고속 엔터프라이즈 네트워크에서 성능 저하 특성 규명

종신회원 주 홍 택*, 준회원 홍 성 철**, 종신회원 홍 원 기**

On the Performance Degradation Characteristics of High-Speed Enterprise Network

Hong-Taek Ju* *Lifelong Member*, Seong-Cheol Hong** *Associate Member*,
James W. Hong** *Lifelong Member*

요 약

기업이나 대학 등 대규모 기관들은 고속 네트워크를 구축하여 운영하고 있다. 이와 같은 고속 엔터프라이즈 네트워크 내에서 네트워크 이용률(utilization)이 저조함에도 불구하고 종단간 성능은 네트워크 속도에 비하여 상당히 저조하다. 이러한 원인은 특정 장비에서 아주 작은 시간에 트래픽이 폭주하는 미세폭주(micro-congestion)가 발생하기 때문이다. 미세폭주는 패킷손실(Packet Loss)나 지연(Delay), 패킷역전(Packet Reordering)을 발생시키고 이것이 성능 저하의 원인이 된다. 본 논문에서는 미세폭주를 발생하는 시점을 검출하는 방법과 미세폭주를 검출한 시점에 트래픽을 수집하여 패킷손실, 지연, 패킷역전과 트래픽의 특성과의 상관관계 분석하여 성능저하를 발생시키는 미세폭주의 특성을 규명한다.

Key Words : Microcongestion, Network Utilization, Packet Loss, Packet Reordering

ABSTRACT

ISPs and Enterprises are equipping their networks with sufficiently high speed facilities and provide large bandwidths members. However the high speed enterprise network does not have satisfying end-to-end network performance within the network in spite of under utilization. The root cause of this performance degradation is a micro-congestion, which is a short-live event of traffic congestion. A micro-congestion causes packet loss, delay and packet reodering, and finally results in end-to-end network performance degradation. In this paper, we propose a micro-congestion detection method and find out the characteristics of performance degradation by analyzing traffic archives which is collected from a network link when a micro-congestion occurs.

Ⅰ. 서 론

기업이나 대학, 대규모 공공기관들은 고속의 네트워크를 구축하고 있다. 이들 단체들은 구성원의 업무처리에 네트워크가 방해가 되지 않도록 1Gbps에서 10Gbps까지 충분한 대역폭을 가지는 엔터프라이즈 네트워크를 구축하여 제공하고 있다. 또한 구축된 고속 네트워크를 충분히 활용하기 위하여 VoIP, 멀티미디어 스트리밍, 화상회의 등 네트워크 성능에 민감한 서비스 (QoS Sensitive Services)를 도입하여 활용하고 있다.

네트워크를 고속화하여 구성원들에게 충분한 대역폭을 제공하고 있지만 네트워크 성능에 민감한 서비스가 원활히 제공되지 못하고 있다. 뿐만 아니라 단대단 성능도 네트워크의 성능을 충분히 이용하지 못하고 있다. 예를 들면, 시스템 성능요소를

※ 이 논문은 2007년 정부(교육과학기술부)의 재원으로 한국학술진흥재단의 지원을 받아 수행된 연구임(KRF-2007-013-D00087)
* 계명대학교 컴퓨터공학과 (juht@kmu.ac.kr), **포항공과대학교 컴퓨터공학과
논문번호 : KICS2009-09-393, 접수일자 : 2009년 9월 7일, 최종논문접수일자 : 2009년 11월 2일

제외하고 네트워크 성능만 고려할 때 1Gbps의 백본과 100Mbps의 종단 연결을 가지는 두 컴퓨터 사이의 파일전송이 1분이 넘지 않아야 하지만 실제로는 보통 5분이상이 소요되고 있다. 트래픽이 많아서 엔터프라이즈 네트워크의 성능을 충분히 활용 못하는 것은 아니다. 일반적으로 엔터프라이즈 네트워크에서 대역폭 사용율(Utilization)을 측정해 보면 40%를 넘지 않으므로 트래픽이 많은 것은 아니다. 사용율이 낮은 네트워크에서 네트워크 성능을 충분히 이용하지 못한다는 것은 역설적이다.

이 역설은 사용율 측정과 사건의 발생의 시간단위 불일치에 기인한다. 네트워크 사용율은 일반적으로 5분, 시, 일단위의 사용율을 측정하고 있다. 반면 기업 네트워크의 성능을 저하시키는 미세폭주(micro-congestion)는 수 밀리초(millisecond) 동안 지속되는 사건이다. 즉 네트워크 사용율을 측정하는 시간단위가 긴 것에 반하여 종단간 성능을 저하시키는 미세폭주의 지속시간이 아주 작기 때문에 이러한 역설이 나오게 된 것이다.

미세폭주에 대한 이전의 연구들은 미세폭주가 발생함을 사용율 측정과 패킷손실을 측정으로 증명하였다[5],[10]. 또한 미세폭주를 수학적으로 규명을 하거나[3],[8],[9] 가능성 있는 몇가지 원인을 상정한 후 이들 중 어떤 것이 미세폭주의 주요 원인인지를 규명하였다[1]-[2].

본 논문에서는 미세폭주 발생을 검출하고 검출된 미세폭주 시점에 트래픽을 수집하는 방법을 제시한다. 또한 수집된 트패릭을 분석하여 미세폭주에 의한 패킷 손실(Packet Loss), 패킷순서역전(Packet Reodering)과 트래픽 특성이 어떤관계인지 규명하였다. 예를 들면 긴 지속시간을 갖는 TCP 플로우의 수와 미세폭주에 의한 패킷손실과의 관계를 제시하였다.

논문의 구성은 서론에 이어서 2장에서는 관련연구를 제시하였다. 3장에서는 미세폭주 검출 방법과 미세폭주 시점에 트래픽을 수집하는 방법에 대하여 설명하였다. 4장에서는 수집된 트래픽을 분석하여 미세폭주에 의한 네트워크의 성능을 평가하였다. 마지막으로 5장은 본 논문의 결론과 향후 연구방향을 제시하였다.

Ⅱ. 관련연구

POSTECH에서는 네트워크 이용률이 낮은 엔터프라이즈 네트워크에서 미세폭주에 의한 패킷손실이 발생함을 보여주었다[6]-[7]. SNMP를 이용하여 라우터와 스위치로 부터 네트워크 사용율과 패킷손실을 측정하였다. 이 연구에서는 네트워크 이용률이 낮음에도 불구하고 패킷 손실이 발생하고 있고, SNMP 데이터 수집 시간을 최소화 하여도 작은 시간에 발생한 미세폭주를 검출할 수 없었다. 단지 미세폭주가 SNMP 데이터 수집 주기 사이에 발생한 것은 분명하나 이의 지속시간이나 원인을 알 수 없었다.

Papagiannaki는 미세폭주가 백본 네트워크에서 떨어진 액세스 라우터에서 주로 발생한다고 설명하였다[1]. 이들은 미세폭주의 근본적인 이유로써 다음과 같이 3가지를 제시하였다. 첫째는 고속의 코어 네트워크 링크의 트래픽이 저속의 액세스 네트워크 링크로 전달될때 대역폭의 감소이고 둘째는 여러개의 다른 링크의 트래픽이 하나의 링크로 몰리는 트래픽 집중, 셋째는 하나의 링크에서 과다한 트래픽이 유입되는 것이다. 이 연구에서는 이 3가지 원인 중에서 어떤한 것이 주요 원인인지를 밝히기 위하여 대기행렬 모델(queuing model)을 적용하여 알아보았다. 이들은 또 다른 연구에서 미국 스프린트(Sprint)사의 IP 백본 네트워크에서의 미세폭주현상의 특성에 대한 연구를 수행하였다[2]. 이 연구에서는 미세폭주의 발생을 측정하기 위해 다양한 시간 스케일로 링크 이용률을 분석하였다. 그러나 트래픽 집중(burst)에 대해서는 탐지를 한 반면 트래픽과의 연관성을 제시하고 있지 않다. 즉 이들 연구는 네트워크 장치의 동작에서 미세폭주의 원인을 알아 보았다. 우리는 미세폭주와 트래픽의 특성과의 관계에 중점을 두고 있는 것이 두 연구의 차이점이다.

Hohn은 하나의 라우터의 모든 입출력 링크를 모니터링하여 폭주현상의 규모와 시간적 구조에 대하여 연구하였다[3]. 그러나 이 연구에서 사용된 모델은 유용한 전달지연 정보를 얻을 수 있지만 패킷손실이나 미세폭주에 대한 언급은 되지 않았다. 또한 Hohn은 Tier-1 액세스 라우터에서 모든 IP 패킷을 캡쳐하여 라우터 혼잡(congestion)과 패킷 지연에 관해 상세히 분석하였다[4]. 이 연구에서 미세폭주(micro-congestion) 행위가 빈번하게 발생하고 있음을 보여주는데, 이용률(utilization)에 기반한 접근이 기본적으로 잘못되었음을 설명하고 있다. Mochalski는 네트워크의 여러 지점에서 TAP을 사용하여 트래픽 모니터링을 수행하고 트래픽 패턴의 변화를 분석하였다[5]. 라우터와 방화벽에서 발생하는 지연시간을 측정하고, 이러한 긴 지연시간이 라우터에서의 미세폭주 및 패킷손실과 연관되어 있다고 밝혔다.

Ⅲ. 미세폭주 검출과 트래픽 수집

본 장에서는 미세폭주 발생을 검출하고 검출된 미세폭주 시점에 트래픽 수집방법을 설명한다. 네트워크 구성도와 모니터링 지점에 대하여 기술한 후, 모니터링 시스템의 구조를 보여주고 모니터링 시스템의 성능을 증명한다. 마지막으로 이를 이용하여 미세폭주 검출 및 트래픽 수집을 어떻게 해야 하는지 설명한다.

본 논문에서 제시하는 실험은 실제 운영 중인 포스텍(POSTECH) 네트워크에서 실시되었다. 그림 1은 미세폭주 검출 및 트래픽 수집을 위한 네트워크 구성도와 모니터링 지점을 보여주고 있다. 모니터링 지점은 인터넷 구간과 분배 스위치, 액세스 스위치 구간을 선정하였다.

이 구간을 모니터링 지점으로 선정한 이유는 인터넷 구간 트래픽 수집을 통해 전체 네트워크의 현황을 파악할 수 있고, 기존 연구 결과를 바탕으로 했을 때 분배 스위치와 액세스 스위치 구간에서 미세폭주의 발생 가능성이 크기 때문이다[1]. 또한, 동시에 여러 지점에서 트래픽을 수집하여 두 지점 사이에서 발생된 트래픽의 변화를 파악하여 미세폭주에 대한 분석에 활용하였다.

미세폭주 검출 및 트래픽 수집을 위한 모니터링 시스템의 구조는 그림 2와 같다.

우선 네트워크 라우터로부터 SNMP 폴링을 통해

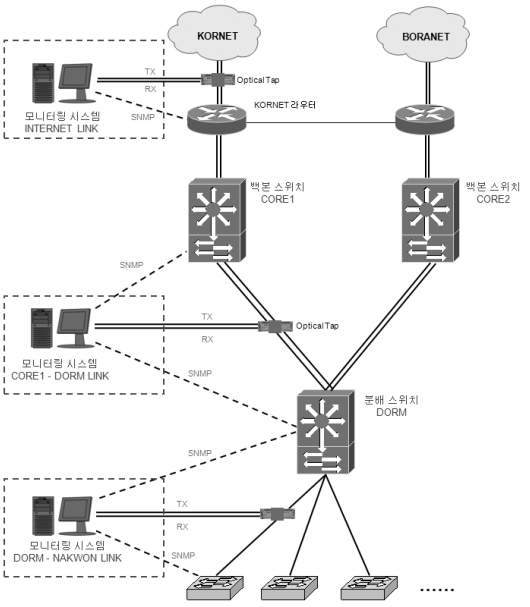


그림 1. 네트워크 구성도

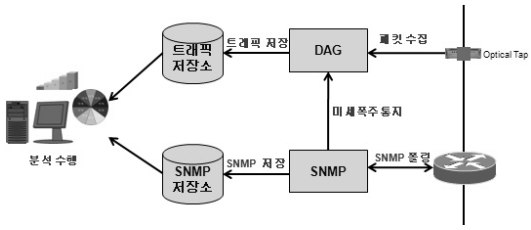


그림 2. 모니터링 시스템 구조

미세폭주가 발생하는지를 주기적으로 모니터링 한다. 수집된 SNMP 데이터는 MRTG와 유사한 시간 스케일에 따른 통계 정보로 변환되어 SNMP 저장소에 보관된다. 미세폭주 검출 시에는 수집된 패킷과 관련지어 미세폭주가 트래픽 특성과 어떤 관계인지를 분석한다.

트래픽 패킷 수집은 광학분리기(Optical Tap)와 DAG[11] 카드를 사용하였다. 광학분리기는 전체네트워크에 영향을 주지 않으면서 트래픽 수집을 할 수 있고, DAG 카드는 일반 네트워크 카드보다 대용량의 트래픽 수집이 가능하다. 또한 수집은 상향과 하향 트래픽을 모두 수집하였고, 각 패킷마다 헤더를 포함하여 94 바이트를 저장하였다. 94 바이트는 TCP 헤더까지의 54 바이트와 TCP 데이터 40 바이트를 포함한 것이다. TCP 데이터 40 바이트는 TCP 응용 프로토콜이 무엇인지 분석을 위한 것이다.

미세폭주 검출을 위해서는 SNMP 데이터의 수집 주기가 중요하다. 미세폭주의 발생시간을 정확히 파악할수록 좀 더 정확한 분석이 가능하기 때문이다. SNMP 폴링 주기는 원하는 대로 작게 할 수는 없다. 왜냐하면 네트워크 장치에서 SNMP MIB 값을 실시간으로 갱신하지 않고 보통 1초 이상의 시간 간격을 가지고 갱신하기 때문이다. 따라서 SNMP MIB 폴링 주기를 짧게 하였을 때 검출된 값의 신뢰성에 대한 분석이 이루어져야 한다. 이를 위해 백본 스위치 CORE1에 대하여 SNMP GET 요청을 1초마다 수행하였을 때 InOctets 값의 변화를 그림 3에 보여준다. 이 그래프를 근거로 백본 스위치

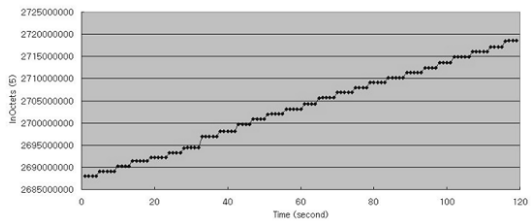


그림 3. 백본 스위치 CORE1의 MIB 갱신 주기

CORE1의 MIB 갱신 주기는 4~5초 임을 알 수 있다. 같은 실험을 통해 분배 스위치 DORM의 경우는 8~9초로 나타났다. 따라서 SNMP 폴링 주기는 장비의 성능과 밀접하게 관련하여 지정하여야 함을 알 수 있다.

다음으로 패킷을 수집하기 위한 DAG 카드의 성능을 검증하였다. 미세폭주 발생 시 정확한 패킷 수집시간 기록과 함께 손실되는 패킷이 없이 수집할 수 있는지 여부는 대단히 중요하다. 그림 4는 패킷 생성기 SmartBit를 이용하여 패킷 크기를 변경해가면서 1Gbps의 트래픽을 발생시켰을 때 DAG 카드의 패킷 수집 성능을 그래프로 보여준다. 패킷손실이 발생하지 않는 패킷의 크기는 475Byte 이상으로 475Byte 때의 초당 패킷 수는 약 280,000pps이다. 그림 1에서 보여준 네트워크 링크에서의 트래픽 양을 고려하였을 때 최대 폭주에서도 손실 없이 패킷을 수집할 충분한 성능을 제공하고 있다.

앞서 언급한 바와 같이 SNMP 표준 MIB으로는 네트워크 장치에서 패킷손실을 알 수 없다. 우리는 패킷손실 정보를 얻기 위해 Cisco 엔터프라이즈 MIB을 사용하였다[12]-[13]. 패킷손실 정보를 제공하는 MIB 변수는 locIfInputQueueDrops와 locIfOutputQueueDrops이다. 라우터의 모든 인터페이스는 입력 큐와 출력 큐를 각각 가지고 있는데 큐가 꽉 차게 되는 경우 발생되는 패킷손실 수를 해당 MIB 변수에 기록한다. 큐가 꽉 찼다는 것은 패킷이 갑자기 몰림으로써 라우팅 프로세서가 처리할 수 있는 한도를 넘었다는 의미이다. 따라서 이러한 미세폭주로 인해 발생되는 패킷손실이 네트워크 성능, 특히 TCP 같이 패킷손실에 민감한 프로토콜에 많은 영향을 주게 된다.

모니터링 시스템은 앞서 설명한 SNMP MIB 변수를 주기적으로 폴링하여 패킷손실 여부를 감지하여 미세폭주 발생 여부를 판단한다. 만약 미세폭주가 발생하게 되면 이를 DAG 모듈에 알린다. DAG 모듈은 들어오는 모든 패킷을 계속 저장하는 것이 이상적이지만, 대용량 링크를 모니터링 하는 경우 저장 공간의 한계 때문에 현실적으로 불가능하다. 따라서 미세폭주에 대한 분석에 활용될 수 있을 만큼의 윈도우를 두어 오래된 데이터를 삭제하고 새로운 데이터를 기록하는 방식으로 저장소를 관리한다. 본 연구에서는 윈도우의 크기를 24시간으로 지정하고 1시간 단위로 트래픽을 기록하였다. 단, DAG 모듈이 SNMP 모듈로부터 미세폭주 통지를 받았을 경우에는 오래된 데이터도 계속 유지하면서, SNMP 모듈이 미세폭주라고 통지해 주는 시점 이후의 데이터도 계속해서 저장을 수행한다. 이는 추후 미세폭주와 관련된 네트워크 성능 분석에 활용된다.

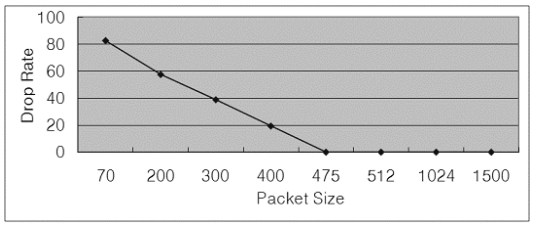


그림 4. 패킷 크기에 따른 패킷 손실

Ⅳ. 트래픽 분석과 성능 평가

트래픽 모니터링 시스템은 4개월 동안 구동하였고 통상적으로 2~3일에 한 번씩 수집된 데이터를 분석하였다. 네트워크의 상태를 전반적으로 파악하기 위해, SNMP를 이용하여 각 네트워크 장치의 패킷손실과 이용률을 분석하였다. 실제로 이용률이 저조함에도 패킷손실이 발생하는지 여부를 확인하였다. 앞서 언급한 바와 같이 이용률을 계산하기 위하여 스위치의 각 인터페이스마다 송수신된 데이터 양은 SNMP 표준 MIB변수로 제공된다(예: ifInOctets). 하지만 각 인터페이스의 패킷손실은 표준 MIB 변수로는 제공되지 않아서 장치 제조사 마다 다른 비표준 MIB 변수를 활용하였다(예 Cisco의 locaIIfInputQueueDrops).

대부분의 네트워크 링크에서 사용율은 저조하였으며 여러 장치 중에서 분배 스위치 DORM에서 패킷손실이 발생하였고 10000초(약3시간) 구간의 SNMP 데이터를 10초 단위로 폴링하여 수집하고 분석하였다. 모니터링 대상이 되는 DORM 분배 스위치의 각 인터페이스의 유입, 유출 트래픽의 사용율과 각 인터페이스의 패킷손실을 측정하여 분석한 결과 모니터링 대상이 되는 DORM과 NAKWON 링크의 이용률은 평균 1.7%이었고 DORM과 CORE1 링크의 이용률은 평균 26.5%이었다. 이렇게 충분히 낮은 이용률에도 불구하고 DORM과 NAKWON 사이 링크는 DORM 스위치로 유입되는 인터페이스에서 10초당 최대 135개, 총 464개(약 3시간동안)의 패킷손실이 있었다. 이때 DORM과 CORE1 스위치 사이에는 패킷손실이 없었다. 또한 NAKWON 스위치와 DORM 스위치 사이의 링크에 패킷손실이 없는 경우에 대하여 분석해 보면 이때 DORM 스위치

에서 DORM과 CORE1 스위치 사이의 링크에서 유출 패킷손실이 있었다. 이전의 Papagiannaki 연구[1]에서 제시한 3가지 원인 중에서 DORM 스위치를 기준으로 트래픽 과다에 의한 미세폭주는 NAKWON 스위치와 연결된 인터페이스에서 발생하고 대역폭 축소나 트래픽 몰림에 의한 미세폭주는 전체 인터페이스에서 골고루 발생함을 유추할 수 있다.

구내연결 트래픽과 외부연결 트래픽을 분리하여 분석하였다. 구내연결 트래픽은 교내 시스템 간의 발생한 트래픽이고 외부연결 트래픽은 교내 시스템과 학교 외부 시스템간에 발생한 트래픽이다. 분석결과 NAKWON 스위치에서 발생하는 트래픽 중에서 구내연결이 평균 0.351Mbps이고 최대가 0.926 Mbps이었으며 외부연결이 평균 11.837Mbps이고 최대가 31.785Mbps이었다. 또한 표 1에서 보는 바와 같이 1일 동안의 총 트래픽에서도 내부연결이 2.823%이고 외부연결 트래픽이 97.177%이다. 대부분의 엑세스 스위치에서 발생하는 트래픽은 외부연결 트래픽이며 미세폭주의 원인도 외부연결 트래픽에 의한 것임을 알 수 있다.

DORM 스위치와 NAKWON 스위치 사이의 IP 트래픽을 TCP, UDP와 그 외로 나누었다. 표 1은 1일 동안 수집된 모든 패킷을 분석하여 IP 구성을 표로 나타낸 것이다. TCP 트래픽이 전체의 99% (96.7+2.8)이고 UDP 트래픽이 작은 부분을 차지하며 그 외 트래픽은 아주 미미하다. 따라서 미세폭주의 원인이 TCP 트래픽과 관련 있을 것이라 추측되며 이후 분석도 TCP에 초점을 맞추고 있다.

TCP 트래픽과 패킷손실과의 관계를 알아보기 위하여 TCP 트래픽의 시간적 분포에 패킷손실을 표시하였다. 그림 5은 하루 동안의 TCP 트래픽의 분포이고 원으로 표시한 부분이 패킷손실이 발생한 시점이다.

그림 5에서 몇 개의 피크가 보이며 2개의 패킷손실 시점과 일치한다. 그러나 모든 피크에서 패킷손실이 발생한 것이 아니므로 트래픽 폭주가 원인이 될 가능성만 제시할 뿐이다. 큰 파일 전송에 TCP가

표 1. 트래픽의 내외부 및 IP 구성

내외부연결	TCP	UDP	그 외	총계
내부연결	26,384 (2.8%)	221 (0.02%)	28 (0.003%)	26,633 (2.823%)
외부연결	891,082 (96.7%)	3,665 (0.39%)	111 (0.01%)	894,858 (97.177%)

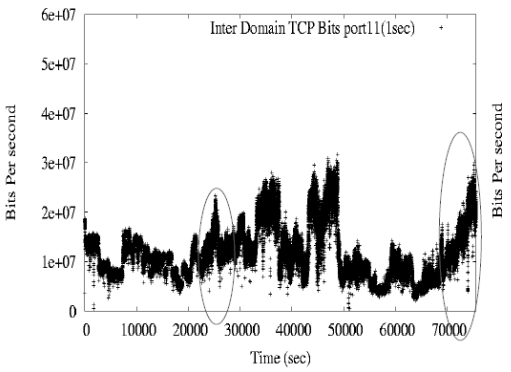


그림 5. TCP 트래픽 양과 패킷손실

사용되면 TCP의 슬로우 스타트(slow start) 알고리즘 때문에 혼잡이 발생하고 미세폭주의 원인이 될 수 있다. TCP 뿐만 아니라 UDP, ICMP(그 외 트래픽의 대부분을 차지함)에 대하여도 동일한 분석을 실시하였으나 TCP에 비하여 그 양이 현저히 적어서 패킷손실과의 특별한 관계가 없는 것으로 판명되었다. 바이러스나 봇에 의하여 발생하는 폭주 트래픽이 일반적으로 IP가 아닌 경우가 많고 또 브로드캐스팅 트래픽일 경우가 많이 있다. 이러한 트래픽은 스위치의 자원을 많이 사용하는 트래픽으로서 스위치에 상당한 부하를 준다. 따라서 IP가 아닌 트래픽도 하루 동안의 트래픽 양과 패킷손실과의 관계를 분석하였다. 분석결과는 ARP가 대부분을 차지하였고 ARP 중에서 ARP REQ가 ARP REP보다 폭주 경향이 있고 MAC 레이어의 브로드캐스팅 패킷이기 때문에 스위치에 부하를 줄 가능성이 있다. 하지만 그 양이 초당 200개를 넘지 않아서 미세폭주를 발생시킨다고 볼 수 없고 시간적인 분포에서도 관련이 없었다.

앞의 분석에서 TCP 트래픽이 전체 트래픽의 99%이상임을 알았으므로 TCP 트래픽에 대하여 세밀한 분석을 실시하였다. 분석은 DORM 스위치와 NAKWON 스위치 사이의 링크에서 수집한 트래픽으로서 DORM 스위치 인터페이스의 인입 큐(Input Queue)에서 패킷손실이 발생할 때 저장된 것이다. 저장된 TCP 패킷정보를 기반으로 TCP 플로우의 플로우 수, 지속시간, 크기와 같은 특성에 대한 패킷손실과의 관계를 분석하였다. 하나의 TCP 플로우는 일정시간 내에서 발신지 주소, 목적지 주소, 발신지 포트번호, 목적지 포트번호가 동일한 송수신 패킷의 묶음이다.

패킷손실이 발생한 구간에서 10msec 단위로 TCP

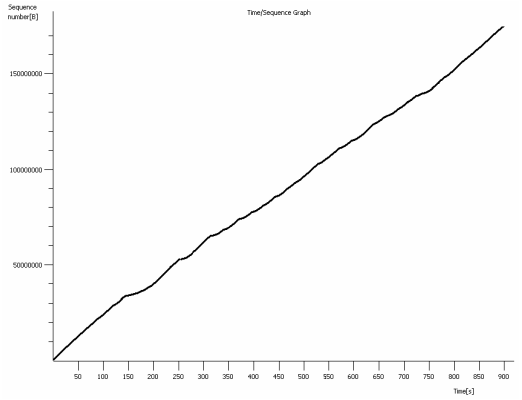


그림 6. 큰 TCP 플로우의 순서번호 시간분포

플로우 수 분포를 분석하였다. 약간의 피크는 보였지만 그러한 피크가 미세폭주 시점이라고 단정할 정도로 특징을 발견할 수 없었다. 또한 TCP 플로우의 플로우당 바이트 크기에 대하여도 동일한 분석을 실시하였으나 역시 특별한 특징을 발견할 수 없었고 단지 이 구간에서 TCP 트래픽이 적은 수의 플로우로 많은 데이터를 보내는 특징(heavy-tail)이 유지됨을 알 수 있었다. 더욱이, 새로 생성되는 TCP 플로우의 수에 대하여 시간적 분포를 분석하였으나 이 결과도 특별한 특징을 발견할 수 없었다. TCP 플로우의 수, 데이터 양, 새로 생성된 플로우의 수와는 미세폭주가 관련이 없는 것으로 분석되었다.

미세폭주의 존재나 영향을 알아보기 위해서 긴 지속시간을 갖으며 많은 데이터를 보내는 TCP 플로우에 대한 분석을 실시하였다. 이러한 TCP 플로우를 큰 TCP 플로우라고 규정하였고 이러한 큰 플로우에 대하여 관심을 갖는 이유는 미세폭주 의한 효과가 큰 TCP 플로우에 반영되기 때문이다. 즉 큰 TCP 플로우를 분석하면 미세폭주가 플로우에 어떤 영향을 미치는지 알 수 있다.

우선 전체 플로우에 대하여 데이터의 양으로 CDF(Cumulative Distribution Function) 그래프를 생성하였다. 이 분석의 결과 10개의 큰 플로우가 전체 트래픽의 50%를 차지하고 50개의 큰 플로우가 80%를 차지함을 알 수 있었다. 세밀한 분석을 위하여 지속시간과 데이터 양을 모두 고려하여 몇 개의 큰 TCP 플로우를 선택하여 분석하였다. HTTP는 선택하여 분석하기에 부적절하다. 왜냐하면 HTTP는 하나의 TCP로 여러 개의 독립적인 파일을 전송(HTTP 1.1 Persistent Connection)하므로 긴 지

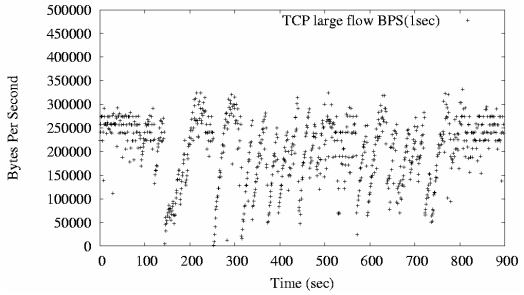


그림 7. 큰 TCP 플로우의 데이터 양 시간분포

속시간을 가지면서도 적은 데이터를 보내는 경우가 많다. 15분이상의 지속시간을 가지면서도 패킷사이의 시간간격이 10msec 이하이고 평균 패킷크기가 1000byte 이상인 10개의 플로우를 선택하여 분석하였다.

10개 플로우들은 비슷한 결과를 나타내었고 그림 6과 7은 이 중에서 한 개의 플로우에 대한 TCP 순서번호(Sequence Number)와 데이터양의 분포를 나타내고 있다.

큰 플로우의 순서번호에 의하면 이 플로우는 중단 없이 계속적으로 데이터를 보내고 있음을 알 수 있다. 또한 순서번호가 계단식으로 증가하는 곳을 볼 수 있다. 패킷손실이 없을 때 큰 플로우에서는 이러한 계단식 증가를 볼 수 없었다. 또한 데이터양의 분포에서 처리되는 양의 변화가 심하게 나타난다. 이것은 미세폭주의 영향으로 판단된다.

큰 플로우의 순서번호 그래프에서 계단식 증가가 있고 데이터양이 급격히 감소되는 구간을 미세폭주가 발생한 시점으로 판정하여 이 구간에 대하여 시간간격을 줄여 밀리초(msec) 단위의 세밀한 분석을 하였다. 그림 8은 미세폭주 시점에서의 50초 동안의 큰 플로우의 데이터 양의 분포를 나타내며 그림 9는 미세폭주가 없는 플로우에 대한 데이터 양 분

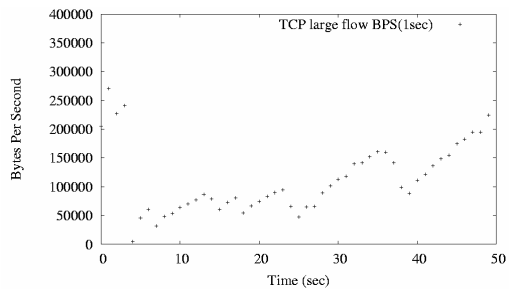


그림 8. 미세폭주가 있을 때 TCP 플로우 데이터 양

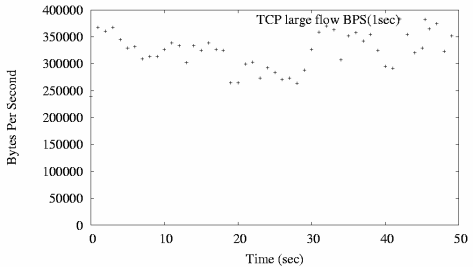


그림 9. 미세폭주가 없을 때 TCP 플로우 데이터 양

포를 나타낸다.

미세폭주가 있을 때와 없을 때 TCP 플로우의 데이터양을 보면 미세폭주 시에 톱니바퀴형태의 데이터 처리양이 확실히 나타남을 알 수 있다. 그러나 이 분석으로 미세폭주의 지속시간을 알 수는 없다. 톱니바퀴형태의 피크가 미세폭주에 의한 영향으로 볼 수 있지만 이 후에 미세폭주가 지속되는지는 알 수 없기 때문이다. 큰 플로우 몇 개를 동일한 분석을 한 결과 톱니바퀴형태의 서로 연관성을 찾을 수 없어서 더욱이 미세폭주의 지속시간을 계산할 수 없었다. 추가적으로 미세폭주가 발생한 시간에 TCP 재전송 패킷의 수와 SNMP의 패킷손실 수와 관계를 분석하였다. 이론적 추정과 맞게 TCP 재전송 패킷이 나타나는 시점과 톱니바퀴형태의 시간이 일치하였으며 초단위의 SNMP 패킷손실 수와도 일치하였다.

네트워크 성능에 영향을 주는 다른 요소로 패킷 순서역전(Packet Reordering)을 들 수 있다. TCP 세션의 순서 번호를(sequence number)를 기준으로 패킷이 보내진 순서를 알 수 있으며, 두 모니터링 지점에서 수집된 같은 TCP 세션에 대하여 순서 번호가 앞뒤로 서로 역전된 것을 통해 패킷순서역전을 알 수 있다. 미세폭주가 발생하고 두 지점사이의 경로가 하나 이상이라서 우회경로가 있으면 패킷순서역전으로 나타난다. 예를 들면 실험 네트워크 구성에서 DORM 스위치는 미세폭주가 NAKWON 링크에서 발생하면 우회경로인 CORE2로 패킷을 우회시킬 수 있고 따라서 패킷순서역전이 나타나게 된다.

패킷순서역전 분석에 사용된 모니터링 지점은 INTERNET LINK와 CORE1-DORM LINK이고, 패킷수가 100개 이상인 TCP 세션에 대하여 분석을 하였다. 패킷순서역전은 일반적으로 패킷을 분석하여 처리하는 IPS(Intrusion Prevention System)이나 TS(Traffic Shapper)에서 많이 발생시킨다고 알려져

표 2. 패킷순서역전 세션 비율

트래픽 방향	IPS, TS 참여 여부	
	O	X
상향 트래픽	79.41%	71.21%
하향 트래픽	83.12%	79.67%

있다. 우선 INTERNET LINK 구간에 있는 IPS와 TS가 패킷순서역전을 유발시키는지 알기 위하여 두 모니터링 지점 사이에 인터넷 장비가 있는 경우와 없는 경우를 비교하였다. 표 2는 대상이 되는 전체 세션에 대하여 패킷순서역전이 발생한 세션의 비율을 보여주고 있다. 표 2에서 볼 수 있듯이 이러한 인터넷 장비들은 패킷순서역전에 영향을 주지 않음을 알 수 있다.

결국 엔터프라이즈 네트워크 내에서 네트워크 이중화로 인한 경로 우회에서 미세폭주가 발생하면 패킷순서역전이 발생한다고 볼 수 있다. 초당 패킷수와 패킷순서역전과의 분석에서 패킷 수가 많아지면 패킷 간의 시간 간격이 짧은 TCP 플로우에서 패킷순서역전이 발견되었다.

V. 결론 및 향후 연구

본 논문에서는 이용률이 낮는 엔터프라이즈 네트워크의 성능 저하 원인인 미세폭주와 트래픽과의 관계를 규명하였다. 미세폭주가 유발하는 패킷손실과 패킷순서역전을 검출하고 이 시점에 트래픽을 수집하여 미세폭주와 트래픽의 관계를 분석하였다. 미세폭주 시점을 검출하는 방법도 제시하였다.

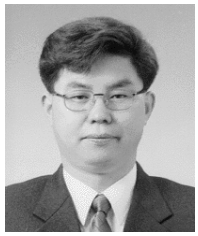
향후 미세폭주의 지속시간이나 발생빈도를 알아보는 연구가 필요하다. 본 논문에서는 미세폭주가 발생한 것은 확실하나 정확한 시점과 지속시간 등을 알아내지 못하였다. 또한 이 논문에서는 트래픽의 특성과 미세폭주 사이의 관계를 분석하였는데 트래픽과 스위치의 동작, 예를 들면 큐의 길이, 등과 각 인터페이스 트래픽과의 관계를 분석하여 종합적으로 미세폭주의 원인 및 네트워크에 미치는 영향을 분석하는 연구가 필요하다.

참 고 문 헌

〔1〕 Konstantina Papagiannaki, Darryl Veitch and Nicolas Hohn, “Origins of Microcongestion in an Access Router,” Passive & Active Measurement Workshop, Antibes, France,

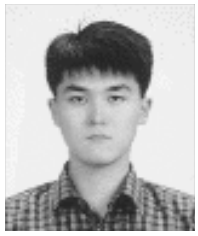
April, 2004.
〔2〕 Konstantina Papagiannaki, Rene Cruz and Christophe Diot, "Network Performance Monitoring at Small Time Scales," Internet Measurement Conference, Miami, Florida, USA, October, 2003.
〔3〕 Nicolas Hohn, Dattyl Veitch, Konstantina Papagiannaki and Christophe Diot, "Bridging Router Performance and Queuing Theory," ACM SIGMETRICS, New York, USA, 2004.
〔4〕 Nicolas Hohn, Konstantina Papagiannaki and Darryl Veitch, "Capturing router congestion and delay," IEEE/ACM Transactions on Networking, Volume 17, Issue 3, June, 2009, pp.789-802.
〔5〕 Klaus Mochalski, Jorg Micheel and Stephen Donnelly, "Packet Delay and Loss at the Auckland Internet Access Path," Passive and Active Measurement Workshop, Fort Collins, Colorado, USA, March, 2002.
〔6〕 Seung-Hwa Chung, Deepali Agrawal, Myung-Sup Kim, James W. Hong and Kihong Park, "Analysis of Bursty Packet Loss Characteristics on Underutilized Links Using SNMP," E2EMON, San Diego, California, USA, October, 2004.
〔7〕 Seung-Hwa Chung, Young J. Won, Deepali Agrawal, Seong-Cheol Hong, James W. Hong, Hong-Taek Ju and Kihong Park, "Detection and Analysis of Packet Loss on Underutilized Enterprise Networks," E2EMON, Nice, France, May, 2005.
〔8〕 Zhi-Li Zhang, Vinay J. Ribeiro, Sue Moon and Christophe Diot, "Small-Time Scaling Behaviors of Internet Backbone Traffic: An Empirical Study," INFOCOM, San Francisco, USA, March, 2003.
〔9〕 Wenyo Jiang and Henning Schulzrinne, "Modeling of Packet Loss and Delay and Their Effect on Real-Time Multimedia Service Quality," ACM NOSSDAV, Chapel Hill, North Carolina, June, 2000.
〔10〕 Velibor Markovski, Fei Xue and Ljiljana Trajkovic, "Simulation and Analysis of Packet Loss using User Datagram Protocol," The Journal of Supercomputing, Kluwer, Vol.20, No.2, pp.175-196, September, 2001.
〔11〕 Endace, DAG 4.3GE card, User Manual, EDM01.02-01.
〔12〕 Cisco, "MIB compilers and Loading MIBs," Cisco Technical NOtes, http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a00800b4cee.shtml.
〔13〕 Cisco, "Input Queue Overflow on an Interface," Cisco Technical Notes, http://www.cisco.com/en/US/products/hw/modules/ps2643/products_tech_note09186a0080094a8c.shtml.

주 홍 택 (Hong-Taek Ju) 종신회원



1989년 8월 한국과학기술원 전산학 학사
1991년 8월 포항공과대학교 컴퓨터공학 석사
2002년 2월 포항공과대학교 컴퓨터공학 박사
1991년 9월~1997년 2월 대우통신, 종합연구소, 선임연구원
2002년 9월~현재 계명대학교 컴퓨터공학과 부교수
<관심분야> Web-based Network Management, Network Monitoring, Mobile Device Management

홍 성 철 (Seong-Cheol Hong) 준회원



2003년 포항공과대학교, 컴퓨터학과 학사
2003년~현재 포항공과대학교, 컴퓨터공학과 석박사통합과정
<관심분야> 인터넷 트래픽 모니터링 및 분석, 네트워크 보안, 네트워크 관리 및 관리 시스템

홍 원 기 (Won-Ki Hong) 종신회원

1983년 Univ. of Western Ontario, BSc in Computer Science
1985년 Univ. of Western Ontario, MS in Computer Science
1985년~1986년 Univ. of Western Ontario, Lecturer
1986년~1991년 Univ. of Wasterloo, PhD in Computer Science
1991년~1992년 Univ. of Wasterloo, Post-Doc fellow
1992년~1995년 Univ. of Western Ontario, 연구교수
1995년~현재 포항공과대학교 컴퓨터공학과 교수
2005년~2009년 IEEE ComSoc CNOM Chair
2009년~현재 포항공과대학교 정보전자융합공학부 교수
<관심분야> 네트워크 트래픽 모니터링, 네트워크 및 시스템 관리, Network Security