A Survey on Various Mechanisms and IP Traceback Schemes to Defend DDoS Attacks

Jatin Mahendroo
ECE Dept, GNDU
RC Jalandhar

Vinit Grewal
ECE Dept GNDU
RC Jalandhar

ABSTRACT

Distributed Denial of Service (DDoS) attacks are the major threat to Internet today that can make the server unavailable for legitimate user and finally take down the service. A number of mechanisms, approaches and various Traceback schemes are developed to defend such attacks. This paper surveys the various defensive techniques and various IP Traceback schemes to prevent various DDoS attacks.

Keywords

DDoS attacks, IP Traceback, Packet logging, PPM, DPM, RIHT, Defense mechanisms.

1. INTRODUCTION

DDoS attacks makes the resources unavailable for the users for a particular time or can even crash the resource [1]. These attacks perform by sending a stream of packets that drowns their network bandwidth and processing power thus blocking access to legitimate users. DDoS uses common protocols like TCP, UDP, ICMP etc which make it tough to make a distinction between the legitimate traffic and attack traffic [2]. DDoS attacks are possible due to vulnerability present in the architecture of Internet. IP spoofing make it tough to trace the origin of packets or attacker. Figure 1 depicts a scenario of typical DDoS attacks representing the path travelled by the attack packets.

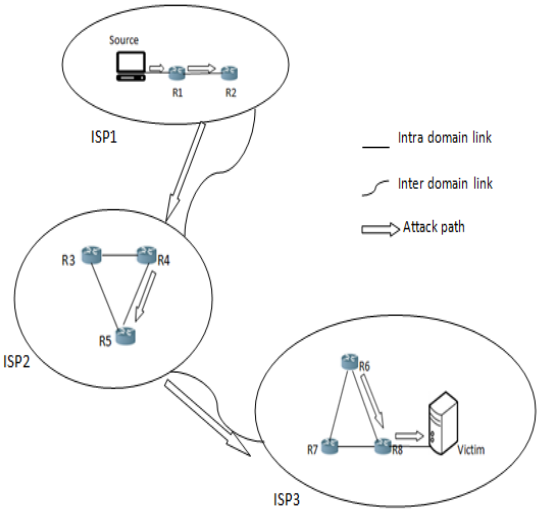

Figure 1 A scenario of typical DDoS attack

This path can be defined by number of routers from source to destination as { R1, R2, R4, R5, R6, R8}. The link between various routers in an ISP is known as intra domain link whereas link between various ISP's is called as Inter domain link. The attack may vary from various ISP's to construct the attack path. It is not easy for the user to use data safely. Packet Dropping Ratio increased to an extent as the attack is performing. Various mechanisms and approaches and Traceback schemes can be used to prevent such attacks. DDoS Defense Mechanisms is described in this paper. Section 2. Section 3 and 4 describe the approaches used and techniques used to prevent such attacks. Section 5 and 6 presents various IP Traceback schemes on network layer and metrics for various IP Traceback schemes respectively. Section 7concludes the paper. This paper is organized as follows.

2. DDOS DEFENSE MECHANISMS

DDoS attack is an attempt to make a server unavailable for the legitimate users and finally to take the service down[2]. DDoS defense mechanisms are classified according to the activity deployed and has generally four categories. It is generally shown in figure2.

2.1 Intrusion Prevention

In such type various methods are discussed to prevent the various DDoS attacks. Various methods as well as techniques can be used to prevent such attacks. Filters like ingress as well as Egress filters and various honeypots can be used to prevent such attacks.

2.1.1 Using Filter

Various filters can be used to defend DDoS mechanism. These can be categorized as Egress filter and Ingress filters.

A. Egress Filter: - It is having similar behaviour like ingress filter, but it is a kind of out band filter [3]. It ensures that only allocated IP address leaves the network.

B. Ingress Filter:- It is an approach which sets up a router that does not accepts packet from the illegitimate user. In such mechanism, the IP address that does not match to the prefix domain in the router is rejected, In this way the packets are dropped and the attack is prevented.

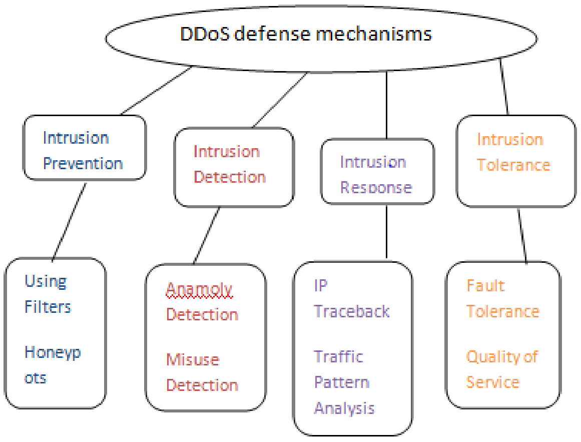

Figure2 Classification of DDoS Defense mechanisms

2.1.2 Route based distributed packet filter

In such type, only the packets with the prefixed route is allowed to reach on destination and the other is rejected []. Hence in such mechanism the illegitimate packets are rejected. Such filter is better than that of ingress and egress filter.

2.1.3 Using Honey pots

In this method the system is secured by the temporary system called the honey pots. It's a kind of trick such that whenever attacker wants to attack, the attack will not perform on the system. Hence in this way the system can be secured. The advantage of using such technique is that the information about the attacker, type of attack can be known.

2.1.4 Changing IP address

Changing an IP address can prevent the DoS attack to an extent, but it is no longer validated because attackers can find the new IP address by tracing it with the various tools.

2.2 Intrusion Detection

Intrusion detection systems detects the DDoS attacks either by using the database of known signatures or also by recognizing the anomalies in system.

2.2.1 Anomaly Detection

Various factors can be termed under baseline like bandwidth, protocols, devices used etc. If the value finds changing from the baseline it alerts the user that some bad activity is performed. for anomaly detection of the DDoS attacks. Some of its mechanisms are discussed as follows.

2.2.2 NOMAD

NOMAD system can be used to detect network anomalies by making statically analysis of IP packet header [2]. It can also be used for detecting the anomalies of local network traffic.

2.2.3 Misuse Detection

Identifies the well known patterns and search for such kind of patterns. These patterns can be any condition, arrangement, structure that leads to breakage of the signal between source to destination. Such types of mechanism are regarded under the signature based mechanism.

D-WARD

It is a kind of system that does DDoS attack detection at the source so that DDoS attacks should be stopped as close to the sources as possible. D-WARD is installed at the edge routers of a network and monitors the traffic being sent to and from the hosts in its interior.

2.3 Intrusion response

If the attack is identified the next step is to blocking the source and the traffic accordingly. The blocking part is done manually either by contacting the higher administrations or by accessing control lists.

2.3.1 IP Traceback

It is the method that traces the original identity or source from which the attack is performed [7]. For performing this it is necessary to construct the attack path. It is very efficient method to construct the path, but various packets are required for this. Hence in this way manually the attack can be control.

2.3.2 Internet Control Message Protocol (ICMP) Tracebook is another mechanism with the assumption that there is having a very low probability of sampling the packets by the router and sends the ICMP trace messages to the destination. If the enough tracebook messages are received then the path can be constructed. Hence in this way the source can be found.

*2.3.3 Probabilistic Packet Marking (PPM)*It is the mechanism in which the tracing is performed through the IP packets [6].The IP packets for tracing can be received from the victim. The advantage of using such mechanism is that no extra traffic is required in this case, also there is no need to communicate with the ISP's.

2.4 Intrusion Tolerance and Mitigation

It ensures that it is not possible to defend the DDoS attacks completely, but the various techniques and factors can be discovered on the basis of such attacks can be tolerated to an extent.

2.4.1 Fault Tolerance is the mechanism introduced in three levels i.e. hardware, software and system, so that the duplicate networks can be made so to control the congestion.

2.4.2 Quality of Service describes the assurance of the ability of network to give the predictable results. Many techniques are also designed under this mechanism.

2.4.3 Throttling is the mitigation approach which don't let the web server down. By installing such throttles all the traffic pass through the router, to the source is rate limited to the throttle rate. This mechanism can distribute the services in max-min way according to the need of packets by the routers servicing them.

3. APPROACHES USED FOR DEFENSE MECHANISMS

Normally three approaches are used to prevent various DDoS Attacks. These are prioritizing in the figure on the basis of merit.

3.1 Signature Based Approach (SBA):-

In SBA system the database is made of the known attacks that generally happened in various organizations. The disadvantage of using this approach is that it cannot detect the new malformed attacks. Hence it is not so much effective approach.

3.2 Anomaly Based Approach (ABA):-

It overcomes the limitation of SBA [7]. It generally uses distribution analysis approaches, statistical approach. A baseline is decided in which its database is prepared on the basis of the bandwidth used in various system, regularly used protocols, ports and devices used are taken into account. If the value finds changing from the baseline it alerts the user that some bad activity is performed. It is also having problem that sometimes it can give false positive alarm due to higher bandwidth and some other consequences.

3.3 Entropy Based Approach (EBA):-

It is the most significant approach. When the monitored values run in normal way, entropy value is smooth. When the attack is done, there will change in entropy. So in this various algorithms can be used to perform fast entropy approach. It is performed to increase the sensitivity of the system.

4. VARIOUS TECHNIQUES USED AND THEIR IMPACT ON SYSTEM

There are various techniques used for defense mechanisms like increasing bandwidth, using firewalls, using various routers and switches. These techniques along with their impact are shown in the Table1. For simple attacks we can use firewalls based on various protocols, but with the increased in complexity they can replaced with switches and routers. IPS based prevention is used in case of known signatures of the attack. The signatures can be updated time to time, whereas connection based attacks can be defend by DDS based techniques or Blackholing and Sinkholing techniques.

5. IP TRACEBACK SCHEMES

The best possible defense against DDoS attack lies not only in preventive measures but to block that malicious attack or origin of the attack by founding the attackers.. This scheme referred as the IP Traceback scheme. It implies to identify the actual source of a packet [8]. Traceback scheme makes difficult for the attacker to hide its identity only by spoofing the source address, so it’s a difficult task for the attacker to execute an attack. The existing IP Traceback schemes falls in these following classes.

Table1 Various Techniques used to prevent DDoS Attacks and their Impact

Defensive Techniques	**Impact**
Increasing Bandwidth	To defend the DDoS attack or to control the traffic flood, it is essential to increase the bandwidth of the system. With the increase in bandwidth, raw processing power should also increase to increase the level of defending.
Using Firewalls	For simple attacks it is beneficial to use firewalls. These are based on protocols and can defend DDoS attacks easily. The disadvantage of using firewalls is that it cannot be used for complex attacks or it cannot defend high level attacks.
Using switches and Routers	The advantage of using switches and r5outers among that of firewalls are its automatic system, traffic shaping, deep packet inspection, rate limiting as well as ACL capability. Due to these capabilities it can handle some complex DDoS attacks.
IPS based Prevention	Intrusion Prevention System (IPS) are effective only if attacks have signatures associated with them. It means that for new signatures or fake certificates it will not perform better. The ASIC based IPS system can detect and block the DoS attacks because of high processing power. The Rate based IPS system also analyze the data and continuously monitor traffic data and determine if there is illegitimate data it will be eliminated.
DDS based Defense	DoS Defense System (DDS) is superior in blocking the connection based DoS attacks. It can also address protocol attacks like Teardrop attack as well as rate based attacks like SYN floods.
Blackholing and Sinkholing	Black holing leads all the traffic from the attacked IP address to the null interface. Sinkholing routes traffic to the valid IP address which passes legitimate packets and reject bad packets.

5.1.1 *Link Testing*

In this scheme the router closest to the victim starts the mechanism by sending the upstream links to determine the source or origin from where attack is initiated. Two techniques fall under this scheme i.e. input debugging and controlled flooding. Figure 3 determines the upstream path between server and client via R4, R2, R1.

A. Input Debugging: When an attack is detected at the victim site, it creates signature of an attack packet. Routers generally have the capability to find the ingress port through which attack packets are coming using attack signature generated by victim site. This process is performed upstream till source of the attack is identified. The limitation of using this scheme is that it does not provide any infrastructure for communicating and coordinating between multiple ISP’s

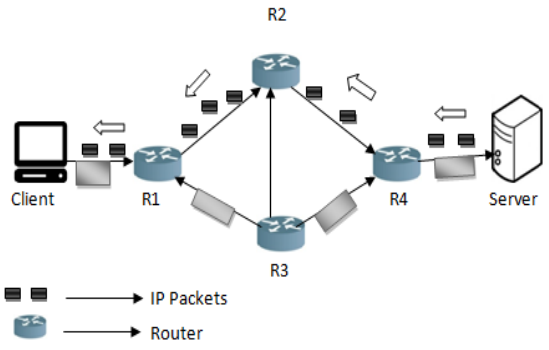

Figure 3 Link Testing Mechanism

B. Controlled Flooding: It does not require any support from ISPs. Victim is known about the topology of Internet. It floods the upstream links continuously with large burst of traffic and monitors its effect on the attack packets. As router share buffers, overloading of attack packet leads to dropping of packets.

5.1.2 *Messaging*

In ICMP (Internet Control Message Protocol) based technique, each router probabilistically generates an ICMP packet, generally known as trace packet directed towards the destination of selected packets. Router generates this message for a particular interval i.e. one in every 20,000 packets passing through it. It contains MAC address, next and previous hop information, timestamp etc.

5.1.3 *Marking*

The key idea behind the packet marking is to record the route information through which packets are travelled from source to destination. This information is used by the victim to resolve the path packets traversed. Packets may contain the partial path or full path of the marking packets depending upon which scheme is used i.e. either PPM or DPM.

5.1.4. Logging

Packet logging identifies the log packets at some crucial routers as shown in figure4. The network path is then determined using logged information at those routers. This approach uses a single packet, hence a much beneficial technique with the limitation that it requires a large processing overhead with them.

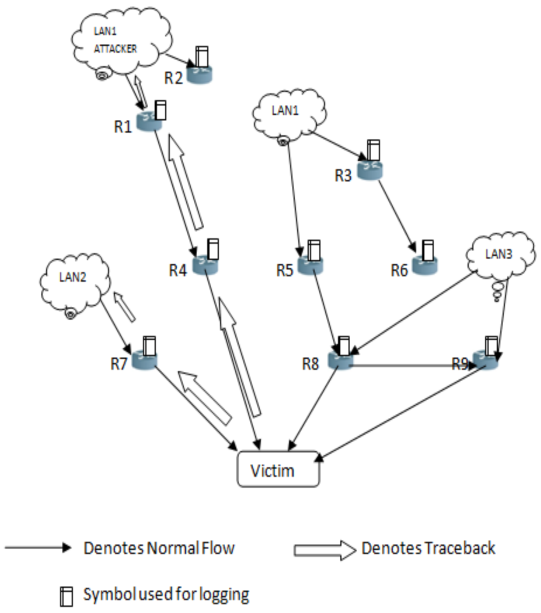

Figure4 Packet logging Mechanism

Various Traceback schemes used based on these classes are

5.2 Probabilistic packet Marking(PPM)

The idea behind this scheme is to mark the packets passing through the router with its identities i.e. IP address with some fixed probability [10]. Figure 5 determines that each router marked their packets and gives their own identity, but still some packets remain unmarked.

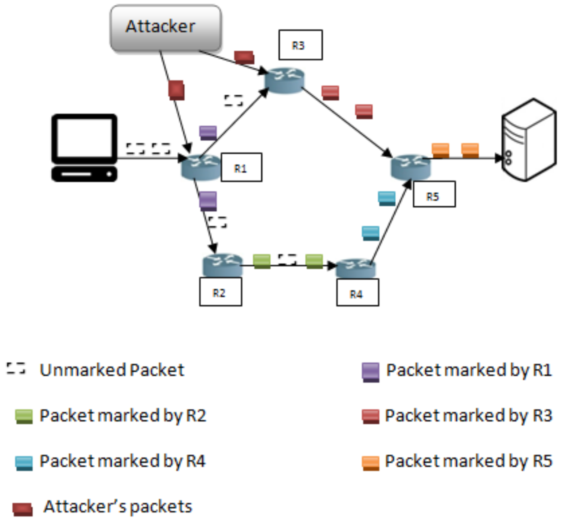

Figure 5 Packet Marking Scheme

Packets marked under this mechanism constructs partial path, hence the rest path is determined probabilistically. There are chances of some unmarked packets due to which packets are not able to construct full path. This is the quite limitation of this technique, which is overcome by further techniques like DPM and DPPM.

5.3 Deterministic Packet Marking (DPM)

DPM [6] is based on marking of all the packets at ingress interfaces with their IP addresses. Marking is done when a packet enters into network by the closest router to the source. This mark remains unchanged, can-not overwritten by any other router. This eliminates the issue of mark spoofing. In such scheme, router only marks the incoming packets, not outgoing packets.

5.4 Dynamic Probabilistic Packet Marking (DPPM)

PPM uses the fixed probability marking, which constructs the partial path, hence number of leftover packets are there. Dynamic probabilistic packet marking (DPPM) [11] eliminates this issue in which dynamic probability replaces fixed probability of marking. It removes the problem of leftover packets. The probability of marking is highest as the packet enters into the network and least when packet is close to destination. For a given attack path, let m ($1 \leq m \leq D$) be the traveling distance of a packet from its source. Router chooses its marking probability P=1/m to mark the packet

5.5 ITrace

The idea behind this scheme is that every router generates an ICMP Traceback messages as ITrace messages corresponding to the selected packets with the probability of 1/20000 destined till end of path. ITrace message consists of next and the previous hop information and a time stamp. Considering these messages help victim to construct the attack path.

5.6 Advanced and Authenticated Packet Marking (AAM)

Advanced marking scheme allows path reconstruction more accurate and efficient while authenticated Marking Scheme supports authentication of marking by routers. This allows victim to avoid the issue of spurious markings. It assumes that routers and victim shares a secret key using the idea of cryptographic technique to provide authentication.

5.7 RIHT: A Novel Hybrid IP Traceback Scheme

RIHT marks interface numbers of routers on packets so as to trace the path of packets [15]. Since the marking field on each packet is limited, packet-marking scheme may need to log the marking field into a hash table, hence store the table index on the packet. The process of marking/logging is repeated till the packets reached to their destination. Reversing of path is also done to trace the attacker. The advantage of using this scheme is that it is the most efficient scheme and it requires fixed storage space.

5.8 Simple, Novel IP Traceback using Compressed Header(SNITCH)

SNITCH uses same principle as that of header compression for making more space available for the Traceback information. To differentiate between the header compression and SNITCH scheme, 1‘s are inserted in IP identification field. In such scheme initial packets are sent with a full header, subsequent packets can be sent without the static content in the header. The advantage of using SNITCH is that probability of finding the attacker is maximum with low false positive rates i.e. (maximum of 0.43% for 5067 simultaneous attackers) .

6. METRICS FOR IP TRACEBACK TECHNIQUES

Various metrics are used for evaluating the performance of IP Traceback techniques These metrics are based on the accuracy, reliability and various factors. These are explained as follows

6.1 Accuracy

Accuracy is an important metric which measures the precision of the scheme. There should be less false positives and false negatives in an ideal Traceback scheme. False positive is tracing a legitimate node as an attacker node, whereas false negative is missing to identify the attacker node. Link testing based schemes does not show fine level of accuracy.DPM and PPM rely on multiple packets to store the IP address, which may also result in false positive. SPIE uses Bloom filter to log the hash digest. RIHT claims zero false positive and false negative.

6.2 Memory Requirement

An ideal Traceback scheme does not require any additional storage on the network devices. ITrace and marking schemes don't have any storage at the routers whereas logging and hybrid scheme needs logging at the intermediate routers in the attack path. Using SPIE, a core router with 32 OC-192 links requires 23.4 GB [15] and RIHT requires a fixed storage of 320 KB [16].

6.3 Number of packets required to Traceback

Various schemes use multiple packets to Traceback the attacker, because the entire information cannot be stored in a single packet. Few techniques like SPIE and RIHT use single packet for tracing purposes. The advantage of using single packet is that they show very less false positive rates. The number of packets required to reconstruct the attack path in ICMP Traceback is given by

$$nH/p \qquad \text{------ (1)}$$

where m is the number of attackers, H is the harmonic number and p is the probability at which the ICMP packet was generated. The expected number of packets using DPM is given by

$$P=1-0.5^{t} \qquad \text{------- (2)}$$

Where t is the number of packets needed to identify one attacker. P is the probability of identifying one IP address. Figure6 shows the expected number of packets required for various Traceback schemes to trace the attack path. In this it is clearly shown that SPIE and RIHT require single packet for Traceback mechanism. DPM requires more number of packets than PPM. ICMP require approx. 20000 packets to identify the attacker

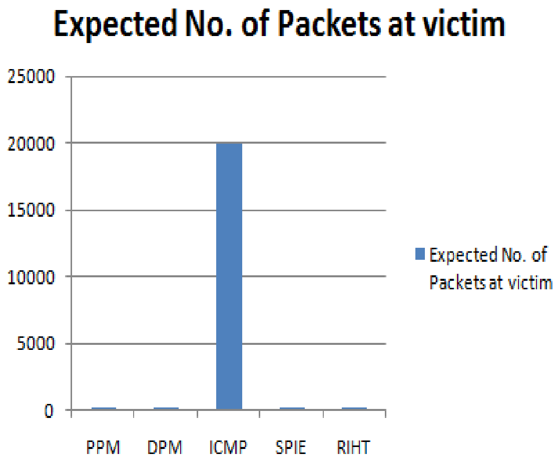

Figure6 Expected number of packets at victim (for various Traceback schemes)

6.4 Protection

A high level protection is preferred in any Traceback scheme. SPIE and RIHT requires computation in every router in the attack path for tracing back to the attacker, hence they provide less protection [15]. DPM and PPM provide much protection compared to log based schemes and ITrace also produce more reliable results even if the intermediate routers are challenged.

6.5 Router involvement during Traceback

Most of the Traceback schemes rely on the fact that router will send the trace information, when the packet is moving towards victim. So it is expected that during second phase, during the reconstruction path router should not be bothered. PPM, DPM, ITrace schemes can Traceback the attacker itself. They do not require router support in Traceback. The number of routers required in SPIE and Hybrid schemes is given by

$$NR = (n-1)h, \quad \text{for SPIE} \qquad \text{------- (3)}$$

$$NR = h, \quad \text{for RIHT} \qquad \text{------- (4)}$$

Where 'n' is the number of routers connected to the router in the attack path. 'h' is the total number of hops in the attack path.

6.6 Processing Overhead

In computing, overhead is any combination of excess or indirect computation time, memory, bandwidth, or other resources that are required to attain a particular goal. These are introduced for security purposes, but also having limitation that much space or memory is required for this. Processing overhead having high value in case of SPIE and SNITCH, medium for Packet marking techniques and low for rest of the techniques

6.7 Comparison of various techniques

We can compare the existing IP Traceback schemes on the basis of some terms like accuracy memory requirement, processing overhead etc. Link testing is the basic technique which use the mechanism of sending upstream packets from the router closest to the network, the advantage of this technique is that it does not require any memory. PPM is the simplest techniques among all the marking techniques, whereas the accuracy, protection and number of attacking packets are increased in DPM and DPPM. ITrace is better technique for less number of packets, it sends an ICMP message after particular interval to find the attacker. SPIE and Hybrid techniques require single packet to find the attacker which increases their accuracy to an extent. Their comparison is shown in table2.

7. CONCLUSION

This paper presents the various mechanisms, techniques, approaches and some IP Traceback schemes to prevent DDoS attacks. IP Traceback is the part of Intrusion response mechanism. The paper reviews the Traceback schemes effect on the Network layer. Among all the techniques PPM is simplest of all techniques but has a number of drawbacks. These drawbacks can further reduced by more advanced techniques like DPPM, AAM, SNITCH, SPIE etc. With the change in time level of attack is increased, so various mechanisms and the schemes need to be highly updated. It is observed that all the Traceback schemes which are introduced time to time require more storage and processing overheads. SPIE and Hybrid schemes require single packet to Traceback the attack path, so they have less false positive rates and considered to be most efficient techniques among all. The research have been done on reflection based passive Traceback schemes. These passive schemes are considered as most effective IP Traceback scheme and best Intrusion response in the future. Various algorithms are also designed for counter such attacks. So far, not a single method or technique is considered to be ideal, but still research is done on some passive Traceback methods which may approach to an ideal technique.

Table 2:-Comparison of existing IP Traceback schemes

Traceback Schemes Metrics	**Link Testing**	**PPM**	**DPM**	**Dynamic PPM**	**ITrace**	**AAM**	**SNITCH**	**SPIE**	**Hybrid Scheme**
Router Involvement	Low	Low	Low	Low	Low	Low	Medium	High, (n-1)h required	Low(equal to no. of hops)
Number of Attacking Packets required for IP Traceback	Large number of packets required	Large	Less as compared to PPM	Large	No. of ICMP message and huge packets required(20000)	Large	Few packets required	One packet	One Packet
Bandwidth Overhead	Low	Low	Low	Low	Low	Low	Low	Low	Low
Memory Requirement	Not Required	Low	Low	Low	High	High	High	High	Low (320kb)
Protection	Low	Low	Low	High	Low	High	Medium	High	Low
Processing Overhead	High	Medium	Medium	Low	Low	Medium	High	High	Low
Ability to Trace Transformed Packets	Poor	Poor	Yes	Yes	Poor	Yes	Yes	Yes	Poor
Accuracy	Medium	Medium, large false positive rates	Good	Good	Good for less no. of packets	Medium	High	Medium, High false positive and false negative rates	High, Less false positive & false negative rates

8. REFERENCES

[1] S.M. Specht, in:, Proceedings of the International Workshop on Security in Parallel and Distributed Systems, 2004, 2004, pp. 543–550.

[2] Loukas Georgios, Oke Gulay. Protection Against Denial of Service Attacks: A Survey COMPUTER JOURNAL Volume: 53 Issue: 7. SEP 2010 . 1020-1037.

[3] L. Santhanam, A. Kumar, D.P. Agrawal, in:, J. Info. Assurance and Security 1 (2006) 79.

[4] S.O. Amen, C.S. Hong, K.Y. Kim, in:, Y.-T. Kim, M. Takano (Eds.), Management of Convergence Networks and Services, Springer Berlin Heidelberg (2006) 263.

[5] Saurabh S, SaiRam A.S Linear and Remainder Packet Marking for fast IP Traceback COSMNET, fourth international journal 2012.

[6] Belenky and N. Ansari: On Deterministic Packet Marking, Computer Networks, Vol. 51, No. 10, 2007, pp. 2677-2700

[7] H. Aljifri, M. Smets, A. Pons, Computers & Security 22 (2003) 136.

[8] Savage S, Wetherall D, Karlin A, Anderson T. Practical network support for IP Traceback. In: Proc of ACM SIGCOMM conference; 2000.

[9] Ming-Hour Yang and Ming-Chien Yang "RIHT: A Novel IP Traceback Scheme", IEEE Transactions on information forensics and security, Vol. 7, April 2012.

[10] A. Hussain, J. Heidemann, C. Papadopoulos, in:, Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, ACM, New York, NY, USA (2003) 99.

[11] M. Long, C.Wu, J. Hung, Denial of Service Attacks on Network-Based Control Systems: Impact and Mitigation, IEEE Transactions on Industrial Informatics 1 (2) (2005) 85–96.

[12] R. Mahajan, S. M. Bellovin, S. Floyd, Controlling high bandwidth aggregates in the network, ACM SIGCOMM Computer Communication Review 32 (3) (2002) 62–73.

[13] Burch H, Cheswick B. Tracing anonymous packets to their approximate source. In: Proceedings of USENIX LISA; 2000. p. 319–27.

[14] H. Burch, in:, Proceedings of the 14th USENIX Conference on System Administration, USENIX Association, Berkeley, CA, USA (2012) 319.

[15] Kaspersky. DDoS attacks in H2 2011. [serial online] 2012 Feb [cited 2013 Jun 21].

[16] M.-H. Yang, M.-C. Yang, IEEE Transactions on Information Forensics and Security 7 (2012) 789.

[17] A. C. Snoeren et al.: Single-Packet IP Traceback, IEEE/ACM Trans. Networking, Vol. 10, No. 6, Dec. 2002, pp. 721-734