韓國 컴퓨터情報學會 論文誌
第13卷 第3號, 2008. 5.

2008-13-3-3-1

SVM을 이용한 플로우 기반 P2P 트래픽 식별

엄남경*, 우성희**, 이상호***

Flow-based P2P Traffic Identification using SVM

Nam-Kyoung Um *, Sung-Hee Woo **, Sang-Ho Lee ***

요 약

P2P 응용 프로그램들은 일반적으로 방화벽과 같은 보호시스템을 피하기 위해, 동적인 포트 번호 등을 사용하기도 한다. 그에 따라 포트 기반의 방법과 시그너처, 패킷 페이로드의 전수 검사 등을 통해 트래픽 식별을 하는 많은 방법론을 이용하지만, 여전히 정성적인 면과 정량적인 면을 만족시키지 못하고 있다. 따라서 이 논문에서는 P2P가 기본적으로 가지는 프로토콜의 성격을 이용하여 P2P의 트래픽 특성들을 분석하고 플로우 단위로 트래픽을 수집한 후, SVM을 이용하여 P2P 트래픽을 식별할 수 있는 방법론을 제안하고자 한다.

Abstract

To avoid some protection systems such as firewall, P2P applications have recently used to apply dynamic port numbers. Reliable estimates of P2P traffic require examination of packet payload, a methodological land mine from legal, privacy, technical, logistic, and fiscal perspectives. Indeed, access to user payload is often rendered impossible by one of these factors, inhibiting trustworthy estimation of P2P growth and dynamics. Despite various methods such as port-based and signature-based techniques, it still dose not satisfy the method which uses both qualitative and quantitative aspects. In this paper, a method using SVM mechanism which discriminate the P2P traffic from non-P2P traffics using differences between P2P and other application traffics is suggested. This is a systematic methodology to identify P2P networks, and without relying on packet payload.

▸ Keyword : Wireless LAN, IDS, IPS, IDPS

• 제1저자 : 엄남경
• 접수일 : 2008. 3. 10, 심사일 : 2008. 4. 10, 심사완료일 : 2008. 5. 24.
* 충북대학교 전기전자컴퓨터공학부 ** 충주대학교 전기전자 및 정보공학부 교수
*** 충북대학교 전기전자컴퓨터공학부 교수

Ⅰ. 서 론

인터넷에 전통적인 트래픽을 모니터링하고 측정하는 작업은 단순 작업으로 여겨졌었지만 근래에 들어 P2P 트래픽, 게임 트래픽, 스트리밍 데이터를 이용하는 트래픽 등이 부각되어지고 있으며[1], 그 중에서도 P2P 트래픽은 특정 네트워크에서는 2004년에서 2006년에 이르기까지 전통적으로 우세했던 HTTP 트래픽의 양을 앞지르는 트래픽의 선두주자가 되어가고 있다[2][3]. P2P의 트래픽 비중이 늘어남과 동시에, P2P는 대용량의 대역폭을 소비하거나 네트워크 통신을 방해하는 역할을 하기도 한다. 또한 불법적인 파일 유통을 위한 통로로 사용되거나, 방화벽차단 이후에도 급격히 감소되지 않는 트래픽의 양, 그리고 동적으로 변화하는 포트번호를 사용하거나 다른 응용프로그램의 포트번호를 사용하여 관리의 혼란을 유발한다는 점은 문제점으로 일컫어지고 있다. 따라서 포트기반의 방법론과 시그너처기반의 방법론 등 P2P 트래픽을 탐지하기 위한 많은 실험과 연구들이 있었음에도 불구하고, P2P 프로토콜을 위한 표준 규격이 없기 때문에 뛰어난 P2P 트래픽 탐지 방법을 찾는 것이 매우 힘들다.따라서 이 논문에서는 P2P 트래픽의 신속하고 정확한 분류를 위해 플로우 그룹핑에 기반한 SVM을 이용한 P2P 식별 방식을 제안하고자 한다.

이 논문의 구성은 다음과 같다. 2장에서는 위에서 언급한 관련연구들에 대해 장·단점을 제시하고, 3장에서는 이에 대한 문제제기를 한다. 4장에서는 P2P 식별을 위한 SVM 모델을 설계하고, 5장에서는 실험과 평가를 통해 6장에서 결론짓고자 한다.

Ⅱ. 관련연구

이 장에서는 기존 P2P 트래픽 구분 방식에 대한 관련 연구를 기술한다. 기존의 P2P 트래픽 구분 방식으로는 포트 기반의 식별법, 페이로드 기반의 식별법, 행위 기반의 식별법 및 통합 기반의 식별법 등을 제시한다.

2.1 포트 기반의 식별법

전통적인 방법으로 IANA 포트 목록에 등록된 "Well-Known" 포트 번호들을 기반으로 식별하는 방법이다[4]. 웹 트래픽은 80, 8080, 443 번등이 분류되어 있으며 우리가 사용하는 일반적인 중요 트래픽은 1024번 이내로 분류되어 있다. P2P 프로토콜 또한 IANA에 등록하여 사용하게 되어 있어 1990년대까지는 충분히 유효했던 방식이다. 그러나 현재는 최신의 인터넷 트래픽 때문에 이 방식에만 의존해서 트래픽을 식별할 수는 없다. 특히 P2P 프로토콜을 사용하는 프로그램뿐만 아니라 스트리밍 관련 프로그램, 게임 프로그램 등도 동적인 포트 번호를 사용하기 때문에 정확한 구분은 더 이상 힘들다. 일반적으로 포트 기반의 식별법은 CoralReef[5] 등의 툴을 이용하며 P2P뿐만 아니라, 그림 1과 같이 다른 프로토콜도 구분한다. IANA 포트목록에 있을 경우, 특정 응용 프로그램으로 분류하고 아닐 경우에는 "Unknown"으로 분류하는 방식이다.

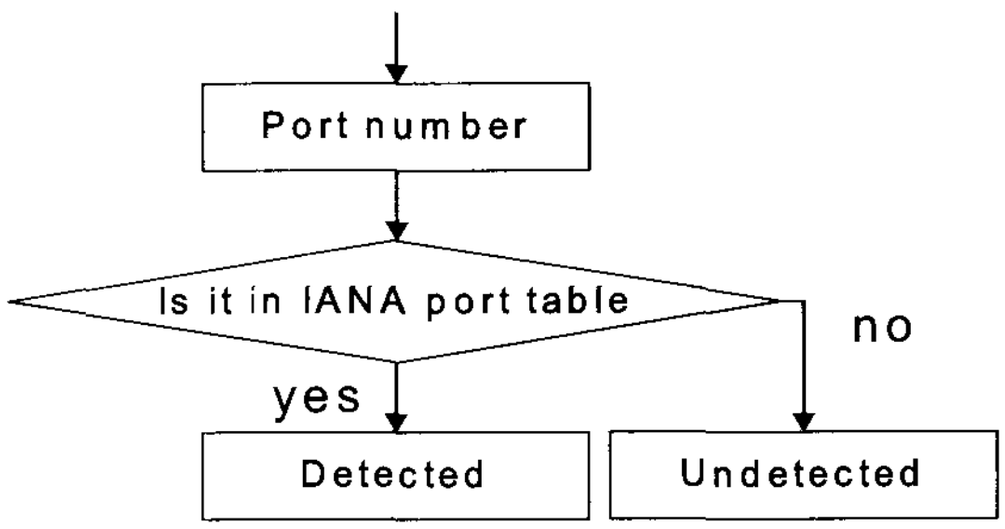


그림 1. 포트 기반 식별 방식
Fig 1. Port-based Identification Method

2.2 페이로드 기반의 식별법

P2P 응용 프로그램의 동적인 포트 선정을 감지하기 위해, 페이로드 검사 방법이 하나의 방안으로 대두되었다. 페이로드를 검사하는 방법은 전체 내용을 모두 검사하는 방법과 페이로드의 k번째 바이트까지를 조사하여 실제의 시그너처와 비교하는 방법으로 나뉜다. 페이로드를 모두 검사하는 방법은 가장 확실한 트래픽 식별 방법이기는 하나, 오늘날과 같은 네트워크상에 대용량의 트래픽이 오고가는 상황에서는 비현실적인 방법으로 여겨진다. [6]에서는 k번째 바이트까지의 페이로드에서 시그너처를 분석하는 방법을 제안하며 페이로드에 기반하여 주요 P2P 프로토콜을 실험하였다. 특히 정확성(Accuracy)과 확장성(Scalability), 견고성(Robustness) 등을 초점으로 실험하였으며 UDP와 TCP 프로토콜, 패킷(Packet)과 스트림(Stream), 시그너처의 위치, 네트워크 영향에 대한 견고성 등을 설계 초점으로 두었다. 페이로드 검사는 byte_match_offset과 word_match_offset, string_match_offset으로 나누어 검사하였다. [1]에서는 그림 2와 같이 페이로드와 포트번호를 모두 검출하는 방법을 제안하였으며 각 프로토콜이 일반적으로 가지는 세션 성격에 따라 특

성을 분류한 후 이를 기반으로 자체적으로 개발한 플로우 기반 모니터링 프로그램을 기반으로 플로우 수집을 한 이후, P2P를 포함한 프로토콜 트래픽을 식별한다.

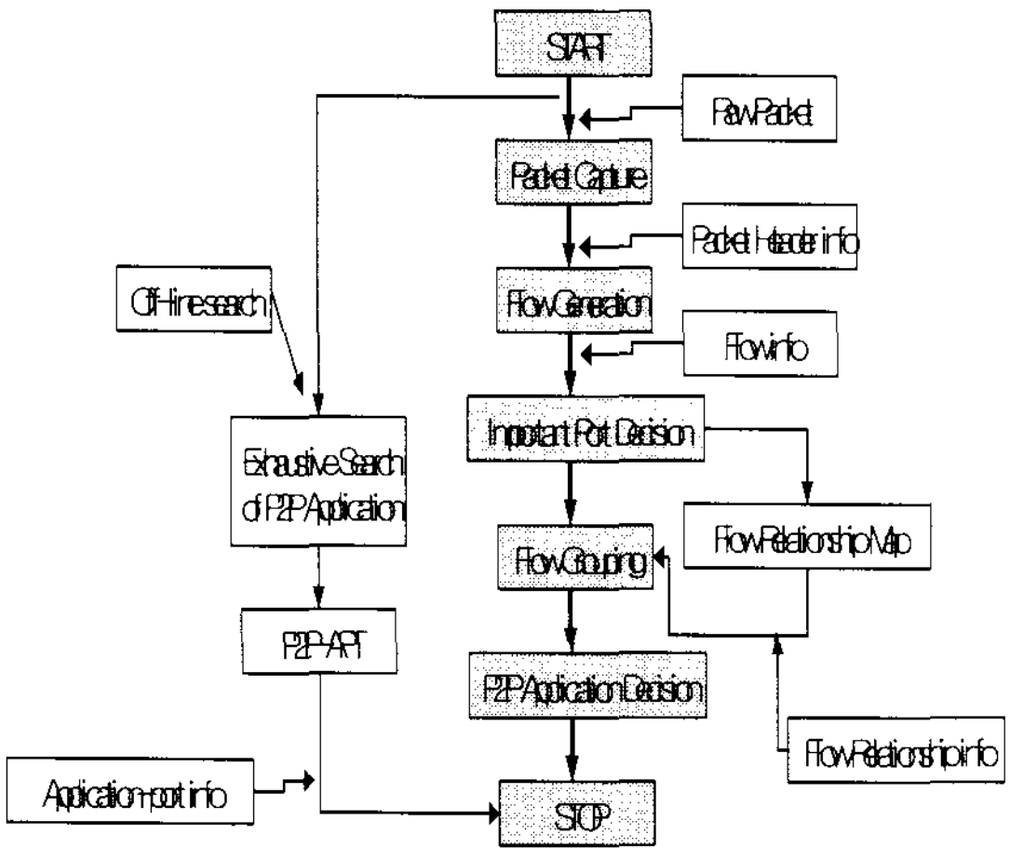


그림 2. [1]에서의 트래픽 분류 방식
Fig 2. Traffic Identification Method in [1]

2.3 행위 기반의 식별법

P2P 트래픽이 HTTP용 80번 포트를 사용하고 새로 생성되는 P2P 응용 프로그램에서는 동적인 포트번호를 사용함으로써 포트 기반의 트래픽 식별 방식으로는 트래픽 구분이 어려워지는 단점으로 P2P 트래픽 등의 새로 생성되는 트래픽의 분류를 위한 행위 기반의 식별법이 대두되었다. 행위 기반의 방법의 대표적인 연구는 BLINC[7] 방식으로 트래픽 분류를 위해 네트워크의 행위를 트래픽의 출발지와 목적지 사이의 관계를 정의하며, 트래픽 분류 단계를 사회적 레벨(Social Level), 기능적 레벨(Functional Level), 응용 레벨(Application Level)로 나누어 분류하며, 같은 트래픽의 출발지-목적지의 IP주소 및 포트 주소의 관계를 정립하여 여러 트래픽 유형들을 그림 3과 같이 분류하였다. P2P 응용프로그램은 일반적으로 출발지와 목적지간의 정해져있거나 동적으로 할당되는 포트 번호 등을 사용한다.

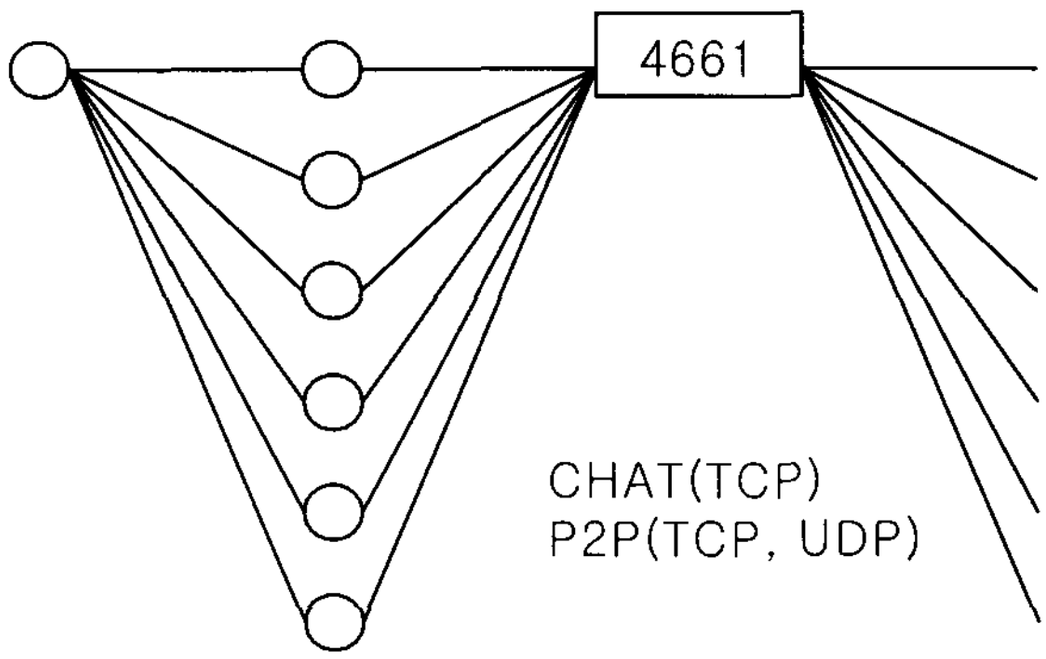


그림 3. P2P의 프로토콜별 출발지와 목적지 매핑 관계[7]
Fig 3. Mapping Relation between Source and Destination Address of P2P[7]

2.4 통합 기반의 식별법

[8]에서는 페이로드를 이용하여 검출하는 그림 4와 같이 혼합적인 방식을 제안하였다.

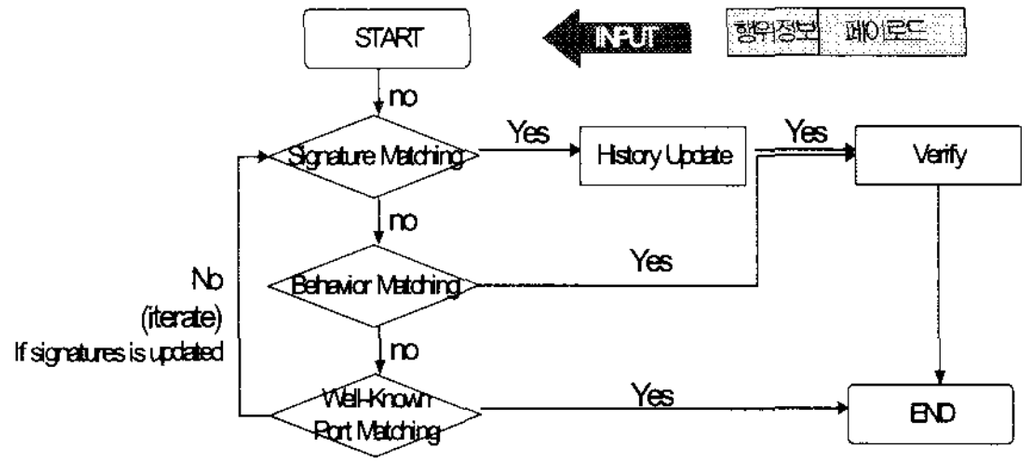


그림 4. 통합 기반의 방법론[8]
Fig 4. Hybrid-based Identification Method[8]

[9]에서는 1단계 포트 기반의 방법론에서 9단계까지 이르는 단계적인 통합적인 트래픽 식별법을 제안한다. 이 방식의 정확성은 99% 이상이나 정확성 기반의 해결 방식일 뿐 모든 단계를 실행하여 트래픽을 식별하는 것은 현실적으로 어렵다.

III. 문제제기

이 장에서는 관련연구에서 제시한 방법론들에 대해 비교평가를 실시하고, 이를 통해 이 연구의 필요성을 부각시키고자 문제 제기를 한다. 표 1은 기존의 방법론에 대해 비교 평가표이다.

표 1. 기존 방식들의 비교 평가
Table 1. Comparison to existing methods

분류	방식	정확성	페이로드 프라이버시 미침해	응용성
포트 기반	[4]	Medium	Yes	Practical
	[10]	Medium	Yes	Experimental
페이로드 기반	[11]	Medium	No	Practical
	[12]	Medium/ High	No	Practical
행위 기반	[13]	Low	Yes	Experimental
	[7]	Medium	Yes	Experimental
통합 기반	[14]	High	No	Practical
	[8]	High	No	Practical

표 1에서는 기존의 포트 기반 식별법의 [4], [10], 페이로드 기반 식별법의 [11], [12], 행위 기반 식별법의 [13], [7], 통합기반 식별법의 [14], [8]을 각각 정확성, 프라이버시 미침해, 응용성 기반으로 평가한다. 평가 기준과 평가 결과는 기존의 연구 [8]와 [14]에서 제시하는 방법론을 이용하였다. 정확성의 분류 기준은 90% 이상일 경우 High, 90이하 60이상일 경우 Medium, 60% 이하일 경우는 Low의 평가치를 두었다. 또한 페이로드 프라이버시 미침해의 Yes/No에 대한 평가치는 해당사항이 있는 경우와 없는 경우로 분류된다. 응용성에 있어 Practical/Experimental 은 각각 실제에 바로 실행되고 있는 방법론과 실험을 통해 연구적으로 좋은 결과를 나타낸 경우이나 실제적으로 산업에는 이용되지 않는 경우를 기준으로 두어 분류하였다. 결과적으로 포트 기반의 식별법은 IF-Then-Else 문을 이용하여 계속 비교를 통하여 측정하는 방법으로 정확성 측면은 Medium의 평가를 가지며, 페이로드의 내용을 모두 수집하여 분석하지 않아도 되므로 페이로드에 대한 프라이버시 침해는 없다. 현재까지 사용되고 있으므로 [4]은 Practical로, [10]은 Experimental로 나누었다. 페이로드 기반의 식별법의 경우, 정확성은 Medium, 페이로드의 내용을 검사해야 하므로 페이로드 프라이버시 침해 가능성이 높음을 알 수 있다. 이와 같이 행위 기반과 통합 기반의 방법에 대해 비교평가를 수행하였으며, 비교한 방법들 모두 트래픽을 식별하기 위해 활용되는 방법적인 장단점을 가지고 있다. 그러나 P2P 트래픽만을 특별하게 분류하는 방법론으로는 P2P의 특별한 포트를 가지고 분류하는 포트 기반의 방법론과 페이로드를 측정하여 검사하는 페이로드 기반의 방법론을 행하고 있으며, BLINC로 대표되는 행위 기반의 방식에서는 빠르게 변모하는 P2P 트래픽의 행위에 따라 정확성이 높지 않음을 알 수 있다. 따라서 이 논문에서는 정성적이고 정량적인 면에서 기존의 방식들보다 우수한 P2P 트래픽 식별 방식을 제안한다. 즉, 정성적인 면에서는 기존의 방법에 있어 페이로드의 프라이버시를 침해하지 않으면서도 변화하는 P2P 응용 프로그램의 속도에 따라갈 수 있는 방법이면서도 정량적으로 P2P 트래픽을 다른 방식들보다 정확성 있게 식별해내는 방법론이 요구된다.

IV. P2P 식별을 위한 SVM 모델 설계

이 장에서는 P2P 트래픽이 가지는 TCP 연결 세션을 이용한 속성을 기술한 후, P2P 트래픽이 가지고 있는 기본적인 연결 속성들을 기반으로 하여 다른 트래픽과 구분될 수 있도록 SVM 모델을 설계한다.

4.1 고려사항

P2P 응용 프로그램을 구분하기 위해서 포트 번호만으로나 패킷을 측정함으로써 분류해내는 것은 최근의 P2P 응용 프로그램에는 충분치 않다. 따라서 다음의 세 가지 조건을 만족시키는 방법을 제안한다.

(1) 분류 기술은 포트 번호에 의존해서만은 안 된다. 포트 번호를 동적으로 사용하는 경우가 많이 발생하기 때문이다.
(2) 분류 기술은 파일의 저작권을 위반해서는 안 된다. 페이로드를 전수 조사하는 것은 파일에 대한 프라이버시를 훼손할 수 있는 가능성을 만든다.
(3) 분류 기술은 그 응용 프로그램에 절대적으로 독립적이어야 한다. 분류 기술을 적용한 후, 다른 시기에 같은 분류 기술을 적용하여 결과값이 다른 비신뢰성을 준다면 소용이 없다.

4.2 트래픽 속성 정의

이 논문에서는 두 개의 물리적 네트워크에서 P2P 트래픽과 P2P로 밝혀지지 않는 트래픽을 분류하기 위한 몇가지 속성을 정의한다. 제시하는 주요 포커스는 SYN과 SYN/ACK 패킷이다. 왜냐하면 이 패킷들은 예외없이 P2P 응용 프로그램의 TCP 연결을 위해 쓰이기 때문이다. 다음은 P2P 트래픽 특성을 제시하기 위한 TCP의 속성들이다. |f(x)|는 함수에

의해 발생된 수를 의미하며, 함수의 입력값으로 표기된 마지막 원소에 대한 크기를 기술한다.

예를 들어 $|f(sip,sport,SYN,\Sigma(dport))|$은 sip, sport, SYN을 가지는 dport의 합에 대한 수를 구하는 것을 의미한다. 표 2는 표기된 약어들을 기술한다.

표 2. 트래픽 속성을 위한 약어
Table 2. Abbreviations for traffic features

표기	기술
sip	Source IP : 출발지 IP
dip	Destination IP : 목적지 IP
sport	Source Port : 출발지 포트
dport	Destincation Port : 목적지 포트
proto	IP 프로토콜 헤더에 포함된 "Protocol" 유형

4.3 제안 모델

SVM을 이용하여 P2P 트래픽 식별을 하기 위해서, 그림 5와 같이 STEP1과 STEP2로 분류한다. STEP1은 전체 분석할 트래픽의 양을 줄이기 위해 플로우 수집과 그룹핑을 하며, STEP2에서는 SVM을 이용하여 "Pure P2P"를 기존의 "Well-Known" 속성을 가지는 "non-P2P" 트래픽으로부터 식별한다

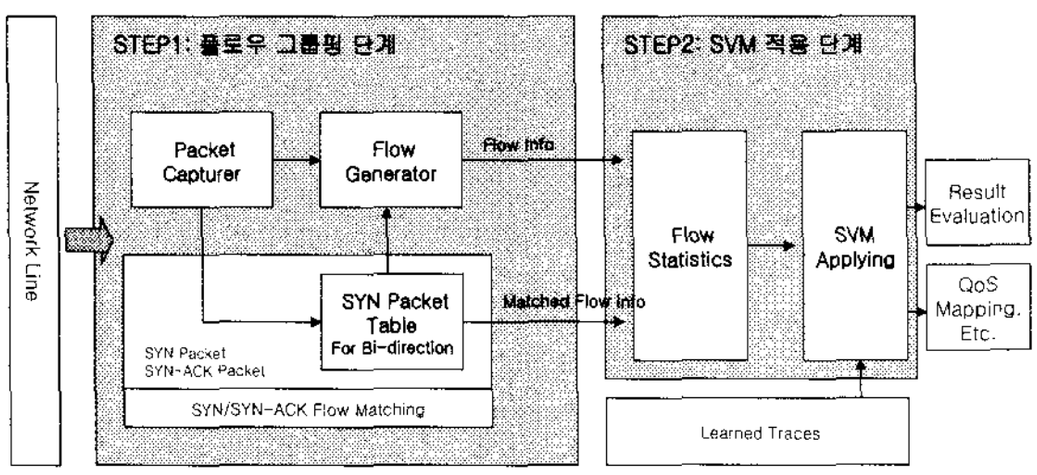


그림 5. P2P 식별 체계 구조
Fig 5. P2P identification system

네트워크로부터 들어온 트래픽을 패킷형태로 캡처하고 플로우 단위로 생성한다. 이를 양방향성을 지니는 트래픽인지를 구분할 수 있는 기준을 이용해 재분류한 후, 해당되는 플로우 형태를 변환시킨다. 이렇게 생성된 플로우 정보를 가진 데이터셋을 구분자로 이용하여 SVM에 활용할 수 있는 트레이닝 데이터셋으로 학습시킨 후, SVM을 이용하여 P2P 트래픽을 식별해낸다. 처리과정 흐름도는 그림 6과 같다.

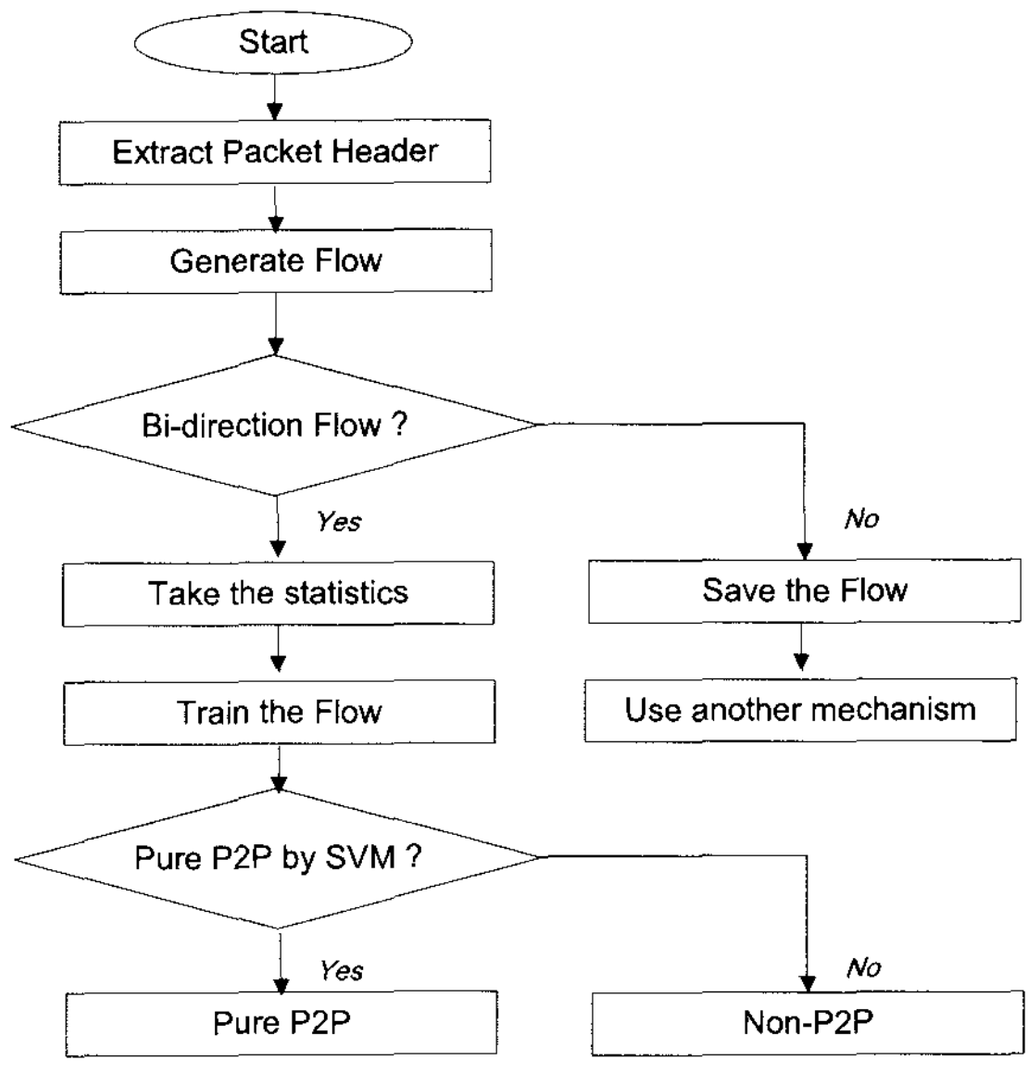


그림 6. P2P 식별 처리 흐름도
Fig 6. Flow chart for P2P identification

V. 실험 및 평가

이 장에서는 실험 데이터와 방법에 대해 정의하고, 기존의 포트 기반의 방식과 페이로드 기반 방식, 행위 기반을 이용한 방식을 대상으로 Accuracy, Precision, Recall 평가측정치에 대한 비교 평가를 수행한다.

5.1 실험방법

실험 데이터는 기존의 연구에서 많이 활용되는 CAIDA 등의 데이터를 사용하며, 상세한 정보는 표 3과 같다.

표 3. 실험 데이터 정보
Table 3. Experimental data

Trace (Country)	Link type	Date (Local day)	Start time & duration	Average Utilization	Payload bytes per each packet
DataSet A (US-JP)	100 ME Backbone	2006.3.3 (Fri)	22:45, 55m	35 Mbps	Max 40
DataSet B (JP)	1 GE Edge	2006.8.8 (Tue)	19:43, 30m	75 Mbps	Max 40
DataSet C (KR)	1GE Edge	2006.9.14 (Thu)	16:37, 21h 16m	28 Mbps	Full payload

실험 방식은 Cisco의 Netflow를 이용해 수집된 데이터를 다시 원하는 플로우 형태로 생성할 수 있도록 sflowtool-3.9와 SVM을 적용하기 위해 WEKA-3.5.5를 이용하였다. WEKA-3.5.5는 SVM 머신으로 효율성이 높음이 입증

LibSVM를 포함하여 선형 분류와 비선형 분류를 위한 SVM을 활용할 수 있다. 실험을 위한 플로우 추출 절차는 그림 7과 같다.

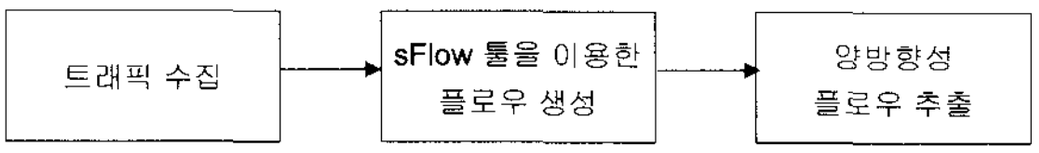


그림 7. 플로우 추출 절차
Fig 7. Flow sampling process

5.2 평가방법

측정치를 위해서는 True Positive, False Positive, False Negative 등을 기반으로 되어 있어야 한다.

- True Positive: P2P를 P2P로 판명하는 경우
- False Positive: P2P가 아닌 파일을 P2P로 판명하는 경우
- False Negative: P2P를 P2P가 아닌 것으로 판명하는 경우

평가측정치는 Accuracy, Precision, Recall 을 기반으로 평가한다. Accuracy는 정확성이며, 모든 데이터에서 올바르게 측정된 데이터양을 의미하여 그 계산식은 (식1)과 같이 정의한다. Precision은 P2P로 판정된 트래픽 중에서 진짜 트래픽은 얼마나 되는가를 의미하며 (식2)와 같이 정의한다. Recall은 진짜 P2P 플로우 중에서 얼마나 P2P로 판정되었는가를 의미하며 그 계산방식은 (식3)과 같다.

$$\text{Accuracy} = \frac{\text{정확하게 분류된 } Flow\text{의 총합}}{\text{전체 } Flow\text{수}} \times 100 \cdots\cdots \text{(식1)}$$

$$\text{Precision} = \frac{True\,Positive}{(True\,Positive + False\,Positive)} \times 100 \cdots \text{(식2)}$$

$$\text{Recall} = \frac{True\,Positive}{(True\,Positive + False\,Negative)} \times 100 \cdots\cdots \text{(식3)}$$

5.3 평가결과

실험은 제안 방식을 포트기반방식, 페이로드기반방식, 행위기반의 방식들과 비교하는 형식으로 진행하였으며, 제안 방식에 대한 최종 결과치는 그림 8과 같다. 이는 플로우를 기반으로 한 실험으로, Dataset A, B, C에 대해 Precision의 경우, 평균 88.3%의 값을 가졌으며 Recall은 43.3%를 가짐을 알 수 있다. Recall이 Precision 보다 낮은 이유는 Precision이 측정된 P2P 안에서의 진짜 P2P를 측정하는 반면, Recall은 진짜 P2P가 실제 P2P 내에서 얼마나 측정된 것인지를 비교하기 때문이다.

이 논문에서 제안하는 방식은 정성적인 면과 정량적인 면에서의 우수성을 가진다. 즉 TCP의 기본 속성을 이용함으로써 P2P 응용 프로그램의 특성 변화에도 강한 적응력을 가진다. 이 논문에서 비교한 포트기반과 페이로드 기반은 활용도가 큰 방식이기는 하나, IANA에 제시되는 포트목록을 이용하는 방식은 네트워크마다 큰 편차를 가짐을 알 수 있었다. 페이로드기반의 식별법은 프라이버시 침해의 문제가 계속적으로 일어나며, 계속적인 시그너처 등의 업데이트가 요구된다. 이에 반해 일종의 행위기반으로 분류될 수 있는 제안 방식은 60~90% 또는 90% 이상의 정확성을 가지고 정량적으로 평가되므로 정확도와 프라이버시 미침해성에 관련된 부분에서 모두 우수함을 알 수 있었다.

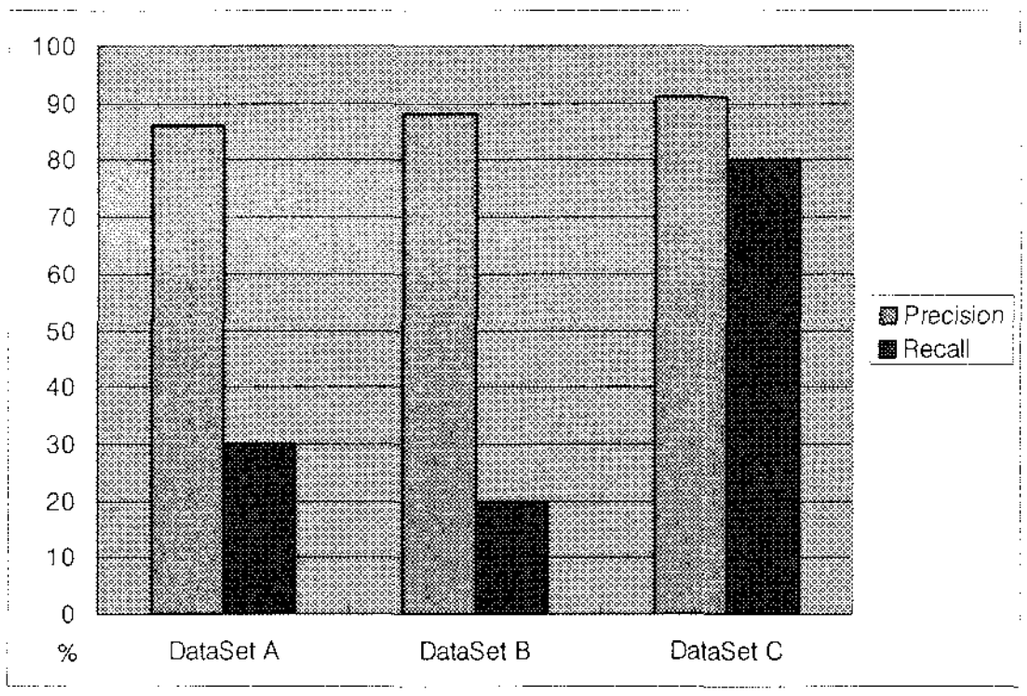


그림 8. 제안 방식의 결과
Fig 8. Result of Proposed Method

Ⅵ. 결론

P2P 기술은 1999년 미국에서 Napster 프로그램의 개발 이후 P2P 네트워킹 기술도 큰 발전을 거듭한 후 "성장성 있는 응용 프로그램"으로 불리며 성장해왔다. 그러나 이러한 성장세로 말미암아 인터넷 네트워크 환경에서의 트래픽 비중 또한 급격하게 늘어나고 있는 추세이다. 이 증가된 트래픽은 대역폭을 소비하고 네트워크 통신을 방해하여 컴퓨터 바이러스나 악성 코드들의 출입구를 제공할지도 모른다. P2P 트래픽을 탐지하기 위한 많은 실험과 연구들이 있었음에도, P2P 프로토콜을 위한 표준 규격이 없기 때문에 뛰어난 P2P 트래픽 탐지 방법을 찾는 것이 매우 힘들다. 따라서 이 논문에서는

P2P 트래픽의 신속하고 정확한 분류를 위해 플로우 그룹핑에 기반한 SVM을 이용한 P2P 식별 방식을 제안하였다. 이를 위해서는 다음과 같은 고려사항을 적용하였다. 첫째, 분류 기술은 포트 번호에 의존해서만은 안 된다. 이를 위해 포트 기반의 방식이 아닌 트래픽의 속성을 활용하였다. 둘째, 분류 기술은 파일의 저작권(copyright)을 위반해서는 안 된다. 패킷의 페이로드를 검사하지 않고 역시 인터넷 프로토콜의 일종인 TCP의 속성을 활용하여 식별하였다. 셋째, 분류 기술은 그 응용 프로그램에 절대적으로 독립적이어야 한다. 포트 번호나 페이로드에 종속하지 않으므로 특정한 응용 프로그램의 속성보다는 트래픽 자체의 속성에 대한 파악이 더 중요하다. P2P 트래픽이 불법파일을 유통시키는 경로이며 대용량의 트래픽을 발생시키는 응용 프로그램이며 동적인 포트를 사용하거나 다른 응용 프로그램의 포트를 사용한다는 문제점에 착안하여, 기본적으로 이용하는 TCP 기본 속성을 통해 기존 방식보다 변화에 적응력이 강하여 정성적인 평가에서 우수한 방식으로 평가된다.

참고문헌

[1] M. Kim et al, "Flow based Internet Application Traffic Analysis," KNOM Review, Vol. 7, No. 1, pp.20-31, Aug 2004.

[2] H. Lee et al, "The method of P2P traffic detecting for P2P harmful contents prevention," ICACT 2005, pp.777-780, Feb 2005.

[3] N. Um et al, "DESIGN AND IMPLEMENTATION OF REAL-TIME MRTG++," ISRS 2005, Oct 2005.

[4] IANA, ttp://www.iana.org/assignments/portnumbers, 2007.

[5] CoralReef Tool, "http://www.caida.org", 2007.

[6] S. Sen et al, "Accurate, Scalable In-Network Identification of P2P traffic using Application signatures,"

[7] T. Karagiannis et al, "BLINC: Multilevel Traffic Classification in the Dark," SIGCOMM 2005, Philadelphia, USA, Aug 2005.

[8] Y. Won et al, "A Hybrid Approach for Accurate Application Traffic Identification," IEEE/IFIP E2EMON, Vancouver, Canada, pp.1-8, Apr 2006.

[9] A. Moore et al, "Internet Traffic Classification Using Bayesian Analysis Techniques," SIGMETRICS 2005, Banff, Canada, Jun 2005.

[10] M. Kim et al, "Internet Application Traffic Monitoring and Analysis," Dissertation of, Postech, Feb 2005.

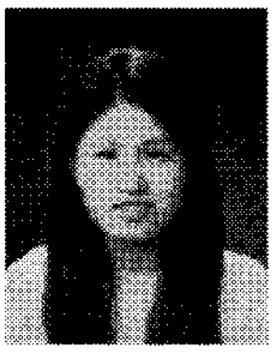
[11] S. Sen et al, "Analyzing peer-to-peer traffic across large networks," SIGCOMM 2002, Nov 2002.

[12] T. Karagiannis et al, "Transport Layer Identification of P2P Traffic," IMC 2004, Taormina, Italy, Oct 2004.

[13] T. Karagiannis et al, "Is P2P dying or just hiding?", GLOBECOM 2004, pp.1532-1538, Dallas, TX, USA, Nov 2004.

[14] A. Moore et al, "Toward the Accurate Identification of Network Applications," PAM 2005, Boston, Apr 2005.

저 자 소 개



엄 남 경(Um nam-kyoung)

1999년2월 충북대학교 컴퓨터과학과 졸업

2002년2월 충북대학교 전자계산학과 석사

2007년8월 충북대학교 전자계산학과 박사

〈관심분야〉 유비쿼터스네트워크, 네트워크보안, 침입탐지시스템, 프로토콜테스팅

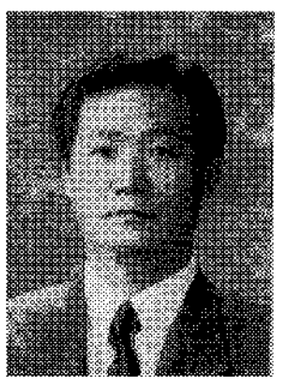
우 성 희(Woo sung-hee)

1992년2월 충북대학교 전자계산학과 박사

1995년9월~2006년2월 청주과학대학 컴퓨터과학과 부교수

2006년3월~현재 충주대학교 전기전자 및 정보공학부 교수

〈관심분야〉 네트워크보안, 침입탐지시스템, 프로토콜 테스팅



이 상 호(Lee sang-ho)

1976년2월 숭실대학교 전자계산학과 졸업

1981년2월 숭실대학교 전자계산학과 석사

1989년2월 숭실대학교 전자계산학과 박사

1981년6월~현재: 충북대학교 전기전자 및 컴퓨터공학부 교수

〈관심분야〉 통신 프로토콜 공학, 네트워크 관리, 네트워크 보안