情報保護學會論文誌
第 22 卷 第 3 號, 2012. 6

클러스터 정보를 이용한 네트워크 이상상태 탐지방법*

이 호 섭,† 박 응 기, 서 정 택‡
ETRI 부설연구소

A New Method to Detect Anomalous State of Network using Information of Clusters*

Ho-sub Lee,† Eung-ki Park, Jung-taek Seo‡
The Attached Institute of ETRI

요 약

최근 우리는 급격한 정보통신 기술의 발달로 큰 변화를 겪었으며, 기존의 기반 시설들 및 서비스들이 정보통신기술과 융합되면서, 다시 한 번 환경 변화를 눈앞에 두고 있다. 정보통신의 발달은 이러한 이점들 외에도 여러 부작용을 낳고 있으며, 이러한 부작용들은 금전적 피해뿐만 아니라 국가적인 재난 상황으로 발전될 소지가 있다. 따라서 이들에 대한 탐지 및 신속한 대응이 중요하며, 이와 관련한 많은 시도가 이루어지고 있다. 이러한 예로는 침입탐지시스템이 있을 수 있다. 그러나 침입탐지시스템은 특정 트래픽이나, 파일이 악성인지 여부를 판단하는데 중점을 두고 있으며, 현재까지 변종이나 새롭게 개발된 악성 코드에 대한 탐지는 힘들다. 따라서 본 논문에서는 네트워크의 현재의 상황과 과거의 상황들을 비교하여, 현재 시점의 네트워크 모델이 정상인지 비정상인지를 판단할 수 있는 방법에 대해 제안한다.

ABSTRACT

The rapid development of information technology is making large changes in our lives today. Also the infrastructure and services are combinding with information technology which predicts another huge change in our environment. However, the development of information technology brings various types of side effects and these side effects not only cause financial loss but also can develop into a nationwide crisis. Therefore, the detection and quick reaction towards these side effects is critical and much research is being done. Intrusion detection systems can be an example of such research. However, intrusion detection systems mostly tend to focus on judging whether particular traffic or files are malicious or not. Also it is difficult for intrusion detection systems to detect newly developed malicious codes. Therefore, this paper proposes a method which determines whether the present network model is normal or abnormal by comparing it with past network situations.

Keywords: Intrusion Detection System, Machine Learning, Clustering

I. 서 론

정보통신 기술의 발달로 우리는 많은 편의를 제공받고 있다. 또한 컴퓨터를 활용한 서비스들뿐만 아니라 기존의 기반 시설들 및 서비스들이 정보통신기술과 융합되면서, 우리는 또 한 번의 큰 기술 도약 및 환경 변화를 눈앞에 두고 있다.

접수일(2011년 11월 21일), 수정일(2012년 2월 22일), 게재확정일(2012년 3월 13일)
* 본 연구는 2010년도 지식경제부의 재원으로 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 연구 과제입니다. (No. 2010101040046A)
† 주저자, leehosub@ensec.re.kr
‡ 교신저자, seojt@ensec.re.kr

정보통신기술의 발달이 이런 순기능만을 가지는 것은 아니다. 정보통신기술의 결함이나 그 환경들을 악용하여 부당한 이익을 챙기거나, 타인에게 피해를 주는 사례가 많아 졌다. 대표적인 예로 서비스 거부 공격(denial of service)을 들 수 있다. 현재는 단순 서비스 거부 공격이 아닌, 전 세계에 퍼져있는 PC들의 제어권을 획득하고, 이들을 통해 제3의 목표물을 공격하는 형태를 가진다. 뿐만 아니라 이러한 공격은 인터넷 포털 서비스의 상위 검색어 변조 등에도 영향을 줌으로써, 금전적인 이득을 취하기 위한 목적으로도 사용된다. 만약 정보통신기술이 이러한 공격들에 대한 대비 없이, 기존의 기반 시설 및 서비스에 융합된다면, 누구도 예상치 못한 사태가 벌어질 수 있다.

본 논문은 이러한 사태를 미연에 방지하기 위한 일환으로 네트워크 상태이상 탐지방법을 제안한다. 기존의 분산 서비스 거부공격에 대한 탐지 방법은 각 패킷을 보고, 해당 패킷이 공격 패킷인지 여부를 판별함으로써, 네트워크 내부의 컴퓨터가 외부로 공격을 하고 있는지, 혹은 외부로부터 공격을 받고 있는지 여부를 판단한다. 그러나 이러한 방법은 네트워크 특성에 매우 제한적이며, 진화하는 공격이나 새롭게 발생하는 네트워크 공격 유형에 유연한 대처가 어렵다는 문제가 있다. 본 논문에서 제안하는 방법은 특정 공격을 분류하지는 못하지만, 네트워크의 상태 이상 정도를 파악하여 알람을 울림으로써, 기존의 공격은 물론이고, 알려지지 않은 공격 등에 대한 네트워크 및 보안 담당자의 빠른 대응을 유도할 수 있는 방안을 제시한다.

본 논문의 구성은 다음과 같다. 2장에서는 대표적인 네트워크 이상상황이라 볼 수 있는 분산 서비스 거부공격과 그 탐지 방법에 대한 연구들에 대해 설명한다. 3장에서는 본 논문에서 제안하는 방법을 설명하며, 4장에서 제안하는 방법을 검증하기 위한 실험을 설명하고, 그 결과를 분석한다. 그리고 마지막으로 5장에서 결론을 맺는다.

II. 관련 연구

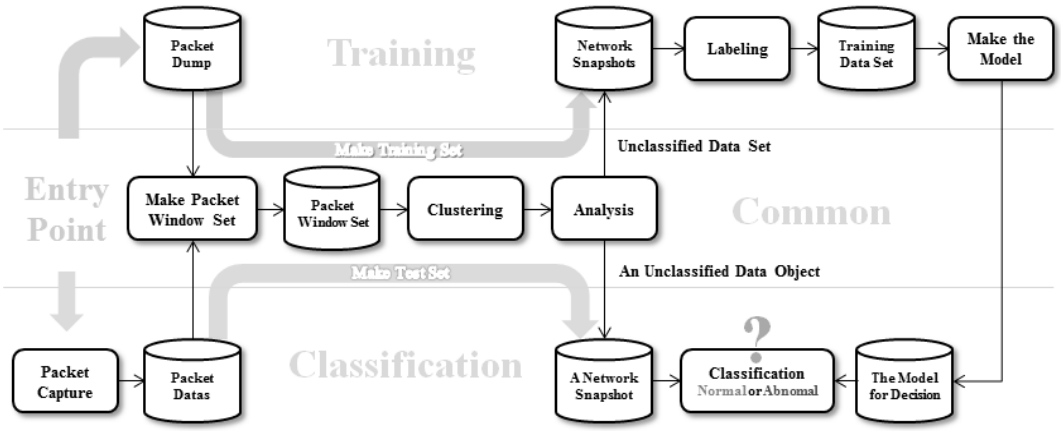
2.1 분산 서비스 거부 공격

최양서 등의 논문에서는 분산 서비스 거부공격을 분석하였으며, 공격 형태와 시기를 중심으로 4개 세대로 세분화하여, 분산 서비스 거부공격을 분석하였다. 1세대 공격은 2000년 초반까지 주로 나타났으며, 트래픽 폭주의 공격 형태를 띄고, 2세대 공격은 2000년 초/중반에 나타났으며, 자동 전파기능을 가진 완전 자동화된 웜 형태의 공격양상을 띈다고 말한다[1]. 또한 3세대는 2000년 중반에 들어서 나타났으며, 봇넷을 이용한 공격 형태를 띄고, 4세대는 2009년 7월 7일 발견되었으며, 3세대와 비슷한 형태를 가진다고 말하고 있다.

2.2 분산 서비스 거부 공격 탐지방법

최양서 등[1]의 논문에서는 DDoS의 공격 프로세스를 4단계로 정의하고, 각 단계에서 공격자가 의도한 대로 이루어지지지 않도록 하면 공격이 이루어지지 않는다는데 초점을 두고, 각 단계에서의 대응 방법을 제안하였다. 이세열 등[2]은 퍼지인식도(fuzzy cognitive maps)를 적용한 결정모듈의 분석결과를 활용하여, 서비스 거부 공격의 위험도 측정을 통해 서비스 거부 공격에 대응하도록 하는 모델을 연구하였으며, 이제학 등[3]은 inbound 트래픽에 대해 트래픽 매트릭스를 구성하여 스트림의 분산을 구하고, 이들에 유전 알고리즘을 적용하여 분산 서비스 거부공격을 탐지하고자 하였다. Paul Barford 등[4]은 네트워크 트래픽 플로우를 분석하여 트래픽의 특성을 분류하는 논문을 제시하였다. 이들은 논문에서 FlowScan을 이용하여 연구를 수행하였으며, 수집된 트래픽 데이터에 대해 사전에 정의한 3가지 분류로 그룹화하고, 시계열분석(time series)를 통해 분석하였으며, 비정상 데이터에 대해 웨이블렛 분석을 적용하여 서비스 거부공격에 대한 탐지실험을 수행하였다. Xei Xiong 등[5]은 발산지수(Lyapunov exponent)와 시계열 분석을 이용한 네트워크 이상탐지 방법을 제시하였다. 이 방법에서 발산지수는 위상궤적 상에서 두 점을 구한 뒤, 두 점의 거리가 얼마나 멀어지는가를 정량화한 변수를 의미한다.

Georgios Androuliakis 등[6]은 opportunistic sampling 방법을 사용하여 네트워크의 이상탐지를 수행하였다. 이들은 네트워크의 이상상태를 분산 서비스거부공격, 웜 전파, 포트 스캐닝, Flash Crowd, Alpha Flow 등 4가지 형태로 정의하였고, 엔트로피를 이용하여 네트워크 이상상태를 탐지하였다. 이처럼 최근에는 네트워크 대역폭이 증가하고, 컴퓨팅 속도가 빨라짐에 따라 연산량이 적으면서도 효과적인 탐지를 위한 방안에 대한 연구를 진행하였는데, 이러한 방법의 하나로 Gergios Androuliakis 등처럼 엔트로피를 이용하여 트래픽의 복잡도를 측정하고,



〔그림 1〕 제안하는 방법

그 결과를 분석하여 서비스 거부 공격을 탐지하는 방안이 제안되고 있다[6-10].

III. 제안하는 방법

제안하는 방법의 단계는 크게 학습과 분류, 두 단계로 이루어지며, 두 단계 모두는 수집한 패킷 데이터로부터 네트워크 스냅샷을 생성하는 과정은 동일하다.

본 논문에서 제안하는 방법은 다음과 같다.

공통 단계.

1. Entry Point : 학습 단계의 경우 사전에 수집된 패킷 덤프 데이터를, 분류 단계의 경우에는 실시간 패킷 데이터를 수집한다. 본 논문에서는 실험을 위해 테스트 데이터 역시 사전에 수집된 데이터를 이용하였다.
2. Make Packet Window Set : 수집된 네트워크 트래픽 데이터를 이용하여, 네트워크 스냅샷을 만들기 위한 패킷 윈도우 셋을 생성한다. (분류단계의 경우 하나의 윈도우만을 생성한다.)
3. Clustering : 생성된 패킷 윈도우 셋에 대해 클러스터링을 실행한다.
4. Analysis : 각 패킷 윈도우 셋에 대한 클러스터링 결과를 분석하여, 네트워크 스냅샷을 생성한다.

학습 단계.

5. 생성된 네트워크 스냅샷들의 속성 값 마지막 열에 사전에 침입탐지시스템 등으로 분류한 결과(정상 혹은 비정상)를 입력하여 학습 데이터 셋을 생성한다.
6. 생성된 학습 데이터 셋을 이용하여 분류기를 실행하고, 분류 모델을 생성한다. 이 분류 모델은 분류 단계에서 최종적으로 정상인지 비정상인지를 판단할 때 사용한다.

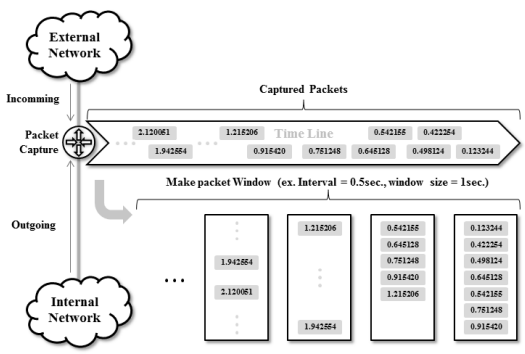
분류 단계.

5. 생성된 네트워크 스냅샷과 학습 단계 6의 결과로 생성된 분류 모델을 이용하여, 해당 네트워크 스냅샷이 정상인지 비정상인지 판단한다.

제안하는 방법의 각 단계에서 세부적으로 설명하지 못한 부분은 아래에서 설명하도록 한다.

3.1 패킷 윈도우 구성

네트워크 상태 검사를 위한 버퍼는 슬라이딩 윈도우 형태로 구성한다. 이 때, 버퍼의 크기와 윈도우 사



〔그림 2〕 패킷 윈도우 구성

이즈를 변수로 가질 수 있다. [그림 2]는 윈도우의 크기가 1초이며, 윈도우의 생성 간격이 0.5초라고 가정했을 때, 생성되는 윈도우들을 나타낸 것이다.

앞서 설명한 것과 마찬가지로, 학습 단계의 경우에는 사전에 수집된 패킷 데이터를 사용하며, 분류 단계에서는 실시간으로 수집되는 패킷 데이터를 이용한다. 그러나 본 논문에서는 실험을 위해서 사전에 수집된 패킷 데이터에서 일부를 학습 데이터로, 나머지를 분류 데이터로 나누어 사용하였다.

3.2 클러스터링을 위한 특징벡터 추출

본 논문에서 제안한 방법에 따르면, 패킷 윈도우를 구성한 다음의 단계로 네트워크 스냅샷을 생성하기 위해 클러스터링을 수행한다. 클러스터링을 수행하기 위해서는 각 패킷 윈도우에 속한 패킷 데이터로부터 특징벡터를 추출해야 한다. [표 1]은 패킷 데이터에서 추출할 특징벡터를 도식화 한 것이다.

우선 앞선 패킷과 이전패킷의 시간차이의 경우, 네트워크를 통한 서비스거부공격이 발생한다면, 네트워크 장비에 잼이 발생할 확률이 높아지며, 이럴 경우 네트워크 장비는 스위칭을 포기하고 브로드캐스팅 한다고 예상하였다. 그렇다면 패킷의 시간간격이 좁혀질 것이라 판단하여 해당 특징을 추가하였다. 또한 IP에 대한 특징 4개를 설명하면, 아이피 주소가 A.B.C.D로 이루어져 있을 때, 각 출발지 및 도착지 IP에 대해 각각의 동일한 위치에 해당하는 값의 차를 구하였다. 즉 $A_{sourceIP}$-$A_{destinationIP}$등의 계산을 통해 특징 값을 구하였다. 그 이유는 IP는 원래 4바이트 값으로 전송되어지나, 4바이트 값에 대한 차를 구하면 동일한 서브넷에서의 움직임인지, 혹은 요청메시지 및 응답메시지인지에 대한 표현이 안될 것이라 판단하여 각각에 대한 값을 특징 값으로 하였다. 그 다음 출발지 IP와 도착지 IP는 각 특징 값을 인덱스화하여, 특징 값으로 사용하였다. 또한 도착지 포트는 특정 서비스에 대한 패킷 여부를 판별할 수 있기 때문에 특징으로 선정하였으며, 시퀀스 값과 윈도우 사이즈, 최상위 프로토콜 등은 패킷에 대한 오류여부와 패킷 사이즈의 변화 등을 분석하기 위해 추가하였다.

[표 1] 특징 벡터

특징	설명
DIFF TIME	이전 패킷과의 시간 차이
DIFF IP A	출발지 IP와 도착지 IP의 차이 (출발지 IP - 도착지 IP) A.B.C.D
DIFF IP B	
DIFF IP C	
DIFF IP D	
출발지 IP	패킷을 발송한 컴퓨터 주소
도착지 IP	패킷을 수신할 컴퓨터 주소
DST PORT	도착지 포트
SEQ	시퀀스 번호
WIN	윈도우 사이즈
PROTO	최상위 프로토콜 (3레이어까지)

예를 들어 서비스거부공격이 발생한다면 특정 IP 및 포트로 발송되는 패킷의 양이 급격히 증가할 것이다. 또한 하나의 패킷 윈도우 안에 다른 패킷에 비해 출발지IP와 도착지IP의 차이 값이 동일한 패킷의 비율이 증가하게 될 것이다.

3.3 K-평균 클러스터링

본 논문에서는 네트워크 스냅샷을 생성하기 위한 클러스터링 방법으로 K-평균 클러스터링(k-means clustering)을 사용하였다. K-평균 클러스터링은 각 클러스터의 중심점과 오브젝트 사이의 유클리드 거리에 기반을 둔 방법으로써 기준점에서 가까운 곳의 데이터들을 하나의 클러스터로 묶는 방법을 사용한다. 이 방법은 우선 K개의 클러스터 수와 위치를 선정하고, 각각의 데이터와 K개의 점 사이의 거리를 계산하여, 가장 가까운 클러스터에 속하도록 한다. 그 후 각 클러스터로 나누어진 데이터들을 기준으로 클러스터의 중심점을 다시 설정하고, 다시 각 데이터와의 거리를 계산한 후, 데이터들의 소속이 변경되지 않으면 알고리즘을 종료하는 방법이다[11].

이와 같은 방법을 식으로 나타내면 다음과 같다.

$$V=\sum_{i=1}^{k}\sum_{j\in S_i}|x_j-\mu_i|^2 \quad (1)$$

식 (1)을 설명하면, i 번째 클러스터의 중심을 μ_i, 클러스터에 속하는 점의 집합을 S_i라고 할 때, 전체의 분산 값을 나타낸 것이며, 값 V를 최소화하는 S_i를 찾는 것을 목표로 한다. 이 방법은 구조가 간단하여 비교적 연산 속도가 빠르다. 그러나 고정된 K개의 클러스터로 데이터를 강제로 구분하기 때문에, 사용자가 입력하는 K 값의 영향을 많이 받는다는 단점이 있다.

3.4 네트워크 이상상태 탐지를 위한 2차 특징벡터 생성

앞서 설명한 K-평균 클러스터링의 수행 결과로 얻

〔표 2〕 네트워크 스냅샷

특징	설명
패킷 총 개수	각 클러스터를 구성하고 있는 패킷의 개수 합 (버퍼를 구성하는 패킷의 총 개수)
평균	각 Cluster를 구성하는 패킷 개수의 평균 값
표준편차	각 Cluster를 구성하는 패킷의 표준 편차

어진 패킷 윈도우에 대한 클러스터 정보를 이용하여, 네트워크 이상상태를 분류하기 위해 2차 특징벡터를 생성한다. 〔표 2〕는 특징벡터의 각 항목에 대한 설명을 나타낸다.

이렇게 생성된 특징 벡터로 이루어진 버퍼는 해당 시점의 네트워크 상태로 볼 수 있기 때문에, 본 논문에서는 표 2의 특징들로 이루어진 네트워크 상태를 네트워크 스냅샷이라고 정의하였다. 각 스냅샷을 구성하는 패킷 중 공격 패킷의 구성이 50% 이상일 경우, 이 스냅샷은 정상이 아니라고 정의하였다.

3.5 네트워크 이상상태 탐지

본 논문에서는 네트워크의 이상상태를 탐지하기 위해서 베이지안 분류기를 사용하였다. 베이지안 분류기는 식 (2)와 같은 베이스 정리(bayes theorem)를 이용한 확률기반의 분류기이다〔11-13〕.

$$P(A_i|B) = \frac{P(A_iB)}{P(B)} = \frac{P(B|A_i)P(A_i)}{\sum_{k=1}^{n} P(B|A_k)P(A_k)} \quad (2)$$

베이지안 분류기는 확률을 기반으로 하는 방법으로 기존에 나타나지 않은 사건에 대해서는 분류결과가 취약하다는 단점이 있다. 또한 변수의 개수가 많으며, 각 변수 당 경우의 수가 많아질 경우 분류 결과에 대한 신뢰도가 낮아진다. 따라서 본 논문에서는 나이브 베이지안(naive bayesian)을 사용하며, 앞서 설명한 단점을 보강하기 위해 각 변수의 경우의 수를 입력값으로 받아 한정짓도록 한다. 이 방법을 수식으로 나타내면 식 (3)과 같다.

$$x' = floor\left(\frac{x - \min(x)}{\max(x) - \min(x)} \times C\right) \quad (2)$$

식 (3)은 변수의 값 x가 주어질 때, 해당 변수의 최소값 $\min(x)$로 빼고, 그 값을 $\max(x)$ - $\min(x)$한 값으로 나누어 준다. 이 과정은 스케일링(scaling) 과정으로써, 해당 변수의 최소값을 0으로, 최대값을 1로 변환하여, 이후에 분류 시 각 변수간의 영향력을 동일하게 적용하도록 하기 위해 수행하는 방법이다. 여기에 추가적으로 경우의 수를 한정짓기 위해 C를 곱한 뒤, floor 함수를 통해 소수점 이하의 값을 버림으로써 특정한 정수 값에 강제로 적합시킨다. 이 과정은 특정한 값의 범위에 대한 인덱싱(indexing)으로 볼 수 있다.

IV. 실험 및 실험 결과

4.1 실험 데이터 분석

본 실험을 위해서 MIT/LL의 DARPA 2000 Dataset을 실험 데이터로 사용하였다〔14〕. DARPA 2000 Dataset은 Mstream을 이용한 분산 서비스 거부 공격을 포함하는 네트워크 트래픽 데이터와 솔라리스 BSM 감사 데이터로 이루어져 있다. 이 데이터는 크게 5 단계를 통해 수집되었다. 첫 단계는 IPsweep을 이용하여 미 공군 기지 내부의 호스트를 스캐닝 하였다. 두 번째 단계에서는 각 호스트에 대해 sadmind 데몬의 실행 여부를 스캐닝 하였으며, 세 번째 단계에서 버퍼오버플로우(buffer overflow) 공격을 통해 sadmind를 공격하여 호스트로 침입하였다. 네 번째 단계에서는 해당 호스트에 분산 서비스 거부 공격을 하기 위해 Mstream을 설치하였으며, 마지막 단계에서 분산 서비스 공격을 수행한다.

이 데이터 셋의 특징으로는 공격이 단 한 번이며, "Mstream 131.84.1.31 5"라는 명령을 통해, 약 5초 동안 131.84.1.31로 TCP 프로토콜의 ACK 패킷을 발송했다는 점이다. 이때 발송되는 모든 패킷은 스푸핑(spoofing) 되어, 랜덤한 출발지 아이피를 가진다. 또한 패킷 수집 시작 후 97초 이후부터 약 4초간 수행되었으며, 공격 이외에 〔표 3〕과 같이 8가지의 공격패킷 특징이 나타난다.

〔표 3〕 실험 데이터 셋 중 공격 패킷의 특징

번호	속성	값
1	출발지 IP	랜덤
2	도착지 IP	131.84.1.31
3	출발지 포트	랜덤
4	도착지 포트	랜덤
5	제어비트	ACK
6	시퀀스번호	1
7	윈도우사이즈	16384
8	패킷길이	0

보다 자세한 사항은 MIT/LL의 DARPA 2000 Dataset을 참고하도록 한다.

4.2 실험 및 실험 결과

우선 실험에 사용된 DARPA 2000 Dataset의 총 패킷 개수는 74,480개 이다. 본 논문에서 제안하는 방법을 통해 실험한 결과는 다음과 같다. 이 데이터는 총 904.348018초 동안 수집되었으며, 약 1,800 개의 네트워크 스냅샷을 생성하였다. 또한 95.708467초부터 101.568442초 까지 서비스 거부 공격이 실행되었으며, 191번 스냅샷에서부터 약 12장의 스냅샷에 걸쳐 공격이 나타났다.

이를 가지고 우리는 2가지 실험을 수행하였다.

우선 모든 실험에서 시간적인 요소를 배재하고, 정상 스냅샷과 비정상 스냅샷으로 나누어 7:3의 비율로 학습 데이터와 실험 데이터를 구성하였고, 학습 및 탐지 테스트를 1,000회 수행하였다.

첫 번째 실험은 DARPA 2000 Dataset 만을 사용하였으며, 두 번째 실험은 웹 서비스, TELNET, FTP, SSH, 메신저 등을 사용하는 공개된 환경에서 데이터를 약 900초 동안 수집하여, 적절한 수정을 거친 뒤, 첫 번째 실험에서 사용한 DARPA 2000 Dataset과 혼합하여 데이터 셋을 구성하였다. 이 때, 데이터필드는 모두 삭제하였으며, 데이터를 수집한 노드를 기준으로 상위 2바이트가 같은(XXX.XXX.?.?) IP를 DARPA 2000 Dataset의 IP로 수정하여 적절히 배치하였다.

실험에는 WEKA[15] 3.6.5 64Bit를 사용하였으며, 나이브 베이지안을 사용하여 분류 실험을 진행하였다.

4.3 실험 결과 분석

첫 번째 실험의 경우, 정상상태와 이상상태를 모두 100% 정확하게 판단하였는데, 이는 특정 도착지 IP로 동일한 패킷이 급격히 발생하였으며, 초당 패킷 수 역시 급격히 증가하였기 때문에 완벽히 탐지된 것으로 분석되었다. 즉, 정상상태와 이상상태가 확연히 다른 형태를 가졌기 때문에 각각의 상태를 정확하게 판단할 수 있었다.

[표 4] 실험 결과에 대한 Confusion Matrix

〈첫 번째 실험〉

	TP Rate	FP Rate
정상상태	100 %	0 %
이상상태	100 %	0 %

〈두 번째 실험〉

	TP Rate	FP Rate
정상상태	98.2 %	1.3 %
이상상태	98.7 %	1.8 %

비현실적인 데이터를 이용한 실험이었던 첫 번째와는 달리, 두 번째 실험의 경우 공개된 네트워크에서 데이터를 수집하여 첫 번째 데이터와 병합하였기 때문에, 첫 번째보다 현실의 상황과 비슷하다고 할 수 있다. 이 실험에서는 정상상태를 이상상태로 잘못 판단한 비율이 약 1.8%이며, 이상상태를 정상상태라고 잘못 판단한 비율이 약 1.3%였다. 각각의 데이터를 분석해보면, 정상상태를 이상상태라고 잘못 판단한 경우는 P2P와 관련된 패킷의 급증으로 인해 전체적인 스냅샷 내 패킷 수가 급증하였고, 여러 호스트로부터 단일 호스트로 트래픽이 집중되었던 것으로 나타났다. 또한 이상상태인데 정상상태로 판단된 경우는 네트워크 스냅샷 내 전체적인 패킷수가 증가하여, 서비스 거부 공격으로 인한 급격한 패킷 증가 패턴이 일부 들어간 경우에는 큰 영향을 주지 못했기 때문으로 생각된다.

따라서 보다 여러 가지 상황을 염두에 두고 네트워크 상태 탐지를 하려한다면, K-평균 클러스터링의 클러스터 개수인 K 값을 적절히 실험을 거쳐 크게 하거나, 자동적으로 결정할 수 있도록 하는 알고리즘이 필요하며, 클러스터링 분석의 경우도 단순한 계산치 만이 아닌, 중심점 사이의 거리, 클러스터의 평균 면적, 데이터의 분산 등 보다 다양한 분석을 통해 정확도를 높일 수 있을 것으로 생각된다. 또한, 시계열 분석(time series)을 통해 각 네트워크의 시간적(계절별, 월별, 주간별, 시간별 특성)이고, 공간적인(네트워크) 특성을 분석해내서 탐지 기법에 반영한다면 보다 좋은 탐지율을 가지는 결과를 가져올 것으로 예상된다.

V. 결론

본 논문은 특정 시간단위로 네트워크 스냅샷을 만들어, 네트워크의 이상상태를 탐지하는 방법을 제안했다. 제안한 방법은 특정 시간 동안의 패킷 버퍼에 대한 클러스터링을 통해 네트워크의 상태를 정의하고, 이를 네트워크 스냅샷이라고 하였다. 이후 이들 스냅샷의 변화에 대한 분류를 통해 네트워크 이상상태를 탐지하는 방법을 제안하였다.

논문에서 제안한 방법은 특정 공격 유형이나 패킷

이 공격 패킷인지 여부를 판단하는 데는 무리가 있다. 또한 공격을 시작하는 시점에 바로 네트워크의 상태가 변한다는 보장이 없고, 해당 시점의 패킷이 버퍼에 입력되기 까지 시간이 걸리기 때문에 이상상태 탐지에 대한 지연시간이 발생할 수 있다. 따라서 본 방법은 침입탐지시스템이나 침입방지시스템, 네트워크 모니터링 시스템 등 다른 보안 및 관제 시스템들과 연동되어 사용되어야 한다는 단점이 있다.

그 동안의 데이터마이닝 등을 이용한 침입탐지 연구는 실험에 사용한 학습 데이터와 실험 데이터 모델에 의존하여, 실제 환경에서의 성능이 결정되는데 반해, 본 논문에서 제안하는 방법은 추가적으로 해당 네트워크 환경을 학습하고, 특정 상황에 대해 이전의 상태들과 비교하여 비정상 여부를 판단하기 때문에 비교적 다양한 환경에 대해 효과적일 것으로 예상된다. 또한 본 연구 결과물은 네트워크의 이상상태를 탐지한다는 특성 때문에 보안 분야 이외에 네트워크 관리 분야에서도 사용될 수 있을 것으로 기대된다.

참고문헌

〔1〕 최양서, 오진태, 장종수, 류재철, "분산서비스거부(DDoS) 공격 통합 대응체계 연구," 정보보호학회지, 19(5), pp. 11-20, 2009년 10월.

〔2〕 이세열, 김용수, 심귀보, "서비스 거부 공격에서의 퍼지인식도를 이용한 네트워크기반의 지능적 침입방지 모델에 관한 연구," 퍼지 및 지능시스템학회논문지, 13(2), pp.148-153, 2003년 4월.

〔3〕 이제학, 김동성, 김태환, 박종서, "트래픽 매트릭스와 유전 알고리즘을 이용한 분산 서비스 거부 공격 탐지," 2010년도 한국인터넷정보학회 학술발표대회, pp. 453-458, 2010년 6월.

〔4〕 Paul Barford and David Plonka, "Characteristics of network traffic flow anomalies," IMW '01 Proeedings of the 1st ACM SIGCOMM Workshop on Internet Measurement, pp. 69-73, Dec. 2001.

〔5〕 Wei Xiong, Hanping Hu, Yue Yang, and Qian Wang, "Anomaly detection of network traffic based on the largest lyapunov exponent," Advanced Computer Control(ICACC), 2010 2nd International Conference on, pp. 581-585, Mar. 2010.

〔6〕 Androulidakis, G., Chatzigiannakis, V., and Papavassiliou, S., "Network anomaly detection and classification via opportunistic sampling," IEEE Network, pp. 6-12, Mar. 2009.

〔7〕 김태훈, 서기택, 이영훈, 임종인, 문종섭, "엔트로피를 이용한 분산 서비스 거부 공격 탐지에 효과적인 특징 생성 방법 연구," 정보보호학회논문지, 20(4), pp. 63-73, 2010년 8월.

〔8〕 Anna T. Lawniczak, Hao Wu, and Bruno Di Stefano, "Entropy based detection of DDoS attacks in packet switching network models," Complex Sciences, LNICS, Social Informatics and Telecommunications Engineering, Vol. 5, Part 1, pp.1810-1822, Jun. 2009.

〔9〕 Ke Li, Wanlei Zhou, Shui Yu, and Bo Dai, "Effective DDoS attacks detection using generalized entropy metric," Algorithms and Architectures for Parallel Processing, LNCS 5574, Springer, pp. 266-280, 2009.

〔10〕 Shui Yu and Wanlei Zhou, "Entropy-based collaborative detection of DDoS attacks on community networks," 2008 Sixth Annual IEEE International Conference on Pervasive Computing and Communications, percom, pp.566-571, Mar. 2008.

〔11〕 Sergios Theodoridis and Konstantinos Koutroumbas, Pattern recognition, 4th Ed., Elsevier, Nov. 2008.

〔12〕 오일석, 패턴인식, 교보문고, Aug. 2008.

〔13〕 Rechard O. Duda, Peter E. Hart, and David G. Stork, Pattern classification, 2nd Ed., Wiley, Oct. 2000.

〔14〕 MIT LINCONLN LABORATORY, 2000 DARPA intrusion detection scenario specific data sets, MIT/LL, http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/data/2000data.html

〔15〕 Machine Learning Group at University of Waikato, WEKA 3 : data mining software in java, http://www.cs.waikato.ac.nz/ml/weka

〈著者紹介〉

사 진

이 호 섭 (Ho-sub Lee) 정회원
2006년 2월: 동국대학교 컴퓨터학과 졸업
2009년 2월: 고려대학교 정보경영공학과 공학석사
2009년 7월~2010년 6월: 한국인터넷진흥원 주임연구원
2011년 3월~현재: 한국전자통신연구원 부설연구소 연구원
〈관심분야〉 스마트그리드 보안, 정보보호, 데이터마이닝, 패턴인식, 네트워크 시뮬레이션

사 진

박 응 기 (Eung-ki Park) 정회원
1986년 2월: 중앙대학교 전자계산학과 졸업
1988년 2월: 중앙대학교 전자계산학과 공학석사
2005년 2월: 아주대학교 컴퓨터공학과 공학박사
1988년 2월~2000년 1월: 한국전자통신연구원 선임연구원
2000년 1월~2000년 4월: 한국전자통신연구원 부설연구소 책임연구원
2000년 4월~2002년 11월: ㈜니츠 기술이사
2002년11월~현재: 한국전자통신연구원 부설연구소 책임연구원
〈관심분야〉 정보보증, 컴퓨터 네트워크 보안

사 진

서 정 택 (Jung-taek Seo) 정회원
1999년 2월: 충주대학교 컴퓨터공학과 졸업
2001년 2월: 아주대학교 컴퓨터공학과 공학석사
2006년 2월: 고려대학교 정보보호대학원 정보보호공학 공학박사
2000년 11월~현재: 한국전자통신연구원 부설연구소 선임연구원/과제책임자
〈관심분야〉 스마트그리드 시스템 및 통신 보안, 제어시스템 보안, 제어시스템 통신 프로토콜 보안, 취약성 분석평가, DDoS 공격 탐지 및 대응