韓國 컴퓨터情報學會 論文誌
第9卷 第1號, 2004. 3.

2004-9-1-1-6

Neuro-Fuzzy를 이용한 이상 침입 탐지

김 도 윤*, 서 재 현**

Anomaly Intrusion Detection using Neuro-Fuzzy

Do-yun Kim*, Jae-hyun Seo**

요 약

컴퓨터 네트워크의 확대 및 인터넷 이용의 급속한 증가에 따라 컴퓨터 보안문제가 중요하게 되었다 따라서 침입자들로부터 위험을 줄이기 위해 침입탐지 시스템에 관한 연구가 진행되고 있다. 본 논문에서는 네트워크 기반의 이상 침입 탐지를 위하여 뉴로-퍼지 기법을 적용하고자 한다. 불확실성을 처리하는 퍼지 이론을 이상 침입 탐지영역에 도입하여 적용함으로써 오용 탐지의 한계성을 극복하여 알려지지 않은 침입 탐지를 하고자 한다.

Abstract

Expasion of computer network and rapid growth of Internet have made computer security very important. As one of the ways to deal with security risk, much research has been made on Intrusion Detection System(IDS). The paper, also, addresses the issue of intrusion detection, but especially with Neuro-Fuzzy model. By applying the fuzzy logic which is known to deal with uncertainty to Anomaly Intrusion, it not only overcomes the difficulty of Misuse Intrusion, but also ultimately aims to detect the intrusions yet to be known.

▸ Keyword : Intrusion Detection, Anomaly Intrusion, security

* 목포과학대학 의료정보시스템과 전임강사
** 목포대학교 정보공학부 부교수

Ⅰ. 서 론

최근의 정보통신 기반구조는 컴퓨터 시스템의 네트워크를 통한 연결로 다양한 서비스를 제공하고 있다. 특히 인터넷은 개방형 구조를 가지고 있어 서비스 품질의 보장과 네트워크의 관리가 어렵고, 기반구조의 취약성으로 인하여 타인으로부터의 해킹 및 정보유출 등의 위협으로부터 노출되어있다. 불법 및 고의로 네트워크를 통한 컴퓨터 시스템에 접근하여 피해를 야기하는 문제에 대해 침입 차단, 인증 그리고 접근제어 등의 다양한 방법이 제공되고 있지만 역부족 상태이다. 보안 위협에 대한 능동적인 대처 및 침입 이후에 동일한 또는 유사한 유형의 사건 발생에 대해 실시간의 대응 할 수 있는 방법이 중요하게 되었으며 이러한 해결책으로서 침임 탐지 시스템에 대한 연구가 활발히 진행되고 있다[1].

침입 탐지 시스템은 단순한 접근 제어 기능을 넘어서 침입 패턴을 데이터베이스로 구축하고, 전문가 시스템을 사용해 네트워크나 컴퓨터 시스템의 사용을 실시간 모니터링하고 침입을 탐지하는 보안 시스템이다. 침입 탐지 기법은 크게 비정상적인 침입탐지 기법과 오용침입탐지 기법으로 나눌 수 있다. 오용 탐지는 알려진 침입 방법들을 수집하여 지식 베이스에 유지하고 동일한 침입 유형을 지식 베이스 검색을 통한 비교에 의해 침입을 탐지하는 방법이다. 또한, 이상 탐지는 정상 행위로부터 벗어나는 주목할만한 특이한 행위 패턴을 침입으로 규정하여 침입을 탐지한다.

본 논문에서는 네트워크 기반의 이상 침입 탐지를 위하여 뉴로-퍼지 기법을 적용하고자 한다. 불확실성을 처리하는 퍼지 이론을 이상 침입 탐지영역에 도입하여 적용함으로써 오용 탐지의 한계성을 극복하여 알려지지 않은 침입 탐지를 하고자 한다.

본 논문의 2장은 관련연구로써 공격 기법과 침입 탐지 모델을 분류하고, 퍼지와 신경망에 대해 기술한다. 3장은 이상 침입 탐지에 뉴로-퍼지기법의 적용을 위한 방법을 제시하였으며, 4장은 뉴로-퍼지를 적용한 이상 탐지 기법을 네트워크 환경에서 시뮬레이션을 수행한다. 그리고 5장에서는 결론 및 향후 연구방향을 기술한다.

Ⅱ. 관련 연구

이상 침입 탐지를 연구하기 위해서는 먼저 공격기법을 분류하고, 공격 기법에 대한 침입 탐지 모델을 분류한다. 이상 침입 탐지를 위한 여러 관련 기술을 분석하고, 새로운 침입을 탐지하기 위한 탐지 기법을 논의한다. 그리고 본 논문의 주제가 되는 퍼지와 신경망에 대해서 기술한다. 공격 기법의 분류는 공격의 대상이 호스트이거나 네트워크 또는 네트워크 자원에 따라 호스트 기반과 네트워크 기반으로 분류되며, 공격에 대한 침입 탐지 모델에 따라서 오용 침입 탐지와 이상 침입 탐지로 구분할 수 있다.

1. 네트워크 기반의 공격 유형

네트워크 공격 유형 또한 침입 탐지 모델에 의해서 오용과 이상 침입 탐지 모델로 분류된다. 네트워크 기반의 오용 침입 탐지는 네트워크를 지원하는 호스트의 서버 프로그램들의 설계 결함, 환경설정 결함 등의 취약점을 악용하거나 혹은 TCP/IP 프로토콜의 취약점을 이용하는 공격을 탐지할 수 있다. 네트워크 기반의 이상 침입 탐지는 네트워크상의 서비스를 방해하거나 네트워크 자원을 도용하기 위한 지금까지 사용되지 않았던 새로운 공격형태나 변형된 공격을 탐지한다.

2. 이상 침입 탐지 기술

이상 침입 탐지 시스템은 비정상으로 보이는 행위 패턴을 탐지한다. 이상 행위는 오용 침입과 합법적인 사용으로 명확히 알려진 것 이외의 행위를 말한다. 예를 들면, 임의의 사람이 허가된 ID로 한밤중에 들어와서 시스템을 사용했다. 그러나 평소에 그 ID의 소유자는 일과시간에만 시스템을 사용해 왔다면 이를 이상행위로 간주한다.

2.1 통계적 분석

이상 행위 탐지에서 가장 많이 사용되고 있는 방법이 통계적 분석(Statistical Measures)이다. 통계적 분석은 확률과 통계를 기반으로 표현하며 실제 환경에서 적용하고 구현하기 쉽다. 통계적 분석 방법의 장점은 통계값이 결정되었을 때 주기적인 변경이나 유지보수가 필요 없으며 통계적

학습을 통하여 합법적인 사용자로 위장한 침입자를 인식할 수 있다는 것이다[2]. 이러한 이점에도 불구하고 통계적 분석 방법은 이상 침입 탐지에서 분석용으로 쓰이며 실제 탐지에는 많이 사용되고 있지 않다. 그 이유는 통계적 분석을 사용하였을 경우 오판율이 높게 나타나기 때문이다.

2.2 규칙 기반 분석

규칙 기반 분석(Rule-based Approaches)은 오용 침입 탐지의 규칙과는 달리 비정상행위 탐지를 위한 여러 가지 척도(Measure)를 조합하는 방식이다. 이것은 여러 이벤트의 연관된 확률을 구하는 방식으로 여러 가지 척도가 있을 때 그에 대한 확률을 구하여 조합하여 형태로 표현한다.

2.3 신경망

신경망(Neural Networks)은 인공지능의 한 분야이다. 이것은 주로 직관적인 결정을 하는데 있어서 컴퓨터의 지능을 향상시키기 위한 것이다. 주로 패턴 분류에 이용되는데 전통적인 컴퓨터와는 달리 사람의 뇌를 모방하여 시뮬레이션하는 방식이다. 일반적으로 신경망을 이용하는 방법은 정상행위에 대한 로그를 학습하여 신경망 데이터를 생성하는 것과 발생한 이벤트 데이터를 신경망에 적용하여 판단하는 것의 두 단계를 거친다[3].

2.4 모델기반 방식

모델기반(Model-based) 침입탐지 방법은 침입탐지에 필요한 특성 모델을 결정하고 실제 행위에 대한 모델의 대응 결과로써 판단하게 된다. 이상행위 탐지방법에서는 일정한 모델을 기준으로 학습을 수행하며 실제 이벤트가 그 모델에서 어떠한 값을 갖는지를 검사한다.

3. 새로운 공격 탐지기술

새로운 공격에 대한 탐지기술은 이상행위 탐지기술의 주요 목적이었다. 그러나 이상행위 탐지기술의 정확성 문제로 다른 각도의 접근방법이 필요하게 되었다.

3.1 데이터 마이닝

데이터 마이닝(Data Mining) 기술은 데이터베이스 영역에서 많은 연구가 되고 있는 분야이며 이상행위 침입탐지 분야에서도 많은 연구가 진행되고 있다. 데이터 마이닝은 침입탐지 분야에서 프로그램과 사용자 행위를 표현하는 시스템 특징의 유용한 패턴을 발견하는데 이용된다[4].

3.2 면역 시스템

생물계의 면역시스템은 바이러스, 병원균, 독소 등의 항원으로 통칭하는 다양한 외부 유기체나 단백질에 대하여 생명체를 보호할 수 있는 정교하고 복잡한 구조로 구성되었다. 이와 유사하게 컴퓨터 시스템내의 자원이나 정보 등에 대한 공격의 형태가 매우 다양해지고 변형되어 위협함에 따라 컴퓨터 시스템을 안전하게 보호하는 것이 필요하게 된다. 컴퓨터 시스템을 생물계의 면역시스템과 유사하게 모델링하는 연구가 계속 진행되고 있다.

3.3 유전 알고리즘

인공유전시스템인 유전알고리즘(Genetic Algorithms)은 자연세계의 진화 과정에 기초한 계산 모델로서 John Holland에 의해서 1975년에 개발된 전역적 최적화알고리즘이다. 침입탐지 분야에서는 직접적인 탐지보다는 기존 침입탐지의 단점을 보완하는 수준에 응용되고 있다. 비정상행위 탐지 방법에 있어서 적절한 임계치를 구하는 문제가 존재하는데, 상황에 따라 진화하여 임계치를 조정할 수 있도록 유전 알고리즘을 적용할 수 있다.

4. 퍼지와 신경망

4.1 퍼지 개념과 퍼지 집합의 연산

퍼지 이론은 오늘날 퍼지 제어, 신경망, 소프트 컴퓨팅, 퍼지 컴퓨터, 인공 지능 시스템 등의 과학과 공학분야 뿐 아니라 의료진찰, 유전자, 퍼지 의사결정, 퍼지 선형계획법과 같은 의학 분야, 경영학, 교육학 등의 여러 분야에서 널리 응용되고 있다. 퍼지집합은 일반집합과 마찬가지로 여집합, 합집합, 교집합과 같은 기본연산이 존재한다. 임의의 퍼지집합 A의 여집합은 $\overline{A}$의 여집합으로 나타내고, 일반집합과 마찬가지로 1에서 모든 멤버쉽값을 빼서 구한다. 그러나 여집합 $\overline{A}$ 은 경계가 명확하지 않는 퍼지집합이 된다.

임의의 두 퍼지집합 A와 B의 합집합은 $A \cup B$로 나타내고 전체집합 내의 각 원소에 대해 두 집합 A와 B의 멤버쉽값 중에서 큰 것으로 구성한다. 임의의 두 퍼지집합 A와 B의 교집합은 $A \cup B$ 로 나타내고 전체집합 내의 각 원소에 대해 두 집합 A와 B의 멤버쉽값 중에서 작은 것으로 구성한다. 이외에도 여러 가지 퍼지집합간의 연산방법이 있는데 자세한 것은 여기서는 생략하기로 한다. 한 가지 중요한 점은 퍼지집합간의 연산이 대부분 Max, Min 연산자를 기본으로 하여 이루어진다는 것이다. 따라서 이 두 가지 연산자를 표준연산자라고 부른다.

4.2 역전파 신경망

신경망 모형을 구성하는 가장 기본적인 단위는 뉴런(neuron)이며 기본적인 정보처리의 단위이다. 이는 입력값들

을 가중 합산하여 그 결과를전이함수(transfer function)로 전환하여 결과를 전달하는 기능을 수행한다.

신경망은 뉴런의 연결방식과 학습방법에 따라 여러 종류로 구분된다. 그 중에서 가장 많이 사용되는 신경망 모형은 다층 퍼셉트론(multilayer perceptron)으로서, (그림 1)은 3층 구조를 가진 다층 퍼셉트론을 도식화하고 있다. 각 층은 입력값을 갖는 입력층, 정보처리 과정이 일어나는 은닉층, 출력값을 나타내는 출력층으로 구분된다. 신경망은 충분한수의 은닉층이 있으면 어떠한 함수라도 표현할 수 있는 보편적인 함수식이라고 할 수 있다[5].

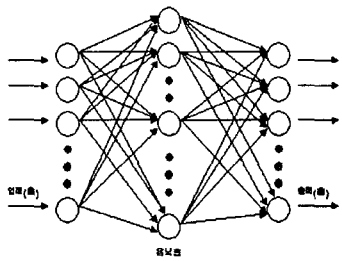

그림 1. 3층구조를 가진 다층 퍼셉트론

신경망이 주어진 자료의특성을 학습하는데 사용되는 학습 알고리즘(learning algorithms)에는 여러 가지가 있으나 그 중에서 오차를 최소화시켜 나가는 역전파(back propagation) 방법이 흔히 사용된다. 역전파 알고리즘은 최소자승알고리즘의 비선형적 확장으로 볼 수 있는 가장 많이 쓰이는 지도학습 기법이다. 즉, 입력층의 각 노드에 입력패턴을 주면 이 신호는 각 노드에서 변환되어 은닉층에 전달되고 계산과정을 거쳐 출력층에서 신호를 출력하게 된다. 이때 출력값과 목표값을 비교하여 둘 사이의 차이, 즉 오차를 줄여나가는 방향으로 가중치를 반복적으로 조정해 나가는 방법이 역전파법이다[6][7].

III. 뉴로-퍼지 IDS

이상 침입 탐지에 기계 학습 기법인 신경망과 불확실성을 해결하기 위한 방법인 뉴로-퍼지를 (그림 2)과 같이 이용한다.

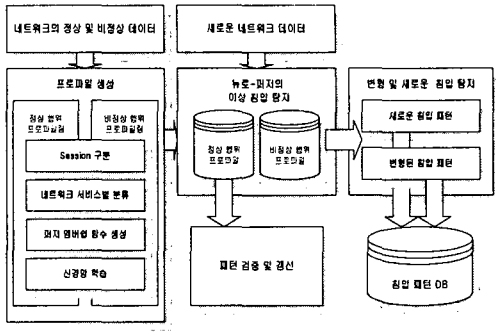

그림 2. 뉴로-퍼지 기법의 이상 침입 탐지 구성도

네트워크 기반의 이상 침입을 탐지하기 위해서는 먼저 세션을 구분하고, 네트워크 서비스별로 분류하여 네트워크의 행위 패턴을 생성한다. 정상적인 네트워크 행위 패턴을 이용하여 네트워크의 정상 행위를 프로파일링하고, 비정상적인 네트워크 행위 패턴을 이용하여 네트워크의 비정상 행위를 프로파일링한다. 정상 행위 프로파일을 이용하여 퍼지멤버쉽 함수를 생성하고, 정상 행위의 퍼지 멤베쉽 함수를 지도 학습 신경망에 적용하여 이상 침입 탐지를 수행한다.

1. 네트워크 데이터의 행위 패턴 생성과 프로파일링 구축

네트워크 정상 행위의 프로파일을 구축하기 위해서는 하나의 행위를 기술할 수 있는 표현법이 필요하다. 본 논문에서 사용하는 네트워크 행위를 나타내는 표현법은 다음의 〈표 1〉과 같다.

표 1. 네트워크 행위패턴 표현법

네트워크 행위 패턴 표현법	
플래그 값	네트워크 패킷 헤더에 포함된 플래그를 사용
〈, 〉	패턴의 시작과 끝은 각각 〈와 〉으로 표시하거나, 순차 패턴의 분기와 병합을 표시.
-	패킷과 패킷을 '-'에 의해 구분
X	심볼 X는 모든 플래그에 대응
[ ]	[ ]중괄호는 다양한 플래그를 의미
{ }	중괄호는 제외된 플래그를 의미
( )	괄호()는 반복을 의미
A,...,Z	임의의 심볼은 특이 패턴을 정의

네트워크 행위를 표현하기 위하여 DARPA 2000년 NT 데이터 일부를 표현하면 다음의 〈표 2〉와 같이 나타낼 수 있다.

표 2. 네트워크 행위의 표현 예제

〈S-./ack(2)-P/ack-./ack-P/ack(3)-./ack-P/ack-./ack-P/ack(2)-./ack(2)-P/ack(2)-./ack(2)-P/ack(2)-./ack(2)-P/ack-./ack-F/ack〉

〈표 2〉와 같이 표현된 네트워크 행위들을 모아서 정상 행위 프로파일 구축에 사용된다. 네트워크 기반의 침입 탐지에는 네트워크 데이터인 패킷의 헤더 정보를 이용하여 이상이나 오용 침입을 탐지한다. 본 논문에서는 TCP/IP 기반의 서비스에 대한 네트워크의 패킷 헤더 정보를 이용하여 서비스별로 분류하며,네트워크 서비스별로 정상 행위를 프로파일링하여 이상 침입을 탐지한다. 대부분의 네트워크 침입 탐지는 단지 TCP/IP의 패킷의 이상 유무와 침입시의 패킷의 여러 특징에 의해서 이상 침입을 탐지한다. 본 논문에서는 패킷의 헤더 정보에다가 특정한 서비스에 대해 제약을 적용함으로써 네트워크 이상 침입을 명확히 구분하고자 한다.

2. 퍼지 멤버쉽 함수 생성

뉴로-퍼지 이상 침입 탐지에 사용될 퍼지 멤버쉽 함수는 네트워크 서비스별 정상 행위 프로파일을 이용한다.

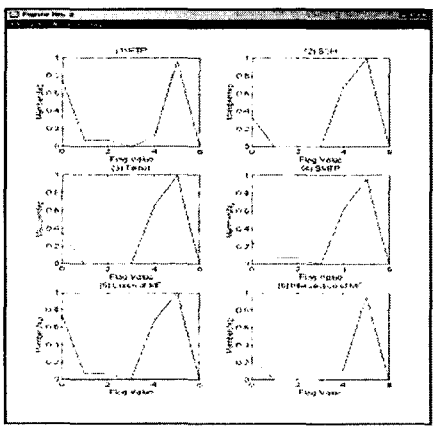

그림 3. 네트워크 서비스별 플래그 분포와 멤버쉽 함수의 합집합과 교집합

(그림 3)의 (1)은 SSH 서비스, (2)는 FTP와 FTP-Data 서비스, (3)은 Telnet 서비스 그리고 (4)는 SMTP 서비스의 퍼지 멤버쉽 함수를 나타낸다. 네 가지의 네트워크 서비스의 멤버쉽 함수를 퍼지 집합의 합집합과 교집합의 연산을 수행하면, (그림 3)의 (5)와 (6)이 된다. 퍼지 집합의 합집합은 상한을 나타내고, 퍼지 집합의 교집합은 하한을 나타낸다. 퍼지 집합의 합집합과 교집합에 의해서 좀더 명확한 정보를 제공한다.

3. 퍼지 멤버쉽 함수를 이용한 BPN 학습

역전파 신경망의 학습은 입력 x와 와 은닉계층의 가중치 w의 곱의 합에 은닉 계층의 편의 θ를 더하여 순입력으로 식 (1)과 같이 사용된다.

$$net_{pj}^{h} = \sum_{i=1}^{N} w_{ji}^{h} x_{pi} + \theta_{j}^{h} \quad \cdots\cdots (1)$$

순입력에 의한 은닉계층의 전달함수의 출력 i가 식 (2)와 같이 계산된다.

$$i_{p}^{h} = f_{j}^{h}(net_{pj}^{h}) \quad \cdots\cdots (2)$$

은닉 계층의 출력을 출력 계층의 입력으로 하고, 출력 계층의 가중치의 곱의 합에 출력 계층의 편의가 더하여 출력 계층의 순입력으로 식 (3)과 같이 사용된다.

$$net_{pk}^{o} = \sum_{j=1}^{L} w_{kj}^{o} i_{pj} + \theta_{k}^{o} \quad \cdots\cdots (3)$$

순입력에 의한 출력 계층의 전달함수의 출력 o가 식 (4)와 같이 계산된다.

$$o_{pk} = f_{k}^{o}(net_{pk}^{o}) \quad \cdots\cdots (4)$$

출력 계층과 은닉 계층의 오차는 식 (5)와 (6)에 의해서 계산된다.

$$\delta_{pk}^{o} = (y_{pk} - o_{pk}) f_{k}^{o'}(net_{pk}^{o}) \quad \cdots\cdots (5)$$

$$\delta_{pj}^{h} = f_{j}^{h'}(net_{pj}^{h}) \sum_{k} \delta_{pk}^{o} w_{kj}^{o} \quad \cdots\cdots (6)$$

출력 계층과 은닉 계층의 가중치의 수정은 식 (7)과 (8)에 의해서 계산된다.

$$w_{kj}^{o}(t+1) = w_{kj}^{o}(t) + \eta \delta_{pk}^{o} i_{pj} \quad \cdots\cdots (7)$$

$$w_{ji}^{h}(t+1) = w_{ji}^{h}(t) + \eta \delta_{pj}^{h} x_{i} \quad \cdots\cdots (8)$$

퍼지 멤버쉽 함수를 이용한 역전파 신경망 학습 알고리즘은 식 (2)와 (6)을 다음의 식 (10)과 (11)로 수정한다.

$$i_{p}^{h} = MF_{j}^{h}(net_{pj}^{h}) \quad \cdots\cdots (9)$$

$$\delta_{pj}^{h} = MF_{j}^{h'}(net_{pj}^{h}) \sum_{k} \delta_{pk}^{o} w_{kj}^{o} \quad \cdots\cdots (10)$$

은닉계층의 전달함수를 신경망의 전달함수 대신에 퍼지 멤버쉽 함수로 대처하여 신경망 학습을 수행한다. (그림 3)의 (5)와 (6)의 퍼지 멤버쉽 함수의 합집합과 교집합을 신경망의 전달함수로 이용하여 학습을 수행한다.

IV. Nuro-Fuzzy 이상 침입 탐지 시뮬레이션

뉴로-퍼지 기법을 적용한 이상 침입 탐지 시뮬레이션은 MIT의 DARPA Intrusion Detection Data 집합의 2000년 윈도우 NT 네트워크 공격 데이터를 이용하였고, 시뮬레이션 툴은 Windump, Tcptrace, Perl 그리고 Matlab을 이용하였다. Windump와 Tcptrace 툴을 이용하여 세션을 구분하고, 네트워크 서비스별로 정상 행위 패턴을 생성하였다. DARPA 침입 데이터에 사용된 네트워크 서비스는 20여개 이상이었으나 시뮬레이션에서는 SSH, FTP와 FTP-Data, Telnet, SMTP 서비스만 추출하여 사용하였다. 생성한 서비스별 정상 행위 패턴들을 모아서 서비스별 정상 행위 프로파일을 구축하였다.

표 3. 네트워크 서비스의 플래그 분포

서비스	세션 (패킷)	플래그			
		종류	패킷	종류	패킷
FTP	650 (18946)	·	14240	R	12
		S	1269	P	2097
		F	1304	ack	18264
SSH	37 (23281)	·	7632	R	3
		S	22	P	15595
		F	29	ack	23266
Telnet	364 (434788)	·	153653	R	11
		S	383	P	280302
		F	439	ack	434567
SMTP	1663 (44386)	·	11045	R	49
		S	3161	P	26864
		F	3267	ack	42709

구축된 프로파일의 패킷 플래그 정보를 이용하여 네트워크 서비스 SSH, FTP와 FTP-Data, Telnet, SMTP에 대한 각각의 퍼지 멤버쉽 함수를 구축하였다. 구축된 네트워크 서비스별 정상 행위 프로파일을 뉴로-퍼지 이상 침입 탐지의 지도학습 데이터로 사용한다. 네트워크 서비스의 정상 프로파일의 서비스, 패킷 개수, 플래그 그리고 Tcp 세션 등의 11개 특징 벡터를 이용하여 뉴로-퍼지 이상 침입 탐지를 수행한다. 뉴로-퍼지 이상 침입 탐지를 위한 구성도는 (그림 4)와 같다. 오차율 0.01과 epoch수를 20,000번 이하로 학습을 수행하였다.

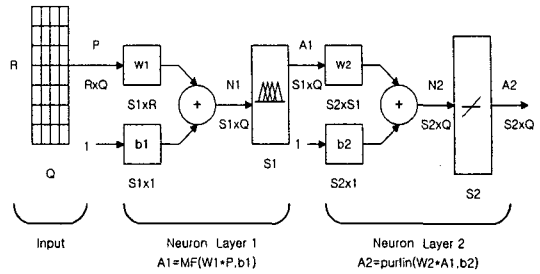

그림 4. 2 계층의 뉴로-퍼지구성도

MIT's Lincoln Lab의 DARPA 데이터 집합의 네트워크 서비스의 플래그 분포는 〈표 3〉과 같으며, 시뮬레이션에서 사용될 침입 데이터 집합의 공격유형은 다음의 〈표 4〉와 같다.

표 4. DARPA 2000년 NT의 공격 유형

공격유형	서비스(포트번호)	공격 횟수
portsweep	smtp	1
	ssh	1
	ftp	1
sechole_setup	ftp	2
	ftp-data	2
	telnet	1
ntis	ftp	3
	ftp-data	12
	telnet	1

뉴로-퍼지 이상 침입 탐지는 portsweep, sechole-setup 그리고 ntis 공격에 대해 시뮬레이션하였다.

시뮬레이션 결과는 (그림 5) 와 같다.

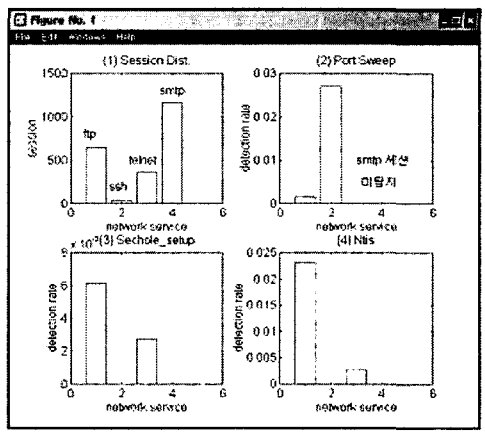

그림 5. 뉴로-퍼지 이상 침입 탐지 결과

V. 결론

최근의 정보통신 기반구조는 인터넷의 개방형 구조를 가지고 있어 서비스 품질의 보장과 네트워크의 관리가 어렵고, 기반구조의 취약성으로 인하여 해킹 및 정보유출 등의 위협으로부터 노출되어있다. 불법 및 고의로 네트워크를 통한 컴퓨터 시스템에 접근하여 피해를 야기하는 문제에 대해 침입 차단, 인증 그리고 접근제어 등의 다양한 방법이 제공되고 있지만 역부족 상태이다. 본 논문에서는 이상 침입 탐지에 기계 학습 기법인 신경망과 불확실성을 해결하기 위한 방법인 뉴로-퍼지를 이용한다. 즉, 신경망 학습의 전달함수를 불확실성을 해결하기 위한 퍼지의 멤버쉽 함수로 수정하여 수행한다. 네트워크 서비스의 정상 프로파일의 서비스, 패킷 개수, 플래그 그리고 Tcp 세션 등의 11개 특징 벡터를 이용하여 뉴로-퍼지 이상 침입 탐지를 수행한다. 그리고 오차율 0.01과 epoch수를 20,000번 이하로 학습을 수행하였다. 시뮬레이션에 사용한 데이터는 DARPA 200년 NT 데이터를 이용하여 portsweep, sechole-setup 그리고 ntis 공격에 대해 이상 침입 탐지를 수행하여 portsweep 공격은 67%, sechole_setup 공격은 100% 그리고 ntis 공격은 100% 탐지하였다. portsweep 공격의 ftp와 ssh 세션은 탐지하였으나, smtp 세션을 탐지하지 못하였다. smtp의 정상 프로파일에 의한 학습량이 많고, 세션에 대한 정보를 완벽하게 학습이 이루어지지 않아 portsweep 공격의 smtp 세션을 탐지하지 못하였다.

참고문헌

[1] R.G.Bace, "intrusion Detection", Macmillan Technical Publishing, 2000.

[2] K. L. Fox, R. R. Henning, J H. Reed, and R. p Simonist. "A Neural Network Approach Towards Intrusion Detection", In Proceedings of the 13th National Computer Security Conffrence : Udlrmation Systems Security Standards - the Key to the Future, Washington, DC, October 1990. NIST, Gaithersburg, MD. Vol. 1, pp. 125 - 134,1990.

[3] H. Debar, B. Dorizzi, "An application ofa recurrent network to an Intrusion detection system", IEEEInternational Conference on Neural Network Conference, Vol.2, pp.478-483,1992

[4] H. Debar, M. Booker, and D. Siboni, "A neural network component for an intrusion detection". Proceedings of the 1992 IEEE Computer Society Symposium on Research in Security and Privacy, pp.240-250,1992.

[5] K. Tan, "The application of neural networks to UNIX computer security", Proceedings of the International Conference on Neural Networks '95, Vol. 1, pp.476-481, 1995.

[6] G. p. Kumar and p. Venkateram, "Security management architecture for access control to network resources", IEEE Proceedings on Computers and Digital Techniques, Vol. 144-6, pp.362-370, Nov. 1997

[7] D. Endler, "Intrusion detection. Applying machine learning to Solaris audit data", Proceedings of the 1998 Annual Computer Security Applications Conference (ACSAC '98), pp.268-279, Los Alamitos, CA, December 1998.

저 자 소 개

김 도 윤
목포과학대학 의료정보시스템과
전임강사

서 재 현
목포대학교 정보공학부 정보보호
전공 부교수