논문 13-38B-07-03

한국통신학회논문지 '13-07 Vol.38B No.07
http://dx.doi.org/10.7840/kics.2013.38B.7.519

응용 트래픽의 지역성을 이용한 페이로드 시그니쳐 기반 트래픽 분석 시스템의 성능 향상

박 준 상◆, 윤 성 호*, 김 명 섭°

Performance Improvement of the Payload Signature based Traffic Classification System Using Application Traffic Locality

Jun-Sang Park◆, Sung-Ho Yoon*, Myung-Sup Kim°

요 약

응용 레벨 트래픽 분류는 안정적인 네트워크 운영과 자원 관리를 위해서 필수적으로 요구된다. 트래픽분류에 있어서 페이로드 시그니쳐 기반 응용 레벨 트래픽 분류 방법은 고속 링크의 트래픽을 실시간으로 처리하는 과정에서 헤더 정보 및 통계 정보 이용 방법론에 비해 상대적으로 높은 부하를 발생시키며 처리 속도가 느린 단점을 갖는다. 본 논문에서는 페이로드 시그니쳐 기반 트래픽 분류 시스템의 처리 속도를 향상 위하여 응용 트래픽의 지역성을 이용한 서버 IP, Port캐쉬 기반 트래픽 분석 시스템을 제안한다. 제안하는 방법을 학내 망의 실제 트래픽에 적용하여 최대 10배 이상의 처리 속도 향상과 10% 이상의 플로우 분석률을 향상 시킬 수 있었다.

Key Words : payload signature, Internet traffic identification, cache

ABSTRACT

The traffic classification is a preliminary and essential step for stable network service provision and efficient network resource management. However, the payload signature-based method has a significant drawback in high-speed network environment that the processing speed is much slower than other method such as header-based and statistical methods. In this paper, We propose the server IP, Port cache-based traffic classification method using application traffic locality to improve the processing speed of traffic classification. The suggested method achieved about 10 folds improvement in processing speed and 10% improvement in completeness over the payload-based classification system.

Ⅰ. 서 론

네트워크의 고속화와 더불어 다양한 서비스와 응용프로그램이 개발됨에 따라 기업이나 개인들은 인터넷으로 대표되는 네트워크에 대한 의존이 상당히 커져가고 있다. 이와 같은 현실 속에서 네트워크의 효율적 운용과 관리를 위한 응용 레벨의 트래픽의 모니터링과 분석은 네트워크 사용현황 파악과 확장 계획 수립 등의 다양한 분야에서 필요성이 커져가고 있다. 예를 들어 종량제 과금, CRM, SLA, 보안 분석 등 트래픽 모니터링 및 분석에 대한 필요성은 지금뿐만 아니라 앞으로 더욱더 크게 증가할 것이

※ 이 논문은 정부(교육과학기술부)의 재원으로 2010년도 한국연구재단-차세대정보컴퓨팅기술개발사업(20100020728) 및 2012년도 한국연구재단(2012R1A1A2007483)의 지원을 받아 수행된 연구임.
◆ 주저자 : 고려대학교 컴퓨터정보학과 네트워크 관리 연구실, junsang_park@korea.ac.kr, 학생회원
° 교신저자 : 고려대학교 컴퓨터정보학과 네트워크 관리 연구실, tmskim@korea.ac.kr, 종신회원
* 고려대학교 컴퓨터정보학과 네트워크 관리 연구실, sungho_yoon@korea.ac.kr, 학생회원
논문번호 : KICS2013-03-127, 접수일자 : 2013년 3월 7일, 최종논문접수일자 : 2013년 6월 25일

다. 이를 위해서는 다양한 종류의 응용 레벨 트래픽을 정확하게 분류할 수 있는 방법과 고속 링크에서 발생하는 대용량의 트래픽을 실시간으로 처리하는 방법이 요구된다.

응용 레벨 트래픽 분류 방법에 있어 페이로드 시그니쳐 기반 분석 방법은 패킷의 헤더 정보나 통계 정보를 이용하는 다른 분석 방법들에 비해 상대적으로 높은 분류 정확성과 분석률을 보인다[1,2]. 하지만 분류 시스템의 처리 속도에 있어 현재의 고속 네트워크 상에서 발생하는 대용량 트래픽을 실시간으로 처리하기에 부적합한 방법이다. 응용의 수와 대용량의 트래픽을 발생시키는 응용의 사용이 증가하고 있는 추세를 고려했을 때 페이로드 기반 분석 방법의 처리 속도 문제는 반드시 해결되어야 하는 과제이다. 이를 해결하기 위해 기존의 다양한 연구에서는 패턴 매칭 알고리즘의 성능 개선 기법에 대한 연구가 주를 이룬다[4-7]. 하지만 매칭 알고리즘의 성능 개선은 제한적이며 현재의 고속 링크의 대용량 트래픽을 수용할 수 없는 것이 현실이다.

본 논문에서 응용 트래픽의 발생 특징을 분석 시스템에 반영하여 트래픽 분류 시스템의 성능을 향상 시킬 수 있는 방법을 제안한다. 분석 대상 네트워크에서 발생하는 응용의 종류는 다양하지만 트래픽의 발생량 측면에서 소수의 응용에 의해서 대부분의 트래픽이 발생한다. 또한 특정 응용에서 접속하는 서버 IP, Port는 제한적이다. 학내망에서 발생하는 트래픽을 대상으로 조사한 결과, 전체 TCP 플로우의 80%가 10,000개 이하의 서버 IP, Port로 접속하는 확인할 수 있었다. 이러한 현상을 본 논문에서는 응용 트래픽의 지역성이라고 정의하고, 이를 이용하여 페이로드 시그니쳐 기반 분류 시스템의 처리 속도를 향상 시킬 수 있는 방법을 제안한다.

본 논문의 구성은 다음과 같다. 본 장의 서론에 이어, 2장에서는 관련연구에 대해 기술하고, 3장에서는 제안하는 방법의 배경이 되는 응용 트래픽의 지역성에 대해 설명한다. 4장에서는 실험 결과를 바탕으로 제안하는 방법을 기술한다. 5장에서는 제안하는 방법을 분류 시스템에 적용하여 그 타당성을 증명한다. 마지막으로 6장에서는 결론 및 향후 연구에 대해 기술한다.

Ⅱ. 관련 연구

응용 프로그램 서비스 제공자는 방화벽을 우회하여 사용자에게 원활한 서비스를 제공하기 위해 복잡한 구조의 응용 레벨 프로토콜 구성하기 때문에 시그니쳐 또한 복잡하고 다양한 형태로 나타난다. 또한 인터넷에 기반한 응용의 증가로 인해 시그니쳐의 개수가 증가하고 있다. 시그니쳐의 복잡도가 커지고, 개수가 증가하면서 페이로드 시그니쳐 기반 분류 시스템의 처리 속도는 트래픽 분류 시스템의 성능을 결정하는 중요한 요소로 작용하게 되었다.

응용 프로그램 트래픽 분류를 위한 도구로 많이 사용되고 있는 L7-filter는 시그니쳐를 정규표현식으로 표현하고 패턴 매칭 알고리즘으로 NFA(Nondeterministic Finite Automata)를 적용한다. 하지만 70여 개의 시그니쳐를 적용하였을 때 3.5Mbps 이하의 처리 속도를 보인다[4]. NFA의 처리 속도를 향상 시키기 위해 DFA(Deterministic Finite Automaton) 기반의 분석이 제안되고 활용되고 있지만 100Mbps 이하의 처리속도를 갖는다[5,6]. 분류 시스템의 처리 속도 향상을 위해 패턴 매칭 알고리즘의 성능 향상을 위한 방법을 제안하지만 매칭 알고리즘의 성능은 입력 데이터의 구성에 의존적이며, 제한적인 성능 향상을 나타낸다[5]. 패턴 매칭 알고리즘으로 오토마타에 기반한 NFA와 DFA 알고리즘의 성능 향상을 위한 방법론들이 제시되고 있지만 오토마타를 이용한 방법은 '.*'와 같은 와일드 카드의 사용 빈도에 따라 시간 및 공간 복잡도 급격하게 증가하여 성능이 저하되는 문제점이 있다[6,7].

Abhishek Mitra et al.[8]은 NFA에 기반한 패턴 매칭 알고리즘을 FPGA로 구현한 하드웨어 기반 방법론을 제시하였다. 하지만 하드웨어 기반 분석 방법은 고가의 비용을 요구되며, 현재와 같이 응용 프로그램의 출현, 소멸, 갱신들의 변화가 잦은 환경에는 소프트웨어 적인 방법에 비해 상대적으로 유연성이 부족한 방법이다.

기존 연구에서 서버의 3-tuple(IP, Port, L4 Prot.)을 시그니쳐로 정의하고 응용 트래픽을 분석하는 방법을 제시하였다[3]. 하지만 이러한 방법은 트래픽 분석 전에 사전에 추출한 시그니쳐를 이용하기 때문에 응용 프로그램의 서버 IP, Port 정보가 변경되면 분류 정확도가 감소되는 문제점이 존재한다.

응용 레벨 트래픽 분류 방법으로 과거에는 잘 알려진 포트 기반 트래픽 분석 기법이 많이 활용되었다[3]. 포트 기반 트래픽 분석 방법은 다른 분석 방법에 비해 분석 속도가 빠르고 높은 정확도를 보장하는 방법이었다. 하지만 동적 포트를 사용하는 응용의 증가와 알려지지 않은 포트의 사용으로 분류 정확도를 신뢰할 수 없는 문제점이 발생하여 그 활용도 감소되었다. 동

적 포트를 사용하는 응용의 트래픽을 페이로드 시그니쳐 기반 분석하여 그 정보를 분석 결과에 활용한다면 포트 기반 분석의 장점을 유지하면서 페이로드 기반 분석 방법의 단점인 처리 속도 문제를 보완할 수 있다.

기존의 연구는 페이로드 시그니쳐 기반 트래픽 분류 시스템의 처리 속도 향상을 위해서 패턴 매칭 기법을 소프트웨어 또는 하드웨어적으로 개선하려는 노력이 주를 이루었다. 하지만 이러한 방법은 네트워크 대역폭 증가에 비해 상대적으로 제한적인 성능 향상을 보인다.

Ⅲ. 응용 트래픽의 지역성

본 장에서는 제안하는 방법론의 배경이 되는 응용 트래픽의 지역성을 트래픽 발생 패턴 이용하여 정의하고, 학내망의 실제 트래픽을 통해서 트래픽의 지역성을 실험적으로 확인한다.

3.1. 트래픽 트레이스 구성

본 절에서는 응용 트래픽의 지역성을 확인하고, 제안하는 방법의 타당성을 증명하기 위해 사용된 트래픽의 구성에 대하여 기술한다.

표1은 실험에 사용된 트래픽 트레이스와 실험 기간을 보여주고 있다. 학내 망과 인터넷의 연결 지점에서 하루동안 3,000여대의 호스트에서 발생한 트래픽을 플로우와 페이로드 데이터를 포함한 패킷 형태로 수집하였다.

Table 1. Traffic trace

measure	Flows	Packets	Bytes
Volume	51,477K	2,012M	1,578GB
Duration	2012.09.12 00:00 ~23:59		

표2는 본 연구진에서 수행한 선행 연구[1]를 통해 개발한 페이로드 시그니쳐 기반 트래픽 분석 시스템의 을 기반으로 분류한 결과에 대해 응용의 유형 별로 Top 10의 트래픽양을 보여주고 있다.

학내 망의 전체 인터넷 트래픽을 대상으로 분석하여 선행 연구를 통해 개발한 검증 네트워크[11]에 적용한 결과 flow/byte/packet 단위로 99%이상의 정확도와 85% 이상의 분석률을 보였다. 표2의 결과는 응용 레벨 트래픽 분석 분양에 많이 사용되는 Bro[10] 시스템에 적용한 결과와 유사하였다. 플로우를 기준으로P2P 파일공유 응용들이 50% 이상을 차지하고 있고, 웹 브라우져 트래픽이 다음으로 많은 양을 발생하고 있는 것을 알 수 있다.

이와 같이 분석 대상 네트워크에서 발생하는 트래픽은 소수의 응용에 의해서 대부분의 트래픽이 발생한다. 이러한 응용에 대한 분석 시간을 단축 시킬 수 있다며 분류 시스템의 처리 속도를 향상 시킬 수 있다.

Table 2. Top 10 application break-down

Top 10	App. Type	Flows	Packets	Bytes
1	p2pfilesharing	25.39M	561M	356GB
2	web browser	17.04M	1,037M	864GB
3	im	1.08M	30M	16GB
4	utility	0.97M	41M	32GB
5	multimedia	0.75M	205M	172GB
6	game	0.69M	31M	18GB
7	sns	0.44M	9M	6GB
8	security	0.24M	6M	4GB
9	vaccine	0.23M	28M	28GB
10	commercial	0.12M	22M	20GB

3.2. 서버 IP, Port의 분포

그림 1은 표1의 트래픽에 대해 서버/클라이언트를 결정할 수 있는 TCP 플로우의 개수와 TCP 플로우를 서버의 IP, Port, L4 프로토콜로 그룹하였을 때 그룹의 개수를 나타내고 있다. 서버의 IP, Port, L4 프로토콜이 동일한 플로우 그룹을 SSIP(Same Server IP Port)라고 명명하도록 하겠다. SSIP 개수의 비율은 전체 TCP 플로우 개수 대비 최소 45.79%, 최대 16.34%, 평균 29.59%로 나타났다. 이와 같이 특정 분석 대상 망에서 발생하는 응용 트래픽은 접속하는 서버에 대한 지역성을 갖는다.

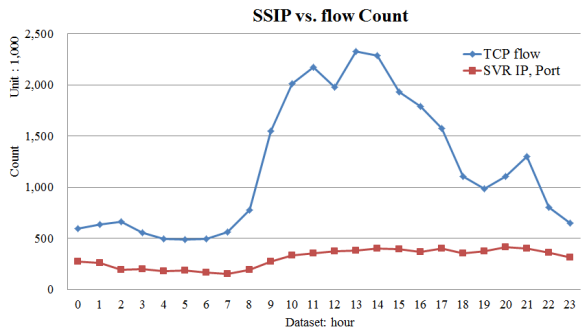

Fig. 1. SSIP vs. Flow

그림 2는 그림 1의 TCP 플로우에 대하여 서버 IP,

Port별로 플로우 개수에 대한 CDF 그래프를 보여주고 있다.

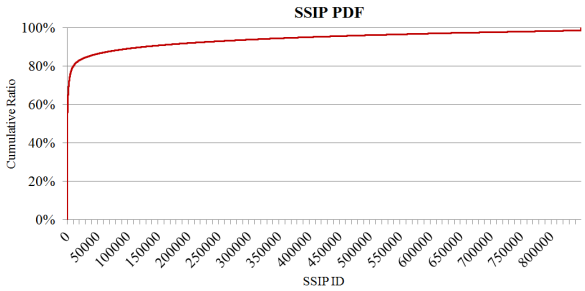

Fig. 2. SSIP CDF

그림2에서 알 수 있듯이 TCP 전체 플로우의 80%가 10,000개 이하의 SSIP로 접속하는 것을 알 수 있다. 서버의 IP, Port는 응용 프로그램의 특정 서비스를 연결하는 주소로 사용된다. 따라서 10,000개 이하의 서버 IP, Port가 제공하는 응용의 분류 결과를 분석 시스템에서 유지할 수 있으면 동일한 서버 IP, Port로 접속하는 플로우를 페이로드 시그니쳐 기반 분석없이 식별할 수 있게 된다. 응용 트래픽의 지역성은 분석 대상 네트워크에서 특정 응용 서버의 IP, Port로 접속하는 flow가 존재하면, 가까운 시간 내에 해당 서버로 접속하는 또 다른 flow가 존재할 확률이 높음을 의미한다.

Ⅳ. 제안하는 방법

본 장에서는 논문에서 제안하는 SSIP 캐쉬 기반 페이로드 시그니쳐 분석 방법론을 기술한다.

4.1. SSIP 캐시 기반 분석 효과

그림 3은 제안하는 트래픽 분류 방법론의 개념도를 보여주고 있다.

클라이언트 A와 B가 같은 응용을 사용하여 동일한 서버의 IP에 동일한 Port로 접속한다. 이때 클라이언트 A가 발생한 플로우가 페이로드 시그니쳐 기반으로 분석되면, 클라이언트 B의 플로우는 페이로드 시그니쳐로 분석하지 않고 Server의 IP, Port만을 비교하여 분석할 수 있다. 페이로드 시그니쳐 기반 분석기에 의해서 특정 플로우가 분석되면 해당 플로우의 서버 IP, Port 정보가 SSIP 캐쉬 테이블에 업데이트된다. SSIP 캐쉬에 정보가 저장되어 있으면 트래픽 분류 시스템은 SSIP 캐쉬를 통해 플로우를 분석하고, 분석되지 않은 플로우에 대해서 페이로드 시그니쳐 기반 분석을 수행한다.

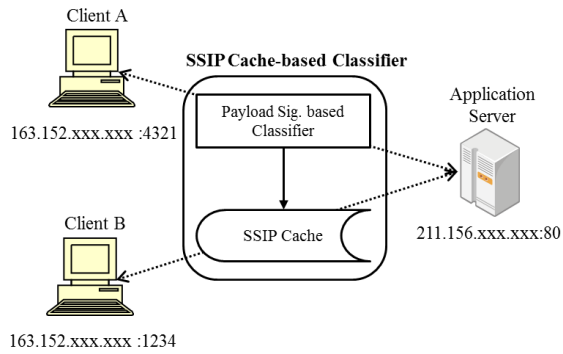

Fig. 3. Conceptual diagram of proposed method

그림 4는 표1의 트래픽에 대해 페이로드 시그니쳐 기반 분석 방법과 SSIP 캐쉬 기반 분석 방법으로 분석 가능한 트래픽의 비율을 나타내고 있다. A 영역은 순수하게 페이로드 시그니쳐 기반으로 분석할 수 있는 트래픽의 비율을 나타내며, B영역은 페이로드 시그니쳐 기반으로 분석된 플로우의 모든 서버 IP, Port를 SSIP캐쉬에 등록하고, 이를 기반으로 분석할 수 있는 비율을 나타낸다.

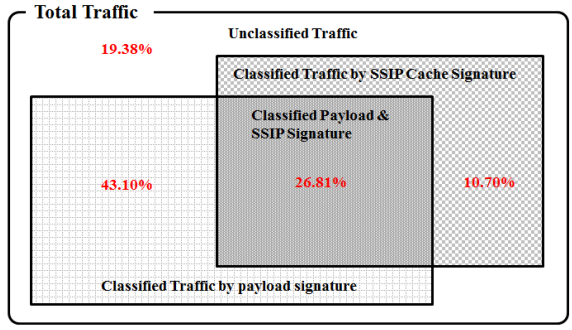

Fig. 4. Completeness of each classifier

A∩B 영역은 분석 시스템의 처리 속도를 향상 시킬 수 있는 트래픽에 대한 비율을 나타낸다. 페이로드 시그니쳐 기반 분석기는 A∩B 영역의 트래픽을 페이로드 시그니쳐 매칭을 수행하여 분석하지만 SSIP 캐쉬를 적용하면 서버 IP, Port 정보만을 매칭하여 분석할 수 있는 영역이기 때문에 분석 시스템의 처리 속도를 향상 시킬 수 있다. 학내망에서 발생하는 전체 트래픽의 26.81%의 플로우는 서버의 IP, Port 정보만을 비교하여 분석할 수 있다. B-A 영역은 제안하는 분석 방법론이 추가적으로 분석할 수 있는 트래픽이다. 이는 1개의 서버 IP, Port로 여러 개의 기능을 제공하는 응용프로그램의 모든 기능에 대한 페이로드 시그니쳐를 추출하지 못하고, 일부 기능에 대한 시그니쳐만을 추출한 경우에 페이로드 시그니쳐 기반으로 분석하지

못한 트래픽이 SSIP 캐쉬로 분석되는 경우이다. 제안하는 방법을 통해 트래픽의 분석률을 향상 시킬 수 있음을 알 수 있다. 암호화로 인해 페이로드 시그니쳐를 추출하지 못한 플로우의 트래픽을 서버 IP, Port 정보만으로 분석 가능함을 의미한다.

4.2. SSIP 캐시 데이터 교체 정책

SSIP 캐쉬를 통해 처리 시간과 분석률을 향상 시킬 수 있지만 캐쉬에 영구적으로 정보를 저장하고 분석하면 탐색하는 정보의 양이 증가하여 처리 속도가 늦어지는 문제점이 발생한다. 또한 P2P 응용의 서버 호스트 정보를 캐쉬에 유지하면 분류 정확도가 감소되는 문제점이 발생한다. 따라서 캐쉬의 정보를 교체하는 정책이 반드시 요구된다.

그림 5는 표1의 트래픽에 대해 순수하게 페이로드 시그니쳐 기반 분류 방법으로 분석한 분류 시간을 기준(100%)으로 하여 SSIP 캐쉬의 LT(life-time) 를1시간씩 증가 시키면서 분석 시간의 비율을 측정한 결과이다. 이 때 LT는 서버 IP, Port 정보가 SSIP 캐쉬에 유지되는 기간을 의미하며, 각각의 서버 IP, Port 별로 마지막으로 분류에 사용된 시각을 기준으로 업데이트 된다. 따라서 분석에 지속적으로 사용되는 서버 IP, Port 정보는 SSIP 캐쉬에 유지되며, 그렇지 않은 경우에는 캐쉬에서 제거된다.

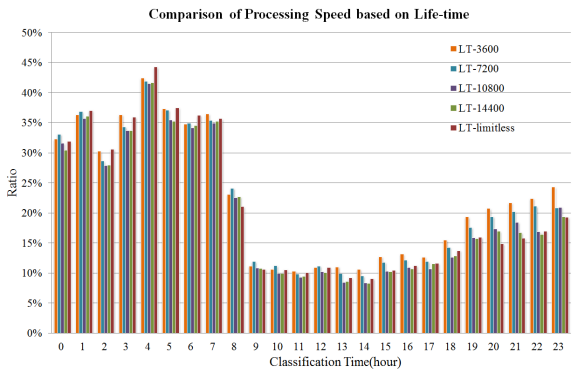

Fig. 5. Comparison of processing speed based on LT

서버 캐쉬의 LT를 1시간 단위로 증가시킨 결과, 3시간까지 증가 시키면 캐쉬로 분석 가능한 플로우의 양이 증가하여 분석 시간이 감소된다. 반면에LT를 4시간 이상으로 적용하면 분류 속도가 오히려 저하된다. 또한 LT에 대한 제한이 없는 경우에도 분석 시간이 감소되는 것을 알 수 있다. 이는 SSIP 캐쉬에 저장되는 서버 IP, Port 정보의 양이 증가하여 분류 시스템의 처리 속도를 저하시키기 때문이다. 이러한 결과를 바탕으로 SSIP 캐쉬에 저장되는 정보는 최종적으로 분석에 사용된 시점부터 3시간동안 저장하는 정책으로 캐쉬를 관리한다.

4.3. SSIP 캐시 기반 트래픽 분류 방법

그림6은 제안하는 분석 방법론의 흐름도를 나타내고 있다.

분류 시스템은 페이로드 시그니쳐와 1분 단위로저장된 분석 대상 트래픽을 입력으로 받아 최종적으로 응용의 이름이 식별된 트래픽 데이터를 결과로 제공한다. 분류 시스템은 크게 시그니쳐를 매칭하는 부분과 SSIP 캐쉬를 관리하는 부분으로 구성된다.

시그니쳐를 매칭하는 부분은 SSIP 캐쉬 기반 매칭 모듈과 페이로드 시그니쳐 기반 매칭 모듈로 구성된다. 시그니쳐 매칭 모듈은 SSIP 캐쉬를 먼저 매칭하고, 분류되지 않은 트래픽은 페이로드 시그니쳐 기반 매칭을 수행한다.

SSIP캐쉬를 관리하는 부분은 캐쉬 업데이트 모듈과 캐쉬 교체 모듈로 구성된다. 캐쉬 업데이트 모듈은 캐쉬 기반 매칭이 성공하면 캐쉬에 해당 서버 IP, Port 정보가 존재하기 때문에 Life-time 정보만를 수정하며, 페이로드 시그니쳐 기반으로 분석되는 플로우에 대해서는 캐쉬에 새로운 서버 IP, Port 정보를 등록하는 기능을 수행한다. 캐쉬 교체 모듈은 1분단위로 수집된 플로우 데이터에 대한 분석이 완료되면 SSIP 캐쉬에 저장된 모든 서버 IP, Port 정보를 검색하여 Life-time이 만료된 정보를 제거하는 역할을 수행한다.

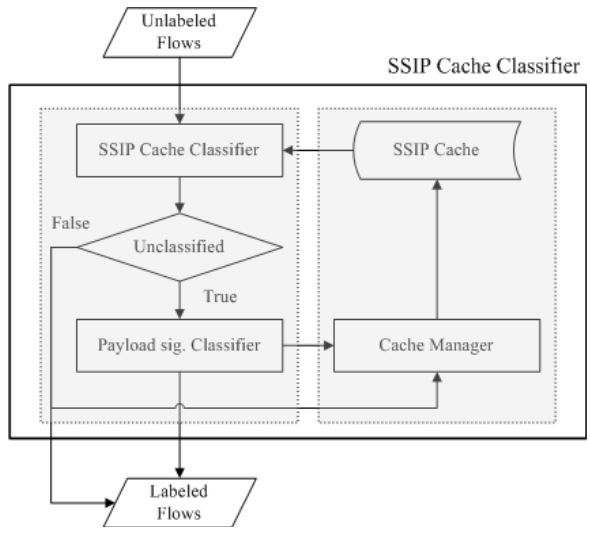

Fig. 6. Flow-chat of proposed method

V. 성능 평가

본 장에서는 4장에서 기술한 SSIP 캐쉬 기반 트래픽 분류 방법론을 적용하여 분류 시스템의 처리 속도와 분석률을 평가한다.

그림 7은 페이로드 시그니쳐 기반 분류 방법과 SSIP 캐쉬 기반 분석 방법론의 분류 시간을 비교한 그래프이다. 제안하는 방법론은 페이로드 기반 분석 방법에 비해 최대 10배 이상의 처리 속도가 향상되는 것을 알 수 있다. 페이로드 시그니쳐 기반 분석 방법은 트래픽의 발생량의 많은 09시~21시에 처리 시간이 급격하게 증가하는 반면에 제안하는 방법의 처리 시간은 크게 증가하지 않는 것을 알 수 있다.

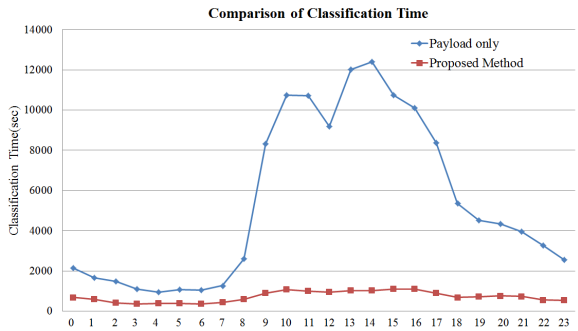

Fig. 7. Comparison of processing time

표3은 페이로드 시그니쳐 기반 분석 방법과 제안하는 방법의 분석률을 보여주고 있다.

Table 3. Comparison of completeness

Method \ Measure		Flow		Packet		Byte	
		#(K)	%	#(M)	%	#(G)	%
Total		51,477	100	2,012	100	1,578	100
Payload	Classified	35,988	69.91	1,281	63.69	1,025	64.99
	Unclassified	15,488	30.09	730	36.31	552	35.01
Payload + SSIP Cache	Classified by payload	22,032	42.80	686	34.10	583	36.98
	Classified by SSIP Cache	19,553	37.98	662	32.93	466	29.58
	Unclassified	9,891	19.22	663	32.97	527	33.43

제안하는 방법은 페이로드 기반 분석 방법에 비해 10% 이상의 플로우를 추가적으로 분석하는 것을 알 수 있다. 이는 1개의 서버 IP, Port에서 제공하는 여러 가지의 응용 프로그램의 기능 중 페이로드 시그니쳐가 추출되지 않은 기능에 대해서도 서버 IP, Port로 분석되기 때문이다.

Ⅵ. 결론 및 향후 과제

본 논문에서는 페이로드 시그니쳐 기반 응용 레벨 트래픽 분류 시스템의 처리 속도 향상을 위해서 SSIP 캐쉬 기반 분석 방법론을 제안하였다. 제안하는 분류 방법론은 페이로드 시그니쳐 기반 분석 방법과 비교해 최대 10배 이상의 처리 속도를 향상 시킬 수 있었다. 또한 페이로드 시그니쳐로 분석하지 못한 트래픽을 추가적으로 분석하여 10% 이상의 분석률을 향상 시킬 수 있었다.

본 논문에서는 서버 IP, Port 캐쉬의 Life-time을 기반으로 캐쉬 교체 정책 세웠다. 향후 연구로 서버 IP, Port 캐쉬의 사용 빈도 등 다양한 요소를 고려한 캐쉬 관리 방법에 대한 연구를 수행할 계획이다.

References

[1] J. S. Park, J. W. Park, S. H. Yoon, Y. S. Oh, and M. S. Kim, "Development of signature generation system and verification network for application level traffic classification," in *Proc. KIPS Conf.*, pp. 1288-1291, Pusan, Korea, Apr. 2009.

[2] S. H. Yoon, H. G. Roh, and M. S. Kim, "Internet application traffic classification using traffic measurement agent," in *Proc. KICS Summer Conf.*, pp. 1747-1750, Jeju Island, Korea, July 2008.

[3] S.-H. Yoon, J.-W. Park, Y.-S. Oh, J.-S. Park, and M.-S. Kim, "Internet Application Traffic Classification Using Fixed IP-port," *Lecture Notes in Computer Science*, vol. 5787, pp. 21-30, 2009.

[4] F. Yu, Z. Chen, Y. Dino, T. V. Lakshman, and R. H. Katz, "Fast and memory efficient regular expression matching for deep packet inspection," in *Proc. ACM/IEEE Symp. Architecture Networking Commun. Syst. (ANCS '06)*, pp. 93-102, San Jose, U.S.A., Dec. 2006.

[5] C. L. Hayes and Y. Luo, "DPICO: a high speed deep packet inspection engine using compact finite automata," in *Proc. ACM/IEEE Symp. Architecture Networking Commun Syst. (ANCS '07)*, pp. 195-203, Orlando, U.S.A.,

Dec. 2007.

[6] G. Vasiliadis, M. Polychronakis, S. Antonatos, E. P. Markatos, and S. Ioannidis, "Regular expression matching on graphics hardware for intrusion detection," in *Proc. 12th Int. Symp. Recent Advances Intrusion Detection (RAID '09)*, pp. 265–283, Saint-Malo, France, Sep. 2009.

[7] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein. *Introduction to Algorithms*, 2nd Ed., MIT Press and McGraw-Hill, 2001.

[8] A. Mitra, W. Najjar, and L. Bhuyan, "Compiling PCRE to FPGA for accelerating SNORT IDS," in *Proc. 3rd ACM/IEEE Symp. Architecture Networking Commun. Syst. (ANCS '07)*, pp. 127-136, Orlando, U.S.A., Dec. 2007.

[9] S. H. Yoon, J. S. Park, J. W. Park, Y. S. Oh, and M. S. Kim, "A study of evaluation and verification method for internet traffic classification," in *Proc. KICS Fall Conf.*, pp. 864-865, Seoul, Korea, Nov. 2009.

[10] S. Campbell and J. Lee, "Prototyping a 100G monitoring system," in *Proc. 20th Euromicro Int. Conf. Parallel, Distributed Network-Based Process. (PDP '12)*, pp. 293-297, Garching, Germany, Feb. 2012.

박 준 상 (Jun-Sang Park)

2008년 고려대학교 컴퓨터 정보학과 졸업
2010년 고려대학교 컴퓨터 정보학과 석사
2010년~현재 고려대학교 컴퓨터 정보학과 박사과정
<관심분야> 네트워크 관리 및 보안, 트래픽 모니터링 및 분석, 트래픽 분류

윤 성 호 (Sung-Ho Yoon)

2009년 고려대학교 컴퓨터 정보학과 졸업
2011년 고려대학교 컴퓨터 정보학과 석사
2011년~현재 고려대학교 컴퓨터 정보학과 박사과정
<관심분야> 네트워크 관리 및 보안, 트래픽 모니터링 및 분석

김 명 섭 (Myung-Sup Kim)

1998년 포항공과대학교 전자계산학과 졸업
2000년 포항공과대학교 컴퓨터공학과 석사
2004년 포항공과대학교 컴퓨터공학과 박사
2006년 Post-Doc. Dept. of ECE, Univ. of Toronto, Canada
2006년~현재 고려대학교 컴퓨터정보학과 부교수
<관심분야> 네트워크 관리 및 보안, 트래픽 모니터링 및 분석, 멀티미디어 네트워크