http://dx.doi.org/10.7236/JIWIT.2012.12.2.1
JIWIT 2012-2-1

DDoS 공격 가능성 완화를 위한 효율적인 버퍼 관리 기술

Efficient Buffer Management Scheme for Mitigating Possibility of DDoS Attack

노희경, 강남희*

Heekyeong Noh, Namhi Kang

요 약 DDoS 공격은 분산된 다수의 좀비 시스템들을 이용하여 타겟 시스템이나 네트워크 자원을 고갈시켜 정상적인 서비스를 방해하는 공격이다. 2000년 초 등장된 DDoS 공격은 시간이 갈수록 더욱 진화된 형태로 다양하게 시도되고 있다. 본 논문은 이러한 공격들 중 많은 부분을 차지하고 있는 네트워크 프로토콜의 제어 패킷을 이용한 DDoS 공격들을 탐지하고 공격 가능성을 줄일 수 있는 방법을 제안한다. 제안하는 시스템은 네트워크 혼잡 제어를 위해 일반적으로 사용되는 버퍼 관리 기술을 응용하여 공격의 상태를 파악하고 대처할 수 있는 방안을 제공한다. 제안하는 시스템은 정확한 DDoS 공격 탐지를 제공하지는 않는다. 하지만 내부 시스템의 과부하 가능성을 최소화하고 공격이 확신 시 될 경우 순간 증가하는 제어 패킷을 폐기하여 DDoS 공격을 완화시킬 수 있다. 또한 순간적 트래픽 양의 증가를 공격 탐지로 오인하는 기존 시스템과 달리 유동적으로 적응할 수 있는 장점도 제공한다.

Abstract DDoS attack is a malicious attempt to exhaust resources of target system and network capacities using lots of distributed zombi systems. DDoS attack introduced in early 2000 has being evolved over time and presented in a various form of attacks. This paper proposes a scheme to detect DDoS attacks and to reduce possibility of such attacks that are especially based on vulnerabilities presented by using control packets of existing network protocols. To cope with DDoS attacks, the proposed scheme utilizes a buffer management techniques commonly used for congestion control in Internet. Our scheme is not intended to detect DDoS attacks perfectly but to minimize possibility of overloading of internal system and to mitigate possibility of attacks by discarding control packets at the time of detecting DDoS attacks. In addition, the detection module of our scheme can adapt dynamically to instantly increasing traffic unlike previously proposed schemes.

Key Words : DDoS attack, Attack detection, Attack mitigation, buffer management

Ⅰ. 서 론

서비스 거부 (Denial of Service : DoS) 공격이란 악의적인 의도로 대상 시스템의 자원을 고갈시키고 성능을 저하시켜서 정상적인 서비스를 제공하지 못하게 하는 것이다. 이 중 분산된 다수 시스템들의 자원을 이용하여 대상 시스템을 공격하는 형태가 분산 서비스 거부 (Distributed Denial of Service : DDoS) 공격이다[1].

*정회원, 덕성여자대학교 디지털미디어학과(교신저자)
접수일자 2012.3.15, 수정완료 2012.4.5
게재확정일자 2012.4.13.

Received: 15 March, 2012, Revised: 5 April, 2012
Accepted: 13 April, 2012
*Corresponding Author: kang@duksung.ac.kr
Dept. of Digital Media, Duksung Women's University, Korea

2000년대 초, C&C서버를 이용하여 좀비 시스템을 관리하고 공격하는 초기 DDoS 공격은 점차 다양한 형태로 발전되고 있다. 7.7 공격과 3.4 공격의 경우, P2P 사이트를 통한 악성코드 배포로 좀비 PC를 확보했고, 공격 에이전트와 C&C의 접속에 의존하지 않고 자동화된 방식으로 공격을 제어하는 기술로 발전했다. 당시 공격은 TCP, UDP, ICMP 등의 표준화 프로토콜이 갖는 취약점을 주로 이용했다. 또한 공격 후 좀비 PC의 하드디스크를 파괴하여 목표 시스템뿐만이 아니라 좀비 시스템까지 피해 범위를 확대했다[2].

다양한 형태의 DDoS 공격들 중, 본 논문에서는 작은 크기의 제어패킷을 악용하여 수행되는 DDoS 공격들을 주요 연구대상으로 고려한다. 여기에 해당하는 DDoS 공격은 다음처럼 구분된다[3].

- 트래픽 과부하를 유발하는 플러딩(Flooding) 공격
- 과도한 세션을 요구해 연결 가능 범위를 초과하게 하는 커넥션(Connection) 공격
- 응용 계층 프로토콜의 특성을 이용한 공격

제어패킷을 이용한 DDoS 공격에서 Flooding 공격은 큰 비중을 차지한다. TCP Flooding 공격, ICMP echo request/reply 공격, UDP Flooding 공격 등이 이에 포함된다. 커넥션 공격은 서버에 과도한 HTTP 처리 커넥션 요청을 하여 커넥션 용량을 초과시켜서 정상적인 서비스 제공을 방해하는 형태이다. 애플리케이션 기반 공격은 프로토콜의 취약점을 이용한 형태의 공격이며 웹서버에게 재전송 요청을 과도하게 전송하여 과부하 시키는 refresh 공격, VoIP에서 SIP(Session Initiation Protocol) 메시지를 이용한 REGISTER storm 공격, INVITE 공격, BYE 공격 등이 있다.

DDoS 공격에 대응하기 위해 다양한 공격 탐지 및 방어 기법들이 제안되었다. 이 중 역추적 기법은 라우터가 역추적 경로 정보를 사전에 패킷에 삽입하거나 목적지로 전달하여 공격 발생 시 공격 근원지를 판별하는 방식이다. 이와 달리 라우터에서 공격을 탐지하고 방어하는 기술로 Pushback 기법과 Rate-limit 기법이 있다. 이렇게 다양한 탐지 및 방어 기법이 개발되고 있지만 DDoS 공격을 완벽히 방어할 수는 없다. 특히, 대부분의 DDoS 공격이 네트워크 프로토콜의 취약점을 이용한 것이기 때문에 표준화된 프로토콜을 전면 수정하지 않는 이상 완전히 제거할 수 없다. 따라서 공격에 효과적으로 대처할 수 있는 방안이 필요하다.

본 논문에서는 제어 패킷을 이용한 DDoS 공격의 유형과 방어 시스템에 대해 분석하고 DDoS 공격을 효율적으로 제어 및 탐지할 수 있는 시스템을 제안한다.

제안하는 공격 탐지 시스템은 인터넷에서 많이 사용하는 버퍼관리 기술인 RED(Random Early Detection)[4]와 유사하게 2개의 임계값을 이용하여 DDoS 공격을 효율적으로 판단하고, 공격 의심 시 제어패킷을 확률적으로 폐기하여 공격 가능성을 줄이게 된다.

본 논문의 구성은 다음과 같다. 2장에서는 DDoS 공격 형태와 기존에 연구되었던 공격 제한 기법들에 대해 분석한다. 3장에서는 DDoS 공격을 효율적으로 탐지하기 위한 시스템을 제안한다. 4장에서는 시스템 구현을 통해 얻은 결과를 분석하고, 5장에서 결론을 정리한다.

II. 관련연구

1. DDoS 공격 유형

본 절에서는 표준 프로토콜에서 정의하고 있는 제어 패킷의 동작 특성을 악용하는 DDoS 공격을 기술한다.

TCP SYN Flooding 공격은 연결지향적인 TCP의 3-way handshaking을 이용한 공격 방법이다. 공격자가 송신 주소를 위조한 SYN 패킷을 전송한 뒤 서버가 보낸 ACK에 SYN/ACK로 응답하지 않음으로써 서버의 대기 큐를 과부하 시키는 형태다. 이와 유사한 LAND 공격은 패킷의 출발 IP 주소와 목적 IP 주소를 공격 목표 시스템의 IP 주소로 설정하여 공격 목표 시스템으로 패킷을 전송하는 형태이다. 결국 공격 목표 시스템이 자신의 IP 주소로 패킷을 보내게 되므로 네트워크에 SYN 패킷이 넘치게 하는 공격이다.

ICMP echo request/reply 공격은 제어 프로토콜인 ICMP를 이용한 공격이다. 공격자가 목적 IP를 공격 대상 서버로 설정한 후, ICMP echo request 패킷을 broadcast 하면 하위 시스템에서 ICMP echo reply 패킷을 공격 대상 서버로 전송하게 되어 서버의 자원을 고갈시키는 방식이다.

SIP Flooding 공격은 VoIP 기반 시스템에서 SIP (Session Initiation Protocol) 메시지를 대량으로 전송하여 VoIP 사용자나 사업자의 정상적인 서비스를 방해한다[5]. 콜을 생성하기 위해 사용하는 SIP INVITE 메시지를 과도하게 전송하는 공격이 대표적이다. INVITE 메시

지를 보내서 서버가 응답 처리하는데 많은 시간을 소비하게 하여 정상적인 서비스를 지연시키고 서버 자원을 고갈시키려는 목적을 갖는다. 또 다른 Flooding 공격으로 REGISTER 메시지를 사용한 형태가 있다. SIP 사용자들은 REGISTER 메시지를 사용하여 등록 서버에 자신의 위치 정보를 제공하는데 REGISTER 요청이 많아지면 서버가 처리할 메시지가 증가하므로 서버 과부하가 발생하여 다른 사용자가 정상 서비스를 받기 어렵게 만드는 공격 방법이다.

제어 패킷을 이용한 다른 형태로 DNS 서버가 재귀하는 특성을 이용한 DNS Amplification 공격이 있다. 공격자가 임의의 도메인과 특정 타입의 자원 기록을 DNS 서버에 등록하고 봇넷에게 공격을 명령하면 봇넷은 공격자가 정해놓은 자원 타입을 요청하는 위조된 DNS 요청 쿼리를 대량으로 전송한다. 쿼리를 받은 서버들이 DNS 요청 쿼리에 대한 응답을 공격 목적 시스템에게 전송함으로써 공격 대상 시스템에 피해를 입히는 공격 방법이다.

2. DDoS 공격 제어 기법

상기 기술한 제어 패킷을 이용한 공격들의 방어 기술로는 Rate limit 기법과 Pushback 기법이 대표적이다.

Rate limit 기법은 시스템의 특정 플로우의 트래픽 양을 측정하여 지정된 허용 대역폭 이하의 패킷은 정상 서비스를 제공하고 그 이상의 패킷들은 제한하는 기술이다[6]. Rate limit은 TCP 프로토콜을 이용한 공격인 SYN Flooding, LAND 공격 발생 시에 패킷을 지연, 폐기 또는 혼잡을 제어하고, ICMP나 UDP 프로토콜을 이용한 UDP Flooding, Smurf 공격, ICMP Flooding 공격에서는 패킷을 지연시키거나 폐기 시킨다. 그러나 최대 허용 대역폭의 값이 상태에 따라 유동적으로 변하지 않고 고정적이기 때문에 환경 변화에 대해 유연한 대응을 하기 어렵다는 단점이 있다.

Pushback 기법은 라우터가 혼잡 상태가 되면 rate limiter와 pushbackd를 사용하여 공격 트래픽을 구분하여 공격 트래픽을 우선 폐기하는 공격 제어 기법이며 구조는 그림 1과 같다.

그림 1의 rate limiter 모듈에서 폐기된 패킷들을 pushbackd 모듈에서 패킷 정보를 파악하여 정상 트래픽과 공격 트래픽을 구분하고 폐기되는 패킷량으로 공격상태 유무를 판단한다.

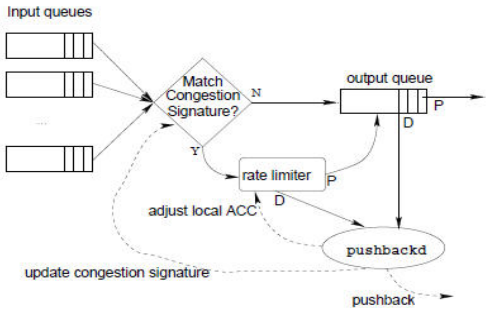

그림 1. Pushback 라우터 일부분
Fig. 1. Part of Pushback Router

Pushback을 사용하면 공격 트래픽을 미리 폐기함으로써 하위 대역폭의 낭비를 방지할 수 있고 공격 상태에서 상위 라우터에서 공격 트래픽의 유입이 감지되면 공격 트래픽을 폐기해 다른 트래픽에 정상 처리를 제공할 수 있다[7]. 그러나 Pushback 매커니즘이 라우터 내부에 구현되는 것이 아니라 외부에 추가적인 보조 장비를 설치해야한다는 단점이 있다.

Ⅲ. 제안 시스템

1. 시스템 모델

본 논문에서 제안하는 기술은 그림 2처럼 네트워크의 입력 라우터에 구현된다.

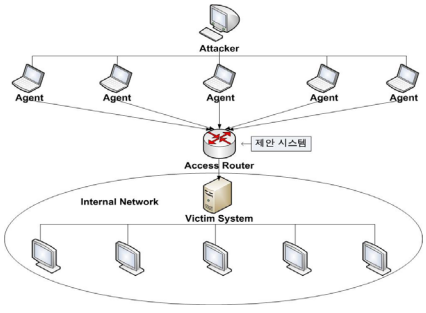

그림 2. 제안 시스템 구조
Fig. 2. Structure of Proposed System

라우터의 입력 버퍼 모습은 그림 3과 같다. 라우터에 입력되는 패킷 중 제어 패킷만을 구분하여 가상 버퍼에 입력 시키고 공격을 판단한다. 따라서 SYN Flooding, LAND 공격, ICMP Flooding, SIP Flooding 등과 같이

제어 패킷을 이용하는 공격에 대응한다.

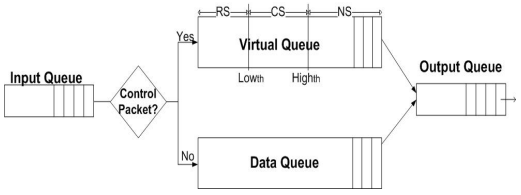

그림 3. 라우터 내부 구조
Fig. 3. Internal Structure of Router

공격 여부를 판단하기 위해 가상 큐는 NS(Normal Section), CS(Cautionary Section), RS(Risky Section)의 3가지 상태로 구분된다. NS는 정상 상태 구간, CS는 서버 버퍼가 과부하 될 가능성이 존재하는 경고 구간 그리고 RS는 서버 버퍼의 과부하가 확실시 되는 위험 구간으로 정의한다. 즉, RS 구간은 입력되는 제어 패킷의 양이 많아진 상태로 DDoS 공격으로 판단한다. RS 구간에 속한 제어 패킷이 정상적인 요청이라 해도 내부 시스템이 처리하기 어려우므로 폐기시켜 서비스 처리 과부하를 최소화하는 것이 주목적이다.

표 1은 본 제안 시스템에서 사용되는 기호를 정의한다.

표 1. 기호 정의
Table 1. Notations and Definitions

기호	정의
C_t	단위 시간동안 버퍼링되는 패킷량
λ_t	입력 패킷량
μ_t	출력 패킷량
Th_{Low}	NS와 CS 구간 임계값 (byte/sec)
Th_{High}	CS와 RS 구간 임계값 (byte/sec)
C_{Avg}	단위 시간 T동안 C_t의 평균값 (byte/sec)
C_{Max}	단위 시간 T동안 C_t의 최대값 (byte/sec)
P_{CS}	CS구간 내 패킷 폐기 확률 (P_{CS}<1)
P_{RS}	RS구간 내 패킷 폐기 확률 (P_{CS}<P_{RS}<1)
$Timer_{CS}$	CS 상태 타이머
$Timer_{RS}$	RS 상태 타이머

가상 큐에 단위 시간동안 버퍼링되는 패킷량은 $C_t = \lambda_t - \mu_t$ 으로 표현된다. 초기의 Th_{Low}는 평상시의 학습 상태를 기반으로 하여 C_{Avg}로 설정된다. 초기 Th_{High}도 평상시의 학습 상태를 기반으로 하며 C_{Max}로 설정된다.

본 논문에서는 학습상태에서 C_t의 평균값 C_{Avg}를 $C_{Avg} = (\sum_{t=0}^{T} C_t)/T$ 로 정의하고 C_{Max}는 학습기간 동안 측정된 C_t의 값 중 최대값으로 정의한다. 초기 단계 이후의 Th_{Low}와 Th_{High}는 상황에 따라 지수가중평균값으로 갱신한다.

NS 구간의 패킷들은 서버 버퍼가 처리 가능한 용량이므로 모든 패킷을 내부로 전달한다. CS는 서버의 과부하 가능성이 있으므로 버퍼 과부하를 방지하기 위해서 해당 구간 내의 패킷들에 대해 P_{CS}의 확률로 폐기한다. RS는 서버 과부하를 유발시키는 대량의 패킷이 유입된 상태이므로 P_{CS}보다 큰 P_{RS}의 확률로 패킷들을 폐기한다. 폐기율 P_{CS}, P_{RS}는 구현 환경과 시스템에 따라서 달라질 수 있으며 관리자가 적절한 값을 설정할 수 있다.

2. 제어패킷 처리 기술

2장에 기술한 것처럼 DDoS 공격에 제어 패킷이 많이 악용된다. 따라서 본 제안 시스템에서는 라우터로 유입되는 패킷 중 제어 패킷만 구분하고 유입되는 패킷량을 측정하여 패킷을 사전에 부분적으로 폐기함으로써 공격을 제어한다. 공격 탐지 시스템에서 임계값을 일정한 값으로 설정하면 이벤트 시즌 등의 급격히 변하는 상황에 유동적으로 대응을 하기가 어렵다. 반면 동적인 임계값을 설정하면 패킷량의 변동에 따라서 임계값을 갱신하므로 정적 임계값을 갖는 시스템보다 오탐률을 감소시킬 수 있고 이에 따라 정상 패킷이 폐기되는 확률을 줄일 수 있다. 따라서 본 논문에서는 두 임계값(즉, Th_{Low}, Th_{High})을 상황에 따라 조절한다.

C_t가 Th_{Low}를 넘어서 CS 구간에 진입하면 CS 구간 내의 패킷은 P_{CS}의 확률로 폐기하고 NS 구간 내의 패킷은 정상 서비스를 제공한다. C_t가 Th_{High}를 넘어서 RS 구간에 진입하면 RS 구간의 패킷은 P_{RS}의 확률, CS 구간의 패킷은 P_{CS}의 확률로 폐기하고 NS 구간의 패킷은 정상 서비스를 제공하여 내부 망에 유입되는 제어 패킷 수를 제한한다.

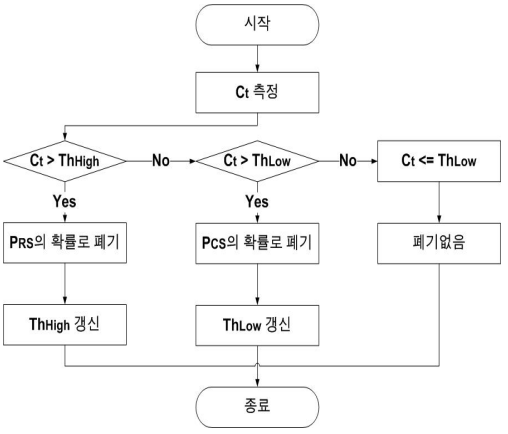

그림 4. 순서도
Fig. 4. Flowchart

Th_{Low}, Th_{High}는 지수가중평균에 의해서 결정되며 지수가중평균값을 이용하면 과거의 트래픽 양과 현재의 트래픽 양을 동시에 반영할 수 있다. 또한 입력되는 제어 패킷의 측정량의 변동이 순간적으로 큰 경우에 현재 측정량의 비중을 낮추면 큰 변동을 상쇄시킬 수 있다.

앞 절에서 언급한 학습상태에서 결정된 C_{Avg}와 C_{Max}를 기준으로 초기 Th_{Low}는 C_{Avg}, Th_{High}는 C_{Max}로 설정한다. 이후 C_t가 CS나 RS 구간에 진입하게 되면 각 구간의 타이머 $Timer_{CS}$, $Timer_{RS}$가 작동한다. 각각의 타이머는 해당 임계값의 초기화 여부를 결정한다. Th_{Low}에 대한 처리는 식 (1)과 같이 표현되며 $Timer_{CS}$가 만료되기 전에는 C_t를 α_1만큼 반영한 지수가중평균값으로 갱신하고 $Timer_{CS}$ 만료 후에는 Th_{Low}를 C_{Avg}로 초기화한다. Th_{High}에 대한 처리는 식 (2)과 같이 표현되고 $Timer_{RS}$ 만료 전에는 C_t의 반영비율이 α_2인 지수가중평균값으로 갱신하고 $Timer_{RS}$가 만료되면 Th_{High}를 초기값 C_{Max}로 재설정한다.

$$\begin{cases} Th_{Low} = C_{Avg} & ,\text{if } Timer_{CS} \ \ termination \\ Th_{Low} = Th_{Low} \times (1-\alpha_1) + C_t \times \alpha_1 & ,else \end{cases} \quad (1)$$

$(\text{if } C_t > Th_{Low})$

$$\begin{cases} Th_{High} = C_{Max} & ,\text{if } Timer_{RS} \ \ termination \\ Th_{High} = Th_{High} \times (1-\alpha_2) + C_t \times \alpha_2 & ,else \end{cases} \quad (2)$$

$(\text{if } C_t > Th_{High})$

위의 식 (1)의 α_1, 식 (2)의 α_2는 현재 패킷량 C_t의 반영 비중에 대한 값이며 이 값이 높아지면 C_t의 반영비중이 높아져 변동이 큰 결과값을 얻게 되고 C_t의 반영비중을 낮추면 안정적인 결과값을 얻을 수 있다. α_1, α_2, $Timer_{RS}$와 $Timer_{CS}$ 값은 해당 구현 시스템의 적용 환경이나 구현 방법에 따라서 달라질 수 있다.

Ⅳ. 실험 및 결과

제안 시스템의 효율성을 증명하기 위해 시뮬레이션을 통한 측정 결과를 분석하였다. 제안 시스템은 네트워크의 입력 라우터에 위치하여 라우터로 유입되는 모든 제어 패킷에 대하여 패킷량을 이용하여 공격을 탐지하고 제어한다.

제안 시스템의 임계값 설정을 위한 α_1, α_2와 패킷 폐기 확률인 P_{cs}, P_{cs}는 표 2와 같이 정의하였다. α_1, α_2값은 임계값의 변화에 영향을 미치므로 알고리즘 적용 시 중요한 역할을 한다.

표 2. 실험 파라미터
Table 2. Simulation Parameters

파라미터	적용 값
α_1	0.2
α_2	0.3
P_{CS}	40%
P_{RS}	90%
$Timer_{CS}$	3
$Timer_{RS}$	3

본 실험에서는 α_1, α_2값을 낮춰 각각의 이전 임계값의 비중을 크게 하여 임계값 변화폭을 줄였다. 폐기 확률 설정 시 공격 오탐률을 최소화하기 위해 CS 구간의 폐기 확률을 작은 값으로 설정하였다. 공격 가능성이 있는 RS 구간에서의 폐기 확률은 높은 값으로 설정하여 서버의 과부하를 방지하도록 하였다. 또한 해당 상태가 지속되면 임계값이 꾸준히 높아지므로 적절한 타이머 값을 설정하였다.

그림 5는 입력되는 패킷의 유입량과 본 시험에서 적용한 가중평균값을 나타낸다.

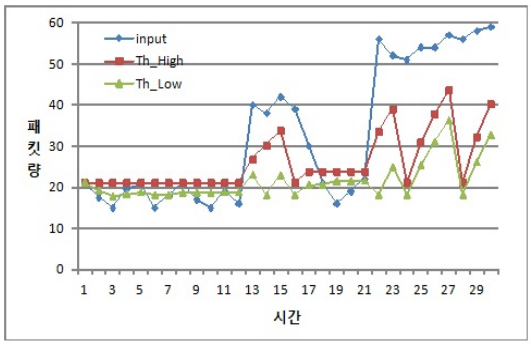

그림 5. 제안 시스템 임계값 변화
Fig. 5. Changes in the proposed system' s threshold

제안 시스템은 패킷 유입량이 증가함에 따라 임계값의 증가량도 커지므로 이를 방지하기 위하여 각 상태에 대한 타이머를 설정하고 만료되면 임계값을 초기값으로 갱신한다.

그림 5에서 임계값이 다시 낮아지는 지점이 타이머 만료 후에 임계값을 갱신하는 지점이다. 타이머를 이용하여 임계값이 지속적으로 증가하는 것을 방지할 수 있다. 또한 버퍼 유입량이 임계값 Th_{High}을 넘는 경우에 공격 상황을 인지하여 공격 탐지가 가능하다.

그림 6은 학습기간 이후 설정된 C_{Avg}, C_{Max}을 Ratelimit의 2개의 임계값으로 설정하여 제안 시스템과 비교한 그래프이다.

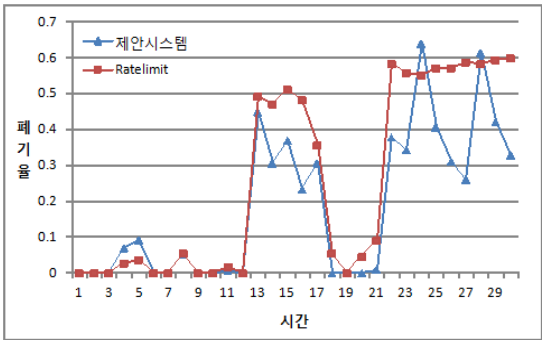

그림 6. Ratelimit과 제안시스템 폐기율 비교
Fig. 6. Drop rate comparison of the proposed system with one using the Ratelimit

그림 6의 공격상태에서 제안시스템의 폐기율이 Ratelimit의 폐기율보다 높은 지점이 발생하는데 이는 제안시스템의 임계값이 증가함에 따라 폐기율이 높아지므로 발생하는 현상이다. 이는 타이머를 조절하여 임계값의 증가 빈도를 낮추면 폐기율을 낮출 수 있다. 제안시스템은 정상 패킷량이 일시적으로 증가하는 상황에서 패킷량에 따라 임계값을 변화시키므로 고정 임계값을 갖는 Ratelimit보다 패킷 폐기율을 줄일 수 있다. 공격상태에서 Ratelimit은 패킷 폐기율이 증가하여 정상 패킷이 폐기될 확률이 높아지므로 정상적인 서비스 제공이 어렵다. 반면 제안시스템은 임계값에 따라 폐기율이 변화하여 정상 패킷이 폐기되는 확률과 시스템 버퍼로의 패킷 유입량을 조절하므로 정상적인 서비스를 제공할 수 있으며 버퍼 과부하를 방지할 수 있다.

V. 결 론

본 논문에서는 2개의 임계값을 기준으로 각 구간에 유입되는 제어 패킷에 대해 각기 다른 폐기율을 적용하여 DDoS 공격을 탐지하고 제어하는 방법을 제안하였다. 적용되는 임계값은 유입된 패킷량이 각각의 임계값을 넘을 경우에 갱신하여 동적인 임계값을 갖도록 한다. 각 구간마다 타이머를 설치하여 임계값이 지속적으로 증가하는 것을 방지한다. 제안한 방법에 맞는 DDoS 탐지 도구를 제작하여 실험하였으며 그 결과 정적 임계값을 갖는 시스템에 비해 일시적인 패킷 증가 상태에서 정상 패킷의 폐기율을 줄일 수 있었고 평균값을 임계값으로 갖는 시스템보다 공격상태에서 버퍼로 유입되는 패킷량을 감소시킬 수 있었다. 따라서 DDoS 공격 시에 버퍼로 유입되는 패킷량을 조절하여 공격 제어를 할 수 있고 일시적인 패킷 증가 상태에 대해서도 정상 패킷의 폐기율을 줄여 보다 높은 서비스를 제공할 수 있다. 제안 기술은 접속 네트워크의 진입점 이외에도 침입방지시스템[8], 클라우드 컴퓨팅 보안[9] 등 다양한 환경에 적용될 수 있다.

참 고 문 헌

[1] Tao Peng, Christopher Leckie, and Kotagiri Ramamohanarao, "Survey of Network-based Defense Mechanisms Countering the DoS and DDoS Problems," ACM Comput. Surv. 39, 1, Article 3, April 2007.

[2] Kyukjoon Kim and Sangjin Lee, "Distributed

Denial of Service attacks through the Network Forensic Compariso," The Journal of the Korean Institute of Information and Communication Engineering, 21(4), 7-74, 2011.6.
[3] Jelena Mirkovic and Peter Reiher. "A taxonomy of DDoS attack and DDoS defense mechanisms," ACM SIGCOMM Computer Communication Review, 34(2), April 2004.
[4] Sally Floyd and Van Jacobson, "Random Early Detection Gateways for Congestion Avoidence," IEEE/ACM Transactions on Networking, Vol.1(4), pp.397-413, Aug 1993.
[5] Hemant Sengar, "Overloading vulnerability of VoIP networkss" Proceedings of the 2009 IEEE/IFIP International Conference on Dependable Systems and Networks DSN 2009, 419-428.
[6] QPM Command Reference, http://www.cisco.com/en/US/docs/ios/12_0/qos/command/reference/qrcmdr.html
[7] John Ioannidis and Steven Michael Bellovin, "Implementing Pushback:Router-Based Defense Against DDoS Attacks," In Proceedings of the Network and Distributed System Security Symposium (NDSS), February 2002.
[8] I. Jeon, S. Kang, H. Yang, "Development of Security Quality Evaluate Basis and Measurement of Intrusion Prevention System," Journal of the Korea Academia-Industrial cooperation Society, v.11, no.4, April 2010.
[9] C. Park, "Study on Security Considerations in the Cloud Com," Journal of the Korea Academia-Industrial cooperation Society, v.12, no.3, March 2011.

※ 본 연구는 덕성여자대학교 2011년도 교내연구비 지원에 의해 수행되었음

저자 소개

노 희 경(학생회원)

- 2007년 3월 ~ 현재: 덕성여자대학교 컴퓨터공학부

<주관심분야: 인터넷통신, 통신보안>

강 남 희(정회원)

- 1999년 3월~2001년 2월: 숭실대학교 공학석사
- 2004년 12월: University of Siegen, 공학박사
- 2009년 3월 ~ 현재: 덕성여자대학교 디지털미디어학과 조교수

<주관심분야: 인터넷통신, 통신보안>