네트워크 트래픽 분포 엔트로피를 이용한 비정상행위 탐지 방법

강 구 홍[†] · 오 진 태[††] · 장 종 수[†††]

요 약

악의적인 네트워크 트래픽은 흔히 공격의 성질을 구체적으로 알지 않고서도 평상시 트래픽과 구별된다. 본 논문에서는 네트워크 인바운드 트래픽 분포를 이용해 네트워크 트래픽 비정상행위를 탐지하는 방법을 제시한다. 이를 위해 먼저 실제 캠퍼스 네트워크의 트래픽 특성을 프로토콜, 패킷 길이, 목적지 IP/포트 주소, TTL 값, TCP SYN 패킷, 그리고 프래그멘트 패킷 분포 등을 통해 조사하였다. 이렇게 구해진 다양한 베이스라인 트래픽 분포로부터 엔트로피를 계산하고 이를 기준으로 비정상행위를 탐지하는 방법을 제시하였다. 특히 본 논문에서는 잘 알려진 서비스거부공격을 실제 캠퍼스 네트워크를 대상으로 실시하였고 그 결과를 제시함으로서 제안된 기법의 타당성을 검증하였다.

키워드 : 비정상행위, 침입탐지, 네트워크 보안, 엔트로피

Anomaly Detection Method Using Entropy of Network Traffic Distributions

Kang, Koo Hong[†] · Oh, Jin Tae[††] · Jang, Jong Soo[†††]

ABSTRACT

Hostile network traffic is often different from normal traffic in ways that can be distinguished without knowing the exact nature of the attack. In this paper, we propose a new anomaly detection method using inbound network traffic distributions. For this purpose, we first characterize the traffic of a real campus network by the distributions of IP protocols, packet length, destination IP/port addresses, TTL value, TCP SYN packet, and fragment packet. And then we introduce the concept of entropy to transform the obtained baseline traffic distributions into manageable values. Finally, we can detect the anomalies by the difference of entropies between the current and baseline distributions. In particular, we apply the well-known denial-of-service attacks to a real campus network and show the experimental results.

Key Words : Anomaly, Intrusion Detection, Network Security, Entropy

1. 서 론

오늘날 산업, 정부, 그리고 심지어 일반 개인 생활이 인터넷에 점점 더 의존해 감에 따라 네트워크를 통한 정보 흐름에 관한 중요성이 더욱 강조되고 있다. 그러나 해커들에 의한 네트워크 혹은 주요 서버 컴퓨터에 대한 침입이나 공격은 네트워크를 마비시키거나 서비스거부공격(DoS: Denial of Service)으로 인해 전자 상거래 서비스 중단과 같은 심각한 경제적 손실뿐만 아니라 인터넷 서비스 중단에 따른 극심한 사회적 혼란을 초래하고 있다. 침입탐지시스템(IDS: Intrusion Detection System)은 이러한 악의적인 공격으로부터 컴퓨팅 시스템 혹은 네트워크를 보호하는 장치이다[1-3].

IDS는 공격을 탐지하는 방법에 따라 시그너처(signature) 기반과 비정상행위(anomaly) 기반으로 구분된다. 시그너처 기반 IDS는 Snort 혹은 Bro와 같은 보안 전문가들에 의해 만들어진 규칙(rule)을 사용하여 잘 알려진 공격(known attacks)를 확인하기 위해 트래픽을 검사한다[1]. 그러나 새로운 형태, 즉 공격의 규칙이 아직 확인되지 않은 새로운 공격에 대해서는 탐지가 불가능한 단점을 가지고 있다. 이에 반해, 비정상행위 기반 IDS는 일반 혹은 정상 트래픽을 모델링한다. 악의적인 트래픽은 흔히 이러한 정상 트래픽 모델을 벗어나게 되며 IDS 시스템은 이를 감지하게 된다. 따라서 비정상행위 기반 시스템은 규칙이 만들어질 필요가 없기 때문에 새로운 공격을 탐지할 수 있다. 그러나 공격의 가능성만 알려줄 뿐 공격의 성격을 밝혀내지는 못하며 정상 트래픽이 경우에 따라 모델을 벗어날 수 있어 오탐(false alarms)을 발생시킬 수 있다[3].

본 논문에서 제안하는 새로운 네트워크 트래픽 비정상행위 탐지 방법은 인터넷 프로토콜의 각종 헤더 정보에 기반

† 정 회 원 : 서원대학교 컴퓨터정보통신공학부 조교수
†† 정 회 원 : 한국전자통신연구원 네트워크보안그룹 팀장
††† 정 회 원 : 한국전자통신연구원 네트워크보안그룹 그룹장
논문접수 : 2005년 11월 1일, 심사완료 : 2006년 4월 4일

한다. 이런 유형의 기존 비정상행위 탐지 시스템은 "패킷 헤더 필드 값의 학습"에 의존하고 있다. 즉 평소 이들 헤더 내 필드의 값을 학습하고 자신이 학습한 이외의 값들이 들어오게 되면 적절한 알고리즘을 통해 비정상행위를 선언하게 된다[7-9]. 그러나 본 논문에서는 이들 헤더 정보로부터 다양한 트래픽 분포를 조사하고 이들 수집된 분포만을 이용해 트래픽 비정상행위를 탐지하는 방법을 제안한다. 한편 수집된 트래픽 분포를 이용하여 비정상행위를 탐지하기 위해 엔트로피(entropy) 개념을 도입하였으며, 궁극적으로 이들 트래픽 분포로부터 엔트로피를 계산해 비정상행위를 탐지하게 된다.

서론에 이어 제2장에서는 트래픽 분석을 통한 기존의 검출 방법을 간략히 설명하고 본 논문에 대한 보다 자세한 연구 동기를 기술한다. 제3장에서는 캠퍼스 네트워크의 인바운드 트래픽 조사를 위한 실험 환경 및 관련 기술을 설명하고 수집된 트래픽 분포를 기준으로 캠퍼스 네트워크 트래픽 특성을 분석한다. 제4장에서는 비정상행위 탐지를 위한 엔트로피 개념을 설명하고, 가장 흔히 해커들이 사용하고 있는 DoS 공격툴을 이용해 실질적인 트래픽의 변화를 보여주고 이를 이용한 비정상행위 탐지 과정을 보여준다. 제5장에서 결론과 향후 연구방향에 대해 기술한다.

2. 연구 동기

2.1 기존 검출 방법

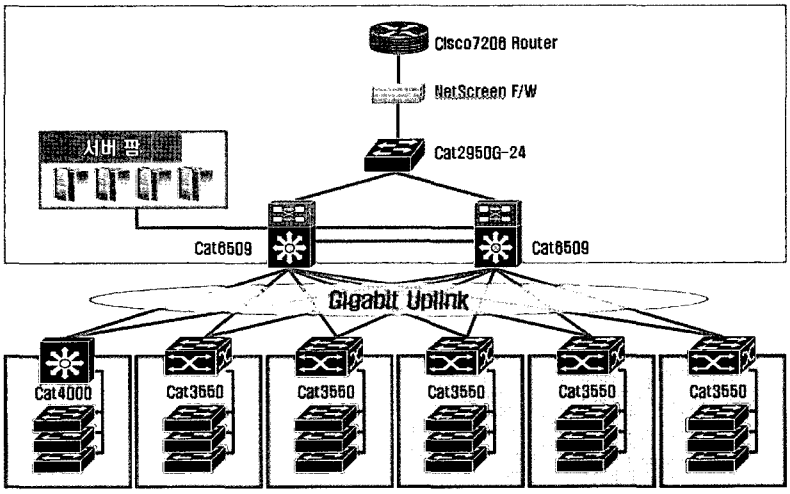
트래픽 분석을 통해 비정상행위를 검출하기 위한 기존의 방법은 크게 두 가지 카테고리로 구분된다. 즉 단순히 트래픽 볼륨의 변화를 조사하기위해 트래픽을 타임시리즈로 모델링[4-6]하거나 패킷 헤더 내 필드 값을 학습하는 방법[7, 8]을 채택하고 있다.

첫 번째 방법은 패킷 헤드 정보, 즉 TCP/IP 프로토콜 속성을 검사하여 이를 기반으로 비정상행위를 탐지한다. 이러한 방법은 오늘날 많은 공격들이 비정상적인 TCP 플래그 혹은 IP 옵션, 유효하지 않은 일련번호(sequence number), 잘못된 체크섬(checksum), 위장된 주소(spoofed address) 등을 이용하기 때문이다. 특히, PHAD(Packet Header Anomaly Detector) 방법은 데이터링크 (이더넷), 네트워크 (IP, ICMP), 트랜스포트 계층 (TCP, UDP)의 각 패킷 헤더 필드 내 정상적인 값의 범위를 학습하기위해 공격이 없는 트래픽에서 이들 필드 값들을 학습한다. 학습기간 동안 적어도 한번 이상 발생하는 이들 필드 값들을 기록하고 새로운 필드 값이 최초로 관찰될 경우 이를 비정상행위로 간주한다. 따라서 학습기간 동안 각 필드에 대한 비정상행위 발생 확률 $P(=r/n)$는 해당 필드를 가진 패킷이 입력된 수 n과 해당 필드의 비정상행위 수 r에 의해 결정된다. 한편, PHAD는 실제 비정상행위 검출을 위해 하나의 패킷이 입력될 때마다 학습한 P를 사용하여 패킷 스코어를 계산하고 이를 이용해 비정상행위를 검출하는 방법을 사용하였다[7, 8].

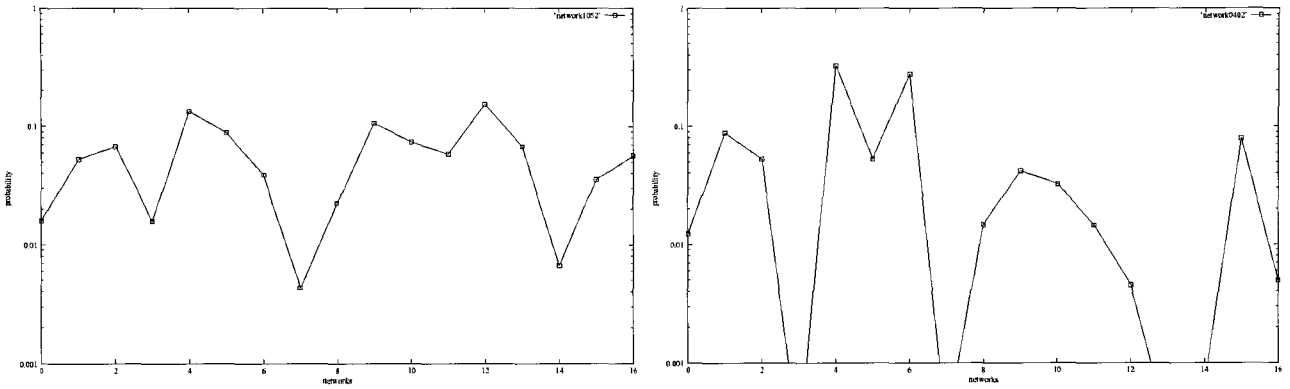
두 번째 방법은 네트워크 트래픽을 타임 시리즈로 모델링하고 이 모델링으로부터 정상 트래픽을 정의하기 위해 통계적 편차(statistical deviations)를 결정한 다음 이들로부터 벗어나는 트래픽을 네트워크 비정상행위로 탐지하는 방법이 있다[4-6]. 이러한 타임시리즈 모델링 방법은 시간의 변화에 따른 트래픽 변화를 정확히 예측할 수 있어야 한다. 특히 트래픽 변화 패턴은 하루 혹은 계절적 변화에 따른 주기적 특성과 사회적 사건 혹은 새로운 소프트웨어 릴리즈 등과 같은 일시적인 변화를 잘 반영할 수 있어야 한다. Holt-Winters 예상 알고리즘[6]을 이용한 타임시리즈 모델링의 경우, 세 가지 요소 즉 베이스라인, 선형 추이, 그리고 계절적 추이를 고려하여 트래픽 변화를 예측한다. 한편 wavelet 분석[4, 5]을 이용한 주파수 대역별 세분화를 통해 트래픽 변화를 추적하고 계층화된 이들 트래픽 변화 추이를 기준으로 단기, 중기, 그리고 장기적인 비정상행위를 검출한다. 그러나 이러한 방법은 결국 시간에 따른 트래픽 볼륨 변화를 예상하는 방법으로 요약할 수 있다.

2.2 새로운 접근 방법

다음 (그림 1)은 본 연구를 통해 사용될 캠퍼스 네트워크 구성도이다. 이중화된 두 개의 기가비트 백본 스위치를 중



(그림 1) 캠퍼스 네트워크 구성도



(a) 10:52 (b) 04:02

(그림 2) 인바운드 트래픽의 목적지 IP 주소의 서브 네트워크별 확률분포

심으로 서버팜(server farm)과 각 빌딩별로 서브네트워크들이 구성되어 있으며 17개의 클래스 C 네트워크 ID를 가지고 있다. 본 연구의 목적상 바이러스 월과 IDS 장비들은 (그림 1)에서 나타내지 않았으며 이들 장비의 영향을 최소로 줄이기 위해 보드 라우터(BR: border router) 인바운드 트래픽의 분포를 조사해 모델링하였다. 한편, 이러한 형태의 네트워크 토폴로지는 캠퍼스 네트워크뿐만 아니라 일반 엔터프라이즈급 네트워크에서도 흔히 볼 수 있는 구성도이다.

먼저, 본 연구의 첫 번째 연구 동기는 캠퍼스 네트워크의 인바운드 트래픽 특성을 파악하는 것이다. 즉 네트워크 관리자들은 네트워크 보안 혹은 트래픽 엔지니어링 등을 위해 외부로부터 보호해야할 자신의 네트워크로 어떤 형태의 트래픽이 들어오고 있는지 매우 궁금해 한다. 물론 시간에 따른 단순 트래픽 양이나 프로토콜 분포 등은 여러 가지 방법을 이용해 수집할 수 있다. 그러나 보안상 혹은 기술적 문제로 인해 이러한 자료들을 공식적인 문서 혹은 논문을 통해 찾아보기란 쉽지 않다. 본 논문에서는 실제 캠퍼스 네트워크의 트래픽 특성을 프로토콜, 패킷 길이, 목적지 IP/포트 주소, TTL 값, TCP SYN 패킷, 그리고 프래그멘트 패킷 분포 등을 통해 보다 구체적으로 조사하였다. 따라서 본 논문을 통해 제시될 이들 분포들은 캠퍼스 네트워크의 트래픽 엔지니어링과 보안 등과 같은 연구를 위해 훌륭한 연구 자료가 될 것임을 확신한다.

이제 본 연구의 두 번째 연구 동기는 네트워크 비정상행위 탐지이다. (그림 1)의 네트워크 구성에서 네트워크 사용 패턴을 한번 상상해 보자. 이들 네트워크 사용 패턴을 추적하면 다음과 같은 사실들이 쉽게 예상된다.

- 주중과 주말, 평일과 공휴일, 그리고 시간대 별로 상이한 네트워크 사용 패턴을 유지
- 각 서브 네트워크 별로 서로 다른 네트워크 사용 패턴을 유지

만약 우리가 외부 인터넷 망에서 BR로 유입되는 인바운드 트래픽의 IP 패킷의 목적지 주소를 관찰한다고 가정해 보자. 그리고 이들 목적지 IP 주소를 서브네트워크 별 확률분포를 구한다고 가정해 보자. (그림 2)는 본 연구를 통해 조사된 BR의 인바운드 트래픽의 목적지 별 IP 서브 네트워크 확률분포이다. (그림 2) (a)는 10:52, 그리고 (b)는 04:02 분에 각각 조사된 결과다. 우리는 이들 두 그림으로부터 시간대 별로 분명 서로 다른 확률분포를 가진다는 사실을 확인할 수 있다. 이러한 결과는 각 서브 네트워크 별로 서로 다른 네트워크 사용 패턴을 가질 것이 분명하기 때문에 우리가 쉽게 예상할 수 있었든 결과이기도 하다. 즉 저녁 늦게 새벽까지 컴퓨터를 사용하는 빌딩과 근무시간 이외에는 거의 네트워크를 사용하지 않는 빌딩과는 네트워크 사용 패턴이 같을 수가 없을 것이다. 따라서 평소와는 다른 네트워크 사용 패턴을 탐지할 수 있다면 이것은 분명 우리가 네트워크 비정상행위를 탐지할 수 있는 좋은 접근법이 될 것이다.

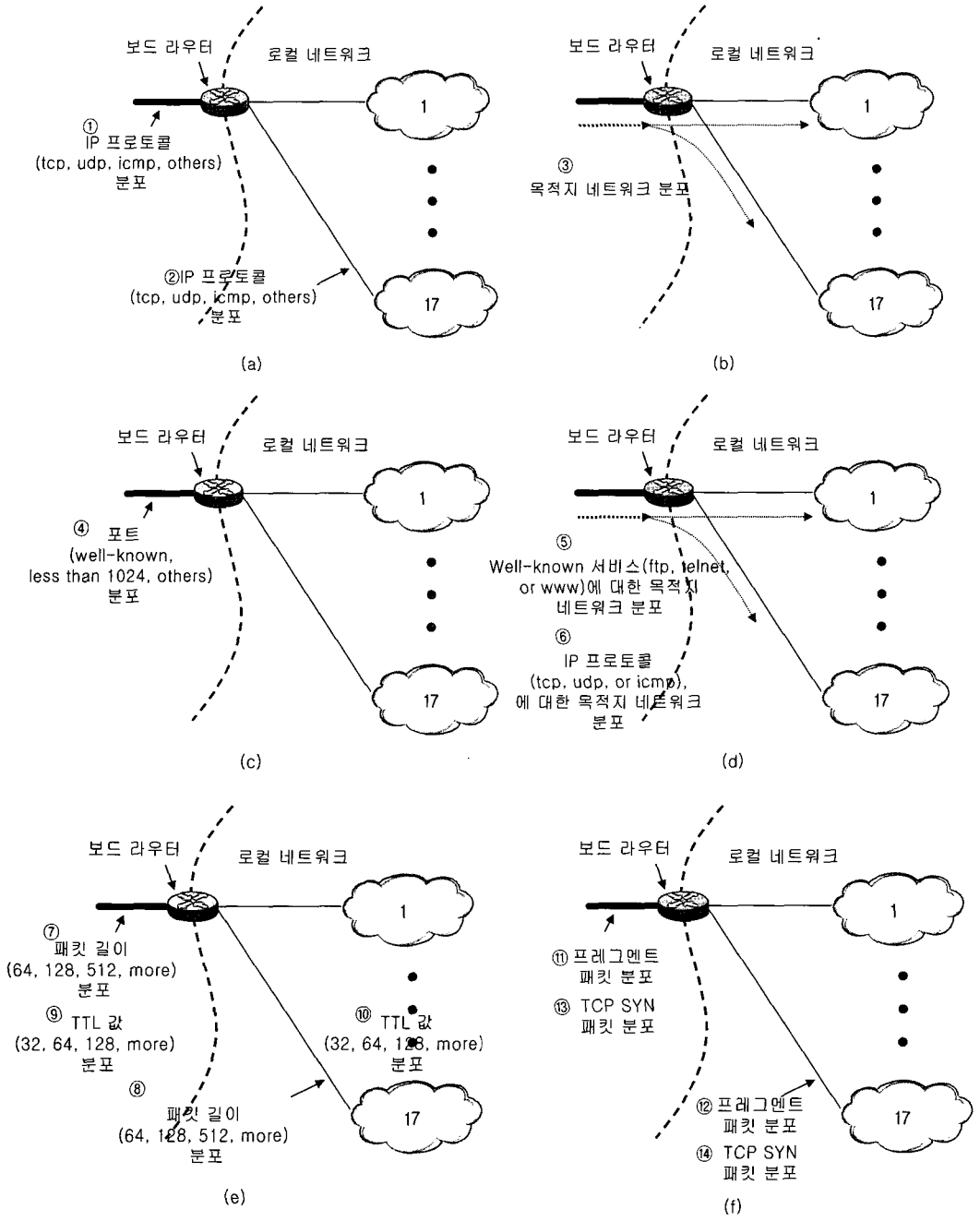
이제 또 하나의 문제점이 남았다. 비록 우리가 다양한 네트워크 사용 패턴에 대한 확률분포를 구했다고 가정하여도 이를 비정상행위 탐지에 어떻게 이용할 것 인가?에 있다. 즉 평상시의 정상적인 확률분포와 현재의 확률분포를 어떤 방법으로 비교할 것인가? 가장 쉽게 생각할 수 있는 것이 확률분포를 근간으로 한 모멘텀(moments)를 계산해 비교하는 것이 될 것이다. 예를 들면, 평균치와 표준편차가 될 것이다. 그러나 본 연구에서는 좀 더 새로운 접근을 시도하기로 한다. 즉 엔트로피 개념을 사용한다. 엔트로피는 하나의 변수에 대한 불확실성의 정도를 나타내는 정보이론의 측정단위이다[11](엔트로피 개념은 4.2절에서 상세히 설명). 따라서 (그림 2)를 기준으로 (그림 2) (a)는 (b)와 비교해 상대적으로 엔트로피가 높게 된다. 결국 본 논문에서 조사한 다양한 트래픽 분포로부터 엔트로피를 계산하여 이를 이용해 트래픽 분포의 비정상적인 분포를 탐지할 수 있다.

3. 캠퍼스 네트워크 트래픽 분포

3.1 조사 대상 트래픽 분포

본 논문에서는 (그림 3)과 같이 로컬 네트워크 (보호할 대상 네트워크)의 외부 인터넷 연결을 위한 BR에서 인바운드 트래픽 특성을 조사한다. 조사할 트래픽 분포의 종류는 비정상행위 탐지에 직접 관련됨으로 적절하게 선정되어야 한다.

먼저, (그림 3) (a)는 IP 프로토콜의 종류를 조사한다. 이

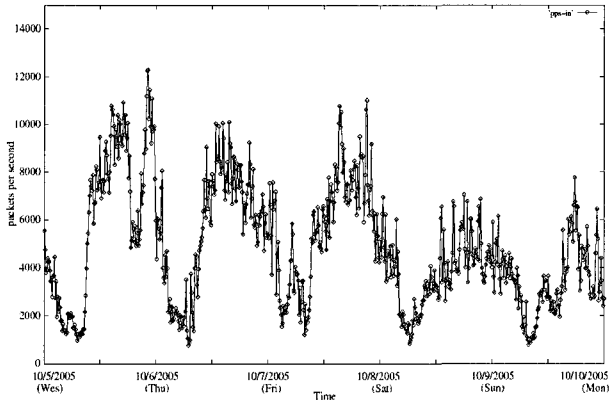


(그림 3) 트래픽 분포 조사 대상

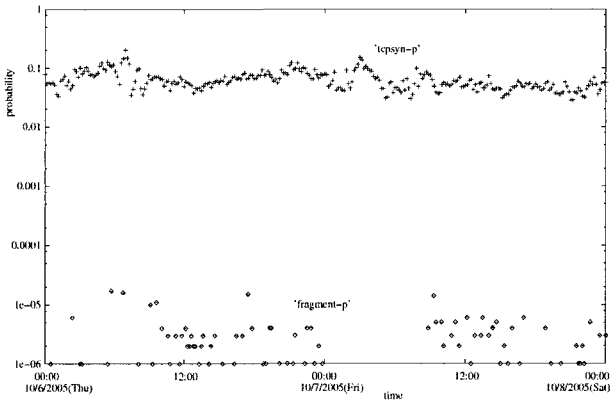
때 IP 프로토콜 종류는 네 가지 즉 TCP, UDP, ICMP, 그리고 이들 외의 모든 프로토콜로 구분한다. 또한 각 서브네트워크 별 IP 프로토콜 분포를 조사한다. (그림 3) (b)는 목적지 IP 주소 분포를 각 서브네트워크를 기준으로 조사한다. (그림 3) (c)는 목적지 포트 주소 분포를 세 가지 즉 잘 알려진(well-known) 포트 (20(ftp), 21(ftp), 23(텔넷), 25(SMTP), 53(DNS), 80(HTTP), 111(RPC), 161(SNMP)), 1024 보다 작은 경우, 그리고 1024 보다 큰 경우로 구분하여 분포를 조사하였다. (그림 3) (d)는 잘 알려진 서비스 즉 ftp, 텔넷, 그리고 웹 서비스의 경우 목적지 서브네트워크 분포를 조사하고, IP 프로토콜에 즉 TCP, UDP, 그리고 ICMP의 목적지 서브네트워크 분포를 조사한다. 따라서 이들은 조건(conditional) 분포가 된다. (그림 3) (e)는 BR의 인바운드 트래픽과 각 서브네트워크에서 IP 패킷 길이 분포를 조사한다. 이때 패킷 길이는 네 가지 즉 64 바이트 보다 작은 경우, 64-128 바이트의 경우, 128-512 바이트의 경우, 그리고 512 바이트 보다 큰 경우로 구분한다. 또한 BR의 인바운드 트래픽과 각 서브네트워크에서 IP 패킷의 TTL(Time to Live) 필드 값 분포를 조사한다. 이때 TTL 필드 값은 네 가지 즉 32 보다 작은 경우, 32-64의 경우, 64-128의 경우, 그리고 128 보다 큰 경우로 구분한다. 마지막으로 (그림 3) (f)는 BR의 인바운드 트래픽과 각 서브네트워크 별 TCP SYN 패킷 분포를 조사

〈표 1〉 조사 대상 트래픽 분포

번호	분포	대상	번호	분포	대상
1	IP 프로토콜 분포	전체	8	패킷 길이 분포	네트워크 별
2	IP 프로토콜 분포	네트워크 별	9	TTL 값 분포	전체
3	목적지 네트워크 분포	전체	10	TTL 값 분포	네트워크 별
4	포트 분포	전체	11	fragment 패킷 분포	전체
5	well-known 서비스에 대한 목적지 네트워크 분포	전체	12	fragment 패킷 분포	네트워크 별
6	IP 프로토콜에 대한 목적지 네트워크 분포	전체	13	TCP SYN 패킷 분포	전체
7	패킷 길이 분포	전체	14	TCP SYN 패킷 분포	네트워크 별



(그림 4) 4일간 BR의 인바운드 트래픽 양(pps: packets per second)



(그림 5) TCP SYN 패킷 및 프래그멘트된 패킷의 확률

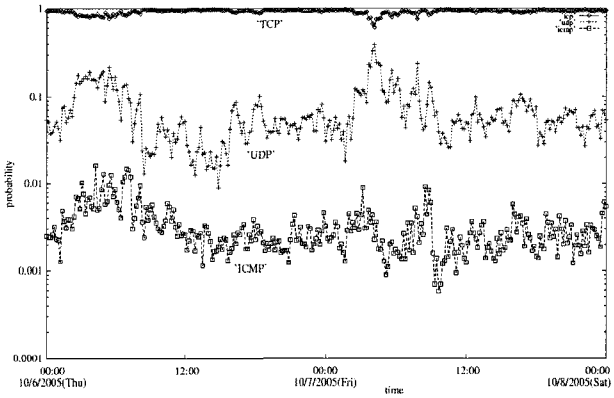
한다. 이들을 요약하면 <표 1>과 같다.

3.2 캠퍼스 네트워크 트래픽 특성

본 절에서는 제3.1절에서 설명한 (표 1)의 조사대상 트래픽 분포를 중심으로 캠퍼스 네트워크의 트래픽 특성을 알아보도록 한다. 그러나 지면의 제약성을 감안해 조사된 일부 흥미로운 자료만 제시하도록 한다. (그림 4)는 주말을 포함한 5일 (2005년 10월 5일 수요일 00:00시-9일 일요일 24:00시) 동안 BR의 입력 트래픽을 초당 패킷 수(pps : packets per second)로 나타내었다 (본 논문에서 제시된 모든 자료들은 모두 10분마다 측정된 값을 기준으로 계산하였다). 이미 기존의 여러 논문에서 밝혀진 바와 같이 트래픽 양은 하루를 주기로 반복적인 패턴을 보여준다. 그러나 캠퍼스 네트워크의 특성 상, 주말의 트래픽 양이 주중에 비해 작으나 일반 엔터프라이즈 네트워크와는 달리 현저한 차이를 보이는 것은 아니다. 이런 현상은 주말 역시 많은 사용자들이 캠퍼스 내에 존재한다는 사실이다. 이제 이들 구간 중 6일(목요일)과 7일(금요일) 이틀 동안 관찰된 다양한 트래픽 특징을 알아보자.

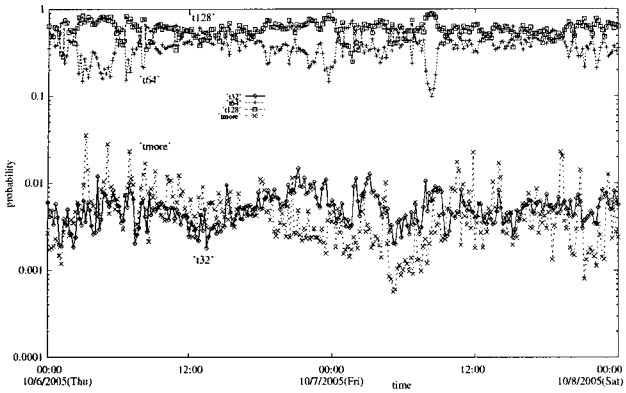
(그림 5)는 프래그멘트된 IP 패킷과 TCP SYN/SYNACK 패킷의 확률을 보여준다. 그림을 통해 프래그멘트된 IP 패킷이 들어올 확률은 10^{-5} 이하이고 SYN 플래그가 세팅된 TCP 패킷이 들어올 확률은 $10^{-2}-10^{-1}$ 수준에 있음을 확인할 수 있다. 특히 이러한 특징은 하루를 통해 일정하게 유지됨을 확인할 수 있다. 즉 특별한 주기성을 찾을 수는 없다.

(그림 6)은 IP 프로토콜의 분포를 보여준다. 이미 우리가 예상한 바와 같이 TCP가 대부분을 차지하고 있음을 확인할 수 있다. 그러나 네트워크 사용이 상대적으로 감소한 새벽

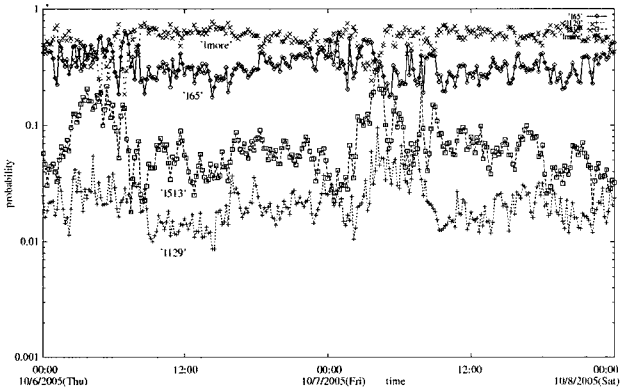


(그림 6) IP 프로토콜 (TCP, UDP, ICMP)의 확률

시간대(02:00-07:00에는 UDP와 ICMP 패킷이 다소 증가하는 미세한 주기적 패턴을 보여준다. (그림 7)은 IP 패킷의 TTL 필드 값의 분포를 보여준다. 그림으로부터 $32 \leq ttl < 64$와 $64 \leq ttl < 128$ 가 대부분을 차지하고 있으며, 네트워크 사용량이 많은 09:00-19:00 사이에서는 다른 시간대에 비해 상대적으로 일정한 패턴을 유지하고 있음을 확인할 수 있다. (그림 8)은 IP 패킷의 길이 분포를 보여준다. 그림으로부터 513바이트 이상 혹은 64바이트 이하의 긴 패킷들이 대부분을 차지하고 있음을 확인할 수 있다. 그러나 새벽 시간대에는 513 바이트의 패킷 분포 ($129 \leq length < 513$)가 다소 증가함을 볼 수 있다. 이것은 (그림 6)에서 관찰한 UDP 패킷의 증가와 관련된 현상으로 판단된다. (그림 9)는 목적지 포트 번호에 대한 분포를 보여준다. 그림으로부터 1024번 이상의 목적지 포트 번호가 대부분을 차지하고 있음을 확인할 수 있다.



(그림 7) IP 패킷의 TTL 필드 값(t32 ($ttl < 32$), t64($32 \le ttl < 64$), t128($64 \le ttl < 128$), tmore($ttl \ge 128$))의 확률



(그림 8) IP 패킷의 길이 필드 값(l65 ($length < 65$), l129 ($65 \le length < 129$), l513($129 \le length < 513$), lmore ($length \ge 513$))의 확률

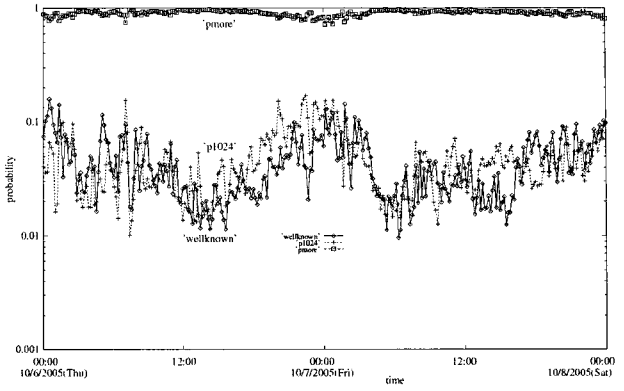
(그림 10)은 IP 패킷의 목적지 IP주소를 17개의 로컬 네트워크 ID를 기준으로 분포를 보여준다. 이미 (그림 2)를 통해 언급한 바와 같이 네트워크 사용량이 많은 09:00-19:00 사이에서는 이들 분포가 비교적 균일한 반면, 이들 시간대 이외에서는 네트워크 사용이 일부 로컬 네트워크에 편중되어 있음을 확인할 수 있다.

이상과 같이 조사된 각종 트래픽 특성들은 네트워크 트래픽 비정상행위를 탐지하기 위한 베이스라인 모델로서 사용될 것이다.

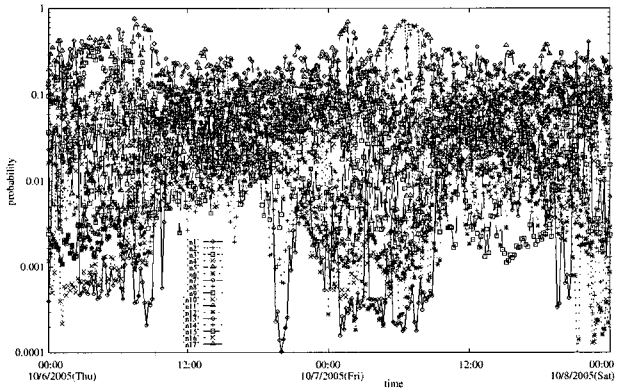
4. 네트워크 트래픽 비정상행위 탐지

4.1 DoS 공격에 따른 네트워크 트래픽 분포 변화

비정상행위 탐지를 실제 네트워크에 적용해 실험하기란 쉬운 작업이 아니다. 비정상행위가 의미하듯이, 알려지지 않은 공격을 시도하여 이들 공격의 탐지 여부를 보여야 할 것이다. 이러한 실험을 위한 인위적인 비정상행위 공격 이외에 실제 네트워크에서 발생되는 각종 비정상행위를 통합해 실험하기 위해서는 오랜 시간에 걸친 자료 수집 및 수집된 트래픽 자료를 분석해 비정상행위를 정의해야 하는 어려움이 있다. 따라서 본 논문에서는 이미 알려진 몇몇 DoS 공격



(그림 9) IP 패킷의 목적지 포트 번호(wellknown (포트 번호 = well-known port(20, 21, 23, 80)), p1024(포트 번호 < 1024(well-known port 제외), pmore(포트 번호 ≥ 1024))의 확률



(그림 10) BR의 인바운드 트래픽에 대한 목적지 네트워크의 분포

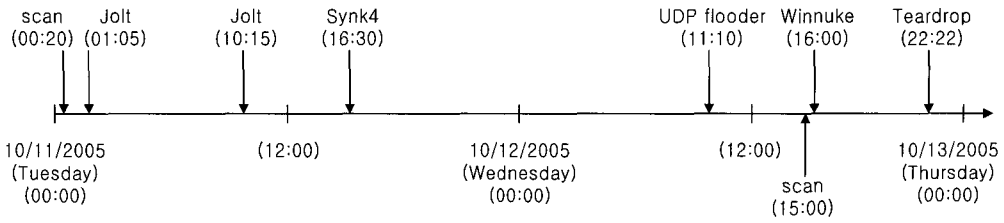
(표 2) 사용된 DoS 공격 툴

DoS 공격 툴	특징
Ping of Death (Jolt)[16]	IP 패킷의 최대길이 이상을 가진 ICMP 패킷 전송
winnuke[12]	포트 139번으로 "junk"(쓰레기) 정보 전송
Synk4[13]	TCP SYN flooder 공격
Teardrop[17]	프래그먼트 오프셋을 이용한 버퍼 넘침
UDP flooder[15]	UDP flooder 공격

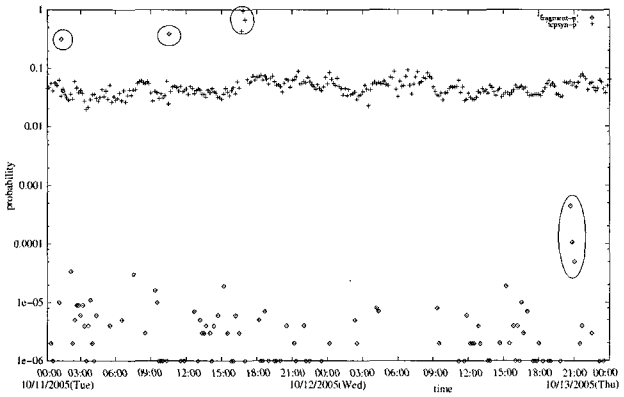
용 툴을 사용한 인위적인 방법을 채택하였다.

먼저, 리눅스용 스캔(scan) 툴인 nmap[14]과 DoS 공격 툴인 datapool[11] 소스코드를 사용하여 앞에서 설명한 (그림 1)의 실제 컴퍼스 네트워크를 대상으로 외부 망에서 공격을 시도하였다. 이때 다음 (표 2)와 같이 이미 알려진 Syn4k, Winnuke, Jolt, UDP flooder, teardrop DoS 공격과 호스트/포트 스캔을 시도하였으며 공격 시간은 각각 (그림 11)과 같다. 참고로, 결과 그래프를 잘 표현하기 위해 2일간에 걸쳐 공격을 시도하였다.

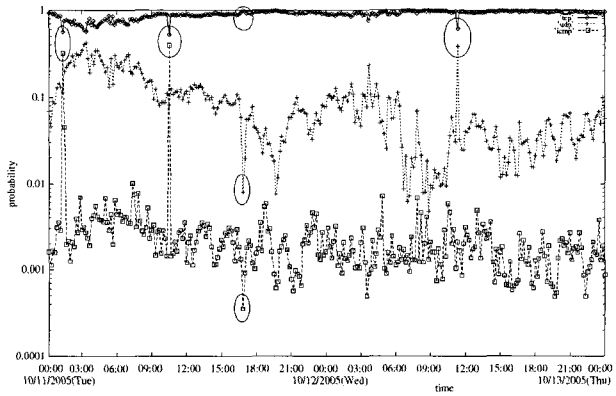
(그림 12)는 입력 IP 패킷이 프래그멘트되었을 확률과 TCP SYN 플래그가 '셋팅' 되어 있을 확률을 각각 보여준다. IP 프래그멘테이션을 이용하는 jolt 공격인 경우 평소 10^{-5} 수준을 크게 넘어서는 것을 확인할 수 있으며 TCP



(그림 11) 공격 종류 및 시점



(그림 12) TCP SYN 패킷 및 프래그멘트된 패킷의 확률

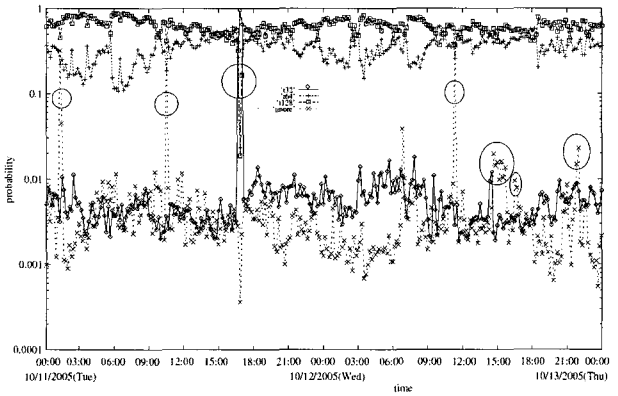


(그림 13) IP 패킷 프로토콜 분포

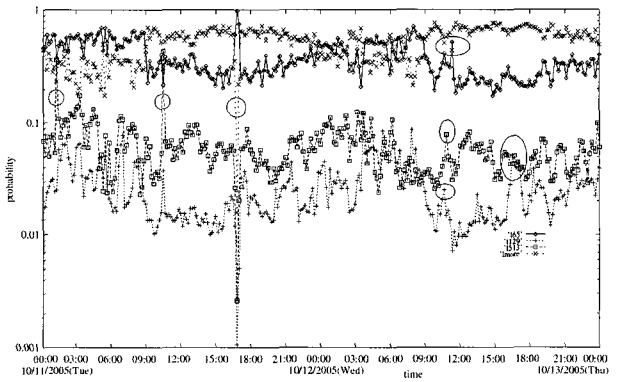
SYN 플러딩을 이용하는 synk4 공격인 경우 평소 0.1 수준을 크게 넘어선다. 따라서 망 관리자가 단순히 이들 두개의 확률만 제대로 추적한다고 해도 외부로부터 들어오는 많은 공격을 탐지할 수 있으리라 판단된다. 그러나 플러딩(flooding) 공격 형태가 아닌 winnuke, teardrop 공격, 그리고 스캔 공격은 이들 분포로부터 쉽게 확인되지 않는다. 참고로, 10월 12일 20:40-21:00 탐지되는 과도한 프래그멘트 확률은 인위적으로 시도된 공격이 아닌 실제 네트워크에서 발생된 비정상행위 시점으로 판단된다. 이에 대한 논의는 (그림 16)에서 다시 언급하기로 한다.

(그림 13)은 입력 IP 패킷의 프로토콜 필드의 분포를 보여준다. ICMP를 이용하는 jolt 공격, TCP를 이용하는 synk4 공격, 그리고 UDP를 이용하는 udpflooder 공격 시점에 해당 프로토콜 분포의 현저한 변화를 보인다.

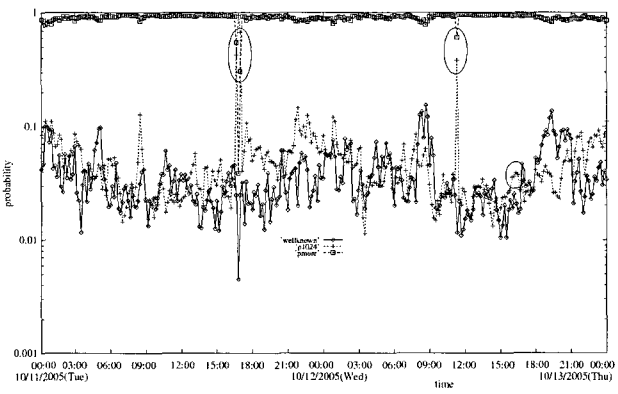
(그림 14)는 IP 패킷의 TTL 필드 값의 분포를 보여준다. 우리는 (그림 11)에서 시도한 모든 공격을 (그림 14)를 통해



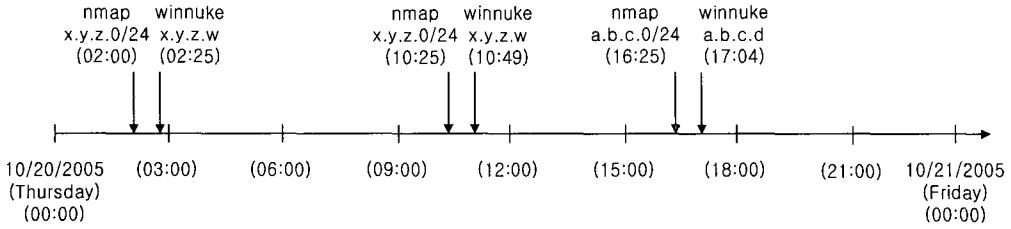
(그림 14) IP 패킷의 TTL 필드 값(t32 ($ttl < 32$), t64($32 \le ttl < 64$), t128($64 \le ttl < 128$), tmore($ttl \ge 128$))의 확률



(그림 15) IP 패킷의 길이 필드 값(l65 ($length < 65$), l129 ($65 \le length < 129$), l513($129 \le length < 513$), lmore ($length \ge 513$))의 확률



(그림 16) IP 패킷의 목적지 포트 번호(wellknown (포트 번호 = well-known port(20, 21, 23, 80)), p1024(포트 번호 < 1024(well-known port 제외), pmore(포트 번호 ≥ 1024))의 확률



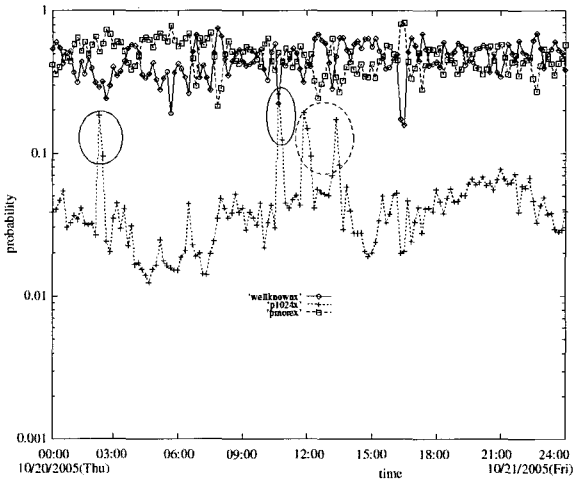
(그림 17) 포트-스캔 및 winnuke 공격

확인할 수 있으며, 특히 nmap에 의한 호스트/포트 스캔에 이은 winnuke 공격이 확인된다. 이러한 분포 변화에 대해서는 하나의 특정 외부 컴퓨팅 시스템에서 공격을 시도하고 있으며, 사용하는 공격 툴에 그 원인이 있는 것으로 판단된다. 따라서 이 분포가 비정상행위 탐지에 실질적으로 이런 정도로 효과적일지는 좀 더 세심한 연구가 진행될 예정이다.

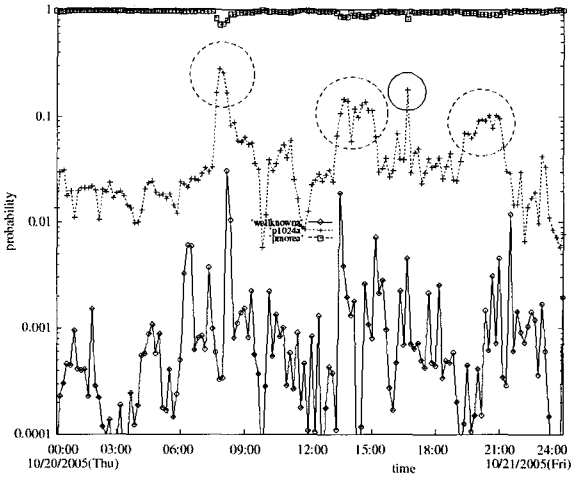
(그림 15)는 IP 패킷의 패킷길이 분포를 보여준다. 프래그멘테이션 및 짧은 패킷을 사용하는 공격은 이 분포를 통해 쉽게 탐지할 수 있다. (그림 16)은 목적지 포트주소 분포를 보여준다. 특정 포트를 공격하는 DoS 공격은 이 분포를 통해 쉽게 탐지된다. 그러나 winnuke 공격의 경우 139번 포트의 공격에 따른 트래픽 분포의 변화를 감지할 수는 있으나 그 변화의 폭이 우리가 원하는 수준만큼 크지 않음을 알 수 있다. 한편, (그림 12)를 통해 설명한 바와 같이 10월 12일 20:40-21:00에 탐지된 과도한 프래그멘트 패킷의 확률은 (그림 16)을 통해 잘 알려진(well-known) 포트로 집중되었음을 확인할 수 있다. 따라서 우리는 이 시점에 본 연구진에의해 인위적으로 만들어지지 않은 비정상행위로 의심할 수 있다.

(그림 12)에서 (그림 16)까지는 모두 BR의 인바운드 트래픽을 기준으로 수집되었음을 다시 한번 밝혀둔다. 따라서 플러딩 형태의 공격이 아닌 winnuke, teardrop, 그리고 스캔 공격들을 이들 그림으로부터 뚜렷하게 확인할 수 없는 것은 어떻게 보면 당연한 것인지 모른다. 즉 많은 트래픽이 중첩된 상태에서는 이들 분포의 변화를 확인하기란 쉽지 않을 것이다. 따라서 이제 포트 스캔과 winnuke 공격에 대해 해당 희생(victim) 서브네트워크 트래픽 분포의 변화를 확인해 보기로 한다. 다음 (그림 17)은 nmap을 이용한 스캔 공격과 winnuke 공격 시점을 각각 보여준다. 하루 동안 세 번의 공격을 시도하였으며 각각의 공격은 약 10-15분간 지속되었다. 한편 성격이 서로 다른 두 개의 서브네트워크를 공격대상으로 선택하였으며 (그림 17)에서 보여지는 x.y.z.0/24 네트워크는 서버팜이 존재하는 네트워크이다.

(그림 18)과 (그림 19)는 각 서브네트워크에 대한 IP 패킷의 목적지 포트주소의 분포를 보여준다. 이미 예상한 바와 같이 네트워크 x.y.z.0/24에는 well-known 포트로 향하는 트래픽이 상당 수준에 이르고 있으며 네트워크 a.b.c.0/24에는 대부분 1024 이상의 포트번호가 차지하고 있다. 한편 139번 포트를 공격하는 winnuke의 영향을 이들 두 그림을 통해 확인할 수 있다. 따라서 플러딩 형태가 아닌 특정 포트를 공격하는 비정상행위는 트래픽 중첩의 효과가 비교적 적은 서브네트워크 분포의 변화를 관찰해야만 한다. 한편, 이들



(그림 18) 네트워크 x.y.z.0/24 에 대한 IP 패킷 목적지 포트주소 분포

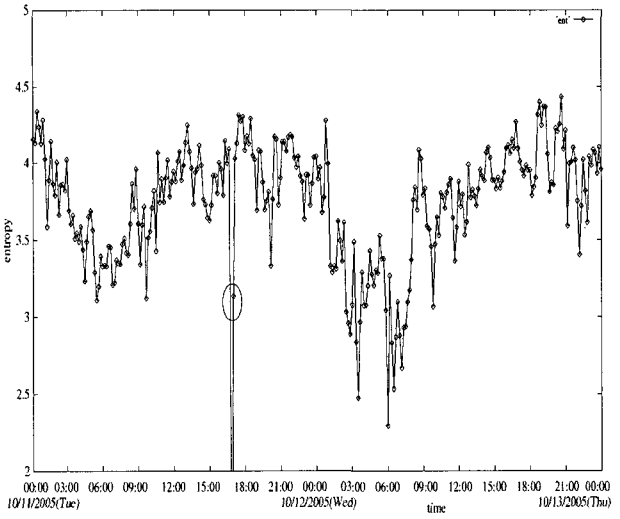


(그림 19) 네트워크 a.b.c.0/24 에 대한 IP 패킷 목적지 포트주소 분포

두 그림을 통해 인위적으로 시도한 공격 시점 이외에도 몇 군데에서 비정상행위로 의심되는 트래픽 변화가 존재한다. 그러나 이들 트래픽 변화를 비정상행위로 확신하기 위해서는 보다 면밀한 로그파일 분석과 오랜 시간에 걸친 트래픽 수집 및 분석이 필요하다.

4.2 엔트로피와 불확실성

엔트로피는 하나의 변수에 대한 불확실성(uncertainty)의 정도를 나타내는 정보-이론 측정단위이다[11]. Shannon의



(그림 20) IP 목적지 네트워크 분포에 따른 엔트로피 변화

초창기 연구를 시작으로 암호화와 정보 이론가들은 그들의 의미를 모호하게 만들기 위해 메시지를 얼마나 잘 변화시켰는지 결정하기 위해 엔트로피를 사용하였다. 따라서 엔트로피는 암호화, 암축, 코딩 이론을 포함한 매우 다양한 학문분야의 응용들을 가지고 있다. 본 논문에서는 3.1절에서 설명한 바와 같이 네트워크 트래픽 분포를 조사하고 이를 이용해 비정상행위를 탐지하게 된다. 그런데 실질적으로 정상 트래픽 분포와 현재 입력되고 있는 트래픽의 분포를 1:1로 직접 비교한다는 것이 좀처럼 쉬운 작업은 아니다. 따라서 본 논문에서는 이들 네트워크 트래픽 분포로부터 엔트로피를 계산하고 현재의 입력 트래픽의 엔트로피와 비교함으로서 비정상행위 탐지를 용이하게 한다.

랜덤변수 X가 가지는 값은 $\{x_1,\cdots,x_n\}$이고, x_i 값을 가질 확률은 $p(X=x_i)$이다. 여기서 $\sum_{i=1}^{n}p(X=x_i)=1$이다. 이때 X의 엔트로피 혹은 불확실성은 다음과 같이 정의된다.

$$H(X)=-\sum_{i=1}^{n}p(X=x_i)\lg p(X=x_i)$$

여기서, "$\lg x$"는 x의 베이스가 2인 로그함수이다. 한편, $\lg 0=0$로 정의한다. 한편, 랜덤변수 Y가 가지는 값은 $\{y_1,\cdots,y_m\}$이고, y_j 값을 가질 확률은 $p(Y=y_j)$이다. 여기서 $\sum_{j=1}^{n}p(Y=y_j)=1$이다. 두 변수 X, Y의 joint 엔트로피의 정의는 다음과 같다.

$$H(X,Y)=-\sum_{j=1}^{m}\sum_{i=1}^{n}p(X=x_i,Y=y_j)\lg p(X=x_i,Y=y_j)$$

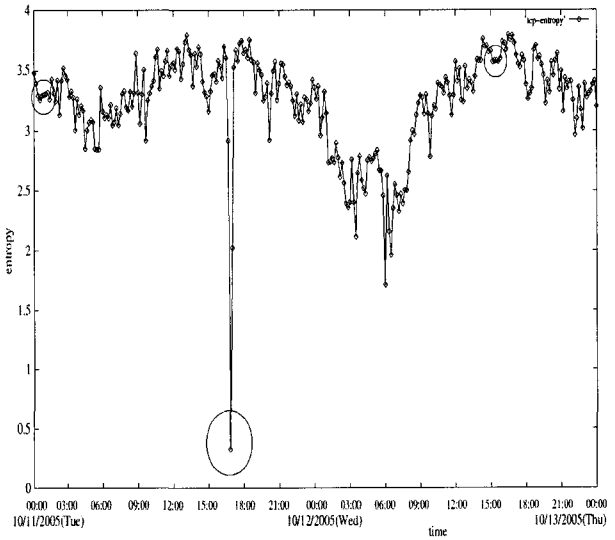
한편, 두 변수 X, Y의 conditional엔트로피의 정의는 다음과 같다.

$$H(X|Y)=-\sum_{i=1}^{n}p(X=x_i|Y=y_j)\lg p(X=x_i|Y=y_j)$$

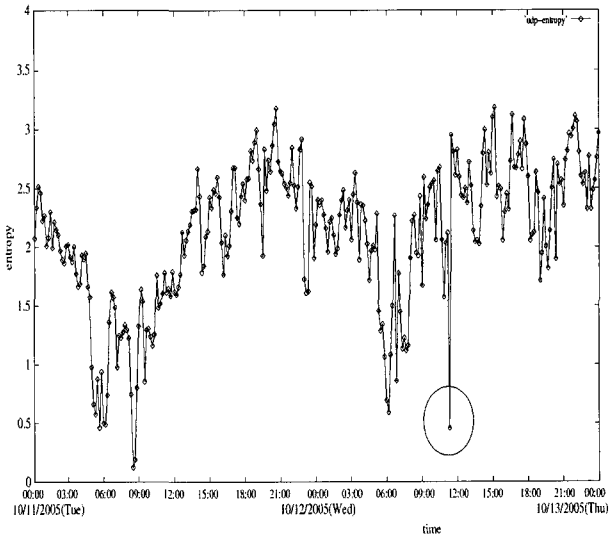
4.3 비정상행위 탐지 결과분석

4.1절을 통해 수집된 트래픽분포((그림 12)~(그림 19))로부터 이들 각각에 대한 엔트로피 변화를 4.2절에서 설명한 수식을 이용해 모두 구할 수 있다. 그러나 본 논문에서는 지면의 제약성 및 중복설명을 피하기 위해 일부 결과만 제시하도록 한다.

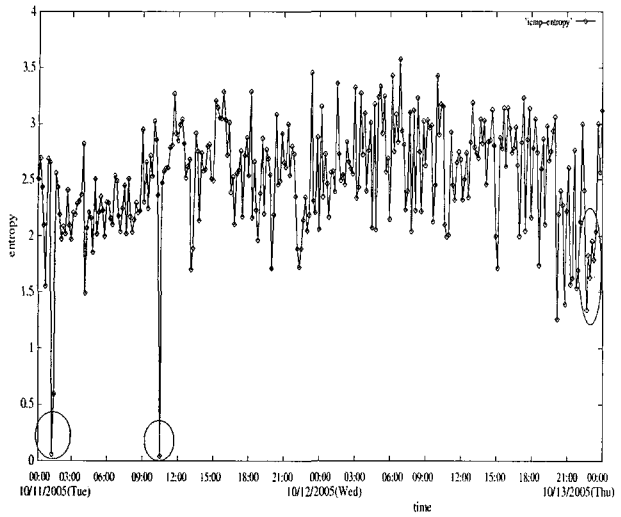
(그림 20)은 BR에서 IP 목적지 네트워크 분포에 대한 엔트로피 변화를 보여준다. 하루를 주기로 주기성의 패턴을 엔트로피 변화 추이를 통해서도 확인할 수 있다. 특히 (그림 11)에 따른 각 공격 시점에 엔트로피의 감소현상이 관찰된다. 이것은 이들 공격이 해당 시점에 특정 네트워크를 대상으로 이루어지고 따라서 트래픽의 편중 현상이 발생됨에 따른 엔트로피 감소 현상으로 판단할 수 있다. 그러나 이들 엔트로피 변화는 syn4k 공격을 제외하고는 변화의 정도가 모호해 판단이 쉽지 않다.



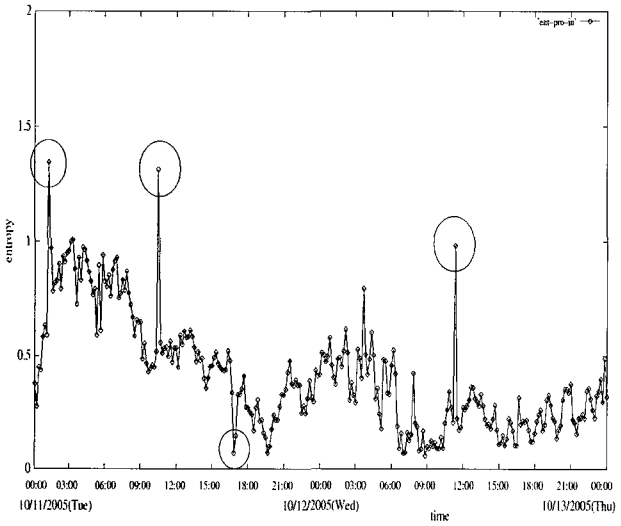
(a)



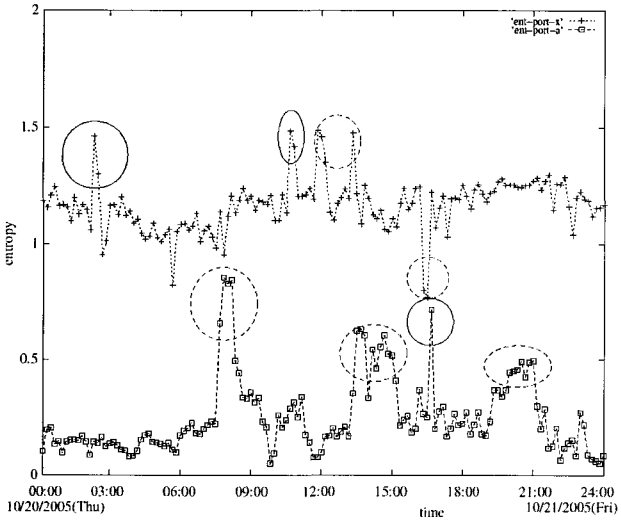
(b)



(그림 21) TCP(a), UDP(b), ICMP(c) 조건에서의 IP 목적지 네트워크 분포에 따른 엔트로피 변화



(그림 22) (그림 13)의 엔트로피 변화 추이



(그림 23) (그림 18)과 (그림 19)의 엔트로피 변화 추이

(그림 21)은 BR의 입력 트래픽이 TCP, UDP, 혹은 ICMP일 경우, 목적지 네트워크 분포에 대한 엔트로피 변화를 각각 보여준다. 즉 4.2절의 조건 엔트로피 계산식에 의해 얻어진 그림이다. (그림 21) (a)로부터 synk4 공격뿐만 아니라 TCP를 사용하는 nmap에 의한 스캔공격에 따른 엔트로피 변화의 특징도 일부 관찰할 수 있다. 즉 스캔 시점에 엔트로피가 비교적 일정하게 유지되고 있음을 관찰할 수 있다. 한편 (그림 21) (b)와 (그림 21) (c)로부터 udp flooder 공격과 jolt 및 teardrop 공격을 감지할 수 있다. 따라서 (그림 20)에 의한 단순한 목적지 네트워크 분포의 엔트로피변화에 의존하기 보다는 이들 프로토콜 조건 엔트로피 변화를 관찰하는 것이 보다 유리하다. 그러나 winnuke 공격의 경우 여전히 목적지 네트워크 분포에 따른 엔트로피 변화를 통해서는 쉽게 감지할 수 없음을 알 수 있다.

(그림 22)은 (그림 13)에 대한 엔트로피 변화를 보여준다. (그림 22)을 통해 jolt와 UDP flooder 공격시점에서 엔트로피 상승(ICMP 혹은 UDP 패킷의 증가에 따라 엔트로피 상승)과 synk4 공격시점에서 엔트로피 감소(TCP 패킷의 증가에 따라 엔트로피 감소)를 보여준다. 따라서 이들 공격을 (그림 22)를 통해 쉽게 탐지할 수 있다. 그러나 winnuke와 teardrop 공격은 (그림 22)을 통해 확인하기란 불가능하다.

winnuke 공격을 감지하기 위해 (그림 23)은 스캔과 winnuke 공격 시 ((그림 17) 참조) 해당 희생 서브네트워크의 목적지 포트주소 분포에 대한 엔트로피 변화 추이를 보여준다. 그림으로부터 이들 공격 시점에 엔트로피 변화(실선 원)를 감지할 수 있다. 그러나 이들 이외의 시점(점선 원)에서도 비정상행위가 탐지되고 있으며 앞에서 설명한 바와 같이 이에 대한 분석은 현재 진행 중에 있음을 밝힌다. 한편, teardrop 공격 역시 특정 목적지 포트를 지정해 공격이 이루어짐에 따라 winnuke와 거의 유사한 탐지결과를 얻을 수 있었다.

5. 결론 및 향후 연구방향

본 논문에서는 네트워크 인바운드 트래픽 분포를 이용해 네트워크 트래픽 비정상행위를 탐지하는 방법을 제시하였다. 이를 위해 먼저 실제 캠퍼스 네트워크의 트래픽 특성을 프로토콜, 패킷 길이, 목적지 IP/포트 주소, TTL 값, TCP SYN 패킷, 그리고 프래그멘트 패킷 분포 등을 기준으로 조사하였다. 외국의 경우 몇몇 네트워크를 대상으로 제한적이나마 일부 트래픽 분포에 대한 연구 결과가 발표되긴 했으나 국내의 경우 구체적인 트래픽 분포에 대한 연구 결과가 부족한 상태다. 따라서 본 논문을 통해 제시된 다양한 트래픽 분포는 네트워크 보안 연구를 위한 좋은 기초 자료가 될 것으로 믿는다.

한편, 인터넷 프로토콜의 헤더 정보를 이용한 기존 비정상행위 탐지 기법은 헤더의 각종 필드 값을 일정 기간 학습하고 이들 학습된 값의 범위를 벗어나는 트래픽을 비정상행위로 판단하는 방법을 채택하고 있다. 그러나 본 연구에서는 수집된 다양한 트래픽 분포를 직접 비정상행위 탐지에

적용하였다. 이를 위해 엔트로피 개념을 도입하고 이를 기준으로 비정상행위를 탐지하였다. 특히 본 논문에서는 잘 알려진 서비스거부공격을 실제 캠퍼스 네트워크를 대상으로 실시하고 그 결과를 제시함으로서 제안된 기법의 타당성을 검증하였다.

네트워크 트래픽 분포는 여러 가지 요소에 의해 영향을 받는다. 특히 캠퍼스 네트워크의 경우 매우 다양한 요소(주별, 달별, 계절별, 학기별, 실험 기간, 수강신청, 성적 열람, 새로운 버전의 소프트웨어 출시에 따른 다운로드 등)에 따라 변화한다. 이러한 요소를 정확하게 반영하기 위해서는 지속적인 트래픽 조사와 함께 비정상행위를 판단할 수 있는 적절한 트래픽 자료가 필요하다. 따라서 본 논문을 통해 제시된 결과는 이제 시작단계로서 다양한 트래픽 분포만을 이용해 비정상행위를 감지할 수 있는 가능성을 제시한 수준이라고 볼 수 있다. 장기간 관찰된 트래픽을 데이터베이스화하고 다양한 변화 요소를 반영한 결과는 현재 계속 수집 중에 있으며 추후 발표할 예정이다.

참 고 문 헌

[1] M. Roesch, "Snort Lightweight Intrusion Detection for Networks," Proc. USENIX LISA'99 pp.101~109, 1999.

[2] H. Debar, M. Dacier, and A. Wespi, "Towards a taxonomy of intrusion-detection systems," Computer Networks, Vol.31, No.8, pp.805~822, 1990.

[3] F. Gong, "Next Generation Intrusion Detection System (IDS)," IntruVert Networks Report, 2002.

[4] Paul Barford and David Plonka, "Characteristics of Network Traffic Flow Anomalies," in Proceedings of the ACM Internet Measurement Workshop, Nov. 2001.

[5] paul Barford, Jeffery Kline, David Plonka and Amos Ron, "A Signal Analysis of Network Traffic Anomalies," in Proceedings of the ACM Internet Measurement Workshop, Nov. 2002.

[6] Jake D. Brutlag, "Aberrant Behavior Detection in Time Series for Network Monitoring," in Proceedings of the USENIX Fourteenth system Administration Conference LISA XIV, 2000.

[7] M.V. Mahoney, "Network Traffic Anomaly Detection Based on Packet Byte," SAC2003, Melbourne, Florida, 2003.

[8] M.V. Mahoney and P.K. Chan, "PHAD: Packet Header Anomaly Detection for Identifying Hostile Network Traffic," Florida Institute of Technology Technical Report CS-2001-04, 2001.

[9] R. Lippmann et al, "The 1999 DARPA Off-Line Intrusion Detection Evaluation," Computer Networks, Vol.34, No.4, pp.579~595, 2000.

[10] A. Papoulis, Probability, Random Variables, and Stochastic Processes, 3rd Ed., McGraw-Hill, 1991.

[11] Spender, "릭눅스용 DoS 툴 datapool", available at http://packetstorm.linuxsecurity.com/DoS/indexsize.html

[12] www.nac.net, The WinNuke Relief Page, available at http://www.users.nac.net/splat/winnuke/

[13] Zakath, Syn Flooder, http://packetstorm.linuxsecurity.com/Exploit_Code_Archive/synk4.c

[14] Fyodor, The Art of Port Scanning, available at http://www.insecure.org/nmap/nmap_doc.html

[15] www.cert.org, CERT Advisory CA-1996-01 UDP Port Denial-of-Servie Attack, http://www.cert.org/advisories/CA-1996-01.html

[16] www.cert.org, CERT Advisory CA-1996-26 Denial-of-Service Attack via ping, available at http://www.cert.org/advisories/CA-1996-26.html

[17] www.cert.org, CERT Advisory CA-1997-28 IP Denial-of-Service Attacks, available at http://www.cert.org/advisories/CA-1997-28.html

강 구 홍

e-mail : khkang@seowon.ac.kr

1985년 경북대학교 전자공학과(공학사)

1990년 충남대학교 전자공학과(공학석사)

1998년 포항공과대학교 전자계산학과 (공학박사)

1985년~1993년 한국전자통신연구소 선임연구원

1998년~1999년 한국전자통신연구원 선임연구원

2002년~2003년 한국전자통신연구원 초빙연구원

2000년~2001년 서원대학교 컴퓨터정보통신공학부 전임강사

2002년~현재 서원대학교 컴퓨터정보통신공학부 조교수

관심분야 : 성능평가, 컴퓨터 네트워크, 네트워크 보안 등

오 진 태

e-mail : showme@etri.re.kr

1990년 경북대학교 전자공학과(공학사)

1992년 경북대학교 전자공학과(공학석사)

1992년~1998년 한국전자통신연구원 선임 연구원

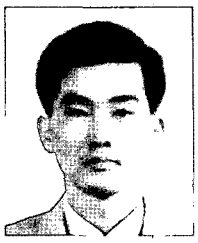
1998년~1999년 MinMax Tech. 연구원

1999년~2001년 Engedi Networks Inc. Director

2001년~2002년 Winnow Networks Incs. CTO 부사장

2003년~현재 한국전자통신연구원 보안게이트웨이 팀장

관심분야 : 네트워크 보안, 비정상행위탐지기술, 고성능침입탐지 기술 등



장 종 수

e-mail : jsjang@etri.re.kr

1984년 경북대학교 전자공학과(공학사)

1986년 경북대학교 전자공학과(공학석사)

2000년 충북대학교 컴퓨터공학과(공학박사)

1989년~현재 한국전자통신연구원 네트워크 보안 그룹장

관심분야 : 네트워크 보안, 센서네트워크, 정책기반보안관리, QoS 등