Destination Address Monitoring Scheme for Detecting DDoS Attack in Centralized Control Network

Sang-Heon Shim○, Kyoung-Min Yoo, Kyeong-Eun Han, Chol-Ku Kang, Won-Ho So*, Jong-Tae Song**, and Young-Chon Kim

Dept. of Computer Engineering, Chonbuk National University, Jeonju Korea
* Dept. of Computer Education, Sunchon National University, Suncheon Korea
** ETRI BcN Architecture Team, Daejeon Korea

Abstract— As DDoS (Distributed Denial of Service) attack becomes more diversified, the conventional detection methods based on single source router can't detect the attack efficiently. In order to combat this problem, centralized control is required to analyze and collect traffic generated in several source routers. This paper presents defense/detection scenario to protect against DDoS attack in centralized control network. A destination address monitoring scheme is also proposed to detect DDoS attacks in real-time. It measures the number of packets with same destination IP address by using modified Bloom filter. Because the modified Bloom filter uses extra table that manages relation among each address fields of destination IP address, it can reduce wrong detection rate. Simulation result shows the proposed scheme reduces the wrong detection rate than the conventional one.

***Index Terms*— DDoS, Bloom filter, Attack detection.**

I. INTRODUCTION

Recently, the DDoS attack problem has attracted much attention from the research community. Various forms of DDoS attacks have led to an increased need for service diversification and developing techniques to analyze and monitor network traffic.

The motivation of this work comes from a need to detect DDoS attacks. In order to detect malicious attack that uses vulnerability of application program or network system, an efficient analysis tools are required.

On the other hands, as DDoS attack occurs in several hosts simultaneously, centralized control is required to cope with attacks efficiently. Therefore, next generation network (NGN) also adopt a centralized control [1].

In order to accommodate these network condition, we presents DDoS attack defense/detection scenario in centralized control network. The NCP is defined as the system that offers a centralized control function in this paper. The NCP collects traffic that destined to each source router and controls the whole network by performing synthetic analysis and judgment.

We also propose the abnormal traffic detection scheme. The proposed abnormal traffic detection scheme is first-hand destination address monitoring scheme. Unlike the conventional schemes, which manages each of address fields in destination IP address separately, our scheme uses extra table that manage the relation among address fields of destination IP address. Due to using extra table, it can detect abnormal traffic exactly and lower the wrong detection rate.

This paper is organized as follows. Section II gives an overview of related works. In section III, we describe the structure and defense/detection scenario with respect to centralized control network. Our destination address monitoring scheme to detect abnormal traffic is proposed in section IV. In section V, we illustrate the simulation results. Section VI is a concluding remark.

II. RELATED WORK

To detect abnormal traffic in source router, network monitoring tools such as Netflow or MRTG (Multi Router Traffic Grapher) are widely used. These tools measure quantity of TCP, UDP or ICMP traffic among the generated traffic and sort IP addresses which cause a great quantity of traffic by analyzing the characteristic of packets. In order to monitor the network traffic, 5-tuple (source address, destination address, protocol type, source port number and destination port number) has to be analyzed. Therefore, these network monitoring tools offer functions that collect and analyze the 5-tuple. However, if the transmission capacity of a router is large, the efficiency of these tools shrinks sharply because they monitor 5-tuple with respect to all transit packets.

On the other hands, monitoring schemes based on destination address to detect the DDoS attack in real time have been proposed. The representative schemes are IDR (Intrusion Detection Router) [2, 3] and MULTOPS (Multi-Level Tree for Online Packet Statistics) [4].

Firstly, MULTOPS uses a four-level 256-ary tree to monitor the IP address space at successive levels of detail. But, since it allocates memory dynamically, memory management can be a computational burden for heavily loaded routers. The MULTOPS data structure can also become the subject of memory exhaustion attack if large number of nodes are expanded. In addition, delay is introduced when a node is expanded due to the monitoring time required to gather statistics for each new address range.

Secondly, IDR scheme detects the DDoS attack by using Bloom filter. Whenever packet is generated, it converts the destination address to index value of table by using predefined hash function and increases the value of relevant space by 1. Without the loss of generality, the relevant space will be called

bin in this paper.

In IPv4 addressing, each IP address is 32 bits long detached by dot every 1 byte (equivalently, 4bytes). We name each byte as 'separate filed'. Figure 1 shows Bloom filter structure that is used in IDR.

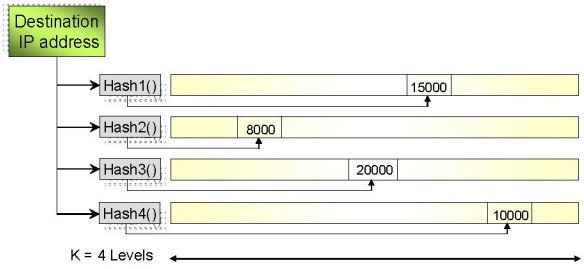

Figure 1. IDR's Bloom filter structure

The Bloom filter structure of IDR consists of two-dimensional arrays having dimension [k][m], where 'k' represents separate field and 'm' represents the number of *bin*s[3]. In this method, k is set to 4 and m is set to 256 for simulation. Accordingly, array is divided into 4 tables and each table has 256 bins. Hash_i() plays the role to change separate field of IP address (0~255) to table's index value. According to the result of the Hash_i() function, relevant bin's value increases by 1. If all counter values of 4 bins exceed certain threshold, the additional packets destined for the destination address is considered as an attack traffic.

By the way, since IDR maintains the separate fields independently, the counter value of a *bin* may not increase by unique IP address but by different IP address. For instance, we can assume the flows of addresses such as (100.xxx.xxx.xxx, xxx.50.xxx.xxx, xxx.xxx.200.xxx and xxx.xxx.xxx.150) are generated many times. Suppose that IP address (100.50.200.150) is generated for the first time. In this case, this packet is regarded as attack traffic because the counter value of relevant *bin* of each separate field already exceeds the threshold. To solve this problem, we propose a new destination address monitoring scheme that can manage relation among separate fields.

In this paper, we describe only a scenario about centralized control network and focus on the successful detection of DDoS attack. Other module (NCP's architecture, defense scheme) is in progress and will be reported in sequel papers.

III. CENTRALIZED CONTROL NETWORK: STRUCTURE AND ATTACK DETECTION SCENARIO

A. *The structure of centralized control network*

The structure of centralized control network is shown in figure 2. The main function of centralized control network is as follows. Each edge router collects the information of flow (The group of packets distinguished by Source IP address, Destination IP address, Source Port, Destination Port, and Protocol) and transmits the flow's information to the NCP (Network Control Platform).

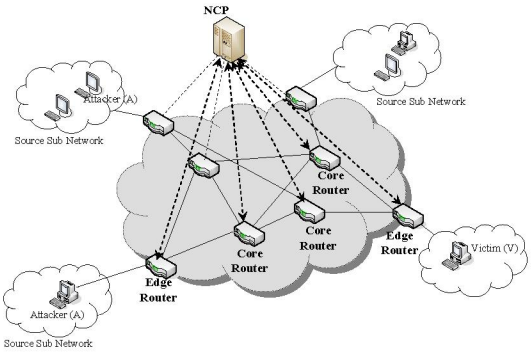

Figure 2. The structure of centralized control network

The NCP analyzes the flow information that it receives from the edge routers and controls the flow. Since there are too many flows transmitted to the NCP, an efficient scheme which monitors only flows with attack traffic is required. In case of monitoring normal traffic as well as abnormal traffic, lots of system resources can be utilized unnecessarily. Therefore, to reduce the waste of system resources, in section IV, we propose an efficient detection scheme that monitors only the abnormal traffic.

B. *Detection/defense scenario of centralized control network*

Figure 3 is the detection/defense scenario for centralized control network.

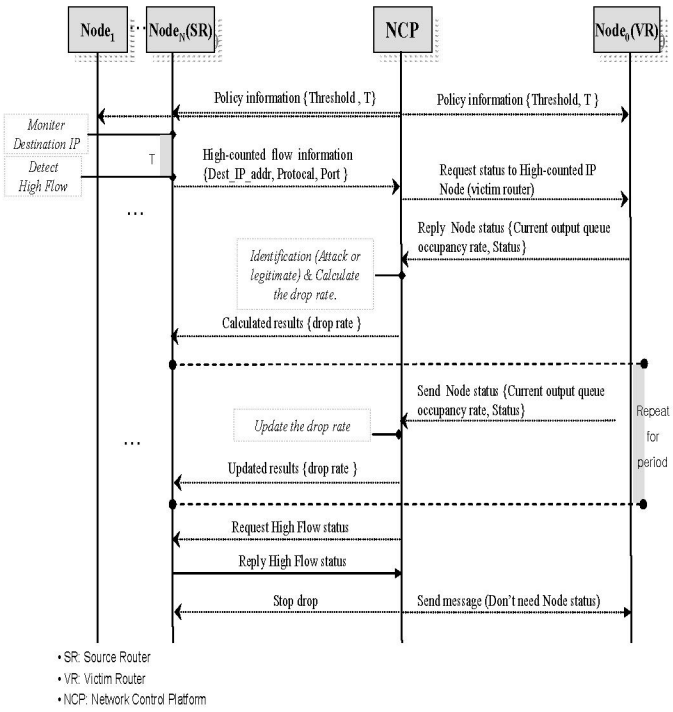

Figure 3. Detection/defense scenario with Bloom filter scheme

In this scenario, NCP calculates policy information (threshold and period) to apply for each edge router and transmits policy information to each edge router. Each edge router applies the policy information and monitors to find the

abnormal traffic by analyzing amount of packets generated from sub-network. If edge router detects abnormal traffic, then it transmits the detected traffic information to NCP. NCP analyzes the information and requests the victim router (VR) to transmit status information (current output queue occupancy rate, drop rate of queue etc). After receiving the status information from destination router (VR), NCP judges whether the status is an abnormal status or not. If the status information indicates that the destination router is being attacked, NCP transmits the calculated drop rate for eliminating abnormal traffic to each source router (SR). Drop rate depends on the input queue's status of the destination router (VR). After predefined time, destination router transmits the status of itself to NCP and then NCP analyzes the status information transmitted from destination router (VR). Afterwards, NCP calculates a new drop rate and transmits the drop rate to source router (SR) again. In addition, NCP analyzes the information of abnormal traffic transmitted from source router (SR) and decides whether to regulate the traffic continuously.

IV. PROPOSED ABNORMAL TRAFFIC DETECTION SCHEME

To implement the proposed scheme, a source router is divided into IP Bloom filter module and statistics module. Figure 4 shows the diagram of our proposed scheme executed in source router.

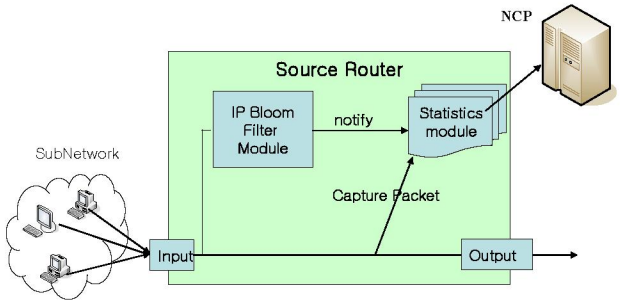

Figure 4. Structure of system using proposed scheme

IP Bloom filter module receives packets that enter the source router and monitors by measuring packet's amount based on destination IP address. The result of monitoring is notified to the statistics module. Statistics module only monitors those packets regarded as abnormal destination IP address and grasps packet's detail information such as source port, destination port and protocol.

Figure 5 is a structure of IP Bloom filter module used in the proposed scheme.

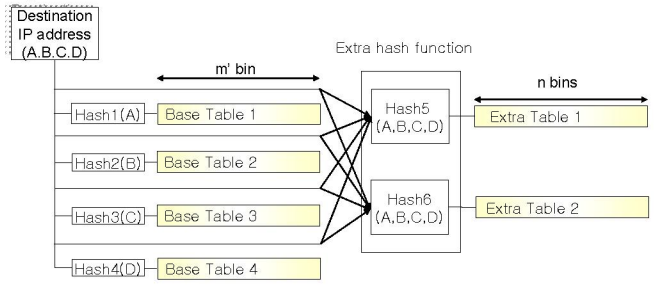

Figure 5. Enhanced Bloom filter structure

The proposed Bloom filter module consists of base table and extra table. Operational function of base table is defined equally with the function of IDR method. Extra table uses hash function to extract relation among separate fields of destination IP address. Proposed scheme reduces the number of base table's bins in comparison with existing scheme. Instead, the reduced bins of base table are used for extra table. Finally, our scheme occupies the same memory space as existing scheme. The result value of extra hash function is converted to extra table's index value, in the same way as base table and increases the counter value of extra table's bin by 1. The work about optimal extra hash function for extra table is under progressing.

If the number of packets with the same destination IP address exceeds a certain threshold, the IP Bloom filter module will take them as abnormal traffic and informs the relevant IP address to statistics module. The statistics module analyzes and classifies according to components of the packet (i.e. source IP address, destination address, protocol, source port number, destination port number, and average packet size etc). After finishing the process of statistics module, the source router informs the processed results and abnormal traffic's occurrence to NCP simultaneously.

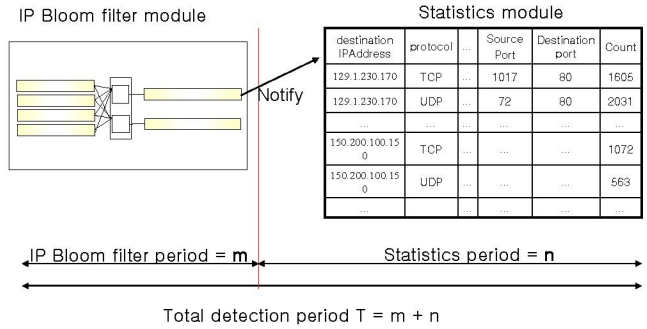

Figure 6. Relation of IP Bloom filter module and Statistics module during detection sampling period (T).

Figure 6 shows the correlation of IP Bloom filter module and statistics module during the sampling period (T). The sampling period 'T' is the sum of IP Bloom filter module's detection sampling period 'm' and statistics module's detection sampling period 'n'.

Figure 7 shows the flow chart of proposed detection algorithm. The operations of our scheme are as follows.

1. Each separate field of destination IP address of generated packet divided by dot is called as A.B.C.D and is converted to index values (a, b, c and d) by hash function.
2. Index values (a, b, c and d) become each base table's index. Once the index value is calculated, the bin's value increases by 1.
3. At the same time, extra table's index value (i, j) is calculated by using extra hash function. Extra table's index value is used as an index of extra table and increases the value kept in corresponding bins of extra table by 1.
4. After increasing the value of corresponding bins of 4 base tables and 2 extra tables, if the value of all bins exceeded the threshold, the packets that are destined toward the IP address (A.B.C.D) are regarded as abnormal packet.

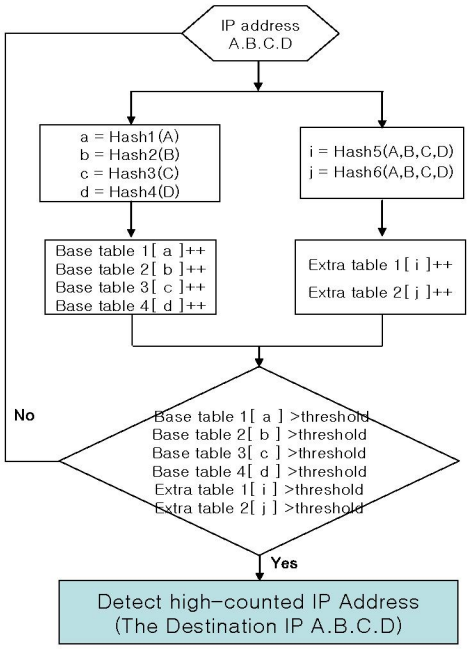

Figure 7. The flowchart of proposed abnormal traffic detection algorithm

V. SIMULATION AND PERFORMANCE ANALYSIS

For fairness of performance estimation, we make a simulation model, in which, the bin's number is the same with that in the existed scheme. The conventional scheme uses 4 tables that have 256 bins but the proposed scheme uses 4 base tables having 128 bins and 2 extra tables having 256 bins. The simulation is executed in Pentium 4, using java (jdk1.4.2) and total 50,000 packets of 3 kinds are generated during the sampling period T.

The simulation scenario is as follows.

1. Background packet: Background traffic was formed by random IP numbers between 0 ~ 255. Background packets are generated in total 38,000 times.
2. Suspicious packet: To verify the scheme's accuracy, we define suspicious packets that are similar to abnormal packet. Although the packets are normal, they might be misunderstood as abnormal packets due to their excessive packet generation in normal state. In this simulation, totally 10,000 suspicious packets are generated during sampling period T.
3. Abnormal packet: Generally, the packet with the object of attacking aims for one destination IP address during sampling period T. In this simulation, we set the 2 independent attack IP addresses each of 1000 attack packets.

For the proposed scheme's performance estimation, we compare the simulation result of proposed scheme with the IDR scheme. The table 1 shows abnormal IP addresses detected by IDR scheme.

Table 1. The simulation result of IDR scheme

Detection type	Detected IP address number	
Wrong detection (normal IP address)	150.200.100.110	129.200.100.170
	60.210.230.150	129.200.230.150
	150.200.230.170	150.200.100.120
	60.210.230.170	129.1.100.150
	60.210.190.150	150.1.100.170
	60.210.190.140	60.210.190.110
	150.200.100.140	150.200.100.160
	60.210.190.130	60.210.230.160
	150.200.100.130	60.210.190.120
Correct detection (abnormal IP address)	129.1.230.170	150.200.100.150

As shown in table 1, in IDR scheme, the number of IP addresses detected as attack traffic are total 20. However, actually the number of abnormal IP addresss are 2. Hence, 18 IP addresses are detected as wrong.

Table 2. Simulation result of proposed scheme

Detection type	Detected IP address number
Wrong detection (normal IP address)	150.200.100.140
Correct detection (abnormal IP address)	129.1.230.170
	150.200.100.150

Table 2 shows simulation result of proposed scheme. As we see, detected abnormal IP addresses are 3. Among them, two abnormal IP addresses are correctly detected and one normal IP address is detected as wrong. We simulated several times repeatedly in the same environment altering IP address number of abnormal packets and normal packets. The wrong detection in IDR scheme is 17 on the average. But the wrong detection in the proposed scheme is less than 1 on the average and thus we can verify that our scheme is more accurate.

VI. CONCLUSIONS

In this paper, we presented defense/detection scenario to cope with DDoS attack in centralized control network

We also proposed the destination address monitoring scheme based on modified Bloom filter. As the modified Bloom filter uses extra table that manages relation among each address fields of destination IP address, it can reduce wrong detection rate. In simulation, the proposed scheme shows lower wrong detection rate than the conventional one.

As a result of our proposed scheme, each source router simply collects the information of abnormal traffic in real- time. We confirmed that our proposed scheme detects abnormal traffic accurately. The study of centralized control network using NCP is in progress.

REFERENCES

[1] Podhradsky, P, "Migration scenarios and convergence processes towards NGN (present state and future trends)", Electronics in Marine, 2004. Proceedings Elmar 2004. 46th International Symposium, pp.39 - 46, 16-18 June 2004.

[2] Abdelsayed S, Glimsholt D, Leckie C, Ryan S, "An efficient filter for denial-of-service bandwidth attacks", IEEE Global Telecommunications Conference, 2003(GLOBECOM '03) Vol. 3, pp.1353 - 1357, 1-5 Dec. 2003.

[3] Chan EYK, Chan HW, "IDR: an intrusion detection router for defending against distributed denial-of-service (DDoS) attacks", Parallel Architectures, Algorithms and Networks, 2004, 10-12 May 2004.

[4] Thomer M. Gil and Massimiliano Poletto, "MULTOPS: a data-structure for bandwidth attack detection", Proceedings of the 10th USENIX Security Symposium, pp. 23-38, August 2001.