PCA와 TDNN을 이용한 비정상 패킷탐지

정성윤*, 강병두*, 김상균**
*인제대학교 전산학과
**인제대학교 컴퓨터공학부
e-mail:yuni66@korea.com

An Intrusion Detection System Using Principle Component Analysis and Time Delay Neural Network

Sung-Yoon Jung*, Byung-Doo Kang*, Sang-Kyoon Kim**
*Dept of Computer Science, InJe University
**Dept of Computer Engineering, InJe University

요 약

기존의 침입탐지 시스템은 오용탐지모델이 널리 사용되고 있다. 이 모델은 낮은 오판율(False Alarm rates)을 가지고 있으나 새로운 공격에 대해 전문가시스템(Expert Systems)에 의한 규칙추가를 필요로 하고, 그 규칙과 완전히 매칭되는 시그너처만 공격으로 탐지하므로 변형된 공격을 탐지하지 못한다는 문제점을 가지고 있다. 본 논문에서는 이러한 문제점을 보완하기 위해 주성분분석(Principle Component Analysis ; 이하 PCA)과 시간지연신경망(Time Delay Neural Network ; 이하 TDNN)을 이용한 침입탐지 시스템을 제안한다. 패킷은 PCA를 이용하여 주성분을 결정하고 패킷이미지패턴으로 만든다. 이 연속된 패킷이미지패턴을 시간지연신경망의 학습패턴으로 사용한다.

1. 서론

정보통신서비스가 급속히 발전함에 따라 해킹이나 웜 바이러스, 대규모 서비스 거부공격과 같은 네트워크상의 범죄가 급증하고있다. 이에 대한 대책으로 방화벽이나 침입탐지시스템(Intrusion Detection System ; 이하 IDS)과 같은 기술이 보급되고 있다[1].

IDS는 알려져 있거나 잠재적 위협으로부터 네트워크를 보호하는데 목적이 있다. 네트워크 기반 IDS 모델에는 알려진 침입행위를 이용하여 침입을 탐지하며 정해진 모델과 일치하는 경우를 침입이라 하는 오용 침입탐지 기법(Misuse Detection)과 사용자의 패턴을 분석하여 입력패턴과 비교하여 정해진 모델을 벗어나는 경우를 침입으로 간주하는 비정상 침입탐지 기법(Anomaly Detection)이 있다[2]. 이러한 탐지방법 중에서 오용탐지기법이 낮은 오판율(False alarm rates) 때문에 가장 널리 사용되고 있다[3]. 이 기법은 대부분 알려진 공격탐지를 위해 규칙기반 시스템을 사용한다. 이 시스템은 새로운 공격 발생 시 전문가 시스템(Expert Systems)에 의해 규칙이 추가되어야한다. 그리고 그 규칙과 완전히 매칭되는 시그너처만을 공격으로 탐지하기 때문에 변형 또는 우회 공격에 대한 유연성이 없다. 기존의 IDS는 스니핑(Sniffing)속도의 한계로 인해 네트워크 상의 모든 패킷을 수집하고 분석하는 것이 불가능하다.[4] 따라서 새로운 변종의 공격뿐만 아니라 패킷 일부분만으로 공격을 탐지할 수 있는 연구가 필요하다. 본 논문에서는 이러한 문제점을 해결하기 위해 PCA와 TDNN을 이용한 침입탐지 시스템을 제안한다.

본 논문에서 제안하는 침입탐지 시스템은 입력 값으로 패킷 헤더의 특정 값이나 감사자료를 통한 접근방식과는 달리 PCA를 통한 패킷이미지패턴을 사용함으로써 더욱 광범위한 공격 유형을 탐지할 수 있다. 이러한 이유로, 다변량 통계분석방법 중 하나인 PCA를 이용한다. 패킷정보를 최대한 설명할 수 있는 독립적인 인공변수(Artificial Variable)들을 유

도하여 주성분을 구한다. 이러한 주성분은 일련의 패킷정보들의 선형결합으로 표시되며, 단순한 구조로 요약되는 패킷이미지패턴을 만든다. 정상적인 흐름과 비정상적인 흐름에 대한 패킷이미지패턴을 학습하는 TDNN 분류기를 구현한다.

논문의 구성은 다음과 같다. 먼저, 2장에서는 제안한 PCA와 TDNN을 이용한 침입탐지시스템에 대해 설명하고 3장에서는 실험 및 결과를 다루었다. 끝으로 4장에서는 결론을 말한다.

2. PCA와 TDNN을 이용한 침입탐지시스템

2.1 침입탐지시스템의 구성

본 논문에서 제안하는 PCA와 TDNN을 이용한 침입탐지 시스템의 전체 흐름도는 그림 1과 같다.

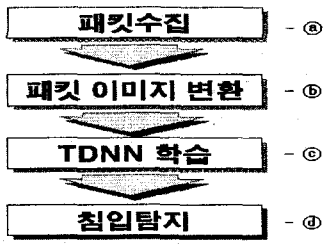

그림 1. 침입탐지시스템의 구성

ⓐ 패킷 수집기는 libpcap 라이브러리를 이용하여 패킷을 수집하고 시간, 길이, 로우(raw) 데이터 정보를 가지는 패킷 구조체를 반환한다.

ⓑ PCA를 통해 패킷이미지패턴을 만든다.

ⓒ 패킷이미지패턴을 신경망 학습을 위해 정규화하고 TDNN 학습을 위해 사용된다.

ⓔ 학습이 완료되면 실시간 네트워크 침입탐지를 하게되고, 그 결과를 정상 패킷과 비정상 패킷으로 구별한다. 패킷을 연속한 패킷이미지 패턴으로 처리함으로써 공격 이미지 일부분만을 감지하더라도 이와 가장 유사한 패턴으로 구별해 낼 수 있다.

2.1.1 패킷수집

패킷 수집을 위해 libpcap 라이브러리를 사용한다. 이것은 Berkeley 대학에서 개발한 것으로 시스템에 독립적으로 사용자 레벨에서 개발한 패킷 수집을 효과적으로 할 수 있도록 만든 공용 라이브러리이다. 패킷을 수집하려는 시스템에서 Promiscuous 모드의 상위수준 인터페이스를 제공한다[5]. 네트워크 패킷은 libpcap 라이브러리에서 제공하는 인터페이스를 사용하여 접근할 수 있다. 이 라이브러리는 거의 모든 유닉스 시스템에서 사용가능하며 tcpdump와 같은 네트워크 모니터링 도구가 이 패킷 수집 라이브러리를 사용하고 있다[5,6,7,8].

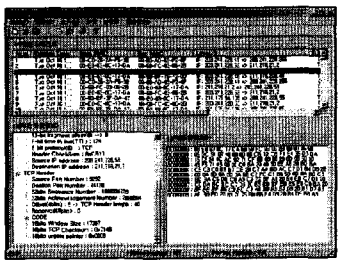

그림 2. 패킷 수집 과정

정상적인 흐름과 비정상적인 흐름에 대한 패킷 패턴을 학습하기 위해 한 대의 공격 시스템, 다섯 대의 정상사용자 시스템 그리고 패킷 수집 시스템으로 실시간 패킷 수집을 한다. 그리고 PCA를 통하여 패킷이미지패턴을 만든다. 그림 2의 상단부분은 수집된 패킷의 정보로써 수집 시간과 패킷헤더의 정보를 나타낸다. 하단부분 중 왼쪽은 선택한 패킷의 세부 정보를 보여주고, 오른쪽은 선택한 패킷의 내용을 16진수의 바이트 코드 값으로 나타낸다.

2.1.2 주성분분석 (Principle Component Analysis)

PCA는 여러 개의 변수들 사이의 관계를 분석하여 이 변수들의 선형결합으로 표시되는 새로운 주성분(principal components)을 찾고, 이 중에서 중요한 몇 개의 주성분으로 전체변동을 설명하고자 하는 다변량 통계분석법이다. 자료의 요약이나 선형관계식을 통하여 차원(dimension)을 감소시켜 해석을 용이하게 하는데 목적이 있다. 자료가 갖고 있는 전체적인 변동의 대부분을 원래변수의 수(p개)보다 적은 수(m개)의 주성분으로 설명할 수 있다고 하면, p개의 변수가 갖고 있는 정보의 대부분을 m개의 주성분으로 대체(p>m)할 수 있다. 이렇게 함으로써 변수의 차원을 감소시킬 수 있으며, 상관관계가 있는 변수들의 경향이나 변수들이 상관관계를 이루며 나타내는 변동을 몇 개의 주성분으로 파악할 수 있게 한다.[9]

2.1.3 패킷이미지패턴변환

그림 3. 패킷이미지패턴

하나의 패킷에 대한 주성분을 크게 설명하는 개별 측정치수 여덟 개를 선정하여 순차적으로 60개를 모아 패킷이미지패턴을 만든다. 패킷이미지패턴을 만들면 그림 3과 같은 Spectrogram을 생성한다. 세로줄은 하나의 패킷주성분을 나타내고 그것이 시간 순서로 60개(time step)를 본 것이다.

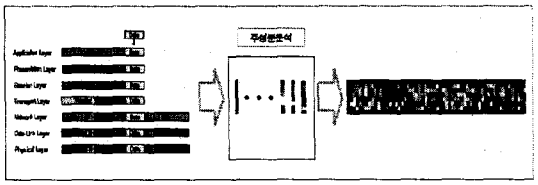

그림 4. 패킷의 학습패턴 변환

그림 4는 수집한 패킷을 PCA를 통해 패킷이미지 패턴을 만드는 과정을 보여주고 있다. 이러한 연속된 패킷이미지패턴을 TDNN의 입력으로 사용한다.

2.2 침입탐지 시스템의 TDNN 구성 및 학습

TDNN은 정적구조 신경망에 동적 요소(delay, integration)를 첨가하여 패킷이미지패턴과 같이 동적인 특성을 가진 데이터에 대해 인식할 때 좋은 인식률을 가진다.

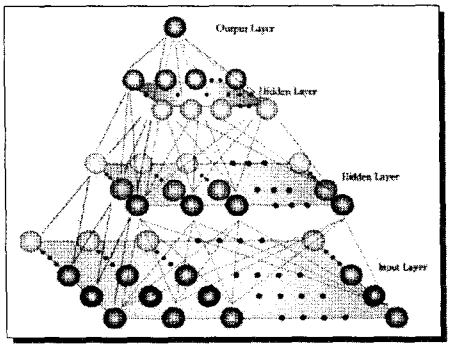

그림 5. TDNN의 전체구조

그림 5은 TDNN의 전체적인 구조를 나타내고 있다. TDNN을 사용하는 방법은 Temporal back-propagation이나 Back-propagation등 다양한 방법이 있지만 본 논문에서는 TDNN을 처음 만든 Waibel이 했던 방법을 사용하였다.

표 1. 침입탐지 시스템의 TDNN 구성

	Spatial Size	Kernal Size	Step Size	노드 개수
입력층	8	0	0	60 × 8
은닉층 1	4	4	2	29 × 4
은닉층 2	2	5	2	13 × 2
출력층	1	13	0	1 × 1

본 논문에서 구현한 TDNN은 두 layer사이에 공간축 방향으로는 항상 완전 연결(fully connected)되어 있고, 시간축 방향으로는 부분적 연결(partial connection)을 사용할 수 있다. 그림 5는 TDNN을 옆에서 시간축 방향으로만 본 그림이다. 첫 번째 은닉층에서 입력층 사이의 연결이 부분적인 것을 알 수 있다. 첫 번째 은닉층의 각 node의 시간적으로 받아들일 수 있는 kernel size가 현재 5로 설정되어 있고 step size는 4로 설정되어 있다.

TDNN 신경망에서 각 계층의 구조 결정에는 입력층의 구조가 가장 큰 영향력을 가진다. 그리고 응용 데이터의 특성을 효과적으로 수용하기 위한 각 계층의 시간축 크기(Temporal size)와 공간축 크기(Spatial size)의 결정이 다음 계층(layer)에 존재하는 node 수 결정으로 직결된다. 표 1은 TDNN을 이용한 침입탐지 시스템에서 각 계층에 대한 세부구성이다.

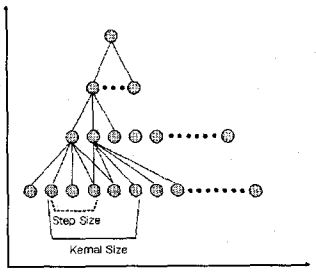

그림 6. TDNN의 단면구조

3. 실험

제안한 PCA와 TDNN을 이용한 침입탐지 시스템은 Pentium-4 PC, Windows 환경에서 Visual C++로 구현하였다. 제안한 시스템의 성능을 평가하기 위해 추출된 각 패킷 데이터 중 학습에 사용된 데이터와 학습에 사용되지 않은 데이터로 구분하여 실험하였다. 구성된 시간 지연 신경망을 학습하기 위해 SYNFlooding, Land, TearDrop, New TearDrop공격 각각에 대한 공격패킷 6000개, 정상패킷 6000개를 수집하여 랜덤하게 섞은 후에 PCA를 통해 100개의 비정상 패킷이미지패턴을 만들고 순수한 정상 패킷이미지패턴 100개와 테스트하였다. 원하는 에러값은 0.000001로 지정하여 학습하였다.

TearDrop을 학습한 신경망으로 변종공격인 New TearDrop을 테스트 한 결과는 그림 7과 같다. Target값은 데이터의 기대 값으로 0인 것은 정상 데이터이고, 1인 것은 비정상 데이터이다. Result 항목은 TDNN이 구분해낸 결과로 Normal은 정상이고, Abnormal은 공격을 나타낸다.

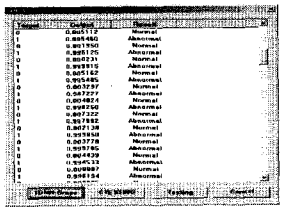

그림 7. New TearDrop결과

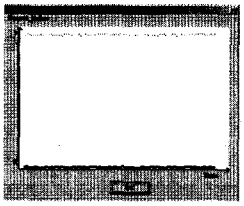

그림 8. New TearDrop (PCA적용)

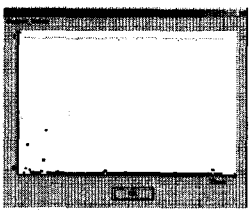

그림 9. New TearDrop (PCA미적용)

그림 8은 그림 7에서 얻은 실험 결과를 그래프로 나타낸 것이다. 하단에 분포되어 있는 "x"표시는 정상패킷, 상단에 분포되어 있는 "■"표시는 비정상패킷을 말한다. 그림 9는 PCA를 거치지 않은 패킷을 TDNN으로 실험한 결과이다. PCA를 거쳐 8개의 주성분으로 실험을 했을 때 더 잘 탐지하였다. 패킷의 차원을 축약하여, 분류할 때 영향을 미치는 불순한 요소를 제거함으로써 보다 더 좋은 결과를 가져올 수 있었다.

표 2는 TDNN을 이용한 침입탐지 시스템의 각각의 공격에 대한 실험결과를 나타낸다. SYN Flooding, Land, TearDrop, New TearDrop 공격은 정상을 비정상으로 탐지(false positive)하거나 비정상을 정상으로 탐지(false negative)하는 것 없이 정확하게 정상패킷과 비정상 패킷을 탐지해냈다. 뿐만 아니라, TearDrop 공격 이미지를 학습한 제안된 시스템은 변종 공격인 New TearDrop 공격 이미지를 20개를 제외하고는 모두 탐지해 내었다.

표 2. 제안된 시스템의 실험 결과

	false positive	false negative
SYN Flooding	0	0
Land	0	0
TearDrop	0	0
New TearDrop	0	0
변종공격 Test	0	20

4. 결론

규칙기반 침입탐지 시스템은 탐지 모듈이 정의된 시그너처 데이터베이스에서 조금이라도 그 조건에 맞지 않으면 탐지하지 못한다. 예를 들어 TearDrop 공격의 시그너처 데이터베이스만을 가지고 있고 New TearDrop공격의 시그너처 데이터베이스를 가지고 있지 않은 규칙기반 시스템은 TearDrop 공격의 변형 공격인 New TearDrop공격을 탐지해 내지 못한다. 왜냐하면 규칙기반 시스템에 있어서 TearDrop공격의 시그너처 데이터베이스는 IP 패킷의 Fragmentation된 패킷의 길이정보만을 비교하기 때문이다. 그러나 New TearDrop공격은 IP와 UDP를 모두 사용하고 있으므로 UDP헤더 정보를 탐지하지 않는 규칙기반 시스템은 New TearDrop공격을 찾아낼 수가 없다. 그러나 PCA와 TDNN을 이용한 침입탐지 시스템은 패킷패턴을 분석해서 변형되었지만 TearDrop공격과 유사한 패킷이미지패턴으로 New TearDrop공격을 분류해 낼 수 있었다.

참고문헌

[1] R. Seker, A High-Performance Network Intrusion Detection System, ACM ISBN: 1-58113-148-8 pp. 8-17 Oct. 1999

[2] Vern Paxson, Bro: A System for Detecting Network Intruders in Real-time, Computer Networks, 31(23-24), pp. 2435-2463, 14 Dec. 1999.

[3] Giorgio Giacinto, Fabio Roli, Luca Didaci, Fusion of multiple classifiers for intrusion detection in computer networks, Pattern Recog. Lett. 2003

[4] http://www.snort.org

[5] 이장현, 신경회로망을 이용한 비정상적인 패킷 탐지, 정보보호학회, vol.11 no.5 pp. 105-117, october 2001.

[6] 포항공대 유닉스 보안 연구회, Security PLUS for UNIX, 영진출판사, ISBN: 89-314-1490-0, pp. 251-254, pp. 383-400, 2001.

[7] S. McCanne and V. Jacobson, The BSD Packet Filter: A New Architechure for User-level Packet Capture, USENIX conference, January pp. 25-29, 1993, San Diego, CA.the 1993 Winter

[8] Bob Quinn, Dave Shute, Windows Sockets Network Programming, Addison Wesley Publishing Company, ISBN 0-201-63372-8, 1996.

[9] Richard A. Johnson, Dean W. Wichern, Applied Multivariate Statistical Analysis, Prentice Hall, ISBN : 0-13-092553-5, pp. 356-395, 2002.