American Journal of Applied Sciences 4 (10): 741-745, 2007
ISSN 1546-9239

A Novel Packet Marketing Method in DDoS Attack Detection

[1]Changhyun Beak, [1]Junaid Ahsenali Chaudhry, [2]Keonsoo Lee, [1]Seungkyu Park and [1]Minkoo Kim
[1]Graduate School of Information and Communication,
[2]College of Information and Communication Engineering,
Ajou University, Suwon, Kyyongi do, Paldal gu, Korea. 443-749

Abstract: Functionality and availability are one of the main characteristics of internet and hence very inviting for attackers to try to provoke a denial-of-service attack. As the intensity and frequency of DDoS attacks has increased, various preventive mechanisms have also been proposed. One of the most effective defence mechanisms proposed was Path Identification (Pi). This method tracks the packet transmission path. With this packets carrying path information, the victim node can defend itself from DDoS attack by filtering the packets transmitting via/from an attacking node. The Pi method has advantages such as trivial operation, filtering on a per-packet and independency on router for blocking over the other trace back methods etc. As the Pi method uses the router's IP address to construct the path information of each packet, which was stored in each packet's ID field. However, because of the limitation of the ID field, only two bits of resulted message digest of router's IP address are used, which results in same path information representing different paths. To ad-dress this problem, we propose using Link-ID's instead of IP addresses or routers to construct the path information of each packet. A Link-ID was the in-formation of path between Border Gateway Protocol (BGP) routers in the Autonomic Systems (AS) and each BGP router's connection to the outside of the AS. Further analysis shows promising results if compared with contemporary filtering methods.

Key words: Denial of Service Attacks, Computer Security, Packet Marking, Computer Virus

INTRODUCTION

A Denial-of-Service (DoS) attack is characterized by an explicit attempt to prevent legitimate users of a service from using that service [1]. It is an attempt to make computer resources unavailable to intended users. Normally the victims are high profile, recourse rich machines that further provide service to one or many machines attached with it. A DoS attack can force the victim machine(s) to reset/change their states or consume its resources so much that it could not provide service to either perspective or existing or both types of consumers. A Distributed Denial-of-Service (DDoS) attack deploys multiple machines to attain the goal that is creating a DoS attack. This distribution of attackers makes it is more difficult than facing a singled out attacker. With the increasing use of internet and technological advancement in distributed computing, innovative types of DDoS attacks are showing up on regular bases. Since internet was created with the intention of functionality, not security, these attacks exploit the fact that unidentified clients can access the online service providing server. Because of this basic limitation of a server, it automatically announces the denial of service when the number of service requests exceeds it capability.

The DoS attacker's goal is to try and stop the server serving the service requests made by any user, intended or non-intended, by frequently sending useless service requests. As the capability of servers to entertain a number of service requests have increased, it seems to be impossible for a single attacker to create DoS attack to server system. This difficulty spawns the distributed denial-of-service attack (DDoS). As more attackers send the trash requests, the server gets sucked into the flood of fake service requests and denial of service takes place. Since attackers are distributed, it is harder to identify "who is the attacker?" than singled out attacker in DoS attack.

In order to defend the victim server from the DDoS, several methods have been proposed. One of the most efficient methods is by path identification (Pi). The Pi method has advantages such as trivial operation, filtering on a per-packet and independency on router for

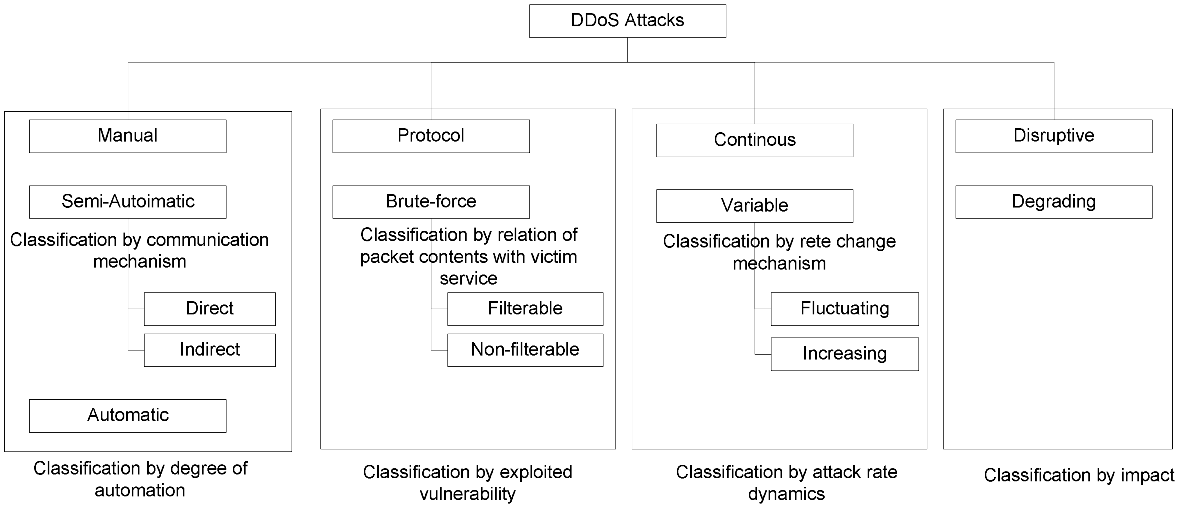
DDoS Attacks
Manual
Semi-Autoimatic
Classification by communication mechanism
Direct
Indirect
Automatic
Classification by degree of automation
Protocol
Brute-force
Classification by relation of packet contents with victim service
Filterable
Non-filterable
Classification by exploited vulnerability
Continous
Variable
Classification by rete change mechanism
Fluctuating
Increasing
Classification by attack rate dynamics
Disruptive
Degrading
Classification by impact

Fig. 1: Classification of Distributed Denial-of-Service (DDoS) attacks

blocking over the other trace back methods etc. As the Pi method uses the router's IP address to construct the path information of each packet, which is stored in each packet's ID field. However, because of the limitation of the ID field, only two bits of resulted message digest of router's IP address are used, which results in same path information representing different paths. To address this problem, we propose using Link-ID's instead of IP addresses or routers to construct the path information of each packet. A Link-ID is the information of path between Border Gateway Protocol (BGP) routers in the Autonomic Systems (AS) and each BGP router's connection to the outside of the AS. Using Link-ID as path information guarantees a unique path identification with low computing load.

In section 2, we discuss the modern studies being carried out for DDoS attacks and their prevention mechanisms. We discuss the proposed method in section 3 and analyze the proposed method with contemporary methods in section 4. We conclude our work in section 5.

The DDoS attack is an attempt to consume the victim's resource with useless re-quests. This attack can be classified according to its type such as degree of automation, exploited vulnerability, attack rate dynamics and impact. These DDoS attack are classified in Fig. 1.

In order to defend the resources from these attacks, the most important thing is to detect where the malicious request are coming from. As the attacker usually spoof the source information, the service request source identification gains primary importance.

The Deterministic Packet Marking (DPM) [4] is based on *traceback* methods. The 16-bit Packet ID field and 1-bit Reserved Flag in the IP header is used to mark packets. The Probabilistic Packet Marking (PPM) [3] is based on marking packets with a fixed probability by all routers. The information marked by PPM shows which router the packet passes with the hop count that indicates the number of nodes between the router and victim. When the distance between attacker and victim is long, the distribution of path information marked by PPM is skewed because of the fixed probability of marking. For this Adjusted Probabilistic Packet Marking (APPM) [5] is proposed but to change the probability value we have to change it at each router separately. The *iTrace* [10] involved probabilistic sending of a message to either the source or the destination of the IP packet indicating the IP address of the router (that sent the message). The main benefit of this scheme was that it did not require changes to packets in-flight, but it also suffered from the drawback of generating extra traffic. The schemes in are [11, 12] are promising but not scalable.

Path Identification (Pi) [2] uses filtering techniques to identify the attack packets by analyzing their path. It suggests routers' mark information on packets en-route to the victim. With this mark information, the victim can sense packet sender. It's better than *traceback* mechanisms in following aspects;

1- The victim can filter the packet independently from other upstream routers,
2- The victim decides whether to drop or receive each packet,

3- It is easier to decide the packet source.

In almost all the schemes discussed above, once the attack path is recognized, the target server can drop the packet which has the same path identifier to the attack path. Because of suitable routing policy and network condition, the packets sent by an attacker can have the different path identifier. Therefore we propose a strongly type checking yet flexible method because just checking the exact path is not sufficient.

PROPOSED METHODOLOGY

The core of Pi is finding a path of each packet and filtering the packet which has the attack path. As the classification of packet is based on its path, marking a unique path into the packet is the most important part of Pi. In order to mark a unique path between the attackers and the victim, the original Pi considers four factors of marking. These factors are which part of router's IP address to mark, where to write the IP information in each packet's ID field, how to omit the needless nodes in the path, and how to distinguish the paths that have the partially same links of routers.

The original Pi method uses these processes for packet marking. The packet's ID field is divided by the number of the bits of IP information marked by the router. Then, according to the packet's TTL, the section of marking is selected. The IP information of each router marks is a very small part of the full IP address; generally 2 bits. Therefore the IP hashing method is employed. For the probability of same marking for paths which have the same intermediate routers, the edge marking method which adjusts the marking information by significant bits of the MD5 hash is used. Because of the limitation of packet's ID field, the suppressing nearby router marking method which ignores the information of routers which are in the same autonomous systems (AS) is hired. These processes are employed because of the limitation of packet's space for marking all the path routers' information. Therefore in this paper, we suggest a packet marking method using Link-ID instead of IP address of routers.

An AS is the unit of router policy, either a single network or a group of networks that is controlled by a common network administrator on behalf of a single administrative entity such as a university, a business enterprise, or a business division. In an AS, as the routing information is spread, the BGP routers can know to which router the packets egress and by which router the packets ingress outside the AS. The Link-ID is this information of path between BGP routers in an AS and each BGP router's connection to the outside of the AS. The Link-IDs between routers should be knows to all the routers in the AS. The Link-IDs of each router's out-connection is its own private.

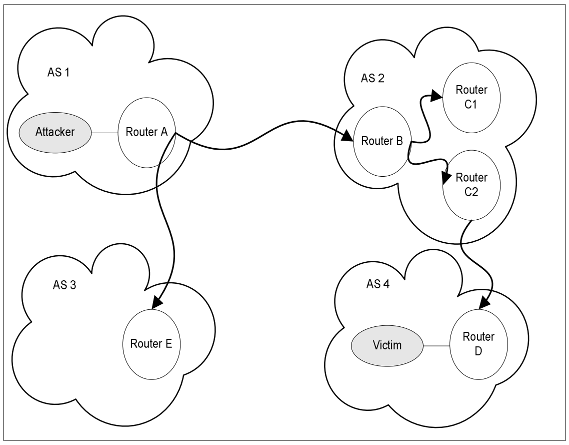

Fig. 2: Example of BGP Community

The example of BGP community is shown in Fig. 2. The attacker in AS 1 tries to DoS attack to the victim in AS 4. The packet from attacker is initially marked by *RouterA* in AS 1. Because the ingress router information is not marked in the packet, the *RouterA* is recognized that it is the initial router. The *RouterA* has two out-connection links for AS 2 and AS 3. Each connection is entitled as 1 and 2. The entitled id of each connection is the *RouterA's* own decision. The packet is forwarded to *RouterB* in AS 2 with marked information of initial router IP and its out-connection link id. In AS 2, there are 3 BGP routers. Therefore the number of BGP routers' pair in AS 2 is 9 by computing 3P2. The pair table consists of these elements such as (*RouterB*, NULL), (*RouterB*, *RouterC1*), (*RouterB, RouterC2*), (*RouterC1, RouterC2*) and so on. According to the packet's destination IP, the *Link-ID* of *AS2* is (*RouterB, RouterC2*) which is entitled as 2. The internal BGP Link-ID should be announced to all the BGP routers in that AS, which is different from the BGP router's out-connection Link-ID. The *RouterC2* forwards the packet to AS 4 as the *RouterA* did. The *RouterD* in AS 4 receives the packet and checks the packet's destination IP is in its own AS.

```
Main Process

/* intoAS : AS's ingress checker */

If(!intoAS)
/* Step 1 */
      initial router = current router
      marking Link-ID

Else(DestinationIP in CurrentAS)
/* Step 2 */
      ending router = current router

Else
/* Step 3 */
      marking Link-ID
```

```
Marking router information

Temp = strcat(AS's ID , router's ID in that AS)
Result = Hasing (Temp)
Insert (Result, router ID in packet)
```

```
Marking Link-ID

If(sending packet outside the AS)

   betweenR = lookupTable(intoAS, current_router)
   outConnect = current router's out-link
   insert(betweenR, outConnect, Path Link-ID)

ElseIf(sending to another router in AS)

   if(!intoAS)
     intoAS = currentAS
```

Fig. 3: Detail process of marking steps

The *RouterD* marks its IP in the ending section and forwards to the victim. Therefore the ID field of the packet that the victim received is marked as shown in Table 1.

Table 1: The sample pocket marking result

Title	Initial Router ID	Path Link-ID	Ending Router ID
Value	RouterA	1,2,1	RouterD

This marking process operates in BGP routers. Fig. 3 shows the detail process of this method. When the router tries to mark its information, it checks if the packet is en-router from other BGP router or other AS. If the check result is negative, the router marks its information as the packet's initial router. If the check result is positive, the router checks the packet's destination. If the destination is in the same AS, the router marks its information as the packet's ending router. If the check result is in other AS, the router finds Link-ID to that AS and writes the id into Path Link-ID field.

As this suggested method using Link-ID, there are several advantages over the original Pi. First is the unnecessary of IP hashing. Even if the hashing is necessary in the path Link-ID field when the size of internal BGP Link-ID table is large, the load of the router is much less. Second is unnecessary of edge marking process. As the ambiguousness of each path is decreased according to the clearness of the initial router field, the representation of initial router is the only thing that needs to be considered. Third is unnecessary of nearby routing marking process. As the Link-ID is based on the AS unit, the probability of overwriting is much less. These advantages of proposed method, the uniqueness of each path can be guaranteed than the original Pi. Therefore the filtering packets which are not from attackers for the non discrimination of path identity from the attack path can be reduced.

SIMULATION RESULTS

Simulation environment: In order to simulate the proposed method, we use SSFNet simulator [6]. Based on this simulator, we employ 2000 hosts using 20 ASs. The basic routing protocol is OSPF and the packet marking function is installed on each BGP routers. The attack scenario is assumed like this. The victim is a web host serving http service using DNS. Each host in the networks produces the background traffic. The attacker employs two slave systems from other AS. The packets are marked by BGP routers and the victim filters the attack packets using this information marked by routers.

Figure 4 shows the simulation test environment on SSFNet. Attacker is in the network marked as 7 and the victim is in the network marked as S1.

Simulation results: The result of simulation is shown in Fig. 5. In Fig. 5, the attacks occur two times. When the defense mechanism does not employed, the victim is flooded with packets which are over 10000. With the proposed method, the number of packets is reduced to less than 4000. But this number is bigger than the original Pi. As the path identities can be discriminated better than the Pi, the innocent requests need not to be filtered.

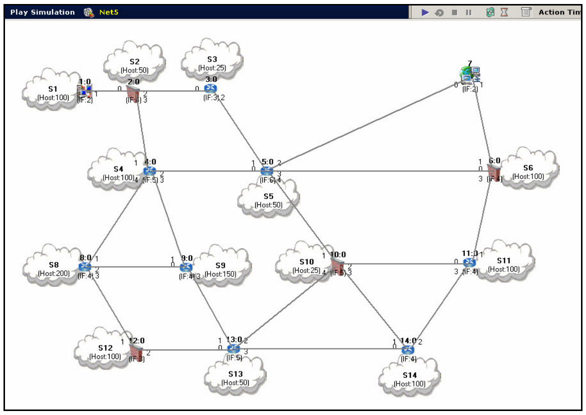

Fig. 4: Simulation Environment

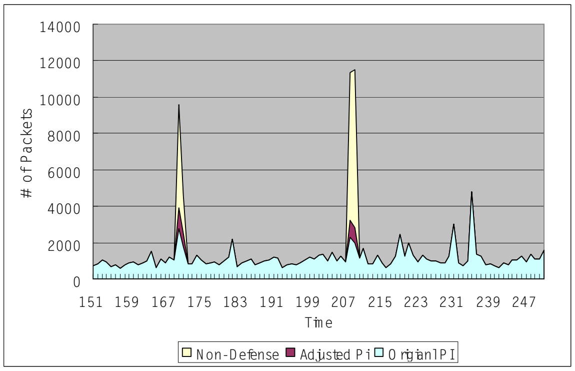

Fig. 5: Simulation Results from the experiments.

CONCLUSION

DDoS means the attack which drains the victim's capability of responding the service request using packet floods to consume network and server resources. In order to guard the victim from these attacks, the victim should know which request to answer and which request to ignore. The path identification is one of the most effective solutions for this object. However, the router's IP address that the Pi uses to mark the path is too large to write into the packet's limited space. The disadvantage of writing routers' IP addresses into the limited space may result the same path identification for different paths. The proposed method of marking path using each router's Link-ID can make a unique identity for each path. With these more specific path identities, the DDoS attacks can be protected more effectively.

ACKNOWLEDGEMENT

This research is supported by the ubiquitous autonomic computing and network project; the Ministry of Information and Communication (MIC) 21st Century Frontier R&D Program in Korea.

REFERENCES

1. Mirkovic, J., J. Martin and P. Reiher, 2004. A Taxonomy of DDoS Attack and DDos Defense Mechanisms. ACM SIGCOMM Computer Comm. Review 34(2).
2. Yaar, A., A. Perrig and D. Song, 2003. Pi: A Path Identification Mechanism to Defend against DDoS Attacks. Proceedings of Symposium on Security and Privacy, pp: 93-107
3. Savage S., D. Wetherall, A. R. Karlin and T. Anderson, 2000. Practical network support for IP traceback. SIGCOMM, pp: 295-306
4. Savage S., D. Wetherall, A. Karlin, and T. Anderson, 2001. Network support for IP traceback. IEEE/ACM Trans. Networking, 9(3), pp. 226–237
5. El-Gendy M. A., and K. G. shin, 2002. Equation-Based Packet Marking for Assured Forwarding Services. IEEE INFOCOM'02, pp: 845- 854
6. SSFNet http://www.ssfnet.org/ last access 2004-11-21
7. Oe M., Y. Kadobayashi, S. Yamaguchi, 2003. An implementation of a hierarchical IP traceback architecture. Proceedings of Applications and the Internet Workshops, pp :250 - 253
8. Belenky A, N. Ansari, 2003. On IP traceback. IEEE Communications Magazine. 41(7): 142 - 153
9. Belenky A., N. Ansari, 2003. Tracing multiple attackers with deterministic packet marking (DPM) Communications. Computers and signal Processing, 1(1): 49 - 52
10. Bellovin S., M. Leech, and T. Taylor, 2001. The ICMP traceback message Internet-Draft, October 2001. Work in progress, available at ftp://ftp.ietf.org/
11. Dean D., M. Franklin, and A. Stubble, 2002. An algebraic approach to IP traceback. ACM Transactions on Information and System Security, 5(2):119--137
12. Micah A., 2002. Tradeos in probabilistic packet marking for IP traceback. In Proceedings of 34th ACM Symposium on Theory of Computing (STOC), pp: 407-418