JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지 Vol. 24, No. 12: 1670~1675, Dec. 2020

DRDoS 공격에 대한 다단계 탐지 기법

백남균*

Multi-level detection method for DRDoS attack

Nam-Kyun Baik*

*Assistant professor, Department of Information Security, Busan University of Foreign Studies, Busan, 46234 Korea

요 약

본 연구에서는 DRDoS 공격에 대한 효과적인 네트워크 기반 대응책을 수립하는데 필요한 기초 자료를 제공하고자, DRDoS의 네트워크 기반 특징을 식별하고 이에 대한 확률 및 통계 기법을 적용한 새로운 'DRDoS 공격 다단계 탐지기법'을 제안하고자 한다.

제안된 기법은 DRDoS의 특징인 반사 서버의 증폭에 의한 네트워크 대역폭에서 무제한 경쟁으로 정상적인 트래픽이 무분별하게 차단될 수 있는 한계를 제거하고자 'Server to Server' 및 이에 대한 'Outbound 세션 증적' 여부를 비교하여 정확한 DRDoS 식별 및 탐지가 가능하고 이에 대한 트래픽에 대해서만 통계 및 확률적 임계값을 적용하기에, 네트워크 기반 정보보호 제품은 이를 활용하여 완벽하게 DRDoS 공격 프레임을 제거가 가능하다.

시험을 통해 제안한 기법이 DRDoS 공격에 대한 식별 및 탐지 정확성을 높이고 희생자 서버의 서비스 가용성을 확보함을 확인하였다. 따라서 본 연구결과는 DRDoS 공격 식별 및 대응에 크게 기여할 수 있을 것으로 기대한다.

ABSTRACT

In this study, to provide the basis for establishing effective network based countermeasures against DRDoS(Distributed Reflection Denial of Service) attacks, we propose a new 'DRDoS attack multi-level detection method' that identifies the network based characteristics of DRDoS and applies probability and statistical techniques.

The proposed method removes the limit to which normal traffic can be indiscriminately blocked by unlimited competition in network bandwidth by amplification of reflectors, which is characteristic of DRDoS. This means that by comparing 'Server to Server' and 'Outbound Session Incremental' for it, accurate DRDoS identification and detection is possible and only statistical and probabilistic thresholds are applied to traffic. Thus, network-based information security systems can take advantage of this to completely eliminate DRDoS attack frames.

Therefore, it is expected that this study will contribute greatly to identifying and responding to DRDoS attacks.

키워드 : DRDoS, DDoS, 트래픽 증폭, well-known 포트, 임계값

Keywords : DRDoS, DDoS, Traffic amplification, well-known port, Threshold value

Received 10 September 2020, **Revised** 16 September 2020, **Accepted** 18 September 2020

***Corresponding Author** Nam-Kyun Baik(E-mail:namkyun@bufs.ac.kr, Tel:+82-51-509-6136)
Assistant professor, Department of Information Security, Busan University of Foreign Studies, Busan, 46234 Korea

Open Access http://doi.org/10.6109/jkiice.2020.24.12.1670 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

DRDoS(Distributed Reflective Denial of Service)은 별도의 에이전트 설치 없이 네트워크 통신규약의 취약성을 이용하여 정상적으로 서비스를 하고 있는 공개된 서버를 DRDoS 공격의 반사 서버로 사용한다. 따라서 DRDoS 공격은 공격자가 출발지 IP 주소를 희생자 시스템의 IP 주소로 위조해 정상적인 서비스를 제공하는 반사 서버에게 요청을 보내고, 그 응답은 재전송 또는 증폭되어 희생자 서버가 받게 되는 것이다. 요청되는 패킷(세그먼트 또는 데이터그램)은 SYN, NTP, DNS 쿼리 등으로 응답이 재전송 또는 증폭되는 모든 통신규약의 패킷들이 활용될 수 있다.

DRDoS 공격은 ① 불특정 다수를 대상으로 공개된 서버를 반사 서버로 활용, ② 반사 서버에 대한 권한을 얻기 위한 별도의 봇넷이 불필요, ③ 공격자 트래픽 대비 공격대역폭의 증폭, ④ 출발지 IP 위조로 근원지에 대한 추적 불가 등으로 정보보안과 침해영향력에 있어 가장 위협적인 존재이나, 아직도 DRDoS 공격에 대해 효과적인 탐지 방법의 적용에는 어려움이 있다.

이에 대한 식별 및 탐지를 위해 침입차단시스템, 침입탐지시스템, 침입방지시스템, DDoS 대응 장비 등 네트워크 기반 정보보호제품이 대응되고 있으나 탐지방식은 통계적 기법인 트래픽 임계치 값 모니터링 대응방식으로 한계를 가질 수 밖에 없다.

본 연구에서는 DRDoS 공격에 대한 효과적인 대응책을 수립하는데 필요한 기초 자료를 제공하고자, DRDoS의 네트워크 기반 특징을 식별하고 이에 대한 확률기법을 적용한 새로운 다단계 탐지기법을 제안하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 여러 DRDoS 기법들과 대응의 한계점에 대하여 설명한다. 3장에서 단일한 네트워크 기반 보안장비에서 DRDoS 공격을 좀 더 정확하게 탐지할 수 있는 'well-known port'로 구성된 'Server to Server' 통신연결 식별과 확률적 트래픽 부하량 비교의 다단계 탐지기법을 제안하며 4장에서는 시험을 통하여 상용되어 운영되는 대표적인 '통계적 임계치 방식'과 제안된 'DRDoS 공격 다단계 탐지기법'에 대한 공격 패킷 탐지 비교・분석을 수행하고 5장에서 결론을 정리한다.

Ⅱ. DRDoS 공격 기법들

DRDoS 공격 기법들은 네트워크 트래픽이 증폭만 되어 진다면 해당되는 모든 프로토콜이 악용되어 질 수 있으며 공격 메커니즘은 아래의 그림 1과 같이 동일한 개념이다[1][2].

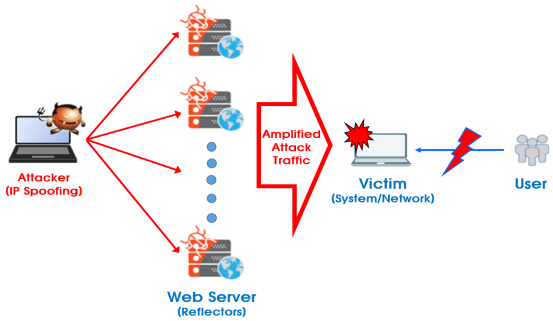

Fig. 1 DRDoS Attack Mechanism

• SYN+ACK 반사 공격

공격자는 희생자 서버의 IP로 위조한 후 반사 서버(인터넷상에 있는 공개된 모든 서버)들에게 TCP 연결을 위한 SYN 패킷(TCP 80 port)을 보내면 반사 서버는 희생자 서버에게 응답으로 SYN/ACK 패킷을 전송한다. 하지만 TCP 연결 요청을 하지 않은 희생자 서버는 TCP 3way Handshake의 마지막 단계인 ACK 패킷을 전송하지 않으며 이에 반사 서버는 패킷이 목적지에 정상적으로 전달되지 못한 것으로 판단하여 TCP 프로토콜에 의해 SYN/ACK 패킷을 재전송한다[3][4]. 운영체제 마다 다를 수 있지만 반사 서버는 수배 이상으로 재전송을 수행하며 이를 통해 요청 패킷의 수배 이상으로 트래픽이 증폭되는 것이다.

• NTP 반사 공격

공격자는 희생자 서버의 IP로 위조한 후 반사 서버(인터넷상에 있는 공개된 NTP서버)들에게 NTP monlist (UDP 123 port) 요청을 하면, NTP 서버는 최근 접속한 시스템 목록을 요청에 대한 응답하기 위해 대량(최근 접속한 최대 600개의 접속 호스트 리스트)의 네트워크 트래픽을 유발시킨다. NTP 서버의 응답이 증폭기술에 의해 공격자가 보낸 요청보다 훨씬 큰 트래픽을 발생하여 희생자 서버 네트워크 대역폭을 모두 소진하여 정상적인 사용자에 대한 서비스 장애가 발생한다[5][6].

• DNS 반사 공격

공격자는 희생자 서버의 IP로 위조한 후 반사 서버(인터넷상에 있는 공개된 공용 DNS 서버)들에게 DNS 조회(UDP 53 port) 요청(지정 옵션 'ANY' 사용)을 하면, 공용 DNS 서버는 IP 주소에 해당되는 모든 DNS 정보를 반환한다. DNS 서버의 반환 정보가 증폭기술로 활용되어 공격자가 보낸 요청보다 훨씬 큰 트래픽을 발생하여 희생자 서버 네트워크 대역폭을 모두 소진하여 정상적인 사용자에 대한 서비스 장애가 발생한다[7].

DRDoS 공격은 침해되지 않은 정상적인 서버가 반사서버가 되어 정상적인 통신규약에 의해 네트워크 트래픽을 증폭시키는 것으로 보안관리자는 정상적인 트래픽과 공격 트래픽을 구별하여 내기가 쉽지 않다. 또한 IP 주소가 위장으로 공격 또는 명령 근원지를 파악하기 어려우며, 공격 트래픽이 수많은 반사 서버를 경유하므로 모든 경로를 확인할 수도 없다[8]. 따라서 기존의 정보보호 제품 또는 정보보안 대응체계(Anti-Spoofing Detection, Protocol Patch 등)에서는 DRDoS 공격에 대한 탐지 또는 공격대상에 대한 대응이 가능하지 않다. 하지만, 네트워크 기반의 몇 가지 특징을 추려낼 수 있다면 그리고 그 특징을 정확도를 높일 수 있다면 DRDoS 세션에 대한 식별 및 탐지가 가능할 것이다.

Ⅲ. 제안하는 DRDoS 공격 탐지 기법

3.1. DRDoS 세션 식별 및 탐지

DRDoS 공격은 네트워크 및 통신규약 기반 공격이므로 이와 관련된 특징을 찾아내야 한다. 모든 과정이 정상적인 네트워크 통신 과정이나 단 두가지 점이 의심될 수 있다.

1. 근원지 주소 IP 가 위장이 되어 있다.
2. 'Server to Client' 통신 연결이 아니라 'Server to Server' 통신 연결이다.

첫 번째 IP 주소 위장은 인터넷 관문인 ISP(Internet Service Provider)에서만 판단이 가능하기에 본 논문에서 고려하는 희생자 네트워크 또는 서버에서 대응 방식이 될 수 없다.

두 번째 'Server to Server' 통신 연결은 희생자 네트워크 또는 서버에서 4계층 트래픽 내역을 통하여 확인할 수 있다. 즉 DRDoS 공격은 중간매개체가 반사서버로 악용되는 것으로 네트워크 세션은 서버-서버간 연결이 될 수 밖에 없다. 따라서 희생자 네트워크 또는 시스템에서는 이점을 이용하여 포트번호가 1024보다 작은 'well-known port'로 서로 송수신 서버간 연결된 트래픽 세션을 DRDoS 세션으로 우선 특정할 수 있다.

다음으로 해당 세션에 희생자 네트워크 또는 서버로부터의 중간매개체에 대한 아웃바운드(유출) 트래픽이 발생 여부 또는 일정 기간 내의 세션 관리 증적이 없을 경우 최종 DRDoS 세션으로 특정할 수 있다. 그리고 추가적으로 IP로 Domain Name을 확인(nslookup 등)한다면 공개 서버를 이용한 DRDoS 임을 검증 할 수 있다.

이를 통하여 DRDoS 세션 식별 및 탐지에 대한 정확성을 줄 수 있어 보안장비의 오탐율(false-positive) 및 미탐율(false-negative)을 감소시켜 희생자 네트워크 또는 서버에 구축된 정보보호 제품의 안전・신뢰성을 향상시킨다.

3.2. DRDoS 세션 트래픽 부하량 비교 및 제한

DRDoS 공격은 희생자 서버의 서비스 가용성을 침해하고자 하는 것이 목적이므로, 동원된 수많은 중간매개체 서버들이 희생자 서버의 대역폭, 서비스 쓰레드 또는 허용 접속 수 보다 매우 많은 연결 및 전송을 시도할 것이다. 따라서 특정 세션(DNS DRDoS가 Web 사이트에 공격한 경우 : 송신자 포트 = 53, 목적지 포트 =80)에 대한 트래픽에 대해 기존 트래픽 사용량에 비해 매우 큰 배수 이상으로 증가 시, 이 또한 비정상 상태 즉, 서비스 거부공격으로 인식할 수 있다. 따라서 서버 과부하 시에 신속하게 과부하 상태를 식별 및 극복하는 동적 메커니즘을 구현하는데 있어 과부하가 예상되는 적절한 시점을 식별할 수 있는 부하 모니터링은 필수적인 요소이다. 부하 모니터링은 주기적으로 실행되면서 세션(Source IP, Destination IP, Source Port, Destination Port, Service Name) 및 트래픽 부하에 대한 통계(평균 및 표준편차 값) 등을 유지한다. 따라서 상당한 그리고 일정 기간 동안 측정된 DRDoS 세션 트래픽 부하량의 수치를 활용하여 다양한 방법으로 비율제한(rate-limiting)에 대한 임계값 지정 방식을 지정할 수 있다.

첫 번째 방식은 정적 설정값으로 지정하는 것이다. 정보보안 관리자는 경험적인 선에서 보호대상 서버 및 네트워크의 용량과 속도를 고려하여 단순히 일정 부하값

이상에 대해 임계값으로 정하는 것이다. 설정의 편리성은 있으나 향후 시스템, 네트워크 및 서비스 환경 변화에 동적이지 않아 대응에 어려움이 있을 수 있다.

두 번째 방식은 동적 설정값으로 지정하는 것이다. 여러 연구를 통해 네트워크 기반 DoS 지속 시간의 누적 분포가 10분 이내 60%, 30분 이내 80% 임을 고려하면 DRDoS의 평균 공격 시간은 수분에서 십수분 정도이다[9]. 따라서 이 시간 동안의 DRDoS 세션 트래픽 변화량에 따라 여러 가지 통계적 방식들이 적용 될 수 있다. 예를 들어 DRDoS 세션에 대한 트래픽 분포가 정규분포를 따른다고 단순히 가정하면, 평균(a)과의 표준편차(σ) 거리에 의해 정상적인 또는 비정상적인 트래픽 확률 값 범위를 설정할 수 있다. 정규분포 표에 의해 정상이 아닌 3%인(평균에서 '+'로 멀리 떨어진) 경우에 대해서 비정상 설정값으로 의도하고자 한다면 이에 해당되는 과부하 시점 임계값(x')으로 '$a + 1.83\sigma$'을 설정(이하인 값들은 정상일 경우는 97%로 분표)하면 된다. 희생자 네트워크 또는 서버를 보호하는 정보보호 제품은 임계값을 초과하는 DRDoS 세션은 비정상으로 구분하여 ACL (Access Control List)에 등록하고 인바운드 되지 못하게 한다. 이외 확률 및 통계에서 사용되는 여러 가지 방식(이항 분포, 포아송 분포 등)으로 확대 적용이 가능하며 향후 시스템, 네트워크 및 서비스 환경 변화에 동적으로 적응 가능하나 세션 관리에 대한 부담이 있을 수 있다.

이를 통하여 DRDoS 공격에 대해 보다 효과적이고 객관적인 대응 체계를 구축할 수 있어 서비스의 피해 최소화에 따른 가용성을 향상시킬 수 있다.

3.3. DRDoS 공격 다단계 탐지기법 알고리즘

DRDoS 공격 다단계 탐지기법은 네트워크 기반 보안장비에 아래의 그림 2와 같은 순서의 알고리즘으로 구현된다. 먼저 입력된 트래픽 중에서 'well-known port'로 이루어진 'Server to Server' 통신 연결을 구분하여 식별하고 해당 연결에서 중간매개체로의 아웃바운드 트래픽이 발생 여부 또는 일정 기간 내의 세션 관리 증적 여부를 확인하여 DRDoS 세션으로 식별한다. 그리고 선택적으로 IP로 Domain Name을 확인하여 공개 서버가 reflector로 이용되었음을 검증한다. 이후 세션관리를 통하여 DRDoS 세션 트래픽 부하량의 수치가 비율제한(rate-limiting) 임계값과 비교하여 초과되는 경우 트래픽을 차단하여 희생자 네트워크 또는 서버를 보호한다.

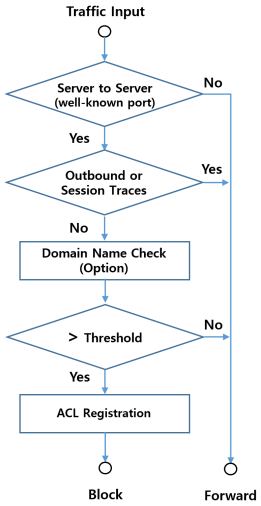

Fig. 2 DRDoS detection algorithm

Ⅳ. 시 험

본장에서는 실제 DRDoS 공격 재현을 통하여 공격의 영향 정도를 알아보고자, 인터넷상에서 가장 많이 사용되고 있는 웹서버를 희생자 시스템으로 설정하여 시험을 수행하고자 한다.

4.1. DRDoS 공격 영향 분석을 위한 성능 평가 지표

DRDoS 공격 다단계 탐지기법이 지금의 모든 네트워크 기반 보안장비에서 활용되고 있는 통계적 기법인 'TCP/IP 계층 패킷(세그먼트 또는 데이터그램) 임계치' 기법보다 성능면에서 우수함에 대한 근거를 제시하고자, 웹서비스 통신규약의 특성이 반영된 웹 서버 중심의 객관적이고 정량화된 가용성 평가 지표를 적용하고자 한다. 웹서버에 대한 서비스는 다수의 세션으로 이루어지므로 하나의 세션이라도 누락되거나 혹은 누락된 세션에 대한 재전송 요구로 부하가 발생할 경우 웹 사용자가 느끼는 서비스의 품질 만족도는 크게 떨어진다. 따라서 원하는 시간에 정상적으로 웹 서버에 접속되어 원하는 모든 문서들을 열람할 수 있는지 여부가 웹 사용자가 실제 느끼는 가용성이라 할 수 있으며 이에 대한 평가 지표는 다음과 같이 나타낼 수 있다[10].

$$\cdot \textit{서비스 접속률(\%)} = \frac{\textit{응답 받은 서비스 수}}{\textit{총 서비스요청 수}} \times 100 \quad (1)$$

$$\cdot \text{콘텐츠 완성률(\%)} = \frac{\text{완성된 컨텐츠 수}}{\text{허용된 서비스에 의해 요구되는 총 컨텐츠 수}} \times 100 \quad (2)$$

※ 서비스: 웹 사용자가 서버에 요청하는 웹페이지(콘텐츠)
※ 콘텐츠: SIP, DIP, Sport, Dport 기반의 TCP/IP 접속으로 정적 또는 동적인 하나의 콘텐츠

4.2. 시험망 구성

DRDoS 공격 트래픽은 공개된 취약점을 참고하여 SYN+ACK, NTP 및 DNS 반사 공격을 혼합하여 수행하고자 하며 이에 대한 각각의 속성 프로파일(반사 서버 수, 초당 요청수 등)을 다음의 표 1과 같이 정의하여 구현한다. 또한 정상 사용자 트래픽도 표 2와 같이 정의하여 트래픽을 실제 발생하고 웹서버에 대한 서비스 제공 한계를 표 3과 같다고 설정한다.

Table. 1 DRDoS Attack Traffic

	Amplification Traffic Properties
SYN+ACK	1,000(Reflector) × 10(Requests Per Sec) × 54bytes(Frame Size) × 10(# of retransmission)
NTP	100(Reflector) × 10(Requests Per Sec) × 46bytes(Frame Size) × 600개(Max IP Reply)
DNS	100(Reflector) × 1(Requests Per Sec) × 4Kbytes(Mean Return Info) × 256(# of any host)

Table. 2 Normal User Traffic

User Number (IP Number)	HTTP Connections per User	TCP connections by HTTP connection	Access data web server request by tcp
10	3/sec	10/sec	Fixed 360bytes

Table. 3 Maximum web-serviceable measurements and content

TCP/IP Connections	HTTP Connections	Average size of web server response data by TCP connection
10,000/s	3,000/s	Fixed 5,840bytes

웹서버에 대한 서비스 가용성 정도를 시험하고자 시험 환경 구성은 그림 3과 같이 구성한다. 정상사용자 및 DRDoS 공격자는 패킷생성 도구(BP, IXIA, Avalanche)를 사용하며 네트워크 기반 보안 장비는 통계적 기법의 임계치(출발지/목적지 IP 및 port에 대한 세션 관리로 TCP flooding 설정 : SYN+ACK, NTP, DNS 패킷에 대한 10,000개) 및 DRDoS 공격 다단계 탐지기법을 선택적으로 적용 가능한 세션 유지형 네트워크 기반 보안 장비(시뮬레이터) 이다. 또한 시험망의 네트워크 대역폭은 내외부 모두 100MB로 구성하였다.

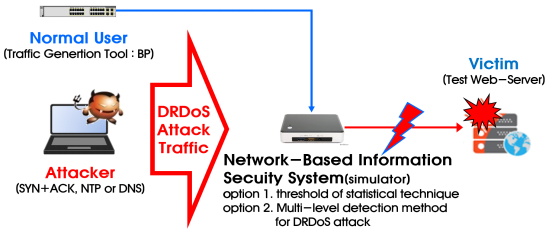

Fig. 3 testing environment

4.3. DRDoS 웹서버 서비스 가용성 측정

위에서 서술된 시험환경과 설정값에 대해서 정상 사용자에 대한 '통계적 기법의 임계치' 기법과 'DRDoS 공격 다단계 탐지기법'에 대해 시간 흐름에 따른 서비스 접속률과 콘텐츠 완성률은 아래의 그림 4와 그림 5와 같다.

'통계적 기법의 임계치' 기법은 시작 시에는 기존 세션 유지로 인하여 정상 사용자의 서비스 접속이 가능하고 요구하는 콘텐츠를 서비스할 수 있다. 하지만 많은 반사 서버를 활용하는 DRDoS 공격에는 세션 관리로 인하여 DRDoS 트래픽 식별이 불가능하다. 따라서 내부망에 대한 트래픽 부하량이 회선의 대역폭을 넘어가는 시점부터는 DRDoS 공격 트래픽과 경쟁을 해야 하기 때문에 상대적인 비율이 크게 낮은 정상 사용자의 요청은 웹서버에 도착할 수 없어 서비스 접속률은 크게 낮아질 수밖 에 없다. 즉, 따라서 해당 웹서버 요청을 위한 서비스 접속률이 크게 떨어지면 웹서버 응답 데이터 및 추가적인 데이터 요청이 있을 수 없어 콘텐츠 완성률도 급격히 감소할 수밖에 없다.

하지만 'DRDoS 공격 다단계 탐지기법'은 'Server to Server' 및 이에 대한 'Outbound 세션 증적' 여부를 비교하여 정확한 DRDoS 식별이 가능하고 이에 대한 트래픽에 대해서만 임계값을 적용하기에 네트워크 기반 보안 장비는 완벽하게 DRDoS 공격 프레임을 제거가 가능하다. 따라서 초기 DRDoS를 식별하지 못하는 시점까지는 증폭된 공격 트래픽과의 경쟁으로 인하여 조금은 가용성이 보장되지는 않지만 이후 DRDoS 트래픽을 식별한 뒤로는 정상 사용자의 트래픽이 과부하된 DRDoS 공격 트

래픽과 경쟁하지 않고 모든 요청이 웹서버까지 도달되고 그 후, 세션관리로 유지되기에 웹 서비스가 정상적으로 제공되며 이에 대한 콘텐츠 완성률로 보장될 수 있다.

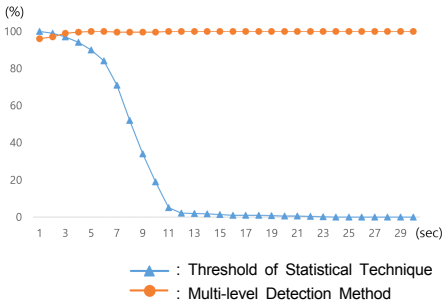

Fig. 4 service access rate

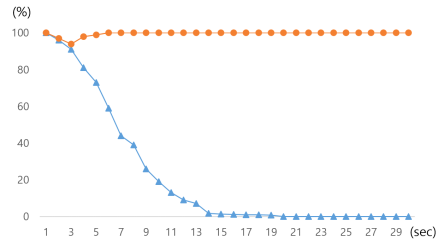

Fig. 5 Content, completion rates

Ⅴ. 결 론

본 연구에서는 DRDoS 공격에 대한 식별 및 탐지 정확성을 높이고 희생자 네트워크 또는 서버의 서비스의 가용성을 확보할 있는 'DRDoS 공격 다단계 탐지기법'을 제안하였다. 제안된 기법은 DRDoS의 특징인 반사 서버의 증폭에 의한 네트워크 대역폭에서 무제한 경쟁으로 정상적인 트래픽이 무분별하게 차단될 수 있는 한계를 제거하고자 'Server to Server' 및 이에 대한 'Outbound 세션 증적' 여부를 비교하여 정확한 DRDoS 식별 및 탐지가 가능하고 이에 대한 트래픽에 대해서만 통계 및 확률적 임계값을 적용하기에, 네트워크 기반 정보보호 제품은 이를 활용하여 완벽하게 DRDoS 공격 프레임을 제거가 가능하다.

제안된 기법이 '통계적 기법의 임계치' 보다 가용성 확보 측면에서 우수함을 검증하기 위해 웹 서비스 특성 기반 성능 평가 지표인 '서비스 접속률'과 '컨텐츠 완성률'을 사용하였다. 시험결과 반사 서버에 의해 증폭된 DRDoS 트래픽은 제안된 기법에 의해 희생자 네트워크 경계선에서 차단되어 희생자 서버의 서비스 상에는 영향을 주지 않음을 확인하였다.

ACKNOWLEDGEMENT

This work was supported by the research grant of the Busan University of Foreign Studies in 2020.

References

[1] DDoS Attack Response Guide for Small and Medium Businesses: [Internet]. Available: https://www.boho.or.kr/data/guideView.do? bulletin_writing_sequence =35135, 2019.

[2] Kaspersky DDOS attacks in Q1 2017: [Internet]. Available: https://securelist.com/ddos-attacks-in-q1-2017/78285/, 2017.

[3] TCP: [Internet]. Available: https://www.rfc-editor.org, 1981.

[4] 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.

[5] H. Huang, L. Hu, J. Chu, and X. Cheng, "An Authentication Scheme to Defend Against UDP DrDoS Attacks in 5G Networks," *Institute of Electrical and Electronics Engineers*, vol. 7, 2019

[6] NTP Amplification DDoS Attack: [Internet]. Available: http://cve.mitre.org, 2013.

[7] CVE-2006-0987 Learn more at National Vulnerability Database (NVD): [Internet]. Available: https://cve.mitre.org, 2006.

[8] R.g Xu, J. Cheng, F. Wang, X. Tang, and J. Xu, "A DRDoS Detection and Defense Method Based on Deep Forest in the Big Data Environment," *Symmetry*, vol. 11, no. 1, Nov. 2019.

[9] Web Server Traffic in Crisis Conditions: [Internet]. Available: https://lup.lub.lu.se/search/ws/files/6029596/625288.pdf, 2005.

[10] N. Baik and N. Kang, "Multi-Phase Detection of Spoofed SYN Flooding attacks," *International journal of Grid and Distributed Computing*, vol. 11, no. 3, Mar. 2018.

백남균(Nam-Kyun Baik)

'98.2. 숭실대학교 전자공학과 공학사
'01.2. 숭실대학교 전자공학과 공학석사
'11.2. 숭실대학교 전자공학과 공학박사
'00~'17.한국인터넷진흥원 수석연구원
'19.3.~현재. 부산외국어대학교 정보보호학과
※ 관심분야 : 스마트융합보안, 정보보안컨설팅