Traceback Techniques against DDOS Attacks: A Comprehensive Review

Dr. Krishan Kumar
Computer Sceinece & Engg.
SBSCET
Ferozpur, India
k.saluja@rediffmail.com

Dr. A.L Sangal
Computer Sceinece & Engg.
NIT
Jalandhar, India
sangal62@yahoo.com

Abhinav Bhandari
Computer Science& Engg.
NIT
Jalandhar,India
bhandarinitj@gmail.com

***Abstract*—Distributed denial-of-service (DDoS) is a rapidly growing problem. In a typical DDOS attacks a large number of compromised hosts (Zombies) are amassed to send useless packets to jam the victim, or its Internet connection or both. The problem of identifying the attack sources is one of the hardest threats in internet security due to the similarity between the legitimate and illegitimate traffic. Firstly, it is important characteristics of the DDOS attacks that they hide their identities/origins (IP Spoofing). Secondly, the stateless nature of the IP routing where routers normally know only the next hop for the forwarding of packets rather than the complete end to end route taken by each packet make IP traceback difficult. IP traceback (the ability to trace IP packets from source to destination) is a significant step toward identifying and, thus, stopping, attackers. This Review paper evaluates and describes the effectiveness of different existing traceback methods. These methods are based on the enhanced router functions or modifications of the current protocols. Advantages and Disadvantages have also been described in existing techniques to carry out research in this problem.**

Keywords-DDoS, Attacks, Zombies,IP Spoofing, IP Traceback

I. INTRODUCTION

A Denial of Service (DoS) attack can be characterized as an attack with the purpose of preventing legitimate users from using a specified network resource such as a website, web service, or computer system [1]. A Distributed Denial of Service (DDoS) attack is a coordinated attack on the availability of services of a given target system or network launched indirectly through many compromised computing systems. The services under attack are those of the "primary victim", while the compromised systems used to launch the attack are often called the "secondary victims." The use of secondary victims in a DDoS attack provides the attacker with the ability to wage a much larger and more disruptive attack than a DoS attack while remaining anonymous since the secondary victims actually complete the attack making it more difficult for network forensics to track down the original attacker. Broadly speaking by [2], there are two types of flooding attacks: direct attacks and reflector attacks as shown in Fig: 1.In a direct attack, an attacker send a large number of attack packets directly towards the victim. Attack packets can be of TCP, ICMP, UDP, or a mixture of them. A reflector attack is an indirect attack in that intermediary nodes (routers and various servers), better known as *reflectors*, are Innocently used as attack launchers. An attacker sends packets that require responses to the reflectors with the packets' inscribed source addresses set to a victim's address. Without realizing that the packets are actually address-spoofed, the reflectors return response packets to the victim according to the types of the attack packets. As a result, as illustrated in Fig: 1b, the attack packets are essentially reflected, in the form of normal packets, towards the victim, and the reflected packets can flood the victim's link if the number of reflectors is large enough.

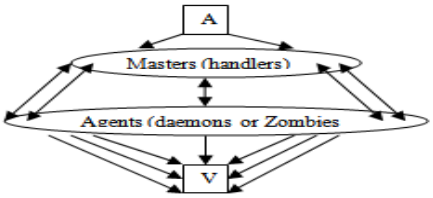

Fig: 1 a) Direct Attack

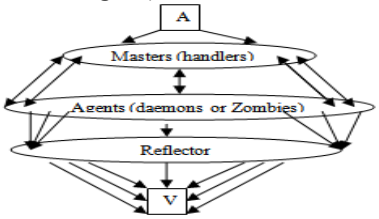

Fig: 1 b) Indirect Attack (Reflector)

I. TRACEBACK AND WHY IT IS NOT STRAIGHTFORWARD?

Once the attack has been detected, the best way of the response is to block the attacked traffic at its source or origin. Traceback which is defined in [3] as identifying the actual source of any packet sent across the Internet. We can define as C= h1+h2+…..h_{n-1}, h_n the connection chain between the hosts h_n (i=1…..n). The Traceback problem is given the identity hosts h_n (i.e IP Address) to recursively identify the identities of h_{n-1}, h_{n-2}….h1, in an automated way.

Traceback attack sources in DDOS attacks is a difficult and non trival problem due to the following reasons

- The ease with which IP address can be forged or modified (IP Spoofing).
- The stateless nature of IP routing , where router normally know only the next hop for forwarding a packet instead of knowing complete end to end path taken by each packet.

- Link Layer Spoofing
- Stepping Stones in modern DDOS Problems

II. METRICS FOR EVALUATING TRACEBACK SCHEMES

a) *ISP Involvement*: There are no incentives given to the ISPs and enterprise network to monitor the attack packets and furthermore if any ISP is involving in Traceback method. *An ideal traceback scheme should involve minimum ISP involvement.*

b) *No of Attacking Packets needed for Traceback:* IP Traceback should able to traceback the attack source based on few packets when the attack has been identified. *An ideal traceback scheme should be able to traceback the attacking source with a one packet.*

c) *Processing Overhead:* Additional Processing Overhead like measuring flow of packets, calculating various statistical parameters is occurred on the network devices like routers. *An ideal traceback method should be able to incur minimal processing overhead during traceback.*

d) *Storage Requirement:* An additional amount of memory is required to store certain information at router to perform traceback. *An ideal traceback method should be able to acquire minimum amount of memory at network equipments*.

e) *Ease of Implementation:* Traceback algorithm is an important part of the solution for stopping DOS and DDOS Attacks. These algorithms attempt to approximate the origin of the attack traffic. *An ideal traceback method should be designed in such a way that it could be easily implemented at network layer.*

f) *Scalability:* It refers to the amount of extra configuration required on the other devices when there is an addition of a single device to the scheme. *An ideal traceback method should be scalable and configuration to the devices is independent to each other*

g) *Bandwidth Overhead:* Additional traffic that the network has to carry for traceback is considered bandwidth overhead. Large bandwidth overhead is undesirable since it may exhaust the capacity of links and routers, forcing the ISP to introduce additional capacity and possibly upgrade or purchase new devices. *An ideal scheme should not assume availability of infinite bandwidth.*

h) *Number of Functions Needed to Implement:*This metric reflects how many different functions a vendor of equipment needs to implement for a given scheme. It is easier for a vendor to implement fewer functions. *Ideally only a single function should need to be implemented.*

i) *Ability to Handle Major DDoS Attacks:* This is an extremely important metric that reflects how well the scheme can perform the traceback of DDoS attack under severe circumstances (e.g., a large number of attackers using reflectors or random address spoofing). Many schemes are not able to cope with all types of attacks. Being able to trace any attack, especially a DDoS attack, is a necessary quality of a traceback scheme. *An ideal scheme would be able to trace back all attacks*.

III. CLASSIFICATION OF TRACEBACK SCHEMES

There are several schemes proposed for traceback in the literature and can be classified primarily along two dimensions as reactive and pro-active schemes. Figures 3 and 4 provide detailed classification of various schemes according to their functionality. Taxonomy of reactive schemes is given in Figure . A ***reactive approach*** is the one that carries out the IP traceback on the fly once an attack is detected. In a reactive scheme, traceback is executed in response to an ongoing attack like a stimuli-response mechanism. It's further classified as IDS assisted and Non-IDS assisted schemes depending upon whether they use an Intrusion Detection System (IDS) in their traceback mechanism. Controlled flooding and Input debugging fall under the category of Non-IDS assisted schemes and need manual intervention of an operator to conduct the traceback.

The IDS assisted schemes can be partitioned into network based and host based schemes. A reactive *host based scheme* executes the traceback from the victim node which is entrusted with this duty. The host based scheme fall into either a logging or link testing scheme. A logging scheme like Blackhole [14] maintains a log of the suspicious packets in its database for scrutinizing. A link based testing scheme like [15] performs traceback hop-by-hop at each upstream router starting from the victim node to the source. A reactive *network based scheme* is the one that is performed using some special infrastructure of the network like special routers/gateway or firmware installed on routers and is based on network traffic monitoring [15]. Some network based schemes like IPSec [16] and IDIP [17] specialized routing mechanism to conduct traceback while other schemes like DWARD SWT [15] use normal routing.

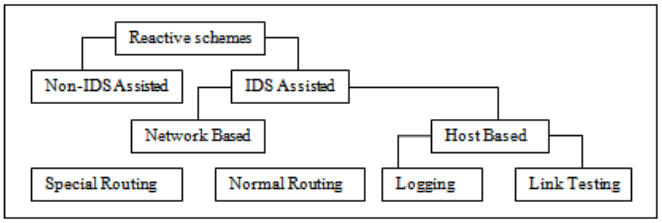

Fig: 2 Reactive Classifications

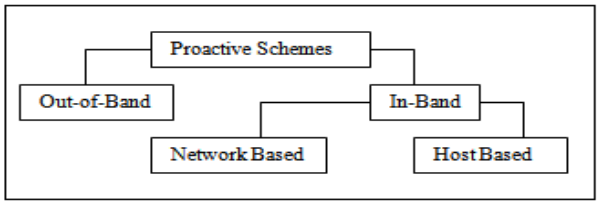

Fig: 3 Pro-Active Classifications

Figure 4 gives the topology of pro-active scheme classification. A ***proactive approach*** takes a different orientation in pinpointing the source by proactively

recording and logging the traffic packets as they flow through the network. These records are useful indicators for the victim in path reconstruction to the actual source and provide timely response on the occurrence of an attack. A pro-active scheme can be divided into two categories depending on whether the trace information is sent as a separate trace packet referred as *out-of-band* or within the data packet header known as *in-band* information. The out of- band scheme like iTrace [12], Intension-driven ICMP [12] and iCaddie [19] are all network based schemes where the path information is collected in a separate trace packet. While the out-of-band scheme incurs additional bandwidth overhead due to the deluge of packets sent in the network; the in-band scheme suffers from severe space constraint as the trace payload is carried within the packet. The in-band scheme again can be classified into network or host based schemes. In a proactive *host based scheme* the path information is encoded within the packet by the routers through which the packet passes through and the victim conducts hop-by-hop traceback. The Algebraic approach [20] is one such host based scheme. In a proactive *network based approach*, the router is actively involved in conducting traceback either by logging packets as in SPIE or by proactively marking few or all packets that traverses through the network. PPM, DPM, AAM, Adjusted PPM, SNITCH, Huffman code, DDoS SCOUNTER, Randomize and link, and Fast Internet Traceback are all marking scheme in which router inscribes its initials on the packets flowing through the network.

Another important dimension of classifying the traceback methods is on the basis of the *nature of the attacks* and based on the flow of information. On the basis of nature of attack the schemes are classified as *active and passive*. Active schemes traceback the source of the attack when the attack is going on while passive schemes do the post packet analysis i.e when the attack had already been occurred. Based on the *flow of information schemes* have been classified as extended flow of information and backtracking of flows. In *extended flow information* each network device sends to the destination some identifying information along with the normal flow and the destination. Destination recovers identification information and tries to determine the path to packets sources.In *Backtracking of flows* the destination under attack recursively determines the immediate neighbors.

All the marking schems like PPM, DPM [7][8] comes under the category of extended flow of information and Pushback [9][10], entropy variation of flow of information[11] falls under the category of backtracking flows.

IV. AVIALABLE EXISTING METHODS FOR TRACEBACK ATTACK SOURCES

The traceback Schemes fall in to following categories.

A. Hop by Hop Tracing (Link Testing)
B. Packet Marking (PPM & DPM).
C. Packet Logging (Hash Based)
D. Pushback Schemes
E. Using Entropy Variations

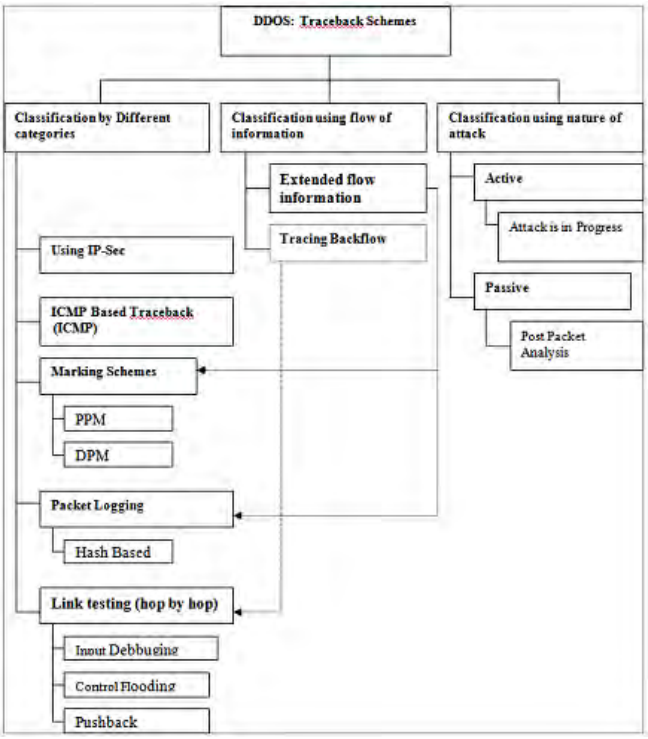

Fig: 4 Classification of Traceback scheme

A. Link Testing or Hop By Hop Tracing

This method tests the network link between routers to determine the origin of the attack traffic. This method starts from the router closed to the victim and tests the incoming links to determine which link caries the attack/malicious packets. This process is iteratively repeated until source is identified. It is a reactive method which in turn is of two types *input debugging* and *controlled flooding.*

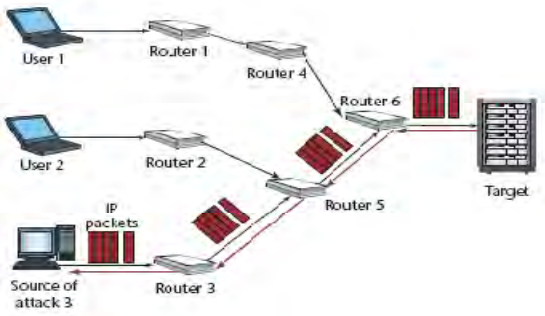

Fig5: Hop by Hot Testing

B. Messaging (ICMP based traceback)

ICMP traceback takes a different approach in determining the full path of the attack. This approach was originally introduced in [13].ICMP messages are generated by the router and sent along with the network traffic to the victim destination machine. These messages contain partial path information, including information about where the packet came from, where it was sent and its authentication as Shown in figure 8. This information is used by the victim to trace the path of a packet to its originating source node.

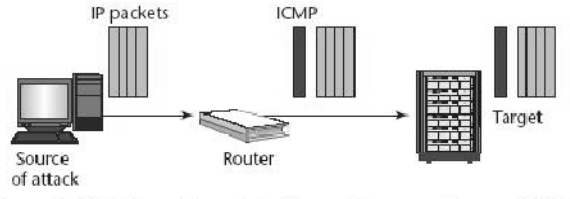

Fig 6: ICMP Traceback

Network managers could piece together these messages to trace a packet's path back to its origin. To limit the additional traffic this method generates, a router would generate an ICMP traceback message for only one in 20,000 packets passing through it (0.005 percent). This low probability limits additional network traffic, but still lets the victim figure out the attack traffic's actual path; in a typical DoS attack, the victim's network receives thousands of packets in a matter of seconds.

C. Packet Marking Schemes

In packet marking method traceback data is inserted into the IP packet by the routers on the path to the destination node. Packet marking information stored in the ID field of the IP header. There are two types of packet marking Schemes

a) Probabilistic Packet marking ((PPM)
b) Deterministic Packet marking ((DPM)

a) Probabilistic Packet Marking

The probabilistic packet marking (PPM) algorithm was carefully designed and implemented by Savage *et al.* [6] to solve the IP traceback problem. It is a used to discover the Internet map or an attack graph during a distributed denial-of-service attack. The idea is that routers mark packets that pass through them with their addresses or a part of their addresses. Packets for marking are selected at random with some fixed probability of being selected. As the victim gets the marked packets, it can reconstruct the full path, even though the IP address of the attacker is spoofed.

The PPM algorithm consists of two procedures: The packet marking procedure and graph reconstruct procedure. In the packet marking procedure the packets randomly encode every edge of the attack graph and the graph reconstruction procedure obtains the constructed graph from this encoded information. Here the constructed graph should be the same as the attack graph. The constructed graph is the graph obtained by the PPM algorithm and attack graph is the set of paths the attack packets has been traversed.To implement an IP traceback service previously they used to allocate enough space in an IP packet header so that one can use this space to record the traversed path of a packet. For example, each router, beside performing the normal packet forwarding and routing functions, records or appends its own ID in the pre-allocated space at the packet's header. In this analogy when a victim receives a marked packet, victim can examine the packet's header and obtain the complete traverse path information of the marked packet. However, one major problem about this simple approach is that the length of a traversed path (e.g., number of hops) of a packet is not fixed. Therefore, it is impossible to pre-allocate sufficient amount of space in the packet's header in advance. Another technical difficulty of recording complete path information of each packet to the victim is that if an attacker can potentially manipulate this path information and fill in false router's identification in the packet's header it misleads the victim site.

The packet marking algorithm proposed by Savage [6] instead of recording the complete path information of a packet, only records each edge traversed from the attacker to the victim site in a probabilistic fashion. The routers encode the information in three marking fields of an attack packet: (start, end, distance). The start and end fields store the IP addresses of the two routers at the end points of the marked edge. The distance field records the number of hops between the marked edge and the victim site.

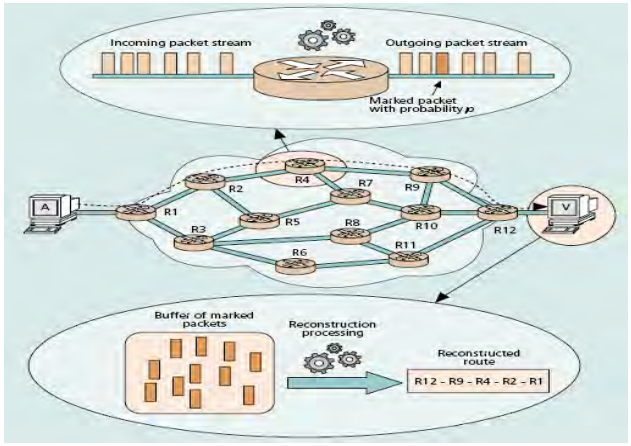

Fig 7: Probabilistic Packet Marking

b)Deterministic Packet Marking Scheme

Belenky and Ansari, outline a deterministic packet marking scheme [7].DPM is based on marking all packets at ingress interfaces. DPM is scalable, simple to implement, and introduces no bandwidth and practically no processing overhead on the network equipment. It is capable of tracing thousands of simultaneous attackers during a DDoS attack. Given sufficient deployment on the Internet, DPM is capable of tracing back to the slaves responsible for DDoS attacks that involve reflectors. In DPM, most of the processing required for traceback is done at the victim. The traceback process can be performed post-mortem allowing for tracing the attacks that may not have been noticed initially, or the attacks which would deny service to the victim so that traceback is impossible in real time. The involvement of the Internet Service Providers (ISPs) is very limited, and changes to the infrastructure and operation required to deploy DPM are minimal. DPM is capable of performing the traceback without revealing topology of the providers' network, which is a desirable quality of a traceback method.

This algorithm is a packet marking algorithm. The 16-bit Packet ID field and the reserved 1-bit Flag in the IP header will be used to mark packets. *Each* packet is marked when it enters the network. This mark remains unchanged for as long as the packet traverses the network. The packet is marked by the interface closest to the source

of the packet on the edge ingress router, as Shown in Fig 8:

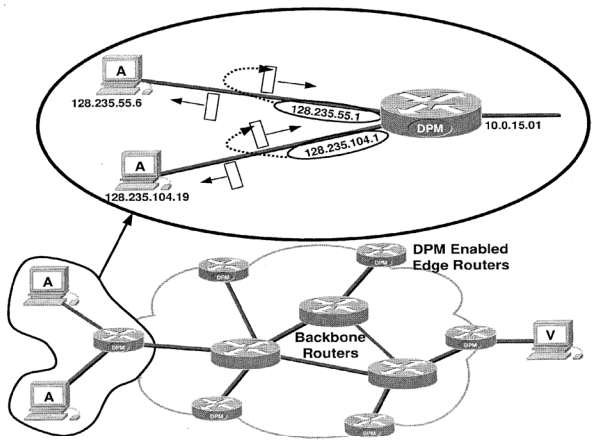

Fig 8: Deterministic packet marking Scheme

The mark is partial address information of this interface. The interface makes a distinction between incoming and outgoing packets. Incoming packets are marked; outgoing packets are not marked. This ensures that egress router will not overwrite the mark in a packet placed by an ingress router. For illustrative purposes, assume that the Internet is a network with a single administration. In this case, only interfaces closest to the customers on the edge routers will participate in packet marking. The marking will be done deterministically. Every incoming packet will be marked. Should an attacker attempt to spoof the mark, in order to deceive the victim, this spoofed mark will be overwritten with a correct mark by the very first router the packet traverses

D.Packet Logging (Hash Based Scheme)

This approach is introduced in [8]. The scheme is officially called Source Path Isolation Engine (SPIE). In hash-based traceback, every router captures partial packet information of every packet that passes through the router, to be able in the future to determine if that packet passed through it. In this scheme such routers are called *data generation agents* (DGAs). DGA functionality is implemented on the routers. The network is logically divided into regions. In every region SPIE collection and reduction agents (SCARs) connect to all DGAs, and are able to query them for necessary information. The SPIE traceback manager (STM) is a central management unit that communicates to IDSs of the victims and SCARs, as seen in Fig:9

As packets traverse the network, digests of the packets get stored in the DGAs. In this scheme, constant fields from the IP header and the first 8 bytes of the payload of each packet are hashed by several hash functions to produce several *digests*. Digests are stored in a space-efficient data structure called a *bloom filter*, which reduces storage requirements by several orders of magnitude. When a given bloom filter is about 70 percent full, it is archived for later querying, and another one is used. The duration of using a single bloom filter is called a *time period*.

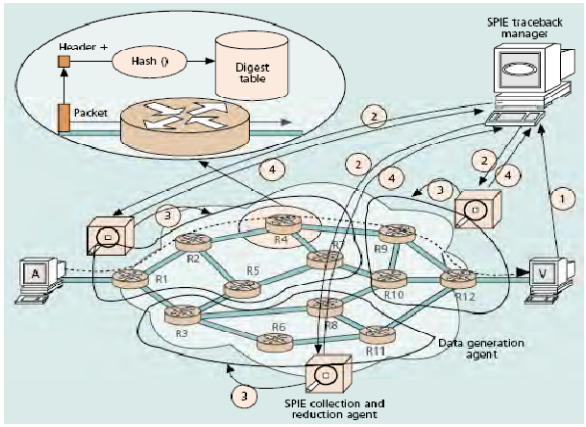

Fig 9: Hash Based Traceback Mechanism

Hash functions also change for different time periods. Also, a DGA is able to record any transformation (NAT, IPSec, etc.) that may affect those fields. The type of transformation and the data necessary to reconstruct it are stored in the transform lookup table (TLT). Each bloom filter for a given time period has its own TLT associated with it. When the STM receives notification of an attack from a victim's IDS (step 1), it sends the appropriate requests to SCARs (step2). SCARs in turn obtain copies of the digests and transformation tables from DGAs for the appropriate time period (step 3). After analyzing and correlating the tables, SCARs are able to figure out which routers in the region, if any,forwarded the packet. The SCAR can then reconstruct the path along which the packet traversed through the region, and reports it to the STM (step 4). Based on this information, the STM is able to reconstruct the path through the network.

E. IP Traceback with IP-Sec

This approach is introduced in [17] as part of a Network-based intrusion detection framework called *DECIDUOUS*. The mechanism is based on an assumption that complete network topology is known to the system. What follows is the underlying principle: If there is an IPSec security association between an arbitrary router and the victim, and the attack packets detected are authenticated by the association, the attack is originated on some device further than this router; if the packets of the attack are not authenticated by this security association, the attack is originated on some device between this router and the victim. By establishing these security associations, it is possible to identify a single router or group of routers from which the attack was initiated. In Fig:10. , when the attack is detected, an IPSec security association is built between **R4** and V. If A was in fact an attacker, attack packets have to be authenticated since they will go through the tunnel. Next, the tunnel from **R1** to V is built. Note that from **R4** to V there will be two tunnels encapsulating traffic from A. In reality (this is not obvious from the figure) the second tunnel will be encapsulated in the first tunnel. Since the traffic is authenticated by two security associations, it is clear that the attack originated from somewhere behind **R1**. If, for example, the attack packets were only authenticated by

the first tunnel and not the second, it would mean that the attack comes from somewhere between **R1** and **R4**; in the case of Fig. , it is **R2**. How the system determines with which routers the victim should build IPSec associations if the source address is not known is a valid question. The answer is not simple. In short, the system goes through many iterations considering every possible path.

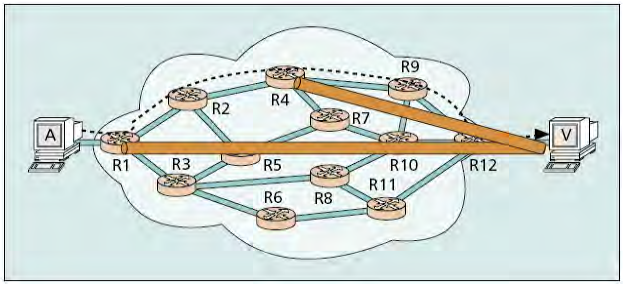

Fig: 10 Traceback with IP Sec

F. Pushback Scheme

Ioannidis and Bellovin[9] have proposed a scheme to recursively propagate the pushback signal to the network It provides not only a solution to identify sources of packets, but also a method to identify DDoS attacks and a way to control high bandwidth aggregates in the network [10]. A high bandwidth aggregate is a set of packets that share similar properties and use a significant proportion of the physical or logical bandwidth available at a network node interface. The basic idea is to extend existing network nodes with the ability to analyze output queues drop packet rates in order to detect congestions. Once congestion is detected, the node (R) is expected to identify the highest bandwidth aggregate (A). This bandwidth aggregate is then rate-limited before the output queue. Once A is rate-limited, its future evaluations will include the bandwidth at the output queue, but also the bandwidth dropped by the rate-limiter. The process to identify new high bandwidth aggregates responsible for packets drop continues as long as the output queue is experiencing a significant packet drop rate.The node identifies the neighbor upstream routers that generated the largest part of A, and sends a message (called *pushback message*) to each of them including a description of the flow F that has to be controlled, and the rate limit to be enforced (Fig:11). The neighbors repeat the same algorithm while they are receiving periodic requests from the R.

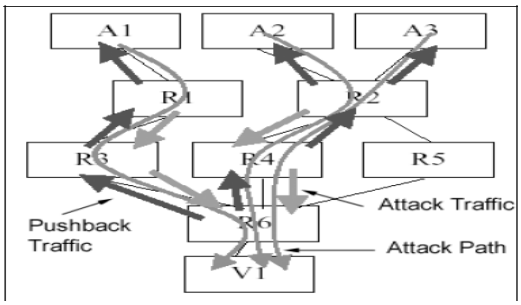

Fig: 11 Pushback Mechanism

G. Traceback based on the entropy variation

Shui Yu et al. [11] 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. Many of the available work on IP traceback depend on packet marking, either probabilistic packet marking or deterministic packet marking. Because of the vulnerability of the Internet, the packet marking mechanism suffers a number of serious drawbacks: lack of scalability; vulnerability to packet pollution from hackers and extraordinary challenge on storage space at victims or intermediate routers. On the other hand, they proposed method needs no marking on packets and therefore avoids the inherent shortcomings of packet marking mechanisms. It employs the features that are out of the control of hackers to conduct IP traceback.

In this Scheme there are two types of algorithms which are implemented at each router in the attack path, one is Local flow monitoring algorithm and the other is IP Traceback Algorithm. Flow monitoring Algorithm is running at the non attack period accumulating information from the normal network flows and progressing suspends when a DDOS attack is ongoing. It also calculates the probability distribution and entropy variation of each flow by using the formulae and record this information. if there is no dramatic change of entropy variation it progresses the mean and standard deviation of all the flows.

Once a DDOS Attack has been confirmed by the existing DDOS detection algorithm, the victim starts the IP Traceback Algorithm. This algorithm is running at routers coming in the attack tree. Victim initiates the IP the routers in the traceback list and delivers the confirmed zombies information to the victim.

V. COMPARISON OF DIFFERENT TRACEBACK SCHEMES

In this section, comparison of different traceback methods is done on the basis of the metrics defined in previous section and shown in the Table 2 and Table 3. Each mechanism is compared with the other categories of traceback schemes such as link testing, input debugging, ICMP traceback, Packet logging, PPM,DPM, Pushback and Entropy variation. Advantages and Disadvantages have been show in the the Table1.

Category	Link Testing[22]	Controlled Flooding[21]	ICMP Traceback[12]	Packet Logging[8]
ISP Involvement	High	None	Low	Moderate
No of Attack Packets needed for Traceback	N-A	Huge	Very Large	1
Processing Overhead	Low	None	Low	Low
Storage Requirement	Low	Low	Low	Fair
Ease of Implementation	Yes	Yes	Yes	Yes
Scalability	High	N-A	High	Fair
Bandwidth Overhead	High	Huge	Low	None
No of Functions Needed to Implement the Scheme	None	1	2	3
Ability to handle major DDOS Attack	Yes	No (only DOS Attack)	Yes	Yes
Classification	IDS Based	IDS Based `	Proactive	IDS Assisted

Table2 Comparison of Traceback Schemes

S.NO	Traceback Scheme	Advantages	Disadvantages
1.	Link Testing Controlled Flooding/Input debugging [3][14][21][22]	• Compatible with existing protocols • It supports for the incremental implementation • Compatible with existing routers and network infrastructure • Allows post packet analysis • ISP cooperation is not required.	• This Scheme is used only for DOS Attacks not for DDOS Attacks • This scheme is not feasible for wide deployment. • It can not trace the attack when it is over i.e attack should remain active until the trace is completed. • Bandwidth overhead is extremely high while tracing the attack origin. • It requires pre generated map of the internet topology.
2.	ICMP Traceback [12]	• Compatible with existing protocols • It supports incremental implementation. • Allows post packet analysis • ISP cooperation is not required. • Compatible with existing routers and network infrastructure	• Bandwidth overhead i.e it generates additional network traffic. • Less protective as there is no encryption scheme implemented with key distribution.
3.	Marking Scheme PPM/DPM [4][6][7]	• It is easy to implement • It has low processing and no bandwidth overhead • It is suitable for a variety of attacks [not just (D) DoS • It does not have inherent security flaws. • It does not reveal internal topologies of the ISPs • It is scalable	• Since every router marks packets probabilistically , some packets will leave the router without being marked • It is too expensive to implement this scheme in terms of memory overhead • One important assumption for PPM to work is that DOS attack traffic will have larger volume than normal traffic. However this assumption is not valid when attack is highly distributed for example in reflector attacks
4.	Logging Hashbased Scheme [8]	• Compatible with existing protocols • Support for incremental implementation • Allows post packet analysis • Insignificant network traffic overhead • Compatible with existing routers and network infrastructure	• Resource incentive in terms of processing and storage requirements • Sharing of logging information among several ISPs leads to logistic and legal issues • Less Suitable for distributed denial of service attacks
5.	IP Traceback Using IP-Sec [16]	• Compatible with existing protocol • Allows post packet analysis • Highly secure	• ISP involvement is required • Less scalable
6.	Pushback [9][10]	• It is easy to implement • It uses aggregate based congestion control algorithm which has been already implemented • Compatible with existing routers and network infrastructure	• When a router receives a pushback signal, it will start to monitor the aggregate arriving rate from the different links and find the links which contributes to the congestion. However, this scheme will not be effective if the attack traffic is uniformly distributed across the inbound links • Since aggregate arriving rate is similar in every link ,router is unable to distinguish between the malicious traffic and normal traffic which leads to the problem of false negative and false positive
7.	Traceback using Entropy Variation [11]	• It employs features that are out of the control of hackers to conduct IP traceback. • This method is scalable • It does not suffer from the problem of packet pollution • Storage space requirement at the router level is not a problem • This model can work as an independent software module with the current routing software which helps in ease in implementation	• This technique does not consider the differentiation of DDOS Attacks and flash crowds, it may treat flash crowd as DDOS Attack resulting in false positive

Table1 Advantages/Disadvantages of different Traceback schemes

Table3 Comparison of Traceback Schemes

Category	Traceback using IP-Sec[16]	PPM[6][7]	Pushback [9][10]	Traceback using Entropy Variation[11]
ISP Involvement	High	Low	No	No
No of Attack Packets needed for Traceback	Fair	Very Large	Large	Very Large
Processing Overhead	High	Low	High	High
Storage Requirement	No	High	N-A	Fair
Ease of Implementation	Yes	No	Yes	No
Scalability	Poor	High	High	Highest
Bandwidth Overhead	High	None	Very low	High
No of Functions Needed to Implement the Scheme	None	2	2	2
Ability to handle major DDOS Attack	No	Poor	Yes	Yes
Classification	IDS Assisted	Proactive	Proactive	Proactive

VI. CONCLUSION

This review paper describes the comprehensive survey of different DDOS traceback mechanisms as discussed above; none of the methods possesses all the qualities of an ideal traceback scheme. Precision, accuracy and timeliness are the three most important characteristics that measure the ingenuity of the traceback technique.As from the review it has been found that methods that are capable of tracking all the way till true source even in the presence of stepping stones, zombies/reflectors are very few in number. No doubt Solutions to a problem are rarely ideal. Very often several solutions produce a useful taxonomy. All the solutions have its own merits, demerits, ethical and legal implications

REFRENCES

[1] Stephen Specht, Ruby Lee," Taxonomies of Distributed Denial of Service Networks Attacks, Tools and Countermeasures: Technical Report". CE-L2003-03 May 16, 2003

[2] CERT Coordination Center, Cert Advisories: CA-2000-01 denial of service developments," http://www.cert.org/ Advisories/CA-2000-01.

[3] A.Belenky, Nirwan Ansari," On IP Traceback,"IEEE communication Magazine, July, 2003

[4] Dawn Xiaodong Song and Adrian Perrig,"Advanced and Authenticated Marking Schemes for IP Traceback". In *Proceedings of the IEEE INFOCOM,* IEEE CS Press, pp. 878-886, 2001

[5] R. K. C. Chang, "Defending against Flooding-Based Distributed Denial-of-Service Attacks: A Tutorial," *IEEE Commun. Mag.*, Oct. 2002, pp. 42–51.

[6.] S. Savage *et al.*, "Network Support for IP Traceback," *IEEE/ACM Trans. Net.*, vol. 9, no. 3, June 2001, pp. 226–37.

[7] A. Belenky and N. Ansari, "Tracing Multiple Attackers with Deterministic Packet Marking (DPM)", Proc. of IEEE Pacific Rim Conference on Communications, Computers and Signal Processing,2003.

[8] A. C. Snoeren *et al.*, "Single-Packet IP Traceback," *IEEE/ACM Trans. Net.*, vol. 10, no. 6, Dec. 2002, pp. 721–34.

[9]J. Ioannidis, S. Bellovin," Implementing Pushback: Router Defense Against DDOS Attacks", Proceedings of Network and Distributed System Security Symposium, San diego , 2002

[10] R. Mahajan, S. Floyd, and D. etherall. Controlling High-Bandwidth Flows at the Congested Router. In *ICNP*, Nov.2001.

[11] Shui Yu, Wanlei Zhou, " Traceback of DDOS Attacks using Entropy Variations", IEEE Transactions on Parallel and Distributed System, 2010.

[12]S. M. Bellovin, "ICMP Traceback Messages," IETF draft,2000;http://www.research.att.com/smb/papers/draftbellovin- itrace-00.txt.

[13] Howard F. Lipson, "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues"CERT Coordination Center, Special Report CMU/SEI-2002- SR-009.

[14] Tatsuya Baba and Shigeyuki Matsuda, "Tracing Network Attacks to their Sources", *IEEE Internet Computing Magazine,* Vol. 6, No. 3, pp. 20-26, March/April 2002.

[15] X. Wang, Douglas S. Reeves, Shyhtsun Felix Wu and Jim Yuill, "Sleepy Watermark Tracing: An Active Network-based Intrusion Response Framework". In *Proceedings of the IFIP Conf. on Security, Paris*, pp. 369-384, 2001, June 11-13.

[16]H. Y. Chang, R. Narayanan, S. F. Wu, B. M. Vetter, X. Wang, M. Brown, J. J Yuill, C. Sargor, F. Jou, and F. Gong, "Deciduous: Decentralized Source Identification for Network-Based Intrusions". In *Proceeding of the 6th IFIP/IEEE Int'l. Symp. Integrated Net. Mgmt.*, pp. 701-714, 1999.

[17]J. Rowe, "Intrusion Detection and Isolation Protocol: Automated Response to Attacks". In *Proceedings of the Recent Advances in Intrusion Detection (RAID)*, University of California Davis, USA, 1999.

[18] X. Wang, Douglas S. Reeves, Shyhtsun Felix Wu and Jim Yuill, "Sleepy Watermark Tracing: An Active Network-based Intrusion Response Framework". In *Proceedings of the IFIP Conf. on Security, Paris*, pp. 369-384, 2001, June 11-13.

[19] Bao-Tung Wang and Henning Schulzrinne, "A Denial-of-Service-Resistant IP Traceback Approach," In *Proceedings of the IEEE 9th international symposium on Computers and Communication, (ISCC)*, Vol. 1, pp. 351-356, June/July 2004.

[20] D. Dean, M. Franklin, and A. Stubblefield, "An Algebraic Approach to IP Traceback". In *proceedings of the ACM Trans. Information and System Security,* Vol. 5, No. 2, pp. 119-137, 2002.

[21] H. Burch and B. Cheswick, "Tracing Anonymous Packets to Their Approximate Source," *Proc. USENIX LISA*, 2000, pp. 319–27.

[22]. R. Stone, "CenterTrack: An IP Overlay Network for Tracking DoS Floods," *Proc. 9th Usenix Security Symp.*, Usenix Assoc., 2000, pp. 199–212.