논문 2004-41TC-6-3

클래스 기반의 대역 제한 기법을 통한 이메일 서버의 보호

(Protecting E-mail Server with Class-Based Rate Limiting Technique)

임 강 빈*, 이 창 희**, 김 종 수***, 최 경 희****, 정 기 현*****

(Kang Bin Yim, Chang Hee Lee, Jong Su Kim, Kyung Hee Choi, and Gi Hyun Jung)

요 약

본 논문에서는 CBQ (Class Based Queuing) 알고리즘을 이용하여 DDoS공격으로부터 메일 서버를 보호할 수있는 효과적인 방법을 제안한다. 제안하는 방법에서는 메일 서버로 입력되는 트래픽을 중요한 메일 트래픽, 덜 중요한 메일 트래픽, 그 외의 공격의 가능성이 있는 알 수 없는 트래픽으로 구분하고 이들 각 트래픽에 서로 다른 대역폭을 할당함으로써 DDoS 공격 하에서도 정상적인 메일의 송신을 가능하게 한다. 제안하는 방법은 입출력 포트의 대역폭을 별도의 서비스(트래픽 클래스)마다 분산 할당하는 데에 유용한 가중치 사용 라운드 로빈 큐 스케줄링을 이용하는 WFHBD(Weighted Fair Hashed Bandwidth Distribution) 엔진을 고속 스위칭 프로세서를 내장한 임베디드 시스템에서 사용하고 실험을 통하여 DDoS 공격으로부터 메일 서버가 효율적으로 보호될 수 있음을 검증한다.

Abstract

This paper proposes an efficient technique to protect e-mail server from DDoS attack using the CBQ (Class Based Queuing) algorithm. The proposed method classifies incoming traffic to an e-mail server into three classes: "more important mail traffic", "less important traffic" and "unknown traffic"and assigns bandwidths differently to the traffics. By differentiating the bandwidths of classes, normal mail traffic may flow even under DDoS attack in the proposed technique. The proposed technique is implemented on an embedded system, which hires a switching processor with the WFHBD(Weighted Fair Hashed Bandwidth Distribution) engine that has been known as an efficient algorithm to distribute a given bandwidth to multiple sources, and it is verified that it can be an efficient way to protect e-mail server from DDoS attack.

Keywords : Bandwidth rate limiting, E-mail, Queue scheduling, WFHBD, Class, DDoS

I. 서 론

통신 기술의 발전과 인터넷의 급속한 성장으로 누구나 쉽게 인터넷 서비스를 사용할 수 있게 되었다. 현재, 가장 많이 사용되는 인터넷 서비스로는 전자메일(E-mail) 서비스와 웹 서비스가 있다. 특히, 전자메일 서비스는 2002년 현재 전체 인터넷 사용자의 72.2%가 사용하고 있음이 한국리서치 미디어 인덱스에 의하여 보고된 바 있다[1]. 이와 같이 전자메일 서비스는 사용의 편리함과 정보 전달의 효율성으로 인하여 폭 넓게 사용되고 있으므로 이를 제공하는 메일 서버의 안정성과 보안방안이 날로 중요해지는 추세이다.

그러나 인터넷 서비스의 사용이 증가함에 따라 이의

* 순천향대학교 정보보호학과
(Dept. of Information Security Engineering, Soon chunhyang university)
** LG전자(LG전자)
(LG electronics)
*** 에스넷시스템(주)
(SNETSYSTEMS INC.)
**** 아주대학교 정보및컴퓨터공학부
(School of Information and Computer Engineering, Ajou University)
***** 아주대학교 전자공학부
(School of Electrical and Electronics Engineering, Ajou University)
※ 본 논문은 과기부 국가지정연구실사업 및 정통부 IT분야 해외교수초빙 국제공동연구사업의 지원으로 연구되었음
접수일자:2004년2월20일, 수정완료일: 2004년5월25일

부작용으로서 인터넷을 통한 해킹이 급속히 증가하고 있다. 대표적인 해킹 방법으로서는 DDoS(Distributed Denial of Service) 공격이 있다. 이 공격은 분산된 다중의 시스템을 이용, 특정 시스템 또는 네트워크에 대량의 트래픽이나 연결 요청을 전송하여 네트워크 대역폭 및 시스템 자원을 고갈시킴으로써 정상적인 서비스를 방해하는 방법을 말한다[2]. 이러한 DDoS 공격은 방어하기가 어렵기 때문에 최근에도 주요 인터넷 사이트들이 이 공격에 의하여 서비스가 중단됨으로써 커다란 경제적 손실을 입은 사례가 있다.[3] 인터넷에 연결되어 있는 모든 시스템은 DDoS 공격의 대상이 될 수 있으며 특히, 상업적으로나 학술적으로 중요한 메일 서버에 대한 공격은 더욱 치명적일 수 있다.

이러한 공격을 막기 위한 방안이 다각도로 연구되고 있는데 대표적인 것으로 침입 탐지 시스템(Intrusion De-tection System)이나 침입 차단 시스템(Firewall)을 들 수 있다. 그러나 이러한 방법들은 데이터 처리를 위한 시스템의 과부화와 네트워크 대역폭에 대한 유연성 결여 등의 문제가 있어 만족스러운 성능을 발휘하지 못하고 있다.[4]

본 논문에서는 이러한 문제점을 보완하기 위하여 네트워크 대역폭 할당에 유연한 클래스 기반 큐잉(Class Based Queuing)기반의 가중치 사용 라운드 로빈 큐잉(Weighted Round-robin Queuing) 스케줄링 방법을 하드웨어적으로 구현한 WFHBD(Weighted Fair Hashed Bandwidth Distribution) 엔진을 실제의 네트워크 시스템에 적용하여 실험함으로써 메일 서버에 대한 DDoS 공격으로부터 메일 트래픽의 대역폭이 고갈되는 것을 막을 수 있음을확인하였다.

WFHBD 엔진에서는 포트의 대역폭을 몇 가지 기준에 의하여 분류된 트래픽 클래스에 대역폭을 분산 할당하여 트래픽 클래스간에 상호 공정성과 독립성을 보장하는 동시에 고속의 네트워크 환경에서의 사용에 적합하다.[5]

WFHBD 엔진을 사용하여 메일 서버를 효율적으로 보호하기 위하여는 입력 트래픽을 적절한 트래픽 클래스로 나누는 것이 중요하다. 메일 트래픽은 웹 트래픽과 다르게 메일을 송신하는 시스템이 한정되어 있어 변화가 많지 않고, 메일을 송신하는 시스템에 따라 그 중요도를 구분할 수 있다.[6] 따라서 메일 서버로 입력되는 트래픽을 중요한 사용자 그룹으로부터의 메일 트래픽(More Important Mail Traffic)과 다소 덜 중요한 사용자 그룹으로부터의 메일 트래픽(Less Important Mail Traffic), 그리고 이외의 공격의 가능성이 있는 알 수 없는 트래픽(Unknown Traffic)으로 나누고 이들 트래픽 클래스간의 대역폭 할당에 차등을 둠으로써 중요한 메일 트래픽을 우선적으로 보호하고자 한다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 메일 서버의 보호를 위한 다양한 방법에 대하여 알아 보고, Ⅲ장에서는 WFHBD 엔진 및 이를 위한 트래픽 분류 방안에 대하여 설명한다. Ⅳ장에서는 제안한 방안을 위한 실험 환경과 실험 결과에 대하여 논하며 끝으로 Ⅴ장에서 결론을 맺는다.

Ⅱ. 관련연구

서론에서 논한 바와 같이 메일 서버에 대한 DDoS 공격은 매우 심각한 문제이며 이의 해결이 절실히 요구된다. 이를 위하여 많은 연구에서 다각도의 시도가 이루어지고 있다. 현재 메일 서버보호를 위하여 사용되고 있는 가장 일차적인 방안은 침입 차단 시스템을 이용하여 메일 서비스 이외의 모든 여타 서비스를 차단하는 것이다. 침입 차단 시스템의 기본적인 작업은 입력창구(ingress) 및 출력창구(egress)를 오가는 모든 패킷을 검사 하여[7] 메일 서비스를 위한 패킷 이외의 것들을 모두 폐기하는 일이다. 이렇게 함으로써 메일 트래픽이 메일 서버로 전달되는 것을 보장 받을수 있다. 그러나, 이는 고속의 네트워크에서 대량의 패킷을 처리하는 경우에는패킷 처리 부하가 지나치게 커지는 문제가 수반된다. 더구나, 위조된 ICMP 패킷을 사용하는 Smurf등의 네트워크 2계층 공격은 차단하기가 매우 어려워서 메일 서버로 그 공격이직접 전달되어 피해에 노출 될 수 밖에 없다.[8]

메일 서버 팜과 같이 메일 서버를 증설함으로써 상기와 같은 문제를 다소간 해결할 수 있다. 다만, 이러한 방법은 근본적인 문제를 해결할 수없을 뿐만 아니라 지나치게 자원을 낭비하는 결과를 초래하며 구축과 관리를 위한 과대한 비용이 소요되는 문제점이 수반된다. 따라서, 한정된 자원을 효율적으로사용하면서 근본적인 문제를 해결할 수 있는 방안이 절실히 요구된다.

이와 같이 네트워크에서 직면하고 있는 대부분의 문제는 한정된 공유 자원을 할당하는 것과 연관되어 있다.[9] 이와 관련하여, 큐 스케줄링 방법은 입력된 트래픽 중에서 한정된 공유 자원으로서의 출력 포트로 출력될 다음 트래픽을 알고리즘에 의해 알맞게 선택함으로써 트래픽 간의 대역폭을 제어할 수 있다. 이러한 특성을 이용하여, 입력되는 트래픽을 적절히 클래스로 나누고

이에 큐 스케줄링 방법을 적용하면 메일 서버에 대한 트래픽을 DDoS 공격으로부터 효과적으로 보호할 수 있다. 이를 위하여 알고리즘의 복잡성과 공정성 사이에서 알맞은 균형을 찾기 위한 여러 가지큐 스케줄링 알고리즘이 있다.

FIFO(First In First Out)는 가장 기본적인 큐 스케줄링 알고리즘으로서 입력 패킷은 도착하는 순서에 따라 버퍼링 및 전송되며 모든패킷은 동등하게 취급된다. 단 하나의 트래픽 클래스만을 서비스하는 단점이 있다.[10]

공정 큐잉(Fair Queuing)은 패킷을 각 트래픽클래스로 분류하고 각 큐에 할당하여 라운드 로빈(Round Robin) 방식으로 한번에 하나의 패킷을 서비스하는방식이다. 이러한 방법은 과도하게 들어오는 패킷이 다른 트래픽 클래스의 대역폭에 영향을 미치지 않는 장점이 있지만 트래픽 클래스마다 같은 대역폭을 할당하기 때문에 트래픽 클래스 마다 다른 대역폭이 요구되는 경우에는 사용될 수 없는 단점이 있다.[11][12] 이러한 단점을 보완하기 위한 방안으로 가중치 사용 공정 큐잉(Weighted Fair Queing)이 있다. 이는 출력 포트 대역폭에 대해 각각다른 비율을 할당하는 가중치를 각 큐에 줌으로써 다른 대역폭을 요구하는 트래픽 클래스를 지원한다.[10] 이러한 방법은 상기와 같이 원하는 트래픽 클래스를 보호하며 동시에 여타 트래픽 클래스의 최소 대역폭을 보장한다. 그러나, 이러한 방법은 많은 양의 트래픽 클래스의 상태와 각 패킷의도착과 출발 상태를 반복적으로 검사 해야 하는 복잡한 알고리즘으로 인하여 하드웨어로의 구현이 거의 불가능하기 때문에 고속의 네트워크 환경에는 부적합하다는 단점이 있다.[13]

상기의 방안에 대하여 가중치 사용 라운드 로빈 큐잉(Weighted Round Robin Queuing) 은 각 트래픽 클래스에 할당되는 대역폭의 비율을 조절할 수 있을 뿐만 아니라 하드웨어로의 구현이 용이하여 고속 처리를 요구하는 네트워크 인터페이스에 적용될 수있으며 실제로 이 방안은 WFHBD 엔진으로 구현되어 있다. [14]

WFHBD 엔진에서는 여러 가지 트래픽 클래스로 분류된 패킷들이 각 트래픽 클래스에 속해 있는큐에 할당되며 각 큐는 라운드 로빈 방식으로 서비스 되어진다. 여기서, 높은 우선순위의 큐들은 서비스 라운드 동안 서비스 될 때마다 하나 이상의 패킷을 전송하며 각 큐들이 서비스 라운드 동안 하나의 패킷만을 전송하게 하고 높은 우선순위의 큐들은 한번의 서비스 라운드 동안 여러 번 서비스 되게 함으로써 서로 다른 트래픽 클래스에 대하여 다른 양의 대역폭을 할당할 수 있다.

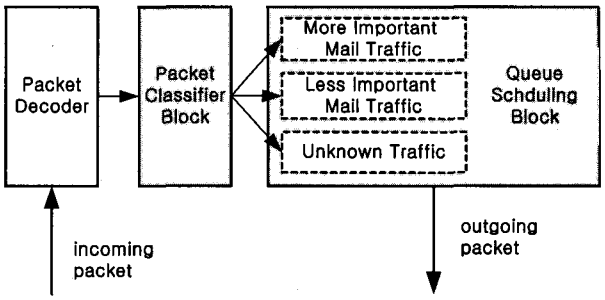


그림 1. 패킷 분류과정
Fig. 1. Packet classification process.

III. 메일 트래픽 보호를 위한 제안 모델

위의 관련 연구에서 보듯이 메일 서버의 트래픽 보호를 위해서는 크게 입력된 메일 트래픽의 분류와 분류된 트래픽에 대한 대역폭의 차등 할당이 필요하다. 이를 위하여 본 연구에서는 고속의 네트워크 환경에서 적용될 수 있는 트래픽 분류 모델과 큐 스케줄링 모델을 제시하였다.

1. 메일 서버를 위한 트래픽 분류

네트워크로 입력되는 트래픽을 클래스 별로 분류하여 이를 스케줄링 하기 위한작업흐름을 기능별로 구분하여 보면 그림 1과 같이 표현할 수 있다. 입력 패킷은 패킷 헤더 분석기(Header Decoder)에 의하여 그 종류가분석되고 패킷 분류기(Packet Classifier)로 전달된다. 패킷 분류기는 패킷 분석기가 제공하는정보를 이용하여 입력 패킷들을 서로 다른 세 개의 트래픽 클래스로 분류하고 분류된 클래스는 가중치 사용 라운드 로빈 큐잉을 위해 큐 스케줄러에 전달된다.

메일 서버로 입력되는 트래픽은 메일을 보내는 시스템의 중요도에따라 중요한 메일 트래픽과 덜 중요한 메일 트래픽, 공격의 가능성이 있는 알 수 없는 트래픽으로 분류된다. 중요한 메일 트래픽과 덜 중요한 메일 트래픽은 사용자의 정의에 따라 메일을 보내는 시스템의 IP 주소에 의해 구분되며 알 수 없는 트래픽은 DDoS 공격의 가능성이 있는 트래픽이다.

패킷 분류기는 3계층 정보(IP 주소)와 4계층 정보(Port)를 조합하여 입력되는 패킷을 상기 세 가지의 클래스로 분류한다. 패킷 분류 과정은 다음과 같다.

표 1에서 보는 바와 같이 입력된 패킷은 3계층 정보를 제공하는 테이블(3계층 그룹 테이블)에 의하여출발지 시스템의 IP에 따라 중요한 사용자 그룹(More Impo-rtant Users)으로부터의 트래픽과 덜 중요한 사용자 그

표 1. 3계층 그룹 테이블
Table 1. Layer 3 Group Table.

Compare Data	Result	비고
IP Addr	L3ID	
192.1.1.1 168.1.2.3 202.30.1.1	L3IDMI	More Important Users
123.2.3.4 301.21.1.5	L3IDLI	Less Important Users

표 2. 4계층 그룹 테이블
Table 2. Layer 4 Group Table.

Compare Data	Result	비고
Port	L4ID	
25(SMTP)	L4IDM	Mail
		Etc.

룹(Less Important Users)으로부터의 트래픽으로 분류된다. 그리고 표2의 4계층 정보를 제공하는 테이블(4계층 그룹 테이블)에 의해 포트(Port) 번호에 따라 TCP 포트번호 25번인 SMTP(Simple Mail Transfer Proto-col) 메일 트래픽과 그 외의 트래픽으로 분류된다. 결과적으로 표 3의 트래픽 클래스 테이블(Traffic Class Table)은 3, 4계층 그룹 테이블의 결과인 L3ID(Layer 3 Identification)와 L4ID(Layer 4 Identification)를 기준으로 위의 세가지 트래픽 클래스로 분류하며 이의 구분자인 TCID(Traffic Class Identification)가 큐 스케줄링 블록으로 전달된다.

2. 메일 서버를 위한 큐 스케줄링

메일 트래픽을 위한 가중치 사용 라운드 로빈 큐 스케줄링은 WFHBD 엔진이 담당한다. 여기에서 트래픽 클래스에 실제적으로 할당되는 대역폭을 계산하기 위하여 다음과 같은 매개 변수를 사용한다. 물리적인 포트의 대역폭($BWport$)이 정의되며, 포트를 통하여 흐르는 트래픽 클래스들의 최소, 최대 대역폭을 설정하기 위하여 각각 최소 대역폭($BW\min$)과 최대 대역폭($BW\max$) 이 정의된다. 그리고 대역폭의 할당에 차등을 두기 위하여 각각에 가중치(W)값을 설정할 수 있다.

하나의 포트에 여러 개의 트래픽 클래스(트래픽 클래스의 수는 N)가 할당되므로 포트의 대역폭보다 하나의 트래픽 클래스의 최대 대역폭이나 각 트래픽 클래스의 최소 대역폭의 합은 작거나 같아야 한다.(수식1)

표 3. 트래픽 클래스 테이블
Table 3. Traffic Class Table.

Compare Data		Result	비고
L3ID	L4ID	TCID	
L3IDMI	L4IDM	TCIDMIM	More Important mail Traffic
L3IDLI	L4IDM	TCIDLIM	Less Important mail Traffic
**	**	TCIDU	Unknown Traffic

**은 정의되지 않은 데이터

$$BWoutport \geq BW\max(i),\ BWoutport \geq \sum_{n=0}^{N-1} BW\min(n) \quad (1)$$

그리고 수식2에서 보는 바와 같이 최소 대역폭들의 합이 포트의 대역폭보다 작을 경우에 한하여 최소 대역폭들을 할당하고 난 후의 남은 대역폭($BWremain$)을 가중치를 기반으로 하여 각 클래스에 추가 할당할 수 있다.

$$BWremain = BWport - \sum_{n=0}^{N-1} BW\min(n) \quad (2)$$

이 때 가중치에 기반을 두고 남은 대역폭을 할당하기 위하여 각 트래픽 클래스의 가중치 비율(Pw)이 계산되어야 하기 때문에 아래 수식3을 이용한다.

$$Pw(i) = \{1/\sum_{n=0}^{N-1}(1/W(n))\}/W(i) \quad (3)$$

수식1, 2, 3을 이용하여 최종적으로 각 트래픽 클래스에 할당되는 실제 대역폭($BWactual$)은 수식4와 같다. 그러나 특정 트래픽 클래스의 실제 대역폭이 최대 대역폭 보다 크다면 실제 대역폭은 최대 대역폭으로 한정되어야 한다.

$$BWactual(i) = BW\min(i) + BWremain \times Pw(i)$$
$$BWactual(i) = BW\max(i),\ if\ BWactual(i) > BW\max(i) \quad (4)$$

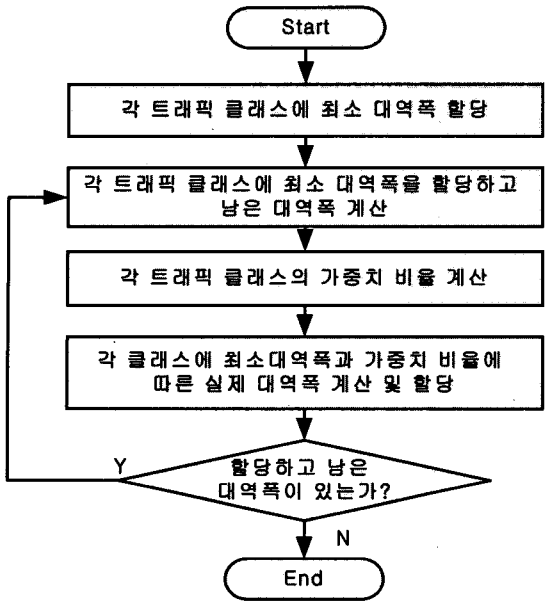


그림 2. WFHBD에서의 대역폭 분산과정
Fig. 2. Bandwidth Distribution Process of WFHBD.

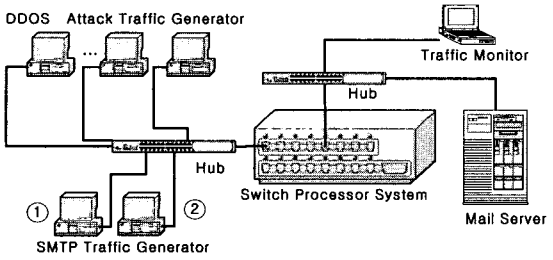


그림 3. 실험환경
Fig. 3. Experimental Environment.

위의 수식과정을 적용하여 WFHBD 엔진에서 트래픽 클래스에 대역폭을 분산 할당하는 과정은 그림 2에 표시되어 있다.

IV. 실험 및 성능평가

1. 실험환경

실험환경은 그림 3과 같이 메일 트래픽 생성기(Traffic Generator)와 DDoS 트래픽 생성기, WFHBD 엔진을 적용한 스위치 프로세서 시스템, 보호되어야 하는 메일 서버, 네트워크 트래픽을 모니터링하기 위한 트래픽 모니터(Traffic monitor)로 구성되어 있으며 100Mbps의 이더넷 환경에서 실험되었다.

스위치 프로세서 시스템은 그림 4와 같이 시스템의 관리를 위한 주 프로세서부(Motorola PowerPC)와 네트워크 패킷을 처리하기 위한 스위치 프로세서부(Switch-core Switch Processor)로 구성되어 있다. 이 시스템에는 네트워크 인터페이스로서 1Gbps 패킷 처리를 위한 2

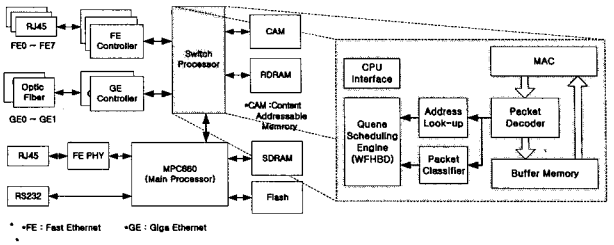


그림 4. 스위치 프로세서 시스템의 구조
Fig. 4. Switch Processor System Architecture.

개의 기가 이더넷(Giga Ethernet;802.3ad) 포트와 100Mbps 패킷 처리를 위한 8개의 고속 이더넷(Fast Ethernet;802.3u) 포트가 있으며 패킷의 버퍼링(Buffe-ring)을 위하여 RDRAM(Rambus DRAM)을, 네트워크 2, 3계층 테이블의 저장과 비교하기 위하여 고속 CAM(Contents Address Memory)을 사용하였다. 그리고 주 프로세서의 프로그램 메모리로서 SDRAM을 사용하였고 운영체제로 리눅스 커널 버전 2.4.14가 사용되었다.

일반적인 프로세서에서는 패킷의 분류 및 필터가소프트웨어적으로 구현되므로 고속의 네트워크 패킷을 처리하기 어렵지만 본 연구에서 사용된 스위치 프로세서는 2, 3, 4 계층에 대한 패킷 분류 및 필터링그리고 전송(Forwarding)을 위한 기능 블록들이 하드웨어에 의하여 구성되어 있고 이들을 프로세서가제공하는 레지스터의 설정에 의하여 큐 스케줄링 알고리즘을 구현함으로써 고속으로 알고리즘을 수행할 수 있다. 스위치 프로세서[15]에는 그림4와 같이 패킷 헤더 분석기와 고속 어드레스 검색기(Address Look-up), 패킷 헤더에 따른 필터링을 수행하는 패킷 분류기, 패킷의 전송 및 QoS(Quality of Service)에 관련된 큐스케줄링을 담당하는 WFHBD 등이 구성되어 있다.

메일 트래픽 생성기로는 Windows 운영체제 기반의 소프트웨어인 Sniffer Pro[16]가 사용되었으며, 그림 3의 ①, ②와 같이중요한 메일을 위한 트래픽과 덜 중요한 메일을 위한 트래픽을 별도로 생성할 수 있도록 하였다.

DDoS 트래픽 생성기로는 Linux 운영체제 기반의 소프트웨어인 Mgen[17]을 사용하였다. Mgen은 UDP 패킷 생성기로서 여러 대의 PC에서 동시에 UDP flooding 공격을 메일서버에 가할 수 있다. 결과적으로 메일 트래픽과 DDoS 트래픽은 스위치 프로세서 시스템을 거쳐 메일서버로 전송되는데 스위치 프로세서 시스템에서는 이들 패킷에 대한 트래픽 클래스 분류와 큐 스케줄링을 설정된 정책에 따라 수행하여 메일 서버를 보호하게 된다.

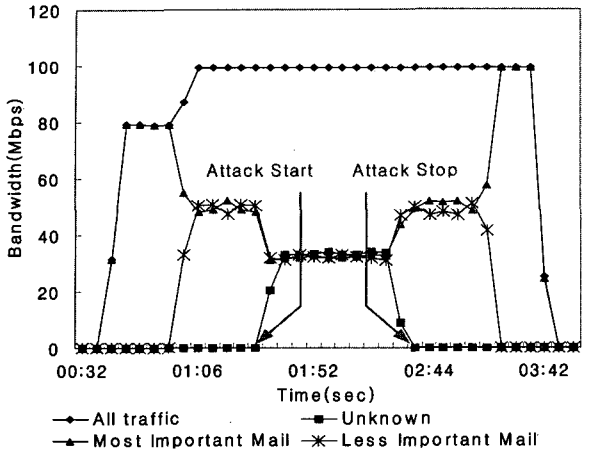


그림 5. FIFO일 경우 트래픽 상황
Fig. 5. Traffic Throughput under FIFO.

2. 실험 결과 및 성능평가

메일 서버보호를 위한 성능을 비교하기 위하여 큐스케줄링 알고리즘을 제외한 모든 조건을 동등하게 설정하고 FIFO(Fist In Fist Out)을 사용한 경우와 WFHBD를 사용한 경우로 구분하여 실험하였다. 또한 WFHBD를 사용한 경우에는 매개 변수인 최소, 최대 대역폭, 가중치를 각각 다르게 설정하여 DDoS 공격으로부터 메일 트래픽의 대역폭이 어느 정도 보호될 수있는지를 실험하였다. 실험에 사용된 모든 패킷의 크기는 이더넷 패킷의 최대 크기인 1518Byte이며, 포트의 대역폭은 100 Mbps 이다. 모든 실험에서는 세가지 트래픽을 간격을 두고 각각80Mbps의 대역폭으로 전송하였으며, 대역폭 경합 시에 트래픽을 모두 합한(All Traffic) 값이 포트의 대역폭보다 큰 상황이 되게 하였다.

1) FIFO를 사용한 경우

스위치 프로세서 시스템에서 FIFO를 적용한 경우 그림 5와 같이 DDoS 공격이 시작된 시점부터 세가지 트래픽 모두 약 33Mbps로 동등하게 낮아진 대역폭 값을 보이고 있다. FIFO의 경우 각 트래픽에 대해 대역폭의 할당에 차등을 둘 수 없고 트래픽의 도착 순서에 따라 처리되므로 DDoS 공격으로부터 중요한 메일 트래픽을 온전히 보호할 수 없었다.

2) 가중치에 영향을 받지 않는 WFHBD를 사용한 경우

이 실험은 스위치 프로세서 시스템에서 WFHBD를 적용한 경우이다. 각 트래픽의 대역폭을 차등 적용할 수 있으므로 표4와 같이 트래픽 클래스마다 다른 최소,최대 대역폭 그리고 가중치를 설정하였다. 그러나 위의 경우

표 4. WFHBD 매개변수 (가중치에 영향을 받지 않음)
Table 4. WFHBD Parameters. (No Weight Effect)

트래픽 종류	최소대역폭	최대대역폭	가중치
More Important mail	50M	50M	16
Less Important mail	30M	30M	32
Unknown	20M	20M	64

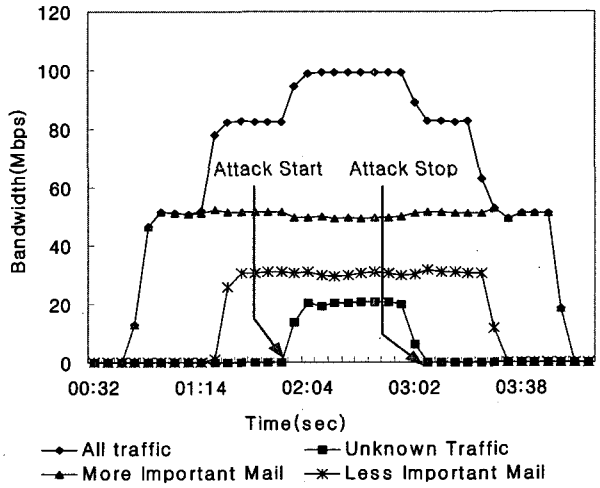


그림 6. WFHBD를 적용시 트래픽 상황
(가중치에 영향을 받지 않음)
Fig. 6. Traffic Throughput under WFHBD.
(No Weight Effect)

각 트래픽클래스의 최소 대역폭의 합이 포트의 대역폭과 같으므로 수식2에 의해 남은 대역폭이 없어서 가중치에 의한 대역폭의 추가 할당이 없게 된다. 결국 각 트래픽 클래스에 할당되는 실제 대역폭은 최소 대역폭과 같다.

이와 경우 그림6과 같이 DDoS공격이 있더라도 각 메일 트래픽은 자신에게 할당된 최소 대역폭인 50Mbps, 30Mbps 만큼은 보장 받고 있어 FIFO의 경우와 비교해 볼 때 메일 서버를 더 효과적으로 보호하기 있음을 알 수 있다. 그러나 중요한 메일 트래픽의 최대 대역폭이 50Mbps로 제한되어 있으므로 공격이 없는 경우에도 실제 전송되어져야 할 대역폭인 80Mbps를 보장받지 못하고 있다.

3) 가중치에 영향을 받는 WFHBD를 사용한 경우

표 5는 표4의 매개변수를 조정한 것으로서 여기에서는 모든 트래픽 클래스들의 최소 대역폭의 합이 포트의 대역폭보다 작으므로 가중치에 의한 대역폭 추가 할당이 가능하다. 위의 경우 수식 3에 의하면 중요한 메일 트래픽, 덜 중요한 메일 트래픽 , 알 수 없는 트래픽이 각각 76% , 19% ,5%로 계산되어 진다. 수식 2, 4를 적

표 5. WFHBD 매개변수 (가중치에 영향 받음)
Table 5. WFHBD Parameters. (Weight Effect)

트래픽 종류	최소대역폭	최대대역폭	가중치
More Important mail	0M	80M	4
Less Important mail	0M	80M	16
Unknown	0M	80M	64

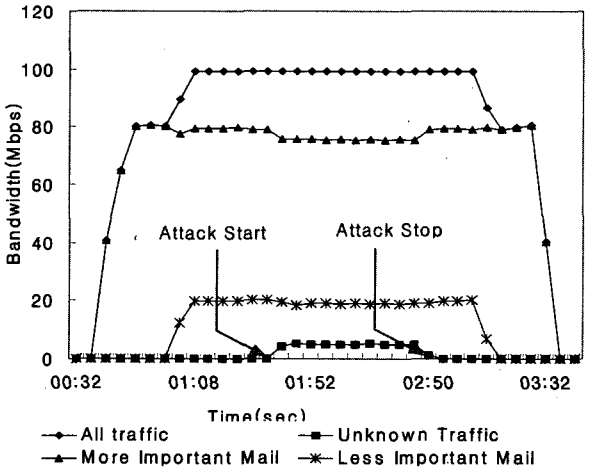


그림 7. WFHBD를 적용시 트래픽 상황 (가중치에 의해 영향 받음)
Fig. 7. Traffic Throughput under WFHBD.(Weight Effect)

용하면 트래픽 클래스 간의 대역폭 경합시 각 트래픽 클래스에 할당되는 실제 대역폭은 각각 76Mbps, 19Mbps, 5Mbps가 된다.

그림 7의 실험결과에 의하면 각 메일 트래픽은 DDoS 공격이 시작된 경우에도 수식에 의하여 계산된 대역폭 만큼을 보장 받고 있으며 특히, 중요한 메일 트래픽의 경우 대역폭의 손실이 거의 없음을 알 수 있다. 또한 2)번 실험에서의 단점인 공격이 없는 경우에서의 중요한 메일 트래픽의 대역폭 손실이 최소화 되었다.

위의 세가지 실험 결과를 종합해 볼 때 2)번 실험의 경우와 같이 낮은 대역폭으로 최대 대역폭이 제한된 경우 DDoS 공격이 없는 경우 FIFO를 적용한 경우보다 대역폭의 할당이 유동적이지 않아 성능이 낮다고 판단될 수 있으나 설정을 3)과 같이 중요하게 보호 되어야 하는 트래픽에 적절히 대역폭의 할당을 하는 경우 우수한 성능을 보이고 있으므로 전체적으로는 WFHBD가 메일 서버를 보호하는데 효과적임을 알 수 있다.

V. 결론 및 향후과제

DDoS 등의 공격을 막기 위한 기존방어 방법들은 패킷 검사에 따른 많은 오버헤드와 대부분 소프트웨어적으로 구현되어 고속의 네트워크 환경에 적합하지 않은 문제점을 가지고 있다. 따라서 본 논문에서는 네트워크 입출력 포트의 대역폭을 트래픽 클래스 간에 분산 할당하는데 유연하며 고속의 네트워크 패킷을 처리할 수 있는 큐 스케줄링 방법을 제공하는 WFHBD 엔진을 사용하는 스위치 프로세서를구현하고 이를 이용하여 메일 서버를 DDoS 공격으로부터 보호하기 위한 방안을 제시하고 그 성능을 실험을 통하여 검증하였다.

트래픽 클래스는 중요한 메일 트래픽과 다소 덜 중요한 메일 트래픽, 공격의 가능성이 있는 알 수 없는 트래픽으로 구분하였으며 실험 결과에서 중요한 메일 트래픽과 다소 덜 중요한 메일 트래픽은 DDoS 공격으로 간주되는 알 수 없는 트래픽과의 대역폭경합시 WFHBD 파라미터의 설정에 따라 대역폭이 보호되는 것을 볼 수 있다.

향후 연구과제로서 좀더 세부적인 기준에 의한 메일 트래픽의 분류와 네트워크 트래픽의 상태를 모니터링하여 큐 스케줄링 파라미터를 동적으로 변화시키기 위한 연구가 필요하다.

참 고 문 헌

[1] 중앙일보, "미디어 리포트-인터넷", http://ad.joins.com/trend /internet-1.asp
[2] Jason Barlow and Woody Thrower, "TFN2K - An Analysis", AXENT Security Team, February 10, 2000.
[3] L. Garber, "Denial-of-Service Attack Rip the Internet", Computer , April , 2000.
[4] 문종욱, 김종수, 임강빈, 정기현, 최경희, "IDS의 성능 향상을 위한 패킷 폐기 방안", 정보처리학회 논문지, 제9-C권 제4호, 2002.06
[5] Switchcore Inc, "Bandwidth Distribution in the CXE Switch", January , pp.10-25 , 2002.
[6] Hyun-Suk Lee, Soojuong Lee, Huisug Jung, Kyunghee Choi, Gihyun Jung, Joongsoon Jang, " Protecting Mail Server using the CBT algorithm", SSGRR Computer & Internet Conference, pp.1-2, July, 2002.
[7] T.Gil and M.Poletto, "MULTOPS: a data-structure for bandwidth attack detection", Vrije Universiteit, Amsterdam, The Netherlands and M.I.T., Cambridge, MA, USA, 2001.
[8] 김주영, 윤상인, 이용학, 이정훈, 전현철, 정현우 공역, "해커스 비웨어", 사이텍 미디어, pp. 208 212, 2002.

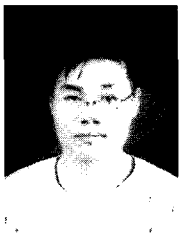
[9] Huitema, Christian, "Routing in the Internet", Prentice Hall PTR, January, 2000.
[10] Kleinrock L., "Queuing Systems", John Wiley & Sons, 1975.
[11] Bennett, J. and Zhang,H. "Hierarchical Packet Fair Queuing Algorithms ", proc. ACM SIGCOMM'96, August 1996.
[12] Demers, A. Keshav, S., and Shenker, S. "Analysis and Simulation of a Fair-queuing Algorithm.", Proc. ACM SIGCOMM'89, 1989.
[13] Chuck Semeria ,"Supporting Differentiated Service Classes : Queue Scheduling Disciplines", Juniper Networks Inc, pp. 4-25, 2002.
[14] Bonaventure, Olivie. "Packet Level Traffic Control Mechanisms", http://enligne.infonet.fundp.ac.be/coursenligne/cours/00-01/INFO2231/INFO2231-2.big/index.htm , 2000.
[15] Switchcore Inc, "CXE-1000 Data Sheet", pp.1-5, May 3, 2002.
[16] Networks Associates Technology, Inc., "Sniffer Pro Getting Started Guide", http://www.sniffer.com
[17] Naval Research Laboratory, "MGEN 3.2 User's Guide", http://manimac.itd.nrl.navy.mil/MGEN/MgenUserGuide.html

저 자 소 개

임 강 빈(정회원)
2001년 아주대학교 전자공학과 (박사)
1999년~2000년 (미)아리조나 주립대 객원연구원
1997년~2002년 아주대학교 전임연구원
2002년~2003년 아주대학교 정보통신대학 대우조교수
2003년~현재 순천향대학교 정보보호학과 전임강사
<주관심분야: 컴퓨터 보안, 실시간 운영체제, 내장형 시스템 등>

김 종 수(정회원)
2000년 아주대학교 전자공학과 (학사)
2002년 아주대학교 전자공학과 (석사)
2002년~2004년 아주대학교 전자공학과 박사과정 수료
2004년 3월~현재 에스넷시스템(주)
<주관심분야: 초고속 통신망, 내장형 시스템, 정보 보안, 실시간 운영체제 등>

정 기 현(정회원)
1984년 서강대학교 전자공학과 (학사)
1988년 Univ. of Illinois, EECS (석사)
1990년 Univ. of Purdue, 전기 전자공학부(박사)
1991년~1992년 현대반도체 연구소
1993년~현재 아주대학교 전자공학부 교수
<주관심분야: 컴퓨터 구조, 멀티미디어 및 실시간 시스템 등>



이 창 희(정회원)
2001년 아주대학교 전자공학과 (학사)
2003년 아주대학교 전자공학과 (석사)
2003년 3월~현재 LG전자 DM연구소 주임연구원
<주관심분야: 내장형 시스템, 실시간 운영체제, 초고속 네트워크 등>

최 경 희(정회원)
1976년 서울대학교 사범대학 수학교육과(학사)
1979년 프랑스 그랑데꼴 ENSEIHT, 정보공학 및 응용수학(석사)
1982년 프랑스 Univ. of Paul Sabatier(박사)
1991년~1991년 프랑스 렌느 IRISA 연구소 교환 교수
1982년~현재 아주대학교 정보 및 컴퓨터 공학부 교수
<주관심분야: 운영체제, 분산 처리, 실시간 시스템 등>