Journal of information and communication convergence engineering
http://jicce.org

J. Inf. Commun. Converg. Eng. 21(3): 192-197, Sep. 2023 Regular paper

Quantitative Approach for Calculating DRDoS Risk

Young-Ryul Choi and Nam-Kyun Baik*, ***Member***, ***KIICE***

Department of IT Media Engineering, Duksung Women's University, Seoul 01369, Republic of Korea

Abstract

A Distributed reflection denial of service (DRDoS) is a variant of DDoS attacks that threatens the availability of services to legitimate users. In response to this evolving threat landscape, the cybersecurity industry and service providers have intensified their efforts to develop effective countermeasures. Despite these efforts, attackers continue to innovate, developing new strategies and tools while becoming more sophisticated. Consequently, DRDoS attacks continue to be harmful. Therefore, ongoing research and development is essential to improve defense against DRDoS attacks. To advance our understanding and analysis of DRDoS attacks, this study examines the unique characteristics of DRDoS attacks and quantifies the risks involved. Additionally, it adopts a quantitative rather than traditional qualitative methods to derive and apply risk, particularly the probability of loss that can be caused by DRDoS attacks.

Index Terms: Amplification, Distributed reflection denial-of-service (DRDoS), Possibility of loss, Reflector Server

I. INTRODUCTION

Distributed reflection denial of service (DRDoS) is a more advanced DDoS attack type. The unique modus operandi of DRDoS leverage the publicly accessible user datagram protocol (UDP) primarily used by non-connection-oriented servers, such as the network time protocol (NTP) and domain name system (DNS), to effectively launch attacks [1]. The ability of UDP to transmit packets without first verifying them facilitates communication connectivity.

However, this reduces the communication reliability. Consequently, despite being unsolicited, connections are successfully established, which causes victims to unintentionally consume traffic [2]. The reflection and amplification functionalities of the protocol relay and amplify a massive amount of traffic, overwhelming the victims in the process. The resulting surge in traffic prevents users from using the service access normally and reduces their availability.

The origin of such attacks can be traced back to a massive DDoS attack on the financial sector in 2008 and a significant DDoS disruption on June 25, 2013 [3]. Popular service providers, such as Gabia, LG Uplus, and KT, recently fell victim to these attacks in January and February 2023, resulting in sustained damage [4].

Cybersecurity is still a major concern regarding persistent attack-related damage. With the continuous evolution of network technology, it is anticipated that increasingly sophisticated attack methods will result in significant damage.

To effectively safeguard services against relentless attacks, it is essential to develop countermeasures that can conduct a comprehensive risk analysis. This study introduces a novel quantitative approach, which supersedes traditional qualitative approaches, to estimate the risk associated with DRDoS attacks and implements this approach to counter such threats.

The remainder of this paper is structured as follows: Section 2 provides a succinct overview of the types and characteristics of DRDoS attacks. Section 3 proposes a methodology for evaluating the risks associated with DRDoS attacks. Sec-

Received 31 May 2023, **Revised** 31 July 2023, **Accepted** 21 August 2023
***Corresponding Author** Nam-Kyun Baik (E-mail: namkyun@duksung.ac.kr)
Department of IT Media Engineering, Duksung Women's University, Seoul 01369, Republic of Korea

Open Access https://doi.org/10.56977/jicce.2023.21.3.192 print ISSN: 2234-8255 online ISSN: 2234-8883

tion 4 validates the arguments presented earlier through experimentation and evaluation. Finally, the paper concludes with a summary of the findings.

II. TYPES of DRDoS ATTACKS

In DRDoS attacks, attackers hijack a victim's IP address and use a public reflector server to transmit packets. The reflector server sends the victim a return packet in response to the transmitted packet it received from the victim's altered IP. Consequently, despite not initiating a request, the victim's client continuously exhausts the bandwidth, violating its availability [5]. The DRDoS attack scheme supports various forms, such as TCP, DNS, and NTP amplification.

A. TCP Amplification Attack

The three-way handshake feature of TCP is manipulated in a TCP amplification attack to increase traffic volume and affect the victim's network.

The following is the underlying principle of the TCP three-way handshake. First, a user sends a SYN packet to the TCP server to establish a connection. Next, the TCP server responds with a SYN/ACK packet. Finally, the user sends an ACK packet back to the server, successfully establishing a connection [6]. To exploit this mechanism, attackers send connection requests to numerous TCP servers while posing as the victim address, in SYN packets. Then, these TCP servers respond with SYN/ACK packets. However, because the IP address of the requesting user has been falsified, the unsuspecting victim server cannot send the final ACK packet. The server retransmits SYN/ACK packets to the victim in accordance with the TCP protocol. Consequently, the victim is overloaded with a backlog of reconnection request packets, which eventually results in service failure owing to excessive traffic.

B. DNS Amplification Attacks

A DNS amplification attack uses the query structure of DNS servers to increase the traffic volume, affecting the victim's network.

A specific record type is identified when transmitting a query to a DNS server to verify a certain record value. If the query transmission type is ANY, the corresponding DNS server reciprocates with all types of record information about the IP address [7]. Using this method, when attackers mimic the source as the victim's address and disseminate ANY-type queries to a multitude of DNS servers, there is a surge in the amount of response traffic relayed to the victim, disrupting service.

C. NTP Amplification Attacks

An NTP amplification attack is an adversarial technique that uses the 'monlist' function of the NTP protocol to dramatically increase network traffic, which adversely affects the targeted network.

The mechanics of an NTP amplification attack are as follows: the attacker uses the 'monlist' function, which provides a list of the most recent clients who have accessed the NTP server. A 'monlist' request triggers approximately 600 responses, totaling more than 4,000 bytes in response packets [8]. Utilizing this principle, when attackers spoof the victim's address as the source and dispatch 'monlist' requests to numerous NTP servers, the amount of response traffic transmitted to the unsuspecting victim significantly outpaces the traffic sent. The victim is then inundated with unsolicited response traffic, which uses up all available network bandwidth and ultimately disrupts service.

D. Amplification Rate Based on the Execution of DRDoS Attacks

DRDoS attacks can manifest in several ways. The amplification factor can also vary depending on the attack protocol that is used, as shown in Table 1 [9]. This study aims to incorporate the variable amplification rates corresponding to each protocol into a model to estimate the risk associated with DRDoS attacks.

Table 1. Amplification rate by protocol

Protocol name	Port number (UDP)	Amplification rate (multiple)
DNS	53	28~54
NTP	123	556.9
SNMPv2	161	6.3
SSDP	1900	30.8
LDAP	389	46~55

Numerous countermeasures have been proposed against DRDoS attacks. For example, upgrading the server with a new version that excludes the 'monlist' function to mitigate attacks that leverage an NTP server.

However, such a solution would necessitate updating all Internet-connected servers that are still running current versions, which would be a challenging task.

Therefore, this study proposes a novel methodology for assessing the risks that DRDoS attacks pose.

III. RISK ASSESSMENT for DRDoS ATTACK RESPONSE

A DRDoS attack uses a publicly accessible reflector server to disrupt services, such as denying regular users access to the services they conventionally use—an infringement on their availability.

This study first expressed the attack risk of DRDoS using Equation (1) as follows:

DRDoS Attack Risk = Degree of loss Probability of loss (1)

The magnitude of the loss indicated by the formula can be interpreted subjectively and depends on the implementing entity. Therefore, this study sought to develop a quantitative approach to assess the likelihood of incurring losses.

A. Rationale for a Limited DRDoS Risk Assessment Approach

Network attacks such as DRDoS affect services by exceeding the capacity of the internal buffers that normal communication protocols allow. Countermeasures should consider the number of internal buffers.

However, a solution that considers the buffer capacity is undesirable. Therefore, Table 2 shows the internal network flow over time for a typical operational service and Fig. 1 shows that after a certain amount of time, depending on the attack, the buffer's capacity is fixed at a maximum and only the number of dropped packets remains constant. Therefore, if the buffer amount is considered when calculating risk, only the same result can be obtained after a certain period. Therefore, this study aims to develop a quantitative method that does not consider the buffer capacity when calculating the risk of DRDoS.

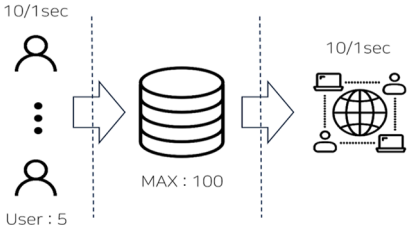

Fig. 1. Basic service operation

Table 2. Internal state according to service operation

Incoming packets	Time	Buffer size	Services	Drop packets
50	1	40	10	0
50	2	80	10	0
50	3	100	10	20
50	4	100	10	40
50	5	100	10	40
50	6	100	10	40

B. Estimation of Potential Traffic Volume Using Identical Reflectors

Publicly accessible servers are used as reflectors in DRDoS attacks. Potential amplification varies depending on the protocol used in the attack, and the frequency of attacks may differ.

This section estimates the traffic volume generated when a single reflector is used exclusively. Fig. 2 shows the configuration of a DRDoS attack that uses an identical reflector.

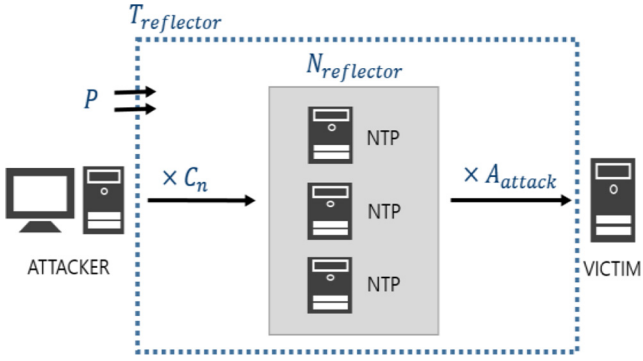

Fig. 2. Configuring an attack using a single reflector

Multiplying the size of the input packet (P) by the frequency of attack execution (C_n) and the number of protocols used during the assault ($N_{reflector}$) yields the risk associated with using an identical reflector. Subsequently, the number of output packets can be calculated by multiplying the amplification rate (A_{attack}) generated by each protocol.

Equation (2) illustrates the traffic volume that can be generated from the same reflector. This equation allows the derivation of the potential traffic volume when an attack is performed using a single protocol.

$$T_{reflector} = P \times C_n \times N_{reflector} \times A_{attack} \quad (2)$$

C. Estimation of Traffic Volume using Multiple Reflectors

In real-world scenarios, an adversary deploys a DRDoS attack that is not confined to a single protocol or reflector. Instead, various attack vectors are used. This section outlines an attack configuration that resembles real-world attack patterns, as shown in Fig. 3. Additionally, it calculates the comprehensive risk associated with launching a DRDoS attack.

The potential traffic volume ($T_{reflector\ -N}$) emanating from different reflectors was computed using Equation (2), which evaluates the traffic volume attributable to each reflector. Using this methodology, we calculated the potential traffic volume from a DRDoS attack execution using the traffic vol-

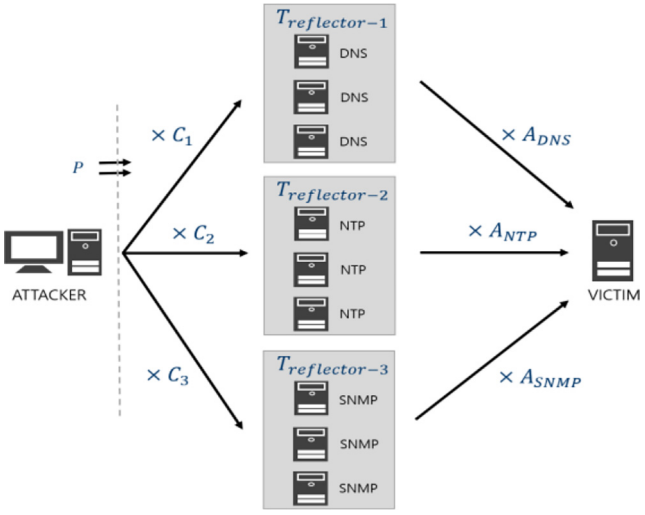

Fig. 3. Configuring an attack using a multiple reflector

umes from all the reflectors involved in the attack. Equation (3) provides the comprehensive traffic volume resulting from a DRDoS attack.

$$T_{total} = \Sigma_{i=1}^{N} T_{reflector-i} = T_{reflector-1} + T_{reflector-2} + \cdots + T_{reflector-N} \quad (3)$$

D. Average Traffic Volume Generated by a Single Reflector

The next step involves determining the average traffic volume ($T_{average}$), which can be generated using a single protocol. This is achieved by dividing the entire traffic volume (T_{total}) generated by the DRDoS attack by the cumulative count of reflectors ($T_{total-reflector}$) used in the attack.

$$T_{average} = T_{total} \div T_{total-reflector} \quad (4)$$

E. Average Traffic Volume Generated by a Single Attack Source within a Single Reflector

This section describes how to calculate the average traffic volume generated by a single attack source within a single reflector. This calculation used the average traffic volume per reflector derived from the preceding equations. Because the calculated traffic volume currently includes numerous attack iterations, the average number of attack executions must be determined. The procedure for computing the average traffic volume for a specific source is described in Equations (5)-(7) as follows:

First, the number of attacks executed per protocol is summed to obtain the total number of attacks conducted during an attack. The average number of attacks executed per protocol is determined by dividing this total by the overall number of reflectors used in the attack. The average traffic volume generated by an each attack source was calculated by dividing the previously estimated average traffic volume per protocol by the currently derived attack count.

$$C_{total} = (C_1 \times N_{reflector-1}) (C_2 \times N_{reflector-2}) + \cdots + (C_n \times N_{reflector-n}) \quad (5)$$

$$C_{average} = C_{total} \div N_{total-reflector} = C_{average} \quad (6)$$

$$T_{attack} = T_{average} \div C_{average} = T_{attack} \quad (7)$$

F. Estimation of Permissible Attack Sources by Load Monitoring

Load monitoring is crucial for mitigating network attacks. It is possible to manage key metrics, such as the number of server connection sessions and traffic load, by periodically executing load monitoring. This approach facilitates the tracking of the server's maximum permissible traffic volume (T_{server}) and enables the expression of the number of attack sources (P_{source}) in accordance with Equation (8).

$$P_{source} = \frac{T_{server}}{T_{attack}} \quad (8)$$

However, in servers that typically provide services, there is inevitable consumption of existing traffic (T_{use}) resulting from service use by existing users. Therefore, Equation (9) can be used to represent the actual number of permissible attack sources (R_{source}) in the event of a DRDoS attack.

$$R_{source} = \left[\frac{T_{server} - T_{use}}{T_{attack}}\right] \quad (9)$$

G. Probability of Loss Incurrence owing to DRDoS Attacks

The likelihood of loss resulting from DRDoS attacks can be illustrated using Equation (10) if represented using a binomial distribution. This suggests that the aggregate probability of loss (P_{loss}), which can occur when an attack attempt (N) exceeds the minimum permissible number of attack sources (R_{source}), causes packet loss.

When determining the success probability using a binomial distribution, the first-in first-out (FIFO) characteristics of network communications make it impossible to prioritize specific traffic for transmission and connection [10]. Additionally, the success probability of attack traffic accessing can vary significantly depending on the testing environment configurations. Thus, for the incoming traffic, this study assumes a 50% success probability.

$$P_{loss} = \binom{N}{R_{source}} p^{R_{source}} (1-p)^{N-R_{source}} \quad (10)$$

IV. EXPERIMENTAL RESULT AND ANALYSIS

The results of the test attack risk can vary significantly when the size of the initial incoming input packet varies.

Therefore, to derive precise results prior to the test, the test environment configuration was adjusted such that the size of all incoming packets was uniformly fixed at 1 byte to enable the evaluation of its impact on the degree of loss occurrence.

A. Experiment and Analysis of the Effect of Amplification Rate Variations on the Number of Permissible Sources

The experiment used a single protocol to examine the impact of the amplification rate (which was incrementally increased by two from ten to 20 in this test) inherent to the execution protocol on the change in the risk of attack (that is, the permissible number of attack sources). The settings for all other tests matched those in Table 3.

Table 3. Test setting value 1

Type	C_n	$N_{reflector}$	T_{server}
50	1	40	10

As shown in Fig. 4, the results demonstrated a decrease in the number of permissible attack sources within the server as the amplification rate increased. This shows that, if a high amplification ratio protocol is used on the same server, even some attack sources can cause service disruptions.

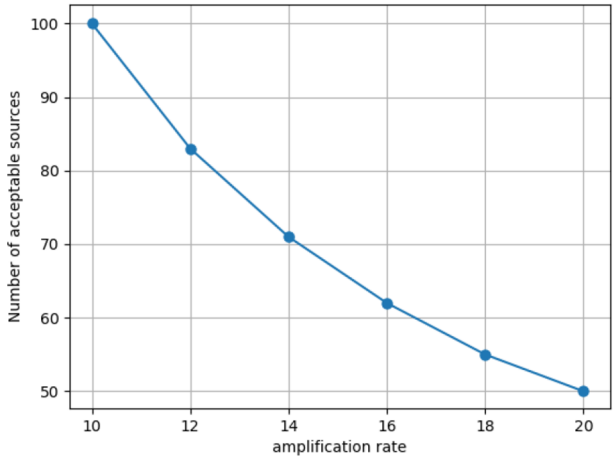

Fig. 4. Test results according to the amplification rate

Additionally, using subsequent experiments, a rapid response to attacks can be facilitated by establishing intrusion network detection, identifying unauthorized traffic access, and referring to the permissible number of attack sources (N) derived from the test execution when traffic access requests exceeds this number.

B. Potential for Loss Incidence Based on the Frequency of DRDoS Attack Executions

The subsequent experimental setup used a multi-protocol configuration and three commonly used protocols in actual DRDoS attack implementations. Table 1 shows the amplification rate values inherent to the test execution protocol and the amplification rate values that might occur during a real attack execution. The experiment was conducted in an environment designed to simulate a real attack. The test settings for the other protocols are listed in Table 4. This experiment was used to validate the impact on attack risk (probability of loss occurrence) given the frequency of DRDoS attack executions.

Table 4. Test setting value 2

Type	C_n	$N_{reflector}$	A_{attack}	T_{server}	T_{use}
DNS	10	5	54		
NTP	15	10	556	10,000	5,000
SNMP	20	15	6		

According to the outcomes of Equations (1)-(10) for such an experimental setup, as shown in Fig. 5, the test results show a sharp increase in the attack risk (probability of loss) as the frequency of attack executions increases. This suggests that packets from existing service users are forced to compete with an influx of DRDoS attack packets, impeding normal user packets from accessing the service. This gradually reduces the number of packets that existing users are permitted to use, resulting in service denial and compromising availability.

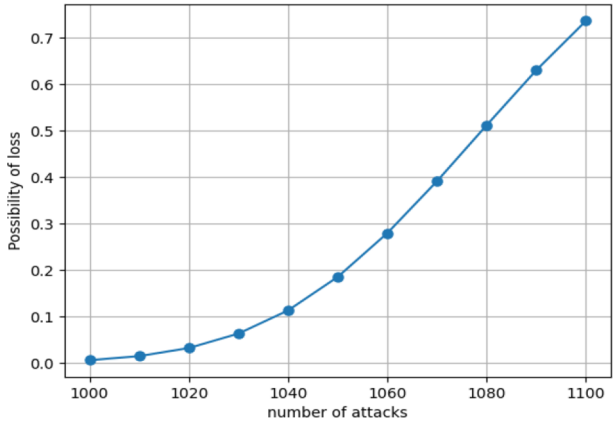

Fig. 5. Risk of DRDoS attacks by number of attacks

IV. DISCUSSION AND CONCLUSIONS

DRDoS attacks continue to be a contemporary , causing significant harm and challenges for effective mitigation because of their escalating sophistication. These difficulties are further exacerbated and made impractical by the defining characteristic of DRDoS attacks, the manipulation of source IP addresses.

Although several strategies have been proposed to counteract DRDoS attacks, many of them pose significant practical implementation challenges. Therefore, this study sought to use a novel quantitative approach rather than qualitative approaches to mitigate DRDoS attacks.

Moreover, we conducted extensive experimentation and verification to evaluate the potential risks associated with DRDoS attacks. This study meticulously modulated the amplification rate unique to each protocol used during DRDoS attacks and altered the frequency of attack execution. We could investigate their individual impacts on the risk of attack (probability of loss) using this process.

The rigorous methodology outlined and the insights generated from this research are intended to provide a robust framework that can be harnessed to strengthen defense against DRDoS attacks.

REFERENCES

[1] S. J. Choi and J. Kwak, "Enhanced server availability for DDoS amplification attack using CLDAP protocol," *Korea Information Processing Society*, vol. 7, no.1, pp. 19-26, Jan. 2018. DOI: 10.3745/KTCCS.2018.7.1.19.

[2] M. Kuhrer, T. Hupperich, C. Rossow, and T. Holz, "Exit from hell? Reducing the impact of amplification DDoS attacks," *Open access to the Proceedings of the 23rd USENIX Security Symposium*, San Diego, USA, pp. 111-125, 2014.

[3] Y. H. lee and J. H. lee, "Analysis of an association between CKC and CSC items in the cases of 7.7 and 3.4 DDoS," *The Korea Society of Information Technology Policy & Management*, vol. 14, no. 4, pp. 3059-3064, 2022.

[4] K. A. Kim. (2023, April 1) [2023 DDoS Response Report] Companies and institutions 'staggered' by DDoS funding bombardment. [Online] Available: https://www.boannews.com/media/view.asp?idx=115528.

[5] Y. A. Hur and K. H. Lee, "A Study on Countermeasures of Convergence for Big Data and Security Threats to Attack D0.RDoS in U-Healthcare Device," *Journal of the Korea Convergence Society*, vol. 6, no. 4, pp. 243-248, Aug. 2015. DOI: 10.15207/JKCS.2015.6.4.243.

[6] M. Kuhrer, T. Hupperich, C. Rossow, and T. Holz, "Hell of a handshake: Abusing TCP for reflective amplification DDoS attacks," *USENIX Workshop on Offensive Technologies*, 2014.

[7] K. T. Lee, S. S. Baek, and S. J. Kim, "Study on the near-real time DNS query analyzing system," *Korea Institute Of Information Security And Cryptology*, vol. 25, no. 2, pp. 303-311, Apr. 2015. DOI: 10.13089/JKIISC.2015.25.2.303.

[8] H. S. Choi and H. J. Lee. "A study on amplification DRDoS attacks and defenses," *Journal of Korea institute of information, electronics, and communication technology*, vol. 8, no. 5, pp. 429-437, Oct. 2015. DOI: 10.17661/jkiiect.2015.8.5.429.

[9] Korea Internet Security Agency. (2021, August) DDoS attack response guide. [Online] Available: https://www.krcert.or.kr/kr/bbs/view.do?bbsId=B 0000127&nttId=36186&menuNo=205021.

[10] Internet Protocol : RFC 791, (1981, Sep 1) [Online] Available: http://www.ietf.org/rfc/rfc791/.

Young Ryul Choi

Young Ryul Choi received his bachelor's degree in engineering from Busan National University of Foreign Studies in 2021. He is currently pursuing his master's degree at Duksung Women's University. His research interests include network security, security consulting, and convergence security.

Nam Kyun Baik

N Nam-Kyun Baik is an assistant professor in the Department of Cyber Security at Duksung Women's University. He held a senior researcher position with Korea Internet & Security Agency (KISA) for 17 years before becoming a professor at Busan National University of Foreign Studies in the Department of Smart Convergence Security. He is passionate about convergence security, security consulting, information security management system, AI security, and IoT security.