A Survey on Defense Mechanism against Distributed Denial of Service (DDoS) Attacks in Control System

YooJin Kwon†

KEPCO Research Institute, Korea Electric Power Corporation,105 Munji-Ro, Yuseong-Gu, Daejeon 34056, Korea
† yoojin@kepco.co.kr

Abstract

Denial of Service (DoS) attack is to interfere the normal user from using the information technology services. With a rapid technology improvements in computer and internet environment, small sized DoS attacks targeted to server or network infrastructure have been disabled. Thus, Distributed Denial of Service (DDoS) attacks that utilizes from tens to several thousands of distributed computers as zombie PC appear to have as one of the most challenging threat. In this paper, we categorize the DDoS attacks and classify existing countermeasures based on where and when they prevent, detect, and respond to the DDoS attacks. Then we propose a comprehensive defense mechanism against DDoS attacks in Control System to detect attacks efficiently.

Keywords : Distributed Denial of Service (DDoS) Attack, Intrusion detection system, DDoS defense

I. INTRODUCTION

Denial of Service (DoS) attack is to interfere the normal user from using the information technology services. With a rapid technology improvements in computer and internet environment, small sized DoS attacks targeted to server or network infrastructure have been disabled. Thus, Distributed Denial of Service (DDoS) attacks that utilizes from tens to several thousands of distributed computers as zombie PC appear to have as one of the most challenging threat. In the summer period of 1999, a real DDoS attack appeared for the first time. Later mobilizing various attack techniques were given a lot of attention as the number of attack attemps has increased in worldwide.

These DDoS attacks are possible nowadays, focusing only to offer rapid networking performance to transfer information between the communicating parties in the internet world. There was less attention to design systems that monitor traffic or adjust traffic volume. Thusif you pass a plethora of information to the receiver, he cannot send the sender information it should process. It threatens the availability of network usage, making the situation where the receiver is threatened by a malicious attack, also known as DDoS attack.

DDoS attacks are prelimenary difficult to defend with using countermeasures due to following reasons. First, it is not possible to protect the current number of devices that are connected to the Internet exactly, even though the system fully configured the security of a part of some servers that are protected with strong security countermeasures. Others are open to a number of vulnerable environment that leads to be used as bot of DDoS attack. In addition, each device when many users request for a certain job at the same time, the limited computing resources to manage together the request wishes to use the service, with greater tisk resources are depleted. Moreover, the lower constituting the Internet of the subnetworks are the point which is impossible to control forcibly with each run by a different policy in the real world. Finally, the DDoS attack patterns in Web site attacks by a simple show-up or personal curiosity, but recently threatened to extort money(ransom),or between two countries or group political attack. And damage size, such as cyber war by military or terrorist organization by the political beliefs of the Group corresponds with a more sophisticated attack techniques are likely to be difficult.

On the other hand, recent control systems are sophisticated information and communication technology to increase the efficiency and interoperability, it is quickly transformed into grafted environment to the existing physical facilities. While the digital substation, power distribution automation, electric vehicle charging infrastructure, energy storage systems, and micro-grid, etc. adopt the international standard protocol and the commercial systems, both the need to connect to the external network and the possibility of malicious attack on the control system increases together, and there is subseequently a growing need for the additional security mechanism other than commercial intrusion detection systems.

II. DDOS ATTACK TECHNIQUES: SCOPE AND CLASSIFICATION

For the classification of the DDoS attack techniques, research is in progress as a recent work in Zarger et al. [1] has been proposed by the attack technique detailed analysis for defense by Table 1. They are classified as a range of techniques, such as scope and classification. For that through well known or newly upcoming attack tactics, it was determined that it is necessary to take measures to detect newly or overlooked a variety of DDoS attack techniques from various aspects.

III. DDOS DEFENSE TECHNIQUES

DDoS defense technique is classified into two categories based on the defense mechanism of the defense mechanisms and defense point in time in accordance with the arrangement position significantly by including Zarger et al [1].

ISSN 2465-8111 DOI http://dx.doi.org/10.18770/KEPCO.2015.01.01.055

Table 1. DDos Attack Technique Classification

Attack techniques					Characteristics
DDoS Flooding	OSI 3, 4 Layer	Flooding			Transport protocol to exceed the allowable capacity in the network (ex) UDP, ICMP, DNS, VoIP Flooding
		Protocol looting			Utilizing specific protocols implemented on the vulnerability or bug in the target (ex) TCP SYN, TCP SYN-ACK, ACK & PUSH ACK, RST/FIN Flooding
		Reflection-based			Techniques utilizing reflector sends the response to the denial of service attack by sending a request to the reflector (ex) ICMP echo request, Smurf, Fraggle
		Amplification-based			When a message of greater capacity and put a plurality of messages in a packet to be sent to the target amplification technique utilizing the effect
	OSI 7 Layer	Reflection/amplification-based			Service denied the request to the reflector technique utilizes a large amount of response to send to the target (ex) DNS amplification, VoIP Flooding
		HTTP Flooding	Session Flooding		Bulk transmission using a plurality of session connection request botnets (ex) HTTP get/post Flooding
			Response Flooding		Bulk insert and send multiple requests in a single session (ex) single-session HTTP get/post Flooding
			Asymmetric	multiple HTTP get/post Flooding	Transmitted in a single session in a random order to insert the plurality of requests in large quantities in a single packet
				Wrong application	Web site design is immature, take advantage of the design errors of the application with the wrong way linked to the database
			Slow request/ response	Slowloris	Send an HTTP request, not the entire part of the socket which can occupy all available. HTTP get-based attacks
				HTTP split	Slowly transfer from the line is not so small as that exceed the time limit of the server splitting HTTP request
				Slowpost	My definition content-length number defined with a large number manually in HTTPheader and the text message is sent slowly such as 1 byte /minute. HTTP post-based attacks
				Slowread	Slow response received after the receive window size set to a smaller size than the transmit buffer of the target
Using exploit					Not the characteristics of network protocols, the software used within the service implementation of a bug or vulnerability to attack

A. DDoS Defense technique in accordance with the arrangement position

DDoS defense techniques in accordance with the placement of the attack source, depending on where you apply the defensive technique as shown in Fig.1 (the attacker), attacked the destination (target) is divided into four network-based and hybrid.

1) OSI 3, 4-layer DDoS defense techniques destination

General flooding by using the features on the network transport layer protocol, if looting spread the protocol, based on reflection, DDoS attacks, such as amplification-based flooding attacks, the source(A.1.1), an attack destination (A.1.2), a network-based (A 1.3) and is divided into four mixed (A.1.4) defense techniques.

a) Attack source-based DDoS defense techniques (A.1.1)

The case placing a defense techniques for detection and response to the attack source host, but the benefits that could allow an attacker to mass consuming detected previously in the vicinity of the attack source quickly and filters the resources, the actual DDoS attacks multiple botnets. The various types distributed throughout the network called near all sources defense techniques are applied if you can accurately detect attack attempts to do is the unknown. Also, each botnet to traffic volume and nine minutes the traffic volume of a normal user to transfer from the attack source in many cases set put to difficult, very likely actually detection is difficult. Also, do not immediately direct benefit to the network availability, protection against security equipment to monitor network traffic to and send-side source which stakeholders have to pay because it is unclear whether the attack should be a source-based defense techniques are less effectiveness.

b) destination-based DDoS attack defense techniques (A.1.1.2)

A case of disposing a protective mechanism near the target to monitor the network traffic to the attack destination combined traffic to the destination and it is possible to recognize the attack low cost compared with other defense mechanism and the positioning ease good there is an advantage, but discard it and start attacking consuming the resources of the target at the same time, it is difficult to accurately detect the attack detection accuracy is lowered difficult to apply solely to the actual environment.

c) Network-based DDoS defense techniques (A.1.1.3)

That is attack the source and the intermediate network is not the destination, and if the router step defense technique is applied. At this time, the router of the Bloom filter or a network in the

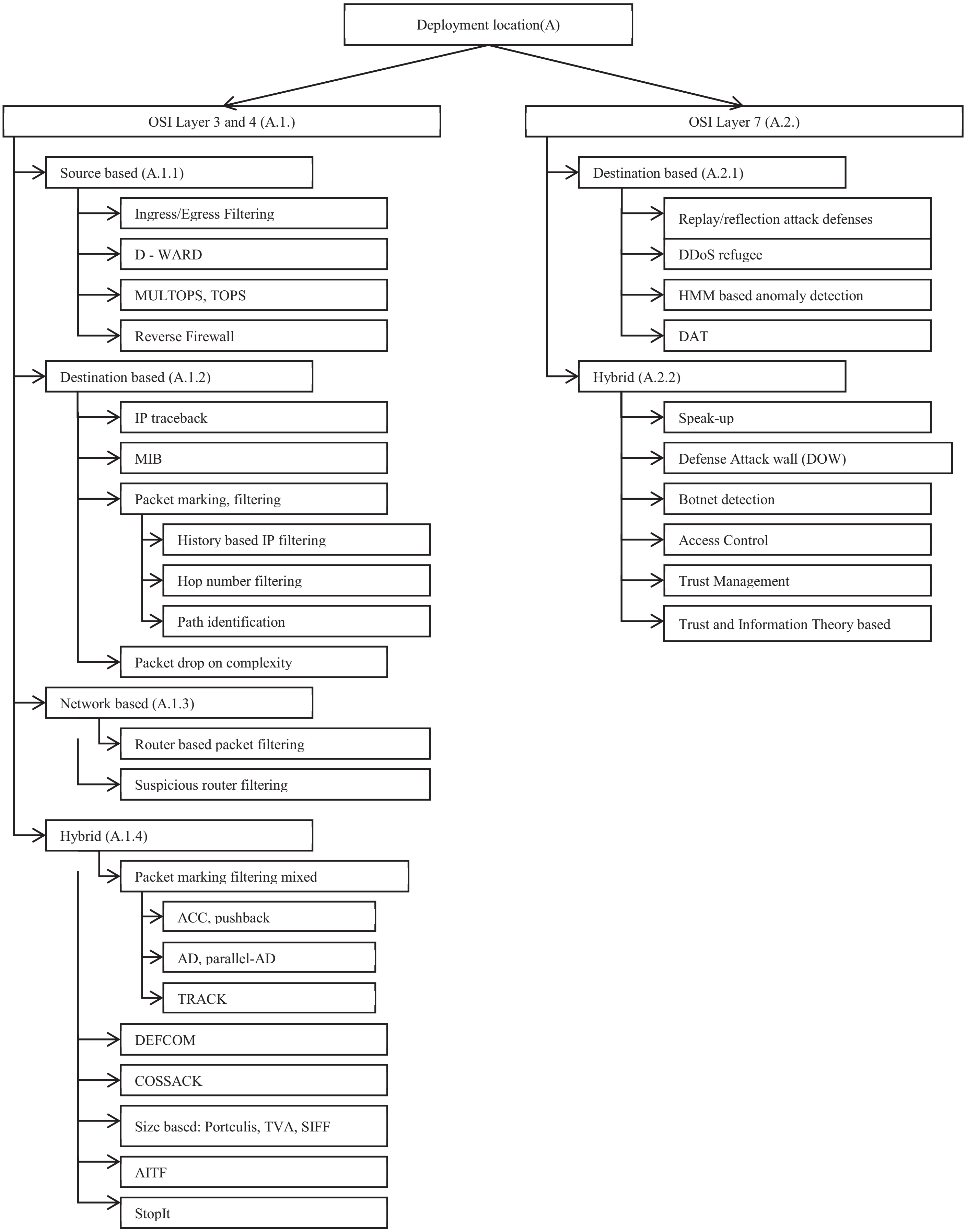

Fig. 1. Classification of DDoS Attack Defense Techniques

middle by a method such as packet sampling is close as possible to the attack source detected DDoS attack, and The wish to block, but each router is much processing overhead capacity consumption is caused to degrade the performance of the router, this process including events related to shares or log combination between routers in actual detection is added if the detection rate is very low drawbacks There is a low effectiveness and efficiency.

d) Hybrid DDoS defense techniques (A.1.1.4)

Attack source, destination, intermediate network based defense techniques, each defense technique is location only where centralized techniques that focus placed inde contrast, mixed DDoS defense techniques and combining all earlier introduced defensive techniques. Network3, the four-tier of the most effective defense mechanism against the target attacks, the arrangement to distribute the defensive techniques in a variety of locations and collaboration between defense techniques are important. For example, packing marking and defending techniques mixed filtering detection module destinations (Attack target), and that the DDoS incurred to placement on the as soon as possible nearby, blocking module attack source (attacker) and to block as quickly as possible the attacker's actions on placed near, but the system complexity for communication between distributed defense techniques brings the performance by increasing the overhead, for reliable communication encryption, electronic signature should provide an authentication scheme. incentive might also not sufficient to pay the costs incurred for the collaboration between the different arrangement positions.

2) OSI 7-layer DDoS defense techniques destination

If you use the features in the network application layer protocols, such as DDoS attacks, expand the reflection/ amplification-based flooding, HTTP flood attack has divided into two destinations (A.2.1) and mixed (A.2.2) defense techniques.

a) destination-based DDoS attack defense techniques (A.2.1)

The case of arranging the server near the attack defense mechanism is to monitor the application layer protocol traffic to attack destination (DNS server or the web server). Merging traffic to destinations defense whether it is possible to recognize the attack the cost is affordable and positioning ease good advantages over the techniques, but because attacks start with abandon to consuming the resources of the target at the same time, it is difficult to detect an attack exactly the detection accuracy decreases hardly alone apply to the room environment.

b) Hybrid DDoS defense techniques (A.2.2)

Mixed DDoS defense techniques after placing a defense method for server and the client to and across the application layer protocol used to communicate between the two detecting DDoS, it is the case block. For Speak-up method uses a method of inducing to the normal user of the traffic increases. Defense/attack wall (DOW) performs abnormality detection using a modified form of Speak-up method, K-means clustering algorithm then it disconnects the session after suspect, but the methods has a problem of lowering the performance increases the server/client communication calculation complexity. When using the pattern will be appreciated CAPTCHA such that a person only to distinguish botnet, dropping the ease of use of the end-user experience problems resulting in service delays intermediate challenge server in the in the case of access control defense technique arrange to manage the number of users connected to the server itself, eliminating the effectiveness if the target of DDoS attacks. If you place your trust management system (TMH), to grant a license on normal clients to manage as best user concept. If the client has suffered an intrusion is difficult to recognize a DDoS attack itself.

B. DDoS defense techniques of the defensive point

A DDoS defense technique of the defensive point of attack before the start time compared to the attacks occurred (prevention techniques), attacks in progress (detection scheme). It is divided into three after attack detection (Attack source identification and response techniques).

1) Before the attack DDoS defense techniques

A series of activities to prevent attacks before they start DDoS responsibilities. The Genget al. [3] proposed protocol incomplete or weak authentication mechanisms, techniques to prevent bug fix vulnerabilities found in advance for such exposure computer. Protocol updates, software patching, being unused software, removal, services, and applications, redundancy, disaster management planning, intrusion detection systems (IDS) introduced load management and methods, such as equivalent network flow control, but the application of unknown vulnerabilities. A new DDoS attack techniques have emerged to prevent DDoS activities with a signature or patch is not to prevent new attack techniques, so it is impossible to eliminate the threat completely.

2) DDoS defense techniques ongoing attack

DDoS attack when starting a series of activities to detect quickly the defense is applicable in this class. For a fast detection target the most practical way to detect DDoS anomalies is to place a detection mechanism close to the target that you want to protect. The attack traffic is classified and the abnormal pattern detecting method of the attack flow that exceeds the limit values of two of the method of detection. Among the abnormal pattern MIB information analysis, D-WARD, MULTOPS, TOPS, DDoS shelter, it is possible to extract from both the transport layer and the application layer in a manner such as DAT [4]. In addition, a variety of data mining to the abnormality detection is introduced to the artificial intelligence techniques, a method for analyzing traffic flow on a variety of placement and examine the packet header have been proposed. By default, sufficient study of the normal pattern by using the information has been gathered in the normal situation below. The measures to detect DDoS anomalies using one of four methods are common.

- Observation of variable definitions
- Using statistical techniques
- Wavelet analysis
- Granular level analysis

However, a method to detect the attack proceeds in various positions on the real Internet. The cost for collaboration between these interoperability verification requires the actual environment to have a solid cooperation framework between institutions with different interests reality it is very difficult.

3) DDoS Attack Detection and Defense Techniques

Corresponding techniques for each type of DDoS attacks has been identified and block network and resource depletion behavior coming from the attack source. To identify the attack source in a variety of trace back techniques, IP traceback method is useful in theory. But to trace back their source in the real world it consumes the high maintenance costs in the information carrier on the Internet. Thus it is difficult in reality to provide the ability to track within the mobile network it manages. Therefore, packet marking, such as control network is considered to provide the availability in the environment.

IV. DDOS ATTACK COUNTERMEASURES IN THE CONTROL SYSTEM ENVIRONMENT

Control system environment is one of information communication system relatively easy to extract a predetermined normal pattern of network packets. It has limited set of commands, and is not connected with the Internet network to establish a separate control network. It is operated in a very special cases that are connected to the internet with limited protocol and port for a couple of the communication connection on the security control center. Therefore, under a DDoS attack protection measures takes into account especifically for these control systems environment in this paper. We propose three countermeasures to defense DDoS attack.

First, in order to prevent DDoS attacks of Ingress / Egress, History-based IP filtering, hop count, filtering, Pi uses the 'local filter' such as a router-based packet filtering. Analyzing DDoS attacks, it is effective to identify and apply the filtering rules. We introduce a systematic and automated detection techniques conventional filter-based response techniques which is an effective filter propagation and management techniques, the last filter-based response Study of Adaptive Probabilistic Filter Scheduling Scheme [2] solves the above problems. In this scheme with a number of hops, Filters managed to take advantage of the availability and links about the router from the packet sender. The results compared to existing techniques showed 44% higher protection rate by applying it to the control system. It is expected to be useful to use an algorithm for selecting an effective filter for the DDoS attack situation.

Second, a defense can use IP spoofing. There is a need to prevent the attack source traffic which exceeds flow through the control network. ISP and IDC to prevent DDoS attacks attempting to maliciously internal staff. In addition, to detect whether the IP spoofing is required to apply the method displays the information in the packet distinguish abnormality.

Lastly, it is important to detect the newly appeared DDoS attack techniques and build control systems with various key logging sensors to respond 'control systems black box' to prevent accidents caused by the attacks. For all administrative institutions it takes the technical protection measures by utilizing a forensic techniques in the event of accidents, analyzing attack methods in a short time to respond. In addition to system administrators and security controllers control system availability undermine the efforts.

V. CONCLUSIONS

Various defense techniques have been studied so far since a single DDoS defense technique is not enough to defend for various DDoS attacks with new tactics. We introduced an automated detection techniques in this paper to prevent DDoS attacks on control systems environment and it is necessary to apply the filtering rule using 'local filter'. After configuring the sequence defense it is essential to have local filter between the ISP and IDC and various organizations. Ultimately, unknown to build a control system black box for DDoS attacks are proposed. Blackbotx detects quickly even when emerging attack techniques are appeared from attackers.

Environments that are installed with high-speed Internet network nationwide, such as South Korea, can adopt survey results proposed in this paper. In Israel, they used the Internet environment to discover the efficient detection of hybrid defense techniques for DDoS attacks under a government driven projects. Thus it is necessary to research and develop corresponding technologies proactively on each nations. The development of technology can be applied by placing the attack source, destination, routers, and many aspects of the defense techniques in the network throughout the state.

According to protection scheme, the public 'National Cyber Security Center (NCSC)' of the national intelligence service is respect to sectors. The Ministry of Defense with respect to national defense, national defense information is controlled in warfare Response Center in the future creation and sciences depertment. Affiliated with respect to private sector 'KISA Internet Incident Response Center’ is in charge of the control tower the role of security of private sector [5]. They primarily conduct research and development for the control system availability, one of the most important system in the country. The case study result of both the public sector and private sector results is desirable to expand into the field. An intensive co-work is required to identify the type of DDoS attacks evolving under the National Cyber Security Center to build a country-driven DDoS defense system that can proactively respond to the attack.

REFERENCES

[1] Samn Taghavi Zargar, James Hoshi, David Tipper, “A Survey of Defense Mechanism against Distributed Denial of Service Mechanism against Distributed Denial of Service Flooding Attacks”, IEEE Comm. Survey and Tutorials, 15(4), pp. 2046-2069, Feb. 2013

[2] Dongwon Seo, “Probabilistic filter Propagation and Scheduling against Distributed Denial-of-Service Attacks”, Ph. D Thesis, Korea University, Feb. 2013

[3] X. Geng and A. B. Whinston, “Defeating Distributed Denial of Service attacks”, IEEE IT Professional, 2(4), pp. 36-42, 2002

[4] R. M. Mutebi and I. A. Rai, “An Integrated Victim-based Approach against IP Packet Flooding Denial of Service”, International Journal of Computing and ICT Research, Special Issue Vol. 4, No. 1, pp. 70-80, Oct. 2010

[5] 2014 KISA report