네트워크기반의 이상침입탐지를 위한 퍼지신경망에 대한 연구

김도윤°, 서재현
목포과학대학° , 목포대학교
kdy@mokpo-c.ac.kr° , jhseo@mokpo.ac.kr

A study on network-based Neuro-Fuzzy network for Anomaly Intrusion Detection

Do-yun Kim° , Jae-hyun Seo
mokpo science college° , mokpo national university

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 이상침입 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.

1. 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] .

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.

2. 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.

2.1 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.

(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.

(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.

(3) 신경망

신경망(Neural Networks)은 인공지능의 한 분야이다. 이것은 주로 직관적인 결정을 하는데 있어서 컴퓨터의 지능을 향상시키기 위한 것이다. 주로 패턴 분류에 이용되는데 이것은 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.[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 기준

위논문은 2003년도 정보통신기초기술연구지원사업에 의해 수행되었음

으로 학습을 수행하며 실제 이벤트가 그 모델에서 어떠한 값을 갖는지를 검사한다.

2.2 퍼지와 신경망

(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.

(2) 역전파 신경망

신경망 모형을 구성하는 가장 기본적인 단위는 뉴런(neuron)이며 기본적인 정보처리의 단위이다. 이는 입력값들을 가중 합산하여 그 결과를 전이함수(transfer function)로 전환하여 결과를 전달하는 기능을 수행한다.

신경망이 주어진 자료의 특성을 학습하는데 사용되는 학습 알고리즘(learning algorithms)에는 여러 가지가 있으나 그 중에서 오차를 최소화시켜 나가는 역전파(back propagation) 방법이 흔히 사용된다. 역전파 알고리즘은 최소자승 알고리즘의 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[3],[4].

3. 뉴로-퍼지 IDS

이상 침입 탐지에 기계 학습 기법인 신경망과 불확실성을 해결하기 위한 방법인 뉴로-퍼지를 그림 1 과 같이 이용한다.

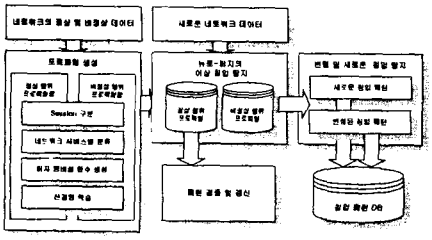

그림 1 뉴로-퍼지 기법의 이상 침입 탐지 구성도

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 퍼지 멤버쉽 함수를 생성하고, 정상 행위의 퍼지 멤베쉽 함수를 지도 학습 신경망에 적용하여 이상 침입 탐지를 수행한다.

3.1 네트워크 데이터의 행위 패턴 생성과 프로파일링 구축

네트워크 행위를 표현하기 위하여 DARPA 2000년 NT 데이터 일부를 표현하면 다음의 표 1와 같이 나타낼 수 있다.

표 1. 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 1와 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.

3.2 퍼지 멤버쉽 함수 생성

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

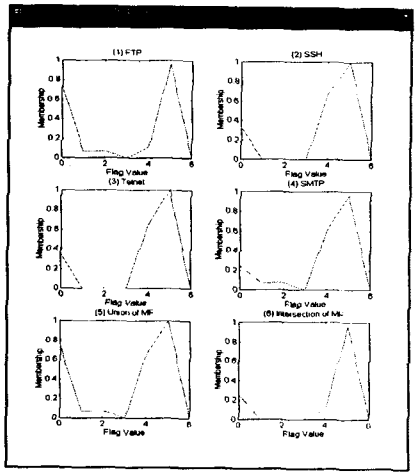

그림 2. 네트워크 서비스별 플래그 분포와 멤버쉽 함수의 합집합과 교집합

그림 2 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 3의 (5)와 (6)이 된다.퍼지 집합의 합집합은 상한을 나타내고, 퍼지

집합의 교집합은 하한을 나타낸다. 퍼지 집합의 합집합과 교집합에 의해서 좀더 명확한 정보를 제공 신경망의 전달함수로 이용하여 학습을 수행한다.

4. Nuro-Fuzzy 이상 침입 탐지시뮬레이션

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.

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. 그리고 뉴로-퍼지 이상 침입 탐지를 위한 구성도는 그림 3와 같다. 오차율 0.01과 epoch 수를 20,000번 이하로 학습을 수행하였다.

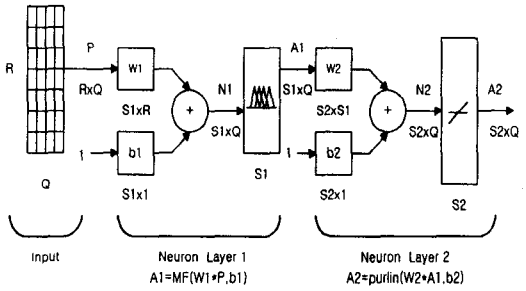

그림 3. 2 계층의 뉴로-퍼지 구성도

뉴로-퍼지 이상 침입 탐지는 portsweep, sechole-setup 그리고 ntis 공격에 대해 시뮬레이션 하였다. 시뮬레이션 결과는 그림 4 와 같다.

5. 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.

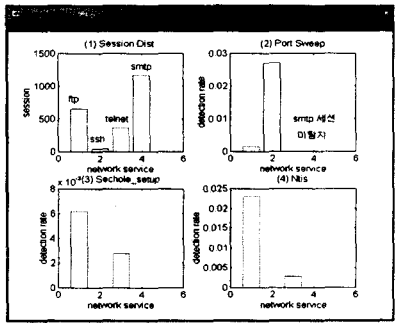

그림 4. 뉴로-퍼지 이상 침입 탐지 결과

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.

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," IEEE International 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.