Practical Approaches to the DRDoS Attack Detection based on Netflow Analysis

Jungtae Kim/Ik-Kyun Kim
Information Security Research Department
Electronics and Telecommunications Research Institute
Daejeon, South Korea
email: jungtae_kim/ikkim21@etri.re.kr

Koohong Kang
Dept. of Information and Communications Eng.
Seowon University
Cheongju, South Korea
email: khkang@seowon.ac.kr

***Abstract*—The paper proposes a practical method of detecting the Distributed Reflection Denial-of-Service Attack (DRDoS) in the Internet with the policy based routing and load balancing applied. To do so, the detection algorithm is provided separately accordingly to the underlying network infrastructure such as routing symmetry or asymmetry. Finally, it provides a practical way of detecting the reflection attacker, which connects the reflectors to command or trigger the IP Spoofed DNS (Domain Name Service)/NTP (Network Time Protocol) requests, by analyzing the connection information available on the Netflow enabled Routers.**

Keywords—DDoS; Reflection DoS; Netflow; Connection Traceback.

I. INTRODUCTION

The Distributed Denial-of-Service (DDoS) attack prevents the availability of a target system from normal user access by consuming computing resources including CPU, memory and network bandwidth that are necessary for network applications. Recent DDoS attack evolved with a series of intelligent attacks rather than a simple large scale traffic volume based attack types. The attack trends are especially targeting the enterprise servers or user applications with a subtle changes of packet header and consequently, spoofing the source IP address to hide identity and distributed reflectors to increase complexity for detection.

The DDoS attack, which triggers a high volume of traffics into the network backbone devices, is classified as three attack types; Volumetric, TCP State Exhaustion, and Application Layer. [1]. Firstly, the Volumetric Attacks mainly trigger a congestion to a target network or service by generating volumes of traffic which bottleneck the bandwidth of the Internet. Secondly, the TCP State Exhaustion Attacks disables the connection state table, which is designed to manage the connections or session states, of the load balancers, firewalls and application servers. Lastly, the Application Layer Attacks targets a particular layer 7 application services with less traffic volumes; consequently, it is hard to predict or release the attacks patterns such as the HTTP Get Flooding attacks.

Recently, the Distributed Reflection Denial-of-Service (DRDoS) attacks are major issues of the Internet and other service operators. A hacker controls several zombie PCs with a spoofed IP address and delivers Domain Name Service (DNS) or Network Time Protocol (NTP) requests to the distributed reflectors by changing the request source IP to a target victim PC's address. Consequently, the reflectors forward the amplified numbers of reply to a target victim PC, which consumes both bandwidth and CPU usages of the target. In other words, such amplification attack generates more reply traffic than requests by utilizing the reflectors and also security weakness of the NTP or DNS servers.

As the number of incidents involving such an amplification attack increases with NTP, DNS, and other UDP based protocols are vulnerable to the attacks, the ISP network suffers with a huge volumes of attack traffics. Although there were researches and practices conducted to prevent the victims from the DRDoS attack, there are no defense measures to detect and prevent the attack [4]. The difficulty of identifying the DRDoS attack is mainly due to the fact that activities of reflectors are not easy to identify whether it is normal or abnormal. To overcome the complexity of identifying the reflectors and DRDoS attacks, the paper reviews a basic context on the DRDoS attack in Section II. A proposal of a practical architecture to detect the attack by managing the netflow information in Section III. Details of the practical approach to identify the reflector at the ISP network with the proposed algorithm is explained in Section IV and also provides a flow based traceback method to identify an actual attacker or C&C those who control the reflectors even though their IP addresses are spoofed. Finally, the Section V introduces an implementation and evaluation on the experimental testbed settings with the conclusion in Section VI.

II. BACKGROUNDS

This section describes a basic information about the DRDoS attack and the conventional defense measures on the DNS Reflection Attacks.

A. Distributed Refection Denial of Service

In the year 2013 and 2014, the DDoS attack with DNS amplification had a maximum of 34.9% of the total DDoS attack traffic and 18.6% of the overall DDoS attack in the network. [2]. For the case of the attack on the Spamhaus in 2013, the DNS amplification attacks triggered a 300 Gbps traffics and the OpenDNS Security Lab reported that more than 5,000 different types of the amplification attacks are progressing at every hour in 2014 [3][4].

The Fig. 1 describes a simple amplification attack based on the DNS protocol that attackers normally send a spoofed DNS request to the open resolver (reflectors) which generates a large reply, such as 3876 bytes, to a target victim by using the ANY record type to produce maximum amplifications of the reply volumes.

 ISBN: 978-1-61208-516-6

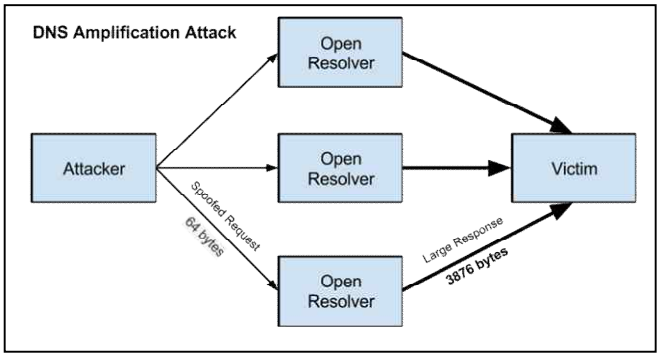

Figure 1. An Example of a DNS Amplification Attack. [3]

The reasons that amplification attack were often utilized by hackers are due to use of the amplification of the traffic volumes to the victim, the IP Spoofing using other distributed reflection servers by hiding own identity, and difficulties for the victims to prevent abnormal DNS services from the normal. Quite similar to the DNS amplification, the NTP is also commonly deployed with the DRDoS attacks which generating a huge volumes of the UDP traffics from the open NTP servers. As the US-CERT identified a list of known protocols and their associated bandwidth amplification factors [5] in the below table I. Most of the protocol is based on the UDP, which is a connection-less protocol that does not validate the source IP addresses, consequently increases chances of the amplification attacks significantly.

TABLE I. LIST OF KNOWN PROTOCOL WITH BANDWIDTH AMPLIFICATION FACTOR AND VULERABLE COMMAND

Protocol	*Bandwidth Amplification Factor*	*Vulnerable Command*
DNS	28 to 54	ANY requests
NTP	556.9	MON_GETLIST
SNMPv2	6.3	GetBulk request
NetBIOS	3.8	Name resolution
SSDP	30.8	SEARCH request
CharGEN	358.8	Character generation request
QOTD	140.3	Quote request
BitTorrent	3.8	File search
Kad	16.3	Peer list exchange
Quake Network Protocol	63.9	Server info exchange
Steam Protocol	5.5	Server info exchange
Multicast DNS (mDNS)	2 to 10	Unicast query
RIPv1	131.24	Malformed request
Portmap (RPCbind)	7 to 28	Malformed request

[a] UDP-Based Amplification Attacks from US-CERT [5]

B. *Conventional Defense on the DNS Reflection Attacks*

Conventionally, the firewall supports a control over the particular packet and IP address in order to prevent query replies but normal traffic can also be blocked which obviously increases the False Positives. Another problem is that attackers can easily manipulate other DNS query types such as the resource record digital signature (RRSIG) and public key (DNSKEY) [6] which triggers a high level of amplification. Also the BCP 38 [7] provides a mechanism to check an abnormal IP addresses from the routers within the ISP networks. As the ISP manages a ranges of the subscribers IP addresses, they can find and block abnormal IP addresses routed from the Internet. But that only is possible when the BCP38 is deployed at the entire ISP network levels. The DNS dampening [8] introduces an idea of penalty based system that prevent abnormal DNS requests based on the analysis of query type, response byte size and other parameters. But the duplicated requests from a single ID trigger false positives by preventing a normal DNS service users. The Response Rate Limiting (RRL) [9] controls the response volumes from the DNS servers with a preconfigured rate limit level. Recent attacks are distributed to stay within the boundary of the RRL limits in order to avoid such a defense mechanism. Lastly, Huistra [5] investigated the reflection attacks based on the netflow data. As the DNS reflection DDoS use a random port number from the distributed zombie PCs, netflow analysis provides a hint to find out a flow record with single DNS request packet with a large MTU up to 1500 bytes of response packet.

III. PRACTICAL APPROACH

Although various methods have been proposed, they have limitation on a practical deployment over the underlying network infrastructure such as technical difficulty on deployment or routing symmetry or asymmetry issues. As the reflection and amplification attacks are not always combined to trigger DRDoS attacks, we propose a generalized way of identifying the attacks based on the netflow analysis that can be collected from routers or switches. As the netflow is most widely used for traffic engineering purposes, we propose a way to overcome the routing asymmetry [10] in the ISP networks. To do so, we initially propose a three stage pipeline architecture to store netflow information in the flow table to manage and detect DRDoS within the time domain as shown in the Fig. 2.

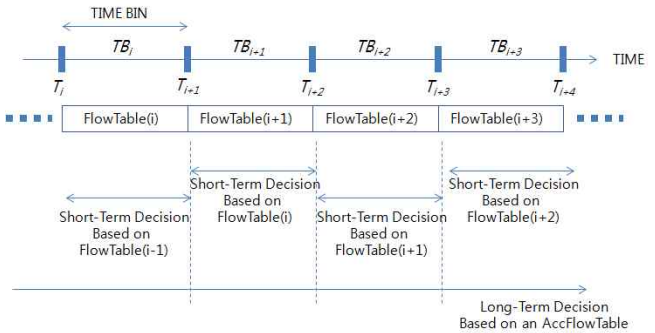

Figure 2. 3 Stage Pipe-Line Architecture for managing netflow information.

According to the proposed architecture in Fig. 2., time related flow information, that exists within a time bin, is saved into a separate flow tables as shown in the Table II. The table helps to identify a short-term decision and the aggregated flow table for a specific time periods are used for the long-term decision making respectively.

TABLE II. SAMPLE FLOWTABLE

Src IP	Dst IP	Src Port	Dst Port	No. of Packet	TotalSize
.	.	.	.	.	.

As shown in the Fig. 3, the flow table is constructed upon the netflow arrival, it initially check whether the DNS (port 53) or NTP (port 123) related flow record exists.

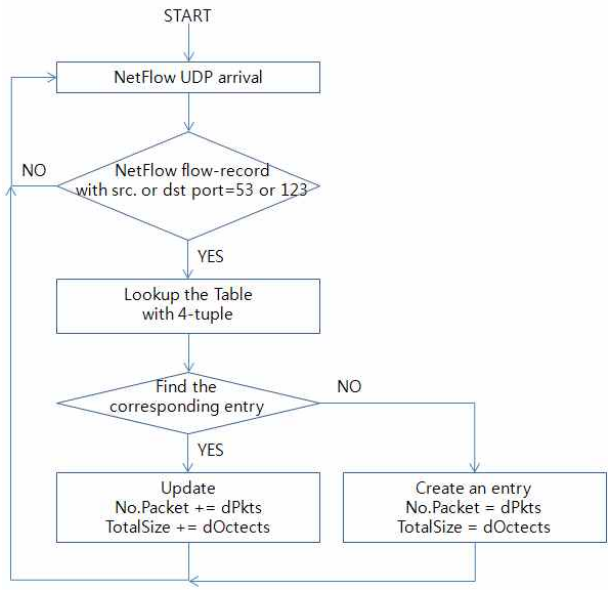

Figure 3. Flow Table Construction Process.

If the condition matches, then check the table entries with the 4 tuple (srcIP, dstIP, srcPort, dstPort) information. If it does exist, then the number of packets and bytes information is incremented, else then the initial entry is recorded into the table.

IV. PROPOSED ALGORITHM

Details of the practical approach to identify the reflector at the ISP network with the proposed algorithm is explained according to the multipath routing scenarios.

A. Routing Asymmetric

With a redundant design, the network traffic flows may follow two or more paths. The packets travelling from a source to a destination may follow a different path than when the packets travelling back. The reasons for the routing asymmetry is due to the Hot-potato routing and multipath routing. [10] Many researches were carried out by assuming the network traffics follows the routing symmetry but it is not the only case applied in real network environments. Consequently, the detection of the DRDoS depends on the monitoring points of the network. Nevertheless, by identifying the statistics information collected for the request and reply of a particular protocol used, DNS and NTP, within the netflow information can help to detect unbalance of the packet counts which can be used as a crucial determination factor for the DRDoS attacks. Consequently, the DRDoS attack detections can be identified by either monitoring the netflow information on attacker or victim side. Firstly, the as the attackers generally hide own IP address by the IP Spoofing, it is not easy to differentiate the normal and abnormal DNS and NTP queries. Nevertheless, in case when a particular flow is obtained in the routing asymmetric condition, we can identify DRDoS with a unidirectional traffics based on the short-term decision from the flow table.

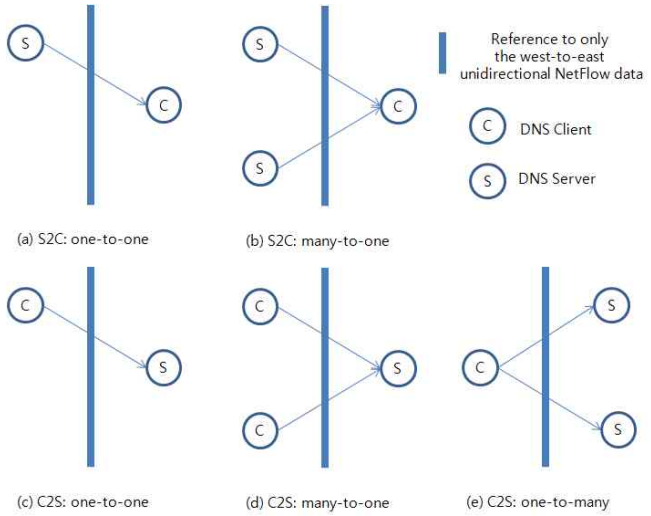

Figure 4. Detection Scenario for the Routing Asymmetric.

When the srcPort information matches with 53 or 123, those flows are unidirectional flows from the server to client (S2C), otherwise they are flows from the Client to Server (C2S). Above Fig. 4 shows every possible considerable detection scenarios for the DNS attacks. As we can only collect a unidirectional flow due to the nature of asymmetric routing, considerable scenario can be separated into (a) and (b) for the S2C connections and (c), (d) and (e) for the C2S connections. Based on the detection scenario, we can summarize the possibility for detecting the DRDoS attacks as follows;

- S2C : in one server-to-one client case, the reflection and amplification detection is possible with the number of packets and its byte size respectively for the point-to-point connection that containing a reply message from a server to a client

- S2C : in many servers-to-one client case, the reflection and amplification detection is possible with the number of packets and its byte size respectively for the multiple servers to a client connections that containing reply messages from the servers to a client. As a normal client use 1 or 2 DNS servers (primary and secondary), more than 3 DNS reply from the servers to a client can be identified as a reflection attack. In case with 2 DNS servers are configured, when the number of packet and byte size between corresponding flows are similar, those servers are acting as the reflectors.

 ISBN: 978-1-61208-516-6

- C2S : in one client-to-one server case, the reflection attacks can be identified with the number of packets and byte size distribution of a request message from a client to a server. Although a general packet size of the DNS request message vary, but the fixed packet size of a reflection attack based on the script program causes a low standard deviation of packet size distribution.

- C2S : in many clients-to-one server case, the reflection attacks can be identified with the number of packets and byte size distribution of the request messages from clients to a server. If the number of packets and byte size distribution of the request messages from a group of clients are similar, then those client have a chance of controlled by a hacker.

- C2S : in one client-to-many servers case, which is similar to the DNS reflection attack with reflectors, the reflection attacks can be identified when more than 3 or more request messages are sent to the servers. When only 2 request messages are detected, the number of packets and byte size distribution of the request messages helps to find reflectors.

According to the scenario, we do not consider the distributions of UDP port numbers due to a script based reflection attacks generally use a fixed port number. The Fig. 5 and Fig. 6 show a pseudo-code for the S2C and C2S scenarios respectively. Lastly, the algorithm 3, in Fig. 7., shows a C2S scenario with many clients-to-one server case.

Algorithm 1 Detecting IPs receiving unusual responses S2C

```
1  flows = getAggregatedResponsesToDestinationIPAddr( );
2  for each flow in flows {
3  if flow.Pkts > N1
4  report flow.DstIPAddr;
5  elseif flow.Pkts > N2
6  if flow.AverageSize > N3
7  report flow.DstIPAddr;
8  endif
9  if flow.NoSrcIPAddr > 2
10 report flow.DstIPAddr;
11 elseif flow.NoSrcIPAddr > 1
12 if (flow1.Pkts-flow2.Pkts < N4
   and flow1.AverageSize-flow2.AverageSize < N5)
13 report flow.DstIPAddr;
14 Endif }
```

Figure 5. Algorithm 1 Detecting IPs receiving unusual responses S2C.

Algorithm 2 Detecting IPs generating unusual requests C2S

```
1  flows = getAggregatedRequestsFromSourceIPAddr( );
2  for each flow in flows {
3  if flow.Pkts > N6
4  report flow.SrcIPAddr;
5  elseif flow.Pkts > N7
6  if flow.StdSize < N8
7  report flow.SrcIPAddr;
8  endif
9  if flow.NoDstIPAddr > 2
10 report flow.SrcIPAddr;
11 elseif flow.NoDstIPAddr > 1
12 if (flow1.Pkts-flow2.Pkts < N9
   and flow1.AverageSize-flow2.AverageSize < N10)
13 report flow.SrcIPAddr;
14 Endif }
```

Figure 6. Algorithm 2 Detecting IPs generating unusual requests C2S.

Algorithm 3 Detecting IPs generating unusual requests C2S

```
1  flows = getAggregatedRequestsToDestinationIPAddr( );
2  for each flow in flows {
3  if (flow.x.Pkts-flow.y.Pkts < N11
   and flow.x.AverageSize-flow.y.AverageSize < N12)
4  report flow.x.SrcIPAddr and flow.y.SrcIPAddr;
5  }
```

Figure 7. Algorithm 3 Detecting IPs generating unusual requests C2S.

The algorithm 1-3 starts with flow generation based on the destination IP address after filtering the destination port number of 53 and 123 (Figs. 5-7). Consequently, the flows collects every DNS or NTP related flow records that are targeted for a single targeted IP.

B. Routing Symmetric

When the forward and reverse paths of the packet streams between the two end points are identical, it is called that the packet streams routed symmetrically. By assuming the routing symmetric, it means that the DNS or NTP request and reply packet exist in a monitoring up and down link simultaneously. When a particular flow is obtained in the routing symmetric condition, we can identify the DRDoS attacks with a set of bidirectional traffics based on the short-term decision from the flow table. Fig. 8 shows a detection scenario for the routing symmetric environment.

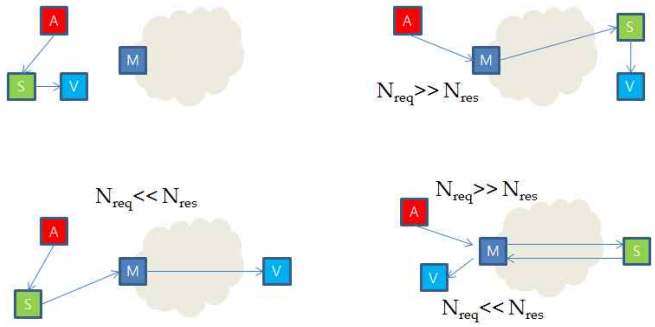

Figure 8. Detection Scenario for the Routing Symmetric. (A: Attacker, S: DNS or NTP Server, V: Victim, M: NetFlow Mornitoring)

As shown in Fig. 8, there are 4 specific cases for the detection scenario based on the routing symmetric.

- Scenario 1 : N_{req} >> N_{res}

It is a case with both reflection server (S) and victim (V) PC existing within a stub network. Therefore the spoofed srcIP of DNS or NTP requests N_{req} count is much higher than the response N_{res} within the flow monitor at the entry to a stub network. By obtaining the spoofed srcIP used for the DRDoS attack, we can find out the victim hosts that reside in a stub network. On the other hand, we can also think of an opposite case where only attacker (A) reside within a stub network, which obviously resulting a numbers of the request N_{req} counts from the srcIP spoofed attack trials.

 ISBN: 978-1-61208-516-6

- Scenario 2 : N_{req} << N_{res}

It is a case when an identifiable victim hosts (V) exist within a stub network. Consequently, the spoofed srcIP of DNS or NTP response N_{res} count is much higher than the requests N_{req} within the flow monitor at the entry to a stub network. On the other hand, we can also think of an opposite case where both attacker (A) and reflector (S) reside within a stub network, which obviously resulting a numbers of the response N_{res} to the victim.

- Scenario 3 : N_{req} >> N_{res} & N_{req} << N_{res}

Scenario 3 is the only case with the reflector (S) residing within a stub network. Therefore, the spoofed srcIP of DNS or NTP requests N_{req} >> N_{res} and reverse relations for the victim IP address. But the problem is that the spoofed srcIP is equal to the victim IP address for the reflection attacks. So the detection is not possible only with variances between request and response packets of those attacks. For this problem, the proposed three scenarios according to the C2S and S2C based algorithm 1, 2, 3 and following algorithm 4, in Fig. 9., helps to identify the DRDoS attacks.

Algorithm 4 Detecting IPs mis-matching requests and responses

```
1  flows = getAggregatedSrc&DestinationIPAddr( );
2  for each flow in flows {
3  if (flow.RequestPkts-flow.ResponsePkts > N13)
4  report flow.SrcIPAddr;
5  elseif (flow.ResponsePkts-flow.RequestPkts > N13)
6  Report flow.DstIPAddr;
7  }
```

Figure 9. Algorithm 4 Detecting IPs mis-matching requests and responses.

The parameters from N1 to N13 are dependent generally on a particular number of devices running NTP and DNS clients within a measuring network domain, but it can be configured depend on daily average counts from the flow statistics.

V. IMPLEMENTATION & EVALUATIONS

The proposed DRDoS detection algorithms are implemented according to the test scenarios as shown in the Fig. 10.

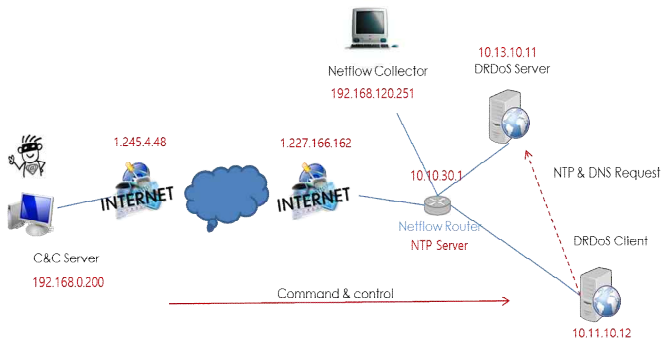

Figure 10. DRDoS Testbed.

The experimental testbed consists of a netflow enabled router with a preconfigured as a NTP server, and DRDoS client and server is configured with different virtual network. The control of the DRDoS client is done via the Command and Control (C&C) server with a ssh connection. The DRDoS scenario based simulation is conducted for a timebin of 3 minutes (180 seconds). Following table summarizes all possible cases for the DRDoS attack with the predefined parameters T1~3.

TABLE III. DRDOS ATTACK AND VICTIM CASES

Network	CASE	Simulation for timebin (180 sec)
Asymmetric network	Attack CASE 1	T1 : 1000 / T2 : 2 - Total Query count (dPkts in flow) for a Source IP > T1 (1000) within a timebin
	Attack CASE 2	T1 : 1000 / T2 : 2 - Total Query count for a Source IP has Number of Destination IPs > T2 (2)
	Victim CASE 1	T1 : 1000 / T2 : 2 / T3 : x900 - Total Response Packet count for a Source IP has Number of Destination IP > T1 (1000)
	Victim CASE 2	T1 : 1000 / T2 : 2 / T3 : x900 - Total Response Packet count for all Destination IP has Number of Response Server > T2 (2)
	Victim CASE 3	T1 : 1000 / T2 : 2 / T3 : x900 - Total Response Packet count for all Destination IP has Total Response Packet Size (dOctets)> Number of Response Packet x T3 (900)
Symmetric network	Attacker CASE 3	T1 : 10 - For a Src & Dst IP Pair, Total Query Packet count - Total Response Packet count > T1 (10)
	Attacker CASE 4	- For all Query Packet, Number of corresponding Reply Packet = 0
	Victim CASE 4	T1 : 10 - For a Src & Dst IP Pair, Total Query Response count - Total Query Packet count > T1 (10)
	Victim CASE 5	- For all Response Packet, Number of corresponding Query Packet = 0

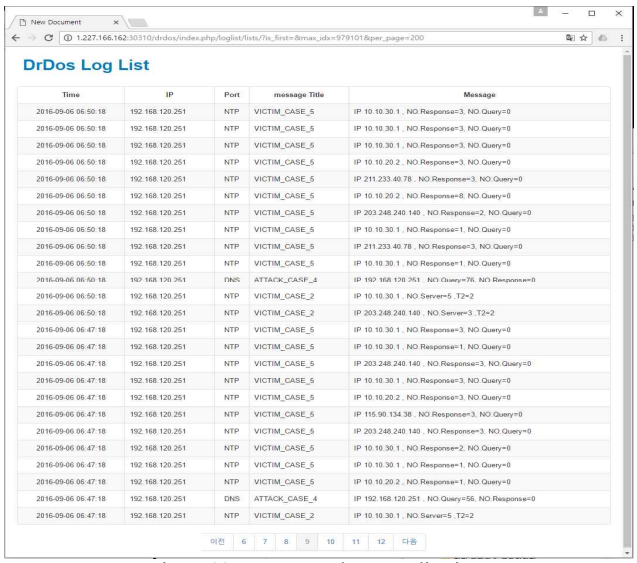

Figure 11. DRDoS Web UI Application.

Results were obtained from a web application in the Netflow Collector (NC) that collect netflow information from the router via established UDP port. The DRDoS log lists, as shown in the Fig. 11., display the information including detection time, netflow collector IP, port, message title, and detailed log messages. Because the testbed was setup in a synchronous network environment with various client PCs exist, many NTP related VICTIM_CASE_5 messages exist due to their NTP client services. The results were shown with actual NTP server IPs including the router (10.10.30.1) that has no corresponding NTP query packet but responses only. Further evaluation is necessary for testing the algorithms and results in the asynchronous network settings.

VI. CONCLUSIONS

The paper proposed a practical method of detecting the Distributed Reflection Denial-of-Service Attack (DRDoS) in the Internet with the policy based routing and load balancing applied. To do so, the detection algorithm is provided separately in order to overcome the technical and practical limitations for deploying over the ISP network infrastructure.

To cope with the technical limitations of the DRDoS detection methods introduced, we have proposed a generalized ways of identifying the attacks based on the netflow information that can be collected from most of the routers or switches. The three stage pipeline architecture was proposed to store netflow information in the flow table to manage and detect the DRDoS attacks within a specific time domain. We also proposed a practical way to overcome the routing asymmetry issues with the three algorithms that help to analyze the variances between request and response UDP attack packets (DNS.NTP). Consequently, the DRDoS attack detections can be identified by either monitoring the netflow information on attacker or victim side depending on the detection scenario. Although the real world ISP network is based on the routing symmetric environment, the proposed detection scenario enables to identify the DRDoS attacks based on the four specific cases depending on the actual location of the attacker, DNS or NTP server, victim, and netflow monitoring point within a stub network. Finally, future work remains for the deployment optimization and evaluations by considering the Internet Autonomous System (AS) topology [11] depending on the existing ISP network infrastructure.

ACKNOWLEDGEMENT

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government (MSIP) (No.R-20160222-002755, Cloud based Security Intelligence Technology Development for the Customized Security Service Provisioning).

REFERENCES

[1] Verisign, “iDefense Threats & Trends Report-Types of DDoS Attacks,” 2015. Available: https://www.verisign.com/en_US/security-services/ddos-protection/types-of-ddos-attacks/index.xhtml [retrieved: Oct, 2016]

[2] D. C. MacFarland, C. A. Shue, and A. J. Kalafut. “Characterizing Optimal DNS Amplification Attacks and Effective Mitigation,” In Passive and Active Measurement, Springer International Publishing, 2015.

[3] D. Cornell, “DNS Amplification Attacks,” March 2014. Available: https://labs.opendns.com/2014/03/17/dns-amplification-attacks/ [retrieved: Oct, 2016]

[4] F. J. Ryba, M. Orlinkski, M. Wahlisch, C. Rossow, and T. C. Schmidt, “Amplification and DRDoS Attack Defense – A Survey and New Perspectives,” arViv preprint arXiv:1505.07892, 2015

[5] US-CERT, “UDP-Based Amplification Attacks- Alert (TA14-017A),“ April 18, 2016. https://www.us-cert.gov/ncas/alerts/TA14-017A [retrieved: Oct, 2016]

[6] R. Arends and et. al. “Request for Comments: 4034 - Resource Records for the DNS Security Extensions”, Network Working Group, IETF, March 2005.

[7] P. Ferguson and D. Senie, “Request for Comments: 2827 - Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing, Network Working Group, IETF, May 2000.

[8] T. Rozekrans, “Defending against DNS reflection amplication attacks”, University of Amsterdam, February 14, 2013.

[9] LISA14, “DNS Response Rate Limiting”, Internet Systems Consortium, November 2014. https://www.isc.org/wp-content/uploads/2014/11/DNS-RRL-LISA14.pdf [retrieved: Oct, 2016]

[10] J. Wolfgang, D. Maurizio, and K. Claffy, “Estimating Routing Symmerty on Single Links by Passive Flow Mesaurements,” in Proc. of IWCMC’10, 2010, pp. 473-478.

[11] K. Park and H. Lee, “On the Effectiveness of Route-Based Packet Filtering for Distributed DoS Attack Prevention in Power-Law Internets,” ACM SIGCOMM 2001.

 ISBN: 978-1-61208-516-6