A Traffic Mitigation Method for DDoS Defense in Large Autonomous System

Ho-Seok Kang and Sung-Ryul Kim*
Konkuk University, Seoul, Republic of Korea
hsriver@gmail.com, kimsr@konkuk.ac.kr

Abstract

Distributed Denial of Service (DDoS) attacks generate enormous traffic by a large number of agents and can easily exhaust the computing and network resources of a victim within a short period. DDoS attack is more difficult to be detected and blocked than other attack method. Therefore, we designed three new methods being able to tolerate the DDoS attack during its detecting and being blocking. With regard to DDoS attacks into Autonomous System (AS), we deploy routers for traffic distribution in connection with Border Router. This structure reduces DDoS attack traffic by protecting not only victims but also network resources. Moreover, in this paper, we also propose a method to reduce traffic in each router.

Keywords: DDoS Attack, DDoS Detection, Traffic, Mitigation Method, AS

1 Introduction

The main aim of DDoS attack is disruption of services by consuming the bandwidth of legitimate client. DDoS attacks may use many different approaches to achieve the disruption of normal services. Their two major goals are to consume bandwidth and overwork the server. Consuming bandwidth can be done using any traffic types. Most of the “zombies” in a DDoS army will send the same kinds of traffic.

DDoS attacks pose an immense threat to the Internet, and many defense mechanisms have been proposed to protect the problem. Attackers constantly modify their tools to bypass these security systems, and researches in turn modify their approaches to handle new attacks. The DDoS field is quickly becoming more and more complex [7]. So, the perfect blocking of DDos attack is almost impossible because of the differentiation between normal and suspicious traffics. The unconditional blocking of mass traffics keeps some users from service inevitably, which is corresponding to success of DDoS attack to some extent. The perfect blocking of DDos attack and maintenance of service, therefore, requires the system to tolerate attacks until the blocking of attack is achieved [1].

Mostly, blocking of DDoS attack is performed in the victim server because major sites or specific servers such as DNS come major target of DDoS attacks. However, DDoS traffic is mostly transmitted to the server even though the victim server blocks traffic. This causes a decrease in the speed of the whole network and more seriously may prevent the network operation.

Therefore, although methods for perfectly detecting and blocking these DDoS attacks are also important, a system to mitigate DDoS attacks traffic is required. The mitigation system should respond not only to DDoS attacks but also to much traffic under normal conditions. Moreover, methods to mitigate them at the border router are required to protect not merely victim servers but also network bandwidth and resources in AS. In order to protect all resources in AS from DDoS attacks and at the same time to satisfy these requirements, this paper proposes several methods to mitigate DDoS attacks as follows:

Research Briefs on Informaiton & Communication Technology Evolution (ReBICTE), Vol. 1, Article No. 11 (January 15, 2015)

[*] Corresponding author: 1305 New Millennium Hall, Konkuk University, 120 Neungdong-ro, Gwangjin-gu, Seoul 143-701, Republic of Korea, Tel: +82-(0)2-450-4134

The first is to solve them by a system structure method. In this method, when traffic is concentrated on a specific router by structurally adjusting routers in AS, several routers share the traffic each other. The second is to aggregate the packets moving toward the same destination using aggregation in all routers. The third is to aggregate or drop packets to trigger DDoS packets or excessive traffic through cooperation between routers in the first system structure. We designed an automatic mitigation system based on the traffic amount at each stage by integrating these three methods.

The rest of this paper is organized as follows. In section 2, we explain some previous works in traffic mitigation method. Section 3 provides three new mitigation methods for defensing DDoS attack. Finally, we conclude in section 4.

2 Related Work

It is difficult to detect and block DDoS attacks immediately because network traffic is not necessarily increased by DoS or DDoS attacks. This is because normal network traffic is likely to increase. Therefore, techniques to mitigate DDoS attacks are required to protect specific servers and network resources before detecting DDoS attacks.

In previous studies [9, 3, 10, 4, 8], damage was mitigated by searching signatures of all malicious codes, detecting and blocking attacks in order to defend against DDoS attacks. In this method, detection and blocking are performed by accurately separating normal packets from malicious codes. Therefore, although normal packets are seldom blocked, services cannot be performed frequently without being able to detect DDoS attacks. In other words, these methods are not appropriate to mitigate DDoS attacks [9].

Methods [10, 4] among these methods detect DDoS attacks according to the detection rule using victim and attacker IP addresses. Based on these accurate addresses, router blocks them. However, in this method, the detection rule may not be formed because of depending on the strength of DDoS attacks. In particular, they can be perceived only in the network around victim nodes and are not likely to be able to activate services [9].

Methods [6, 2] use traffic aggregation, and the same destination IP and packet traffic aggregation are forced to drop to take responsibility for the congestion when link congestion is detected. ACC [6] and [2] allocate bandwidth using the destination IP and prefix, respectively. Packets over the allocation drop when excessive traffic occurs. However, in fact, traffic in specific servers or networks can be concentrated in a certain time or a specific day. Therefore, in this case, normal traffic requiring beyond the allocated bandwidth can be removed because they are mistaken for DDoS attacks [9].

In these studies, it is difficult to mitigate DDoS attacks using heavy traffic in many zombie servers in real-time. Moreover, it may cause blocking of normal traffic. Above all, it is difficult to reduce the burden not only on the victim servers but also on the whole network in AS. Therefore, this paper proposes several methods to mitigate DDoS attacks more effectively.

3 Proposed Methods

Network managers try to protect network resource, router and major servers, against defending DDoS attack in the Autonomous System. They are monitored and blocked suspicious traffics. And they are watched some suspicious hosts as zombie PCs. However, the blocking of all the DDoS attack is almost impossible. Therefore, a traffic mitigating method need to necessary until the attack is confirmed to be DDoS attack. In this section, we propose three traffic mitigation methods for defending DDoS attack. Figure 1 shows a normal AS structure.

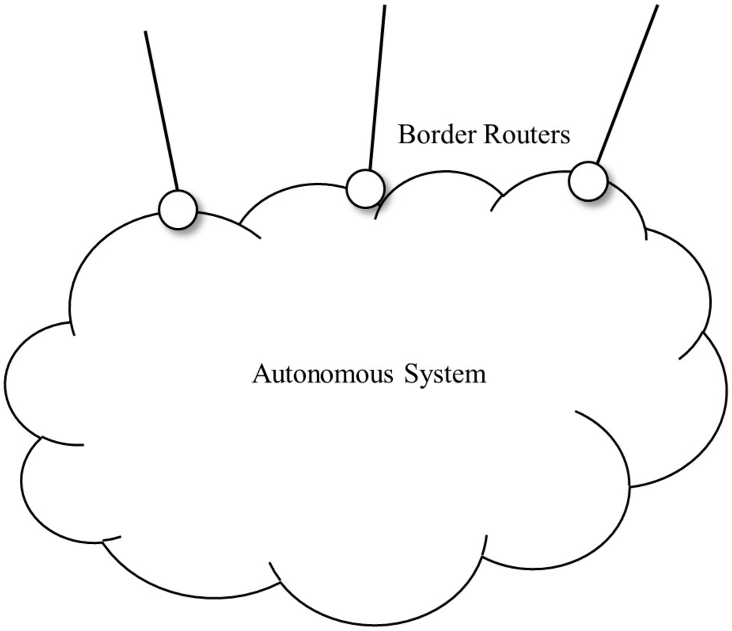

Figure 1: A Normal Autonomous System Structure

3.1 Traffic Sharing Method

This method is to distribute traffic without structurally modifying the existing routers in AS, a network management unit. Figure 2 shows the overall structure of the traffic sharing method. A specially made router capable of distributing traffic between the border routers connected to external AS and inner border routers. We call this router as Traffic Control Router (TCR). TCRs play a role not only in preventing DDoS attacks but also in distributing the load on the entire network in AS when a large amount of traffic enters inside AS.

TCR works using normal routing algorithms under normal conditions. However, A TCR distributes traffic by transmitting the overall traffic to another adjacent TCR when traffic over α (traffic amount previously set by the administrator) passes them. If traffic over β similar to DDoS attacks occurs in this system, TCR transmits the traffic to all other TCRs. The traffic is transmitted by tunneling or source routing. The each TCR performs the following roles:

- All TCRs monitor structure and traffic of their sub-network. They should be recognized it by using "trace route" in order to determine the load capacity of sub-networks in AS.
- The TCRs should distribute incoming traffics equally to their inner border routers.
- If the traffics exceed the amount of the capacities of sub routers, the exceed traffics are distributed to nearby TCRs by tunneling method.
- When the transmitted traffic from nearby TCRs exceeds the capacity, some traffic must be dropped.

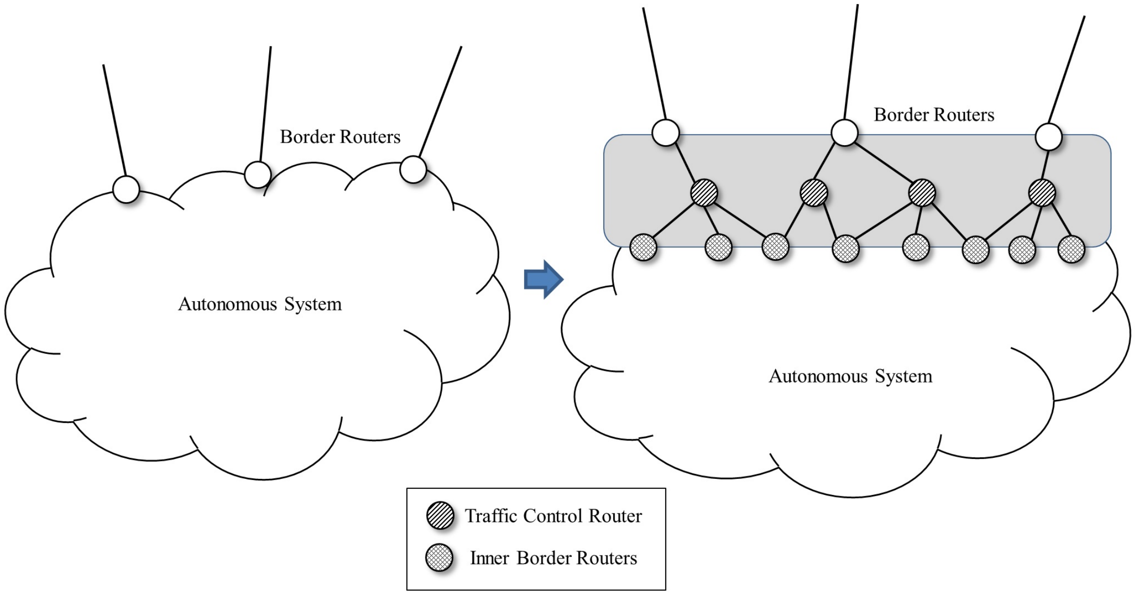

Figure 2: The AS Structure using Traffic Sharing Method

- The dropping traffics are selected from overlapped and repeated packets under the policies set by AS operators.

If some traffic is not dropped in TCRs on DDoS attack, systems nearby victim and victim are damaged from DDoS attack. So, TCR delay the traffic. Then it chooses some dropping traffics and dropped. The selection of traffics to be dropped is very important issues. If some meaningful packets are dropped in this process, attacker is said to be satisfied to some purpose. The selection method is shown as follows:

- Random Selection
- Duplicated Packet Selection (Destination Address, Port Number etc..)
- Stream Traffic First Selection
- Control Message First Selection

The selection of appropriate method is dependent on the factors such as amounts of traffic and processing time during delay. The advantages and limitations of this method are as follows:

- The traffics by DDoS attack are mitigated only by TCRs area without modifying AS structures and routers.
- This system mitigates damage in network resource topology from DDoS attack.
- The effect of traffic distribution is small in the case of small scale AS
- The effects are absent when the traffics are transmitted outside.
- The traffics are distributed equally to all routers in AS, therefore some services may be affected.

3.2 Traffic Resizing Method

This method is to reduce traffic in each router. Most routers are connected to two or more routers. This method is also to remove duplicate and removable traffic using these multiple edges. Fig. 3 shows the construction of the router to describe Traffic Resizing Method.

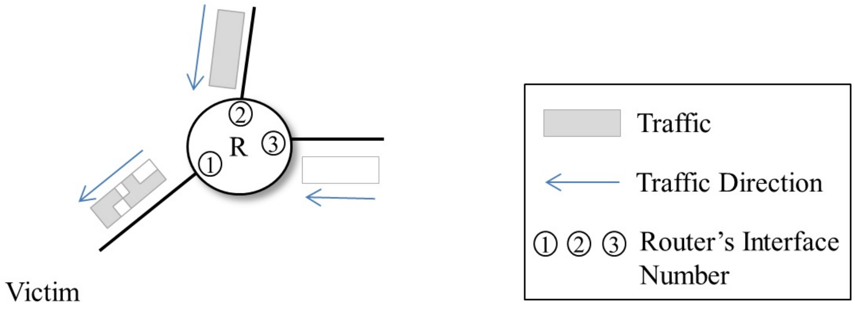

Figure 3: An Example of Traffic Resizing Method

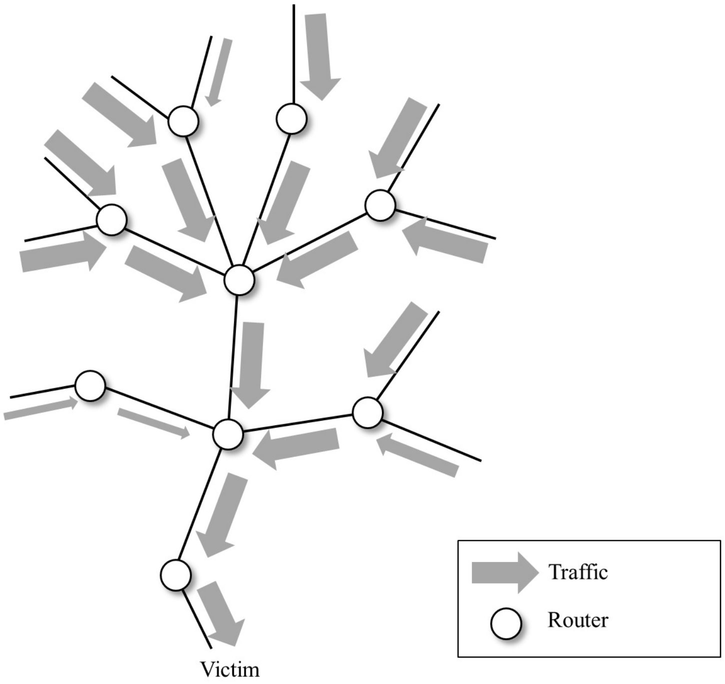

Figure 4: The Tree Structure View nearby Victim

With regard to the actual DDoS traffic, the traffic that cannot detected by host defense systems such as TCR can affect a victim because traffic is concentrated in the router around a victim. Therefore, each router (especially near the victim) is required to reduce traffic. Figure 4 shows the tree structure using traffic resizing method.

In this method, when router has n edges, traffic can be decrease by 1/(n-1) at most. However, this method can work only if all routers are modified. Moreover, it is often difficult to identify a packet for dropping. Furthermore, it is extremely likely to fail to transmit normal packets to the destination.

3.3 Cooperative Dropping Method

This method uses the structure in Fig. 2. In other words, TCR is located at previous AS structures to work. In addition, control units are required as shown in Figure 5, and all TCRs should be connected.

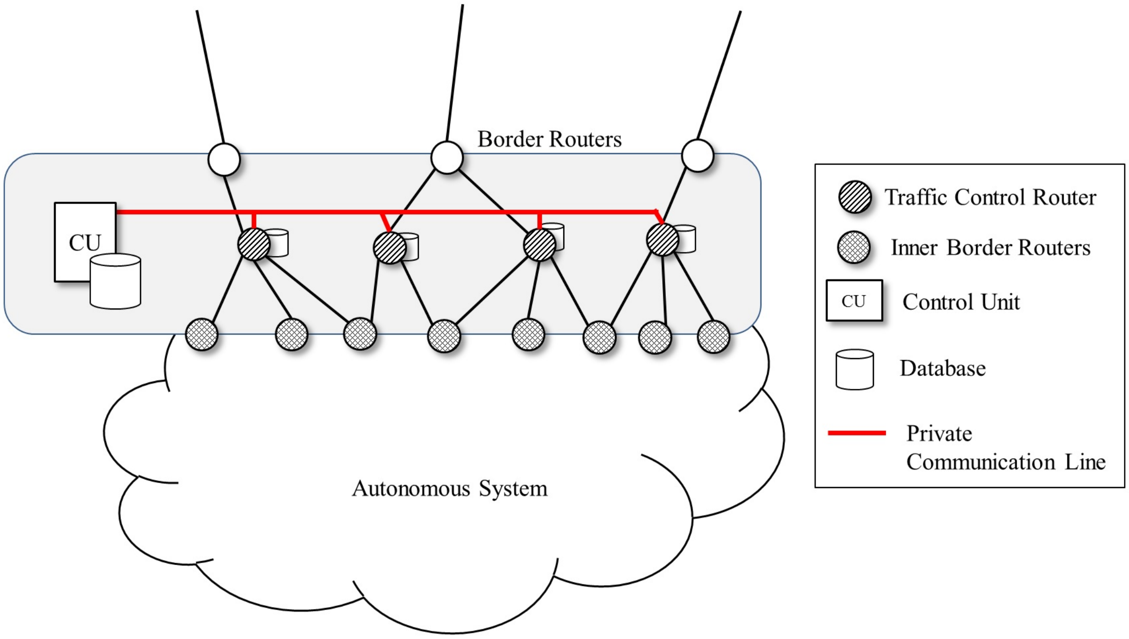

Figure 5: The System Overview using Cooperative Dropping Method

All TCRs inspect passing packets and briefly organize specific information such as source IP, destination IP, destination port, ... , count and then send the results to the control unit at fixed time intervals. The control unit is received information from all PCRs. And, it try to find suspected traffics by DDoS attack using searching integrated information. If the control unit finds suspected traffics, it is transmit this fact to all TCRs. If each TCR received a certain level of traffic, it stores main information of all the packets to the database (DB) without transmitting it to internal routers. In addition, if this traffic is a DDoS attack, stored DB information in all PCRs is used to find the attack source.

In this method, PCRs collaborate to quickly block DDoS attacks through various paths. This method can handle attacks against multiple paths because this method inspects all the packets entering AS and seldom drops normal packets because it mitigates DDoS attacks. However, the following operations require an excellent performance machine:

- Operations to inspect all packets and to create summary information

- Operations to rapidly transmit data to the control unit
- Operations to integrate all the collected information by the control unit

The advantages and disadvantage of this method are as follows:

- This method does not need to modify network structure and routers.
- It is possible traffic analysis and IP traceback after the DDoS attack is over.
- It can mitigate excessive entering traffic through various paths because of inspecting all the packets entering AS.
- It is difficult that the normal packet is dropped in this method.
- This method may cause a delay in the transfer time throughout AS.

All the methods proposed in this paper have advantages and disadvantages. In order to make up for the disadvantages, we will integrate the three proposed methods. If the traffic sharing method and the cooperative dropping method get together, integrated system will be good in mitigation performance. Moreover, this system can be handled efficient network management, because of using analyzed data after DDoS attack. However, in case of DDoS attack generating inside AS and coming from multiple border routers, these two method cannot solve them. These problems will be able to resolve by using the traffic resizing method.

Various methods have been studied in this approach [11]. Specially, Packetscore [5] is similar method, because of using packet-dropping method. However, in this paper, we try not to change the established routing structure (except traffic resizing method). Moreover, our methods can be found multipath DDoS traffic including generated traffic inside AS in a very short time.

4 Conclusion and Future Works

We designed and proposed some methods that are able to tolerate the traffics in large AS until the completion of detecting and blocking DDoS attack traffic. We proposed traffic sharing method to distribute traffic by making full use of all the network resources in AS and Cooperative Dropping Method to block traffic toward specific locations by rapidly inspecting all the packets entering AS. For these purposes, we located Traffic Control Router called TCR and added Control Unit to AS. However, in order to prevent DDoS attacks in AS or multiple DDoS attacks found only around all victims, we also proposed cooperative dropping method. Although these three methods have advantages and disadvantages, an integrated system design is required to compensate for the weakness while operating them together.

In this paper, we proposed three methods to mitigate damage against DDoS attack. But, these methods are not yet have the formal definitions and detailed operation way. In future work, these methods are required to quantitative explanation, intensive analysis and various comparison experiments.

Acknowledgments

This research was supported by Next-Generation Information Computing Development Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT & Future Planning (2011-0029924)

References

[1] Y. Choi, J. Oh, J. Jang, and J. Ryou. Integrated ddos attack defense infrastructure for effective attack prevention. In *Proc. of the 2nd International Conference on Information Technology Convergence and Services, Cebu, Philippines*, pages 1–6. IEEE, August 2010.

[2] J. C.-Y. Chou, B. Lin, S. Sen, and O. Spatscheck. Proactive surge protection: a defense mechanism for bandwidth-based attacks. *IEEE/ACM Transaction on Networking*, 17(6):1711–1723, December 2009.

[3] M. Goldstein, M. Reif, A. Stahl, and T. Breuel. High performance traffic shaping for ddos mitigation. In *Proc. of the2008 ACM CoNEXT Conference (CoNEXT'08), Madrid, Spain*, pages 41–41. IEEE, December 2008.

[4] S. H. Khor and A. Nakao. Daas: Ddos mitigation-as-a-service. In *Proc. of the IEEE/IPSJ 11th International Symposium on Applications and the Internet (SAINT'11), Munich, Bavaria*, pages 160–171. IEEE, July 2011.

[5] Y. Kim, W. C. Lau, M. C. Chuah, and H. Chao. Packetscore: a statistics-based packet filtering scheme against distributed denial-of-service attacks. *IEEE Transactions on Dependable and Secure Computing*, 3(2):141–155, April 2006.

[6] R. Mahajan, S. M. Bellovin, S. Floyd, J. Ioannidis, V. Paxson, and S. Shenker. Controlling high bandwidth aggregates in the network. *ACM SIGCOMM Computing Communication Review*, 32(3):62–73, July 2002.

[7] J. Mirkovic and P. Reiher. A taxonomy of ddos attack and ddos defense mechanisms. *ACM SIGCOMM Computer Communication Review*, 34(2):39–53, April 2004.

[8] C. L. T. Peng and K. Ramamohanarao. Survey of network-based defense mechanisms computing the dos and ddos problems. *ACM Computing Survey*, 39(1):3–3, April 2007.

[9] F. Wang, X. Hu, X. Wang, J. Su, and X. Lu. Unfair rate limiting on traffic aggregates for ddos attacks mitigation. In *Proc. of the IET International Conference on Information Science and Control Engineering (ICISCE'12), Shenzhen, China*, pages 1–5. IEEE, December 2012.

[10] X. Y. X. Liu and Y. Lu. To filter or to authorize: Network-layer dos defense against multimillion-node botnets. *ACM SIGCOMM Computer Communication Review*, 38(4–4):195–206, October 2008.

[11] S. T. Zargar, J. Joshi, and D. Tipper. A survey of defense mechanisms against distributed denial of service (ddos) flooding attacks. *IEEE Communications Surveys and Tutorials*, 15(4):2046–2069, March 2013.

Author Biography

Ho-Seok Kang is a postdoctoral fellowship of the division of Internet and Multimedia Engineering at Konkuk University, Seoul, Korea. He received his Ph.D. degree in computer enginnering at Hongik University, Korea. His recent research interests are in network security, network protocol, mobile security, distributed algorithms and cloud computing.

Sung-Ryul Kim is a professor of the division of Internet and Multimedia Engineering at Konkuk University, Seoul, Korea. He received his Ph.D. degree in computer enginnering at Seoul National University, Korea. His recent research interests are in cryptographic algorithms, distributed algorithms, security in general, cloud computing, and data mining.