Design and Experiments of small DDoS Defense System using Traffic Deflecting in Autonomous System

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

Abstract

DDoS (Distributed Denial of Service) attacks are a serious threat to the legitimate use of the Internet. Many defense methods against DDoS attacks have been suggested. However, the deployment of defense systems becomes an important issue. A previous work, called the Shield [3], brought up the deployment problem and handles the issue with traffic trapping and traffic black-holing techniques. In this paper, a framework for redirection and filtering that works within an AS (Autonomous System) is proposed, while the Shield works outside an AS. This system is designed for protecting legitimate resources from DDoS attacks and for dispersing traffics in small-scale networks such as an AS. In addition, we design the structure that can be deployed and work without changing pervious routers. We also show the optimal number of deployed systems and deployment location through simulation.

Keywords: DDOS Attack, traffic deflection, routing update, RIP, AS

1 Introduction

As the Internet widely spreads and services on it become various, malicious activities on the Internet also tend to continuously increase and spread at the same time. In addition, methods and objectives of attacks have been diversified and sophisticated. Among the malicious attacks, DDoS (Distributed Denial of Service) attacks have three times higher increasing rate than the others [3, 5, 2]. DDoS attacks hindering, generally, normal usage of a service targeted as attack objective can be conducted by either methods, which disturb utilizing resources in the targeted server or methods which attack infrastructure of whole network containing its attack objective. According to the types of attacks, DDoS attacks can be also classified in the following three categories: Flooding attack, Connection attack, and Application attack. As examples of Flooding attack there are SYN/ACK Flooding, TCP/IP Null attack, FIN Flooding, and, Over TCP Connection attack and HTTP attack belong to the class of Connection attack. Lastly, FTP, VoIP, DNS attack are in the class of Application attacks using features of the corresponding application [6, 4, 1].

There are four main ways of prevention and response against DoS attacks and the stronger DDoS (Distributed Denial of Service) attacks: attack prevention, attack detection, attack source identification, and attack reaction [6, 4]. These types of prevention and response measures involve preventing DDoS attacks in advance, blocking DDoS attacks, and identifying the source of attack to mount a response. But the literature only describe how to defend against DDoS attacks, leaving out details of where to actually deploy the attack defense system [3].

Attack defense systems can be deployed at the following locations: core routers; a terminal of an AS (Autonomous System); and near the nodes of an actual victim. Shield [3] is a method to deploy DDoS

Journal of Internet Services and Information Security (JISIS), volume: 2, number: 3/4, pp. 43-53
*Corresponding author: Konkuk University, New Millennium Hall 201-1, 120 Neungdong-ro, Gwangjin-gu, Seoul 143-701, Republic of Korea, Tel: +82-10-8987-3335

defense filters. It is not a design of a DDoS defense filter. Many existing high-quality filters could be efficiently implemented on the Shield nodes, providing first-class protection for participating parties [3].

In this paper, we propose a new DDoS defense system that can work inside an AS using Traffic Deflecting method similar in principle to that of the Shield. The main difference between our proposal and the Shield is the location of the defense system, i.e., our proposal is to be deployed inside an AS. This difference is important in two aspects. Firstly, the Shield is designed only to work outside an AS, thus it misses the opportunities for efficient DDOS prevention within an AS and is unable to prevent DDOS attacks that arises from within an AS. In DDoS attacks many traffic go from outside of the AS to the inside. But for a large AS, there may be victims inside the AS by zombie machines created inside, and thus a measure against this is needed [3] Also, many defense methods immediately block external traffic if it comes in, and so it's difficult to give sustained damage. Therefore, from the attacker's perspective it is advantageous to create many reflectors or zombies inside of the target AS and launch a DDoS attack from the inside. Bandwidth may be quickly consumed by the network traffic inside the AS, causing greater damage. Secondly, we need different implementation techniques for the inside of an AS from that for the outside of an AS. Our framework is designed so that it works similar in principle to the Shield using the internal RIP (Routing Information Protocol). It works in three different levels, which will be explained later in the paper. Hence, the location where this system is deployed and the number of deployed systems are also important factors. To find out the optimal number of deployed systems and deployment location, we experiment some simulations in virtually created ASes.

The rest of this paper is organized as follows. In the following chapter, the Shield is explained as reviewing related works, chapter 3 explains the system which makes it possible for the Shield to work at RIP. Chapter 4 suggests the optimal number of deployed systems and deployment location with results from our experiments; finally, chapter 5 serves as a conclusion.

2 Related Work

Kline et al. (2011) [3] study the optimal deployment location of DDoS defense systems, which is different from previous researches concerning how to defend attack objectives from DDoS attacks. In other words, they don't discuss issues on which traffic should be chosen to deploy the filters but on how to move traffic toward the filters. By controlling traffic, it is possible to examine lots of traffic, and, at the same time, to convey harmless traffic to its destination. Kline et al. (2011) establish the Shield by using the traffic trapping and traffic black-holing which are widely used. The traffic trapping and traffic black-holing are the idea that passes the legitimate users' traffic but blocks the attackers' traffic at the Shield by redirecting the traffic to the Shield node as in figure 1.

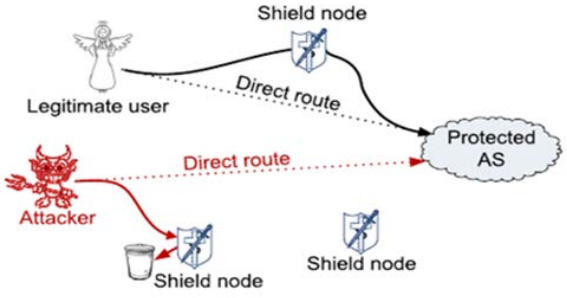


Figure 1: Diverting traffic flow from a direct route to pass through filtering node(Shield)

If there is suspicious traffic, an AS redirects traffic to the Shield node by altering and conveying AS-

PATH of BGP. If DDoS attack actually occurs, whole traffic is sent to the Shield and is blocked. Thus, IXPs (Internet Exchange Points) can be highly recommended as the optimal location for deployment of the Shield because the attack may make a detour through the other routes if the Shield is not deployed at all IXPs. However, the Shield has some weaknesses.

First, Shield implemented using BGP can work only on the outside of AS. Generally, routing of BGP works outside of AS, whereas RIP, which works by the exchange of table among routers, operates inside of AS. Two protocols use different methods.

Second, For DDoS attacks, traffics sent by the attacker should be filtered but legitimate traffics should arrive at their original destination. But with the Shield, along with the traffics from the attacker, even legitimate traffics can't arrive at the destination. To solve this problem, an IP-IP tunneling may be employed with a routable IP prefix or a source routing technique may also be used. But these methods cause some amount of network overhead.

Third, frequent attack brings about frequent correction of AS-PATH, which will weaken the consistency of the network, and if an attacker abuses it, Shield itself can cause the overhead in a network.

3 System Design

In this paper, we propose a system design concerning where and how to deploy the system that redirects and blocks traffic as the Shield does. We design the Shield working at the inside of ASes which is different from the Shield working at the outside of ASes by using BGP. To distinguish the Shield using in our suggested system from the Shield working at the outside of ASes, we define ours as the sShield (small Shield). RIP is used as the routing protocol on the inside of ASes. The sShield is under control of AS's administrator, and several sShields should be deployed. Moreover, for efficient management of the system, we systemize the sShield to work differently with each different phase among three phases classified according to degrees of the attacks' risk.

3.1 System Overview

The sShield is deployed between routers on the inside of ASes as in figure 2, and it works as a router. The sShield is structured so that there is no traffic via sShield when there is no attack.

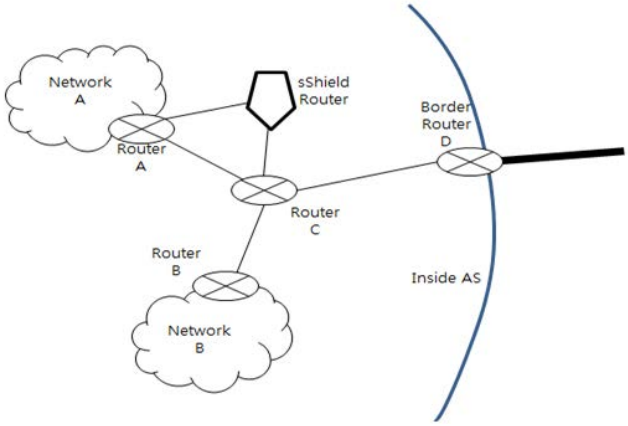


Figure 2: Deployment of sShield

As mentioned before, for efficient management of the system, the sShield has three defense modes which are, respectively, normal routing mode, preventive routing mode, and protected routing mode, and

the sShield differently works according to each mode. The administrator of an AS determines each mode in accordance with the progress of attacker's attack as the flow in figure 3. The normal routing mode that operates when there is no attack is a normal and stable state that the sShield does not work and no traffic passes through the sShield. However, if the AS detects traffic suspected as an attack through several paths, the administrator changes the mode to the preventive routing mode and the routing path to the sShield. Furthermore, if the actual attack is on progress, the traffic generated by the attacker is blocked by changing the mode to the protected routing mode. The way that the sShield operates is explained with the three routing modes.

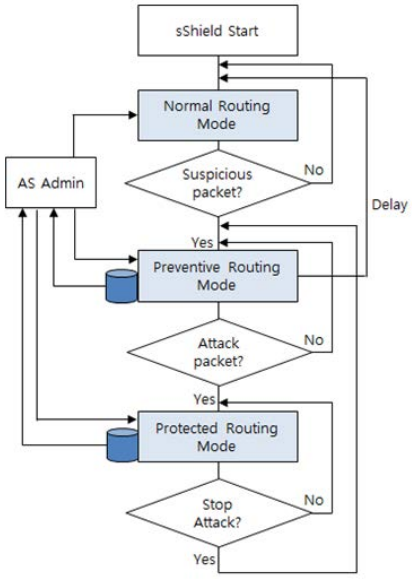


Figure 3: Three routing mode flowchart

3.2 Three Routing Mode

The mode in the state that there are neither attacks nor symptoms of the attacks is called the normal routing mode. Figure 4 is the picture when the sShield is deployed between router A and router B. Each router's routing table is stabilized, and no traffic passes through the sShield. Elements in each routing table are Destination Networks, Hop-Count, and Next hop in order.

The preventive routing mode starts to work in the case where an AS believes that there is a network suspected as the victim of the attack based on the collected information from several places. Figure 5 shows the changes of routing tables in the preventive routing mode when network B is considered as the potential victim by the attacks.

The AS reports to the sShield that there is network B which may be under the attacks. Then, the records in the field toward the sShield's network are saved in a DB. As the following procedure, after the value of Hop-count in the corresponding field is reduced by two and recorded as n-2 (n is the original value of the Hop-count), the routing table is sent to the directions (S1) except the location of the Next-hop in the corresponding field by using the triggered update. Because periodical routing update disturbs the immediate changes of tables, the triggered update is used for ensuring the immediate changes of routing tables in router A. Furthermore, the triggered update is also used to promptly cope with DoS attacks. Router A sends the traffic to the sShield through A1 instead of network B to which the traffic is originally heading because the sShield's Hop-count is reduced.

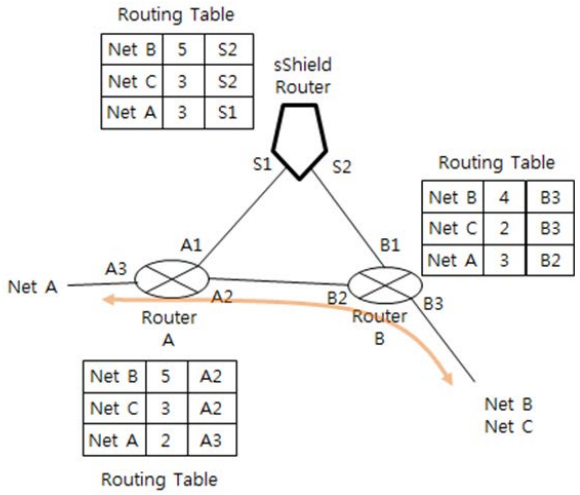


Figure 4: Routing tables by normal routing mode

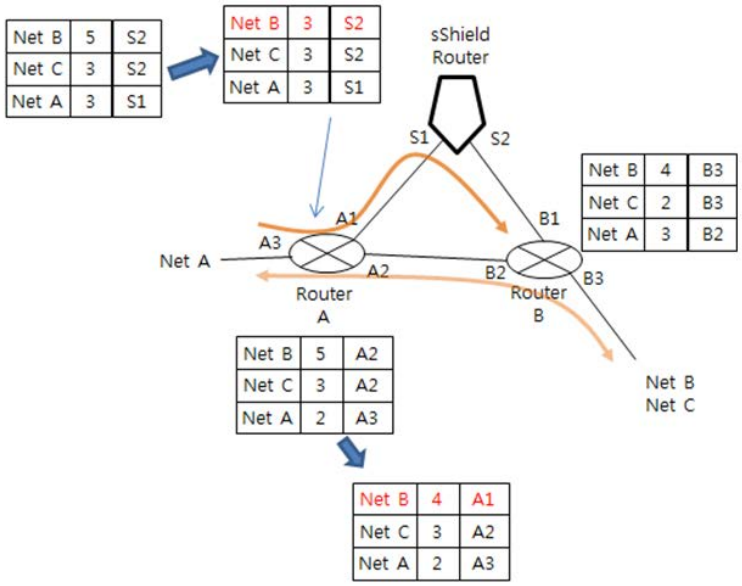


Figure 5: Routing tables by preventive routing mode

If the AS confirms that DDoS attack toward network B occurs, the AS commanded the sShield to change the mode to the protected routing mode, and all packets matched to the filtering rules are blocked at the sShield. The other harmless traffic arrives at its destinations through S2 of the sShield. Figure 6 describes the situation that the attack traffic is blocked at the sShield.

Once the AS considers that the attacker's attacks are finished, the AS orders the sShield to change its mode to the preventive routing mode. Since the routing path passes through the sShield in the preventive routing mode, routing tables are not altered. In the case that there is no suspicious traffic in the preventive routing mode for a fixed time, the mode should be changed to the normal routing mode. To make the change, routing tables should be changed as described in figure 7.

The sShield which is ordered to change its mode to normal routing mode by the AS retrieves the original value of the Hop-count in network B from the records previously saved in the DB. After that, the

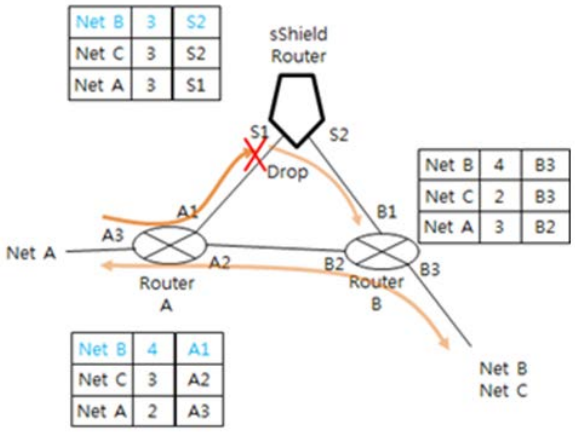


Figure 6: Packet filtering by protected routing mode

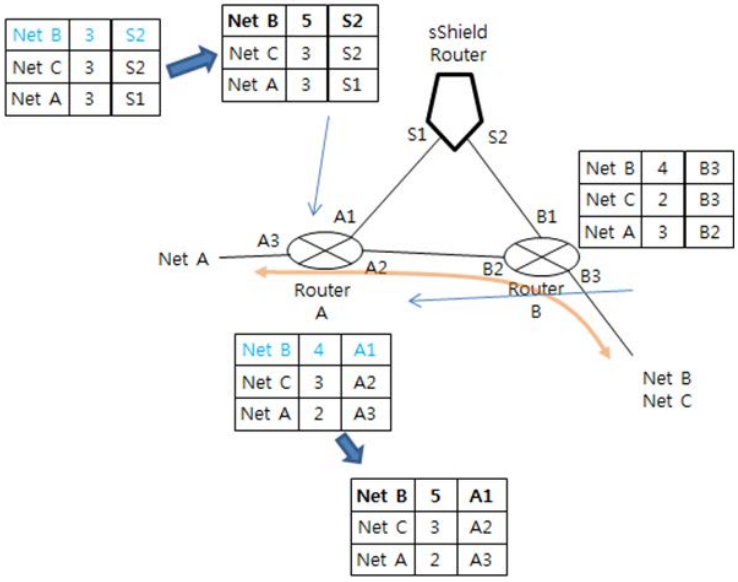


Figure 7: Return to the normal routing mode

routing table of router A is altered to the normal path by periodical exchange of routing update messages.

3.3 Strength and Weakness

We have proposed a novel system about routing deployment mechanism. This system can be deployed at any location, as with the Shield. But the sShield have some strong and weak points.

First, in case of Shield, the method to modify the AS-PATH of BGP and change its path is applied and it works only in the outside the AS. But, sShield can be deployed and work in the inside of AS by using the representative protocol of IGP and RIP. In other words, when it cooperates with Shield, it can be established in any place on the Internet.

Second, Shield can transfer appropriate traffic only through the methods with much overhead, such as tunneling and source routing. However, sShield can transfer the traffic not blocked by RIP to the

destination.

Third, while Shield cannot control traffic accurately due to the limitation of BGP, sShield using the table update of RIP can by taking a circuitous way or blocking the network unit under attack. In addition, the existing routers except for sShield are operated not knowing the existence of sShield. Therefore, established routers do not need to be changed and it helps a network maintain its consistency.

In spite of these merits, there are some weaknesses. Because of the RIP structure, the sShield that is connected to the network that is directly adjacent to the router can't protect against attacks to the network because the hop count of the routing table of sShield cannot be reduced to less than one. Also, an attacker who knows the structure of the router inside the AS can attack through the route avoiding sShield. However, these cases can be dealt with when multiple sShields are set up and cooperate. Moreover, because the logical structure is simple, the deployment location of sShield can be frequently changed to defend against the DDoS attacks.

4 Experiments

In this chapter, we study the optimal number of deployed sShields and deployment location with experiments. For this purpose, the deployment environment defines the topology of the AS and classifies methods of the deployment. Then, we find out the optimal method of deployment and the optimal number of deployed sShields.

4.1 Environment of Deploying Experiment

The locations, scales, and connection structures of routers inside of ASes are different in each AS, and they also differ according to the environmental factors and the policy of an AS. Furthermore, all ASes does not disclose the above information for security reasons [3]. Hence, we constructed a radial shaped AS as in figure 8 by employing roles of routers such as CR (Core Router), ER (Edge Router), DR (Distribute Router), and AR (Access Router) which are used in ASes. Since ASes do not have tree-structures and each AS can't have environmentally similar structures with our virtual AS, we create a topology which adds random connections. In every experiment, we alter the topology 10 times for each round, and the deployment is changed 20 times for each topology. After conducting 20 times DDoS attacks for each deployment, we record the probability of successful defense by the sShield.

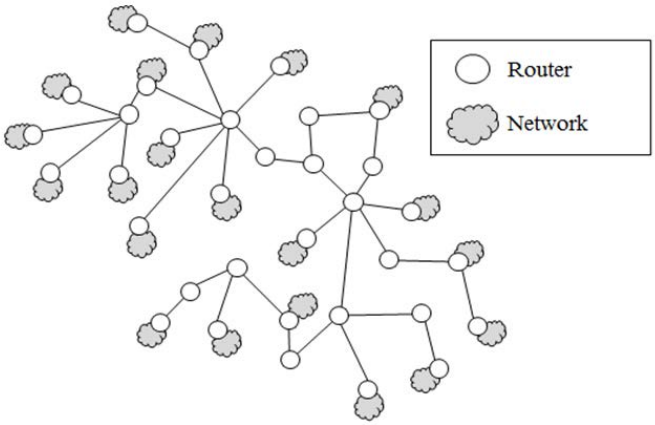


Figure 8: Example of Autonomous System topology

Figure 8 shows an example of AS's topologies which is used in our experiment. When a router is considered as a node and the connection of routers as an edge, it can be seen as a graph. From now on, a part of terminologies in graph theory will be employed to describe the methods of sShields' deployment in the followings. The following deployment methods are used in our experiments.

- Random Deployment: The deployment locations are randomly selected and sShields are deployed at those locations whenever the number of sShields which are to be deployed increases.
- Adjacent Network First Deployment: The sShields are deployed at routers which are adjacent to a network and edges connected to a router whenever the number of sShields which are to be deployed increases. Networks are randomly selected, and, in the case where sShields are deployed at every neighborhood of networks, edges that are not adjacent to the networks are randomly chosen to deploy sShields.
- High Degree Router First Deployment: After selecting the router that has the largest number of edges in its neighborhood, sShields are deployed first at the edge connected to the corresponding router.

4.2 Result of Simulation

At first, we gauge the change in success rates of defense against DDoS attacks in the AS which has 100 routers and 50 networks as increasing the number of deployed sShields. Figure 9 shows the result from the above simulation, and the random deployment is employed at this simulation. As one can easily notice, the balance between defense success rates and the number of deployed sShields is required because the numbers of deployed sShields should be extremely high for the perfect defense.

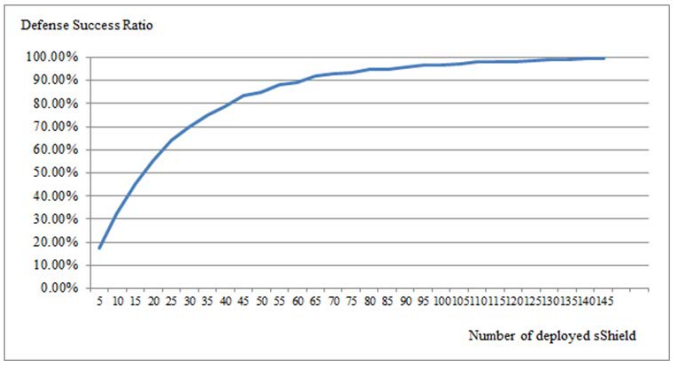


Figure 9: The change in defense success rates according to increase in the number of deployed sShields (the number of routers: 100, the number of networks: 50, random deployment)

Before conducting experiments regarding each deployment method, we measure the change in defense success rates, respectively, according to the change in scales of ASes and according to the change in ratios between the number of routers and networks to determine the number of routers and network which represent the scale of an AS. Figure 10 is the graph that shows the change in defense success rates according to scales of ASes, and the graph in figure 11 depicts the results from the estimation of defense success rates according to the change in ratios between routers and networks. As shown in figure 10, while the curves exhibit similar patterns in ASes which have at least 60 routers, there is clear decrease in defense success rate as the number of routers reduces in ASes which have routers less than 60. That is, 100 can be chosen as the appropriate number of routers within the RIP's maximum Hop-Count, 15,

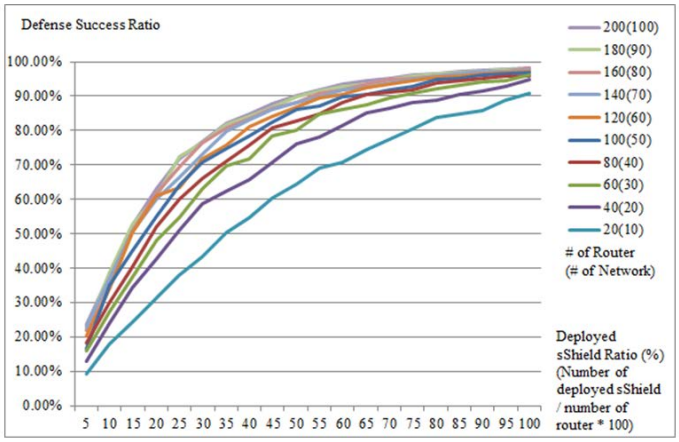
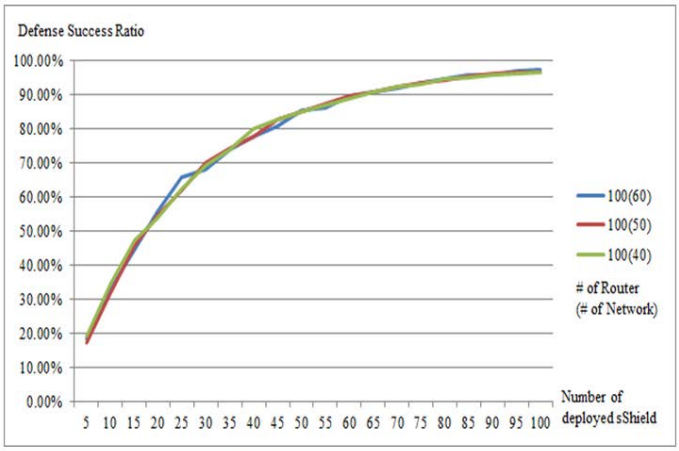
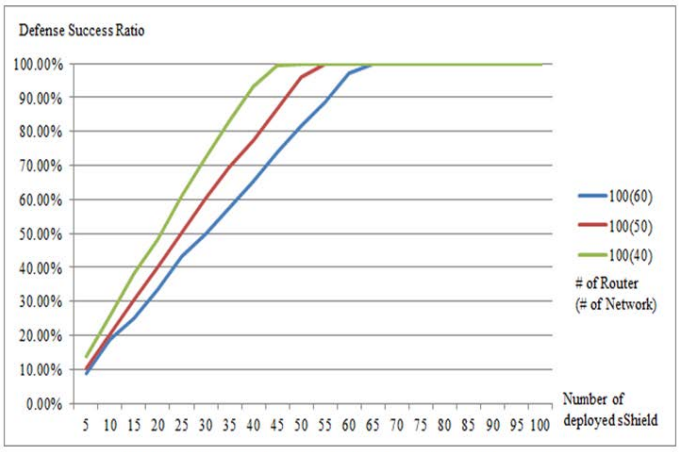


Figure 10: The change in defense success rates according to the change in scales of ASes (random deployment)



(a) Random Deployment



(b) Adjacent Network First Deployment

Figure 11: The change in defense success rates according to ratios between the number of routers and networks

when ASes are not small-scale. We can get the graph in Figure 11 by making a change in the number of networks after the number of routers is fixed to 100. In the case of random deployment, the change in defense success rates is almost independent to the change in the number of networks. However, the slope of curves decreases in the case of adjacent network first deployment as the number of networks increases. That is, the ratio between the number of routers and networks only has an effect in the case of adjacent network first deployment. For the following experiments, we choose the number of networks as one-half of the number of routers.

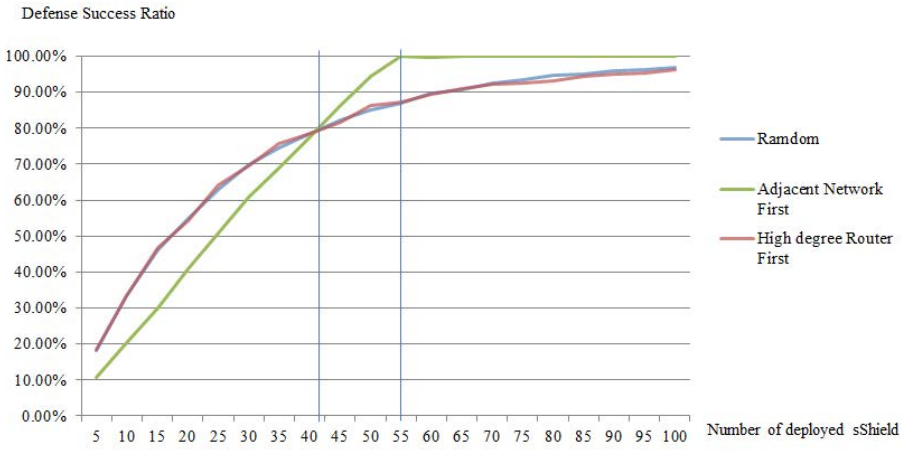


Figure 12: The change in success rates of defense against DDoS attacks in accordance with different methods for deployment of sShields (The number of routers: 100, the number of networks: 50)

Figure 12 shows the change in defense success rates according to different deployment methods when the number of routers and networks determined in the previous paragraph are employed. As in the above, in an AS that the number of networks is one-half of the number of routers, the random deployment is appropriate method if the number of deployed sShields should be restricted in a small number, however, if the number of deployed sShields can be large, the adjacent network first deployment is more appropriate.

However, because the number of networks is an important factor in the adjacent network first deployment, the number of networks which is one-half of the number of routers can't be the only one we should consider. See graph (b) in figure 11 with considering figure 12. As mentioned before, since the slope of curve in the AS with more number of networks is lower than that in the AS with less number of networks, the random deployment can have better results in the AS with many networks. On the other hand, since the slope of curve increases as the ratio of network to routers decreases, the adjacent network first deployment can be more efficient in the AS with the small number of networks.

5 Conclusion

In this paper, we proposed a criterion concerning where filtering systems are deployed and the system that not only blocks attacks but also stabilizes networks through traffic diversion, which is different from previous researches regarding defense systems against DDoS attacks. In addition, we design the system that diverts and blocks the sShield system located between routers to establish DDoS defense system on the inside of small-scale ASes by modifying routing tables of RIP. We classify three phases according to progress of DDoS attacks and design the system so that it properly works for the different objectives in each different phase. Moreover, we propose the optimal number of deployed sShields and deployment location in accordance with several types of ASes, and figure out actual defense success

rates with experiments. If the proper number of deployed sShield on the inside of an AS can work along with the Shield on the outside of the AS, it can give a help to traffic load balancing and monitoring and detection of DDoS attacks.

Acknowledgments

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MEST) (No. 20120006492).

References

[1] J. M. Erik Klisne, Matt Beaumont-Gay and P. Reiher. Rad:reflector attack defense using message authentication codes. In *Proc. of the 25th Annual Computer Security Applications Conference (ASAC'09), Honolulu, Hawaii, USA*, pages 269–278. IEEE, December 2009.

[2] K. Garg and R. Chawla. Detection of ddos attacks using data mining. *International Journal of Computing and Business Research (IJCBR)*, 2(1), 2011.

[3] E. Klisne, A. Afanasyev, and P. Reiher. Shield: DoS Filtering Using Traffic Deflecting. In *Proc. of the 19th IEEE International Conference on Network Protocols (ICNP'11), Vancouver, British, Columbia Canada*, pages 37–42. IEEE, October 2011.

[4] J. Mirkovic and P. Reiher. A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review*, 34(2), April 2004.

[5] T. SpiderLabs. The web hacking incident database semiannual report. july to december 2011. Technical report, Computer Science, Trustwave SpiderLabs, 2011.

[6] C. L. Tao peng and K. Ramanohanarao. Survey of network-based defense mechanisms countering the DoS and DDoS problems. *ACM Computing Survey (CSUR)*, 39(1), April 2007.

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.