시간지연 신경망을 이용한 침입탐지 시스템

강흥식[†] · 강병두[††] · 정성윤[†††] · 김상균[††††]

요 약

기존의 규칙기반 침입탐지 시스템은 사후처리식 규칙 추가로 인하여 새로운 변종의 공격을 탐지하지 못한다. 본 논문에서는 규칙기반 시스템의 한계점을 극복하기 위하여, 시간지연 신경망(Time Delay Neural Network; 이하 TDNN) 침입탐지 시스템을 제안한다. 네트워크상의 패킷은 바이트 단위를 하나의 픽셀로 하는 0에서 255사이 값으로 이루어진 그레이 이미지로 볼 수 있다. 이러한 연속된 패킷이미지를 시간지연 신경망의 학습패턴으로 사용한다. 정상적인 흐름과 비정상적인 흐름에 대한 패킷이미지를 학습하여 두 가지 클래스에 대한 신경망 분류기를 구현한다. 개발하는 침입탐지 시스템은 알려진 다양한 침입유형뿐만 아니라, 새로운 변종에 대해서도 분류기의 유연한 반응을 통하여 효과적으로 탐지할 수 있다.

An Intrusion Detection System using Time Delay Neural Networks

Heung-Seek Kang[†], Byoung-Doo Kang[††], Sung-Youn Jung[†††] and Sang-Kyoon Kim[††††]

ABSTRACT

Intrusion detection systems based on rules are not efficient for mutated attacks, because they need additional rules for the variations. In this paper, we propose an intrusion detection system using the time delay neural network. Packets on the network can be considered as gray images of which pixels represent bytes of them. Using this continuous packet images, we construct a neural network classifier that discriminates between normal and abnormal packet flows. The system deals well with various mutated attacks, as well as well known attacks.

Key words: Intrusion Detection, Network, Packet, Time Delay Neural Network

1. 서 론

인터넷 확산은 다양한 인터넷 서비스를 가능하게 하여 정보화 사회에 많은 이점을 가져왔다. 그러나, 이러한 이점 못지 않게 해킹을 통한 부당한 이득을 얻으려는 사이버 범죄가 증가하고 있으며, 사용법이 쉬운 해킹 프로그램의 소스 공개로 인해 다양한 해킹 방법들이 생겨나고 있어 인터넷 발전을 저해하고 있다. 야후와 같은 지명도 있는 인터넷 사이트들도 해킹 피해를 입고 있다. 그러므로, 안전한 인터넷 서비스를 위해서 침입을 탐지하고 이를 알려줄 침입탐지 시스템이 필요하다[1,2].

침입이란 비 인가된 사용자가 자원의 무결성(integrity), 기밀성(confidentiality), 가용성(availability)을 저해하는 일련의 행동들과 보안 정책을 위반하는 행위를 말한다. 이러한 침입 행위를 탐지하는 시스템을 침입탐지 시스템이라 한다.

네트워크 기반 침입탐지 모델에는 알려진 침입행위를 이용하여 침입을 탐지하며 정해진 모델과 일치하는 경우를 침입이라 하는 오용 침입탐지 기법

본 논문은 2001년도 인제대학교 학술연구조성비 보조에 의한 것임.
접수일 : 2002년 5월 17일, 완료일 : 2003년 2월 4일
[†] 인제대학교 정보컴퓨터공학부 부교수
[††] 준회원, 인제대학교 대학원 박사과정
[†††] 준회원, 인제대학교 대학원 전산학과 석사과정
[††††] 종신회원, 인제대학교 정보컴퓨터공학부 조교수

(Misuse Detection)과 사용자의 패턴을 분석하여 입력패턴과 비교하여 정해진 모델을 벗어나는 경우를 침입으로 간주하는 비정상 침입탐지 기법(Anomaly Detection)이 있다[3].

현재의 오용탐지에 대한 대부분의 접근방식은 알려진 공격에 대한 탐지를 위해 규칙기반 전문 시스템 사용을 필요로 한다. 그러나 규칙기반 침입탐지 시스템은 사후처리식 규칙추가로 인하여 새로운 변종의 공격을 탐지할 수 있는 능력이 없다. 즉, 특정 공격형태가 발견되면 형태에 따른 패킷의 흐름을 규칙화하고 시스템에 추가하는 형식으로 구현된다, 따라서 변화해나가는 다양한 공격형태를 효과적으로 탐지할 수 없다. 뿐만 아니라, 기존의 네트워크 IDS는 스니핑(sniffing)속도의 한계로 인해 네트워크 상의 모든 패킷을 수집하고 분석하는 것은 불가능하다[4]. 따라서 변형된 형태와 일부분의 공격 패킷만으로 탐지할 수 있는 방법론적 연구가 필요하다. 본 논문에서는 이러한 문제점을 해결하기 위해 시간지연 신경망을 이용한 침입탐지 시스템을 제안한다.

본 논문에서 제안하는 침입탐지 시스템은 입력 값으로 패킷 헤더의 특정 값이나 감사자료를 통한 접근방식과는 달리 패킷이미지를 사용함으로써 더욱 광범위한 공격 유형을 탐지할 수 있다. 네트워크상의 패킷은 바이트 단위를 하나의 픽셀로 하는 0에서 255사이 값으로 이루어진 그레이 이미지로 볼 수 있다. 패킷의 흐름을 시간적인 측면에서 나타내었을 때, 연속되는 여러 패킷은 일련의 연속된 이미지로 볼 수 있다. 본 연구에서는 이러한 특징을 가지는 패킷이미지들을 신경망 학습을 위한 0에서 1사이 값의 학습패턴으로 정규화(normalization)한다. 생성된 패턴들을 시간지연 신경망의 입력 값으로 사용하여, 정상적인 흐름과 비정상적인 흐름에 대한 패킷 이미지를 학습하는 시간지연 신경망 분류기를 구현한다.

기존의 다층 퍼셉트론, Kohonen Network, ART 신경망등은 데이터의 시간적인 관계를 효과적으로 반영하기 힘들다. 즉 영상과 같은 시간과는 독립적이고 정적인 데이터에 대한 패턴인식에 활용되고 있다[5,6]. 그러나 시간지연 신경망은 데이터의 시간적 관계를 수용할 수 있는 구조로서 음성과 같은 동적인 데이터의 처리 및 동적인 특성을 반영하여 정보를 추출하기 위한 방법론으로 활용되고 있다[7]. 따라서 시간지연신경망은 패킷의 전후 관계를 고려하여 침입여부를 판단해야하는 탐지 시스템의 구현을 위한 보다 적절한 분류도구이다.

개발하는 침입탐지 시스템은 알려진 다양한 침입유형뿐만 아니라, 새로운 변종의 침입에 대해서도 분류기의 유연한 반응을 통하여 효과적으로 탐지함으로써 규칙기반 시스템의 한계점을 극복하고 인터넷을 통해 들어오는 다양한 패킷들을 실시간으로 탐지할 수 있다.

2. 관련연구

2.1 규칙기반 침입탐지 시스템

규칙기반 침입탐지 시스템은 시그너처 데이터베이스를 이용해 패턴을 분석한다. 센서가 네트워크에서 트래픽 데이터를 수집해 침입 분석 엔진으로 보내 분석한 후, 침입 시그너처 데이터 베이스와 비교해 침입 흔적을 찾는다. 센서는 일반 스니퍼 프로그램과 원리가 같아서 네트워크 카드를 무작위 모드(promiscuous mode)로 세팅하고 로우 소켓이나 libpcap 등을 이용해 네트워크에서 패킷을 읽어 들이고, 침입 분석 엔진은 시그너처 데이터베이스를 참조해 패킷에서 침입의 흔적을 찾는다. 이러한 시그너처 데이터베이스는 Snort의 경우 Rule Set 파일이라는 이름으로 존재한다. 본 논문에서 제안한 시간지연 신경망을 이용한 침입탐지 시스템에서는 패킷을 읽어드리는 부분까지는 규칙기반 시스템과 같지만 침입 패킷을 탐지하는 부분에서는 패킷의 이미지를 분석한다는 점이 다르다. 규칙기반 침입탐지 시스템의 경우 Tear-Drop 패킷 분석 및 탐지법은 다음과 같다.

- 규칙기반 침입탐지 시스템의 경우 TearDrop 패킷 분석 및 탐지법

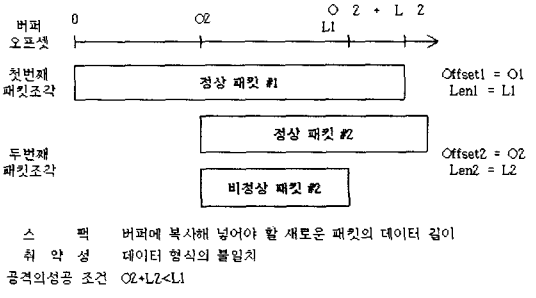


그림 1. 규칙기반 침입탐지 시스템의 TearDrop 탐지모듈

○ TearDrop 패킷 분석
- 조작된 IP 패킷 조각(Fragmentation IP Packet) 두개를 쌍으로 보냄.
- 목적지 호스트의 재조합(Reassembly)과정에서 꼬이게 만들어 오버플로어를 발생시킨다.

○ 규칙기반 침입탐지 시스템의 TearDrop 탐지법
- 처음 IP 패킷 조각(Fragmentation IP Packet)의 길이와 마지막 패킷의 길이와 옵셋(Offset) 정보를 비교해서 탐지한다.

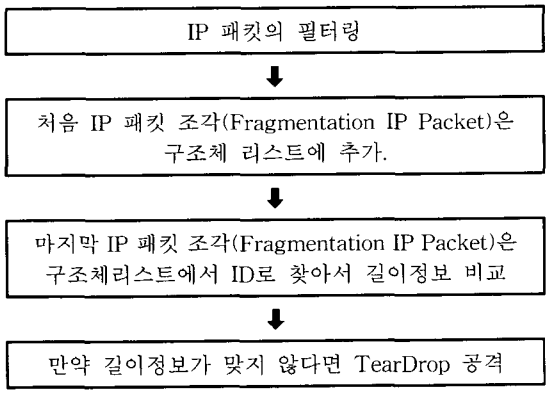


그림 2. TearDrop탐지모듈

● 규칙기반 침입탐지 시스템의 경우 New TearDrop 패킷 분석 및 탐지법

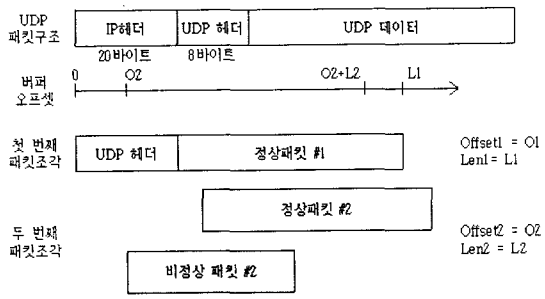


그림 3. 규칙기반 침입탐지 시스템의 New TearDrop 탐지 모듈

○ New TearDrop 패킷 분석
- 서로 중첩되도록 헤더를 조작된 IP 패킷 조각(Fragmentation IP Packet)과 UDP 패킷 조각(Fragmentation UDP Packet)을 쌍으로 수 차례 전송.
- 수신 호스트는 불완전한 UDP 패킷들이 생성되어서 시스템 자원을 낭비시킴
- 만약 수신호스트가 윈도우시스템일 경우 속도가 저하되거나 푸른화면이 뜬다

○ 규칙기반 침입탐지 시스템의 New TearDrop 탐지법
- 연속된 쌍으로 들어오는 IP와 UDP 패킷을 탐지.
- 일정개수(8개) 이상을 탐지할 때 해킹으로 간주.

규칙기반 침입탐지 시스템은 이러한 탐지 모듈이 정의된 시그너처 데이터베이스에서 조금이라도 그 조건에 맞지 않으면 탐지하지 못한다. 예를 들어 TearDrop공격의 시그너처 데이터베이스만을 가지고 있고 New TearDrop공격의 시그너처 데이터베이스를 가지고 있지 않은 규칙기반 시스템은 TearDrop공격의 변형 공격인 New TearDrop공격을 탐지해 내지 못한다. 왜냐하면 규칙기반 시스템에 있어서 TearDrop공격의 시그너처 데이터베이스는 IP 패킷의 조각난 패킷(Fragmentation Packet)의 길이정보만을 비교하기 때문이다. 그러나 New TearDrop 공격은 IP와 UDP를 모두 사용하고 있으므로 UDP헤더 정보를 탐지하지 않는 규칙기반 시스템은 New TearDrop공격을 찾아낼 수가 없다. 그러나 시간지연 신경망을 이용한 침입탐지 시스템은 패킷 이미지를 분석해서 변형되었지만 TearDrop공격과 유사한 패킷이미지로 New TearDrop공격을 분류해 낼 수 있다.

규칙기반 시스템은 스니핑(sniffing)속도의 한계로 인해 네트워크 상의 모든 패킷을 수집하고 분석하는 것은 불가능하다. 결국 침입 시그너처 데이터베이스와 비교할 수 있는 패킷을 모두 수집하지 못한다면

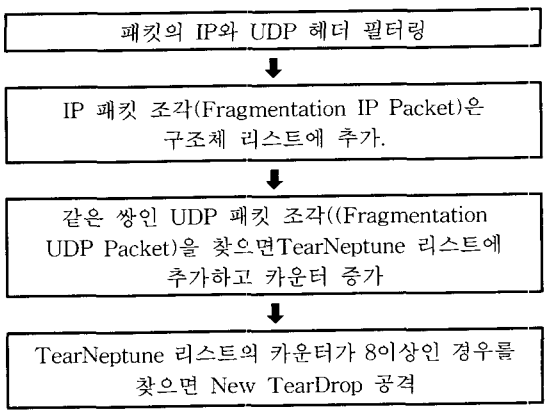


그림 4. New TearDrop 탐지모듈

탐지할 수 없다. 그러나 시간지연 신경망을 이용한 침입 탐지 시스템은 변형된 형태 일부분의 공격 패킷만으로 탐지할 수 있는 유연한 반응성을 가지고 있으므로 규칙기반 시스템보다 우수한 성능을 발휘한다.

2.2 신경망을 이용한 침입탐지 시스템

신경망은 유한하고 불안전한 데이터에 기초한 네트워크 활동을 식별하고 분류하기 위한 잠재적 가능성을 제공한다. 이는 규칙기반 침입탐지시스템의 단점중의 하나인 명세화된 규칙의 유지관리를 쉽게 해주고, 보다 정확한 매칭방법을 제공한다.

신경망을 이용한 침입탐지시스템에 대한 연구는 패킷헤더의 특정 비트 값을 신경망에 적용한 오용탐지 시스템이 있다[8]. 표 1은 신경망 입력 값을 얻기 위한 전처리 과정의 결과로 헤더의 특정 부분의 이름과 그 내용을 나타낸다. 표 1의 두 번째 행은 정상적인 패킷을 의미하며 세 번째 행은 공격 패킷을 의미한다. 신경망은 아홉 개의 입력노드, 한 개의 출력노드를 가진 다층 퍼셉트론을 이용하였고, BP(Back Propagation) 알고리즘으로 학습하였다. 표 1의 아홉 개 열의 값은 신경망의 아홉 개의 입력노드에 사용되며, 나머지 한 개의 열은 출력노드에 사용될 목표 값(Target value)이다.

이 연구는 한 개의 패킷만을 조사하며 또한 패킷헤더의 특정 비트 값만을 사용하여 공격여부를 판단하기 때문에 오용탐지에만 국한되어진다.

이러한 문제점을 해결하는 연구로 패킷헤더의 확률적인 값으로 감사자료를 도출하고, 이것을 다층 퍼셉트론 신경망 입력 값으로 사용한 연구가 제시되었다[9]. 이 연구에서는 수집된 패킷 헤더의 발신지 IP, 수신지 IP, 수신지 port등에 대한 상관관계 테이블을 이용해 각각의 개별 사건사이에는 독립사상이 나타나지 않음을 확인한다. 즉, 헤더 데이터의 연계성을 가지고 발생하는 사건으로 나타낼 수 있다는 조건부 확률(Conditional probability)을 통해 특성화하고 규칙화한다. 따라서 규칙기반 침입탐지 시스템의 Rule Set에서 사용하는 특정 비트 값의 결정을 확률적 근거에 의해 결정하고 이렇게 구해진 데이터를 정적인 다층 퍼셉트론 신경망의 입력 값으로 사용하였다. 결국 규칙기반 침입탐지 시스템의 Rule set에서 누락될 수 있는 헤더의 특정 비트 값을 확률적 관점에서 찾아낸다. 그러나 시스템의 환경에 따라 감사자료를 선택하는 부분을 관리자의 몫으로 남겨두고 있으므로 관리자에 따라 다른 결과를 얻을 수 있다. 따라서 기존의 신경망을 이용한 침입탐지 시스템의 문제점은 다음과 같이 요약할 수 있다: 1) 패킷의 국한된 특정 비트의 정보만으로는 효과적인 침입탐지 시스템을 구성하기 힘들다; 2) 다층 퍼셉트론의 특성상 패킷의 시간적 관계를 고려할 수 없다.

본 논문에서는 패킷헤더의 특정 비트 값만이 아니라 일정한 시간 이내의 패킷들을 일련의 연속된 이미지로 구성하여 신경망의 입력으로 사용하였다. 그리고 패킷들간의 시간적 특성을 수용할 수 있는 시간지연 신경망(TDNN)을 이용하여, 정상적인 흐름과 비정상적인 흐름에 대한 패킷 이미지를 학습하고 분류하는 시간지연 신경망 분류기를 구현하였다.

3. 시간지연 신경망을 이용한 침입탐지시스템

3.1 침입탐지 시스템 전체구성

본 연구에서 제시하는 시간지연 신경망을 이용한 침입탐지 시스템의 전체 흐름도는 그림 5와 같다.

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

ⓑ 패킷 수집기에서 반환받은 패킷 구조체의 정보를 통해 그레이 이미지 패킷으로 변환한다.

ⓒ 신경망 학습을 위한 패턴으로 정규화(normalization)된 후 시간지연 신경망 학습을 위해 사용된다.

ⓓ 학습이 완료된 침입탐지 엔진은 실시간 네트워

표 1. 신경망 입력 값을 얻기 위한 전처리 결과

Protocol ID	Source Port	Destination Port	Source Address	Destination Address	ICMP Type ID	ICMP Code ID	Raw Data Length	Data ID	Attack
0	2314	80	1573638018	-1580478590	1	1	401	3758	0
0	1611	6101	801886082	926167166	1	1	0	2633	1

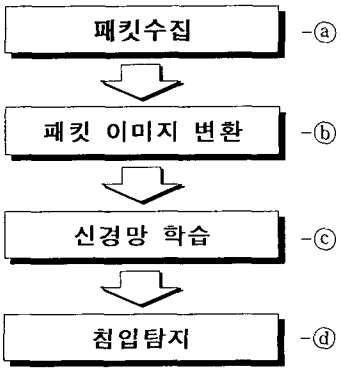


그림 5. 침입탐지 시스템 흐름도

크 침입탐지를 하게되고, 그 결과를 정상 패킷과 비정상 패킷으로 구별한다. 패킷을 연속한 그레이 이미지로 처리함으로써 공격 이미지 일부분만을 감지하더라도 이와 가장 유사한 패턴으로 구별해 낼 수 있다.

3.2 패킷수집

패킷 수집을 위해 사용한 libpcap 라이브러리는 Berkeley 대학에서 개발한 것으로 시스템에 독립적으로 사용자 레벨에서 개발한 패킷 수집을 효과적으로 할 수 있도록 만든 공용 라이브러리이다. 패킷을 포착하려는 시스템에서 무작위 모드(Promiscuous mode)의 상위수준 인터페이스를 제공한다[8]. 네트워크 패킷은 libpcap 라이브러리에서 제공하는 인터페이스를 사용하여 접근할 수 있는데, 이 라이브러리는 거의 모든 유닉스 시스템에서 사용가능하며 tcpdump와 같은 네트워크 모니터링 도구가 이 패킷 수집 라이브러리를 사용하고 있다[9-12].

정상적인 흐름과 비정상적인 흐름에 대한 패킷 이미지를 학습하기 위해 한 대의 공격 시스템, 다섯 대의 정상사용자 시스템 그리고 패킷 수집 시스템으로 실시간 패킷 수집을 한다. 이를 정규화하여 학습패턴을 만든다. 그림 6의 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.

3.3 패킷 이미지 변환 및 학습패턴 생성

하나의 패킷은 1비트 단위로써는 0과 1로 이루어진 바이너리 이미지이지만 1바이트를 이미지의 한

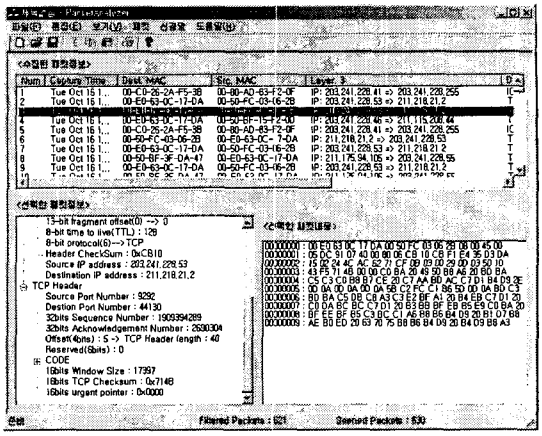


그림 6. 패킷 수집 과정

픽셀로 나타내면 그레이 이미지가 된다. 그림 7은 패킷의 그레이 이미지로써 세로줄은 하나의 패킷을 나타내고 그 길이는 60바이트를 나타낸다. 그리고 오른쪽으로는 순차적으로 60개의 패킷이 나열되어 있다. 이를 정규화(normalization) 과정을 통해 신경망 학습을 위한 0에서 1사이의 그레이 이미지가 된다. 이러한 연속된 패킷이미지를 시간지연 신경망의 입력으로 사용한다.

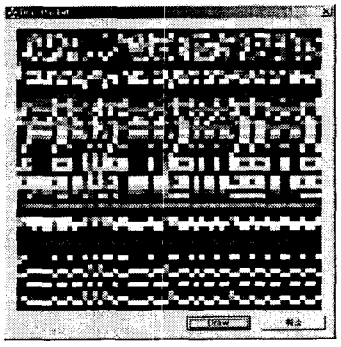


그림 7. 패킷 이미지

3.4 침입탐지 시스템의 TDNN 구성

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

TDNN용으로 사용되는 data는 그림 7과 같은 spectrogram이다. 직사각형 모양을 하고 있으며, 세로축은 공간축, 가로축은 시간축을 나타낸다. 패킷을

공간적으로 60차원인 data를 60개(time step)로 본 것이다.

그림 8은 TDNN 구조를 보여주고 있다. TDNN을 사용하는 방법은 Temporal back-propagation이나 Back-propagation등 다양한 방법이 있지만 본 논문에서는 TDNN을 처음 만든 Waibel이 했던 방법을 사용하였다.

본 논문에서 구현한 TDNN은 두 layer사이에 공간축 방향으로는 항상 완전연결(fully connected)되어 있고, 시간축 방향으로는 부분적 연결(partial connection)을 사용할 수 있다. 그림 9는 TDNN을 옆에서 시간축 방향으로만 본 그림이다. 첫 번째 은닉층에서 입력층 사이의 연결이 부분적인 것을 알 수 있다. 첫 번째 은닉층 각 node에서 시간적으로 받아들일 수 있는 kernel size가 현재 5로 설정되어 있고 step size는 4로 설정되어 있다.

TDNN 신경망에서 각 계층의 구조 결정에는 입력

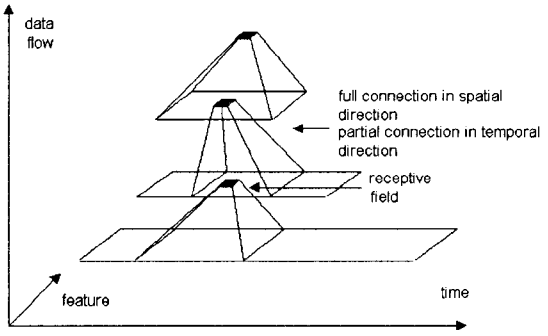


그림 8. TDNN 구조

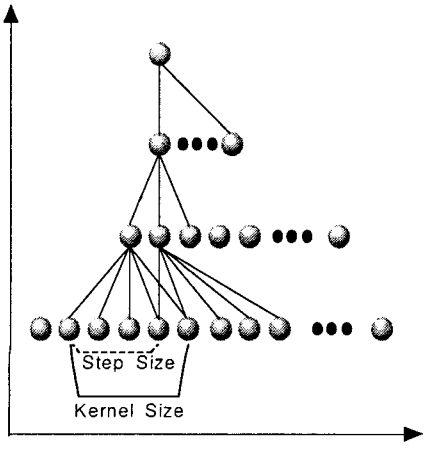


그림 9. TDNN의 단면구조

층의 구조가 가장 큰 영향력을 가진다. 그리고 응용 데이터의 특성을 효과적으로 수용하기 위한 각 계층의 시간축 크기(Temporal size)와 공간축 크기(Spatial size: 패킷 한 개의 길이)의 결정이 곧 node의 수 결정으로 직결된다.

입력층에서의 시간축 크기(Temporal size)는 네트워크 상의 지속적인 패킷 흐름 중에서, TDNN분류기의 입력으로 사용될 패킷의 수를 의미한다. 따라서 시간축 크기(Temporal size)가 너무 작으면 시간 간격이 긴 공격 패킷을 탐지하기 힘들다. 반면에 시간축 크기(Temporal size)를 크게 설정하면 한번에 보다 많은 패킷을 대상으로 분석하겠다는 것이다. 많은 정보에 기초하여 탐지를 수행한다는 것 자체는 신뢰도를 높일 수 있으나, 네트워크 상에서 이미 상당량의 공격이 수행된 상태이므로 실시간 탐지 시스템으로서의 기능을 충분히 발휘하지 못하게 된다. 무엇보다도 학습패턴들의 크기가 너무 커짐으로 해서 학습이 잘되지 않았다. 따라서 효과적인 탐지와 신경망의 학습을 고려하여 시간축 크기(Temporal size)를 60 패킷으로 하였다. 네트워크상의 패킷의 최대 허용길이(Maximum Transfer Unit)는 한 프레임 당 1500바이트를 넘지 않는다. 본 연구에서는 SYN Flooding, Land[10,13], 그리고, TearDrop공격에 대해 실험하였고 이러한 공격들은 패킷의 60바이트 이내의 헤더 정보에서 식별할 수 있으므로 공간축 크기(Spatial size)는 60바이트로 하였다. 따라서 입력층 노드의 개수는 60×60으로 결정된다.

첫 번째 은닉층의 노드 수를 결정하기 위한 시간축 크기(Temporal size)는 입력층의 kernel size와 step size에 종속된다. kernel size와 step size가 크다는 것은 패킷을 그만큼 많이 건너뛰면서 읽어 들이겠다는 것이고 작다는 것은 패킷을 세밀하게 읽어 가중치를 부여하겠다는 것이다. 보다 유연한 반응을 위해 시간축 크기(Temporal size) 안에서 설정될 수 있는 kernel size와 step size의 모든 경우의 값들 중에서 가장 작은 값을 선택하였다. 따라서 입력층의 kernel size가 4이고 step size가 2인 것에 의해 첫 번째 은닉층의 Temporal size는 29가 된다. 공간축 크기(Spatial size)는 Waibel[14]에서 제시된 모델을 인용하여 입력층의 50%로 하였다. 따라서 첫 번째 은닉층의 개수는 29×30로 결정된다.

두 번째 은닉층의 노드 수는 이전 단계와 마찬가

지로 첫 번째 은닉층에서의 kernel size와 step size에 의해 결정된다. 그런데 두 번째 은닉층의 kernel size는 첫 번째 은닉층에 비해 조금 더 큰 kernel size가 요구된다[14]. 상위 계층에서는 하위 단계의 국부적으로 추상화된 정보들을 취합할 수 있도록, 하위 단계의 kernel size 보다는 넓은 범위의 입력 값으로 학습해야 하기 때문이다. 본 연구에서는 kernel size를 5로 하였고 step size는 첫 번째 은닉층과 동일하게 2로 하였다. 따라서 두 번째 은닉층의 시간축 크기(Temporal size)는 13이 된다. 공간축 크기(Spatial size)는 첫 번째 은닉층에서와 같이 50% 감소시킨 15로 하였다. 그러므로 두 번째 은닉층의 노드 개수는 13×15로 결정된다.

출력층 노드 수는 정상과 비정상의 두 가지 클래스의 비교 문제이므로 하나의 노드로 구성된다.

표 2는 시간지연 신경망을 이용한 침입탐지 시스템(TDNN)에서 각 계층에 대한 세부 구성이다.

본 논문에서 사용한 TDNN은 입력층(input layer), 2개의 은닉층(hidden layer), 출력층(output layer)의 다층으로 구성된다. 은닉층에서는 시간 지연 요소를 통한 입력으로 패킷의 국부적인 특징을 감지해내고 출력층에서는 전단 은닉층의 시간적인 지연을 갖는 출력의 제곱을 더하여 출력을 한다. 이렇게 해서 최종적으로 은닉층에서는 패킷이 가지는 국부적인 특성을 감지함으로써 패턴을 시각적으로 굴곡(time-warping)하게 되고, 출력층에서는 전단의 시간적으로 지연된 출력들을 합함으로써 입력패턴에 지연현상이 발생하여도 같은 출력을 낼 수 있는 특징을 갖는다[14].

3.5 TDNN의 학습

제안한 TDNN을 이용한 침입탐지 시스템은 펜티엄4 PC, Windows 환경에서 Visual C++로 구현한다. 그림 10은 TDNN의 학습과정을 보여주고 있다. 구성

표 2. 침입탐지 시스템의 TDNN 구성

	Spatial Size	Kernal Size	Step Size	노드 개수
입 력 층	60	0	0	60×60
은닉층 1	30	4	2	29×30
은닉층 2	15	5	2	13×15
출 력 층	1	13	0	1×1

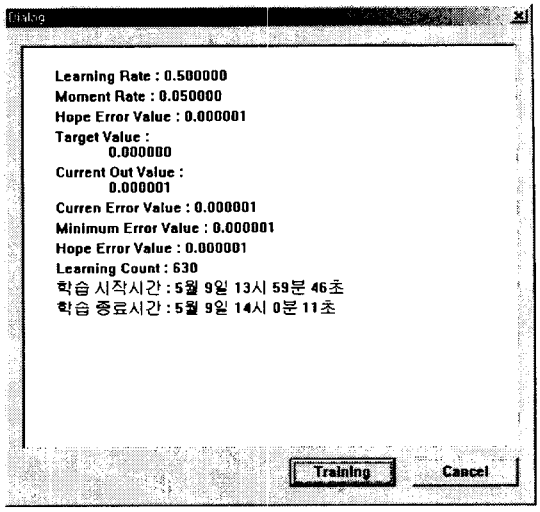


그림 10. TDNN 학습

된 시간 지연 신경망을 학습하기 위해 SYN Flooding, Land, TearDrop, New TearDrop공격 각각에 대한 정상 패킷 6000개와 비정상 패킷 6000개를 수집하여 랜덤하게 섞은 후에 60개 단위의 학습 패턴으로 사용한다. 원하는 에러값은 0.000001로 지정하여 학습한다. 학습이 완료되면 가중치(weight) 값들이 저장된다.

4. 실험 및 결과

학습된 침입탐지 시스템의 성능을 평가하기 위해 추출된 각 패킷 데이터 중 학습에 사용된 데이터와 학습에 사용되지 않은 데이터로 구분하여 실험하였다. 공격패킷 6000개, 정상패킷 6000개를 랜덤하게 섞어서 100개의 비정상 패킷이미지를 만들고 순수한 정상 패킷이미지 100개와 테스트하였다.

TearDrop을 학습한 신경망으로 변종공격인 New TearDrop을 테스트 한 결과는 그림 11과 같다. Target값은 데이터의 기대 값으로 0인 것은 정상 데이터이고, 1인 것은 비정상 데이터이다. Result 항목은 시간지연 신경망이 구분해낸 결과로 Normal은 정상이고, Abnormal은 공격을 나타낸다.

그림 12는 그림 11에서 얻은 실험 결과를 그래프로 나타낸 것이다. 좌표의 하단에 분포되어 있는 "x" 표시는 정상패킷, 상단에 분포되어 있는 "■"표시는 비정상패킷을 말한다. 표 3은 시간지연신경망을 이용한 침입탐지 시스템의 각각의 공격에 대한 실험결

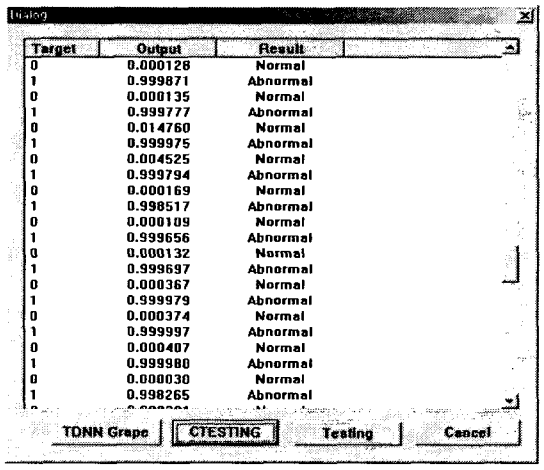


그림 11. New TearDrop 결과

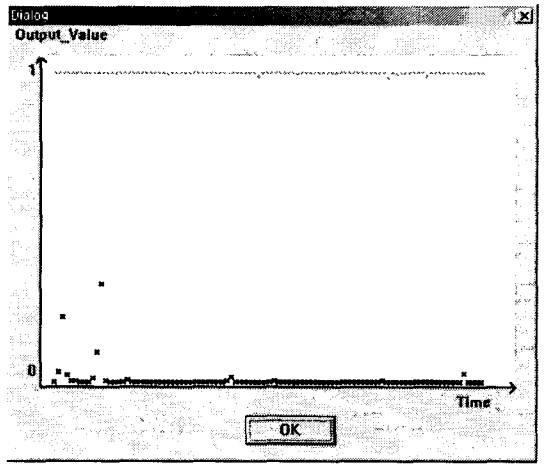


그림 12. New TearDrop 결과 그래프

표 3. 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	6

과를 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 6개를 제외하고는 모두 탐지해 내었다.

보다 다양한 환경에서 탐지 시스템의 성능을 평가하기 위해 테스트에 사용된 공격패킷을 10개 단위의 overlap 데이터 패킷이미지 595개로 만들어 정상 패킷이미지와 함께 테스트하였다. 그림 13은 TearDrop overlap 데이터 결과를 그래프로 나타낸 것이다. 그리고 각각의 공격에 대한 결과는 표 4에 나타나 있다. 동일한 공격 패킷 이미지는 오류 없이 모두 잘 분류해 냈다. 특히 TearDrop 공격 패킷 이미지를 학습한 제안된 시스템은 변종공격인 New TearDrop 공격 패킷 이미지를 변형한 overlap 데이터를 분류하는데 있어서, 정상을 비정상으로 잘못 탐지하는 경우가 1개이고 비정상을 정상으로 탐지하는 경우가 28개로, 학습하지 않은 많은 패킷이미지를 분류해 내었다

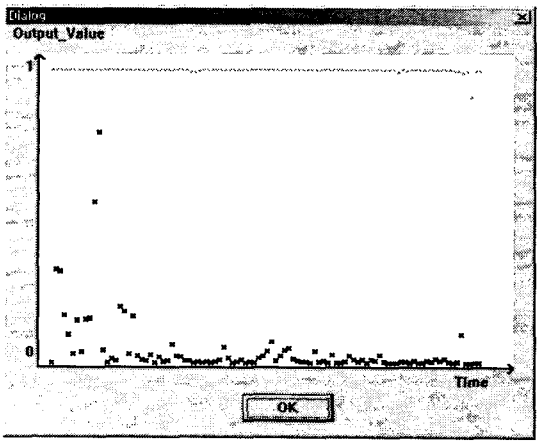


그림 13. TearDrop overlap 데이터 결과 그래프

표 4. overlap 데이터 실험 결과

	false positive	false negative
SYN Flooding	0	0
Land	0	0
TearDrop	0	0
New TearDrop	0	0
변종공격 Test	1	28

5. 결론 및 향후 과제

인터넷은 다양한 서비스 부가사업을 위해 계속해

서 확대될 것이며, 네트워크를 통한 침입은 그 유형만 달리할 뿐, 계속될 것이다. 따라서 본 논문에서는 네트워크상의 다양한 변화에 유연한 대응을 필요로 하는 침입탐지 시스템에 시간지연 신경망을 이용하여 비정상 패킷을 탐지하는 시스템을 제안하였다.

본 논문에서 제안된 시간지연 신경망 기반의 침입탐지 시스템은 패킷을 0에서 255사이 값으로 이루어진 그레이 이미지로 분석함으로써 공격패킷의 일부 이미지만으로도 구별해낼 수 있는 특징을 가지고 있다. 일반적인 영상 이미지는 픽셀의 위치정보 보다는 영상에 나타난 객체에 가중치가 있는 반면에 패킷은 Protocol ID, Port, Adress, 등, 각각의 바이트마다 의미하는 위치정보의 특색이 강하다. 이것은 신경망의 각각의 노드에 독특한 가중치를 부여하게되는 입력 데이터의 특징을 가지고 있다. 그리고 그림 7의 연속된 패킷 이미지는 spectrogram을 그리게 되는데 시간적인 순서에 따라 패킷이미지들의 특정 위치의 픽셀마다 독특한 그림을 나타내는 것을 알 수 있다. 이러한 점은 연속된 패킷이미지가 시간지연 신경망으로 분류가 잘 되는 특징을 가지고 있다.

실험 결과에 따르면, 제안된 시스템은 학습된 패킷 이미지를 정확히 분류해 내었고, 기존의 학습된 시스템으로 학습시키지 않은 변형된 패킷 이미지를 잘 분류해 내었다. 이는 크래커들이 변형 또는 우회하는 공격을 하더라도 탐지해 낼 수 있으므로 탐지 시스템의 성능을 높일 수 있다. 그러므로 시간지연신경망을 이용한 침입탐지 시스템은 기존의 규칙기반 침입탐지 시스템과 상호 연동 시 보다 높은 성능의 탐지 시스템이 될 것이라 기대된다.

네트워크 기반 침입탐지시스템들은 호스트 기반 침입탐지시스템들이 보안위반 사건 탐지를 위하여 사용하는 감사 정보를 통하여 탐지할 수 없는 네트워크로부터 기인되는 보안위반을 탐지하는 것을 목적으로 한다. 이와 같이 네트워크 상에서 발생하는 보안위반 사건의 탐지를 위해서는 네트워크로 유입되는 패킷 정보와 트래픽 정보에 대한 분석이 요구되기 때문에 네트워크 기반 침입탐지시스템은 감사 데이터 생성을 위하여 네트워크 패킷정보, 네트워크 관리 정보를 기반 정보로서 사용한다. 시간지연 신경망은 패킷 이미지를 입력 값으로 사용하고 있기 때문에 많은 네트워크의 트래픽을 보아야만 한다. 이는 시스템의 속도에 많은 영향이 있으므로 보다 높은 속도 및 탐지성능을 만족시킬 수 있는 다양한 학습알고리즘을 개발하여 이를 적용시킬 수 있는 방법에 대한 연구도 필요할 것이다.

참 고 문 헌

[1] http://www.certcc.or.kr

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

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

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

[5] 김대수, 신경망 이론과 응용(I), 하이테크정보, 제21-100호, pp. 176-187, pp. 191-210, pp. 243-282, 1995.

[6] Simon Haykin, Neural Networks, Macmillan, ISBN: 0-02-352761-7 pp. 498-533, 1994.

[7] B. Parmanto et al., Detection of hemodynamic changes in clinical monitoring by time-delay neural networks, International Journal of Medical Infomatics, Vol. 63, pp. 91-99, 2001.

[8] James Cannady, Artificial Neural Networks for Misuse Detection, Proceedings of the 1998 National Information Systems Security Conference (NISSC'98) pp. 5-8 Oct. 1998. Arlington, VA.

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

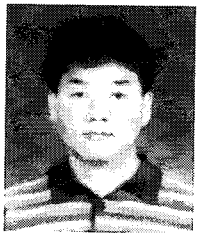
[10] 포항공대 유닉스 보안 연구회, Security PLUS for UNIX, 영진출판사, ISBN: 89-314-1490-0, pp. 251-254, pp. 383-400, 2001.

[11] 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

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

[13] Stephen Northcutt, Judy Novak, Network Intrusion Detection An Analyst's Handbook, New Riders Publishing, ISBN: 0-7357-0868-1, pp. 149-150, pp. 169-307, 1999.

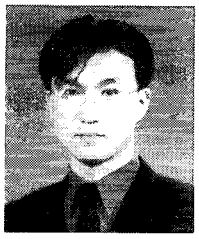
[14] A. Waibel, T. Hanazawa, G. Hinton, K. Shikano, K. J. Lang, "Phoneme Recognition Using Time-Delay Neural Networks," IEEE Transactions on Acoustic, Speech, and Signal Processing ASSP, vol. 37, no. 3, pp. 328-339, Mar. 1989.



강 흥 식

1982년 서울대학교 계산통계학과 졸업(이학사)
1984년 서울대학교 대학원 계산통계학과 졸업(공학석사)
1995년 부산대학교 대학원 컴퓨터공학과 수료
1985년~현재 인제대학교 정보컴퓨터공학부 부교수

관심분야 : 정보보호
E-mail : hskang@cs.inje.ac.kr



강 병 두

2001년 인제대학교 정보컴퓨터학부 졸업(정보컴퓨터학사)
2003년 인제대학교 대학원 전산학과 졸업(전산학석사)
2003년 인제대학교 대학원 박사과정

관심분야 : 정보검색, 정보보호, 패턴인식
E-mail : dewey@cs.inje.ac.kr

정 성 윤

2002년 인제대학교 정보컴퓨터학부 졸업(정보컴퓨터학사)
2002년 인제대학교 대학원 전산학과 석사과정

관심분야 : 정보검색, 정보보호, 패턴인식
E-mail : yuni66@korea.com

김 상 균

1991년 경북대학교 통계학과 졸업(이학사)
1994년 경북대학교 대학원 컴퓨터공학과 졸업(공학석사)
1996년 경북대학교 대학원 컴퓨터공학과 졸업(공학박사)
1996년~현재 인제대학교 정보컴퓨터공학부 조교수

관심분야 : 정보검색, 정보보호, 패턴인식
E-mail : skkim@cs.inje.ac.kr

교신저자

김 상 균 621-749 경남 김해시 577 인제대학교 컴퓨터공학부