it receives a significant fraction of the aggregate traffic. It also determines the rate-limit amount for each of its upstream routers according to the max min fairness algorithm. Under this algorithm, a bandwidth share is allocated in such a way that the minimum data rate which a flow can achieve is brought to the maximum first.

Then, the second lowest data rate which a flow can achieve is brought to the maximum etc. In this way, the same share of bandwidth is allocated to all.

COMPARISON OF ALL TRACEBACK TECHNIQUES

Sr. No.	**Traceback *Scheme***	**Advantage**	**Disadvantage**
1	Probabilistic Packet Marking Mechanism (PPM)	The packets are marked by each router with random probability.	The numbers of packet required for reconstruction is very large. Additional burden on network infrastructure is placed.
2	Deterministic Packet Marking Scheme	1. The packets are marked by ingress router with fixed probability. 2. The numbers of packet required for reconstruction is very less.	Poor detection capacity of DOS/DDOS
3	Improved Deterministic Packet Marking	Less number of packets is required at ingress router compare to DPM.	In the case of dynamic routing, there could be multiple ingress routers. Due to this increase in reconstruction time of IP address at victim.
4	Ingress/Egress Filtering	Easy to deploy as ISPs and network administrators have the knowledge of assigned IP address space allocated to different customer networks.	The sophisticated attackers can spoof IP address from the subnet range. Not able to detect HTTP flood attack. More administrative overhead due to filtering policies and rules.

5	D-WARD	D-WARD that is deployed at the source end Networks (stub networks or ISP networks) and prevents the machines from participating in DDoS attacks.	D-WARD is not efficient in following cases: (1) Repeated Attacks (2) Detection of UDP Attacks (3) Asymmetric Routers
6	Hope Count Filtering (HCF)	HCF does not require any change in existing protocol. It is compatible with IPV6 header format also. HCF also provides low false alarm and the packet filtering is executed close to attack sources.	HCF is only valid for static IP Address. Protocol dependent technique so it is not efficient for all kind of protocol.
7	ICMP Traceback Scheme	Easy to implement. Less network overhead. Efficient in single source attack system.	Large packet is required in reconstruction path. Less efficient in the case of Multiple attackers.
8	Deterministic Flow Marking	DFM reduces the required number of packets for trace backing accurately by 90% on average with no false positives. Moreover, DFM eliminates the spoofed marking embedded by the compromised routers in the attack path, and traces the attack source up to the attacker node, even if the attack has been originated from a network behind a NAT, firewall, or a proxy server.	Implementation is difficult. Require more efficient router in networks.
9	Hash-Based IP Trackback Scheme	This scheme reduces the size of storage space to store path information by using hash functions.	This scheme use SPIE to trace attacks on high rate interface, We must perform the action within a very short period of time. This is scheme worse if the victim does not realize he/she is under attacks.
10	Packet Logging or SPIE	Efficient in reconstruction path using SCAR and SPIE in small time.	This scheme has been identified as the requirements of enormous computational power and storage capacity.
11	Pushback Traceback Scheme	Better management in router congestion control.	Increase Network overhead.

III. REFERENCES

[1] S. Tritilanunt, T Salakit and P Achwacheewanthornkul, " IP Traceback system for denial –of – service Attacks" in April 2014 IEEE publication.

[2] Prinyanka Dembla, Chander Diwaker, "DDOS Attack Prevention Techniques in Cloud" ISSN(Online): 2349-932X Volume-1 Issue-1 2014

[3] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Network support for IP traceback,"IEEE/ACM Trans. Networking, vol. 9, pp. 226–237, June 2001.

[4] A. Parashar, Dr R Radhakrishnan, "Improved Deterministic Packet Marking Algorithm" IEEE 2013

[5] Andrey Belenky and Nirwan Ansari, "IP traceback with Deterministic Packet Marking" IEEE Communications Letters, Vol.7, No. 4, April 2003.

[6] P. Ferguson, and D. Senie, "Network Ingress Filtering: Defeating Denialof Service Attacks which employ IP Source Address Spoofing," RFC 2827, May 2000.

[7] H. Beitollahi, and G. Deconinck, "Analyzing well-known countermeasures against distributed denial of service attacks," Computer Communications, Elsevier, vol. 35, issue 11, pp. 1312-1332, June 2012

[8] Jelena Mirkovi´c Gregory Prier Peter Reiher, "Attacking DDoS at the Source" IEEE 2010

[9] Bharathi KrishnaKumar* , P.Krishna Kumar**, Prof. Dr. R. Sukanesh, "Hop Count Based Packet Processing Approach to Counter DDoS Attacks", IEEE 2010

[10] H. Wang, C. Jin, and K. G. Shin, "Defense Against Spoofed IP Traffic Using Hop-Count Filtering," IEEE/ACM Transactions On Networking, vol. 15, no. 1, pp. 40-53, February 2007

[11] H. Beitollahi, and G. Deconinck, "Analyzing well-known countermeasures against distributed denial of service attacks," Computer Communications, Elsevier, vol. 35, issue 11, pp. 1312-1332, June 2012.

[12] S. M. Bellovin, "ICMP Traceback Message" IETF draft, http://www.research.att.com/smb/papers/draftbellovin-itrace-00.txt

[13] V. Aghaei-Foroushani and N. Zincir-Heywood, "Deterministic and Authenticated Flow Marking for IP Traceback", The 27th IEEE International Conference on Advanced Information Networking and Applications (AINA-2013), March 2013.

[14] A. C. Snoeren, C. Partridge, L. A. Sanchez, C. E. Jones, F. Tchakountio, B. Schwartz, S. T. Kent, and W. T. Strayer, "Single-Packet IP Traceback", IEEE/ACM Transactions on Networking, vol. 10, no. 6, pp. 721-734

[15] V. M. Bhaskaran, A. M. Natarajan, and S. N. Sivanandam, "Analysis of IP Traceback Systems", International Symposium on Ad Hoc and Ubiquitous Computing (ISAUHC '06), pp. 125-130, Dec 2006

[16] K. Kumar, A. L. Sangal, and A. Bhandari, "Traceback Techniques Against DDoS Attacks: A Comprehensive Review," Proc. of 2nd Intl' Conference On Computer and Communication Technology (ICCCT), IEEE, pp. 491-498, September 2011.

[17] R. Mahajan, S. M. Bellovin, S. Floyd, J. Ioannidis, V. Paxson, and S. Shenker, "Controlling high bandwidth aggregates in the network," ACM SIGCOMM Computer Communication Review, vol. 32, issue 3, pp. 62- 73, July 2002.

[18] H. Beitollahi, and G. Deconinck, "Analyzing well-known countermeasures against distributed denial of service attacks," Computer Communications, Elsevier, vol. 35, issue 11, pp. 1312-1332, June 2012.