ISSN: 2348 - 2117

International Journal of Engineering Technology and Computer Research (IJETCR)
Available Online at www.ijetcr.org
Volume 3; Issue 1; Page No. 34-38

Identification of Real Source of DDoS Attack by FDPM in IP Traceback System

Prashil S. Waghmare

PG student, Sinhgad College of Engineering, Vadgaon, Pune University, Maharashtra, India.

prashil.waghmare14@gmail.com

ABSTRACT
Internet Protocol (IP) traceback is the technology to givesecurity to internet and secure from the internet crime. IP traceback system is also called as Flexible Deterministic Packet Marking (FDPM) which builds such a defense mechanism which has ability to find out real source of attacks on packets that traverse through the network. While a number of other trace back schemes exist, FDPM provides innovative features to trace the source of IP attack and can obtain better tracing capability than others. In this paper we are concentrating on how packet marking is done and how we trace the source of attack so firstly the whole message is splits into number of packets. Then all Packets are marked on marker side according to marking Scheme algorithm. If intruder intrudes and gets access of the packets and modify them then with the help of reconstructor we reconstruct the file at the receivers end. Finally receiver reconstructs the file and gets IP address of sender and hacker Using IP spoofing Technique, MAC address and Location of an intruder also.

Keywords: IP traceback; packet marking; Reconstructor; MACaddress; Intruder.

INTRODUCTION:

Now a day, protection is essential part of our daily life and it becomes easier because many factors working against the intruders, hackers, criminal. Very popular security system i.e. alarm and camera systems protect secure places like banks. Network security is to protect data during their transmission. While transmitting the message between two users, the unauthorized user intercepts the message, alters its contents to add or delete entries, and then forwards the message to destination user. [3] For finding the real source of IP packets we have to use an IP traceback system. In this paper we are presenting an IP traceback system, Flexible Deterministic Packet Marking (FDPM). FDPM belongs to the packet marking family of IP traceback system. There are two main characteristics of FDPM: first it uses the flexible mark length strategy; second it can also change its marking rate according to the routers which are participating in the transmission by flexible flow based marking scheme. [1]. FDPM is very efficient for finding the real source of attack than the other traceback systems and with the low resource requirement on routers.

II. PREVIOUS WORK ON IP TRACEBACK SYSTEM

There are currently five IP traceback schemes are present: link testing, messaging, logging, packet marking, and hybrid schemes. The working of the link testing scheme is to start from the victim and trace the attack to upstream links, and then it determines the source of attack. The main drawback of this scheme is it consumes huge amount of resources, and causes DoS when the number of sources increases. With thr help of routers Messaging schemes sends ICMP messages from the starting routers to destinations. The main disadvantage of messaging schemes is huge amount of traffic would possible. Logging schemes include probabilistic sampling and storing transformed information [1]. The main disadvantage of logging schemes is that they heavily overload the participating routers by requiring them to log information about every packet passing by, although it is claimed that it needs only a single packet to find its origin. Packet marking schemes insert traceback data into an IP packet header to mark the packet on its way through the various routers from the attack source to the destination; then the marks in the packets can be used to deduce the sources of packets or the paths of the traffic. As this method overwrites some rarely used fields in IP header, it does not require modification of the current Internet infrastructure. This property makes it a promising traceback scheme to be part of DDoS defense systems. However, the space in IP header that can be utilized is limited. Thus, the information that one packet can carry is also limited. Therefore, many challenges for this category of traceback schemes are raised. For example, the number of sources that can be traced could be limited, the number of packets required to find one

source could be large, and the load of the traceback router could be heavy. Recently, there has been also some research on hybrid schemes. In [2], a hybrid traceback scheme combining logging and packet marking is presented to achieve the small number of packets needed to trace a single source and the small amount of resources to be allocated to the participating routers. Although the hybrid schemes try to overcome the disadvantages of each traceback scheme, the complexity of such combination and the practicability of their implementation still need more research

III. FLEXIBLE DETERMINISTIC PACKET MARKING

DPM uses fixed bits in the IP header to carry mark, while FDPM [8] uses flexible length of mark. FDPM uses 8-bit TOS field, 16-bit ID field and 1-bit Reserved Flag in IP header. [2]. So the maximum length of mark is 25 bits so more than one packet is having 32 bits source IP address. So with this we required the segment number to reconstruct an IP address to its original order. After all the segments having corresponding address arrived at the reconstruction point IP address can be reconstructed.

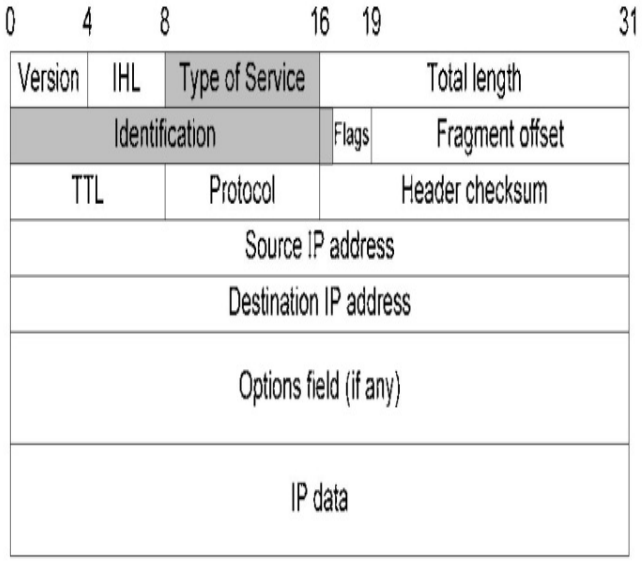

Figure 1: the IP header fields utilized in FDPM

Fig 1 shows a total of 25(8+16+1) bits.

IV. ENCODING SCHEME

Before the FDPM mark can be generated, the length of the mark must be determined based on the network protocols deployed within the network to be protected. According to different situations, the mark length could be 24 bits long at most, 19 bits at middle, and 16 bits at least. Therefore, the flexible length of the marks results in three variations of the encoding scheme, which are named as FDPM-24, FDPM-19, and FDPM-16 in the rest of this paper. FDPM encoding

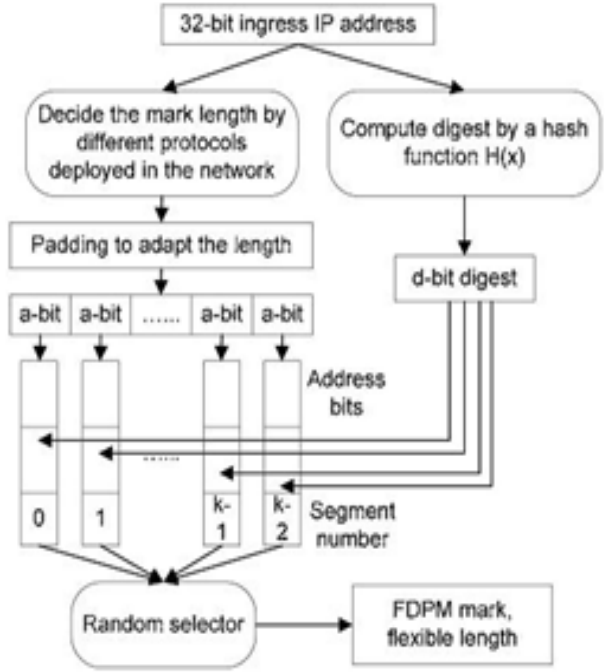

Figure 2: FDPM encoding scheme

Scheme is shown in Fig. 2. The ingress IP address is divided into k segments and stored into k IP packets. The padding is used to divide the source IP address evenly into k parts. For example, if k = 6, the source address is padded with 4 bits of 0, making it 36 bits long, then each segment will be 6 bits long. The segment number is used to arrange the address bits into a correct order. The address digest enables the reconstruction process to recognize that the packets being analyzed are from the same source. Without this part, the reconstruction process cannot identify packets coming from different sources, thus will not be able to trace multiple IP packets.

The encoding algorithm is shown in Fig. 3. In FDPM, before the encoding process begins, the length of the mark must be calculated. If the TOS field in the IP packet is not used by the protected network, the 1-bit Reserved Flag in the header is set to 0, and the length of mark is set to 24. Under other situations, the length of mark will be 19 or 16, with relevant bit(s) in TOS marked. If the network supports TOS Precedence but not TOS Priority, fourth to sixth bits of TOS are utilized for marking; and if the network supports TOS Priority but not TOS Precedence, first to third bits of TOS are utilized for marking.

```
1.  Marking process at router R, edge interface A, in network N
2.  Set the bit array Digest and Mark to 0
3.  if N does not utilize TOS
4.    Reserved_Flag:=0
5.    7th and 8th bit of TOS:=0
6.    Length_of_Mark:=24
7.  else
8.    Reserved_Flag :=1
9.    if N utilizes Differentiated Services Field or
10.   N supports Precedence and Priority
11.     7th and 8th bit of TOS:=1
12.     Length_of_Mark:=16
13.   else if N supports Precedence but not Priority
14.     7th bit of TOS:=1
15.     8th bit of TOS:=0
16.     Length_of_Mark:=19
17.   else if N support Priority but not Precedence
18.     7th bit of TOS:=0
19.     8th bit of TOS:=1
20.     Length_of_Mark:=19
21. Decide the lengths of each part in the mark
22. Digest:=Hash(A)
23. for i=0 to k-1
24.   Mark[i].Digest:=Digest
25.   Mark[i].Segment_number:=i
26.   Mark[i].Address_bit:=A[i]
27. for each incoming packet p passing the encoding router
28.   j:=random integer from 0 to k-1
29.   write Mark[j] into p.Mark
```

Figure 3: Algorithm of FDPM encoding scheme

V. RECONSTRUCTION SCHEME

The reconstruction process includes two steps: mark recognition and address recovery. When each packet arrives at the point that requires reconstruction, it is first put into a cache because, in some cases, the reconstruction processing speed is slower than the arrival speed of the incoming packets. The cache can also output the packets to another processing unit, by this design the reconstruction methods can be applied in a parallel mode (e.g., if the router has multicore architecture). This will be left as our future work. The mark recognition step is the reverse process of the encoding process. By reading the control fields in the mark, the length of the mark and which fields in the IP header store the mark can be recognized. If the RF is 0, the mark length is 24 (both TOS and ID are deployed). If the RF is 1, according to different protocols of TOS used, the mark length is 16 or 19. The second step, address recovery, analyzes the mark and stores it in a recovery table. It is a linked-list table; the number of rows is a variable, and the number of columns in the table is k, representing the number of segments used to carry the source address in the packets. Here, the segment number is used to correlate the data into the correct order.The row of the table means the entry; usually each digest owns one entry (source IP address).

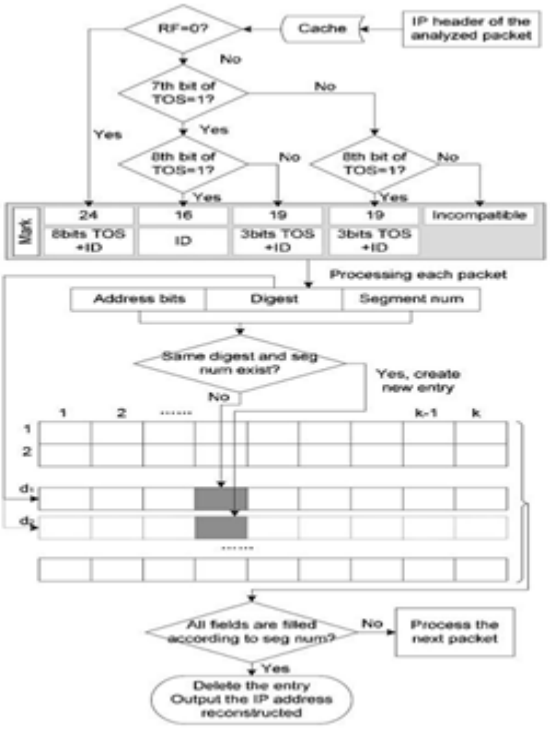

Figure 4: FDPM reconstruction scheme

However, different source IP addresses may have the same digest because the digest is a hash of the source IP address, and is shorter than an IP address. In this case, hash collision is unavoidable. When the hash collision occurs, more than one entry may be created in order to keep as much information as possible. The advantage of this design is that it can reconstruct all possible sources but the disadvantage is it also brings possible irrelevant information. Compared with DPM, our reconstruction process is compatible with different protocols and will not lose any sources even when hash collision occurs. When all fields in one entry are filled according to the segment number, this source IP address is reconstructed and the entry in the recovery table is then deleted. To simplify the description, we present the algorithm of FDPM reconstruction scheme as shown in Fig. 5.

```
1.  Reconstruction at victim V, in network N
2.  for each coming packet p passing the reconstruction point
3.    mark recognition (length and fields)
4.    if all fields in one entry are filled
5.      output the source IP
6.      delete the entry
7.    else
8.      if same digest and segment number exist
9.        create new entry
10.       fill the address bits into entry
11.     else
12.       fill the address bits into entry
```

Figure 5: Algorithm of FDPM reconstruction schem

VI.FLOW BASED MARKING SCHEME The goal of flow-based marking is to mark the most possible DDoS attacking packets (from the same sources but not necessarily with same source IP addresses and to the same destination), then let the reconstruction process in the victim end reconstruct the source by using a minimum number of packets.[1]. The probability of marking incoming packets is roughly proportional to the flow's share of bandwidth through the router. We defined probability as Pr as

$$p_a = \frac{npkts - \min(npkts_i, i \in \{1,n\})}{\max(npkts_i, i \in \{1,n\}) - \min(npkts_i, i \in \{1,n\})} \times \frac{L_{\max} - L}{L_{\max} - L_{\min}},$$

Where np is the number of packets in the flow, T is the current threshold (current load) of router. When the current load of the Router T reaches Tmax, Pr becomes 0, which means no marking is performed.

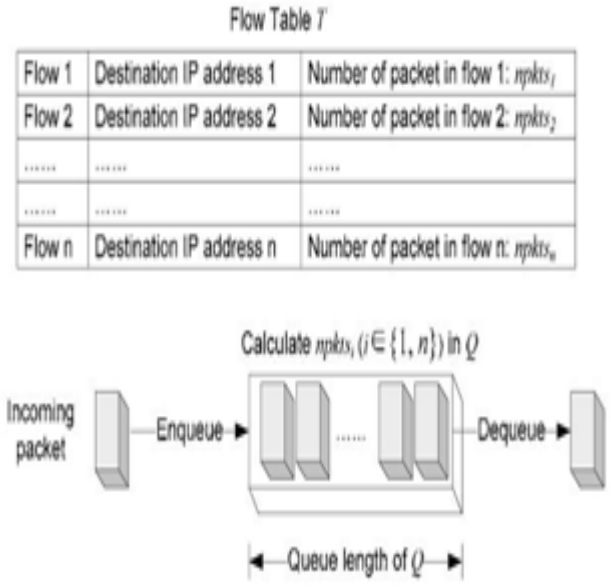

Figure 6: Dynamic flow table T and FIFO queue Q in FDPM flow-based marking scheme.

The router needs to forward, regardless of whether the flow contains large or small number of packets. In our flow based marking scheme, we aim at reducing complexity and increasing efficiency. It does not keep the state for each flow, but simply uses a single first-in, first-out (FIFO) queue which can be shared by all flows. The advantage of this is that it can be easily implemented in current router architecture, with little impact on the router's packet processing capability. This process is similar to some congestion control schemes such as the Random Early Detection (RED), which isolates the flows that have an unfair share of bandwidth and drops the packets in those flows. The flow-based marking scheme needs to isolate and mark the flows that occupy more bandwidth containing most possible DDoS attacking packets. It can mark packets with a certain probability from each flow, in proportion to the amount of bandwidth the flow uses.The simple data structures include a dynamic flow table T and a FIFO queue Q, as shown in Fig. 6. Each record in T stands for a flow. Here, the flow means the group of packets that have defined specific subsets of identifiers and are in the Q at a certain time. In DDoS scenarios, attacking packets are classified into different flows according to the destination IP address in the IP header because the aggregation effect is the major feature in DDoS attack traffic. The flow records in T are the destination IP addresses and the number of packets from this flow in the queue Q, denoted as npkts. The algorithm of flow-based marking is shown in Fig.7.There are two load thresholds Lmax and Lmin for the traceback router. Lmax is the threshold that controls the whole packet marking process, which means the router will not mark any packet if its load exceeds this value. Congestion control mechanisms can be turned on in order to guarantee a best effort service for the router. The load threshold Lmin means that if the load exceeds this value, the router can still work, but it must reduce its marking load. If the load stays below Lmin, then the router will just mark all the incoming packets because the router can process all packets without having performance penalty. These two thresholds should be set according to real situations in routers. For example, they can be decided by the CPU usage of the router, or the input rate of the router, depending on what is the essential measurement of the router's load. In this paper, input rate is chosen to determine these two load

thresholds. How to obtain the best load thresholds is left as a question for future research.

```
1.   if (load of router R > threshold Lmax)
2.     do not mark any packets
3.     turn on congestion control mechanisms
4.   else if (load of router R > threshold Lmin)
5.     turn on flow-based marking at R, edge interface A, in network N
6.     for each incoming packet p
7.       check npkts with same destination address of p from T
8.       if (npkts == 0, means no such flow in T)
9.         add a new entry in T, set its npkts = 1
10.      else
11.        npkts ++
12.      insert packet p into Q
13.      calculate marking probability pa
14.      with probability pa mark the packet (encoding procedure)
15.      if Q is full
16.        dequeue
17.  else
18.    mark all the packets at R, edge interface A, in network N
```

VII. CONCLUSION

FDPM is suitable for not only finding sources of DDoS attacks but also DDoS detection. DDoS is mainly uses multiple attacking sources to attack a single victim. Therefore, at any point in the network, if there is a sudden surge in the number of packets with the same destination address and with the same group of digest marks, it can be a sign of a DDoS attack. More details can be found in [8].

REFERNCES:

1. Y. Xiang and W. Zhou, "Flexible Deterministic Packet Marking:An IP Traceback System to Find the Real Source of Attacks," IEEE transactions on parallel and distributed systems, vol. 20, no. 5, may 2009.

2. H. Wang, C. Jin, and K.G. Shin, "Defense against Spoofed IP Traffic Using Hop-Count Filtering," IEEE/ACM Trans. Networking, vol. 15, no. 1, pp. 40-53, 2007.

3. M.T. Goodrich, "Efficient Packet Marking for Large-Scale IP Traceback," Proc. Ninth ACM Conf. Computer and Comm. Security (CCS '02), pp. 117-126, 2002.

4. H. Aljifri, "IP Traceback: A New Denial-of-Service Deterrent,"IEEE Security and Privacy, vol. 1, no. 3, pp. 24-31, 2003.

5. Belenky and N. Ansari, "On IP Traceback," IEEE Comm.,vol. 41, no. 7, pp. 142-153, 2003.

6. Z. Gao and N. Ansari, "Tracing Cyber Attacks from the Practical Perspective," IEEE Comm., vol. 43, no. 5, pp. 123-131, 2005.

7. H. Burch and B. Cheswick, "Tracing Anonymous Packets to Their Approximate Source," Proc. 14th Systems Administration Conf.(LISA '00), pp. 319-327, 2000.

8. R. Stone, "CenterTrack: An IP Overlay Network for Tracking DoS Floods," Proc. Ninth USENIX Security Symp. (Security '00), pp. 199-212, 2000.

9. S.M. Bellovin, ICMP Traceback Messages—Internet Draft, Network Working Group, 2000.

10. A. Mankin, D. Massey, C.-L. Wu et al., "On Design and Evaluation of Intention-Driven ICMP Traceback," Proc. 10th Int'l Conf Computer Comm. and Networks (ICCCN '01), pp. 159-165, 2001.

11. C. Jin, H. Wang, and K.G. Shin, "Hop-Count Filtering: An Effective Defense against Spoofed DDoS Traffic," Proc. 10th ACM Conf. Computer and Comm. Security (CCS '03), pp. 30-41, 2003.