An Enhanced FDPM Method for Network IP Attacks

S.Gavaskar[(1)], Dr.E.Ramaraj[(2)]
Research Scholar [(1)], Technology Adviser [(2)]
[(1) (2)] Madurai Kamaraj University,
Madurai.

Abstract:

Internet Protocol trace back is the technology to control Internet frauds.Currently a large number of DistributedDenial of Service attack incidents make people aware ofthe importance of the IP trace back technique. IP trace back is theability to trace the IP packets to their origins. It provides asecurity system with the ability to find the original sources of theattacking IP packets. IP trace back mechanisms have beenresearched for years, aiming at finding the sources of IP packetsquickly and precisely. In this paper, we discuss and practical IP trace back system called Flexible Deterministic Packet Marking which provides a defense system for IP packets and denial service attacks that traverse through the network.

Keyword:
FDPM,IP, DDOS

I. Introduction:

a) DDOS:

Denial of service is accomplished technologically. The primary goal of an attack is to deny the victim(s) access to a particular resource. It is an explicit attempt by attackers to prevent legitimate users of a computer-related service from using that service. But, as any information and network security issue, combating denial of service is primarily an exercise in risk management. To mitigate the risk, we need to make business decisions as well as technical decisions. Managing the risks posed by denial of service requires a multi-pronged approach:

- Design the business for survivability. Have business continuity provisions in place.
- Design the network for survivability. Take steps that help to ensure that critical services continue in spite of attacks or failures.

Be a good citizen. The potential to be attacked depends on the security of other sites and vice versa. The threat to network is directly proportional to the extent that other Internet users, including home users, adhere to good practices. Conversely, the threat that your network represents to others is directly proportional to the extent that your organization adheres to good practices. Denial of service may be indistinguishable from a heavy (but otherwise legitimate) load on your network. For example the victim might be flooded with legitimate connections to his web site as a result of a major news event.

b) IP

Internet **P**rotocol Address or IP Address is an unique address that computing devices use to identify itself and communicate with other devices in the Internet Protocol network. Any device connected to the IP network must have a unique IP address within its network. An IP address is like a street address or telephone number in that it is used to uniquely identify a network device to deliver mail message or call a website.

The traditional IP Addresses (IPv4) uses a 32-bit number to represent an IP address and it defines both network and host address. Due to IPv4 addresses running out, a new version of the IP protocol (IPv6) has been invented to offer virtually limitless number of unique addresses. An IP address is written in "dotted decimal" notation, which is 4 sets of numbers separated by period each set representing 8-bit number ranging from (0-255). An example of IPv4 address is 216.3.128.12, which is the IP address assigned to topwebhosts.org.

An IPv4 address is divided into two parts: network and host address. The network address determines how many of the 32 bits are used for the network address, and remaining bits for the host address. The host address can further divided into sub network and host number.

c) IP spoofing

IP Spoofing is one of the major tools used by hackers in the internet to mount denial of service attacks. In such attacks the attackers duplicate the source IP of packets that are used in the attack. Instead of carrying the original source IP of the machine the packet came from, it contains an arbitrary IP address which is selected either random fashion or particularly. The ease with which such attacks are generated made them very popular. There are at least four thousand such attacks happening every week in the Internet. In a spoofing attack, the intruder sends messages to a computer indicating that the message has come from a trusted system. To be successful, the intruder must first determine the IP address of a trusted system, and then modify the packet headers to that it appears that the packets are coming from the trusted system.

c) DPM

The basic idea of ADPM is to transmit the *unary* representationof the *maximum* price seen by a packet as ittraverses the network, appropriate for max-min flow control.
Each packet that arrives at a router contains a threshold value,as provided by the IPid field. Each packet asks each routerit encounters the same question: is your price greater thanmy threshold? The router answers "yes" or "no", providingunary encoding of the price that is robust to packet loss, or to a reordering of the packet arrivals at the receiver.

In what follows, it is convenient to assume that prices havebeen mapped to lie in the unit interval [0*;* 1]; from now on,we will use the term "price" to refer to the mapped value.Similarly, a mapping f is assumed, that maps IP id values to threshold values in [0*;* 1]. Following the terminology of [7],$i \leftarrow f(v)$ will be called the probe type of the packet.

Implementation details behind the above assumptions areexplained in Section V.When a router with link price p forwards a packet of probe type i, it marks the packet if $p > i$, and leaves the markunchanged otherwise. At the receiver, the mark of a packet of probe type I will be set if any router on the path had a price Exceeding i. Decoding is simple. The receiver maintains acurrent estimate of the price, p. If it sees a marked packet of probe type I with $i>p$ or an unmarked packet of probe type I with $i<p$, then it sets p to i.
In this algorithm, the interpretation of each mark is independent
of the values of other marks. In contrast, with binarysignalling [7], a price change from 3 (011) to 4 (100) couldyield any price estimate from 000 to 111, depending on theorder in which bits are signalled.

While a numerous trace back schemes exist, FDPM provides distinct features to trace the source of IP packets and can obtain better tracing capability than others. In particular, FDPM adopts a flexible mark length strategy to make it compatible to different network environments; it also adaptively changes its marking rate respective to the load of the participating router by a flexible flow-based marking scheme

Earlier works:
We have proposed two innovative ideas in our earlier works for avoid the attacks based on IP address**.** The first one based on SYN flooding attacks.

We determine *valid SYN packets* as the pure SYN and SYN/ACK packets, and *valid FIN packets* as the FIN and RST packets that close the TCP connections which either complete the three-way handshake or have a *valid SYN packet* in the same traffic direction before this packet. Then there are more *valid SYN packets* than *valid FIN packets* under SYN flooding.

When we receive a SYN or SYN/ACK packet, the counter of *valid SYN packets* is increased. We use this concept as our research. A filter is a simple space-efficient data structure for representing a set in order to support counting process. When we receive a FIN or RST packet, the item of its *4-tuple* (source &destination IP and ports Address) is also extracted and queried from the filter. If this item is in the filter, the counter of *valid FIN packets* is increased, and this item is deleted from the counting filter. If not, this packet is not a *valid FIN packet*, and nothing is needed. Our Three counters algorithm scheme

utilizes the change of the discrepancy between *valid SYN and FIN packets*.

3.1.1 Efficient Router

An efficient router can detect the SYN flood attacks. Every network should have one router in terms we have to design our network. Ever entry of packet should be monitor then check the IP address if it's legitimate then only it can allow to networks. If there is any IP spoofing technique happen in the IP header that packet will restricted. Using router we can detect the SYN flood attacks because SYN flood attacks happen after the packets came into the system by the unauthorized user. If we use router in every networks the earlier stage itself spoofed packets detected, it's very easy to solve the problem compare with after happen the attack.

3.2. Three Counters Algorithm:

In SYN floods, attacker would send a quick barrage of SYN packets from IP addresses (often spoofed) that will not generate replies to the SYN/ACKs. To remain effective, attacker needs to send new barrages of bogus connection requests frequently. Most of the SYN flooding packets would not be retransmitted. On the other hand, If a legitimate client's SYN packet is lost, it would retransmit the SYN packet several times before giving up. Our mitigation scheme utilizes the characteristic of SYN floods and client's persistence. We use three counting filters [1] to record related information:

• C-1: to record the first SYN packets of each connection;

• C-2: to record the SYN packets, whose connections have completed the three-way handshake?

• C-3: to record the other SYN packets.

The mitigation scheme starts working once detecting SYN floods. If a SYN packet is received, its *4-tuple* is extracted as an item and queried from the three Cs. The results are:

1) The item is not in any of the three Cs. This TCP connection is new, and then we drop this SYN packet and insert the item to C-1;

2) The item is in C-1. This is the next SYN packet. We pass it and move the item from C-1 to C-3;

3) The item is in C-2. We pass the packet;

4) The item is in C-3. We move the packet with a certain conditions *p*. We insert the item to C-3 and obtain the number, *n*, of this item in C-3. Let $p = 1/n$, then p is smaller as the increasing of n. If a ACK packet is received, its *4-tuple* is also extracted as an item and queried from the three Cs. The result is used as follows:

1) The item is not in any of the three Cs or in C-We drop this packet;

2) The item is in C-2. We pass this packet;

3) The item is in C-3. This TCP connection is completed. Then we pass this packet and move the item from C-3 to C-2. If the attacker uses different *4-tuple* of SYN packets, these SYN packets would be classified as the first SYN packets of each connection, and would be dropped. If some SYN packets with the same *4-tuple* are used in the attack, a small portion of SYN flooding packets would reach the victim (such as the second SYN packets). If these SYN packets are retransmitted again and again, they are dropped with higher and higher probability. Therefore, our mitigation scheme can drop most of SYN flooding packets and protect the victim.

Second one is based on compression scheme here is the discussion.The main objective of IP compression is to avoid the overhead, which provides the bandwidth utilization. The IP header compression work initiated ten years ago but still there is some drawback and problem persists. For handling the packet transformation in effective manner we are moving to IPv6 but the header size will increase in IPv6. To increase the bandwidth utilizations, avoid the network traffic, congestion, collision, we go for compression technique. Basically compression used for minimize the size of file into half. For example if the original file size is 100mb after compression it will reduced into 50mb. While decompress your file we have to get original information without lose anything. Basic idea behind in this is remove the unwanted data's or information's.

In our work we incorporate the compression technique into TCP/IP packets. While data transfer two end systems will make the communication between these two end points the session will allocated for temporarily. Both systems has an unique IP

address for identifying the system in network, using this IP address only communication will established. After establishing the end to end point connection the corresponding application will take charge to transactions. Application will identified using the port number. While continues data transfer some information will repeatedly send to the receiving end namely IP address of sender and receiver, port address of sender and receiver. To avoid this kind of information we go for compression technique. Most of the data compression algorithms have been developed and programmed in the traditional way. None of the previous algorithms has been evolved. The use of Evolutionary Computation has not been thoroughly investigated thus far. Researchers in the compression field tend to develop algorithms that work with specific types of data, taking the advantage of any available knowledge about the data. It is difficult to find a universal compression algorithm that performs well on any data type

Algorithm:

- Split the packet header with data
- Applied the GRS compression algorithm
- Apply the cryptography technique
- Transmit the data
- Decryption
- Decompression
- Original information.

First take the original packet then split the packet header with the data. Whenever the data transmission happen that time 4tuple information are common for throughout the data transfer. If we compress these things we can minimize the many space due to that we can utilize bandwidth in optimized manner.
The next step is applying the GRS algorithm which is the novel algorithm what we designed for our implementation. The concept behind in this is group of IP address considered as a single no which is taken as host identification no likewise we have to interchange into 4tuple's. For example 192.168.30.2 this is a one host IP address. This will converted into like this. 2. We have to remember one thing after establishing the connection only the stream of packet will change into like this.

The next step is applying the cryptography technique. There are variety of techniques and complex methods available but in this scenario we couldn't use the complex technique because we going to apply in packet header. If we use complex technique, for encryption and decryption will take too much time. We have to use simple functions; in our implementation we used transformation function as method. It just modify the one value into another form using add or multiply that value into original no. for example the previous 2 will converted onto 6 adding 4 with 2 . The final thing is we have to send the key value for decryption. Key value will add into encrypted value for easy identification similar to the format of IP address 6.4 is the final value that will send to the destination machine likewise all 4tuple's. Again the decryption will happen in reverse manner.

Proposed Method (EFDPM):

Enhanced Flexible Deterministic Packet Marking (EFDPM) utilizes many bits in the IP header that has a flexiblelength. When an IP packet enters the protectednetwork, it will be marked by the interface close to thesource of the packet on an edge ingress router. Thesource IP addresses are stored in the marking fields.
The mark will not be changed when the packettraverses the network. At any point within the network, the source IP addresses can be assembled whennecessary. Here we give a short review of the initialversion of FDPM.
Because the maximum length of mark is 25 bits, atleast 2 packets are needed to carry a 32-bit source IPaddress. Each packet holding the mark will be used toreconstruct the source IP address at any victim endwithin the network. A segment number is also assigned
to the mark, because when reconstructing the packet,the segment order of the source IP address bits must beknown. After all the segments corresponding to thesame ingress address have arrived to the destination, the source IP address of the packets can be reconstructed. In order to keep a track on a set of IPpackets that are used for reconstruction, the identitiesshown the packets come from the same source must begiven. A hash of the

ingress address is kept in the mark, known as the digest. This digest will always remain thesame for a FDPM interface from which the packetsenter the network. It provides the victim end the abilityto recognize which packets being analyzed are from asame source, although the digest itself cannot tell thereal address. Even if the participating router is Compromised by attackers, this scheme will not be affected becausethe packets with irrelevant digest will be discardedduring the reconstruction process.The packet processing consumes resources such asmemory and computing capacity of a participatingrouter. Therefore, it is possible for a router to beoverloaded when there are a large number of arrivalpackets. In this paper we are using the FDPM technique to avoid the IP spoofing. We are going to improve the FDPM concept with security mechanism. In TCP/IP packet header there will be a space available for future enhancement. In that space we can implement the FDPM marking procedure with cryptic technique. To enhance the additional security we are introducing the cryptography technique. We discussed the algorithmic procedure for routers because in internet router play a vital role. If we determine the restriction procedure in router itself, we can eliminate the forged IP packets there itself.

Routing Algorithm:

If (router R >Limit)
Reject the packets
Activate mitigate schemes
Else if (router R<limit)
Enable the FDPM marking and security procedure
InterfaceI, in network N, Router R;
For each attacking packetAP;
Check the number of Packet NP;
If (NP == 0, means no Attack)
Add new packets and set NP = 1;
Elseif (NP<limit to Max)
Increment NP packets
Else
Suspected attacks
End if

For addition security scheme we used simple algorithm ceaser chiper. It is one of the very basic encryption schemes in cryptographic technique. Why we have chosen this algorithm? For testing this is very easy algorithm to implement. According to the user complexity and need we can use some other algorithm to improve the high level security. Even we can also use the two tire three tire security levels also but while improving the complexity of algorithm processing will get slow. We itself giving or open the door for congestion in network path.
While choosing the security algorithm we have to consider two important things, one is time complexity for decrypting and another one is complexity of the algorithm. These two things decide the congestion ratio if these two things increases, network traffic can increase up to some ratio.

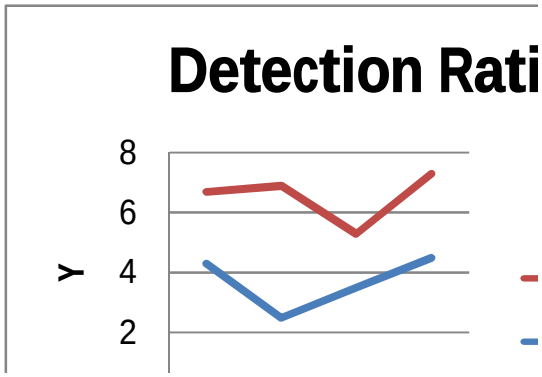
This is kind of preventing mechanism for resolve the IP problems. This is a prevention mechanism for IP spoofing problems in router level itself. While comparing with the DPM it will produce the optimized results and also it will act as flow control method for congestion events.

Result discussion:

This paper gives a most valuable solution compare with the TPM technique. This work simulated in network simulator software. if we work with the real time implementation it will lead more expensive and tough due to that we will carried out an simulation . This simulation gives us satisfactory result. We hope it will give better solution while implementing real time also. The following diagram shows the efficiency of the FDPM technique:

No packets	DPM	EFDPM(proposed method)
100	78	84
500	67	89
2000	77	78

Table: 1
Among sample packets how far both algorithm will detect the attacked packets that will depicts as table and performance graph



Conclusion:

There are varieties of methods available for trace back systems. Every method has its own drawback and features. In this paper we discussed and provided an efficient EFDPM trace back system for packets. Compare with DPM techniques EFDPM gives a better result for IP Trace backs. We hope this method will give a better result in our society.

Reference

[1] B. Al-Duwairi, and M. Govindarasu, "Novel Hybrid Schemes Employing Packet Marking and Logging for IP Traceback" , IEEE Transactions on Parallel and Distributed Systems, V ol.17, No.5, 2006, pp.403-418.

[2] H. Aljifri, "IP Traceback: A New Denial-of-Service Deterrent?", IEEE Security & Privacy, Vol.1, No.3, 2003, pp.24-31.

[3] Y. Xiang, and W. Zhou, "An Active Distributed Defense System to Protect Web Applications from DDoS Attacks", Proc. of the 6th International Conference on Information Integration and Web Based Application & Services (iiWAS2004).

[4] A. Belenky and N. Ansari, .On IP traceback,. *IEEE Communications Magazine*, vol. 41, no. 7, July 2003, to appear.

[5] H.-K. Ryu and S. Chong, "Deterministic packet marking for max-min flow control," *IEEE Commun. Lett.*, vol. 9, pp. 856–858, Sept. 2005.

[6] R. W. Thommes and M. J. Coates, "Deterministic packet marking for time-varying congestion price estimation," *IEEE/ACM Trans. Networking*, vol. 14, no. 3, pp. 592–602, June 2006.

[7] K. Ramakrishnan, S. Floyd, and D. Black, "The addition of explicit congestion notification (ECN) to IP," IETF, RFC 3168, Sept. 2001.

[8] M. Adler, J.-Y. Cai, J. K. Shapiro, and D. Towsley, "Estimation of congestion price using probabilistic packet marking," in *Proc. IEEE INFOCOM*, 2003, pp. 2068–2078.

[9] S. Athuraliya, V. H. Li, S. H. Low, and Q. Yin, "REM: active queue management," *IEEE Network*, vol. 15, pp. 48–53, May/June 2001.

[10] N. G. Duffield and M. Grossglauser, "Trajectory sampling for direct traffic observation", ACM SIGCOMM 2000, pp.271-282.