情報保護學會論文誌
第19卷 第1號, 2009. 2

커널 기반 데이터를 이용한 효율적인 서비스 거부 공격 탐지 방법에 관한 연구*

정 만 현,[1†] 조 재 익,[1] 채 수 영,[2] 문 종 섭[1‡]

[1]고려대학교 정보경영공학전문대학원, [2]한국전자통신연구원 부설연구소

An Efficient Method for Detecting Denial of Service Attacks Using Kernel Based Data*

Man-hyun Chung,[1†] Jae-ik Cho,[1] Soo-young Chae,[2] Jong-sub Moon[1‡]

[1]Graduate School of Information Management and Security, Korea University, [2]The Attached Institute of ETRI

요 약

현재 커널 기반 데이터인 시스템 호출을 이용하는 호스트 기반 침입 탐지 연구가 많이 진행되고 있다. 시스템 호출을 이용한 침입 탐지 연구는 시퀀스 기반과 빈도 기반으로 시스템 호출을 전 처리 하는 방법이 많이 사용되고 있다. 실시간 침입 탐지 시스템에 적용할 때 시스템에서 수집 되는 시스템 호출 데이터의 종류와 수집 데이터가 많아 전처리에 어려움이 많다. 그러나 비교적 시퀀스 기반 방법보다 전처리 시간이 작은 빈도 기반의 주로 방법이 사용 되고 있다.

본 논문에서는 현재에도 시스템 공격 중 비중을 많이 차지하고 있는 서비스 거부 공격을 탐지 하기위해 빈도 기반의 방법에 사용하는 전체 시스템 호출을 주성분 분석(principal component analysis)을 이용하여 주성분이 되는 시스템 호출들을 추출하여 베이지안 네트워크를 구성하고 베이지안 분류기를 통하여 탐지하는 효율적인 방법을 제안한다.

ABSTRACT

Currently much research is being done on host based intrusion detection using system calls which is a portion of kernel based data. Sequence based and frequency based preprocessing methods are mostly used in research for intrusion detection using system calls. Due to the large amount of data and system call types, it requires a significant amount of preprocessing time. Therefore, it is difficult to implement real-time intrusion detection systems.

Despite this disadvantage, the frequency based method which requires a relatively small amount of preprocessing time is usually used. This paper proposes an effective method for detecting denial of service attacks using the frequency based method. Principal Component Analysis(PCA) will be used to select the principle system calls and a bayesian network will be composed and the bayesian classifier will be used for the classification.

Keywords : System call, Principal Component Analysis, Denial of Service, Host based IDS

접수일(2008년 9월 2일), 수정일(2008년 11월 6일),
게재확정일(2008년 12월 10일)
* 이 연구에 참여한 연구자(의 일부)는 '2단계 BK21사업'의 지원비를 받았음
† 주저자, manhyun4@korea.ac.kr
‡ 교신저자, jsmoon@korea.ac.kr

Ⅰ. 서 론

침입탐지 기법은 일반적으로 알려진 공격을 이용한

오용 탐지(misuse detection)와 이상 탐지(anomaly detection)의 두 가지 유형으로 나누어진다[1]. 대부분의 상용제품들은 알려진 공격 기반의 오용탐지 시스템으로 탐지속도와 탐지율 측면에서는 빠르고 효율적이라는 장점을 가지지만, 각각의 공격에 대한 공격 형태를 가지지 않으면 공격을 탐지 할 수 없고, 동일한 형태의 공격을 하더라도 공격 형태를 우회할 수 있는 방법이 있다면 또한 탐지를 할 수 없다는 단점을 갖는다. 반면 이상 탐지 기법은 침입 탐지 기법에 사용되는 유형으로 오랜 기간 축적된 정상적인 데이터나 공격데이터를 수집하여 학습시킴으로써 모델링된 데이터를 이용하여 모델링된 데이터와 다른 형태의 패턴을 가진 데이터를 탐지 하는 기법으로 가장 큰 특징으로 새로운 형태의 공격을 탐지 할 수 있다는 것이다.

호스트 기반[2] 이상 탐지 기법에서 사용자의 행위나 또는 시스템의 행위를 모델링하기 위하여, 일반적으로 커널 기반데이터인 시스템 호출이 사용된다[3,4].

현재 시스템 호출을 이용한 다양한 호스트 기반 침입 탐지 연구들이 다양하게 진행되고 있다. 대표적 연구로 Quan Qian[5]은 Basic Security module(BSM) 데이터와 University of New Mexico의 시스템 호출 번호 만을 사용한다. 데이터를 전 처리 할때 데이터의 각 행을 process ID와 system call number 으로 구성하고 슬라이딩 윈도우를 변형하며 three-Hidden Markov Model에 적용하는 방법을 제안 하였다.

Seung-Hyun Paek[6]는 프로세스 별로 시스템 호출의 빈도를 계산 하여 데이터 마이닝 기법 중의 하나인 C4.5 분류 알고리즘을 개선하여 동일한 탐지 성능을 유지하면서 소형의 침입 탐지 모델을 생성하는 sC4.5 알고리즘을 개발하고 제안하였다. Liao and Vemuri[3] 에서는 프로세스 별로 시스템 호출을 분류하고 문서 분류 알고리즘을 이용하여 전처리 하고, KNN 알고리즘을 사용하여 탐지 하는 방법을 발표하였다. 이 논문에서는 전체 발생한 시스템 호출을 다 사용하지 않고, 각 시스템 호출의 빈도를 계산하여 내림차순으로 50개를 사용하였다. Wenjie Hu and Liao and Vemuri[4] 에서는 위 논문과 같은 방식으로 가중치방법을 사용하고 RSVM (Robust Support Vector Machines)을 이용하여 탐지하고 KNN 알고리즘 , SVM 알고리즘과 비교 평가 하였다.

시스템 호출을 이용한 연구는 전처리에서 위와 같이 크게 시스템 호출의 시퀀스 기반과 빈도기반의 연구위주로 진행 되고 있다. 시퀀스 기반의 연구 경우 빈도 기반의 연구들 보다. 불필요한 전처리 시간을 소비하고 실시간 시스템에 적용이 힘들다. 그래서 본 논문에서는 서비스 거부 공격 탐지를 위해 커널기반 시스템 호출의 빈도를 이용하여 전처리 하고 주성분 분석을 통해 주성분이 되는 시스템 호출을 추출하여 발생하는 전체 시스템호출을 사용하는 것 보다 필수적인 시스템호출만 이용한 효율적인 침입 탐지 방안을 제안한다.

본 논문의 구성은 다음과 같다. 2장은 관련 연구로 커널기반 데이터인 시스템 호출의 빈도를 이용한 연구 사례를 설명하고 3장은 데이터에서 파라미터 추출과 전처리 및 분류하는 제안 방법에 대한 설명하고 4장에서는 데이터 수집 및 데이터 전처리와 결과 분석을 기술한다. 마지막으로 5장은 결론으로 본 논문을 마치고자 한다.

Ⅱ. 관련 연구

침입 탐지 시스템은 네트워크 기반 침입탐지 시스템과 호스트 기반 침입탐지 시스템 두 가지로 분류된다[2]. 네트워크 기반의 침입 탐지 시스템은 네트워크 패킷을 모니터링 하거나 트래픽의 변화량을 분석 하는 방향으로 연구가 진행되고 있으며 호스트 기반 침입탐지 시스템은 시스템에서 발생 하는 커널 기반 데이터나 시스템 로그 기록, 시스템의 메모리, cpu 등의 사용내역을 이용한 연구들이 진행되고 있다. 특히 커널 기반 데이터를 이용한 연구가 활발히 진행되고 있다. 커널 기반 데이터의 경우 시스템에서 발생하는 행위를 표현 할 수 있는 데이터를 말하는데 대표적으로 사용자와 프로세스들의 행위를 나타내는 시스템 호출을 많이 이용한다. 시스템 호출을 이용한 침입 탐지 시스템의 대표적 연구로 Liao and Vemuri[3], Wenjie Hu and Liao and Vemuri[4], Seung-Hyun Paek[6]의 연구가 있다.

Liao and Vemuri는 MIT에서 제공하는 1998 DARPA Basic Security Module(BSM)[7] 데이터의 일반 행위 데이터와 공격행위 데이터에서 시스템 호출을 프로세스 별로 추출하여 시스템 호출 빈도를 계산하고 가장 많은 빈도를 가진 시스템 호출 49개를 추출하고 나머지를 기타로 하여 총 50개의 시스템 호출을 추출하

는 방법으로 전처리를 하고 각 프로세스별 시스템 호출의 빈도를 이용하여 정보 검색분야에서 많이 사용되는 TF-IDF 가중치 방법을 적용하여 시스템 호출의 값을 결정하였다. TF-IDF는 문서에서 각 단어의 가중치를 해당 문서에서 각 단어의 빈도와 역 문헌빈도(IDF) 의 곱으로 나타내는 방식이다[3]. 문서를 프로세스로 문서 안의 단어를 시스템 호출로 하여 계산된 결과 값을 K-Nearest Neighbor 알고리즘에 적용하였고 공격과 일반 행위의 거리 값을 구하기 위하여 Cosine Similarity를 사용하여 침입 탐지를 하는 방법을 제안하였다.

Wenjie Hu and Liao and Vemuri는 Liao and Vermuri가 사용한 MIT데이터를 세션별로 나누어 세션에서 발생하는 프로세스를 정리하여 프로세스에서 발생한 시스템 호출들 전체를 이용하여 시스템 호출의 빈도를 계산한다. 그리고 전 처리된 데이터를 Liao가 사용한 TF-IDF를 이용하여 시스템 호출의 가중치를 계산하고, SVM 과 RSVM 알고리즘에 적용하여 K-NN 알고리즘과의 비교를 하고 SVM 과 RSVM의 비교를 통해 SVM에서 계산에서 사용되는 Support Vector를 개수를 줄여서 같은 성능에 처리시간을 단축하는 방법을 제안하였다.

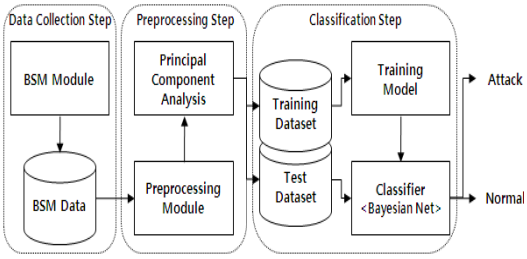
Seung-Hyun Paek 는 University of New Mexico의 수집 데이터에서 프로세서별로 발생한 시스템 호출별 빈도수를 계산하고 KDD99Cup 평가에서 사용된 의사결정나무 분류 기법인 C4.5와 확률론에 기반한 Naive Bayesian, 기계학습에 사용되는 SVM, 인스턴스 기반 분류 기법인 KNN 분류 알고리즘과 C4.5의 문제점을 보완한 sC4.5를 비교 분석하고 개발 하였다.

Ⅲ. 제안 방법

전체적인 구성 방법은 첫 번째 커널의 BSM Module을 이용하여 데이터를 수집하고, 두 번째 수집된 데이터를 전처리 후 주성분 분석을 이용하여 주성분을 구한 다음 세 번째 주성분을 사용하여 공격 데이터와 일반 데이터를 모델링 하고 판별하는 3부분으로 구성되며 다음 [그림 1]과 같다.

3.1 파라메터 추출과정

파라메터 추출 과정은, [그림 1]의 첫 번째와 두 번째

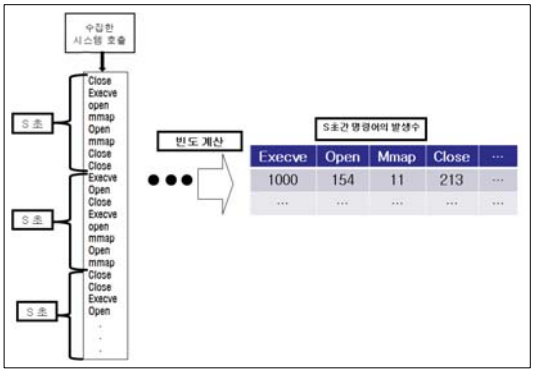


[그림 1] 서비스 거부공격 탐지 시스템 구조도

단계에 해당한다. 일반 행위와 서비스 거부 공격 의 BSM 데이터 수집과, 수집된 BSM 데이터를 전처리후 주성분 분석과 Karhunnen-Loeve(KL) 변환 하여, 모델링 파라메터를 추출한다.

3.1.1 데이터 추출과정

수집된 대용량 커널 기반 데이터를 하루 단위로 분리하여 카이 제곱 검정으로 동질성 검정을 하고, 신뢰범위 95%이내의 데이터 중 하나를 사용하여 일반 행위와 공격행위를 기본적인 통계 값을 갖기 위한 시스템 호출이 발생하는 시간의 임계 S로 하고 단위를 초 단위로 하여 1 ~ *N*초로 빈도를 반복적으로 계산하여 통계적 임계값을 구한다.



[그림 2] 시스템 호출의 빈도 계산

3.1.2 주성분 분석과 KL 변환

통계학의 다변량 분석(Multivariate Anlysis)에서는 각 차원 간에 상관이 있는 변량 데이터를 다룬다. 주성분 분석은 다차원 특징 벡터로 이루어진 데이터에 대하여 높은 차원에서의 정보를 유지하면서 낮은 차원으로

차원을 축소시키는 다변량 데이터 처리 방법 중의 하나이다[10,11].

본 논문에서는 시스템에서 수집된 전체 시스템 호출을 시간 단위로 분리하여 발생한 전체 시스템 호출을 기준으로 각 시스템 호출의 발생 빈도를 수량화 하고 m은 측정 회수, n는 시스템 호출의 빈도로 $m \times n$ 행렬 X로 구성한다. 그리고 수식 (1)에 집합X를 대입하여 평균을 구한다.

$$m_i = E[X] \quad (i = 1 \cdots m) \tag{1}$$

수식 (2)에서 구해진 평균값을 구하고 수식 (2)을 이용하여 데이터의 변화하는 양상을 나타내는 공분산 $n \times n$ 행렬을 만든다.

$$C_x = E[(X - m_x)(X - m_x)^T] \tag{2}$$

위식으로 구해진 공분산 행렬을 이용하여 다음 수식 (3)을 만족하는 고유값과 고유벡터를 구한다. 여기서 구한 고유값과 고유벡터는 전체 행렬에서 전체를 대표할 수 있는 서로 독립적인 인공변수이다.

$$Ax = \lambda x \tag{3}$$

고유 값을 내림차순으로 정렬하고 그에 상응하도록 고유벡터를 정렬하여 주성분 값을 추출하고 새로운 행렬 A를 만들어 이를 변환행렬로 사용하여 벡터 x를 KL 변환 식으로 차원을 축소한다.

$$y = A(x - m_x) \tag{4}$$

위 식에서 구한 y벡터의 평균은 0이 되고, 공분산 행렬은 식 (2)의 C_x로부터 구한 고유 값으로 이루어진 대각 행렬이 되며 y의 공분산과 C_x의 고유 값과 고유벡터가 동일하게 값을 가지게 된다.

그리고 특정 고유 값들의 비율 합이 95% 이상의 고유 값을 사용하여 차원이 변환된 값을 구한다.

위 결과 데이터인 주성분과 차원 변환된 데이터를 비교 분석 한다.

3.1.3 베이지안 네트워크

베이지안 네트워크는 불확실한 상황 하에서 지식을 표현하고 결론을 추론하고자 할 때 유용하게 쓰일 수 있는 도구이다. 그리고, 광범위한 데이터를 변수간의 관계에 따라 그래프로 표시함으로써 단순히 분류하거나 예측 하는 데에서 간과할 수 있는 데이터의 특성을 이해 할 수 있게 해 준다. 베이지안 네트워크는 변수를 노드로 표현하며, 노드와 그 노드들 간의 인과관계를 나타내는 간선들로 구성된 DAG(Directed Acyclic Graph)이다[12,13,14].

여기서 각 노드는 조건부 확률을 나타내는 확률 테이블을 가지고 이것이 각 연결선의 강도를 모델화한다. 이 두 노드 사이에 연결선이 없다는 것은 서로 독립적이라는 의미로 해석된다.

N 개의 시간 단위의 빈도 데이터 D를 n개의 시스템 호출로 구성한 $X = X_1, \ldots, X_n$ 에 대한 베이지안 네트워크는 X의 시스템 호출들 간의 종속적 조건들을 정해주는 네트워크 구조와 각 시스템 호출들에 대한 주변 확률 P로 이루어 져있다. 각 노드를 변수로 하고 $P_a(X)$를 변수 X의 부모 쪽 노드로 표시하면 데이터의 분포를 네트워크 구조에 따른 결합 확률 분포(Joint Probability Distribution)를 식(5)과 같이 나타낼 수 있다.

$$P(x_1, x_2, \ldots, x_n) = \Pi_{i=1}^{n} P(x_i | p_a(x_i)) \tag{5}$$

여기서 $P_a(x_i)$는 x_i의 부모노드를 나타내고, A→B 의 그래프 구조를 가질 때 노드 A는 노드 B의 부모노드가 된다. 다음 식(6)와 같이 표현된다.

$$P(x_1, x_2, x_3, x_4, x_5) = \tag{6}$$
$$P(x_1) P(x_2|x_1) P(x_3|x_1) P(x_4|x_2 x_3) P(x_5|x_4)$$

위의 식으로 구성된 네트워크의 노드 간의 결합 확률 분포와 베이지안 분류기를 이용하여 판별한다.

3.2 데이터 분류 및 평가 방법

본 논문 3.1의 데이터 추출 과정을 통해 얻어진 결합 확률분포를 가지고 베이지안 정리를 통해 분류하고 분류한 결과를 ROC 곡선으로 표현한다.

3.2.1 베이지안 분류기

본 논문에서는 공격데이터를 판별하기 위해서 베이지안 분류기를 사용하였다. 베이지안 분류기는 베이지안 이론을 이용하여 본 논문 3.1.3에서 설명한 베이지안 네트워크를 통해 일반데이터와 공격데이터의 결합 확률분포 표를 구하고 이를 이용하여 베이지안 정리를 이용하여 판별한다. 수집된 일반데이터를 w_1, 공격데이터를 w_2를 구분하여 베이지안 네트워크를 이용하여 X의 확률분포 함수 $P(X)$로 특정 패턴 w_i의 발생 가능 확률을 $P(w_i)$로 특정 패턴 w_i의에서 테스트 데이터 x 가 관측될 조건부 확률 $P(w_i|x)$을 이용 하여 식(7)의 베이지안 정리를 나타낸다.

$$P(w_i|x) = \frac{P(x|w_i)P(w_i)}{P(x)} \quad (7)$$

이때 $P(x)$는 다음 식과 같다.

$$P(x) = \sum_{i=1}^{k} p(x|w_i)P(w_i) \quad (8)$$

관측된 값 x 가 변함에 따라 사전확률 $P(w_i)$가 사후확률 $P(w_i|x)$로 변화되는 것을 확인할 수 있으며 다음 식을 통하며 데이터를 분류한다.

$$P(x|w_i)P(w_i) > P(x|w_j)P(w_j) \quad i \neq j \quad (9)$$

3.2.2 Receiver Operating Characteristic(ROC) 곡선

본 논문에서는 분류기의 성능을 평가하는 기준으로 많이 사용되어 지는 ROC 곡선을 이용하여 분류기의 성능을 평가하고자 한다[15]. ROC 곡선의 가로축은 FPR(False Positive Rate)이고 세로축은 TPR(True Positive Rate)으로 구성되어져 있고, ROC 공간에 주어진 FPR, TPR의 값을 점으로 나타낸다. 분류기를 통해서 얻어진 값을 [표 1]과의 형태의 분할표를 만들고 분활표를 기준으로 FPR, TPR의 값을 구한다.

$$FPR = FP/(FP+TN) \quad (10)$$
$$TPR = TP/(TP+FN) \quad (11)$$

[표 5] ROC 분할표

True Positive	False Positive
False Negative	True Negative

Ⅴ. 실험 결과

4.1 자체 데이터 수집을 위한 실험

일반 행위의 경우 현재 사용 중인 일반 대학시스템의 커널 기반 데이터를 사용하였고, 공격데이터 의 경우 폐쇄망에서 일대일 구조로 공격을 시도 하여 커널 기반데이터를 수집하였다.

4.1.1 데이터 수집 및 검정

본 논문에서는 일반 행위데이터를 수집하기 위해서 일반 대학에서 운영하고 있는 솔라리스 9 시스템에서 BSM 데이터를 2주간 수집하였고, 공격 행위데이터는 폐쇄망에서 일대일 구조로 연결하여 가상의 공격대상 시스템을 솔라리스9 시스템으로 구축하고 TCP SYN flood 공격을 시도하여 시스템이 마비되는 상황까지의 데이터를 총 30회 수집하였다. 그리고 일반 행위데이터는 일일 단위로 분리한 다음 카이 제곱 검정으로 동질성 검정을 통해 하루 데이터를 사용하였고, 공격 행위데이터 역시 카이 제곱 검정의 동질성 검정을 통해 신뢰범위 95%이내의 데이터 중 하나를 사용하여 일반 행위와 공격행위를 기본적인 통계값을 갖기 위하여 30개 이상의 시스템 호출이 발생하는 시간의 임계를 5초에서 확인하였다. 그래서 본 실험에서는 5초단위로 분리 한 다음 5초 동안의 발생 빈도를 계산 하였다.

카이제곱분포는 두 가지 이상의 결과가 나타날 때 관찰도수와 기대도수가 크게 차이가 나는지를 검정하거나 표본분포가 이항분포, 또는 정규분포를 따르는지 등을 검정하거나 두 변수가 서로 독립적인지의 여부를 검정할

[표 5] 5초간 시스템 호출 빈도

순 서	ioctl	close	stat	open-read	lstat	·····	acess
1	53	31	53	6	0	·····	1
2	42	16	10	5	24	·····	0
3	77	43	5	100	1	·····	1
·····	·····	·····	·····	·····	·····	·····	0
17351	0	0	1	0	0	·····	0

때 이용된다. 본 논문에서는 2주간 수집된 일반 행위 데이터와 공격 데이터의 데이터양의 차이가 많아 2주간의 데이터와 주간 데이터중의 하루 데이터를 동질성 검정을 통해 동질성을 검정 한다. 검정 방법은 다음과 같다.

[표 7] 관찰도수와 기대도수

사건	E_1	E_2	E_3	……	E_k
관찰도수	o_1	o_2	o_3	……	o_k
기대도수	e_1	e_2	e_3	……	e_k

위 표는 어떤 표본에서 발생 가능한 사건을 E, 사건에서 발생하는 빈도를 o로 표현하여 이를 확률이론에 따라 e를 기대도수로 표현하였다.

[표 3] 기대도수 계산 예제

	종속변수 A	종속변수 B	close
독립변수A	a	b	a+b
독립변수B	c	d	c+d
계	a+c	b+d	a+b+c+d

- a의 기대도수 = (a+b)(a+c)/(a+b+c+d)
- b의 기대도수 = (a+b)(b+d)/(a+b+c+d)
- 기대도수 = (c+d)(a+c)/(a+b+c+d)
- d의 기대도수 = (c+d)(b+d)/(a+b+c+d)

관찰도수와 기대도수간의 차이를 측정하는 도구를 다음과 식과 같은 X^2 통계량으로 나타낼 수 있다.

$$X^2 = \frac{(o_1 - e_1)^2}{e_1} + \frac{(o_2 - e_2)^2}{e_2} + \cdots + \frac{(o_k - e_k)^2}{e_k} = \sum_{i=1}^{k} \frac{(o_i - e_i)^2}{e_i} \quad (12)$$

본 논문에서는 데이터들이 동질성을 가진다, 라는 귀무가설을 세우고 식(12)로 계산된 X^2 계산 값과 자유도를 통해 구한 임계치 값과 비교하여 동질성 검정을 한다. 본 논문에서는 커널 기반 데이터인 시스템 호출의 빈도를 관찰 도수로 하여 기대도수를 구하고 X^2 통계량을 통해 일반화된 데이터를 본 논문 실험에 사용한다.

본 실험에서는, 수집된 2주간 데이터를 일일 데이터로 분리를 한 후 임의로 하루 데이터 선택하여 2주간 전체 데이터와 선택된 하루 데이터를 전체 데이터와 비교한다. 2주간 나온 데이터에서 발생한 시스템 호출의 빈도를 계산 하여 빈도가 높은 순서로 10개를 선별하여 그것을 비교 속성으로 한다. 다음 [표 4] 같이 계산된 데이터를 이용하여 기대도수를 구한다.

[표 4] 시스템 호출의 관측도수와 기대도수

Day		ioctl	close	stat	open-read	lstat	……
1	관측도수	578903	214138	158911	154379	90363	……
	기대도수	559660.003	234310.358	138795.149	142577.015	98002.038	
2	관측도수	734647	393497	193687	249460	207662	……
	기대도수	864733.045	362033.929	214452.975	220296.350	151423.365	

위 표의 관측도수와 기대도수를 이용하여 X^2의 계산한 값을 구하고 자유도를 다음과 같이 자유도 = (열의 수 -1) * (행의 수 -1)을 구하여 Chi-square 분포표의 유의수준 5%의 수치와 비교하여 데이터의 동질성을 검정한다.

4.1.2 효율적인탐지를 위한 속성 선정

2장에서 설명한 Chi-square 검정을 통해 동질성 검정이 된 24시간 데이터와 공격데이터를 5초 간격으로 나누어 하루 동안 발생한 전체 시스템 호출 64개를 기준으로 발생한 빈도를 계산하여 다음 [표 5]같은 형식으로 이용하여 데이터를 정렬한다. 그리고 본 논문의 2절의 수식 (2)에 대입하여 평균값을 구하고 수식 (3)을 통해 공분산 행렬을 구한다. 마지막으로 수식 (4)를 만족하는 고유값을 구한다음 내림차순으로 정렬하여 다음 수식(13)을 이용하여 구한 각 주성분의 비율의 합이 95%되는 범위의 주성분을 추출 한다.

$$\frac{\lambda_i}{\lambda_1 + \lambda_1 + \cdots + \lambda_k}, \; i = 1, 2, \cdots, k \quad (13)$$

4.1.3 베이지안 분류기를 이용한 탐지

시스템에서 수집된 일반 시스템 호출 데이터와 공격 시스템 호출 데이터를 전처리 후 [표 5]와 같이 각 속성 값의 평균을 구하고 그 평균값 보다 큰 것은 1 작은 것은 0이라고 하여 다시 데이터를 처리한다. 그리고 0 또는 1로 구성된 데이터 테이블로 본 논문 2장 베이지안 분류기에서 서술한 식(5) 이용하여 네트워크 구조와 결합 확률을 만들고 이를 식(6)을 통해 조건부 확률을 구해 베이지안 이론으로 침입 여부를 판별한다.

[표 6] 결합 확률표

순 서	ioctl	close	stat	open-read	lstat	·····	발생 빈도
1	1	1	0	1	0	·····	196
2	1	1	0	1	1	·····	143
3	1	1	1	1	1	·····	46
·····	·····	·····	·····	·····	·····	·····	·····
17351	1	1	1	0	0	·····	50

4.1.4 판별 결과 비교

동질성 검정을 위하여 수집된 2주간 데이터 중에 하루의 데이터와 2주간의 데이터를 Chi-square 동질성 검정을 하였다.

다음 [표 7]는 본 논문에서 제안하는 주성분 분석을 통해 추출된 주성분 비율 합이 98%가 되는 시스템 호출을 나타내는 것이다.

[표 7] 주성분의 비율

순 서	시스템 호출	비율
1	ioctl	49.91%
2	close	14.29%
3	open-read	13.42%
4	stat	11.34%
5	fcntl	8.37%
6	lstat	1.42%

[표 8]은 일반 행위 시스템 호출과 공격 행위 시스템 호출을 모델링한 데이터를 주성분을 이용하는 방법과 전체 발생 시스템 호출을 사용한 방법과 KL 변환을 한 방법을 [표 6]으로 비교 하였다.

[표 8] 탐지율 비교

	전체 시스템 호출	KL 변환	비율 97%
탐지율	99.9808	99.9808	99.9808
오탐율	0.0192	0.0192	0.0192

실험 결과 전체 시스템 호출을 사용 하였을 때와 주성분 비율합이 97% 일 때 까지 동일한 탐지율과 FP를 보여주는 것을 확인할 수 있다. 그리고 주성분 분석과 KL 변환을 통해 차원변환을 한 결과의 탐지율은 99.9808%로 동일한 결과를 나타내었다.

다음은 [표 9]는 비율 97%에 해당하는 Confusion Matrix를 나타낸 것이고 [그림 2]는 결과에 따른 ROC 곡선이다.

[표 9] 비율 97%의 Confusion Matrix

TP rate	FP rate	
1	0.038	정 상
0.962	0	공 격

ROC의 결과는 TP가 1일 때 FP는 0.038이 나왔고 FP과 0일 때는 TP가 0.56을 나타내었다.

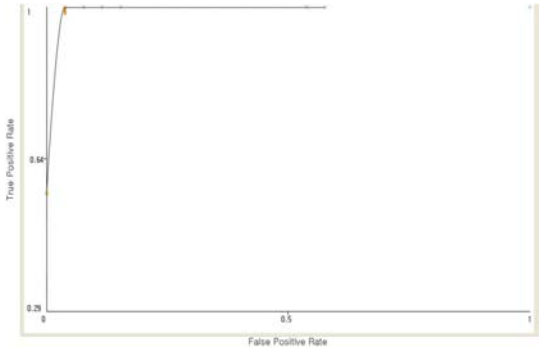
다음 [표 10]은 제안 방법에서 설명한 기존의 호스트 기반 침입탐지 시스템 알고리즘인 KNN 알고리즘에서 사용한 전처리 방법인 TF-IDF와 본 논문에서 제안한 전처리 방법을 각각 사용하여 데이터를 전처리 하고 본 논문의 분류 방법인 베이지안 정리를 사용하여 결과를 비교 하였다.

[표 10] 호스트 기반 알고리즘 탐지율 비교

	베이지안 분류기	KNN
탐지율	99.9808	99.9712
오탐율	0.0192	0.0288

Ⅴ. 결 론

본 논문은 주성분 분석을 통해 서비스 거부공격을 효과적으로 탐지 할 수 있는 방법을 제안 하였다. 기본의 연구들은 시스템 호출을 이용할 때 발생한 전체 시스템 호출을 사용하거나 시스템 호출의 발생 빈도를 체크하여 특정 범위 안의 시스템 호출을 사용하였다. 서비스 거부공격 같은 유형의 공격은 시스템 자원을 지속적으



[그림 2] 제안 방법의 ROC 곡선

로 확보하여 시스템을 마비시키는 형태를 가지는데 시스템 전체에서 발생하는 시스템 호출을 사용한다면 전처리 시간이 많이 소비되기 공격을 탐지하는데 효율적이지 못하다. 이에 본 논문에서는 주성분 분석을 통해 서비스 거부 공격 탐지에 사용될 효율적인시스템 호출을 추출하여 베이지안 분류기를 통해 침입 탐지를 적용하였을 때 6개의 주성분을 이용한 탐지가 전체 시스템 호출을 사용하였을 때와 같은 동일한 탐지결과를 보였다. 그리고 관련 논문에서 설명한 논문의 전처리 방법인 TF-IDF를 적용한 결과는 유사한 탐지율을 보였으나 TF-IDF를 구하는 절차에서 전처리 시간이 본 논문에서 제안하는 전처리 방법보다 전처리 시간이 많이 소비되었다. 다음과 같은 결과를 바탕으로 짧은 전처리를 필요로 하는 실시간 침입 탐지 시스템에 제안 방법을 활용할 수 있다. 향후 연구로 다양한 공격들의 필수 주성분을 찾는 연구가 필요하다.

참고문헌

[1] T.F. Lunt, “A survey of intrusion detection techniques,” Computer & Security, vol. 12, no. 4, pp. 405-418, June 1993.

[2] ISS, “Network vs Host-based intrusion detection,” whitepaper: Oct. 1998.

[3] Y. Liao and V. Vemuri, “Use of K-Nearest Neighbor Classifier for intrusion detection,” Computers & Security, vol. 21, no. 5, pp. 439-448, Oct. 2002.

[4] W. Hu, Y. Liao, and V. Vemuri, “Robust Support Vector Machine for Anomaly Detection in Computer Security,” International Conference on Machine Learning, pp. 4-5, June 2003.

[5] S.H. Paek, Y.K. Oh, J.B. Yun, and D.H. Lee, “The Architecture of Host-based Intrusion Detection Model Generation System for the Frequency Per System Call,” International Conference on Hybrid Information Technology 06, vol. 2, no. 2, pp. 277-283, Nov. 2006.

[6] Q. Qian and M. Xin, “Research on Hidden Markov for System Call Anomaly Detection,” Pacific Asia Workshop on Intelligence and Security Informatics 2007, LNCS 4430, pp.152-159, 2007.

[7] L. Richard, W.Joshua, Haines, J. David, K. Jonathan, and K. Das, “The 1999 DARPA off-line intrusion detection evaluation,” Computer Networks, vol. 34, no. 4, pp.579-595, Aug. 2000.

[8] J. Lemon, “Resisting SYN Flooding Dos Attacks with a SYN Cache,” BSDCon 2002, pp. 89-97, Feb. 2002.

[9] R. Oliver, “Countering SYN Flood Denial-of-Service Attacks,” Invited Talk at The 10th USENIX Security Symposium, p. 2, Aug. 2001.

[10] P.J.B. Hancock, A.M. Burton, and V. Bruce, “Face Processing: Human perception and principal components analysis,” Memory and Cognition, vol. 24, no. 1, pp. 26-40, Aug. 1996.

[11] N. Kambhatla and T.K. Leen, “Dimension reduction by local principal component analysis,” Neural Computation, vol.9, no.7, pp. 1493-1516, Oct. 1997.

[12] 양진산, 장병탁, “베이지안 네트워크를 이용한 전자상거래 고객들의 성향 분석,” 퍼지 및 지능시스템학회 논문지, 1(1), pp. 16-21, 2001년 1월.

[13] D. Heckerman, “A Tutorial on Learning with Bayesian Networks”, Technical Report MSR-TR-95-06, Microsoft Research, pp. 339-377, Mar. 1995.

[14] F. Jensen, An Introduction to Bayesian Networks,

Springer-verlag, pp. 201-208, Oct. 1996.
[15] J.P. Egan, Signal Detection Theory and ROC Analysis, NY Academic Press, p. 157, Dec. 1975.
[16] S. Alok, K.P. Arun, and K.P. Kuldip, “Intrusion detection using text processing techniques with a kernel based similarity measure,” Computers & Security, vol. 26, no. 7-8, pp. 488-495, Dec. 2007.
[17] N. Friedman and M. Goldszmidt, “Learning Bayesian networks with local structure,” Learning in Graphical Models, Kluwer Acadamic Publishers, pp. 421-459, Mar. 1998.
[18] N. Friedman and Y. Singer, “Efficient bayesian parameter estimation in large discrete domains,” Advances in Neural Information Processing systems, pp. 417-423, Mar. 1998.

<著 者 紹 介>

정 만 현 (Man-hyun Chung) 학생회원
2006년 2월: 동국대학교 컴퓨터공학과 학사
2006년 3월～현재: 고려대학교 정보경영공학전문대학원 석사과정
<관심분야> 시스템 보안, 네트워크 보안, 침입 탐지

조 재 익 (Jae-ik Cho) 학생회원
2005년 2월: 동국대학교 컴퓨터학과 학사
2008년 2월: 고려대학교 정보경영공학전문대학원 석사
2008년 3월～현재: 고려대학교 정보경영공학전문대학원 박사과정
<관심분야> 네트워크 모델링, 패턴 인식

채 수 영 (Soo-young Chae) 정회원
1999년 8월: 숭실대학교 대학원 정통신공학과 졸업
2000년 1월～2001년 9월: 한국정보보호진흥원 근무
2001년 10월～현재: 한국전자통신연구원 부설연구소 근무
2006년 2월～현재: 고려대학교 정보경영전문대학원 박사 수료
<관심분야> 정보보호, 침입탐지

문 종 섭 (Jong-sub Moon) 종신회원
1981년～1985년: 금성 통신 연구소 연구원
1991년: Illinois Institute of technology 졸업(전산학 박사)
1993년～현재: 고려대학교 전자 및 정보공학부 교수
<관심분야> 생체인식, 침입탐지, 운영체제