Research on DPM Algorithm Based on Abnormal Flow in IPv6 Network

Hai-xu Long, Shao-qing Meng*, Kai Zhao, Kai-ning Lu
Information and Network Center, Tianjin University
Tianjin, China
e-mail: remilia@tju.edu.cn

Hui-li Sun
Tianjin Medical Devices Quality Supervision and Testing Center
Tianjin, China

Abstract—Distributed denial of service attack has become one of the most serious security threats in the network. This paper researched distributed denial of service under IPv6 network, improved the deterministic packet marking algorithm that existed in IPv4 network and applied it to IPv6 network. Detection of abnormal flow in the network can make the basic deterministic packet marking algorithm improved. Theoretical analysis and experiment show that the algorithm is effectively to packet marking in the IPv6 network and reduce the resource consumption of network and router.

Keywords-IPv6; distribute denial of service; abnormal flow; DPM

I. INTRODUCTION

With the rapid development of network technology, the IPv4 protocol is unable to meet the needs of people, and the IPv6 protocol come into being. Though security issues were taken into consideration in IPv6 protocol, DoS/DDoS attacks and other security threats still exist in IPv6 network. DoS is an attack mean that attacker deliberately caused the network cannot provide the required services to the user or service performance degradation through specific means. DDoS attack is still DoS attack, but it refers to more than one zombie hosts launch DoS attacks at the same time, the zombie hosts are controlled by an attacker [1].

IP address spoofing existing in the most of DDoS attacks and IP address in attack packets are often forged, so other means to track the attacker's source IP are required. P.Ferguson and D.Senie proposed DDoS defense thinking based on false IP address tracking [2].Savage proposed PPM (Probabilistic Packet Marking) algorithm for the flood type DDoS attack in the IPv4 network, sample the part of attack packets and mark the path information, finally reconstruct the complete attack path on the victim side [3]. The basic principle of DPM (Deterministic Packet Marking) algorithm is mark each packet when it pass through the border router, reconstructed the ingress address of the source of the attack on the victim side. To apply above classical algorithms in IPv4 network to IPv6 network needs to make some modifications to the algorithm.

This paper has researched on the application of DPMalgorithm in IPv6 network, proposeda DPM algorithm based on abnormal flow, move mark information to the IPv6 destination option header. Only marking abnormal flow can improve the efficiency of packet marking and reduce the burden of network resources and border router.

II. IPTRACING TECHNOLOGY OVERVIEW

A. The Classification of IP Tracing Technology

IP tracking technology can be divided into two categories: proactive tracking and reactive tracking [4]. Proactive tracking record information when packets were transmitted. When under attack, reference to the previously recorded information can trace the source of the attack. Packet marking and ICMP tracking are two typical proactive tracking. Reactive tracking begin to trace after the attack. Mostly DDoS attack is initiated by the zombiehosts, reactive tracking is backtracking from the end to the source, looking for the real attacker is not easy. In addition, scholars have put forward a number of tracing algorithms recently, such as logging, link test, ICMP tracing, packet marking [5]. Where the research focus is the packet marking algorithm, because compared with other algorithms it has many advantages, such as use less bandwidth and computing resources, do not need coordination between the ISPs, allow analysis after attack. But cannot be directly applied in IPv6 network is its disadvantage.

B. DPM Algorithm Summary

The basic principle of DPM algorithm in IPv4 network is: when packets entering the network, edge ingress router will mark the packet and divide its IP address (ingress address) into two sections, then write it into 16-bit ID field. Sections mark will be written in 1-bit RF field. The main difference between DPM algorithm and PPM algorithm is: the former is only used in edge ingress router, mark ingress address and reconstruct it on the victim side; the latter isused in all routers, mark the identity of the router and reconstruct attack path on the victim side. It can found that DPM algorithm marking process is efficiency from the above difference. But DPM algorithm just reconstruct edge ingressport address, not the attack source address. When the attack source is locked, how to find the attacker is the problem need to solve.

III. DPM ALGORIRHM BASED ON ABNORMAL FLOW

A. Selection of Storing Field and Mark Encoding

In the DMP algorithm based on IPv4 protocol, the mark information is stored in 16-bit ID field and 1-bit RF field. But ID field and RF field are not existed in IPv6 header, it is needed to find a new area to store mark information. As defined in RFC 2460, only 8-bit traffic class field and 20-bit

flow label field is undefined [6]. But using 28-bit space to store 128-bit IPv6 address coding requires a lot of computing resources. Therefore, mark information stored in IPv6 header is not suitable [7]. There are several extension headers defined in IPv6, only destination option header and hop-by-hop option header are not be defined how to use. This paper chooses the destination option header as the information storage area. Destination option header encoding format is shown in Fig. 1.

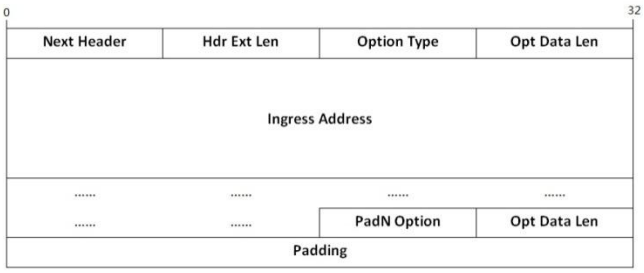

Figure 1. Mark encoding format.

Fig. 1 shows the format of a destination option header used for storing the ingress address. If next header field is set to 59, it indicates this header is the last header; if next header field is set to 60, it indicates next header is a destination option header. Option type field is set to 00011110. The first and second bits of the option type field indicate that if this field cannot be recognized, the router will skip option type field; the third bit can make sure option type field may not be changed during routing; the last five bits of option type field are allocate by Internet Assigned Numbers Authority [8]. The next is 128-bit ingress address, if it is need to mark more than one edge router, just write option type field and option data length field behind the ingress address, then another ingress address can be written. Finally, to make sure the length of destination option header is an integer multiple of 8-byte, some padding bits need to be adding. PadN option is set to 1, that indicates the length of the padding bits needs to be greater than 1-byte, and the following option data length is padding bits length. For example, if marking only one edge ingress address, the padding bits will be 4-byte field encoding with 0.

B. Modification on Path MTU Algorithm

IPv6 protocol uses ICMPv6 message to advertise packet errors encountered in the process of forwarding and providing a simple parameter loopback service for error correction [9]. PMTU is the minimum of all MTU of the path from source node to destination node. In IPv6 network, if the router forward packet is larger than PMTU, the router will discard the packet and send the ICMPv6 Packet-too-big message to the packet source. Network interface MTU and discarded packet leading part are stored in ICMPv6 Packet-too-big message, these information can be used to achieve PMTU discovery and modification. The mark information inserted may result the packet discarded by the router. To avoid such case, the PMTU discovery process needs to bemodified. When write one ingress address in destination option header, the packet increasing length is 24 bytes, choose 24 bytes as the minimum value to recalculate the PMTU.

PMTU value is set to 1280 bytes, because RFC1981 is recommended to use 1280 bytes as the PMTU value, which can effectively prevent the occurrence of fragmentation. When the length of packet is larger than the PMTU value, check this node supporting PMTU discovery algorithm. If it does, MTU increases 24 bytes then notices its neighbors. If not, need to get its existing PTMU value, then using the network interface MTU information in ICMPv6 packet-too-big message to complete the modification of the PMTU value.

C. Detection of Abnormal Flow

One of disadvantages of the DPM algorithm is edge router will mark every packet when network is not be attacked. When attack occurs, the normal packet entering the network will also be marked [10], this will increase the burden on edge router and reduce network performance, even cause paralysis of the network when attack occurs. The router can only mark suspicious packets after detect abnormal flow to reduce its burden. Research on flooding type DDoS attack in IPv6 network should use flood DDoS attack flow characteristics to analyze abnormal flow. [11] has researched on net work flow characteristics of the flood type DDoS attack. It is shown in Fig. 2.

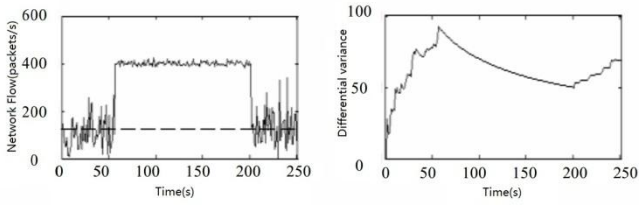

Figure 2. Network flow characteristics.

Fig. 2 shows that when the network is normal, network flow fluctuates on an average. DDoS attack occurs on the 50 second, the network flow burst increase to approximately twice as normal network flow, then maintain a high value. Network traffic differential variance gradually decreases. Using the above flow statistical can complete the process of starting and stopping DPM marking.

D. Procedure

When the router forwarding the packet, sample to the packets, denoted as$f(t)$. I_{min} is a value slightly greater than normal average value, called DPM mark threshold. If $f(t) < I_{min}$, do not start DPM mark algorithm and continue to sampling. Because of normal traffic flow fluctuates on an average, delay a period of time and then determine again can greatly reduce the probability of the false attack report. When network flow exceeds the threshold, DPM algorithm will further increase the burden on the router, need to set a maximum flow value I_{max}, called the alarm threshold. If network flow exceeds the threshold, stop the DPM algorithmand alarm to the administrator. When $f(t) > I_{min}$ and $f(t) < I_{max}$, check if $d(t-1)$ greater than $d(t)$,then calculate probability of packet P_i. P_{min} is a

threshold which called mark probability. If $P_i > P_{min}$, mark the packet. Otherwise, determine that this packet is normal. Procedure of DPM algorithm based on abnormal flow is shown in Fig. 3.

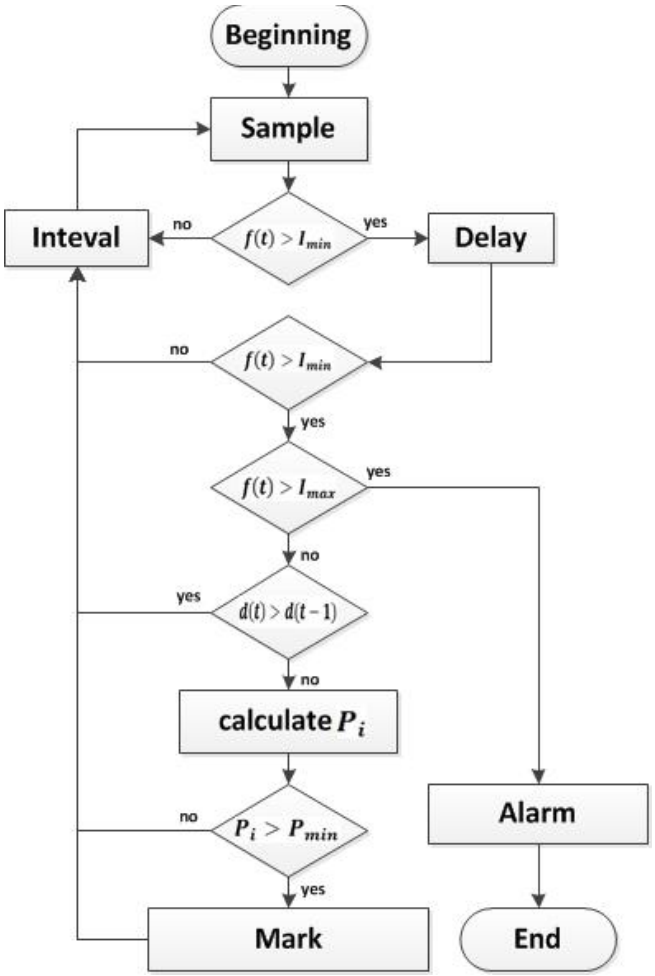

Figure 3. Procedure of DPM algorithm based on abnormal flow.

IV. Simulation Experiments and Results Analysis

A. Simulation Environment

This paper uses NS2 simulation software to simulate DPM algorithm based on abnormal flow. NS2 providessimulation of TCP based on the wireless orwired network, routing and multicast. Some modifications to NS filesneed to be made to simulate the DPM algorithm based on abnormal flow: the ip.cc and ip.h files under the common folderneed to be modified for add destination option header; make supplement to the recv function in classifier class; create DPM agent which inherit agent class to complete the DPM mark process; create UNDPM agent which inherit agent class to extract the ingress address and write it to trace file.

B. Experimental Topology

Experimental topology is shown as Fig. 4.

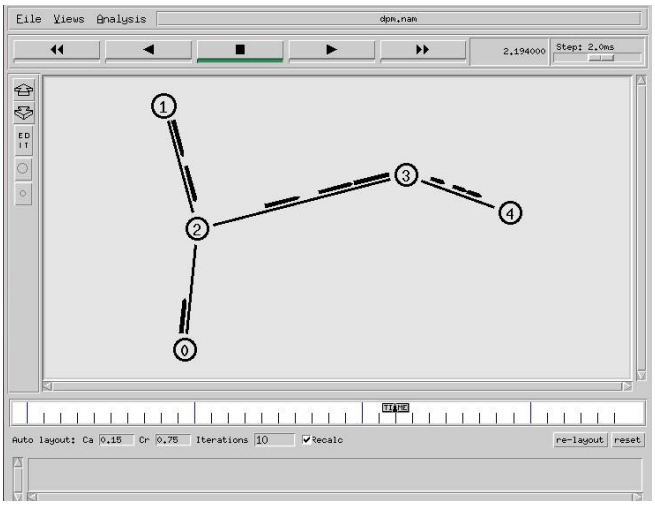

Figure 4. Topology in NS2.

In Fig. 4, node0 is normal user, its IPv6 address is 2000:0:0:1000::2. Node0 connects with one ofnode2 port, its address is 2000:0:0:1000::1. Node0 connects with UDP agent udp0, udp0 connects with flow generator cbr0, cbr0 setting is: packet size 500 bytes and send interval 10ms. The link between node0 and node2 setting is: bandwidth 1Mb, delay 10ms, FIFO. Node1 is attacker, its IPv6 address is 2000:0:0:2000::2. Node1 connects with one ofnode2 port, its address is 2000:0:0:2000::1. Node1 connects with UDP agent udp1, udp1 connects with flow generator cbr1, cbr1 setting is: packet size 500 bytes and send interval 5ms. The link between node1 and node2 setting is: bandwidth 1Mb, delay 10ms, FIFO. Node2 is an edge router, connects with DPM agent dpm0. The port of node2 which connects to node3 IP address is 2000:0:0:3000::2, the corresponding port on node3 IP address is 2000:0:0:3000::1. The port of node3 which connects to node4 IP address is 2000:0:0:4000::2. Node4 is victim, its IP address is 2000:0:0:4000::1. Node4 connects with UNDPM agent. The link between node2 and node3 setting is: bandwidth 2Mb, delay 10ms, FIFO. The link between node3 and node4 setting is: bandwidth 2Mb, delay 10ms, FIFO. Set I_{min} =800Kb/s,I_{max} =1.5Mb/s, P_{min} =0.5. At 0.5s, cbr0 start. At 1s, cbr1 start. At 3s, cbr1 stop. At 3.5s, cbr0 stop. At 5s, finish simulation, close trace and nam files.

C. Analysis of Simulation Result

Simulation result is shown as Fig. 5.

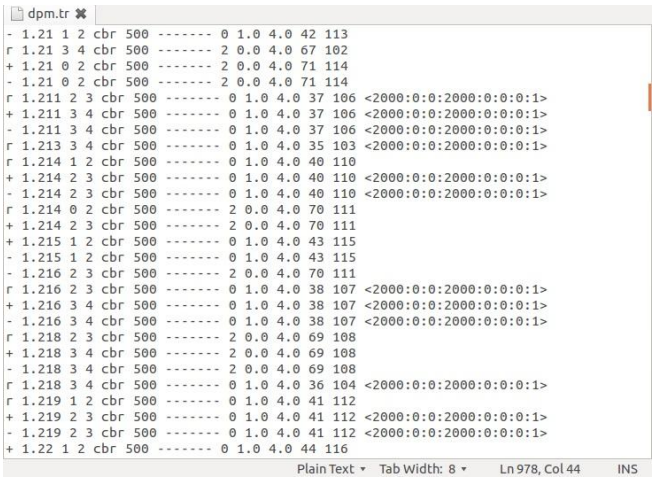

Figure 5. Simulation trace file.

In Fig. 5, after 1.0s, attacker sends a large number of packets which maked network flow exceed DPM mark threshold. Then start the mark algorithm. The algorithm marked packets send from node1 with ingress address. But it did not mark packets send from node0.The result shows that DPM algorithm based on abnormal flow can flexible mark packets andsave network resources.

V. CONCLUSION

Research on DPM algorithm under IPv6 network and a modified DPM algorithm is proposed to trace DDoS attack in IPv6in this paper. Then simulate the modified DPM algorithm, the result shows that the improved algorithm is effective in IPv6 network, can reducing the burden on edge route rnetwork. Network flow characteristics is needed for determine mark threshold and mark probability, it is adisadvantage of this algorithm. The focus of future research is how to measure the mark threshold and mark probability.

REFERENCES

[1] Ting Ding, Guo-ying Feng, and Kai-ning Lu, “Safety analysis and application of the IPv6 campus network based on IPSec,” Journal of Tianjin University, vol. 42 suppl, pp. 28-30, Dec. 2009.

[2] H. Wang,C. Jin,and KG.Shin.“Defense Against Spoofed IP Traffic Using Hop-Count Filtering,”IEEE/ACM TransactionsonNetworking, Jan.2007, pp.180-199.

[3] S. Savage,D. Etherall, and A. Karlin, “Network Support forIP Traceback,”IEEE/ACM Transactions on Networking,Jun.2001, pp.226-237.

[4] T. Baba, S. Matsuda, “Tracing network attacks to their sources,” IEEE Internet Computing, vol. 6, Apr. 2002, pp. 20-26.

[5] L.Chen,T.Longstaff,K.Carley, “Characterization of defense mechanisms against distributed denial of services attacks,” Computer&Security, vol. 23, Dec. 2004,pp.665-678.

[6] S. Deering, R. Hinden, “Internet protocol, version 6 (IPv6) specification,” Network Working Group, RFC2460, Standars Track, Dec. 1998.

[7] You-ye Sun, Cui Zhang, Shao-qing Meng, and Kai-ning Lu, “Modified deterministic packet marking for DDoS attack traceback in IPv6 network,”Computer and Information Technology (CIT), Sept. pp. 245-248.

[8] A. Beleky , N. Ansari, “ Tracing multiple attackers with deterministic packet marking,” IEEE Pacrim’03, Victoria, Canada, 2003, pp. 49-52.

[9] A. Beleky , N. Ansari, “IP traceback with deterministic packet marking,” IEEE Communication Letters, vol. 7, Apr. 2001, pp. 162-164.

[10] R. Stone, “Center trace: an IP overlay network for tracking DoS floods,” Proc. Ninth USENIX Security Symp, 2000, pp. 199-212.

[11] Xin-yu Yang, Lei Li, Guo-dong Zhang, “DoS/DDoS attack flow burst detection in IPv6 network,”Computer Engineering, vol. 34, 2008, pp. 23-25.