엔터프라이즈 네트워크에서 DDoS 공격의 부하 개선을 위한 큐잉 모델

하현태* · 이해동** · 백현철*** · 김상복****

Queueing Model for Traffic Loading Improvement of DDoS Attacks in Enterprise Networks

Hyeon-tae Ha* · Hae-dong Lee** · Hyun-chul Baek*** · Sang-bok Kim****

요 약

오늘날의 기업은 업무의 신속성을 위하여 인터넷과 인트라넷 등 네트워크를 기반으로 하는 정보운영 방법을 채택하여 사용하고 있다. 그러므로 이와 관련한 기업 내 중요 정보 자산의 보호와 업무의 연속성 보장은 기업의 신뢰도와 직결되어 있다고 할 수 있다. 본 논문은 오늘날 심각하게 대두되고 있는 DDoS 공격으로 인한 업무의 단절 문제를 큐잉 모델을 이용하여 인가된 사용자들에게 연결의 연속성을 보장한다. 이를 위하여 웜/바이러스에 의한 DDoS 공격이 발생하였을 때 관련 트래픽 정보와 패킷 분석을 통하여 과부하 트래픽을 개선하는 과정을 큐잉 모델에 반영하였다. 그리고 실험을 통하여 일반적인 네트워크 장비에 대하여 트래픽의 부하 개선에 대하여 비교 분석하였다.

ABSTRACT

Today the company adopts to use information management method at the network base such as internet, intranet and so on for the speed of business. Therefore the security of information asset protection and continuity of business within company in relation to this is directly connected to the credibility of the company. This paper secures continuity to the certified users using queuing model for the business interruption issue caused by DDoS attack which is faced seriously today. To do this I have reflected overloaded traffic improvement process to the queuing model through the analysis of related traffic information and packet when there occurs DDoS attack with worm/virus. And through experiment I compared and analyzed traffic loading improvement for general network equipment.

키워드

트래픽, DDoS, 큐잉, 포아송

Key word

Traffic, DDoS, Queuing, Poisson

* 준회원 : 경상대학교 컴퓨터과학과
** 정회원 : 경상대학교 컴퓨터과학과
*** 정회원 : 경상남도 진주의료원
**** 정회원 : 경상대학교 컴퓨터과학과 교수 (교신저자, sbkim@gnu.kr)

접수일자 : 2010. 07. 19
심사완료일자 : 2010. 11. 03

Ⅰ. 서 론

엔터프라이즈 네트워크에서는 안정성과 보안성을 위하여 네트워크 이중화나 그룹별 보안을 위하여 VLAN(Virtual LAN)[1]을 사용하고 있다. 아울러 원격지 사용자간에는 VPN(Virtual Private Network)[2]을 구성하고 외부 공격에 대하여 IDS(Intrusion Detection System)와 IPS(Intrusion Prevention System)를 네트워크의 상위에 구축 운영하고 있다. 하지만 이러한 보안 시스템도 내부망의 공격에 대하여 완벽한 대응을 보장해 주지 못하고 있다. 또 대역폭과 관련하여 트래픽이 폭주 할 경우 QoS(Quality of Service) 장비를 이용하여 서비스 품질을 제한하고 있다.

일반적인 네트워크 보안 장비는 DDoS 공격을 포함한 과도한 트래픽 발생 시에 이를 탐지해 내고 트래픽이 발생한 IP 주소를 차단하는 방법을 사용하고 있다. 하지만 엔터프라이즈 네트워크의 경우 인가된 사용자의 네트워크 이용이 트래픽 폭주로 인하여 단절된다면 업무 처리에 필요한 정상적인 서비스를 제공 받을 수 없게 된다. 그러므로 인가된 사용자들의 서비스는 트래픽 폭주가 발생하더라도 무조건 차단보다 문제점이 발생한 부분을 개선하여 정상적인 서비스의 연속성을 제공해 줄 필요가 있다. 본 논문에서는 연결된 클라이언트들 중 트래픽 폭주가 발생한 해당 클라이언트를 무조건 차단하지 않고 지속적으로 서비스가 가능하도록 하였다.

이를 위하여 패킷 분석을 통해 웜/바이러스에 의한 트래픽 폭주인지를 판정하고, 인가된 사용자이면 지속적인 서비스 제공을 할 수 있는 큐잉 모델을 제안하고 구현하였다. 본 논문의 구성은 2장에서는 기존 네트워크 관련 연구, 3장에서는 시스템 구현을 위한 알고리즘을 제안하였다. 그리고 4장에서는 시스템 구현과 실험 그리고 그 결과를 보였으며, 마지막 5장에서는 타 시스템과의 비교 분석한 결과를 결론과 함께 정리하였다.

Ⅱ. 관련연구

2.1 네트워크 트래픽 측정

네트워크 트래픽을 측정하는 방법은 크게 능동적 측정과 수동적 측정 두 가지로 분류 된다[5]. 능동적 측정은 네트워크의 상태를 파악하는 측정 방법이고 수동적 측정은 네트워크의 트래픽 특성을 파악하는 방법이다. 전자의 경우는 측정을 위한 트래픽을 별도로 생성하기 때문에 후자와 대비하여 개인 보안 침해 문제 등을 피할 수 있는 장점이 있다. 그러나 전자의 경우 별도의 트래픽 생성으로 인한 망에 부하를 줄 수 있는 단점을 지니고 있다. 후자의 경우에는 망 자체에 부하를 주지 않으면서 네트워크의 성능을 지속적으로 관측, 분석이 가능하다. 그 결과 네트워크의 부하 발생 정도나 발생 가능한 네트워크의 장애를 예측 할 수 있으므로 사전 대비가 가능하여 전체적인 관리 비용을 줄일 수 있는 이점을 가지고 있다. 어느 방법이 더 우월하다고 할 수는 없지만 주로 외국 벤더들의 경우에는 자사 장비에 수동적 측정법이라 할 수 있는 플로우 기반의 트래픽 측정법[6]을 탑재하고 있는 추세이다. 플로우 기반은 일련의 동일한 특성 - 특정 송신자와 수신자 한 쌍 - 을 갖는 패킷을 모아서 이들을 측정하는 방법을 택하여 사용한다.

2.2 큐잉이론

큐잉이론은 네트워크 디자인에서 사용되는 기반 이론이다. 이는 대기와 처리의 개념이 적용되는 대기행렬 큐라고 할 수 있다.

그림1은 일반적인 큐잉 모델을 나타내고 있다.

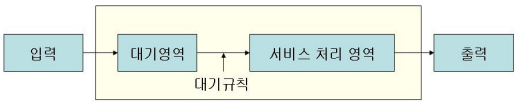

그림 1. 일반적인 큐잉모델
Fig 1. Generally queuing model

큐잉 시스템의 유형은 켄달 기호로 표현 한다. 켄달 기호는 큐잉 유형을 6가지의 기준에 따라 구분한다. 이때 사용하는 기호의 완전한 표현식은 (A/B/C):(K/m/Z)이고 보통 줄여서 앞부분 세자리 형식으로 사용한다. 그 내용은 그림 2와 같다.[7]

Kendall's notation is written as :

A/B/C/K/m/Z	
A	Arrival Process
B	Service Process
C	Number of Servers
K	The size of the queue including any job currently in service
m	The maximum number of customers in the system
Z	Service Discipline - this can include such systems as FIFO(First In, First Out), LIFO(Last In, First Out)

The parameters A and B can take the following values:

Value	Explanation
D	`degenerate'' distribution, or ``deterministic'' service times.
E_k	Erlang Distribution
G	General Distribution
GI	General Independent Distribution
M	Markovian/Random/Exponential Distribution

그림 2. 켄달 기호
Fig 2. Kendall's Notation

켄달 기호는 평형점을 도출하기 위해 수학적 방법을 사용하여 큐잉과 관련한 모델링 시스템을 만들어 내는데 사용한다. 아울러 큐잉 시스템의 수리적 모형을 유도해 내고 시스템의 분석 및 설계를 위해서는 입력 데이터가 큐잉 시스템에 도착하는 방식과 그 데이터가 서비스를 받는데 소요되는 시간을 사전에 파악해야 한다.

2.3 DDoS

분산 서비스 거부 공격은 여러 종류의 공격 방법이 있다. 그 유형은 크게 대역폭에 대한 고갈형과 장비의 자원 고갈형의 두 분류로 나눌 수 있다. 방어를 위한 장비 배치의 방법에는 인라인(in-line) 방식과 아웃오브패스(out-of-path) 방식이 있다. 전자는 네트워크 트래픽의 경로에 탐지 및 방어 장비가 배치되는 방식이고 후자는 트래픽 경로의 외부에서 공격을 탐지해 차단하는 방식이다. 두 가지 방식이 각각 장단점이 있으므로 어느 방식이 월등하다고 할 수 없다. 인라인 방식은 네트워크의 트래픽 특성을 정확히 파악할 수 있는 장점이 있고, 아웃오브패스 방식은 배치 특성상 트래픽 폭주로 인한 장비 다운의 증상이 발생하지 않는다는 것이 가장 큰 장점이다. 방어를 위한 실질적인 기법은 첫째, 학습 행위 기반의 방어 엔진을 구축하는 기법. 둘째, 시그니처 기반의 탐지/방어 기법, 셋째는 자체학습기능 및 탐지/방어인데 이외에도 적용 기법은 여러 가지가 있다. DDoS의 탐지/방어를 위해서는 위에 제시한 방식을 혼용하여 사용하는 경우가 많으며 최근에는 위 세 가지의 탐지/방어의 통합 기법을 사용하는 추세이다.

Ⅲ. 부하개선 관리 시스템의 제안

3.1 관리 시스템 제안

본 논문에서 제안하는 네트워크 트래픽 부하 개선 관리 시스템의 배치 방식은 클라이언트와 서버 사이 즉, 회선상에 위치하는 인라인 방식으로 하였다. 이는 인가된 사용자에 한하여 트래픽 폭주를 탐지/방어하기 때문에 트래픽의 특성을 정확히 파악하는 것이 중요하기 때문이다. 전체적인 구조는 그림 3과 같다.

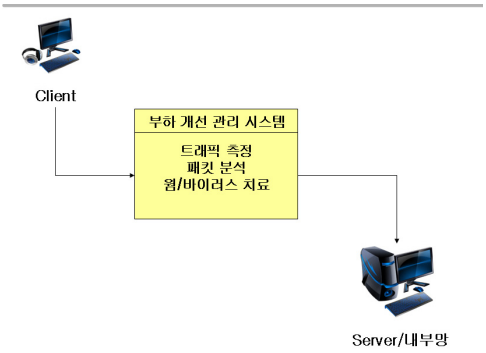

그림 3. 관리시스템 구조
Fig 3. Structure of management system

제안하는 관리시스템으로 진입하기 위한 인가된 사용자 분류 방법은 PDAEN[8]을 이용하고 있다. 이는 트레이스 백을 이용하여 접속자의 IP주소와 관련된 정보를 취득, 관리하며 보유 정보와 취득 정보가 상이한 경우는 일회용 패스워드를 이용하여 인가된 사용자를 인증한다.

그림3의 관리시스템은 인가된 사용자에 한하여 트래픽에 대한 모니터링을 상시 진행하다가 트래픽이 임계

값을 넘어 일정 시간이상 폭주하는 경우 이 트래픽의 정보와 전체 데이터를 큐잉 시스템으로 보내 패킷 분석의 과정을 거친다. 이를 구현하기 위한 알고리즘은 그림 4와 같다. 제안하는 관리시스템과 클라이언트와의 연결 단절을 위한 허용치는 지정한 시간의 값과 큐 대기열 값 사이에 인터섹션으로 지정하였다.

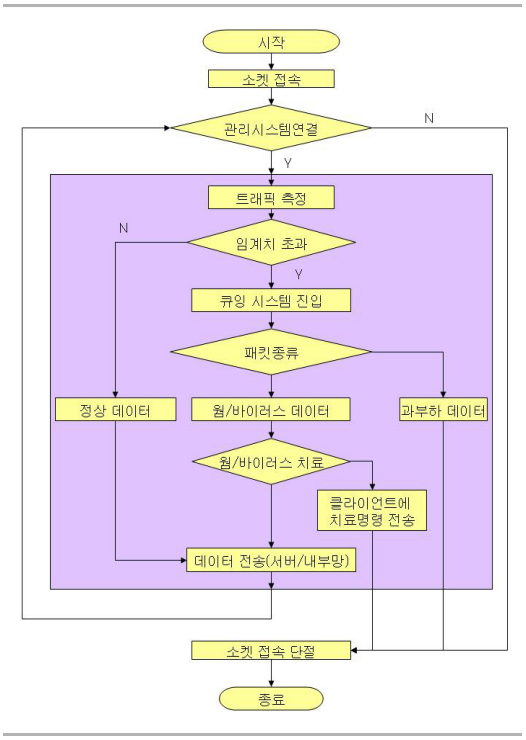

그림 4. 관리시스템 알고리즘
Fig 4. Algorithm of management system

패킷 분석 과정에서 대용량의 트래픽이 발생한 경우에는 연결을 단절하고 알려진 웜/바이러스의 패턴을 가지고 있는 데이터로 분석이 될 경우 이의 연결을 단절하지 않고 웜/바이러스의 치료를 통해 서비스의 연속성과 트래픽의 안정성을 보장해 주는 방법을 선택하고 있다.

본 관리시스템에서 트래픽의 측정 방법은 수동적 측정 방법을 선택한다. 연결된 클라이언트는 IP 주소 별로 각각 소켓통신을 하고 이 과정에서 개별 큐를 하나씩 생성한다. 이 큐들의 용도는 입력되는 트래픽의 부하량을 측정한 뒤 이상 데이터라는 판정이 내려지면 큐에 있는 내용을 추출하여 큐잉 시스템으로 보낸다. 큐잉 시스템으로 입력된 패킷은 분석을 통하여 두 가지로 분류된다. 즉 웜/바이러스 정보를 포함하고 있는 경우와 일반적인 데이터 트래픽이 폭주를 하는 경우이다. 본 논문에서 일반적 과부하 데이터는 분석 대상이 아니므로 큐잉 시스템의 대기열에서 대기하다가 허용치를 초과하면 과부하 데이터의 연결을 끊는다. DDoS 공격은 여러 종류의 트래픽을 생성해서 공격을 시도하는데 그 중 해당 피해 시스템을 좀비PC로 만들기 위해 웜/바이러스 본체를 전달하는 트래픽이 유발되는데[9] 이를 발견하여서 큐잉 시스템으로 데이터와 트래픽의 정보를 보낸다. 큐잉 시스템에서 데이터의 웜/바이러스 검사를 수행하여 이를 치료하고 치료가 불가능한 경우에는 데이터를 폐기하고 클라이언트 측에 감염 데이터 치료를 위한 정보를 알려주고 연결을 종료한다.

3.2 큐잉 시스템의 분석

제안한 알고리즘의 큐잉 시스템 관리를 위한 분석에 사용되는 파라미터는 다음과 같다.

- λ=입력 트래픽의 도착율
- Ts=큐잉시스템의 서비스시간
- ρ=서비스 이용율
- r=큐잉시스템 안의 패킷 갯수
- Tr=시스템 안에 있는 시간

큐잉시스템에는 트래픽이 폭주할 경우 서비스 이용률과 패킷 대기가 일어나는 대기열 큐 사이에 트레이드 오프가 발생한다. 이는 큐의 디자인과 분석시 고려해야 되는 사항이다. 아울러 우리가 알 수 있는 값은 λ, Ts, 시스템의 개수이다. 시뮬레이션에서 입력되는 패킷은 지수분포의 특성을 따르고 큐잉시스템에 대한 분포는 포아송 분포의 특성을 가진다[10]. 이는 발생하는 사상이 독립적이고, 이론적으로 특정 구간에서 관찰 대상 사건이 무한히 많이 발생 할 수 있으며, 주어진 구간에서 특정 사건이 단 한번 일어날 확률의 해당 구간은 길이에 비례하기 때문이다.

본 시뮬레이션에서는 시스템이 안정 상태에 있을 때 캡처한 패킷들 중 무작위로 표본 추출한 10초간의 패킷을 이용하여 분석하였다. 추출한 입력 패킷의 개수는 2778개였으며 이 조건으로 평균 도착율 λ값의 유도를

위한 식은 다음과 같으며

$$\lambda = \frac{Traffic_{input}}{Second} \quad (1)$$

연속적인 입력 트래픽 사이의 대기 시간은 지수 분포의 형식을 가지므로 이의 평균과 분산을 유도하기 위한 식은 다음과 같게 된다.

$$E(T) = \frac{1}{\lambda}, var(T) = \frac{1}{\lambda^2} \quad (2)$$

식 (1)과 식(2)로 유도 할 수 있는 결과 값은 λ = 277.8을 가지게 되고, E(T) ≒ 0.0035997, var(T) ≒ 1.2957926e-5 를 가진다.

위의 λ값을 가지고 t시간 동안에 입력되는 패킷의 수를 유도하는 식은 다음과 같다.

$$P\{X(t)= x\}= \frac{(\lambda t)^x e^{-\lambda t}}{x!}, \; x = 0,1,2,... \quad (3)$$

위 식의 분산과 편차는 다음과 같다.

$$E(X(t))= \lambda t, \quad Var(X(t))= \lambda t \quad (4)$$

이 식들을 이용하여 단위 시간당 도착되는 패킷의 수에 대한 확률 분포를 구할 수 있게 된다.

그리고 패킷의 평균 도착율이 지수분포의 형태를 가지는 λ이므로 x시간동안 가능한 패킷 도착확률은 포아송 분포를 가지게 되는데 이는 식3에서 유도되어 다음과 같이 표기할 수 있다.

$$P(x)= \frac{\lambda^x e^{-\lambda}}{x!}, x = 0,1,2,... \quad (5)$$

서비스 처리율을 구하려면 서비스 시간은 지수분포를 따르게 되므로 다음의 확률변수 식을 사용할 수 있다.

μ : 평균서비스율 (6)

$\frac{1}{\mu}$: 패킷당 평균 서비스 시간

$$P(t_1 \le T \le t_2) = \int_{t_1}^{t_2} \mu e^{-\mu x} dx = e^{-\mu t_1} - e^{-\mu t_2}$$

네트워크에서 도착하는 패킷과 패킷 사이의 시간은 지수분포를 따르며 서비스 시간도 역시 지수분포를 따른다. 그림2 켄달 기호 중에서 M/M/1을 사용가능하다. 여기에서 1은 큐잉시스템의 개수를 나타내고 있다.

본 시뮬레이션에는 패킷이 평균 277.8/sec로 큐잉시스템으로 도착하고, 패킷의 평균 길이는 54옥텟이며 네트워크의 라인 스피드는 100Mbps이다. 이 패킷이 처리되어 나갈 때까지의 시간의 계산을 위한 식은 다음과 같다.

$$\rho = \lambda Ts \quad (7)$$

이를 전제로 패킷이 큐잉 시스템에 머무르는 시간의 식은

$$Tr = \frac{Ts}{1-\rho} \quad (8)$$

대기열에 머무르는 패킷을 포함하여 평균적으로 머무르는 패킷의 수를 구하는 식은 다음과 같이 나타난다.

$$r = \frac{\rho}{1-\rho} \quad (9)$$

이상의 분석을 토대로 큐잉시스템의 개수를 예측 할 수 있으며 Tr값이 λ값을 넘어설 경우 큐잉 시스템을 추가하여 부하 분산 처리할 수 있다.

Ⅳ. 실험 및 분석

4.1 실험

본 논문에서 제안한 알고리즘의 수행을 위해 트래픽의 생성 프로그램과 부하 개선 관리 시스템은 Visual Studio 2008에서 C++(MFC)를 이용하여 구현하였고, 패킷 캡처를 위해서 WireShark를 이용하였다. 실험 트래픽의 생성을 담당하는 클라이언트 측은 정상데이터와 웜/바이러스와 같은 이상 트래픽, 대용량 데이터를 전송하는 트래픽을 생성할 수 있도록 하였다. 그리고 엔터프라이즈 네트워크의 특성상 통신을 위한 포트는 한정되므로 공격을 위한 포트는 임의로 지정하여 분석 하였다. 관리 시스템에서는 이들 각각의 클라이언트간 연결이 완료되면 ip주소와 전송 트래픽 값을 나타내는 접속자의

개별 정보를 표시한다. 차트를 분석하는 방법은 오른쪽에서 왼쪽으로 시간의 경과에 따라 관찰하였다. 실험을 위한 트래픽의 서비스 제한 값은 클라이언트당 1024KB/sec로 지정하였다. 시뮬레이션을 위하여 그림 1에서 제시한 단방향 구조로 트래픽이 흐르게 하고 관리 시스템에서 클라이언트로 보내는 패킷의 양은 논문의 특성상 예외로 한다.

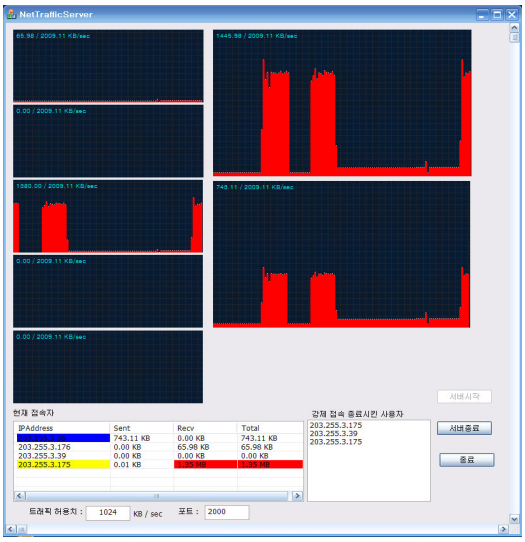

그림 5. 관리시스템의 공격트래픽치료
Fig 5. Treatment of the attack traffic in management system

그림 5에서 왼쪽의 차트는 접속된 클라이언트의 입력 트래픽 정보를 나타내는 화면이고 오른쪽 위의 차트는 입력트래픽, 아래는 출력 트래픽들의 전체 상태를 나타내고 있다. 그림 5 왼쪽의 세 번째 차트는 연결된 인가 사용자의 트래픽을 나타내고 있는 화면인데 일정 시점부터 트래픽이 폭주하는 상태를 나타낸다. 오른쪽의 전체 입력 트래픽을 보면 1445.98KB/sec 인데 출력 트래픽은 743.11KB/sec 를 나타내고 있다. 이 실험은 이상 트래픽의 패킷 분석을 통해서 알려진 패턴을 가지는 웜/바이러스의 치료 과정을 거친 후에 데이터를 목적지로 전송하는 것을 나타내고 있는 것이다. 클라이언트에서 전송되는 데이터는 웜/바이러스가 치료되면 정상적으로 서버/내부망으로 진입하게 되므로 측정한 트래픽 값은 일반적인 데이터 전송값 이하로는 떨어지지 않는다. 그리고 공격 패턴을 가지는 트래픽은 입력되는 패킷에 대한 치료를 수행하더라도 계속 클라이언트 측으로부터 지속적인 이상 데이터의 전송이 임계값 이상 입력될 경우에는 클라이언트 측에 공격 트래픽의 치료를 요하는 정보를 전송하고 연결을 단절한다. 만약 클라이언트에서 치료의 과정을 거치면 연결 단절 없이 인가된 정상 사용자와 동일한 서비스를 제공한다. 일반적인 네트워크 환경하에서 인가된 사용자들은 서로 상이한 대역폭을 점유하는 프로그램을 사용할 수 있다. 이런 경우 QoS를 통하여 사용자별 트래픽 제한을 할 수 있다. 이 부분은 많은 장비가 구현 되어 있는 분야이므로 본 시뮬레이션에서는 지정된 시간을 초과해서 과도한 트래픽이 발생한다면 연결을 단절 시켰다.

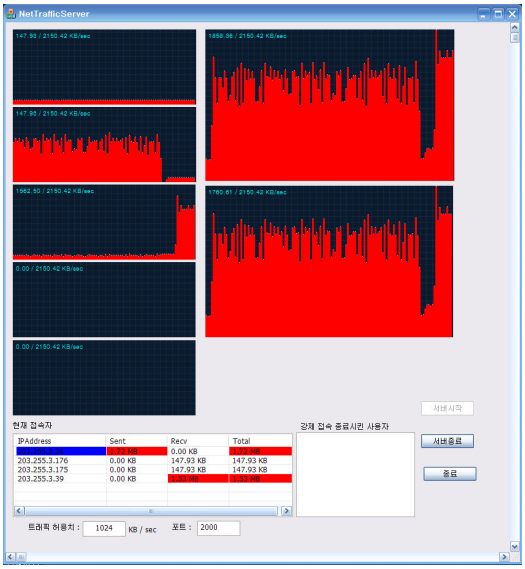

그림 6. 대용량 트래픽 폭주 실험
Fig 6. Experimental of large traffic

그림 6은 연결이 단절되는 상황을 나타내는 차트이다. 그림 오른쪽의 전체 입출력 트래픽을 보면 입력트래픽의 총합은 1858.96KB/sec를 나타내고 있고 출력 트래픽의 총합은 1760.61KB/sec를 나타내고 있다. 이 실험에서는 연결된 클라이언트의 트래픽의 허용치를 15초간 지속적으로 초과하는 경우에만 연결의 단절을 나타내고 그렇지 않은 경우에는 연결의 단절 없이 네트워크의 사용을 유지할 수 있도록 하였다.

그림 6의 왼쪽 두 번째 차트는 대용량 트래픽의 측정값이 지정 시간동안 지속적으로 1024KB/sec를 초과하

지 않아 연결의 단절 없이 서비스를 하였으며 이후는 임의로 전송 데이터를 바꾸어서 진행하였다. 세 번째 차트에서는 차트의 폴이 폭발적 증가가 발생한 시점부터 15초간의 트래픽을 측정하였다. 제안하는 관리시스템은 허용치가 초과될 경우 연결을 단절한다. 이때의 정보를 클라이언트측에 제공하게 되는데 이 결과는 그림 7과 같다.

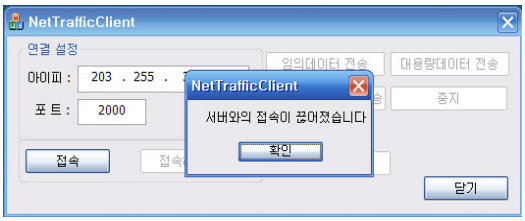

그림 7. 클라이언트 연결 단절
Fig 7. Client disconnection

V. 결론 및 향후 과제

본 논문은 웜/바이러스에 의한 과도한 트래픽 유발시 이를 개선하는 방법에 대한 큐잉모델을 제안하였다. 이를 통하여 일반적으로 사용하는 차단우선 정책보다 트래픽의 상태 개선을 통하여 지속적인 서비스를 유지 할 수 있도록 하였다. 본 시뮬레이션에서 이상 현상이 발생하기 전에는 패킷 분석 없이 통과하는 트래픽 값만 측정한다. 그러므로 이상 패킷의 탐지를 위해 패킷헤더 전부를 검색하는 방식에 비해 시스템 자체 부하는 적게 걸리고 비용의 감소 효과가 있다. 또한 기존 탐지 기법에 비하여 시스템에 대한 통계적 특성을 분석하므로 탐지의 정확도를 높일 수 있고 상황 변화에 따른 효율적인 대응이 쉽다. 본 논문에서 향후 추가로 연구해야 할 부분은 현재의 인라인 배치방식을 아웃오브패스 방식으로 변경하는 방법이다. 더불어 엔터프라이즈 네트워크에서 트래픽 값의 중요한 파라미터중 하나인 시간대별 트래픽 양의 제한 값을 적용한 관리시스템에 대한 지속적인 연구가 필요하다 할 수 있다.

참고문헌

[1] David Passmore, John Freeman, "The Virtual LAN Technology Report," http://www.3com.com/nsc/200374.html.

[2] Farkhod Alisherov, Nayoun Kim, Eun-suk Cho, Seok-soo Kim, "Penetration testing a VPN," 한국정보기술학회 2009년도 Green IT융합기술 워크숍 및 하계 종합 학술 대회 논문집 2009.6, pp. 903~905 (3pages)

[3] 신동진, 양해술, "유출트래픽 분석기반의 침입탐지 시스템 설계 및 구현," 한국정보기술학회논문지 제1권 제1호 2003.3, pp. 55~63(9pages).

[4] 왕정석, 권희웅, 정윤재, 곽후근, 정규식, "시그너처 해싱에 기반한 고성능 침입방지 시스템," 한국정보과학회 2007 한국컴퓨터종합학술대회 논문집 제34권 제1호(D) 2007.6, pp. 489~494(6pages).

[5] 김진규, 이순흠, "능동적 성능 측정 시스템의 구현," 한국콘텐츠학회논문지 제9권 제4호 2009.4, pp. 131~141(11pages).

[6] 김종원, 신현준, 이정일, 최일준, 오창석, "Flow 기반 점유율과 상관성 분석을 통한 유해 트래픽 탐지," 한국정보기술학회논문지, 제7권 제3호 2009.6, pp. 201~209(9pages).

[7] Naranker Dulay, "Stochastic Modelling of Manufacturing Systems," Dr. Naranker Dulay's Homepage(http://www.doc.ic.ac.uk/~nd/surprise_97/journal/vol4/wll1/main.htm).

[8] Yun-Ji Ma, Hyun-Chul Baek, Chang-Geun Kim, Sang-Bok Kim, "Prevention of DDoS Attacks for Enterprise Network Based on Traceback and Network Traffic Analysis," International Journal of Maritime Information and Communication Sciences, v.7, no.2, 2009.6, pp.157-163.

[9] 최양서, 오진태, 장종수, 류재철, "분산서비스거부(DDoS) 공격 통합 대응체계 연구," 정보보호학회지, 제19권 제5호 2009.10, pp. 11~20(10pages).

[10] 김종순, 이상석, 김신중, 윤석민, 곽수환, "엑셀을 활용한 통계학의 이해(제2판)," 도서출판청람 2008.3.5, pp. 141~144(4pages).

저자소개

하현태(Hyeon-Tae Ha)

2008년 한국국제대학교
컴퓨터공학과(공학사)
2011년 현재 경상대학교
컴퓨터과학과(석사과정)

※관심분야 : 네트워크, 네트워크보안

이해동(Hae-Dong Lee)

2009년 경상대학교 컴퓨터과학과
(공학석사)
2011년 현재 경상대학교
컴퓨터과학과 (박사과정)

2011년 현재 (주)이지시스 대표이사
※관심분야 : 네트워크, 네트워크보안

백현철(Hyun-Chul Baek)

1998년 경상대학교 컴퓨터과학과
(교육학석사)
2003년 경상대학교 컴퓨터과학과
(공학박사)

2007년 전국지방의료원 전산기술위원장
2011년 현재 경상남도진주의료원 전산실장
※관심분야 : 네트워크, 네트워크보안

김상복(Sang-Bok Kim)

1989년 중앙대학교 전자공학과
(공학박사)
1984년～현재 : 경상대학교
컴퓨터과학과 교수

2000년～현재 : 경상대학교 컴퓨터정보통신연구소
연구원
2007년～2010년 : 경상대학교 교육정보전산원장
※관심분야 : 멀티미디어 통신, 컴퓨터네트워크,
컴퓨터구조