IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 1, January 2015.
www.ijiset.com
ISSN 2348 – 7968

Efficient Hybrid IP Trace Back Techniques to Mobile Distributed Denial of Service Attacks

M.Sugapriya, Mrs.D.Geetha., M.Sc.,M.Phil.,MCA.,

Research Scholar in Computer Science, Pollachi-642107, Coimbatore, India

Department of PG Computer Application, Sree Saraswathi Thyagaraja College,Pollachi-642107, Coimbatore, India

.

Abstract: Today's life has been revolutionized by Internet. Future of Internet is even more promising because of emerging technologies like ubiquitous computing, context sensitive, adaptive and reconfigurable applications. Security is the most important issue concerned with Internet. Internet is exposed to threats like system diffusion, monetary fraud, theft of proprietary information, Denial of Service (DoS)/Distributed Denial of Service (DDoS) Attacks etc. The proposed system improved hybrid trace back approaches is to identify the sources of attacking traffic and path reconstruction algorithms actually reveal the identity of first router on the path. This is better approach would be to find an algorithm that reveals the identity of first router without requiring the participation of all the routers on the path. In this proposed system, we have used the real time attack and legitimate traces in order to perform the simulation of DDoS attacks. We have simulated the network topology and attach the real time traces with the topology. The impact of attack is measured in terms of metrics such as throughput and Time.

***Keywords*:–** Internet, Distributed Denial of Service Attack, throughput, network, simulation, attack traffic, legitimate traffic

1. INTRODUCTION

The Internet is the basis of number of innovative technologies like the World Wide Web, Email, P2P applications, VOIP etc. It has enabled instant access to vast and diverse resources. But, Internet is also vulnerable to number of attacks from different sources. Major categories of attacks during 2006 were viruses, insider abuse of access, unauthorized access to information, and denial of service (DoS) attack [1]. It is often much easier to disrupt the operation of a network or system than to actually gain access to a network. There are number of freely available tools on Internet, from covertly exchanged exploit programs to publicly released vulnerability assessment software, to degrade performance or even disable vital network services.

The network needs security against attackers and hackers. Network Security includes two basic securities. The first is the security of data information i.e. to protect the information from unauthorized access and loss. And the second is computer security i.e. to protect data and to thwart hackers. Here network security not only means security in a single network rather in any network or network of networks. Now need of network security has broken into two needs. One is the need of information security and other is the need of computer security. On internet or any network of an organization, thousands of important information is ex-changed daily. This information can be misused by attackers.

One of the major security problems in the current Inter-net, a denial-of-service (DoS) attack always attempts to stop the victim from serving legitimate users. Denial-of-service (DoS) and distributed-denial-of-service (DDoS) attacks cause a serious danger to Internet operation. A distributed denial-of-service (DDoS) attack is a DoS attack which relies on multiple compromised hosts in the network to attack the victim [3]. There are two types of DDoS attacks. The first type of DDoS attacks aim of attacking the victim to force it not to serve legitimate users by exploiting software and protocol vulnerabilities. The second type of DDoS attack is based on a massive volume of attack traffic, which is known as a flooding-based DDoS attack. A flooding-based DDoS attack attempts to congest the victim's network bandwidth with real-looking but unwanted data. As a result, legitimate packets cannot reach the victim due to a lack of bandwidth resource.

In distributed DoS (DDoS) attack, the attacker uses hundreds or thousands of compromised hosts, often residing on different networks, to overload and crash target system [5]. Currently, it is not possible to prevent DoS/DDoS attacks because they are based on exploiting weaknesses in the core internet protocols which are embedded in the underlying network technology.

In DoS/DDoS attack, attacker uses fake source IP addresses to make tracing and stopping of DoS difficult. This technique is called IP spoofing. This technique involves the manipulation of the source IP address in the IP header of a transmitted packet. This gives the attacker a form of anonymity. It is difficult to solve problem of IP Spoofing because of lack of security features in TCP/IP specifications. Ingress filtering, Use of cryptographic authentication , IP trace back are some of the approaches used to handle forged IP source addresses[6]. The purpose of IP traceback is to identify the true IP address of a host originating attack packets. IP trace back is vital for quickly restoring normal network functionality and preventing reoccurrences [7].

The rest of the paper is organized as follows. Section 2, gives an overview of related work. Section 3 proposed approach. In Section 4, deal performance analysis. Conclusion is presented in Section 5.

2. RELATED WORK

Flooding DoS attack poses a great threat as it generates large volume of traffic that prevents the legitimate user from accessing the service. It causes the links to be blocked and nodes to crash resulting in decreased network performance and even more sensors become useless due to depletion of energy in sending useless packets. A number of approaches have been proposed to counter the attack.

JelenaMirkovic, P. Reiher [8] proposed taxonomy of distributed denial-of-service attacks. The attack taxonomy is illustrated using both known and potential attack mechanisms. Vrizlynn L. L. Thing, Morris Sloman, and NarankerDulay [9] present a detailed study of the source code of the popular DDoS attack bots, Agobot, SDBot, RBot and Spybot to provide an in-depth understanding of the attacks in order to facilitate the design of more effective and efficient detection and mitigation techniques. Tao Peng, Christopher Leckie, KotagiriRamamohanarao [5] presented a survey of denial of service attacks and the methods that had been proposed for defense against these attacks. In this survey, they analyzed the design decisions in the Internet that have created the potential for denial of service attacks. Monika Sachdeva, Gurvinder Singh, Krishan Kumar and Kuldip Singh [1].Measured the DDoS attack’s impact on web services. Authors simulated network topology and generated legitimate web traffic. The attack traffic is generated at different strengths to measure attack impact on web services. The attack impact is measured in terms of metrics such as throughput, response time, no of active connections, no of request dropouts, ratio of average serve to request rate, percentage link utilization, and normal packet survival ratio. Authors concentrated on web application so accordingly the performance metrics are identified for measuring the impact of DDoS attacks. KetkiArora, Krishan Kumar, Monika Sachdeva [2] presented an overview on DDoS problem and major factors causing DDoS attacks. Authors discuss brief detail of most recent DDoS incidents on online organizations.

A critical look at the literature highlights the fact that although lot of work has been done towards the security of WSN however, nothing has proved to be so significant so as to be considered as best. Moreover, researchers have ignored the fact that software agents especially ants can be used as security staffers and can provide a protection against DDoS in WSN. The upcoming section aims to propose an ant-based framework that would be able to achieve already stated objectives.

A two-tier coordination approach for detecting and mitigating DDoS attacks is used. The first tier traffic filter (lst-TF) filters suspicious traffic for possible flooding. This is achieved by using proactive tests to identify and isolate the malicious traffic. The second tier traffic filter (2nd-TF), which is deployed on network routers, performs online monitoring on queue length status with RED (Random Early Detection)/Droptail mechanism for any incoming traffic . The model requires marking of every packet that comes into the router so as to be able to trace back to the source. But this incurs overhead. The decision making module can be eliminated as the functionalities that are accomplished by this module can also be achieved using the filter module.

The existing authors used congestion algorithms to detect upsurges in traffic that can give rise to DoS but this approach may apply only simplistic signatures and also requires state information to be held on the nodes which is not a feasible solution in sensors because of limited memory.Shyne and Sterne in [11, 12] uses statistical monitoring to detect upsurges in traffic of a particular type and raise alert if something unusual is detected. Here a single alert can notify about many attack packets but it requires human intervention to monitor upsurges so is inefficient.

This approach does not provide total solution as legitimate nodes refusing to pay would be denied of accessing service.

3PROPOSED APPROACH

The proposed scheme extends and leverages on existingIP traceback schemes. IP traceback allowsthe victim to infer the paths that packets from the attackershave traversed. The proposed scheme uses this informationto preferentially filter out packets that are more likely tocome from the attackers. Here first discuss where in thenetwork the filtering will actually take place.

3.1.System Model

A DDoS attack occurs; most of the traffic is dropped by the upstream routers even before it reaches the victim. In this case, nothing can be done by the victim to improve the throughput of the legitimate traffic. To mitigate the attack, proper action needs to be taken at upstream routers. Therefore, we adopt a similar system model. The protected network is connected to the wide area network (WAN) through a gateway access control device (i.e., a firewall). A set of upstream routers will form a “line of defense”, referred to as a perimeter in the sequel. The routers on the perimeter, referred to as perimeter routers, will collaboratively inspect packets going through them. For simplicity of discussion, we assume that all perimeter routers are of the same distance (referred to as perimeter radius) away from the victim2.

3.2. IP Traceback Scheme

Although the proposed scheme may leverage on any ofthe existing IP traceback schemes, inthis paper, we show how it builds on the Advanced MarkingScheme (AMS) proposed. The advantageof the AMS is that it provides faster reconstructionand higher accuracy (hence fewer false positives in identifyingattackers) than other IP traceback schemes, when thereare more than one attackers. However, it assumes that thevictim is able to obtain a map of upstream routers, which isa stronger (arguably less practical) assumption than used in other IP traceback schemes4. Our future research will studyhow our scheme works with other IP traceback techniques.AMS employs a technique similar to the Bloom filteras follows. It uses 8 independent hash functions$\{H_i\} 1 \leq i \leq 8$ to encode network edges. When a packet goesthrough an edge e and the identity of the edge is to bemarked, i will be chosen uniformly between 1 and 8, andthe mark $i|H_i(e)|$ is written into the IP header of the packet(|| representing concatenation). The reconstruction algorithmdetermines that an attacker has e on its path, if andonly if, the algorithm has received attacking packets with atleast k out of the 8 mark values$\{H_i(e)\}1 \leq i \leq 8$. The tunableparameter k is between 6 and 8; larger k results in longer"attack graph" reconstruction time but fewer false positiveswhen identifying infected edges. We view this as a variantof Bloom filter since all the edges that an attacker hastraversed can be viewed as a set, and it is represented bya bit array indexed by the values generated by these hashfunctions.

AMS is used asthe underlying IP traceback scheme. In, tracedrivensimulation is used to estimate the average number of packetsthat needs to be received by the victim in order to reconstructthe attack graph. However, results obtained throughsuch simulation do not explain howthis value changeswhenthe parameters such as the network topology and the numberof attackers vary. We derive the exact closed-form mathematicalformula for calculating a closely-related metric:the average number of marks (denoted as n_l) that needs tobe received from an attacker l hops away for the victim inorder to reconstruct the attack path from this attacker. Thismetric is more accurate since it is independent of the topologyof the network and the sending rate of other attackers.The formula for n_l is characterized by the following theorem.

3.2.1 IP Trace Back Techniques

Let q be the probability of writing a mark intothe IP header by an upstream router and r be the probabilityfor the mark to be a signaling mark. Let h be the numberof independent hash functions H_i's used and k bethe number of $H_i(e)'$s to "convict" an edge e. Then, theaverage number of packets $n_l$that needs to be received forthe victim to reconstruct a path of length l (in number ofhops) is:

$$n_l = \frac{1}{r}\int_0^\infty \left[1 - \prod_{i=0}^{l}\left(\sum_{j=k}^{h}\binom{h}{j}\left(1-e^{-\lambda_i t}\right)j_e - \lambda_e - \lambda_i t(h - j)\right)\right] dt$$

Where $\lambda_i = \frac{q(1-q)^i}{h}, i = 0,1 \dots., l$

The parameter r (the percentage of marks being signalingmarks) is set at a small number (5%) since, for the reasonof "ambiguity" explained above, packets containing signalingmarks generally cannot be *selectively filtered out* toimprove the throughput of legitimate traffic. Therefore, forour scheme to work, the majority of packets should beardata marks.

3.3IPTracebackfor Mobile IP

With the advent of wireless communications, host computers or mobiles can roam geographically and topologically, which results in change of IP address, thus affecting ongoing connections and higher layer applications. Mobile IP was developed to enable computers to maintain Internet connectivity while moving from one internet attachment point to another. Although Mobile IP can work with wired connections, it is particularly suited to wireless connections.Proposed systems consider the following two scenarios in context of Mobile IPv4. When the MN is acting as a source of DoS attack and is residing on the home network.When the MN is acting as a source of DoS attack and residing on the foreign network.

The first case is not specific to Mobile IPv4. It can be treated as a normal attack for IPv4, since the mobile node operates without mobility services, when residing on the home network. So the traffic of the MN is marked in a similar manner as proposed for a wired node. The second case is specific to Mobile IPv4. The MN uses its HoA as the source address when it sends packets to any other node in the internet. If ingress filtering is enabled on the FA then the traffic of the MN would be discarded. Since ingress filtering is an essential part of our technique as well, we propose conditional ingress filtering i.e., if the packet is not having a valid network id, the source address should be checked in the visitor list. If there is an entry for the source address, the packet should be marked with the HA address, otherwise the packet should be discarded. For marking purposes, the same Record Route field. So even if the MN is roaming among different foreign networks while flooding the victim, the victim can trace the attack's source.

It should be noted that in this process, the TTL has to be checked first, to verify the existence of first router (first FA) on the path. The marking scenario of Mobile IPv4, when reverse tunneling is used, changes to the general IPv4 marking scenario but the packet should be marked before encapsulation.

3.4 Hybrid IPTraceback

Propose a new IP trace back technique which is a variant of packet marking and is based on TTL identification. This technique was initially proposed for IPv4 networks. Different IP trace back techniques have been proposed so far. Some of them are compatible with existing infrastructure and some require modification to it, but the effectiveness of any trace back technique can be measured by the following characteristics.

- ❖ Capability of tracing any type of DoS attack.
- ❖ Minimum overhead in terms of storage requirements.
- ❖ Minimum processing requirements on the routers.
- ❖ Least complexity in path reconstruction algorithm (if any).
- ❖ Faster convergence.

This hybrid technique was proposed by taking into account all the above mentioned characteristics. The aim of all the trace back techniques is to identify the sources of attacking traffic but path reconstruction algorithms actually reveal the identity of first router on the path. A better approach would be to find an algorithm that reveals the identity of first router without requiring the participation of all the routers on the path. Since the attacker can forge any field in the IP header, he can't falsify the Time to live (TTL) field. The TTL is an 8-bit field that determines the maximum number of hops a datagram can traverse. Each router decrements the TTL value by 1, after forwarding the datagram. The problem of determining the first router on the path can be solved by using this field. The TTL field is different for different operating systems and is not universally selected, but all the packets sent by a particular operating system will have the same initial TTL value. Default TTL values for different operating systems.

We propose to create a TTL vs. operating system (OS) table and store it on the routers. The router should read the TTL value of all the packets passing through it. If the TTL value matches any entry of the table, the router should mark the packet with its identification. This router would obviously be of the subnet from which the packets originated. All the other routers on the path cannot mark the packet, since the TTL value would not match any entry of the TTL vs. OS table. There is one exception to this. Consider a packet originating with a TTL of 64. It would be marked by its subnet router. But after four hops, its TTL would be 60. Since 60 is an entry of stored table, the packet would again be marked. If this packet was sent by an attacker, trace back would lead to a subnet four hops away from the subnet from which the attack originated. To overcome this problem, we propose to use the reserved flag in IP header (there are 3 flags in IP header, 2 are used with fragmentation and one is reserved). The first router on the path should set the flag to '1' after marking the packet. All the other routers on the path should read both the TTL and reserved flag. The packet should only be marked if a match of TTL is found and the value of reserved flag is '0'. It is however not possible that a packet originating with a TTL of 255 would reach a router with its TTL set to 128 since 95% of the traffic in the internet reaches its destination before 30 hops. The storage requirements on the routers can be minimized by having only a 5 entry TTL table (since most of the values are occurring more than once).

The proposed marking scenario obviously has the first two characteristics of an effective IP trace back technique. We can trace any type of DoS attack because each and every packet is marked by its subnet router. It is possible to trace DoS attacks which require only a single packet, which may not be possible with other marking techniques like PPM and iTrace.

The second challenge is obviously to store the marking information. The question arises where to store the marking information in the IP header. Basic DPM uses the 16-bit 'Identification' field of the IP header. However, choosing Identification field may not be a good idea because it is used for fragmentation purposes. Fragmented traffic constitutes between 0.25% and 0.5% of the total IP traffic [4]. Though the amount of fragmented traffic is small, it does exist and for the worst case scenario, Identification field should be reserved only for fragmentation purposes. Carrying marking information in outbound packets (iTrace) would obviously increase router and network overhead and would require a new and complex protocol to be implemented as well.

We propose to use the Record Route (RR) optional field in the IPv4 header. The IP address of the router would be stored in the first 4 bytes of route data in RR field. Thus the router appends the marking information with the packets. If the RR field is already present, the router should overwrite the first 4 bytes of route data in it. Thus even if the attacker forges the RR field with wrong IP addresses or unnecessary data, it would still be overwritten with the true IP address of the router. The minimum required length of RR field is 7 bytes (4 bytes for route data, 1 byte for option type code, 1 byte for option length and 1 byte for pointer into the route data). The remaining space in the optional field can be used for other options like 'Strict Source Route', 'Loose Source Route', 'Stream Identifier' etc, if required.

3.5Hybrid IP Traceback Implementation

The goal of all the traceback techniques is to identify the sources of attacking traffic, but the reconstruction of an attack path actually reveals the identity of the first router on the path. A better approach would be to find an algorithm that reveals the identity of first router without requiring the participation of all the routers on the path.

Since the attacker can forge any field in the IP header, he can't falsify the Time to live (TTL) field. The TTL is an 8-bit field that determines the maximum number of hops a datagram can traverse. Each router decrements the TTL value by 1, after forwarding the datagram. The problem of determining the first router on the path can be solved by using this field.

The problem of source address spoofing can be solved by a technique called Ingress Filtering, in which the router discards the incoming packets with invalid source IP address. A serious limitation of this technique arises when the attacker forges the address to the one that belongs to the same network as the attacker's host. Ingress filtering is commonly done at the border router. So this technique is not effective for internal attacks.

We propose Egress Filtering at the subnet router, in which the router discards the outgoing packets with illegitimate source IP address. The legitimacy of source IP address can be checked from the network id part of the 32-bit IP address. An effective IP trace back technique can result by combining this filtering technique with the proposed packet marking (based on TTL identification) technique, and thus the name 'Hybrid'. The algorithm for this hybrid technique. The packet is first checked for spoofing and is discarded if the source address is forged (doesn't have a valid network id). If the source address has a valid network id, the packet is marked with router's identity. It should be noted that spoofing attacks from the same subnet cannot be stopped because the router is checking only the network id of the IP address. This hybrid technique is significantly different from the basic DPM. The basic DPM needs an address construction algorithm since the 32-bit IP address is divided into two 16-bit IP addresses which are stored in alternate packets. This technique however doesn't require any address reconstruction algorithm. Also, the Identification field is retained for fragmentation purposes. This technique doesn't require a path reconstruction algorithm since only the first router on the path is participating in marking process. It provides faster convergence as well, since a single packet can provide the trace back capability at the victim side. As far as DDoS attacks are concerned, this technique can prevent reflector DDoS attacks; since the slave zombies cannot send spoofed packets to reflectors (spoofed packets would be discarded). This technique however can trace the direct DDoS attacks till slave zombies only. Once the slave zombies are identified, suitable measures can be taken to prevent reoccurrences of DDoS attacks using these compromised machines.

Pseudo codehybrid IP traceback algorithm

```
#Definenet_id
#Definerouter_ip
Struct datagram
{
Main()
{
    Datagram D;
    Initttl_table[18]
    For (each D)
    {
        For i=0:17
        {
            If D.ttl—table[i]
            {
                Y=compute_netid(D.source_address)
                If y==net_id
                {
                    Write router_i into D.record_route
                    Forward(D)
                }
                Elese if y!=net_id
                Discard(D)
            }
            Else if D.ttl!-table[i]
            Forward(D)
} } }
```

Consider the scenario depicted in figure 8.1. If the MN acted as a source of DoS attack when residing on the home network, its traffic would be marked by the HA with the HA address. In this case there is no need to mark the packets again, if the MN moved to a foreign network after some time. The packet is already marked with the HA address. This is where the importance of setting the reserved flag to '1' comes. The packet is marked only if reserved flag is '0', meeting other conditions. The complete marking process, in case of hybrid wired / mobile IP networks, follows the following sequence of actions at the router / HA / FA:

Step 1. Check the TTL value in the IP header. If a match of TTL value is found with the stored table, the packet is valid for marking. If match not found, simply forward the packet.

Step 2. Check the Reserved Flag. If its value is '1', forward the packet without marking. If its value is '0', the packet is valid for marking.

Step 3. Check the source IP address. If it is having a valid network id, mark the packet. That is, write IP address of router / HA into first four bytes of route data in Record Route (RR) field.

Step 4. If the source address is not having a valid network id, check the IP address in visitor list (on FA). If a match found, retrieve the corresponding HA address from visitor list. Then, write HA address into first four bytes of route data in RR field.

Step 5. If source IP address is not having a valid network id and there is no entry of the source IP address in the visitor list, simply discard the packet.

It should be noted that the marking scenario of Mobile IPv4, when reverse tunneling is used, changes to the general IPv4 marking scenario but the packet should be marked before encapsulation.

4 EXPERIMENTAL RESULS

This hybrid technique was simulated in the Network Simulator (ns-2.34) at network layer to measure the delay for marked traffic as compared to normal (unmarked) traffic. The simulator was running on an Intel based machine having 1.7 GHz processor and 512 MB of main memory. The internal files of ns-2.34 were modified to incorporate packet marking in it. The modified internal files along with the Tcl code are given in Appendix A. Appendix B contains a detailed tutorial on ns-2. The simulated scenario and simulated topology.

The size of the topology doesn't matter because all the delay is incurred at the first router only. Traffic originated from node 7 and was destined for node 3. For this traffic, node 0 acts as the first router on the path. Traffic consisted of TCP packets of 1040 bytes carrying FTP data. The comparison between marked and normal traffic. The additional time taken by marked traffic is just 0.8 milliseconds. Similar delay is also observed for traffic from node 13 to node 8 for which node 12 acts as the first router on the path.

5.PERFORMANCE ANALYSES

Common performance metrics to measure the impact of DDoS attacks, used by various researchers are throughput without attack and with attack. Some others use the percentage of failed transactions as a metric in their work. According to various network performance metrics are affected when DDoS attacks are launched. In current work, our focus is on performing the simulation of

DDoS attack using real legitimate and attack datasets and then measure the effect of attack using following metrics:

PDR is the ratio of the number of data packets received by the destination node to the number of data packets sent by the source mobile node. It can be evaluated in terms of percentage (%). This parameter is also called "success rate of the protocols", and is described as follows:

$$PDR = \left(\frac{SendPacketno}{Receivepacketno}\right) \times 100$$

Throughput is the average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node.

$$X = \frac{C}{T}$$

Where X is the throughput, C is the number of requests that are accomplished by the system, and T denotes the total time of system observation.

Table 5.1: Impact of Throughput

Techniques	4	8	12	16	20	24
Attack Case	11	17	32	41	52	58
IDS Case	10	16	22	31	38	42
Normal Case	8	9	11	15	18	21

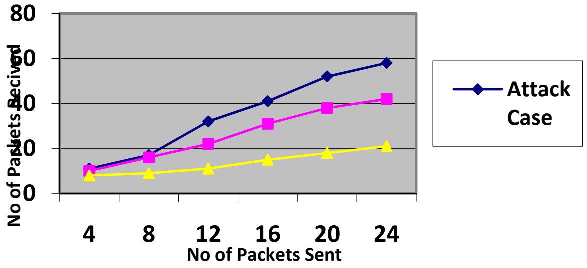

Figure 5.1 Compare throughput under attacks

Table 5.2: Time Vs No of Packets

Techniques	4.00	8.00	12.00	16.00	20.00	24.00
Attack Case	65	142	189	210	234	258
IDS Case	61	108	145	164	182	201
Normal Case	48	53	87	94	105	114

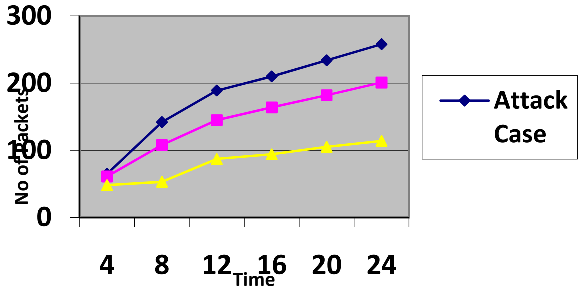

Fig 5.2 Compare throughput with different simulation Time

Table 5.3: No of Flows Vs Delay

Techniques	4	8	12	16	20	24
Attack Case	4.5	8.1	10	10.7	12.6	14.9
IDS Case	2.1	4.3	3.8	6.2	5.8	5.6
Normal Case	1.2	2	1.8	2.8	2.1	2.8

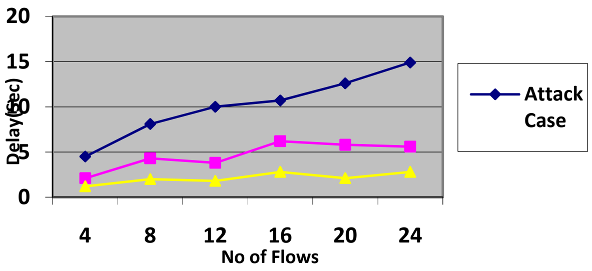

Figure 5.3 Impact of Average End to End Delay

6. CONCLUSION AND FUTURE WORK

The development of IP trace back techniques is motivated by different DoS attacks in recent years. With the development of Mobile IP, more complex DoS attacks can be launched. However, IP trace back is the first step in identifying the attacker behind the attacks. The effectiveness of any trace back technique depends primarily on its overhead, convergence and the ability to trace any type of DoS attack. The hybrid technique presented here is capable of tracing any type of DoS attack because we can trace even a single packet. Today there is a need of practical implementation of an effective technique so that IP trace back could be carried out in real time across the internet. Future work will fold in more topology information and vulnerability information gleaned from automated scanning and mapping tools. When the nodes know more topology information of the global Internet, it can utilize more intelligent gossip strategy to reduce the information sharing overhead while trying to detect attacks with speed. Armed with these more sophisticated methods, our approach can defend attacks more efficiently. We are investigating several important questions that still need to be addressed. These include the consensus algorithm and optimal gossip period. We also plan to validate this scheme by running them on real attack data sets.

.

REFERENCES

[1] Lawrence A. Gordon, Martin P. Loeb, WilliamLucyshyn and Robert Richardson, CSI/FBI ComputerCrime and Security Survey, 2006.

[2] Computer Emergency Response Team. CERT advisoryCA-1999- 17 denial of service tools.http://www.cert.org/advisories/CA-1999-17.html.

[3] Yonghua You, "A Defense Framework for Flooding-basedDDoS Attacks", Master's Thesis, Queen's University Kingston, Ontario, Canada August 2007.

[4] D.Moore, G. M. Voelker and S. Savage, "Inferring Internet Denial of Service activity" ACM Trans.Comput.Syst., vol. 24, no. 2, pp. 115-139, May2006.

[5] Matthew Hutchinson, "Study of Denial of Service", MS Dissertation, Queen's University of Belfast,Aug 2003.

[6] J. Li, J. Mirkovic, M. Wang, P. Reiher and L. Zhang, "SAVE: Source Address Validity EnforcementProtocol", in Proc IEEE INFOCOM, 2002, pp 1557-1566.

[7] S.C. Lee and C. Shields, "Tracing the Source of Network Attack: A Technical, Legal and SocietalProblem", Proc. 2001, IEEE Workshop on Information Assurance and Security, IEEE Press, 2001, pp. 239-246.

[8] J. Mirkovic and P. Reiher."A Taxonomy of DDoS Attack and DDoS Defense Mechanisms", ACM SIGCOMM Computer Communications Review, Volume 34, Issue 2, pp. 39-53, April, 2004.

[9] Vrizlynn L. L. Thing, Morris Sloman, and NarankerDulay, "A Survey of Bots Used for Distributed Denial of Service Attacks", IFIP International Federation for Information Processing, Volume 232, New Approaches for Security, Privacy and Trust in Complex Environments, eds. Venter, H., Eloff, M., Labuschagne, L., Eloff, J., von Solms, R., (Boston: Springer), pp. 229-240, 2007.

[10] Monika Sachdeva, Gurvinder Singh, Krishan Kumar, and Kuldip Singh, "DDoS Incidents and their Impact: A Review", The Interna-tional Arab Journal of Information Technology, Vol. 7, No. 1, January 2010.

[11] S. Shyne, A. Hovak, and J. Riolo, "Using Active Networking To Thwart Distributed Denial Of Service Attacks," in Proceedings of IEEE Aerospace Conference, Vol. 3, 2001, pp: 1103-1108

[12] D. Sterne, R. Balupari, W. La Cholter and A. Purtell, "Active Network Based DDoS Defense", in Proceedings of DARPA Active Networks Conference and Exposition, San Francisco, CA, 2002, pp. 193–203.

13] Dr. James H. Yu and Tom K. Le, "Internet and Network Security", Journal of Industrial Technology, Volume 17, Number 1, January 2001.

[14] J. Mirkovic, S. Dietrich, D. Dittrich and P. Reiher, Internet Denial of Service, Prentice Hall, December 2004.

[15] P. Owezarski, "On the impact of DoS attacks on Internet traffic characteristics and QoS", 14th IEEE International Conference and Computer Communications and Networks (ICCCN'2005), San Diego, CA, USA, 17-19 October 2005.

[16] CharalamposPatrikakis, MichalisMasikos, and Olga Zouraraki, "Distributed Denial of Service Attacks", The Internet Protocol Jour-nal, Vol.7, No. 4, 2004.