논문 02-27-8C-2 한국통신학회논문지 '02-8 Vol.27 No.8C

라우터의 생존성 개념을 이용한 DDOS 공격 방어의 새로운 접근

정회원 송 지 영*, 박 상 준*, 김 관 중**, 김 병 기***

A New Approach to DDOS Attack Defense Using the Survivability Concept of Router

Ji-Young Song*, Sang-Joon Park*, Kwan-Joong Kim**, Byung-Gi kim*** *Regular Members*

요 약

본 논문에서는 새로운 DDOS(Distributed Denial Of Service) 공격 형태와 이를 방어하기 위한 메카니즘을 제안한다. 현재까지의 DDOS는 최종 공격 목표가 특정 호스트이지만, 진보된 공격 형태로 특정 라우터가 공격의 대상이 될 수 있다. 이러한 공격은 특정 라우터의 관리하에 있는 다수의 호스트를 공격 대상으로 하는 것으로 특정 호스트가 서비스 불가능 상태가 되는 것 이상으로 피해는 심각하다고 할 수 있다. 라우터의 생존성 개념을 적용하여 DDOS 공격 하에서도 라우터가 서비스 불능 상태가 되지 않도록 라우터가 능동적으로 링크의 대역폭을 조절하여 트래픽의 양을 조절할 수 있도록 한다.

ABSTRACT

In this paper, we present a new form of DDOS attack and a mechanism to defend systems from it. Up to now the ultimate target of a DDOS attack is a specific host. But in the near future router attacks are expected to appear. Because these kinds of attacks may involve many hosts in the managed domain of a specific router, they will be still more serious than the current DDOS attacks. Also, we present an algorithm to defend against an attack on a router using survivability of the router. By using a survivability of a router, the router can control a quantity of traffic autonomously without an interruption of services even when a DDOS attack occurs.

I. 서 론

DOS는 더 정교해지고 지능화 되는 추세이며 인터넷의 상용화 및 영향력이 증대됨에 따라 피해 규모가 점점 커지고 있다. DDOS는 시스템의 취약성을 이용하는 것이 아니라 시스템이 네트워크에 연결된 점을 이용하기 때문에 방어하기가 어렵다. Trinoo, TFN, Stacheldraft, TEN2k, Shaft와 같은 잘 알려진 DDOS 공격도구들은 보안이 취약한 인터넷상의 많은 호스트를 이용하여 공격을 시도한다. 그림 1은 DDOS공격 과정을 나타낸다. 공격자는 필요한 수만큼의 마스터에 불법 침입하여 공격 프로그램을 설치하며, 마스터는 다시 여러 대의 슬레이브에 공격 프로그램을 설치한다. 마스터는 슬레이브를 원격으로 제어하며, 공격자는 마스터에게 적절한 시간에 특정 목적지를 공격하도록 지시한다.

DDOS의 공격에 대응하기 위한 방법으로 방어벽, 필터링[1], 공격도구의 검색, IP 추적[2]등과 같이 방법들이 연구되었다. 이러한 방법들은 공격 패킷의 일시적인 감소나 공격의 피해를 줄이는 방법으로는 고려될 수 있지만, 근본적인 해결 방법은 되지 못하였다. 최근에는 DDOS가 네트워크의 혼잡을 이용한

* 숭실대학교 컴퓨터학과 컴퓨터구조연구실(jysong@archi.ssu.ac.kr)
** 한서대학교 컴퓨터정보학과
*** 숭실대학교 정보과학대학 컴퓨터학부
논문번호 : 010402-1220, 접수일자 : 2001년 12월 20일

방법임에 착안하여 Pushback 알고리즘[3]이 제안되었다. Pushback은 네트워크의 혼잡 상황이 발생하면 라우터에 입력되는 패킷을 확인하여 ACC (Aggregate-based Congestion Control)개념[4]에 따라 공격 패킷을 폐기하는 방법이다.

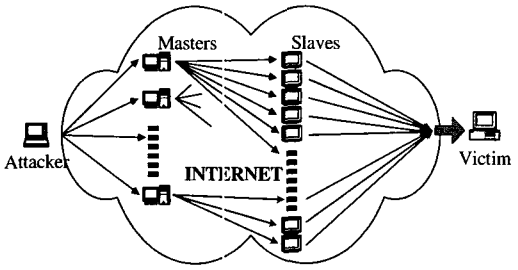

그림 1. DDOS의 공격 과정

현재까지 DDOS는 최종 공격 목표가 특정 호스트이지만, 한 단계 더 진보된 공격으로 특정 라우터의 공격이 예상된다. 라우터 공격은 특정 라우터의 관리하에 있는 다수의 호스트를 공격 대상으로 한다. 라우터가 서비스 불가능 상태가 되면 다수의 호스트는 라우터로부터 패킷을 전송 받거나 전송하지 못한다. 이것은 특정 호스트가 서비스 불능 상태가 되는 것 이상으로 그 피해는 심각하다.

본 논문에서는 DDOS를 방어하기 위해 라우터의 생존성 개념을 제안한다. 라우터 생존성은 라우터가 최악의 상황에서 최소한의 기능을 유지하는 개념이다. 라우터의 생존성 개념을 적용하여 DDOS 공격하에서도 라우터가 능동적으로 트래픽의 양을 조절할 수 있도록 한다. 논문의 구성은 다음과 같다. 2장에서는 라우터의 생존성 개념을 소개하며, 3장에서는 라우터에 생존성 개념을 적용하여 DDOS의 공격 방어 방법을 제시한다. 4장에서는 제시한 방법의 성능평가를 보이며, 마지막 5장에서 결론을 맺는다.

Ⅱ. 라우터의 생존성의 개념

1. 라우터 공격

DDOS의 호스트 공격은 에이전트에서 호스트가 원활한 서비스를 제공하지 못하도록 특정 호스트를 목적지 주소로 하여 TCP SYN 패킷을 플러딩 하거나, UDP 포트 공격이나 ICMP ECHO 패킷을 계속적으로 발생시키는 방법이다[5]. 이에 반하여 라우터 공격은 여러 경로를 통해서 진행될 수 있다. 특정 호스트 공격과 같은 방법으로 진행이 가능하며, 라우터를 경유하여 전달되는 패킷의 경로를 입수하여 여러 개의 목적지 주소를 가지고 분산된 형태로 진행될 수 있다. 그림 2를 고려하자. 그림 2에서 가는 선은 정상적인 링크이며, 굵은선은 공격이 진행중인 링크이다. 최종 공격 대상은 R6이다. 최악의 상황에서 R6은 버퍼 오버플로우나 대역폭 부족으로 인해 라우터는 정상적인 서비스를 할 수 없게 된다. R6이 정상적인 서비스가 불가능해지면 R6으로부터 패킷을 전달받고 있는 다수의 호스트나 라우터들은 서비스가 원활하지 못할 것이다. 결국, 호스트들은 다른 라우터를 통하여 패킷을 전달받아야 하므로 인접한 다른 라우터로 트래픽이 집중되어 또 다른 링크의 혼잡상황을 초래할 것이다.

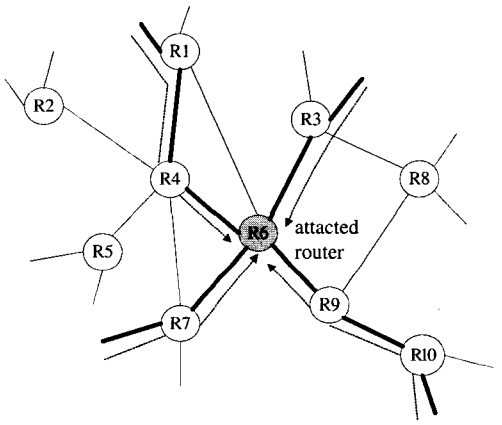

그림 2. DDOS의 라우터 공격 과정

라우터 공격의 심각성은 이미 언급했지만, 그 피해는 호스트 공격에 비해 피해가 더 크고 광범위하다. 호스트 공격은 특정 호스트의 서비스를 불가능하게 하여 호스트 운영자에게만 경제적인 손실을 주지만, 라우터 공격은 라우터의 관리를 받는 다수개의 호스트는 물론 인터넷 서비스 운영자에게도 경제적인 피해를 줄 수 있다.

2. 라우터의 생존성(Survivability of Router)

최근 발표된 논문에는 불법적인 공격과 침입에 방어하기 위한 새로운 개념을 제안하고 있다[6][7]. 현재 대규모로 분산되어 있고 경계가 불분명한 인터넷은 보안정책이 명확하게 정의되어 있지 않고, 중앙 집중적인 관리가 불가능한 시스템으로 많은 침입과 위험요소를 가지고 있다. 생존성은 경계가 불분명한 네트워크 환경에서 시스템이 불법적인 침입

이나 공격에 직면하였을 때 반드시 지켜져야 하는 기본적인 기능들을 수행할 수 있도록 하는 개념이며, 공격에 대한 인식과 침입 이후에 정상적인 서비스가 가능하도록 복구하는 개념이다.

라우터를 공격 목표로 한 DDOS 공격에서는 TCP 개념의 혼잡제어 메카니즘으로는 링크의 혼잡을 해결할 수 없다. 무수히 범람하는 패킷들을 TCP 개념의 혼잡제어 기법으로 해결하기란 한계가 있으며, 결국에는 라우터의 시스템 정지와 같은 최악의 결과를 초래할 수 있다. 따라서, 이에 능동적으로 대처할 수 있는 라우터의 생존성을 위한 전략과 앞으로 전개될 라우터 공격에 방어하기 위한 메카니즘을 제시한다.

3. 생존성을 위한 단계 정의

라우터 생존성을 위한 단계 정의는 표 1과 같다. 라우터의 생존성은 라우터에 트래픽이 집중되는 상황에서도 라우터 최소한의 기본적인 기능은 유지할 수 있어야 하며 최악의 경우에도 자원의 부족으로 다운되는 경우는 없어야 한다. 따라서 2단계인 공격의 인식 상황에서 4단계인 회복 단계까지 라우터는 정상적인 동작을 하고 있어야 한다.

표 1. 라우터의 생존성을 위한 단계 정의

분 류	설 명
정상 (Normal)	o 라우터의 공격을 모니터링하는 단계
인식 (Recognition)	o 특정 입출력 포트로 패킷이 집중되며, 입력 큐의 길이가 임계치를 초과한 경우 o 공격을 인식한 상태, 라우터의 위험등급 평가
핸들링 (Handling)	o 평가된 라우터의 위험도를 바탕으로 라우터의 기능 유지를 위한 링크의 대역폭 관리 단계
회복 (Recovery)	o 핸들링 방법에 따라 처리하여 라우터의 위험도가 떨어지고, 정상적인 상태로 회복된 단계

결국 라우터의 생존성을 위한 네 가지 단계는 그림 3과 같이 순환한다고 할 수 있다. 라우터가 정상적인 상태에서 공격 인식, 그리고 공격에 대한 핸들링, 마지막으로 라우터의 자원이 정상적으로 회복되어 공격 이전과 같이 정상적인 동작이 가능하도록 하는 회복 단계의 순환 상태로 표현 할 수 있다.

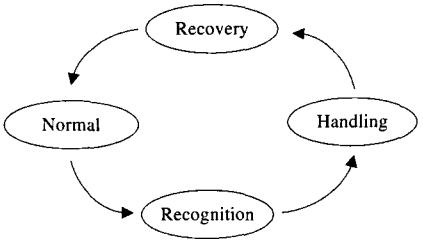

그림 3. 라우터의 생존성을 위한 순환

4. 라우터의 위험등급 정의

라우터의 위험 등급 정의는 라우터의 생존성을 위한 단계별 정의에서 공격 패킷의 입력 상황에 따른 라우터의 상태를 나타낸다. 라우터의 위험등급을 네 개의 등급으로 분류하여 표 2와 같이 정의하였다. A는 가장 위험도가 낮은 상태이며, C는 위험상태가 가장 높은 상태이다.

표 2. 라우터의 위험등급 단계 정의

Classification	Range of α
Normal	$\alpha < 0$
A	$0 <= \alpha < 0.15$
B	$0.15 <= \alpha < 0.3$
C	$0.3 <= \alpha$

q_{tot}를 전체 큐의 길이, q_{cur}를 현재 큐의 길이, q_{th}를 큐의 임계치라고 정의하자. 공격으로 인해 임계치를 초과한 큐의 길이 q_d는 q_{tot} / q_{cur}로 구할 수 있다. 전체 입력 큐의 길이에서 임계치를 초과한 비율 α 는 (1)과 같이 구한다.

$$\alpha = q_d / q_{tot} \quad (1)$$

α 값에 따라 라우터의 위험 등급을 결정한다. 일반적으로 링크의 로드가 80% 이상이면 큐의 길이와 패킷 지연이 현저히 증가하므로 임계치는 전체 큐 길이의 50~70%가 적정하다[8]. 그림 4는 α 의 분포에 따른 위험등급을 나타낸다. 임계치와 현재의 큐의 길이는 모두 전체 큐 길이에 대한 비율로 표현하였다. α 가 0 보다 작으면 큐의 길이가 임계치를 초과하지 않은 상태이므로 정상적인 상태이며, 0 보다 같거나 크고 0.15보다 작으면 위험등급 A로 분류하였다. α 가 0.15보다 같거나 크고 0.3보다 작으면 위험등급 B, 그리고 0.3보다 같거나 크면 위험등급 C로 분류하였다.

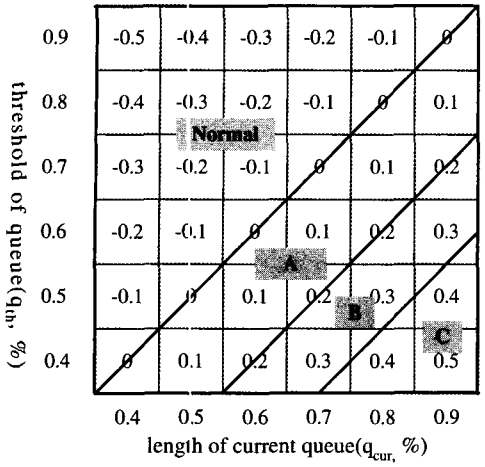

그림 4. α의 분포에 따른 위험등급 범위

Ⅲ. 라우터 DDOS 공격 방어 메카니즘

라우터는 정상상태에서 공격을 인식하면 공격인식 상태로 천이 한다. 라우터 공격은 여러 개의 입출력링크중에서 특정 라우터로 전달되는 패킷의 증가로 인해 해당 링크에 패킷이 집중된다. 입력 큐의 길이가 임계치를 초과한다고 하여 공격으로 간주하는 것은 합법적인 트래픽의 증가로 인한 혼잡 상태일 경우를 배제할 수 없기 때문에 특정 라우터 공격을 예측할 수 있는 방법이 필요하다.

입력 큐의 길이가 임계치를 초과하면서 여러 개의 입출력링크 중 특정 입출력링크의 이용율이 다른 링크보다 현저히 높으면 공격 상태로 판단한다. 그림 5는 라우터에서 공격인식을 나타낸다. 라우터의 상태는 아래의 조건 1과 조건 2, 조건 3을 동시에 만족하는 경우에 공격인식 상태로 천이 한다. 조건 1은 입력 큐의 크기가 임계치를 초과하였는지를 판단하며, 조건 2와 조건 3은 입출력링크의 이용율에 대하여 판단한다.

- 조건 1 : $q_{cur} > q_{th}$
- 조건 2 : 특정 입력링크가 다른 입력링크에 비해 이용율이 현저히 높다.
- 조건 3 : 특정 출력링크가 다른 출력링크에 비해 이용율이 현저히 높다.

물론 위에서 제시한 조건들을 모두 만족시킨다고 하여 공격 패킷에 의한 혼잡상황이라고 할 수 없지만, 합법적인 패킷의 혼잡상황이나 공격 패킷에 의한 혼잡상황은 정상적인 서비스 기능을 저하시키므로 혼잡발생에 대한 제어는 반드시 필요하다.

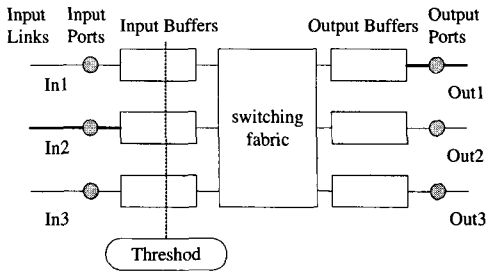

그림 5. 공격 인식

그림 6은 두개의 라우터 사이에 진행되는 핸들링 과정을 나타낸다. R3에서 R6으로 공격 패킷이 전달되고 있으며, 굵은 선이 공격 링크이다. R3의 입력링크 2로부터 유입된 공격 패킷은 출력링크 1을 통하여 R6의 입력링크 1을 통해 전달된다. R3은 공격인식 규칙에 따라 공격 상태로 인식이 되면, 표 2에 따라 라우터의 위험 등급을 결정한다. 그 다음, 공지 메시지를 작성하여 R6으로 전송한다. 공지 메시지 수신한 R6은 자신의 위험 상태를 결정한 후 핸들링 방법을 선택하여 응답메시지를 R3에게 전송한다. 응답 메시지를 받은 R3은 R6의 지시에 따라 출력링크의 대역폭을 조절한다. 이와 같은 방법으로 네트워크상의 모든 라우터들은 독립적으로 핸들링을 진행한다. 공지 메시지와 응답 메시지 형식 및 핸들링 결정 방법은 다음에 설명한다.

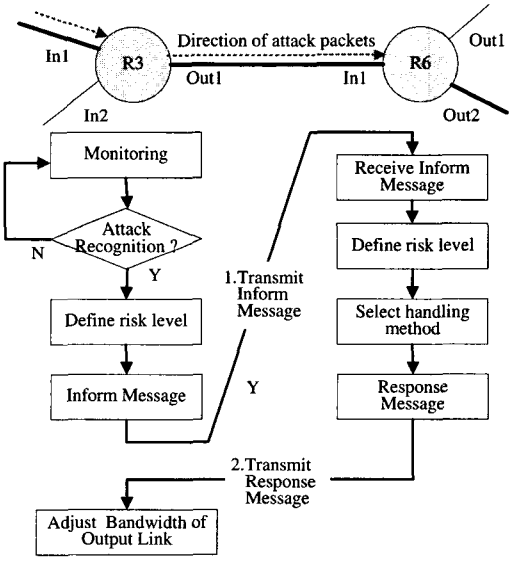

그림 6. 핸들링 과정

(1) 공지 메시지(Inform Message)

공지 메시지는 라우터가 공격상태를 인식한 후에

R6에게 현재의 상태를 알려주는 메시지이다. 메시지 형식은 표 4와 같다. 첫 번째와 두 번째 필드에는 메시지를 보내는 라우터와 수신하는 라우터의 ID를 기입하며, 혼잡이 발생하는 입력 인터페이스와 출력 인터페이스를 기입한다. 위험 등급(risk level)은 R3의 위험 상태를 나타낸다.

표 3. 공지 메시지 형식

Source Router
Destination Router
Input Interface
Output Interface
Risk Level

(2) 응답 메시지(Response message)

R3으로부터 공지 메시지를 받은 R6은 자신의 현재 상태를 결정한 후 핸들링 방법을 결정하여 응답 메시지를 보낸다. 표 5는 응답 메시지의 형식을 나타낸다. 위험 등급은 R6의 위험 정도를 나타내며, 핸들링 필드는 R6의 위험 정도에 따라서 R3에서 수행하게 될 핸들링 방법을 기입한다. 응답 메시지를 받은 R3은 R6의 핸들링 지시에 따라 출력링크의 대역폭을 조절하여 R6으로 전송되는 패킷의 양을 조절한다.

표 4. 응답 메시지 형식

Source Router
Destination Router
Input Interface
Output Interface
Risk Level
Handling

(3) 핸들링 방법의 결정

핸들링 방법은 공지 메시지를 수신한 R6에서 결정 한다. R6은 자신의 위험 상태를 기반으로 하여 핸들링 방법을 결정하여 R3의 출력링크 대역폭을 동적으로 조절하도록 한다. 대역폭을 조절하는 파라미터 β는 α의 범위에 따라 정해진다. α가 임계치를 기준으로 현재 입력 큐 길이를 나타내므로 α에 따라 β가 결정한다. 핸들링 등급은 H1에서 H4의 4개의 등급으로 분류된다. α의 범위에 따른 β의 값은 표 5와 같다. 응답 메시지를 받은 라우터 R3는 R6에서 정한 파라미터 β값에 따라서 출력링크 대역폭을 (2)와 같이 조정한다.

$$BW_{new} = BW_{old} * (1-\beta) \quad (2)$$

현재의 사용중인 대역폭을 최대 40%까지 줄여 공격이 진행되고 있는 링크의 대역폭을 감소 시켜 전송되는 패킷의 양을 조절한다.

표 5. 핸들링 방법 정의

분류	범 위	β
H1	α < 0.1	0.1
H2	0.1 <= α < 0.2	0.2
H3	0.2 <= α < 0.3	0.3
H4	0.3 <= α	0.4

Ⅳ. 성능평가

본 장에서는 시뮬레이션을 통하여 제안한 기법의 성능을 평가한다. 성능평가의 목적은 공격 패킷이 집중되는 라우터에서 현재 큐의 길이를 모니터링 하여 미리 정의한 위험등급으로 평가되면, 공격 패킷을 전송해주는 라우터에게 현재의 대역폭을 조절하여 라우터의 위험 상태를 완화시키도록 한다. 따라서, 동일한 성능평가 환경에서 라우터에 생존성 알고리즘이 적용된 경우와 그렇지 않은 경우의 큐의 길이를 비교 분석한다.

1. 성능평가 모델

성능평가를 위한 도구는 NS-2(Network Simulator-2)를 사용하였다. 그림 7은 성능평가를 위한 간단한 네트워크 모델을 나타내고 있다. 각 노드사이의 모든 링크는 양방향 링크이며 대역폭은 2Mbps로 하였다. 전송지연은 20ms이다. 각 노드의 큐의 길이는 20 Packets이며 RED 큐를 이용하였다. 각 노드의 입력 큐 임계치는 12로 하였다. 노드별로 발생되는 트래픽의 특성은 표 6과 같다.

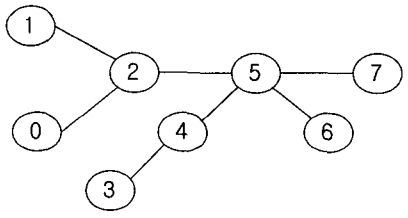

그림 7. 성능평가를 위한 네트워크 모델

표 6. 공격 트래픽의 특성

공격지 (노드)	공격 Agent	Traffic Generator	Packet Size	Rate
0	UDP	Application/Traffic /CBR	200 Bytes	0.7Mb
1				0.6Mb
3				0.5Mb
4				0.4Mb
6				0.3Mb

각각의 공격 노드에서 생성된 패킷은 노드 5를 경유하여 노드 7로 향한다. 따라서 노드 5는 5개의 공격 노드에서 생성된 패킷이 집중된다. 각각의 공격 노드는 1초 간격으로 공격 패킷을 발생시키며 5초 후에는 모든 공격노드에서 동시에 공격 패킷이 발생하게 된다. 성능평가 시간은 모든 트래픽이 발생되는 경우 일정시간 후에는 큐의 길이 변화가 안정상태에 접어드는 20초로 하였다.

2. 성능평가 결과

각 공격 노드에서 발생한 패킷은 노드 2나 노드 4를 경유하여 노드 5로 집중되며, 최종적으로 노드7로 전달 된다. 따라서 SCR은 생존성 개념이 적용된 경우이며, Non_SCR은 생존성 개념이 적용되지 않은 경우이다. 그림 8과 그림 9는 노드 5에서의 큐의 길이와 평균 큐의 길이를 각각 나타낸다. 5초 이후는 모든 공격 트래픽이 동시에 전달되므로 5초에 큐의 길이가 급격히 증가한다. Non_SCR은 5초 이후에는 큐에 길이가 포화상태에 이른 상태로 지속된다. 이런 상황에서 라우터는 정상적인 동작을 할 수가 없으며 합법적인 트래픽도 전달되지 못한다. 상황이 계속되면 라우터는 본래의 기능을 상실하게 된다. 이에 반해, SCR은 생존성 개념이 적용되어 핸들링이 되는 6초 이후에는 큐의 길이가 12와 14 사이에서 변화한다. 큐의 길이가 유동적으로 조정됨을 볼 수 있다.

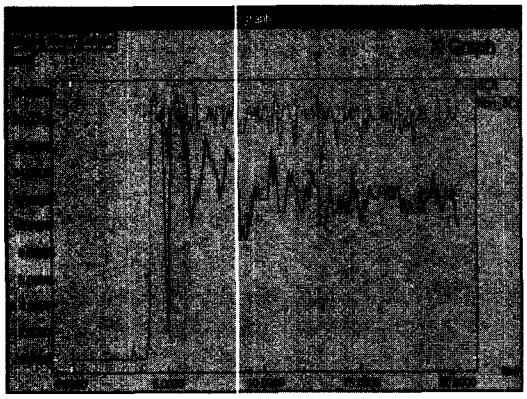

그림 8. 노드 5의 큐 길이 변화

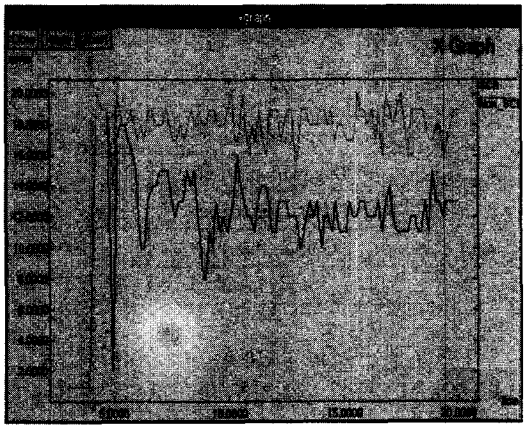

그림 9. 노드 5의 평균 큐 길이 변화

따라서, 생존성 개념이 적용된 라우터는 위험 상태를 인식하고 그에 따른 적절한 방어로 DDOS공격으로부터 자신을 보호 할 수 있음을 보여 주고 있다. 공지 메시지와 응답 메시지를 통해서 공격 트래픽으로 혼잡이 발생하는 링크의 대역폭을 조정함으로써 입력 큐의 오버플로우를 예방하여 라우터 스스로가 최소한의 기능을 유지 할 수 있음을 보여 주고 있다.

V. 결 론

지금까지의 DOS나 DDOS의 문제 해결을 위해서는 패킷 필터링이나 공격 근원지 추적, 네트워크의 혼잡 제어를 통해서 해결하려고 노력하였다. 본 논문에서는 DDOS의 새로운 공격 형태인 라우터 공격과 이를 방어하기 위한 메카니즘을 제시하였다. 기존의 제안들은 네트워크 관리자의 수동적인 조작을 통해서 가능하였다. 우리는 라우터 스스로 위험 상황을 인식하고 이에 따른 적절한 핸들링을 통하여 능동적으로 공격 방어를 할 수 있는 방법을 제안하였다. 공격 트래픽이 집중되면 라우터는 큐의 길이를 바탕으로 위험등급을 결정하고 공지 메시지를 전송한다. 공지 메시지를 받은 라우터는 핸들링 방법을 결정하여 응답 메시지를 보낸다. 응답 메시지를 받은 라우터는 핸들링 방법에 따라 출력링크의 대역폭을 조정하여 공격 트래픽을 제어하도록

하였다. 또한 성능평가를 통하여 생존성 개념이 적용된 라우터가 공격 상황에서도 안정적인 서비스를 제공하며 큐의 길이를 적절히 유지하고 있음을 보였다. 호스트에 대한 공격은 최근 들어 심각성이 더해지고 있다. 라우터의 생존성 개념은 공격 상황에서 수동적인 방어 방법에서 벗어나 능동적이고 적극적인 공격 방어 방법이라고 할 수 있다. 향후 합법적인 트래픽의 손실을 최소화하는 연구가 필요하다.

참 고 문 헌

[1] Kihong Park, Heejo Lee, "On the Effectiveness of Route-Based Packet Filtering for Distributed DOS Attack Prevention in Power-Low Internets", *In Proceeding of ACM SIGCOMM'01*, 2001.

[2] Dawn xiaodong Song and Adrian Perrig "Advanced and authenticated techniques for ip traceback," *IEEE INFOCOM'01*, 2001.

[3] John Ioannidis, Steven M. Bellovin, "Pushback : Router-Based Defense Against DdoS Attacks", *Technical report*, 2001.

[4] Ratul Matajan, Steven M. Bellvin, Sally Floyd, "Controlling high bandwidth aggregates in the network," *Submitted to ACM SIGCOMM'01*, 2001.

[5] Christoph L. Schuba, Ivan V. Krsul, Markus G. Kuhn, Eugene H. Spaffold, Aurobindo Sundaram, and Diego Zamboni. "Analysis of a denial of service attack on TCP," *IEEE Symposium on Security and Privacy*, pp.208-223, 1997.

[6] R.C. Linger, R.J. Ellison, H.F. Lipson, T.A.Longstaff, N.R.Mead, "The Survivability Imperative : Protecting Critical Systems," *Technical Report, Software Engineering Institute, Carnegie Mellon University*, 1997.

[7] David a. Fisher and Howard F. Lipson, "Emergent Algorithm : A New Methodf for Enhancing Survivability in Unbounded Systems," *CERT Coordination Center Software Engineering Institute*, 1999.

[8] Willian Stalling, "Data And Computer Communications", *Prentice-Hall*, 1997.

송 지 영(Ji-Young Song) 정회원

1999년 2월 : 청운대학교 컴퓨터과학과 졸업
2001년 2월 : 숭실대학교 컴퓨터학과 공학석사
2001년 3월~현재 : 숭실대학교 컴퓨터학과 박사과정

<주관심 분야> 인터넷 QoS, 네트워크 생존성 및 위험분석, 네트워크 보안

박 상 준(Sang-Joon Park) 정회원

한국통신학회논문지, 재25권 제7B호, 2000년 7월호, pp.1178-1184 참조

김 관 중(Kwan-Joong Kim) 정회원

1983년 2월 : 숭실대학교 전산학과 졸업
1988년 2월 : 숭실대학교 전산학과 공학석사
1998년 8월 : 숭실대학교 컴퓨터학과 공학박사

1997년 3월~현재 : 한서대학교 컴퓨터정보학과 교수

<주관심 분야> 컴퓨터구조, 마이크로 프로세서, 병렬처리, VLSI 설계

김 병 기(Byung-Gi Kim) 정회원

한국통신학회논문지, 재25권 제7B호, 2000년 7월호, pp.1178-1184 참조