퍼지 멤버쉽 함수와 신경망을 이용한 이상 침입 탐지

차 병 래†

요 약

컴퓨터 네트워크의 확대 및 인터넷 이용의 급격한 증가에 따른 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 노출되어 있다. 보안 위협에 대한 능동적인 대처 및 침입 이후에 동일한 또는 유사한 유형의 사건 발생에 대해 실시간 대응할 수 있는 방법이 중요하게 되었으며 이러한 해결책으로서 침입 탐지 시스템에 대한 연구가 활발히 진행되고 있다. 본 논문에서는 지도학습 알고리즘에 의한 침입탐지 시스템의 성능을 향상시키기 위해서 불확실성을 해결하기 위한 방법인 퍼지를 적용한 뉴로-퍼지 모델의 이상 침입 탐지 시스템에 대해서 연구한다. 즉, 신경망 학습의 전달함수를 불확실성을 해결하기 위한 퍼지 멤버쉽 함수로 수정하여 지도학습을 수행하였다. 제안한 뉴로-퍼지기법을 DARPA 침입 데이터를 이용하여 오용 탐지의 한계성을 극복한 네트워크기반의 이상침입 탐지에 적용하여 성능을 검증하였다.

Anomaly Intrusion Detection using Fuzzy Membership Function and Neural Networks

Byung-Rae Cha†

ABSTRACT

By the help of expansion of computer network and rapid growth of Internet, the information infrastructure is now able to provide a wide range of services. Especially open architecture - the inherent nature of Internet - has not only got in the way of offering QoS service, managing networks, but also made the users vulnerable to both the threat of hacking and the issue of information leak. Thus, people recognized the importance of both taking active, prompt and real-time action against intrusion threat, and at the same time, analyzing the similar patterns of intrusion already known. There are now many researches underway on Intrusion Detection System(IDS). The paper carries research on the intrusion detection system which hired supervised learning algorithm and Fuzzy membership function especially with Neuro-Fuzzy model in order to improve its performance. It modifies tansigmoid transfer function of Neural Networks into fuzzy membership function, so that it can reduce the uncertainty of anomaly intrusion detection. Finally, the fuzzy logic suggested here has been applied to a network-based anomaly intrusion detection system, tested against intrusion data offered by DARPA 2000 Intrusion Data Sets, and proven that it overcomes the shortcomings that Anomaly Intrusion Detection usually has.

키워드 : 이상 침입 탐지(Anomaly Intrusion Detection), 퍼지 멤버쉽 함수(Fuzzy Membership Function), 신경망(Neural Network)

1. 서 론

최근의 정보통신 기반구조는 컴퓨터 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 위협에 노출되고 있다. 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 대응할 수 있는 방법이 중요하게 되었으며 이러한 해결책으로서 침입 탐지 시스템에 대한 연구가 활발히 진행되고 있다.

침입 탐지 시스템은 단순한 접근 제어 기능을 넘어서 침입 패턴을 데이터베이스로 구축하고, 전문가 시스템을 사용해 네트워크나 컴퓨터 시스템 사용을 실시간 모니터링하여 침입을 탐지하는 보안 시스템이다. 침입 탐지 기법은 크게 이상침입탐지 기법과 오용침입탐지 기법으로 나눌 수 있다. 오용 탐지는 알려진 침입 방법들을 수집하여 지식 베이스에

† 준 회 원 : 여수대학교 전산학과 시간강사
논문접수 : 2004년 5월 11일, 심사완료 : 2004년 8월 2일

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. 일반적으로 오용탐지 방법이 많이 상업화되어 사용되지만 새로운 침입 패턴과 변형된 침입 패턴을 탐지할 수 없는 문제점이 있으며, 오용 탐지를 위한 공격 유형을 분석하여 오용 탐지 규칙 등의 인코딩 작업에 비용과 시간이 많이 소요되는 문제점을 갖고 있다. 해결책으로 정상 및 비정상 행위로부터 침입을 탐지하는 이상 침입 탐지 연구가 진행되고 있으나 아직은 연구 단계에 있으며 상업화되지는 못하고 있다.

네트워크 기반의 이상 침입 탐지 시스템은 네트워크 상의 패킷 데이터를 수집하여 이상 침입을 탐지하는 시스템이다. ADAM[1], NIDES[2], SPADE[3] 등의 네트워크 이상 탐지 시스템들은 감사 데이터로 패킷의 헤더 정보인 IP 주소, 포트, TCP 상태 등을 이용하여 이상행위를 탐지한다. Matthew[4]는 네트워크 이상 탐지 시스템에 PHAD와 ALAD의 두 요소로 구성하여, 패킷 헤더 데이터의 이상 탐지와 응용 계층의 이상 탐지를 수행하였다.

초기 침입탐지 시스템들은 이미 알려진 공격에 대한 징후를 수동으로 전문가 시스템에 인코딩하여 침입 여부를 판단하였다. 그러나 수동적인 방법에 의한 규칙의 생성 및 확장은 매우 어려운 일이며, 그 효율성이 매우 떨어지는 방법이다. 이러한 문제를 해결하기 위하여 인공지능, 기계학습 및 데이터마이닝 기법들을 침입탐지에 이용하기 시작하였다. 지도학습에 기반을 둔 많은 침입탐지 시스템은 학습과 침입탐지 과정이 구분되어있다. 따라서, 침입탐지를 위해서는 학습과정이 반드시 필요함으로 시스템의 안정된 성능이 나오기까지 많은 비용이 들며, 시스템 학습을 위해 많은 양의 학습 데이터를 필요로 한다. 이러한 방대한 학습 데이터의 수집 및 분류는 매우 어려운 일이며, 학습 데이터의 질에 의해 시스템의 성능이 크게 좌우된다. 현재 침입탐지에 사용되고 있는 많은 알고리즘은 방대한 데이터의 처리 및 점증적 학습을 동시에 수행하기가 매우 어렵다. 따라서, 실시간 침입탐지를 위한 온라인 시스템의 구축과 학습된 데이터 이외의 침입 유형에 대한 탐지 및 침입 유형에 대한 정보 제공이 어렵다[5-8].

본 논문에서는 지도학습법에 근간을 둔 침입탐지 시스템들이 가지고 있는 문제점들을 해결하기 위하여 신경망에 퍼지 멤버쉽 함수를 적용하여 네트워크기반의 뉴로-퍼지 기법을 적용하고자 한다. 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 이용한 퍼지 멤버쉽 함수를 생성하고, 정상 행위의 퍼지 멤버십 함수를 지도 학습 신경망에 적용하여 이상 침입 탐지를 수행한다. 불확실성을 처리하는 퍼지 이론을 이상 침입 탐지영역에 도입하여 적용함으로써 오용 탐지의 한계성을 극복하여 알려지지 않은 침입 탐지를 하고자 한다.

본 논문의 2장은 관련연구로써 이상 침입 탐지 모델을 분류하고, 퍼지와 신경망에 대해 기술한다. 3장은 이상 침입 탐지를 위한 네트워크 행위 프로파일 구축, 퍼지 멤버쉽 함수 생성 그리고 뉴로-퍼지 기법 적용을 위한 알고리즘을 제시하였으며, 4장은 신경망과 뉴로-퍼지를 적용한 네트워크 기반의 이상 탐지 기법의 시뮬레이션 수행 및 비교/분석한다. 그리고 5장에서는 결론 및 향후 연구방향을 기술한다.

2. 관련 연구

2.1 이상 침입 탐지 시스템

침입 탐지란 1980년 Anderson에 의하여 침입의도를 가지고 비인가된 정보로의 접근 및 분석 정보조작, 그리고 시스템의 무기력화에 대한 고의적 시도에 대한 모든 가능성을 탐지하는 것이라 정의하였다. 또한 서비스 거부원인, 백도어 생성, 바이러스 생산, 공격용 도구에 의한 컴퓨터 자원의 무결성, 신뢰성을 손상시키고자 하는 시도를 침입으로 정의하였다. 침입은 크게 두 가지로 정의 할 수 있다 첫 번째는 컴퓨터가 사용하는 자원의 무결성, 비밀성, 신뢰성을 저해하는 일련의 행위들의 집합을 침입이라 할 수 있으며 두 번째는 컴퓨터 시스템의 보안정책을 파괴하는 행위를 침입이라고 할 수 있다. 이러한 침입은 행위의 결과에 따라 이상 침입과 오용침입으로 두 가지로 분류된다[3].

이상 침입 탐지는 컴퓨터자원의 비정상적인 행위에 근거하며 오용 침입 탐지는 잘 만들어진 공격 패턴을 의미한다. 침입 탐지 시스템은 컴퓨터 시스템의 비정상적인 행위를 규정하는 시스템으로 모델에 따라 오용탐지, 이상행위탐지, 복합탐지로 나뉘고 침입탐지 정보를 획득하는 영역에 따라 호스트 기반 침입 탐지 시스템과 네트워크 기반 침입 탐지 시스템으로 분류하고 있다.

이상 침입 탐지의 대표적인 방법으로는 통계적 방법, 컴퓨터 면역학, 신경망 학습 등이 있다 이러한 탐지 방법들은 어떤 방법이나 매개체를 사용하느냐에 따라 분류되지만 본질적으로 비정상적인 침입을 탐지하는 방법은 거의 유사하다.

통계적 방법은 이상 행위탐지에서 가장 많이 이용되는 방법으로서 과거의 데이터를 통계적으로 처리한 특정 데이터나 사건에 대한 임계치, 행위강도 중심으로 생성된 정보를 근거로 하여 특별한 행위 및 유사 사건을 방지하는 방법으로 대부분 시스템은 변수에 평균을 유지하며 표준편차에 의한 임계값을 초과하였는지를 검사한다[9]. 통계적 방법을 이용한 예로서 탐지 방법은 사용자나 사용자가 실행시킨 행위

를 관찰하고 행위에 대한 프로파일을 생성하며, 이 생성된 프로파일들을 토대로 주기적으로 프로파일의 비정상적인 행위를 측정한다.

신경망은 이론적으로 오용탐지에 적합하지만 비정상 행위 탐지에 많이 사용되었으며, 명령어의 순서를 신경망으로 학습시켜서 다음에 수행될 명령어를 미리 예측할 수가 있으며, 다음에 수행될 명령어를 예측 가능하기에 사용자가 정상인지 비정상인지를 탐지할 수가 있다. 현재의 명령어와 과거에 수행시켰던 명령어들을 입력계층에 입력시키면 신경망은 학습을 통하여 다음에 나올 명령어를 출력계층에서 예측할 수가 있다. 신경망을 사용하면 통계적 방법에 비해 변수들 간에 비 선형적 관계를 간단하게 표현할 수 있으며, 신경망의 자율 학습 알고리즘 등이 있다.

컴퓨터 면역학은 생물계의 면역시스템을 연구한다. 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[10].

네트워크 기반의 이상 탐지 모델은 비정상적인 패킷에 대하여 탐지를 하는 모델로서 정상적인 상태를 다양한 방법으로 정보를 수집하고 정상에서 벗어나는 네트워크의 비정상적인 행위를 탐지하는 방법으로, 감사 자료는 네트워크 상의 패킷 데이터를 수집한 패킷 데이터를 사용하며, 프로파일은 정상과 비정상의 패킷에 대하여 정상 프로파일과 비정상 프로파일을 생성하며, 이 프로파일은 지속적으로 새로운 프로파일을 생성하면서 공격에 대한 패킷을 탐지한다.

2.2 퍼지와 신경망

2.2.1 퍼지 개념과 퍼지 집합의 연산

인공지능 분야의 퍼지이론은 1965년 미국 버클리대학의 Zadeh교수에 의해 처음 소개되었다. 일반적으로 불확실성을 처리하는 이론들이 많으나 그 중에서도 퍼지 이론은 성능이 우수하기 때문에 다른 불확실성 처리 이론보다 많이 사용된다. 또한 퍼지이론은 모호하게 표현된 자료를 이용하여 우리에게 유용한 자료로 만들기 위해 퍼지집합, 퍼지논리, 퍼지숫자, 퍼지관계 등의 개념을 포함하고 있으며 수학적인 계산방법도 잘 발달되어 있다[11].

일상 언어에서 '매우 아름답다', '다소 젊다'와 같은 모호한 표현을 퍼지집합이라 하고 이것의 의미를 개념적으로 그래프화하여 나타낸 것을 멤버쉽 함수(membership function)라 한다. 일반집합과 퍼지집합과의 차이점을 설명하면, 어떤 원소 x가 집합 A에 속하느냐, 속하지 않느냐 만을 나타내는 일반집합을 퍼지집합에 반해 크리스프 집합이라고 한다.

퍼지집합은 일반집합과 마찬가지로 여집합, 합집합, 교집합과 같은 기본연산이 존재한다.

여집합(compliment)은 퍼지집합 A의 여집합은 $\overline{A}$로 나타내고, 일반집합과 마찬가지로 1에서 모든 멤버쉽값을 빼서 구한다. 그러나 여집합 $\overline{A}$는 경계가 명확하지 않는 퍼지집합이 된다. 합집합(union)은 두 퍼지집합 A와 B의 합집합은 $A \cup B$로 나타내고 전체집합 내의 각 원소에 대해 두 집합 A와 B의 멤버쉽 값 중에서 큰 것으로 구성한다. 교집합(intersection)은 두 퍼지집합 A와 B의 교집합은 $A \cap B$로 나타내고 전체집합 내의 각 원소에 대해 두 집합 A와 B의 멤버쉽 값 중에서 작은 것으로 구성한다.

2.2.2 신경망

신경망은 두뇌 활동의 매커니즘을 수학적으로 재현한 인공지능의 한 분야이다. 신경망은 인간의 두뇌를 모방하여 같은 지적능력을 학습을 통하여 컴퓨터에 지식베이스로 구축하고, 구축된 지식베이스를 이용하여 주어진 자료를 추론하고 그 결과를 예측하고 설명하는 기능을 말한다.

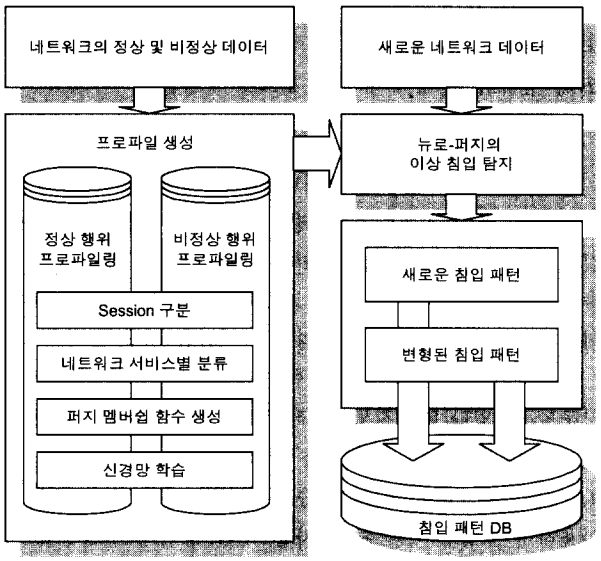
신경망의 학습방법은 지도학습, 자율학습, 경쟁학습으로 구분할 수 있다[12]. 지도 학습 방법은 신경망을 학습시키는데 있어서 반드시 입력 x와 원하는 목표치 d의 순서쌍 (x, d)가 필요하며, 이를 학습 패턴이라 한다. 학습 패턴을 이용하여 학습을 수행한다. 자율 학습 방법은 신경망을 학습시키는데 목표치가 필요없이 알고리즘에 의해서 자율적으로 학습이 이루어진다. 경쟁 학습 방법은 지도 학습 방법과 동일한 절차이지만, 각 단계에서 전체 연결강도를 변경시키지 않고 단지 특정 부분의 연결강도만을 변화시키는 방법이다. 이 방법은 연결강도를 변화시키는 과정이 축소되므로 신경망의 학습에 소요되는 시간을 상당히 감소시킬 수 있다.

신경망이 주어진 자료의 특성을 학습하는데 사용되는 학습 알고리즘에는 여러 가지가 있으나 그 중에서 오차를 최소화시켜 나가는 역전파 방법이 흔히 사용된다. 역전파 알고리즘은 최소자승 알고리즘의 비선형적 확장으로 볼 수 있는 가장 많이 쓰이는 지도학습 기법이다. 즉, 입력계층의 각 노드에 입력패턴을 주면 이 신호는 각 노드에서 변환되어 은닉계층에 전달되고 계산과정을 거쳐 출력계층에서 신호를 출력하게 된다. 이때 출력값과 목표값을 비교하여 둘 사이의 차이, 즉 오차를 줄여나가는 방향으로 가중치를 반복적으로 조정해 나가는 방법이 역전파 신경망 학습법이다.

3. 뉴로-퍼지 IDS

이상 침입 탐지에 기계 학습 기법인 신경망과 불확실성을 해결하기 위한 방법인 퍼지 이론을 (그림 1)과 같이 이상 침입 탐지 시스템을 구성한다.

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.



(그림 1) 뉴로-퍼지 기법의 이상 침입 탐지 구성도

3.1 네트워크 행위 패턴 생성과 프로파일링 구축

네트워크 기반의 침입 탐지에는 네트워크 데이터인 패킷의 헤더 정보를 이용하여 이상이나 오용 침입을 탐지한다. 본 논문에서는 네트워크의 패킷 헤더 정보를 이용하여 서비스별로 분류하며, 다양한 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. TCP를 이용하여 두 호스트 사이에 전달되는 데이터의 단위를 세그먼트라고 한다. 세그먼트는 20에서 60바이트의 헤더와 응용 프로그램으로부터 발생되는 데이터로 구성된다. 헤더는 옵션이 없는 경우에는 20바이트이고, 옵션을 포함하는 경우 최대 60바이트로 구성된다. TCP 프로토콜을 분석하기 위해서는 Windump 툴을 이용하여 패킷을 캡처한다. Tcptrace 툴과 Perl을 이용하여 FTP, SSH, Telnet 그리고 SMTP 네트워크 서비스에 대한 정상 행위 패턴을 구축하기 위한 패턴 벡터를 구성한다.

3.2 네트워크 행위 패턴의 표현법

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 행위 패턴 표7현법

메타기호	의 미
플래그	네트워크 패킷 헤더에 포함된 플래그
<, >	세션의 시작과 끝은 각각 <와 >으로 표시하거나, 순차 세션의 분기와 병합을 표시.
-	패킷과 패킷을 '-'에 의해 구분
X	심볼 X는 모든 동작에 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[13]의 일부를 표현하면 다음의 <표 2>와 같이 나타낼 수 있다. <표 2>와 같이 표현된 네트워크 행위들을 모아서 정상 행위 프로파일 구축에 사용된다.

〈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>

네트워크 기반의 침입 탐지에는 네트워크 데이터인 패킷의 헤더 정보를 이용하여 이상이나 오용 침입을 탐지한다. 본 논문에서는 TCP/IP 네트워크의 패킷 헤더 정보를 이용하여 네트워크 서비스별로 분류하며, 네트워크 서비스별로 정상 행위를 프로파일링하여 이상 침입 탐지를 위한 정보를 제공한다. 대부분의 네트워크 침입 탐지는 단지 TCP/IP 패킷의 이상 유무와 침입시의 패킷의 여러 특징에 의해서 이상 침입을 탐지한다. 본 논문에서는 패킷 헤더 정보에 특정한 네트워크 서비스에 대한 각각의 제약 정보를 제공함으로써 네트워크 이상 침입을 명확히 구분하고자 한다.

네트워크의 정상 데이터를 세션 단위로 학습에 적용하기 위해서는 먼저, 패턴을 생성하기 위한 특징 선택이 필요하다. 본 논문에서는 12개의 특징을 선택하였다. 특징으로는 네트워크 서비스, 세션을 구성하는 패킷의 개수, TCP 통신 절차, 리셋연결, 단방향 통신 그리고 패킷의 플래그의 분포로 구성한다. 네트워크 서비스별 세션은 모두 크기가 같지 않으므로 패킷의 개수와 플래그의 분포로 특징 선택하였다.

〈표 3〉 특징 선택에 의한 패턴 벡터의 구성

특징선택	형 식	내 용
서비스	Integer	TCP 네트워크 서비스 종류
세션크기	Integer	세션의 패킷 갯수
TCP 절차	비트값	TCP 통신 절차 수행 여부
리 셋	비트값	RESET 통신 절차 수행 여부
단방향통신	비트값	단방향 통신 수행 여부
No Flag	Integer	No Flag의 수
F	Integer	Fin의 수
S	Integer	Syn의 수
R	Integer	Reset의 수
P	Integer	Push의 수
ack	Integer	ack의 수
U	Integer	Urg의 수

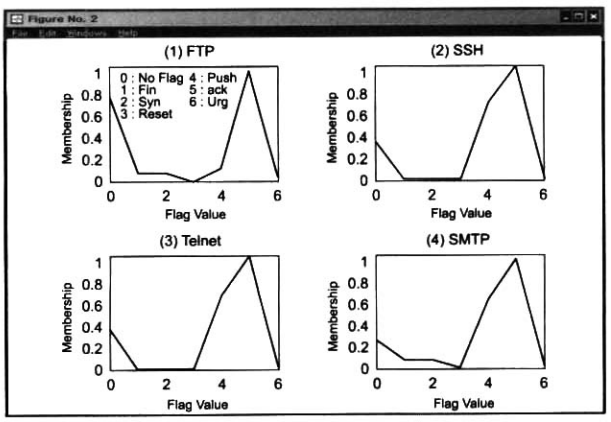
〈표 4〉 학습에 사용될 패턴 수

서비스 종류	패턴의 수	중복제거 패턴	비 고
SSH	37	31	
FTP	650	512	FTP와 FTP-Data
Telnet	364	340	
SMTP	1663	498	
합 계	2,714	1,381	

<표 4>는 시뮬레이션에 사용된 학습 패턴에 대한 정보이다. 프로토콜은 SSH, FTP, Telnet 그리고 SMTP가 사용되었다. 사용된 패턴의 수는 중복을 제거한 SSH는 31개 패턴, FTP는 512, Telnet 340 그리고 SMTP는 498개인 총 1,381개의 패턴을 사용하여 학습을 수행한다.

3.3 퍼지 멤버쉽 함수 생성

뉴로-퍼지 이상 침입 탐지에 사용될 퍼지 멤버쉽 함수는 네트워크 서비스별 정상 행위 프로파일을 이용한다. (그림 2) (1)은 SSH 서비스, (2)는 FTP와 FTP-Data 서비스, (3)은 Telnet 서비스 그리고 (4)는 SMTP 서비스의 퍼지 멤버쉽 함수를 나타낸다.



(그림 2) 네트워크 서비스별 멤버쉽 함수값

네 가지 네트워크 서비스의 멤버쉽 함수를 퍼지 집합의 합집합과 교집합의 연산을 수행하면, (그림 3)(a)와 (b)가 된다. 퍼지집합간의 연산이 대부분 Max, Min 연산자를 기본으로 하여 이루어진다.

〈표 5〉 플래그별 퍼지 멤버쉽 함수의 합집합 계산

$$\mu_{(FTP \cup SSH \cup Telnet \cup SMTP).NF}(x) = Max(\mu_{FTP.NF}(x), \mu_{SSH.NF}(x), \mu_{Telnet.NF}(x), \mu_{SMTP.NF}(x))$$

$$\mu_{(FTP \cup SSH \cup Telnet \cup SMTP).F}(x) = Max(\mu_{FTP.F}(x), \mu_{SSH.F}(x), \mu_{Telnet.F}(x), \mu_{SMTP.F}(x))$$

$$\mu_{(FTP \cup SSH \cup Telnet \cup SMTP).S}(x) = Max(\mu_{FTP.S}(x), \mu_{SSH.S}(x), \mu_{Telnet.S}(x), \mu_{SMTP.S}(x))$$

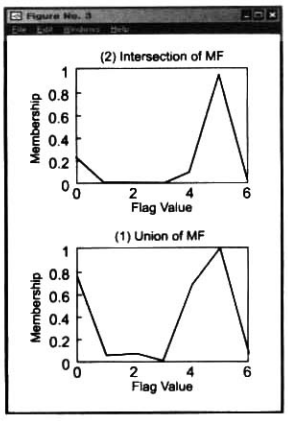
$$\mu_{(FTP \cup SSH \cup Telnet \cup SMTP).R}(x) = Max(\mu_{FTP.R}(x), \mu_{SSH.R}(x), \mu_{Telnet.R}(x), \mu_{SMTP.R}(x))$$

$$\mu_{(FTP \cup SSH \cup Telnet \cup SMTP).P}(x) = Max(\mu_{FTP.P}(x), \mu_{SSH.P}(x), \mu_{Telnet.P}(x), \mu_{SMTP.P}(x))$$

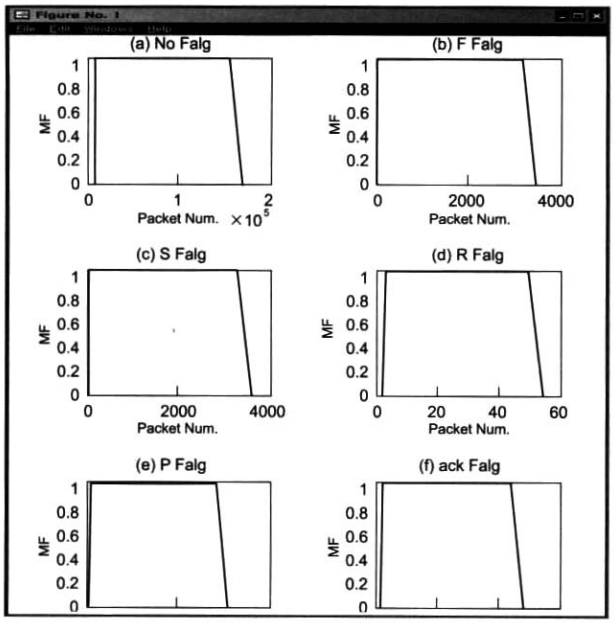
$$\mu_{(FTP \cup SSH \cup Telnet \cup SMTP).ack}(x) = Max(\mu_{FTP.ack}(x), \mu_{SSH.ack}(x), \mu_{Telnet.ac}k(x), \mu_{SMTP.ack}(x))$$

$$\mu_{(FTP \cup SSH \cup Telnet \cup SMTP).U}(x) = Max(\mu_{FTP.U}(x), \mu_{SSH.U}(x), \mu_{Telnet.U}(x), \mu_{SMTP.U}(x))$$

(그림 3)(1)은 퍼지 멤버쉽 함수의 합집합은 네트워크의 FTP, SSH, Telnet 그리고 SMTP 서비스의 각각의 플래그에 대한 멤버쉽값 중에서 가장 큰 값으로 합집합은 <표 5>와 같이 계산된다. (그림 3)(2)은 퍼지 멤버쉽 함수의 교집합은 네트워크의 FTP, SSH, Telnet 그리고 SMTP 서비스의 각각의 플래그에 대한 멤버쉽값 중에서 가장 작은 값으로 교집합 연산에 의해 계산된다.



(그림 3) 네트워크 서비스별 멤버쉽 함수의 합집합과 교집합



(그림 4) 플래그별 사다리꼴 멤버쉽 함수

퍼지 집합의 합집합은 상한을 나타내고, 퍼지 집합의 교집합은 하한을 나타낸다. 퍼지 멤버쉽 함수의 또 하나의 특별한 형태는 사다리꼴 퍼지 멤버쉽 함수이다. 사다리꼴 퍼지 멤버쉽 함수의 형태는 퍼지 멤버쉽 함수의 소속정도가 최대가 되는 점이 여러 개가 되어 사다리꼴 모양이 된다. 즉, 사다리꼴 퍼지 멤버쉽 함수를 정의하면, $trapezoidal_MF = (a_1, a_2, a_3, a_4)$이 된다. 네트워크 서비스의 플래그별 퍼지 멤버쉽 함수의 교집합은 사다리꼴 퍼지 멤버쉽 함수의 하한값에 해당하는 a_2에 할당한다. 퍼지 멤버쉽 함수의 합집합은 사다리꼴 퍼지 멤버쉽 함수의 상한값에 해당하는 a_3에 할당한다. 역전파 신경망 학습의 tansig 전달함수보다 뉴로-퍼지 학습의 은닉계층에서 퍼지 멤버쉽 함수의 합집합과 교집합에 의한 정보에 의해서 이상 탐지를 위한 보다 많은 정보를 (그림 4)와 같이 제공한다.

(그림 4)는 퍼지 멤버쉽 함수에 의해서 플래그별 퍼지 멤버쉽 전달함수 값을 나타낸 것이다. (a)는 No 플래그, (b)는 F 플래그, (c)는 S 플래그, (d)는 R 플래그, (e) P 플래그 그리고 (f)는 ack 플래그 값를 표시하며, 사다리꼴 형태의 함수값을 갖는다.

3.4 퍼지 멤버쉽 함수를 이용한 BPN 학습

침입 탐지 연구에 각각의 신경망 기법과 퍼지 기법를 적용한 많은 침입 탐지 연구가 있었다[14-19]. 본 논문에서는 신경망 구조의 은닉 계층에 퍼지 멤버쉽 함수를 적용한 혼합 모델을 제안한다.

〈표 6〉 역전파 신경망 학습의 알고리즘

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

$$i_p^h = f_j^h(net_{pj}^h) \quad (2)$$

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

$$o_{pk} = f_k^o(net_{pk}^o) \quad (4)$$

$$\delta_{pk}^o = (y_{pk} - o_{pk}) f_k^{o\prime}(net_{pk}^o) \quad (5)$$

$$\delta_{pj}^h = f_j^{h\prime}(net_{pj}^h) \sum_k \delta_{pk}^o w_{kj}^o \quad (6)$$

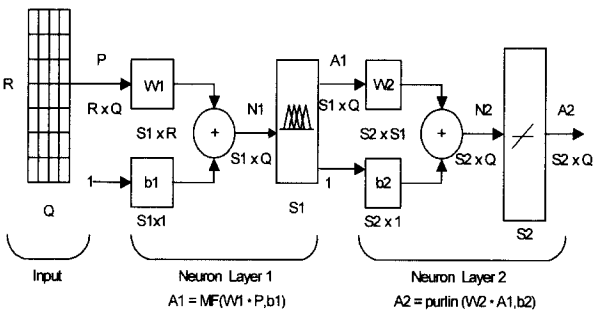
$$w_{kj}^o(t+1) = w_{kj}^o(t) + \eta \delta_{pk}^o i_{pj} \quad (7)$$

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

$$E_p = \frac{1}{2} \sum_{k=1}^{M} \delta_{pk}^2 \quad (9)$$

역전파 신경망 알고리즘은 최소자승 알고리즘의 비선형적 확장으로 볼 수 있는 가장 많이 쓰이는 지도학습 기법이다. 즉, 입력계층의 각 노드에 입력패턴을 주면 이 신호는 각 노드에서 변환되어 은닉계층에 전달되고 계산과정을 거쳐 출력계층에서 신호를 출력하게 된다. 이때 출력값과 목표값을 비교하여 둘 사이의 차이, 즉 오차를 줄여나가는 방향으로 가중치를 반복적으로 조정해 나가는 방법이 역전파 신경망 학습법이다.

역전파 신경망의 학습은 입력 x와 은닉계층의 가중치 w의 곱의 합에 은닉 계층의 편의(bias) θ를 더하여 순입력으로 식 (1)과 같이 사용된다. 순입력에 의한 은닉계층의 전달함수의 출력 i가 식 (2)와 같이 계산된다. 은닉 계층의 출력을 출력 계층의 입력으로 하고, 출력 계층의 가중치의 곱의 합에 출력 계층의 편의가 더하여 출력계층의 순입력으로 식 (3)과 같이 사용된다. 순입력에 의한 출력 계층의 전달함수의 출력 o가 식 (4)와 같이 계산된다. 출력 계층과 은닉 계층의 오차는 식 (5)와 식 (6)에 의해서 계산된다. 출력 계층과 은닉 계층의 가중치의 수정은 식 (7)과 식 (8)에 의해서 계산된다. 출력 계층의 가중치의 값의 변경은 식 (8)과 같고 은닉 계층의 가중치의 변화는 식 (9)와 같다[20].



(그림 5) 퍼지 멤버쉽 함수와 신경망의 소프트웨어 모델

(그림 5)는 2계층의 뉴로-퍼지 모델의 소프트웨어 구성도이다. 퍼지 멤버쉽 함수를 이용한 역전파 신경망 학습 알고리즘은 식 (2)와 식 (6)을 다음의 식 (10)과 식 (11)로 수정한다.

〈표 7〉 퍼지 멤버쉽 함수를 이용한 전달함수

$$i_p^h = MF_j^h(net_{pj}^h) \quad (10)$$

$$\delta_{pj}^h = MF_j^{h\prime}(net_{pj}^h)\sum_k \delta_{pk}^o w_{kj}^o \quad (11)$$

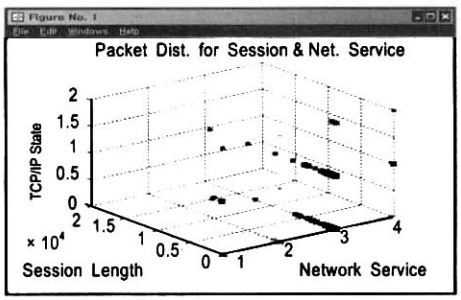
은닉계층의 전달함수를 신경망의 전달함수 대신에 퍼지 멤버쉽 함수로 대처하여 신경망 학습을 수행하며 (그림 4)의 퍼지 멤버쉽 함수의 합집합과 교집합에 의해 산출된 사다리꼴 퍼지 멤버쉽 함수를 신경망의 전달함수로 이용하여 학습을 수행한다.

(그림 5)에서 신경망 은닉계층의 전달함수를 퍼지 멤버쉽 함수값으로 대처함으로써 이상 침입 탐지를 위한 학습에 보다 많은 정보를 제공할 수 있다. 이 퍼지 멤버쉽 전달 함수에 의해 뉴로-퍼지 시스템의 은닉계층에 이용되며, 이상 침입 탐지 시뮬레이션을 수행한다.

4. 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.

본 논문에서는 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 서비스인 SSH, FTP와 FTP-Data, Telnet, SMTP에 대한 각각의 퍼지 멤버쉽 함수를 구축하였다.



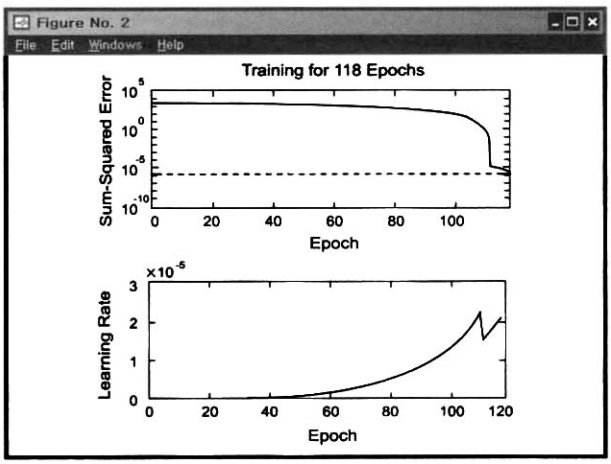
(그림 6) 서비스별 특징 벡터의 분포

(그림 6)은 DARPA 데이터를 네트워크 서비스별로 분류하여 특징 선택하였으며, x축은 특징 벡터인 네트워크 서비스를 나타내며, y축은 세션의 크기를 나타내는 정상 행위 패킷의 개수를 나타낸다. 그리고 z축은 TCP 통신 절차 여부, RESET 절차 여부, 단방향 통신 등의 패킷 플래그 정보의 패턴 벡터 값을 나타낸다.

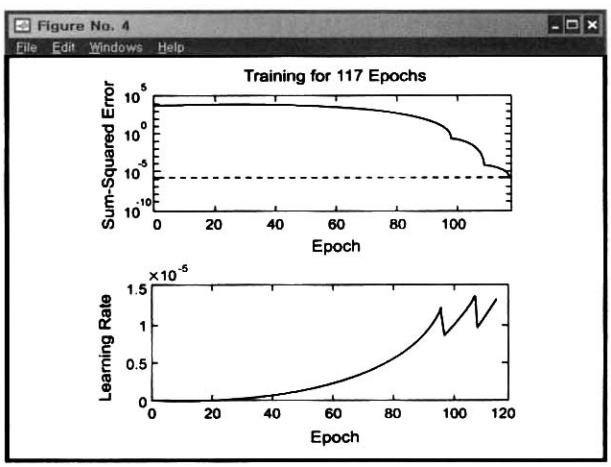
4.1 신경망의 과적합과 미적합

은닉 계층의 뉴런 수를 6에서 15까지 변경하여 학습율과 에러를 (그림 7)에서 (그림 9)까지 나타낸다. 신경망 학습의 단점인 과적합(overfitting)과 미적합(underfitting)을 벗어나기 위해서는 은닉 계층의 뉴런을 결정하여야 한다. 과적합은 학습에 학습 데이터이외에 잡음도 학습하는 경우를 의미하며, 미적합은 학습이 제대로 이루어지지 않은 상태를 의미한다.

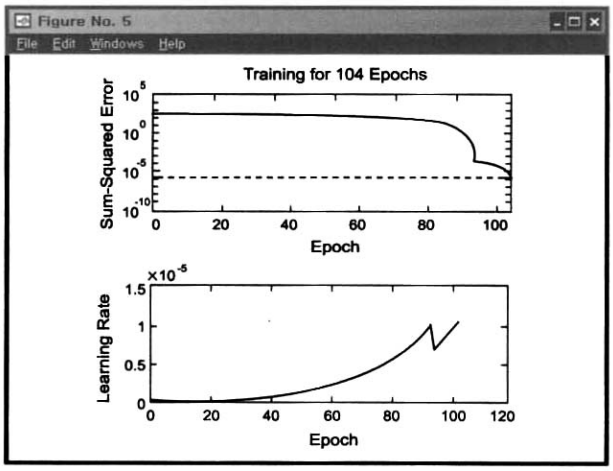
(그림 7)은 은닉 계층의 뉴런의 수가 6인 경우이며, 118 Epoch, (그림 8)은 뉴론 12, 117 Epoch, (그림 9)는 뉴런 15, 104 Epoch가 되어 학습이 완료되었다.



(그림 7) 뉴런 수가 6인 경우



(그림 8) 뉴런 수가 12인 경우



(그림 9) 뉴런 수가 15인 경우

(그림 7)부터 (그림 9)에 의해서 Epoch 측면에 의해서 뉴런 15개가의 104 Epoch로 적당하다. Epoch 수가 크다는 것은 미적합일 가능성이 크며, 은닉 뉴런의 수가 크면 과적합의 경우가 발생할 수 있다. 은닉 계층의 뉴런의 수가 6과 12는 Epoch 118, 177이므로 뉴런의 수는 12가 적합하다고 할 수 있다.

4.2 퍼지 멤버쉽 함수와 신경망을 이용한 이상 침입 탐지

MIT's Lincoln Lab의 DARPA 침입 데이터 집합의 FTP, SSH, Telnet 그리고 SMTP 네트워크 서비스에 사용된 침입 데이터 집합의 공격 유형인 Portsweep, Sechole 그리고 Ntis 공격을 퍼지 멤버쉽 함수와 신경망을 이용한 이상 탐지를 시뮬레이션한다.

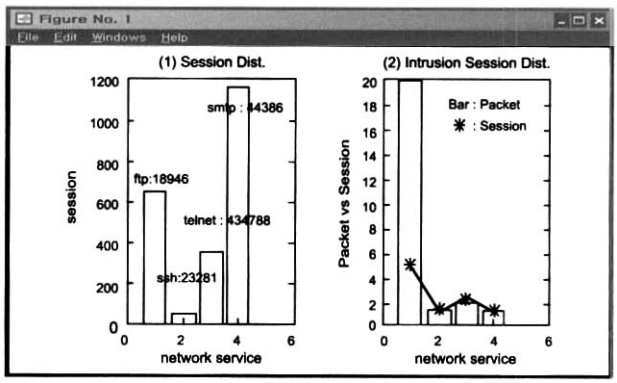
Portsweep 공격은 호스트에서 제공하는 서비스를 알기 위해 많은 포트를 한꺼번에 검사하는 행위이다. Sechole 공격은 공격자가 정상 사용자로 가장하여 시스템에 Sechole 프로그램에 의해서 시스템을 잠그는 행위이다. Ntis 공격은 NT 시스템의 파일 시스템, 접근 허가, 시스템 계정 정보, 그리고 시스템 환경에 대한 정보를 스캔하는 행위이다.

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 12개 특징 벡터를 이용하여 퍼지 멤버쉽 함수와 신경망의 이상 침입 탐지를 시뮬레이션 한다. 오차율 0.000001, 학습율 0.000001과 Epoch수를 200번 이하로 학습을 수행하였다.

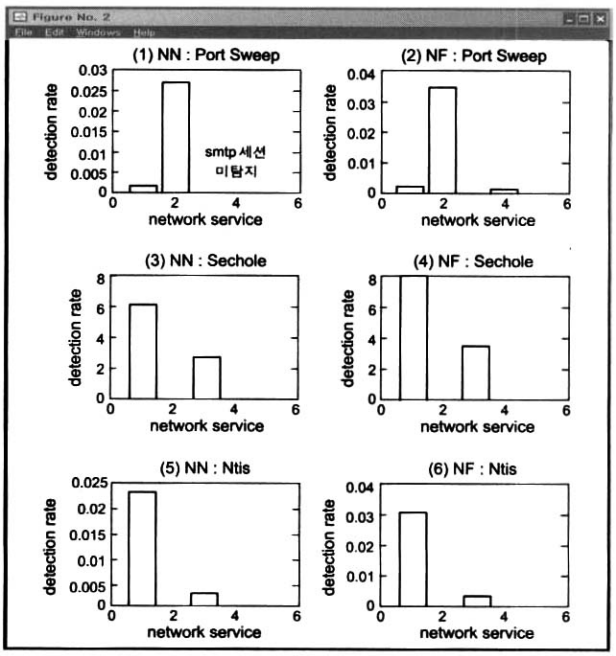
(그림 10)(1)은 정상 데이터에 대한 네트워크 서비스별 패킷과 세션을 나타내고, (2)는 침입 데이터의 패킷과 세션을 나타낸다.

(그림 11)에서는 신경망과 뉴로-퍼지에 의한 이상 침입 탐지의 결과이며, 신경망과 뉴로-퍼지의 출력값을 임계치 0.9를 기준으로 나타낸 것이다. (그림 11)(1), (3), (5)번은 신경망에 의한 침입 탐지 결과이며, (2), (4), (6)은 뉴로-퍼지 의한 이상 침입 탐지 결과이다. 신경망과 뉴로-퍼지를 이용한 이상 침입 탐지 시스템들의 성능 차이는 단지 탐지 값의 스케일링에 국한되었으나, (그림 11)(1)과 (2)를 비교하였을 때, 신경망에 의한 이상 침입 탐지에서는 SMTP 세션에 의한 미탐지 되었으나, 뉴로-퍼지에 의한 이상 침입 탐지에서는 데이터가 값의 스케일링에 의해 SMTP 세션의 미탐지 데이터가 탐지가 되었다.

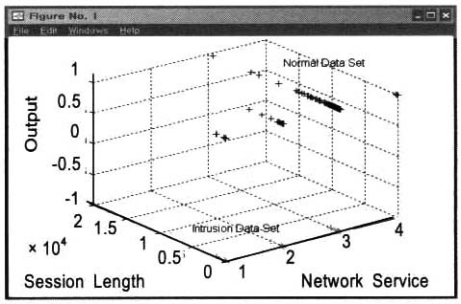
SSH, FTP와 FTP-Data, Telnet, SMTP 서비스에 대한 정상 데이터 량에 비해 상대적으로 비정상 데이터인 Portsweep 공격, Sechole 공격, Ntis 공격 데이터는 매우 적다. 시뮬레이션에 사용된 정상 데이터는 아웃라이어와 같은 특이한 데이터가 존재하지 않아 신경망 학습에 은닉계층의 뉴런 수가 12개면 충분했으며, False Positve는 발생하지 않았다.



(그림 10) 정상과 침입의 세션 분포



(그림 11) 신경망과 뉴로-퍼지에 의한 침입 탐지 결과



(그림 12) 정상 데이터와 침입 데이터의 분포

(그림 12)는 뉴로-퍼지 이상 침입 탐지 시스템에 의해 침입이 탐지된 결과를 보여준다. x축은 네트워크 서비스를 나타내며, y축은 세션의 길이를 나타낸다. z축은 뉴로-퍼지에 의해서 탐지한 정상과 침입의 출력값 분포를 나타낸다. 출력값이 1에 근접하면 정상이고, -1에 근접하면 이상 침입으로 간주한다. 뉴로-퍼지의 출력값이 -1인 경우에는 침입으로 분류하여 침입 패턴 DB로 구축한다. 구축된 침입 패턴 DB는 다음의 학습 정보로 사용하여 보다 효율적인 탐지가 가능하도록 제공한다.

5. 결 론

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 지도 학습 신경망을 이용한 이상 침입 탐지 시스템에 불확실성을 해결하기 위한 방법인 퍼지의 멤버쉽 함수를 적용하여 이상 침입 탐지 성능을 향상시키고자 한다. 뉴로-퍼지를 이용한 이상 침입 탐지는 신경망 학습의 전달함수를 불확실성을 해결하기 위한 퍼지의 멤버쉽 함수로 수정하여 네트워크 기반의 이상 침입 탐지를 수행한다. 네트워크 기반의 이상 탐지를 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 이용한 퍼지 멤버쉽 함수를 생성하고, 정상 행위의 퍼지 멤버십 함수를 지도 학습인 역전파 신경망에 적용하여 이상 침입 탐지를 수행한다. 불확실성을 처리하는 퍼지 이론을 이상 침입 탐지영역에 도입하여 적용함으로써 이상 침입 탐지의 성능을 향상시키며, 오용 탐지의 한계를 극복하기 위한 변형된 침입을 탐지하고자 하였다.

시뮬레이션에 사용한 데이터는 DARPA 2000년 NT 데이터 집합을 이용하여 네트워크 서비스의 정상 프로파일의 서비스, 패킷 개수, 플래그 그리고 TCP 세션 등의 12개 특징 벡터를 이용하여 뉴로-퍼지를 이용한 이상 침입 탐지를 수행한다. 그리고 신경망 학습의 오차율 0.000001, 학습율 0.0000001과 Epoch수를 200번 이하로 학습을 수행하였다. 정상 행위 프로파일을 이용하여 Portsweep, Sechole 그리고 Ntis 공격에 대해 신경망을 이용한 이상 침입 탐지와 뉴로-퍼지를 이용한 이상 침입 탐지를 수행하였다. 신경망을 이용한 이상 침입 탐지에서는 Portsweep 공격은 67%, Sechole 공격은 100% 그리고 Ntis 공격은 100% 탐지하였다. 그리고 뉴로-퍼지를 이용한 이상 침입 탐지에서는 Portsweep, Sechole 그리고 Ntis 공격 모두 100% 탐지하였다.

신경망을 이용한 이상 침입 탐지에서는 Portsweep 공격의 FTP와 SSH 세션은 탐지하였으나, SMTP 세션을 탐지하지 못하였다. SMTP의 정상 프로파일에 의한 학습량이 많고, 세션 정보의 완벽한 학습이 이루어지지 않아 Portsweep 공격의 SMTP 세션을 탐지하지 못하였다. 그러나 뉴로-퍼지를 이용한 이상 침입 탐지에서는 신경망에 의한 이상 침입 탐지와 비슷하였지만, 이상 침입 탐지값이 스케일링되어서 출력되었으며, SMTP 세션에 의해 미탐지 값이 스케일링되어서 탐지되었다. 지도학습 기반의 침입 탐지 시스템에 뉴로-퍼지기법을 적용하여 지도학습의 학습률을 증가시켜서 탐지 성능을 향상시켰다.

향후 뉴로-퍼지 기법에 의한 False Positive에 대한 부가적인 연구가 필요하다. 그리고 이상 침입 탐지를 위한 기존 알고리즘에 비지도 학습 알고리즘을 적용하여 새로운 침입과 알려지지 않은 침입을 탐지하기 위한 연구를 하고자 한다.

참 고 문 헌

[1] D. Barbara, N. Wu and S. Jajodia, "Detecting novel network intrusions using bayes estimators," In Proc. SIAM Intl. Conf. Data Mining, 2001.

[2] D. Anderson, T. Lunt, H. Javitz, A. Tamaru and A. Valdes, "Detecting unusual program behavior using the statistical component of the next-generation intrusion detection expert system(nides)," In Technical Report SRI-CSL-95-06, SRI, 1995.

[3] Silicon Defence. Spade. In http://www.silicondefense.com /software/spice/, 2001.

[4] Matthew V. Mahoney and Philip K. Chan, "Learning Nonstationary Models of Normal Network Traffic for Detecting Novel Attacks," 2002.

[5] Leonid Portnoy, "Intrusion detection with unlabeled data using clustering," Undergraduate Thesis, Columbia University, 2000.

[6] Jack Marin, Daniel Ragsdale and John Shurdu, "A Hybrid Approach to the Profile Creation and Intrusion Detection," Proceedings of DARPA Information Survivability Conference and Exposition, IEEE, 2001.

[7] Nong Ye and Xiangyang Li, "A Scalable Clustering Technique for Intrusion Signature Recognition," Proceedings of 2001 IEEE Workshop on Information Assurance and Security, 2001.

[8] Wenke Lee, Salvatore J. Stolfo, Philip K. Chan, Eleazar Eskin, Wei Fan, Matthew Miller, Shlomo Hershkop and Junxin Zhang, "Real Time Data Mining - based Intrusion Detection," IEEE, 2001.

[9] Dorothy E. Denning, "An Intrusion-Detection Model," IEEE Transaction on Software Engineering, Vol.SE-13, No.2, pp.222-232, February, 1987.

[10] Stephanie Forrest, Steven A. Hofmeyr, Anil Somayaji, Thomas A. Longstaff, "A Sense of Self for Unix Processes," In Proceedings of the 1996 IEEE Symposium on Security and Privacy, IEEE Computer Society Press, pp.120-128, 1996.

[11] 박봉구, 한상언, 차병래, "컴퓨터를 활용한 이산수학", 교우사, pp.231-242, 2003.

[12] LiMin Fu, "Neural Networks in Computer Intelligence," McGraw-Hill, Inc., 1994.

[13] http://www.ll.mit.edu/IST/ideval/data/data_index.html.

[14] Hofmann, A., Schmitz, C. and Sick, B., "Intrusion Detection in Computer Networks with Neural and Fuzzy Classifiers," Springer LNCS, pp.316-324, 2003.

[15] Zheng Zhang, Jun Li, C.N. Manikopoulos, Jay Jorgenson, Jose Ucles, "HIDE : a Hierarchical Network Intrusion Detection System Using Statistical Preprocessing and Neural Network Classification," Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, 2001.

[16] Srinivas Mukkamala, Guadalupe Janoski, Andrew Sung, "Intrusion Detection : Support Vector Machines and Neural Networks," New Mexico Institute of Mining and Technology.

[17] Susan M. Bridges, Rayford B. Vaughn, "INTRUSION DETECTION VIA FUZZY DATA MINING," Accepted for Presentation at The Twelfth Annual Canadian Information Technology Security Symposium pp.19-23, June, 2000.

[18] Jack Marin, Daniel Ragsdale and John Surdu, "A Hybrid Approach to the Profile Creation and Intrusion Detection," Information Technology and Operations Center, United States Military Academy.

[19] Jonatan Gomez and Dipankar Dasgupta, "Evolving Fuzzy Classifiers for Intrusion Detection," Proceedings of the 2002 IEEE Workshop on Information Assurance, 2002.

[20] James A. Freeman and David M. Skapura, "Neural Networks : Algorithms, Applications and Programming Techniques," pp.89-123, Addison Wesley, 1992.

[21] Martin T. Hagan, Howard B. Demuth, MA가 Beale, "Neural Network Design," PWS publishing Company, 1996.

차 병 래

e-mail : chabr69@empal.com

1995년 호남대학교 수학과 학사

1997년 호남대학교 대학원 컴퓨터공학과 석사

2004년 목포대학교 대학원 컴퓨터공학과 박사

1997년~현재 : 여수대학교 전산학과 시간강사

관심분야 : 정보보호, 컴퓨터 네트워크, 신경망 etc.