

DDOS SCOUTER: A SIMPLE IP TRACEBACK SCHEME

Chen Kai

Bell-labs Research China, Lucent Technologies, Beijing, China 100080
kaichen@lucent.com

Hu Xiaoxin

Department of Computer Science and Engineering, University of Electronical Science and Technology of China, Chengdu, China 610054
hux@blrcsv.china.bell-labs.com

Hao Ruibing

Bell-labs Research China, Lucent Technologies, Beijing, China 100080
rhao@research.bell-labs.com

Abstract Defense against distributed denial-of-service attacks is one of the hardest security problems on the Internet. Among those problems, the most difficult problem is to trace the attacks back to its origin for the attackers always use incorrect or spoofed IP addresses in the attack packets. In this paper, we propose a multi-edge marking scheme, which allow the victim to traceback to or near to the origin of the attackers with the help of the network administrator. The scheme features high performance efficiency and no false positive. Compared with the previous solutions, it has high precision and low computation overhead for victim to reconstruct the attack paths. Base on this marking scheme, DDoS Scouter is developed.

Keywords: DDoS attacks, IP traceback, packet marking

1. Introduction

With the wide deployment of Internet, security problems become the extreme threat to the Internet society. Due to the stateless and destination IP address routing natures of Internet, the Denial of Service attacks (DoS) are the most reported one among the security problems. A denial-of-service attack (DoS) aims at denying a victim (host, router, or entire network) providing or receiving normal services in the Internet. Distributed denial-of-service attacks (DDoS), typically conducted by flooding network links with large amounts of traffic(which is the focus of the paper), consume the resources of a remote host or network, thereby denying or degrading service to legitimate users. Such attacks are among the hardest security problems to address because they are easy to implement, difficult to prevent, and very difficult to trace.

In general, there are two types of flooding attacks: direct attacks and reflector attacks. In a direct attack, an attacker arranges to send out a large number of attack packets directly toward a victim. Attack packet types can be TCP, ICMP, UDP, or mixture of them. Before launching a direct attack, an attacker first sets up a DDoS attack network, consisting of one or more attacking hosts, a number of masters or handlers, and a large number of agents. The attacking host is a compromised machine used by the actual attacker to scan for vulnerable hosts and to implant specific DDoS master and agent programs. With an attack network ready, the attacking host may launch a DDoS attack by issuing an attack command with the victim's address, attack duration, attack methods, and other instructions to the masters. Each

master, upon receiving the instructions, then passes them to its agents for execution. A reflector attack is an indirect attack in that intermediary nodes (routers and various servers), better known as reflectors, are innocently used as attack launchers. An attacker sends packets that require responses to the reflectors with the packets' inscribed source addresses set to a victim's address. Without realizing that the packets are actually address-spoofed, the reflectors return response packets to the victim according to the types of the attack packets. As a result, the attack packets are essentially reflected toward the victim, and the reflected packets can flood the victim's link if the number of reflectors is large enough.

Because the results of DDoS attacks are serious financial disaster to the victim, many research results^[3,4,5,10,11,12,13,14,16,17,20], which are aimed at preventing the DoS/DDoS attacks, have been obtained in the research field. They can be divided into three lines: attack prevention and preemption (before the attack), attack detection and filtering (during the attack) and attack source traceback and identification (during and after the attack).

Although, it is infeasible to use IP traceback to stop an ongoing DDoS attack, it could be very helpful in identifying the attacker and collecting evidence for post-attack law enforcement.

Among the above techniques, attack traceback and identification has been much considered recently. It can usually be carried out after or during a DDoS attack. IP traceback refers to the problem, as well as the solution, of identifying the actual source of any packet sent across the Internet without relying on the source information in the packet. Up to now, there are generally two type approaches to the IP traceback problem. One is for routers to record information about packets they have seen for later traceback requests^[3,14], named logging. Another is for routers to send additional information about the packets they have seen to the packets' destinations via either the packets^[5,16] or another channel, such as ICMP messages^[10].

In Bellovin's proposed ITRACE scheme, routers, with a very low probability, send ICMP messages to the destinations of packets they have just forwarded^[10]. For a high-volume flow, the victim will eventually receive ICMPs from all of the ITRACE routers along the path back to the attackers, revealing its location. Savage and colleagues proposed a different scheme, in which routers with considerably higher probability mark the packets they process with highly compressed information that the victim can decode in order to detect the edges traversed by the packets, again enabling recovery of the path back to the attacker^[5]. However, the scheme runs into computational difficulties as the number of attackers increases. This problem is addressed by Song and Perrig by supplementing the scheme with the use of network topology maps^[16]. Recently, Snoeren and colleagues developed a Source Path Isolation Engine (SPIE) that records sets of hashes of packets traversing a given router^[3]. A victim can then locate the path of a given packet by querying routers within a domain for the set of hashes corresponding to the packet, providing that they issue the query soon enough after the packet was transmitted that the record of its presence is still available. SPIE has a major advantage in that it can facilitate traceback of even low volume flows.

There is a dilemma in designing the IP traceback scheme: time and space requirements. Among the above systems, the logging related schemes are said not practical because the storage requirement of the router is too high; the marking related schemes have the disadvantages of high time consumption in marking packets collection and attack paths construction.

In the victim's view, the quick response to the attack is much more desired. However, in order to reduce the marking space requirement, the well recognized schemes proposed in^[5] deployed some code techniques which led to the inefficiency in packet collection and attack path reconstruction, especially for DDoS attacks. The direct result is that the victim has to endure longer attack.

To make the IP traceback technique more practice, it is necessary to make a tradeoff between the time and space requirements. In this paper, we proposed an on-demand probabilistic multi-edge IP marking technique to do IP traceback. It is designed that the marking enabled router only doing marking when it receives the marking instruction from the network administrator. In the scheme, the record route IP option is used to mark the router's (by which the packet is forwarded) IP addresses. In the record route

IP option, several IP addresses can be recorded. So, an attack packet can carry a segment of the attack path with which it can improve process of the attack path reconstruction greatly.

Based on the proposed IP traceback technique, DDoS Scouter system is designed to prevent the DDoS attacks. The system consists of attack detection, IP traceback and packet filtering(intelligent packet filtering using the traceback scheme will be studied in the other paper).

The rest of the paper is organized as follows. Section 2 proposes the basic and authenticated multi-edge marking and traceback algorithms. In section 3, the DDoS Scouter system is presented. The testing results of the system is described in section 4. In section 5, some problems of the system are discussed and it is concluded in section 6.

2. Multi-edge marking

Keeping in mind that the IP protocol should not be modified or just little modification should be made when an IP marking scheme was designed or developed. In addition, the designed or developed system should not add too much process burden to the routers, which would lower the performance of the routers. It is also noticed that, without the help of the network administrator, it is very inefficient and difficult for the victim to do the traceback.

2.1 Record route IP option^[2]

The record route option provides a means to record the route of an Internet datagram. The option type is 7. A recorded route is composed of a series of Internet addresses(see *Table 1*). For the record route IP option is designed for network control use, it is seldom used in today's Internet. In the Multi-edge marking scheme, we make use of the IP option to marking the routers' IP addresses through which the packets traverse. This requires no changes to the IP protocol. Record route option is not copied on fragmentation and goes in first fragment only. It appears at most once in a datagram.

Table 1. The data format of record route IP option

0000011	length	pointer	route data
---------	--------	---------	------------

For the maximal Internet header is 60 octets, the record route IP option header is 3 octets, a typical internet header is 20 octets^[2], and if there are no other IP options in use, the maximum number of IP addresses that the record route IP option can contain is $9(= (60 - 20 - 3)/4)$.

2.2 algorithm

The multi-edge marking is to append adjacent segment attack path to the record route IP option of the packet as it travels through the network from the attacker to victim. Unlike the node append proposed in^[5,16], the algorithm is a probabilistic based and does not append the routers' IP addresses to all packets. Because of the limited space in IP header, it can not mark all the routers' IP addresses into the record route IP option if the attack path is longer than 9. Here, we propose to mark the packet probabilistically. When a marking enabled router forwards a packet destined to the victim and the packet's record route IP option is not opened, it determines probabilistically whether or not to open the record route IP option of the packet to do marking. If it decides to open the option, it appends its IP address to the record route IP option. If a packet destined to the victim, the packet's record route IP option is opened and the number of the appended IP address is less than 9, it appends its IP address to the record route IP option.

After the victim collects enough marking packets, it uses the multi-edges sampled in these packets to create a graph leading back to or near to the source or sources of attack. *Figure 1* depicts the full marking and attack path reconstruction algorithms.

Marking procedure at router R :

```

for each packet  $w$ 
  if destination of  $w$  is victim then
    if record route IP option is set on then
      if the record route number  $< 9$  then
        append  $R$  into  $w$ .record router IP option
      endif
    else
      let  $x$  be a random number from  $[0,1]$ 
      if  $x < p$  then
        set the record route IP option on
        append  $R$  into  $w$ .record router IP option
      endif
    endif
  endif
endif

```

Path reconstruction procedure at victim v :

```

let NodeTable be an empty diagonal matrix, the element of the matrix be of tuples  $nt(node, count)$ 
for each path segment  $(R_1, R_2, \dots, R_n, 1 \leq n \leq 9)$  of attack path in the attack packet
  for each router  $(R_1, R_2, \dots, R_n, 1 \leq n \leq 9)$ 
    if  $R_i$  is not in the column then
      add  $R_i$  into the diagonal matrix
      set  $nt(R_{i-1}, R_i)$  and  $nt(R_i, R_{i+1})$  be  $(1, 1)$ 
    else
      increase  $nt(R_{i-1}, R_i).count, nt(R_i, R_{i+1}).count$  by 1
    endif
  endif
draw the attack path according to the NodeTable established. If  $nt(R_i, R_j).node = 1$ ,  $R_i$  and  $R_j$  are connected directly

```

Figure 1. The multi-edge marking and path reconstruction algorithms

The marking algorithm depicts in *Figure 1* is named uncovered marking, which means that the marked IP address can not be covered by the later router. This would lead to the further the router to victim the less probability that the router's IP address is marked. The marking algorithm can be modified to covered marking, i.e. when the IP option is full and there is another router want to mark its IP address, the very first IP address will be shifted out to give the space for marking the new comer.

If we consider the DDoS attack as propagating in a tree T , where the root of the tree T is the victim, each internal node in T corresponds to a router R on the Internet, and each leaf in T is an attack host. Our goal in the traceback problem is to identify the internal nodes of the tree T and to draw the tree. For the marked packets take the sequential segment of the path through which the packets pass, the victim need not to determine the location of each router(IP address) on the path. It just need to draw a connective graph according to the sequential segment collected. Compared with the available scheme, the victim needs not to determine which router is located before or after the other router(which may dominate the path reconstruction time), so the attack path reconstruction algorithm here is both robust and extremely quick to converge, especially in reconstructing multiple attack paths in DDoS attacks.

2.3 Analysis

The victim uses the edges marked in the attack packets to reconstruct the attack graph. The algorithm is depicted in *Figure 1*. It is noticed that the marking scheme is un-covered, which means that if a packet is marked at router A , the followed routers must mark their IP addresses into the packet unless there is no space in the record route IP option. So the probability of receiving a sample is becoming smaller the further away it is from the victim. The time for the algorithm to converge is dominated by the time to receive a sample from the furthest router. Let L be the length of the attack path, p is the marking

probability and N denotes the number of the IP address that record route IP option can contain, here it is 9. The expected number of marked packet needed to reconstruct the attack path is $\lceil L/Np \rceil$. Some research results^[1,19] indicate that the distance between arbitrary two hosts in Internet would not exceed 30 hops. If every marked packet carries 9 routers' address and no overlap of the path segment, 4 marked packets is enough to reconstruct the longest attack path in the Internet.

2.4 Authenticated multi-edge marking algorithm

A main disadvantage of the basic multi-edge marking scheme is that the packet markings are not authenticated. Consequently, a compromised router on the attack paths could forge the markings by appending spoofed IP address or filling up the IP record option using spoofed IP addresses, preventing the victim from determining the attack paths. To solve this problem, we need a mechanism to authenticate the packet marking. A straightforward way to authenticate the marking of the packets is to have the router digitally sign the marking. However, digital signatures are very expensive to compute and have large space overhead. Here, we propose a much efficient technique to authenticate the packet marking. The technique only uses one cryptographic MAC (Message Authentication Code) computation per marking, which is much more efficient to compute (i.e., HMAC-MD5^[8,9] is three to four orders of magnitude more efficient than 1024-bit RSA signing) and can be adapted so it only requires the 16-bit overhead for storage. It is conjectured that it is computationally infeasible to produce two messages having the same message digest, or to produce any message having a given pre-specified target message digest. For the standard output of MD5 is 128-bit message, it is modified to produce a 16-bit output. In order to avoid collision, the packet-specific information is necessary. Let h_K denote the MAC function using key K . If each router R_i shares a unique secret key K_i with the victim, R_i can apply to its IP address and some packet-specific information, such as the source (S_{IP}) and destination (D_{IP}) IP addresses in the packet, with K_i , i.e. $h_{K_i}(S_{IP}, D_{IP}, R_i.IP)$ to produce the authentication $R_i.auth$. For each R_i , $auth$ is 16-bit long, the IP route record option can contain 6 marking messages at most.

The authenticated marking and attack path reconstruction algorithms are depicted in *Figure 2*.

Marking procedure at router R_i :

```

for each packet  $w$ 
  if destination of  $w$  is victim then
    if record route IP option is ON then
      if the record route number  $< 6$  then
        append  $R_i.IP$  into  $w.record$  route IP option
        append  $h_{K_i}(S_{IP}, D_{IP}, R_i)$  into  $w.record$  route IP option
      endif
    else
      let  $x$  be a random number from  $[0,1]$ 
      if  $x < p$  then
        set the record route IP option on
        append  $R_i.IP$  into  $w.record$  route IP option
        append  $h_{K_i}(S_{IP}, D_{IP}, R_i)$  into  $w.record$  route IP option
      endif
    endif
  endif
endif

```

Path reconstruction procedure at victim v :

```

let NodeTable be an empty diagonal matrix, the element of the matrix be of tuples  $nt(node, count)$ 
for each path segment  $(R_1, R_2, \dots, R_n, 1 \leq n \leq 6)$  of attack path in the attack packet
  for each router  $(R_1, R_2, \dots, R_n, 1 \leq n \leq 6)$ 
    if  $h_{K_i}(S_{IP}, D_{IP}, R_i) = R_i.auth$  then
      if  $R_i$  is not in the column then
        add  $R_i$  into the diagonal matrix
        set  $nt(R_{i-1}, R_i)$  and  $nt(R_i, R_{i+1})$  be  $(1, 1)$ 
      else

```

```

        increase  $nt(R_{i-1}, R_i).count$  and  $nt(R_i, R_{i+1}).count$  by 1
    endif
endif
draw the attack path according to the NodeTable established. If  $nt(R_i, R_j).node = 1$ ,  $R_i$  and  $R_j$  are connected directly.

```

Figure 2. The authenticated multi-edge marking and path reconstruction algorithms

3. DDoS Scouter

To keep in line with the above principles, DDoS Scouter is designed as a query-respond system. Only when the IDSs deployed in the victim's system detect that there exists DDoS attacks aimed at the victim, the network administrator on receiving the marking requests asks the marking enabled routers to do IP marking. The enabled routers mark its IP address only into the specific packet(destined to the victim, the other packets destined to the other destination are not marked). The system involves the victim, intrusion detection system, network administrator or operator, IP marking and/or packet filtering enabled routers. All the communications among any components in the system must be authenticated to avoid being used by invalid users or attackers.

Figure 3 shows the architecture of the system. The DDoS Scouter consists of four entities: victim, Intrusion Detection System(IDS), network administrator and marking and filtering enabled routers.

The IDS responds to detect the DDoS attacks and sends DDoS attack alarm to the network administrators. When IDS detects that there exists DDoS attacks aimed at the victim host or network, it sends DDoS attack alarm to the victim's network administrator with the victim identity and attack characteristics. There are many commercial available IDS systems^[18,21,22,23] and also there are some research results on how to detect DDoS attacks^[18,21].

The network administrator is responsible for controlling the routers to do IP marking and packet filtering. On receiving the DDoS attack alarm, the network administrator authenticates that the alarm is really sent by a valid IDS. Then, it sends IP marking instructions to the IP packet marking enabled routers to start to do IP marking. On receiving the attack paths information, the network administrator decides on which routers the packet filter should be launched to stop or dilute the DDoS attacks aimed at the victim and sends the filtering instruct to the selected routers to do packet filtering.

The marking and/or filtering enabled routers are responsible for carrying out the marking and packet filtering functions. On receiving the mark instructions, the IP packet marking enabled routers begin to mark its IP address into the packets destined to the victim. The packets routed to the other destinations are not marked. On receiving the filtering instructions, the routers filter the packets destined to the victim and forward the packets destined to the other destinations.

Having received the marked packets, the victim collects the IP addresses of routers through which the packets are passed. Using the collected the IP addresses, the victim reconstructs the attack paths or sub-paths and sends the attack paths to the network administrator to do filtering.

4. Simulation

To test the performance of the multi-edge marking scheme, we conduct an experiment on SSFnet^[15], a well known network simulator system. In the simulation, the following three schemes are tested and compared: Compressed edge fragment sampling (CEFS), Un-covering Multi-Edge method (UME) and Random Multi-Edge method (RME). The first one is proposed in ^[5] and the last two are proposed in this paper. The difference between RME and UME lies in whether the marking procedure is random or not. In UME scheme, when the IP option is full, the following router's IP address can not be marked. In the RME scheme, when the IP option is full, the very first router's IP address is shifted out and the new router's IP address is marked in. These schemes are tested in three scenarios:

- S1: one attacker being 10 hops away from the victim.

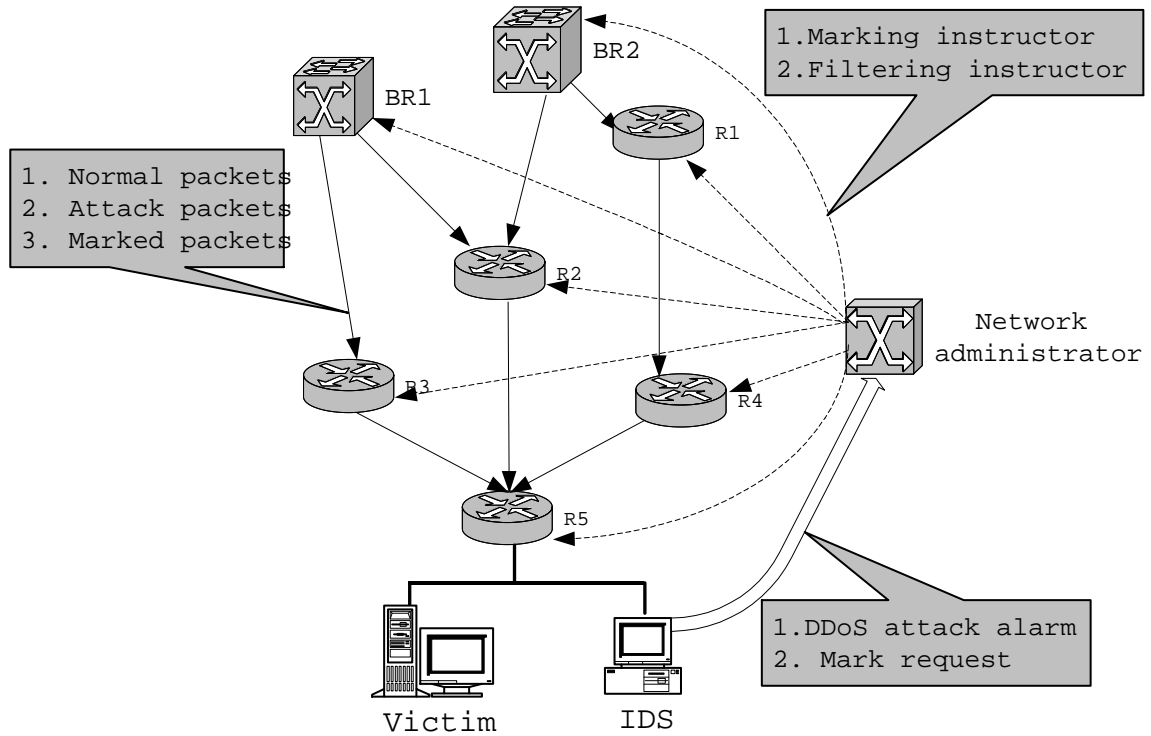


Figure 3. The architecture of the DDoS Scouter

- S2: one attacker being 24hops away from the victim.
- S3: 261 hosts locating at different places and attacking the victim through 14 different paths, i.e. a Distributed DoS attack.

Two criterias are used to make the comparison. The first one is the expected number of the packets required for path reconstruction. *Table 2* shows the simulation results. It indicates that the multi-edge marking schemes needs much less packets than CEFS, especially for the DDoS attacks. For most flooding-style DoS attacks send many hundreds or thousands of packets per second, the victim can collect the enough packet in the moment. In addition, the marking enabled router need to perform the marking function in the short time slot. From the table, we observe that when the length of the attack path increases from 10 to 24, the increment of packets in UME is slight. It indicates that UME has good adaptability for the change of the distance. The second one is the time required for path reconstruction. The simulation results indicates that all of the tests except for the CEFS in DDoS attack scenario, which takes more than one day to do the path reconstruction, can be completed within one second.

Table 2a. Number of packets needed to reconstruct the attack path $p = 0.05$

	S1	S2	S3
CEFS	2000	3600	56000
UME	40	40	800
RME	60	90	2100

Table 2b. Number of packets needed to reconstruct the attack path $p = 0.1$

	S1	S2	S3
CEFS	1400	5900	75000
UME	30	40	400
RME	70	150	2000

5. Discussion

5.1 Fragmentation

It is indicated in^[5] that the main drawback of the marking algorithm is overhead of the packet size increased by the marking, which can lead to the fragmentation and bad interactions with services such as MTU discovery^[6]. Note that the routers just mark the packets destined to the victim, it does not affect the other packets in deed. If the marking results in the fragmentation of the packet, it can be designed to fragment the packet properly that the packet will be not fragmented again later. Furthermore, the fragmented packet will not be marked except for the first segment of the packet. Some research results shows that more than 95 percent attack packets are small packet, such as TCP(SYN,RST), ICMP and so on. These kind of packets have enough space for multi-edge

5.2 Authentication

In the DDoS Scouter system, there are two kinds of channels should be authenticated. The first one is the communications among the victim, the IDS, the network administrator and the marking enabled routers. The malicious users or attackers can send invalid marking request or filtering request to launch another type of DoS attacks. Any authentication and encryption mechanisms available can be deployed in the system.

For the compromised routers could forge the markings according to the precise probability distribution and preventing the victim from detecting and determining the compromised router by analyzing the marking distribution, the second one is to authenticate the marking information and has been considered in section 2.4.

5.3 Cross-domains

In DDoS Scouter, the network administrator acts as the controller to do marking and filtering on demand. Because there exists trust problem among different ISPs or ASs, the network administrator cannot send instructs to routers not belong to his domain. The attack paths reconstructed by victim is just the sub-attack paths. In order to reconstruct the full attack paths, the trust among different ISPs must be established. Based on the trust, the network administrator in the victim's domain sends the marking request and filtering request to the other ISPs network administrators. Thus, DDoS Scouter can trace back exactly to or near to the attackers or agents. A directly solution to this problem may be hierarchical mechanism.

6. Conclusion

To make the IP traceback more practical and efficient, multi-edge marking based scheme was proposed in the paper. According to the analysis and simulation, the scheme is much more efficient than the scheme available up to now. In addition, the authors proposed a DDoS Scouter system, which is an architecture or framework, to prevent the DDoS attacks. Coupled with the fact that attack mechanisms and tools continue to improve and evolve, more effective detect-and-filter approaches must be developed in addition to the use of ingress packet filtering and other existing defense mechanisms and procedures. In the next, for the multi-edge marking scheme, we are exploring some code techniques to decrease the space requirement of one IP address. Based on the architecture, we will introduce the intelligent filtering technique into the system and extend it to a global defense infrastructure to protect the entire Internet from DDoS attacks.

References

- [1] W. Theilmann and K. Rothermel, "Dynamic Distance Maps of the Internet", in Proc. IEEE INFOCOM'00, Tel Aviv, Israel, March, 2000.

- [2] J. Postel, "Internet Protocol", RFC791, Sep. 1981.
- [3] A. C. Snoeren, C. Partridge, L. A. Sanchez, C. E. Jones, F. Tchakountio, S. T. Kent and W. T. Strayer, "Hash-based IP Traceback", SIGCOMM'01, August 27-31, 2001, San Diego, California, USA.
- [4] Rocky K. C. "Defending against Flooding-Based Distributed Denial-of-Service Attacks: A Tutorial", IEEE Communications Magazine, October 2002, pp42-51.
- [5] S. Savage, D. Wetherall, A. Karlin and T. Anderson, "Network Support for IP Traceback", IEEE/ACM Transactions on Networking, Vol.9, No. 3, Jun. 2001, pp226-237.
- [6] J. Mogul and S. Deering, "Path MTU discovery", RFC1191, 1990.
- [7] "Internet mapping," <http://cm.bell-labs.com/who/ches/map/dbs/index.html>, 1999.
- [8] H. Krawczyk, M. Bellare, and R. Canetti, "HMAC: Keyed-hashing for message authentication", Internet RFC 2104, February 1997.
- [9] R. L. Rivest, "The MD5 message digest algorithm", RFC 1321, Internet Activities Board, Internet Privacy Task Force, April 1992, 1992.
- [10] Steve Bellovin, "The icmp traceback message", <http://www.research.att.com/?smb>, 2000.
- [11] P. Ferguson and D. Senie, "Network ingress filtering: Defeating denial of service attacks which employ ip source address spoofing", RFC 2267, January 1998.
- [12] Hal Burch and Bill Cheswick, "Tracing anonymous packets to their approximate source", Unpublished paper, December 1999.
- [13] Robert Stone, "Centertrack: An ip overlay network for tracking dos floods", Unpublished, October 1999.
- [14] Drew Dean, Matt Franklin, and Adam Stubblefield, "An algebraic approach to ip traceback", in Network and Distributed System Security Symposium, NDSS '01, February 2001.
- [15] SSFnet, <http://www.ssfnet.org>
- [16] D. X. Song and A. Perrig, "Advanced and Authenticated Marking Schemes for IP Traceback", in Proc. IEEE INFOCOM'01, April, 2001.
- [17] D. Moore, G. M. Voelker and S. Savage, "Inferring Internet Denial-of-Service Activity", in Proc. Of the 10th USENIX Security Symposium, Washington, D.C., USA, August, 2001.
- [18] H. Wang, D. Zhang and K. G. Shin, "Detecting SYN Flooding Attacks", in Proc. IEEE INFOCOM'02, 2002.
- [19] R. L. Carter and M. E. Crovella, "Dynamic Server Selection Using Dynamic Path Characterization in Wide-Area Networks", in Proc. IEEE INFOCOM'97, Kobe, Japan, April, 1997.
- [20] M. T. Goodrich, "Efficient Packet Marking for Large-Scale IP Traceback", CCS'02, November 18-22, 2002, Washington, DC, USA. p:117-126.
- [21] A. Ramanathan, A.L. N. Reddy, M. Vannucci, "WADeS: A Tool for Distributed Denial of Service Attack Detection", ACM SIGCOMM Internet Measurement Workshop 2002.
- [22] C. Manikopoulo and S. Papavassiliou, "Network Intrusion and Fault Detection: A Statistical Anomaly Approach", IEEE Communications Magazine, October, 2002. p:76-82.
- [23] G. Vigna and R. A. Kemmerer, "NetSTAT: A Network-based Intrusion Detection Approach", Proc. 14th An. Comp. Sec. App. Conf., 1998, p:25-34.