情報保護學會論文誌
第15券 第2號, 2005. 4

사운덱스 알고리즘을 적용한 신경망과 뉴로-퍼지 기법의 호스트 이상 탐지

차 병 래,[1†] 김 형 종,[1] 박 봉 구,[1] 조 혁 현[2]
[1]호남대학교, [2]여수대학교

Host Anomaly Detection of Neural Networks and Neuro-Fuzzy Techniques with Soundex Algorithm

Byung-Rae Cha,[1†] Hyung-Jong Kim,[1] Bong-Gu Park,[1] Hyug-Hyun Cho[2]
[1]Honam University, [2]Yosu University

요 약

본 논문에서는 시스템 호출을 이용하여 이상 침입 탐지 시스템의 성능을 향상시키기 위해, 특징 선택과 가변 길이 데이터를 고정 길이 학습 패턴으로 변환 생성하는 문제를 해결하기 위한 사운덱스 알고리즘을 적용한 신경망 학습을 통하여 이상 침입 탐지의 연구를 하고자 한다. 즉, 가변 길이의 순차적인 시스템 호출 데이터를 사운덱스 알고리즘에 의한 고정 길이의 행위 패턴을 생성하여 역전파 알고리즘과 퍼지 멤버쉽 함수에 의해 신경망 학습을 수행하였다. 역전파 신경망과 뉴로-퍼지 기법을 UNM의 Sendmail Data Set을 이용하여 시스템 호출의 이상침입 탐지에 적용하여 시간과 공간 복잡도 그리고 MDL 측면에서 성능을 검증하였다.

ABSTRACT

To improve the anomaly IDS using system calls, this study focuses on Neural Networks Learning using the Soundex algorithm which is designed to change feature selection and variable length data into a fixed length learning pattern. That is, by changing variable length sequential system call data into a fixed length behavior pattern using the Soundex algorithm, this study conducted neural networks learning by using a backpropagation algorithm with fuzzy membership function. The back-propagation neural networks and Neuro-Fuzzy technique are applied for anomaly intrusion detection of system calls using Sendmail Data of UNM to demonstrate its aspect of he complexity of time, space and MDL performance.

Keywords : *Host anomaly detection, Neural Networks, Neuro-Fuzzy, and Soundex algorithm*

Ⅰ. 서 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. 보안 위협에 대한 능동적인 대처 및 침입 이후에 동일하거나 유사한 유형의 사건 발생에 대해 실시간 대응 할 수 있는 방법이 중요하게 되

접수일 : 2004년 8월 16일 ; 채택일 : 2005년 3월 15일
* 본 연구는 호남대학교 교내 학술연구조성비의 지원에 의하여 수행되었음.
† 주저자, 교신저자 : chabr@honam.ac.kr

었다. 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 시스템의 사용을 실시간 모니터링하여 침입을 탐지하는 보안 시스템이다. 침입 탐지 기법은 크게 이상 침입 탐지 기법과 오용 침입 탐지 기법으로 나눌 수 있다. 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 시간과 비용이 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.

초기 침입탐지 시스템들은 이미 알려진 공격에 대한 징후를 수동으로 전문가가 인코딩하여 침입 여부를 판단하였다. 그러나 수동적인 방법에 의한 규칙 생성 및 확장은 매우 어려운 일이며, 그 효율성이 매우 떨어지는 방법이다. 이러한 문제를 해결하기 위하여 인공지능, 기계학습 및 데이터마이닝 기법 등을 침입탐지 기법으로 이용하기 시작하였다.

호스트 기반의 이상 침입 탐지 기법은 열거형 방법, 빈도 기반 방법, 데이터마이닝 접근 방법 그리고 유한 상태 기계 방법으로 분류할 수 있다. 열거형 순차 방법은 정상 행위를 경험적으로 추적하여 알려지지 않은 패턴을 모니터링하여 이상 탐지한다. 빈도 기반의 방법은 다양한 이벤트의 빈도 분포를 기준으로 하여 침입을 탐지하며, 데이터마이닝 접근 방법은 정상 행위 데이터로부터 발생하는 공통의 원소로부터 특징을 추출하고, 규칙 집합으로 기술함으로서 침입 탐지가 가능하도록 한다. 또한 유한 상태 기계 방법은 기계 학습 기법으로 프로그램을 추적하여 인식하는 유한 상태 기계를 구축하여 이상 침입을 탐지하는 방법이다.[1]

지도학습에 기반을 둔 침입탐지 시스템은 학습과 침입탐지 과정이 구분되어있다. 따라서, 침입탐지를 위해서는 학습과정이 반드시 필요하며 시스템의 안정적 성능을 얻기까지 많은 비용이 들며, 학습을 위해 많은 양의 데이터가 필요하다. 이러한 방대한 학습 데이터의 수집 및 분류는 매우 어려운 일이며, 학습 데이터의 질에 의해 침입 탐지 시스템의 성능이 크게 좌우된다. 현재 침입탐지에 사용되고 있는 많은 알고리즘은 방대한 데이터 처리 및 점증적 학습을 동시에 수행하기가 매우 어렵다. 따라서, 실시간 침입탐지를 위한 온라인 시스템의 구축이 어렵다. 또한 학습된 데이터 이외의 침입 유형에 대한 탐지 및 침입 유형에 대한 정보 제공도 어렵다.[2-5]

이상 침입 탐지 시스템의 최근 연구 경향은 병렬 시스템에 의한 실시간 이상 행위 탐지에 대한 연구[6], 호스트와 네트워크의 감사 데이터를 통합 및 상관관계 패턴을 이용한 침입 탐지에 대한 연구[7] 그리고 개발된 침입 탐지 시스템을 평가하기 위한 평가 기준 및 항목을 설정하고 이를 근거로 퍼지적분에 의한 평가를 수행하는 연구[8] 등이 이루어지고 있다.

본 논문에서는 지도학습 신경망 기반의 침입탐지 시스템에서 학습에 사용되는 가변 길이의 시스템 호출 데이터의 문제점을 해결하기 위하여 사운덱스 알고리즘을 적용하고자 한다. 사운덱스 알고리즘에 의해서 가변 길이의 데이터를 고정 길이의 패턴 변환으로 간결한 학습 알고리즘과 학습을 위한 복잡도 줄일 수 있다. 호스트 기반의 이상 침입을 탐지하기 위해서는 먼저 프로세스 아이디에 의한 세션을 구분하고, 시스템 호출을 이용하여 호스트의 행위 패턴을 사운덱스 알고리즘에 의해 가변 길이를 고정 길이 패턴으로 변환하여 생성한다. 또한 정상적인 행위 패턴을 이용하여 정상 행위를 프로파일링하고, 역전파 신경망과 뉴로-퍼지에 의해서 비정상적 행위를 탐지하고자 한다.

본 논문의 2장은 관련 연구로써 사운덱스 알고리즘에 대한 연구를 기술한다. 3장은 이상 침입 탐지를 위한 사운덱스 알고리즘을 적용한 호스트 기반의 시스템 호출 행위 프로파일을 구축과 이상 침입 탐지를 위한 역전파 신경망과 뉴로-퍼지를 설계한다. 4장은 UNM의 Sendmail 데이터를 사운덱스 알고리즘으로 고정 길이 데이터로 변환하여 역전파 신경망과 뉴로-퍼지를 적용한 시뮬레이션을 수행하여 탐지결과를 비교 분석한다. 그리고 5장에서는 결론 및 향후 연구방향을 기술한다.

II. 관련 연구

항공 회사와 같이 전화로 고객 업무를 처리하는 경우 발음이 부정확하거나 다른 고객의 이름을 검색하는 경우가 종종 발생한다. 이런 문제가 아니더라도 데이터베이스 안에 저장된 고객의 수가 많은 경우에는 고객의 이름을 하나씩 확인해 보는 선형 검색 방

법은 지나치게 많은 시간을 필요로 한다. 이러한 문제점을 해결하기 위해서 Margaret K. Odell과 Robert C. Russell이 사운덱스 알고리즘을 개발하였다. 사운덱스 알고리즘은 미군의 개인 기록부터 인구 통계 조사까지 사용되었다. 또한 여러 가지 소프트웨어의 철자 확인기 엔진 속에도 포함되어 활용되고 있으며, Ancestor Search 웹사이트에서도 사운덱스 알고리즘을 사용하고 있다.

사운덱스 알고리즘은 네 가지의 규칙으로 이루어진다. 규칙 1은 이름의 첫 번째 글자를 저장하고, 첫 번째 글자를 제외한 나머지 글자 중에서 a, e, i, o, u, w, y를 모두 제거한다. 규칙 2는 이름 안에 존재하는 글자들에게 다음과 같은 번호를 부여한다. {b, f, p, v : 1}, {c, g, j, k, q, s, x, z : 2}, {d, t : 3}, {l : 4}, {m, n : 5}, {r : 6}. 규칙 3은 원래 이름에서 서로 인접하여 연속으로 나타나는 글자는 맨 앞에 하나만 남기고 나머지는 제거한다. 규칙 4는 최종적인 결과물 '글자, 숫자, 숫자, 숫자'의 형태로 맞추기 위해서 숫자가 세 개 이상이면 나머지는 생략하고, 세 개 미만이면 뒤에 0을 붙여서 형태를 맞춘다.[9]

Ⅲ. 사운덱스 알고리즘과 신경망 그리고 뉴로-퍼지를 이용한 이상 탐지

시스템 호출 기반의 이상 침입 탐지에 사운덱스 알고리즘을 적용한 신경망 모델과 뉴로-퍼지 모델을 적용하여 성능을 비교를 위한 절차는 그림 1과 같이 구성한다.

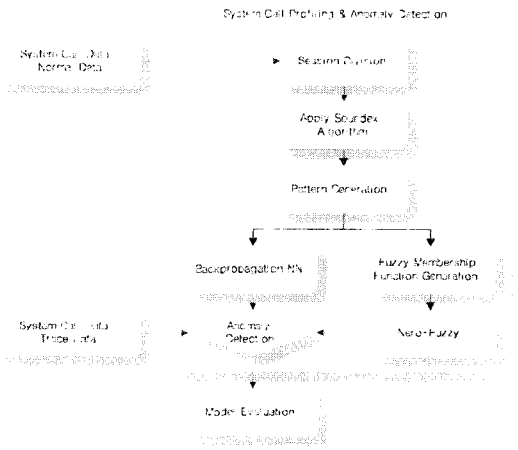


그림 1. 신경망과 뉴로-퍼지의 수행 절차

시스템 호출을 이용한 이상 침입을 탐지하기 위해서는 먼저 프로세스 아이디에 의한 세션을 구분한다. 세션은 행위를 나타내는 단위이며, 하나의 세션이 하나의 행위 패턴으로 변환된다. 가변 길이의 정상적인 시스템 호출 데이터를 이용하여 고정 길이의 정상 행위 패턴을 생성하여 정상 행위 프로파일을 구축한다. 정상 행위 패턴을 이용하여 신경망의 지도 학습을 수행하여 이상 침입 탐지를 수행한다.

정상 행위 프로파일을 구축하기 위해서는 사운덱스 알고리즘의 음성 검색을 위한 알파벳을 시스템 호출 번호로 수정하여 적용한다. 수정된 사운덱스 알고리즘에 의한 고정 길이 패턴을 생성하고, 신경망 모델과 뉴로-퍼지 모델간의 성능을 비교 분석한다.

3.1 행위 패턴 생성

호스트 기반의 침입 탐지에는 호스트의 시스템 호출 정보를 이용하여 침입을 탐지한다. 본 논문에서는 시스템 호출 정보를 이용하여 사운덱스 알고리즘에 의해 정상 행위를 고정길이 패턴으로 프로파일링하여 신경망과 뉴로-퍼지 학습에 의한 이상 침입을 탐지한다.

사운덱스 알고리즘을 이용하여 행위 패턴 생성 과정은 먼저, 객관성을 갖기 위해서 뉴 멕시코 대학(UNM)이 공개적으로 제공하는 Sun SPARC 스테이션의 패치되지 않은 SunOS 4.1.1과 4.1.4에 설치된 Sendmail에서 생성된 UNM의 Sendmail DataSets[10]을 사용하여 프로세스 아이디(PID)에 의한 호출된 시스템 호출 번호를 필터링하여 세션을 구성한다. 그리고 구성된 세션을 사운덱스 알고리즘을 이용하여 고정 길이의 행위 패턴을 생성하며 그림 2와 같이 나타낸다. 그림 2의 (b) 과정의 산출물은 그림 3에 나타낸다.

Phonetic search에 사용되는 soundex 알고리즘을 변형하여 음성 데이터 대신에 시스템 호출 정보를 이용하여 가변 길이의 세션 데이터를 고정 길이의 프로파일 패턴으로 생성한다. soundex 알고리즘에 의해 생성된 고정 길이의 패턴에는 사용된 시스템 호출 번호들과 호출된 시스템 호출 서열의 순서 정보를 갖는다. 참고로, MD4, MD5, SHA-1 등의 해쉬함수를 사용하지 않는 이유는 고정길이의 패턴을 쉽게 만들어 낼 수 있지만, 검색을 위한 임의의 정보를 내포하지 않는다. 동일한 패턴에 대해서만 같은

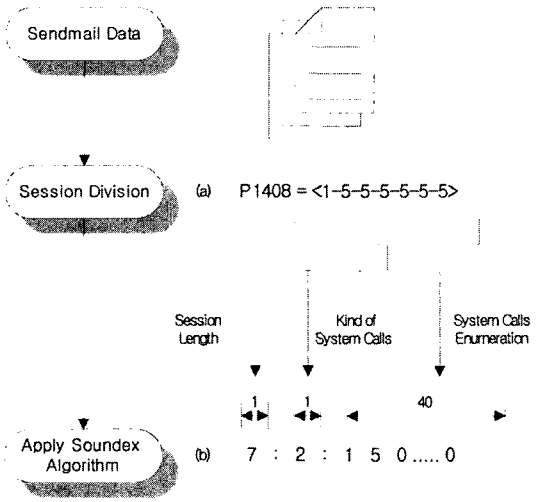


그림 2. 사운덱스 알고리즘을 이용한 행위 패턴 생성 과정

내용의 패턴을 생성하고 약간만 다르더라도 완전히 다른 패턴을 생성하기 때문에 정확한 패턴 매칭에 사용된다. 그러나 soundex 알고리즘에 의해 생성된 고정 길이의 패턴 정보에 의해서 가변 길이의 세션 서열을 호출된 시스템 호출 번호의 종류와 순서에 의한 같은 그룹으로 분류가 가능하기 때문이다.

시스템 호출 정보를 이용하여 프로세스 아이디에 의해서 세션별로 분류하면, 세션의 크기가 고정적이지 않고 가변적이다. 세션에 사용된 시스템 호출 종류가 최소 2, 최대 40 종류이며, 세션의 크기가 최소 7에서 최대 31927로 매우 가변적이다. 또한 세션에 포함된 시스템 호출이 유일하지 않고 계속적으로 반복된 형태를 취한다. 가변 길이의 데이터는 데이터 처리도 어렵지만, 신경망 학습에 학습 패턴으로 적용하기도 어렵다. 그러므로 시스템 호출의 순서를 유지하면서 중복을 제거하고 고정 길이의 패턴 변환이 필요하다.

본 논문에서는 시스템 호출 데이터로 이루어진 가변적인 세션에 수정된 사운덱스 알고리즘을 적용하여 세션 정보를 유지하면서 고정된 행위 패턴의 프로파일을 구축한다. 세션을 이루는 가변의 행위 데이터를 신경망 학습에 적용하기 위해서는 먼저, 패턴을 생성하기 위한 특징 선택이 필요하다. 본 논문에서는 3개의 특징을 선택하였다. 패턴 벡터의 선택으로는 세션의 크기, 시스템 호출의 종류, 그리고 나열로 표 1과 그림 3과 같이 특징 선택으로 생성한다.

특징 선택 중에서 나열 필드는 40개의 항목으로

표 1. 특징 선택에 의한 패턴 벡터의 구성

특징 선택	형태	내용
세션의 길이	Integer	세션을 이루는 시스템 호출의 길이
시스템 호출 종류	Integer	세션의 시스템 호출의 종류
시스템 호출의 나열	Sequential Integer	시스템 호출의 종류별 발생 순서 나열

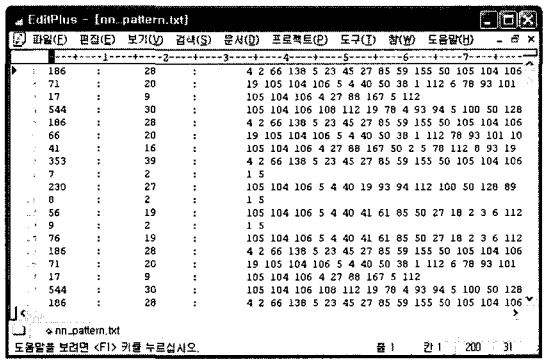


그림 3. 사운덱스 알고리즘을 이용한 패턴 벡터 생성

구성된다. 모든 행위 패턴을 대상으로 조사한 결과 시스템 호출은 182 종류이나, 행위 데이터에 사용된 시스템 호출 종류는 53 종류이었다. 세션 중에서 가장 많이 쓰인 시스템 호출의 종류는 40 종류이었다. 모든 행위 패턴들은 최대가 40이거나 이보다는 작을 것이다. 그러므로 나열 항목의 크기를 40으로 설정하였다.

표 2는 시뮬레이션에 사용된 학습 패턴에 대한 패턴의 특징 정보를 나타낸 것이다. 신경망 학습에 사용될 훈련 패턴은 정상 패턴이며, 학습 후의 검증에 사용될 추적 패턴으로 구분된다. 훈련 패턴은 다시 정상과 비정상 패턴으로 구분된다. 정상 패턴에 사용된 시스템 호출은 53 종류, 비정상 패턴은 48 종류, 그리고 테스트 패턴은 43 종류가 사용되었다. 정상패턴의 세션은 199개, 비정상 패턴의 세션은 15

표 2. 학습에 사용될 패턴 수

패턴 클래스		세션 수	패턴 벡터 수	시스템 호출의 종류	패턴 벡터 수 / 세션의 평균
훈련	정상	199	228,181	53	1,147
	침입	15	4,186	48	279
추적		10	2,569	43	257
합계		224	234,936	53	1,049

개 그리고 테스트 패턴의 세션은 10개로 구성된다. 훈련 패턴은 199개의 정상 행위 패턴을 사용하여 신경망 학습을 수행한다.

3.2 퍼지 멤버쉽 함수 생성

퍼지 논리는 퍼지 집합의 개념으로부터 시작된다. 퍼지 집합은 명확한 경계가 정의되지 않은 뚜렷하지 않은 집합이며, 멤버의 부분적인 정도를 갖는 원소를 포함한다. 퍼지 멤버쉽 함수는 입력 공간의 각 점들에 대해서 0과 1사이의 멤버쉽 값으로 사상하는 곡선으로 정의된다.

뉴로-퍼지 이상 침입 탐지에 사용될 퍼지 멤버쉽 함수는 정상 행위 패턴을 이용한다. 세션을 이루는 시스템 호출의 발생 빈도와 시스템 호출의 종류를 이용하여 다중 서열 정렬(MSA) 알고리즘[11]에 의한 클러스터링을 수행한다. 다중 서열 정렬 알고리즘에 의해서 12개의 클러스터링으로 분류되었으며, 12개의 클러스터링을 이용하여 그림 4와 같이 퍼지 멤버쉽 함수를 구축한다.

시스템 호출의 퍼지 멤버쉽 함수를 구축하기 위해서는 사용된 시스템 호출의 종류와 발생 빈도에 포커스를 맞춘다. 그 이유는 세션별로 시스템 호출 종류가 다르다는 것은 프로세스가 다른 행위를 포함하고 있다는 것을 의미한다.

시스템 호출의 종류에 의해서 퍼지 멤버쉽 함수를 생성한다. UNM의 시스템 호출 종류는 최소 2부터 최대 40 종류까지 한 세션에 포함되었다.

세션의 시스템 호출 종류에 의해서 퍼지 멤버쉽 함수는 12개로 클러스터링 되었으며, 삼각형 함수와 사다리꼴 함수로 그림 3과 같이 생성되었다. 퍼지 멤버쉽 함수의 C는 클래스의 시스템 호출 종류를 나타내며, x축은 발생 빈도를, y축은 퍼지 멤버쉽 함수값을 나타낸다. 시스템 호출에 의한 정상 행위 패턴들은 퍼지 멤버쉽 함수에 의해서 스케일링되어 학습된다.

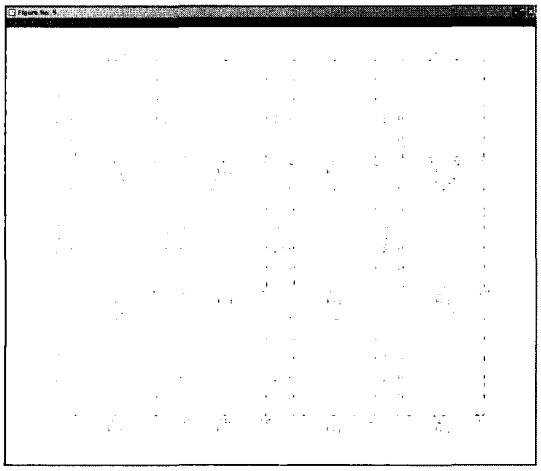


그림 4. 시스템 호출의 퍼지 멤버쉽 함수

3.3 신경망 기법의 학습

반복되는 가변길이의 시스템 호출 세션을 사운덱스 알고리즘에 의한 고정 길이 패턴의 프로파일 구축하여 단순한 패턴 매칭에 의한 이상 탐지도 가능하지만, 패턴 매칭의 단점 중의 하나인 임의의 변화에 대한 일반화를 갖추기 위하여 시스템 호출의 종류, 길이, 시스템 호출의 나열 및 퍼지 멤버쉽 함수에 의한 학습을 적용한다.

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

2 계층 역전파 신경망과 뉴로-퍼지의 소프트웨어에 의한 학습 모델을 그림 5에 나타낸다.

역전파 신경망의 학습은 입력 x와 은닉계층의 가중치 w의 곱의 합에 은닉 계층의 편의(bias) θ를 더하여 순입력으로 식 1과 같이 사용된다. 순입력에 의한 은닉계층의 전달함수의 출력 i가 식 2와 같이 계산된다. 은닉 계층의 출력을 출력 계층의 입력으로 하고, 출력 계층의 가중치의 곱의 합에 출력 계층의 편의가 더하여 출력계층의 순입력으로 식 3과 같이 사용된다. 순입력에 의한 출력 계층의 전달함

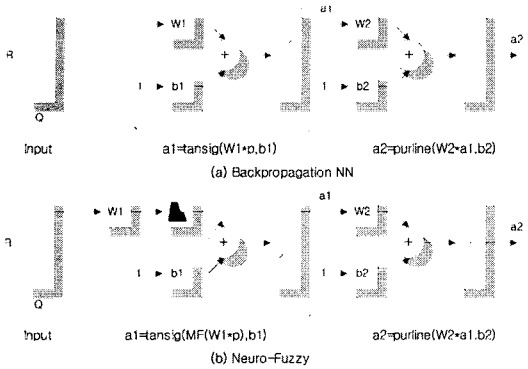


그림 5. 역전파와 뉴로-퍼지의 소프트웨어 구성도

표 3. 역전파 신경망 학습의 알고리즘

$$net^h_{pj} = \sum_{i=1}^{N} w^h_{ji} x_{pi} + \theta^h_j \quad \text{(식 1)}$$

$$i^h_p = f^h_j(net^h_{pj}) \quad \text{(식 2)}$$

$$net^o_{pk} = \sum_{j=1}^{L} w^o_{kj} i_{pj} + \theta^o_k \quad \text{(식 3)}$$

$$o_{pk} = f^o_k(net^o_{pk}) \quad \text{(식 4)}$$

$$\delta^o_{pk} = (y_{pk} - o_{pk}) f^{o'}_k(net^o_{pk}) \quad \text{(식 5)}$$

$$\delta^h_{pj} = f^{h'}_j(net^h_{pj}) \sum_k \delta^o_{pk} w^o_{kj} \quad \text{(식 6)}$$

$$w^o_{kj}(t+1) = w^o_{kj}(t) + \eta \delta^o_{pk} i_{pj} \quad \text{(식 7)}$$

$$w^h_{ji}(t+1) = w^h_{ji}(t) + \eta \delta^h_{pj} x_i \quad \text{(식 8)}$$

$$E_p = \frac{1}{2} \sum_{k=1}^{M} \delta^2_{pk} \quad \text{(식 9)}$$

수의 출력 o가 식 4와 같이 계산된다. 출력 계층과 은닉 계층의 오차는 식 5와 식 6에 의해서 계산된다. 출력 계층과 은닉 계층의 가중치의 수정은 식 7과 식 8에 의해서 계산된다. 출력 계층의 가중치의 값의 변경은 식 8과 같고 출력 계층의 오차의 변화는 식 9와 같다.[12]

그림 5의 (b)에 2계층의 뉴로-퍼지 구성을 위해서는 퍼지 멤버쉽 함수를 이용한 역전파 신경망 학습 알고리즘은 식 1을 다음의 식 10으로 변경하여 적용한다.

표 4. 퍼지 멤버쉽 함수의 적용

$$net^h_{pj} = \sum_{i=1}^{N} MF(w^h_{ji} x_{pi}) + \theta^h_j \quad \text{(식 10)}$$

일반적인 역전파 신경망은 은닉계층에서 입력과 가중치의 곱이 전달함수에 입력된다. 그러나 제안된 방법은 입력과 가중치의 곱이 퍼지 멤버쉽 함수에 의해서 스케일링되어 전달함수에 입력된다. 즉, 그림 3의 삼각형 및 사다리꼴 퍼지 멤버쉽 함수들의 합집합과 교집합 연산을 수행한 결과를 그림 5의 (b)에 적용한다. 신경망의 은닉계층에서 퍼지 멤버쉽 함수를 적용함으로써 이상 침입 탐지를 위한 학습에 보다 많은 정보를 제공할 수 있다.

본 논문에서는 42 항목의 정상 행위 패턴을 이용하여 이상 침입 탐지를 위한 역전파 학습과 뉴로-퍼지 학습을 수행한다. 학습이 완료되면 추적 데이터에 의해서 이상 침입 탐지 성능을 측정하고 신경망과 뉴로-퍼지 기법을 비교한다.

Ⅳ. 시뮬레이션과 비교 분석

신경망 학습의 이상 침입 탐지 시뮬레이션은 UNM의 Sendmail Data Set[10]을 이용하였고, 시뮬레이션 툴은 Perl과 Matlab을 이용하였다. 본 논문에서는 Perl을 이용하여 시스템 호출 데이터의 세션을 구분하고, 정상 행위, 침입 행위 그리고 추적 패턴들을 생성하였다.

4.1 역전파와 뉴로-퍼지 기법

신경망 학습을 위해 은닉 계층의 뉴런 수를 10에서 40까지 변경하여 학습율과 에러를 조사하였다. 신경망 학습의 단점인 미적합과 과적합을 벗어나기 위해서는 은닉 계층의 뉴런 수를 결정하여야 한다. 과적합은 학습에 학습 데이터이외에 잡음도 학습하는 경우를 의미하며, 미적합은 학습이 제대로 이루어지지 않은 상태를 의미한다. 그림 6과 7에서 신경망 기법과 뉴로-퍼지 기법에서 은닉계층의 뉴런이 12개이며, 428 Epoch에 의해서 역전파 학습이 이루어지고, 1776 Epoch에 의해서 뉴로-퍼지 학습이 이루어졌다.

역전파 신경망과 뉴로-퍼지의 학습을 위해 은닉계층의 뉴런의 수를 12로 설정하고 199개의 정상 행위 패턴을 학습을 수행하였다. 정상 행위 패턴은 시스템 호출 데이터를 사운덱스 알고리즘에 의해 42개 항목의 학습 패턴으로 생성하였고, 신경망 학습의 오차율 0.01, 학습율 0.2와 Epoch수를 5000번 이하로 학습을 수행하였다. 그림 8과 9는 학습된 역전파 신경망과 뉴로-퍼지에 의한 침입 데이터와 추적 데이

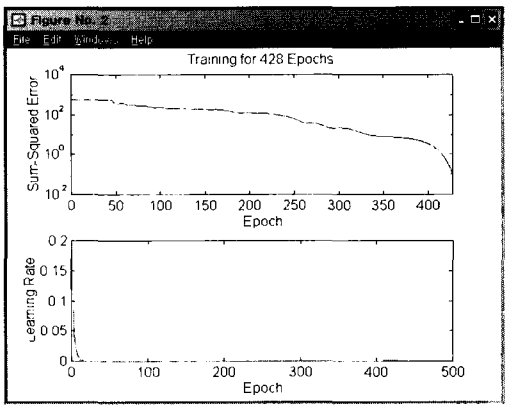


그림 6. 뉴런이 12인 신경망 학습

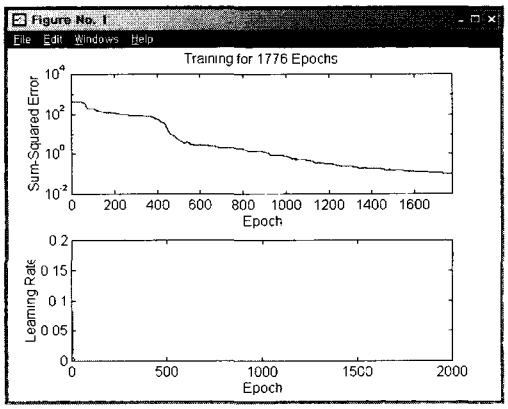


그림 7. 뉴런이 12인 뉴로-퍼지 학습

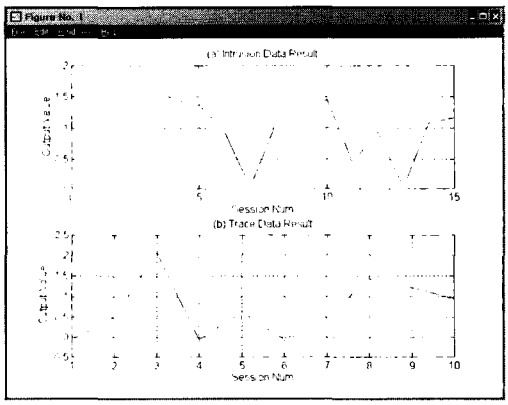


그림 8. Intrusion와 Trace 데이터의 신경망 출력값

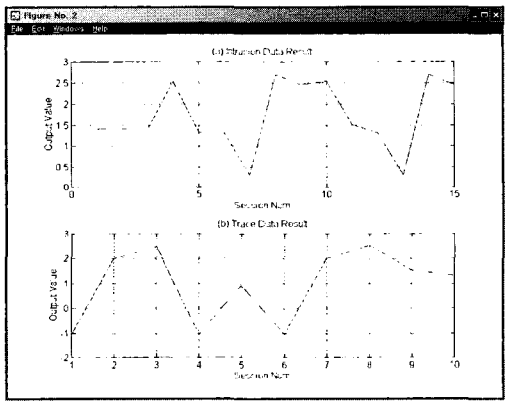


그림 9. Intrusion와 Trace 데이터의 뉴로-퍼지 출력값

터를 입력하여 이상 침입을 탐지한 결과이다. 역전파 신경망과 뉴로-퍼지에 의한 탐지 결과는 추적 데이터의 10개 세션 중에서 9개의 세션을 탐지하여 탐지율 90%를 보였다.

4.2 비교 분석

UNM의 Sendmail 데몬의 시스템 호출 데이터 집합에 대해 사운덱스 알고리즘을 이용한 신경망 기법들의 이상 탐지를 시뮬레이션한다. 시스템 호출 데이터를 사운덱스 알고리즘에 의한 42개 항목의 학습 패턴으로 변환하고, 신경망 학습의 오차율 0.01, 학습율 0.2와 Epoch수를 5000번 이하로 학습을 수행하였고, 이상 행위 탐지를 수행하여 표 5와 같이 결과를 비교 분석하였다.

MDL(Minimum Description Length)[13]은 에러 손실 $L(D|H)$와 복잡도 손실 $L(H)$로 구성된다. MDL은 작은 값을 갖는 모델이 효율적인 모델이 된다. MDL의 복잡도 손실 측면에서 보면, 원 데이터와 사운덱스 알고리즘을 사용하여 패턴을 생성하였을 경우, 패턴의 복잡도가 106분의 1로 축소되며, 중복을 제거한 경우는 470분의 1로 축소되었다. 신경망 기법의 학습을 위한 학습 패턴량 측면에서도 사운덱스 알고리즘을 적용하고 중복을 제거하면 4.9분의 1로 축소되었다.

역전파 신경망과 뉴로-퍼지 모델에 의한 이상 침입 탐지 결과는 90%의 동일한 결과를 보였다. 두 모델간의 에러 손실 측면인 이상 침입 탐지율은 같지만, 복잡도 손실 측면에서는 뉴로-퍼지 모델이 학습을 위한 Epoch 수가 역전파 신경망에 비해서 6배나 많았다.

역전파 신경망 모델은 이상 탐지 성능을 같은 수준을 유지하면서 절대적으로 학습을 위한 시간 복잡도와 공간 복잡도 측면에서 우수하였다. 역전파 신경망과 뉴로-퍼지 모델은 90%의 동일한 탐지율을 보였으며, 역전파 신경망보다 뉴로-퍼지 모델이 많은

표 5. 역전파 신경망과 뉴로-퍼지의 비교분석

항목			역전파	뉴로-퍼지
원본 데이터		세션 수	199	
		데이터량	2.35MB	
사운덱스 알고리즘 적용	중복	세션 수	199	
		데이터량	22KB	
	중복 제거	세션 수	41	
		데이터량	5KB	
학습 Epoch 수			428	1776
탐지율			9/10	9/10

학습을 필요로 하였다. 그러나 뉴로-퍼지 모델은 역전파 신경망 모델보다도 정상과 이상을 구분하기 쉽도록 스케일링된 출력값을 생성하였다.

추가적으로 UNM의 ftp, lpr등과 같은 다른 data set 등의 데이터를 혼합하여 사운덱스 알고리즘에 의한 고정 길이 패턴을 생성하여 학습과 탐지를 수행하였으나 탐지 성능이 매우 저조하였다. 신경망의 은닉계층의 뉴런수 결정의 어려움과 가중치 변화에 의한 학습이 이루어지지 않았다.

V. 결론 및 향후 연구 방향

본 논문에서는 기계학습 기법인 신경망 학습을 이용한 이상 침입 탐지 시스템에 사용될 가변길이 데이터 문제점을 해결하기 위하여 사운덱스 알고리즘을 적용하였다. 사운덱스 알고리즘에 의한 가변 길이의 시스템 호출 데이터를 고정 길이 패턴으로 변환으로 신경망의 학습 알고리즘이 간결해지고 침입 탐지를 위한 학습에 공간과 시간 복잡도를 해결하였다. 호스트 기반의 이상 침입을 탐지하기 위해서는 먼저 세션을 구분하고, 호스트의 행위 패턴을 사운덱스 알고리즘에 의해 가변 길이 데이터를 고정 길이 패턴으로 변환하여 생성한다. 정상적인 행위 패턴을 지도학습 기법인 역전파 신경망을 이용하여 정상 행위를 학습하여 이상 행위를 탐지하였다. 학습에 사용될 가변 길이 데이터 처리의 어려움을 해결하여 학습 알고리즘이 간결하고, 학습을 위한 공간과 시간 복잡도를 줄이는 효과를 가져와 이상 침입 탐지의 성능을 향상시켰다.

시뮬레이션에 사용한 데이터는 UNM의 Sendmail Data Sets을 이용하여 호스트의 Sendmail 데몬의 정상 행위를 세션의 길이, 시스템 호출의 종류, 그리고 사용된 시스템 호출을 나열하는 3개 특징 선택을 하여 42 항목의 패턴 벡터를 생성하여 역전파 학습과 경쟁 학습을 이상 침입 탐지를 수행한다. 그리고 신경망 학습의 오차율 0.1, 학습율 0.2와 Epoch수를 5000번 이하로 학습을 수행하였다.

역전파 신경망과 뉴로-퍼지 모델은 MDL의 에러 손실측면에서 탐지율 90%로 동일하였다. 그리고 학습 알고리즘 수행을 위한 시간과 공간 복잡도 측면에서는 역전파 신경망 모델이 뉴로-퍼지 모델보다 우수하였다. 그러나 뉴로-퍼지 모델은 역전파 신경망 모델보다 많은 학습이 필요하지만, 스케일링된 출력에 의해서 정상과 이상의 구분이 명확하였다.

향후 연구 과제로 UNM의 ftp, lpr등과 같은 다른 data set에 대해 각각의 모델로 전환하여 각각의 모델마다 신경망의 가중치를 다르게 적용하는 방향으로 연구를 진행할 계획이다.

참 고 문 헌

[1] Christina Warrender, Stephanie Forrest, Barak Pearlmutter, "Detecting Intrusion Using System Calls : Alternative Data Models", In 1999 IEEE Symposium on Security and Privacy, IEEE Computer Society, pp. 133-145, 1999.

[2] L. Portnoy, E. Eskin, S. Stolfo, "Intrusion detection with unlabeled data using clustering", In ACM Workshop on Data Mining Applied to Security, 2001.

[3] 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, pp.69-76, 2001.

[4] Nong Ye, and Xiangyang Li, "A Scalable Clustering Technique for Intrusion Signature Recognition", Proceedings of 2001 IEEE Workshop on Information Assurance and Security, pp. 1-4, 2001.

[5] 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", Proceedings of DISCEX II. June 2001.

[6] 유은진, 전문석, "비정상적인 컴퓨터 행위 방지를 위한 실시간 침입 탐지 병렬 시스템에 관한 연구", 통신정보보호학회지 제5권 제2호, 1995년 6월.

[7] 황현욱, 김민수, 노봉남, "감사로그 상관관계를 통한 호스트기반의 침입탐지시스템", 정보보호학회논문지, 제13권 제3호, 2003년 6월.

[8] 김미혜, "퍼지적분을 이용한 침입탐지시스템 평가방법", 정보보호학회논문지, 제14권 제2호, 2004년 2월.

[9] http://www.archives.gov/research_room/genealogy/census/soundex.html

[10] http://cs.unm.edu/~immsec/data/synthsm.html.

[11] Marco Pagni, "Introduction to Patterns, Profiles and Hidden Markov Models", Swiss Institute of Bioinformatics(SIB), August 30, 2002.

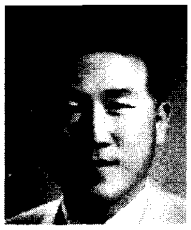
[12] James A. Freeman and David M. Skapura, "Neural Networks : Algorithms, Applications, and Programming Techniques", p89-123, Addison Wesley, 1992.

[13] Christopher M. Bishop, "Neural Networks for Pattern Recognition", Oxford Press, pp.429-433, 1995.

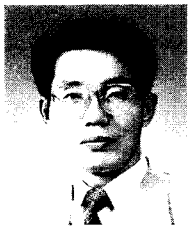
〈著者紹介〉

차 병 래 (Byung-Rae Cha) 정회원
1995년 2월: 호남대학교 수학과 학사
1997년 2월: 호남대학교 컴퓨터공학과 석사
2004년 2월: 목포대학교 컴퓨터공학과 박사
2005년 3월~현재: 호남대학교 컴퓨터공학과 전임강사
〈관심분야〉 정보보안, 신경망, 네트워크 등
e-mail: chabr@honam.ac.kr

김 형 종 (Hyoung-Jong Kim) 정회원
1995년 2월: 조선대학교 전자공학과 학사
1997년 2월: 조선대학교 전자공학과 석사
2000년 2월: 조선대학교 전자공학과 박사
2005년 3월~현재: 호남대학교 전파이동통신공학과 전임강사
〈관심분야〉 이동통신, 인터넷보안, 신호처리
e-mail: joeun777@honam.ac.kr



박 봉 구 (Bong-Goo Park) 정회원
1973년 2월: 공주사범대학교 수학과 학사
1982년 2월: 원광대학교 수학과 석사
1987년 2월: 조선대학교 수학과 박사
1984년 3월~현재: 호남대학교 정보통신공학과 정교수
〈관심분야〉 정보보안
e-mail: bgpark@honam.ac.kr



조 혁 현 (Hyug-Hyun Cho) 정회원
1984년 2월: 홍익대학교 전자계산학과 학사
1989년 2월: 전남대학교 전산통계학과 석사
1997년 2월: 전남대학교 전산통계학과 박사과정수료
1989년 3월~현재: 여수대학교 정보기술학부 교수
〈관심분야〉 데이터베이스, 정보보안, 시스템 및 네트워크 보안 등
e-mail: hhcho@yosu.ac.kr