역전파 알고리즘 기반의 침입 패턴 분석☆

An Analysis of Intrusion Pattern Based on Backpropagation Algorithm

우 종 우* 김 상 영**
Chong-Woo Woo Sang-Young Kim

요 약

침입 탐지시스템 (Intrusion Detection System: IDS)은 기존의 수동적인 탐지 기능에서 벗어나, 보다 다양한 형태와 방법론으로 연구되고 있다. 특히, 최근에는 대용량의 시스템 감사 데이터를 빠르게 처리하고 변형된 형태의 공격에 대비할 수 있는 내구력을 가진 형태의 방법론들이 요구되고 있으며, 이러한 조건을 만족하는 데이터마이닝이나 신경망을 이용한 침입 탐지 시스템에 대한 연구가 활발해 지고 있다. 본 논문에서는 우선, 최근의 다양한 형태의 침입경향들을 분석하고, 보다 효과적인 침입탐지를 위한 방안으로 신경망 기반의 역전파 알고리즘을 이용한 침입 탐지 시스템을 설계·구현 하였다. 본 연구의 시스템은 비정상행위 탐지(Anomaly Detection)와 오용탐지 (Misuse Detection)의 두 가지 방법론을 모두 수용하는 방법론을 사용하였으며, 신뢰성있는 KDD Cup '99의 데이터를 통한 침입패턴의 분석 및 실험을 수행 하였다. 또한 객체지향적인 네트워크 설계를 통하여 역전파 알고리즘 이외의 다른 알고리즘도 쉽게 적용이 가능하도록 하였다.

Abstract

The main function of the Intrusion Detection System (IDS) used to be more or less passive detection of the intrusion evidences, but recently it is developed with more diverse types and methodologies. Especially, it is required that the IDS should process large system audit data fast enough. Therefore the data mining or neural net algorithm is being focused on, since they could satisfy those situations. In this study, we first surveyed and analyzed the several recent intrusion trends and types. And then we designed and implemented an IDS using back-propagation algorithm of the neural net, which could provide more effective solution. The distinctive feature of our study could be stated as follows. First, we designed the system that allows both the Anomaly dection and the Misuse detection. Second, we carried out the intrusion analysis experiment by using the reliable KDD Cup '99 data, which would provide us similar results compared to the real data. Finally, we designed the system based on the object-oriented concept, which could adapt to the other algorithms easily.

Keyword : Intrusion Detection System, Back-propagation, KDD Cup '99

1. 서 론

인터넷의 보급으로 인한 부정적인 측면은 시스템에 대한 악의적인 침입행위라 할 수 있으며, 침입 행위의 형태 및 방법은 나날이 다양해져 가고 있다. 이러한 침입에 의한 피해를 최소화 하기 위한 기술로 침입탐지 시스템 (Intrusion Detection System: IDS)들이 연구되었으며, 그 목적은 시스템이나 네트워크의 다양한 감사 데이터를 이용하여 침입 행위를 탐지 하고 시스템 관리자나 시스템이 이에 대한 조치를 취할 수 있게 하는 데 있다.

IDS가 침입을 탐지하는 기법은 대표적으로 정상적인 행위를 모델링하여 이에 위반하는 행위를 침입으로 간주하는 비정상행위 탐지(Anomaly Detection)와 알려진 침입의 형태를 모델화하여 이러한 모델과 일치하는 행위를 침입으로 간주하는 오용 탐지 (Misuse Detection)가 있다. 그러나 비정상 행위 탐지는 정상적인 행위에 대한 모델링이 어렵다는 단점을 가지고, 오용 탐지는 모델링된 침입 행위만을 탐지하며 이에서 변형되거나 알려지지 않은 형태의 공격에 취약하다는

* 종신회원 : 국민대학교 컴퓨터학부 교수
cwwoo@kookmin.ac.kr(제 1저자)
** 준 회 원 : 시그널 스펙트럼 재직
reborn@neozone.net(공동저자)
☆ 본 논문은 2004학년도 국민대학교 교내연구비 지원을 받아 수행되었음.

단점을 가진다. 최근에는 이러한 단점들을 보완하려는 연구가 진행되고 있다[1]. 또한 근래에는 시스템의 감사 데이터의 양이 급속하게 증가 하여 대용량의 자료를 빠르게 처리하고 변형된 형태의 공격에 내구력을 가진 형태의 방법론이 요구되고 있다. 따라서 이러한 조건을 만족하는 데이터마이닝이나 신경망을 이용한 침입 탐지 시스템에 대한 연구가 활발해 지고 있다[2].

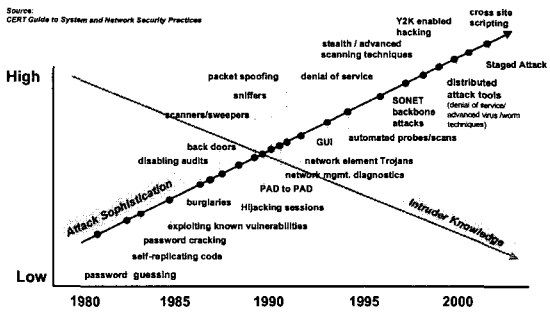
본 논문에서는 이와 같은 대용량의 감사 데이터 처리와 변형된 형태의 공격에 내구력을 가지기 위해 신경망을 이용한 침입 탐지 시스템을 설계·구현하였다. 본 연구의 시스템은 비정상 탐지와 오용 탐지를 모두 수용할 수 있게 설계 되었으며, 신경망 자체의 변형 감내 (Transformation Tolerance) 적인 성질을 이용하여 변형된 형태의 공격에도 대응할 수 있게 하였다. 또한 신뢰성있는 데이터를 통한 시뮬레이션을 수행함으로써 실제 데이터에 대한 적응력을 높였다. 이 시스템에서 사용된 신경망 학습 알고리즘은 역전파 알고리즘으로써 비선형적인 문제에 대해 효과적인 분류가 가능한 특징을 가진다.

본 논문의 구성은 다음과 같다. 2장 관련 연구에서는 최근 침입의 경향, 침입탐지 시스템의 구조 및 실험에 사용할 KDD Cup '99 데이터에 관하여 기술하였다. 3장에서는 시스템의 특성을 중심으로 시스템의 구조 및 구성을 기술하였다. 4장에서는 구현된 시스템에서 감사데이터의 처리 및 탐지를 설명하고, 5장에서 결론 및 연구의 문제점등을 기술하였다.

2. 관련 연구

2.1 침입 행위의 경향

침입이라는 것은 일반적으로 컴퓨터의 보안 정책(Securty Policy)을 위반하는 행위를 의미한다. 이러한 침입의 형태를 분석하고 이에 대한 적절한 대안들을 제시하기 위해서는 현재의 침입의 경향을 파악하는 것이 우선 시 되어야한다 [3].



〈그림 1〉 공격의 정교화와 공격자의 기술 지식의 관계

그림 1에서와 같이 초기의 공격자들의 경우, 개인이 가진 전문적인 지식을 통한 공격이 이루어졌으나 정교함은 낮은 수준이었다. 그러나 이후의 공격들은 보다 정교하고 지능적으로 발전되고 있음을 알 수 있다. 이러한 최근의 공격의 특징을 요약하면 다음과 같다[4].

- 자동화된 도구의 사용으로 무경험자도 쉽게 침입 행위를 할 수 있다.
- 공격자들은 보다 진보된 기술로 정교한 공격 툴을 개발하고 있다.
- 취약성의 발견은 매년 2배씩 증가하여 패치등 유지보수가 어려워진 반면, 이를 역으로 이용하는 공격은 증가하고 있다.
- 방화벽의 투과성이 증대되고 있다. 예를 들면, IPP(the Internet Printing Protocol)와 같은 프로토콜은 이러한 방화벽의 설정을 무시한 채 통과할 수 있다.
- 기타 기반구조 공격(Infra-structure Attack)의 증가와 비대칭 위협의 증가 등이다.

따라서 보다 적극적으로 침입행위를 탐지하고 대응하기위한 방안들이 제기되고 있다.

2.2 침입 탐지 방법론 (Intrusion Detection Methodology)

침입 탐지를 위한 다양한 방법론들이 제시되고

있으나 일반적으로 2가지 방법론이 통용되고 있다. 첫째는 시스템의 알려진 취약점이나 공격과 관련된 패턴 정보를 가지고 해당 정보와 일치되는 것을 침입으로 간주하는 오용 탐지 (Misuse Detection)이고, 둘째는 정상적인 패턴의 정보를 저장하고 이와 다른 형태의 패턴이 들어왔을 경우 이를 침입으로 간주하는 비정상 행위 탐지 (Anomaly Detection)이다[5-6].

비정상 탐지 기법에서 가장 중요한 요소는 정상적인 행위에 대한 모델링이므로 대부분의 연구가 이러한 정상적인 패턴을 모델링하기 위한 기법에 집중하여 이루어지고 있다. 비정상 탐지 모델에서는 호스트 시스템에서의 감사 데이터를 기반으로 정상적인 행위에 대한 시스템 프로파일을 작성하고 이를 주기적으로 갱신하는 과정을 거친다. 이러한 시스템 프로파일을 기반으로 해당 프로파일에 위배되는 패턴을 인식하였을 경우 공격을 알리게 된다. 이와 같은 비정상 행위 탐지 기법들로는 대표적으로 통계적인 모델(Statistical Models), 면역 시스템 접근방법, 프로토콜 검증, 파일검사, 오염검사등의 기법들이 있다.

오용탐지는 시스템을 악용하려는 비정상적인 행위에 대한 모델링을 기반으로 이루어진다. 오용 탐지를 위해서는 먼저 침입에 관련된 정보들을 수집하기 위해서 시스템의 취약점이나 공격, 위협, 공격 도구 등을 관찰하는 과정이 요구 된다. 이렇게 관찰된 정보들을 기반으로 탐지를 위한 패턴이나 시그너처가 정의되고 정의된 공격의 특징이나 이벤트 데이터의 패턴이 일치할 경우 침입을 탐지 하게 된다. 이와 같은 오용탐지 모델링 기법에는 전문가 시스템, 표현매칭, 상태전이 분석 Colored Pertri Net, 유전자 알고리즘, 침입알람(burglar alarm)등이 활용되고 있다.

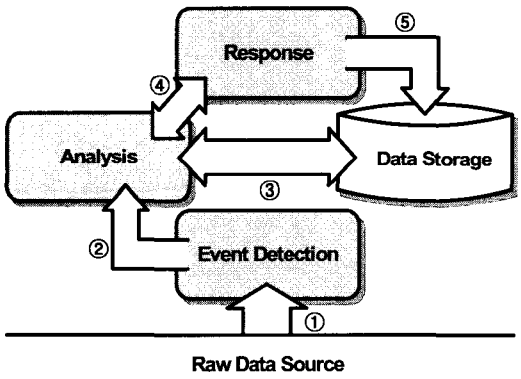
이와 같은 다양한 방법론 가운데 신경망은 다음과 같은 구별되는 장점을 가지고 있다. 첫째, 특별한 규칙을 가지고 있지 않으므로 명령을 내리기 어려운 상황에서 유용하게 사용될 수 있다. 둘째, 학습 능력을 가지므로 특정 패턴을 인식하거나 특정 데이터에 대한 학습을 기반으로 한 문제 해결에 용이하다. 셋째, 네트워크 일부가 문제를 가질 경우 전체적으로 미치는 영향이 적다. 마지막으로 입출력 노드에 이산형, 연속형 변수 사용이 가능하며 기법을 적용할 수 있는 영역이 넓다. 이러한 특징을 기반으로 본 논문에서는 다양한 신경망 알고리즘 중에서 널리 사용되어 검증되어 있고 교사학습 기반의 알고리즘인 역전파 알고리즘을 이용하여 침입 패턴을 분류하였다.

2.3 침입 탐지 시스템 (Intrusion Detection System)

침입탐지 시스템의 절차는 대부분 다음과 같다[7-9]. 첫째, 호스트나 네트워크에서 발생하는 이벤트에 대해서 감사 자료를 수집하고, 둘째, 이러한 감사 자료에서 침입을 탐지 하는 데 필요한 자료만을 선별하여 특정 이벤트만을 분석의 입력으로 사용한다. 셋째, 축약된 감사 이벤트를 기반으로 침입 요소들을 탐지하고, 넷째, 침입이 탐지되면 해당 침입에 대한 조치를 위해서 시스템 자체적인 방어 수단을 동작하거나 시스템 관리자에게 통보한다. 침입 탐지 시스템은 ISO/IEC에 의해서 표준화가 진행되고 있으나 국제 표준 형식이 아닌 기술 문서 형식으로 작성되고 있으며, 2001년 10월 현재로 DTR (Draft Technical Report)이 발표 되었다. 이러한 표준화의 목적은 침입 탐지에 관한 공통적인 개념의 기초확립과 시스템 관리자들에게 자신의 환경에서 침입 탐지 시스템을 사용하는데 도움을 주고자 하는 것이다[10-12].

그림 2는 ISO/IEC에서 제시한 일반적인 침입 탐지 시스템을 도식화 한 것이다. 원시 데이터 소스는 시스템에서 얻어진 감사 데이터를 의미하며 ①과 같이 이벤트 탐지 모듈에 들어가게 된다. 이벤트 탐지에서는 원시 데이터 소스를 정제하는 역할을 수행하며 원시 데이터에서 침입과 관련된 정보만을 선별하

는 기능을 한다. 이렇게 정제된 데이터는 ②와 같이 분석 모듈에 전달되고 분석 모듈에서는 이러한 이벤트들을 ③과 같이 데이터 저장소와 상호 작용하며 침입 여부를 분석 하게 된다. 데이터 저장소에는 탐지된 사건의 결과와 분석에 필요한 데이터, 알려진 침입에 대한 프로파일, 세부적인 원시 데이터들이 저장되며 이것을 보호할 수 있는 정책 하에서 관리되어야 한다. 분석결과 침입을 탐지 하게 되면 ④와 같이 대응 모듈에 전달되어 적절한 조치를 취할 수 있게 하며 이러한 일련의 결과들은 ⑤를 통해서 다시 데이터 저장소에 저장된다. 대부분의 침입 탐지 시스템이 위와 같은 기본적인 모델을 기반으로 동작하며 자신만의 방법론을 통해 원시 데이터를 정제하고 분석, 대응하는 과정을 거치게 된다[13].



〈그림 2〉 일반적인 침입 탐지 시스템 모델

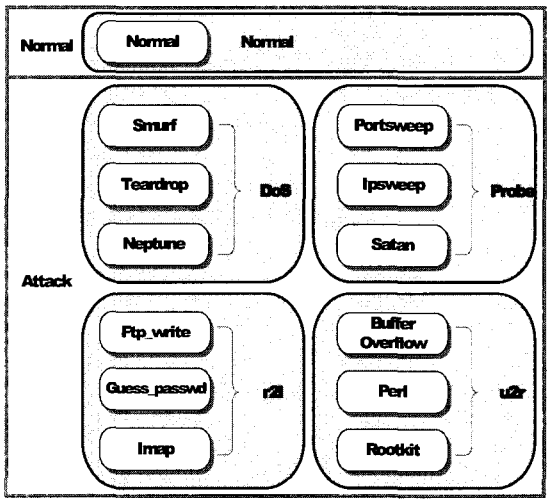
2.4 KDD Cup '99 데이터

본 논문에서는 침입 패턴을 시뮬레이션 하기 위한 데이터로써 KDD Cup 99의 감사 데이터를 사용하였다.

KDD Cup '99 데이터는1998년에 DARPA에서 침입 탐지를 시뮬레이션 하기 위해 제공된 것이며, 미 공군에서 사용되는 지역 네트워크에서의 TCP/IP dump 데이터로 구성되었다. 이 데이터는 각 TCP/IP 연결에 대해서 41개의 필드를 가지고 있으며, 크게 4가지 형태의 공격 유형을 가지며 세부적으로 13가지의 공격으로 이루어져 있다. 이 데이터에서의 공격 형태는 크게 4가지 형태로 나누어 볼 수 있다.

- DoS : 분산 서비스 공격 (Denial of Service)
- r2l : 원격에서의 비인가 접근 공격
- u2r : 슈퍼 유저 권한으로의 비인가 접근 공격
- probing : 시스템의 취약점에 대한 감시 또는 스캔 공격

훈련 집합은 743MByte 크기의 약 5,000,000개의 레코드로 이루어져 있다. 이 중에서 본 논문에서는 실험의 용이성을 고려하여 이 중에서 10%정도를 훈련 데이터로 사용하며, 이것은 75Mbyte의 크기로 총 494,021개의 레코드를 포함한다. 이러한 10%의 데이터는 19.69%가 정상 패턴을 가지고 나머지 영역에서는 다양한 공격의 형태를 명시하는 레이블이 존재한다. 시험 집합은 전체가 430Mbyte 크기이고, 훈련 데이터와 같이 10%인 1.4Mbyte만을 실험 데이터로 사용하였으며, 총 311,029개의 레코드로 이루어진다.



〈그림 3〉 KDD Cup 데이터에서의 공격 유형 분류

시험 집합에는 특정한 공격의 형태를 명시하는 라

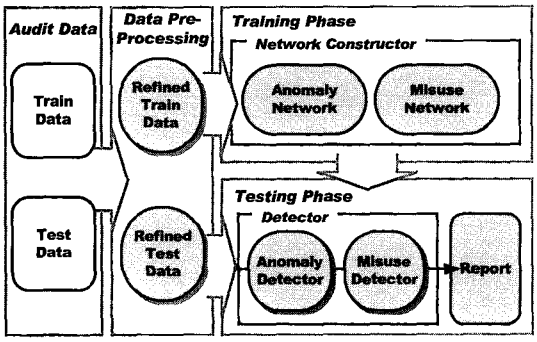
벨을 가지고 있지 않으며, 시험 집합의 분류 결과를 기준으로 침입 탐지 시스템의 오 분류도 및 정확성을 판단할 수 있게 된다. 그림 3은 KDD Cup 데이터에서 나타나는 공격 유형을 분류한 것이다. KDD Cup 데이터의 레코드 형태는 네트워크 시스템 로그에서 볼 수 있는 연속형 데이터 (예: duration, src_bytes, dst_bytes 등) 와 이산형 데이터 (예: protoc ol_type, service, flag 등)를 가지고 있다.

3. 시스템 설계

본 연구의 시스템은 비정상탐지와 오용탐지를 병행하도록 하기 위해서 다음 몇 가지 주요관점을 가지고 설계하였다. 첫째, 본 연구에서는 KDD Cup '99 데이터로 시뮬레이션 함으로써 비 정상 탐지와 오용탐지를 병행할 수 있도록 설계하였다. 둘째, 입력데이터와 출력데이터를 다음과 같이 구성하였다. 즉, 비 정상탐지의 경우 공격일경우 1에 가까운 출력을 정상패턴일 경우 0에 가까운 출력을 나타내도록 구성하였다. 오용탐지의 경우는 교사학습시의 출력노드의 비교를 위해 각 공격의 형태를 나타내는 바이너리 코드를 사용하였다. 마지막으로 신경망에서 학습 효율을 높이기 위해 부가적으로 관성 알고리즘을 사용하였다[15-16].

3.1 시스템 구조

그림 4는 본 논문에서 제안한 침입 탐지 시스템의 구조를 도식화 한 것이다. 이 시스템은 다음과 같이 크게 3가지의 구성부로 나뉘어져 있다. 첫째는 데이터를 네트워크 학습에 맞게 정제하기 위한 데이터 전처리부(Data Pre-Processing)이고, 둘째는 탐지를 위한 엔진에 해당하는 네트워크를 구성하기 위한 훈련부(Training Phase), 마지막은 테스트를 위한 침입 데이터를 가지고 침입을 여부를 탐지하기 위한 시험부(Testing Phase)로 구성된다.

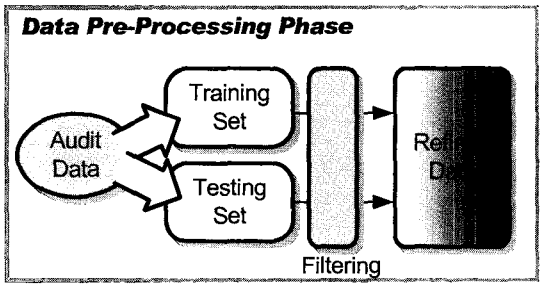


〈그림 4〉 시스템 구조

3.2 시스템 구성

시스템의 구성은 크게 데이터 전처리부와 네트워크 생성부, 침입 탐지부의 세 가지 영역으로 나누어진다.

3.2.1 데이터 전처리부 (Data Pre-Processing Phase)



〈그림 5〉 데이터 전처리부 구조

감사 데이터(Audit Data)에 해당하는 것은 KDD Cup '99에서 제공되는 텍스트 기반의 원시 데이터이다. 이 데이터는 데이터 자체에 몇몇의 잘못된 형식의 데이터를 포함하고 있기 때문에, 데이터 전처리부에서는 이러한 오류들을 제거하고 42개의 데이터 베이스 필드로써 저장하는 과정을 거친다.[그림 5] 이 데이터 중에서 침입에 가장 영향을 미치는 데이터 형태로는 표 1과 같은 6가지를 선택하였으며 이 시스템에서는 이러한 영역의 감사 데이터를 기반으로 훈련과 시험이 이루어진다.

〈표 1〉 시스템에 사용된 감사 데이터 필드

Field	Description	Type
Duration	연결 시간	연속형
Protocol Type	프로토콜의 형태	이산형
Service	목적지에서의 네트워크 서비스	이산형
Flag	연결의 정상이나 에러 여부	이산형
Src_bytes	소스에서 목적지로 향하는 데이터 양	연속형
Dst_bytes	목적지에서 소스로 향하는 데이터 양	연속형

이렇게 선택된 데이터는 네트워크로의 입력을 위해서 다시 한번 변환 과정을 거치게 되는데, 출력의 경우 네트워크의 형태에 따라 데이터를 변환해 주어야 할 필요성을 가지고 있다. 특히, 오용탐지에서의 출력 데이터를 정의하기 위해서 표 2와 같이 바이너리 코드 형태로 인코딩하였다.

〈표 2〉 오용 탐지에서의 출력 데이터 이진 변환 코드

Attack	Binary Code	Attack Type
Smurf	0000	DoS
Teardrop	0001	
Neptune	0010	
portsweep	0011	Probe
Ipsweep	0100	
Satan	0101	
ftp_write	0110	r2l
guess_passwd	0111	
Imap	1000	
buffer_overflow	1001	u2r
Perl	1010	
Rootkit	1011	

KDD Cup '99 데이터에서 훈련 데이터 집합에 포함된 공격의 유형은 총 14가지이므로 출력 노드가 바이너리 출력을 내는 것을 고려하여 4개의 출력 노드로 하나의 공격을 표현하였다. 바이너리 코드에서 가장 앞자리는 첫번째 출력 노드의 출력 값을 의미하고 마지막 자리는 4번째 출력 노드의 출력 값을 의미한다. KDD Cup '99 훈련 데이터에서 명시된 공격의 형태는 12가지이지만, 시험 데이터에서는 이와는 다른 형태의 공격의 형태 또한 명시 되어 있다. 이것은 시스템의 예측 가능성을 판별하기 위한 목적이며, 이 시스템에서도 14개의 코드중 남은 두 코드를 이용하여 다른 형태의 공격이 이루어 졌음을 유추할 수 있다.

3.2.2 네트워크 생성부 (Network Construction Phase)

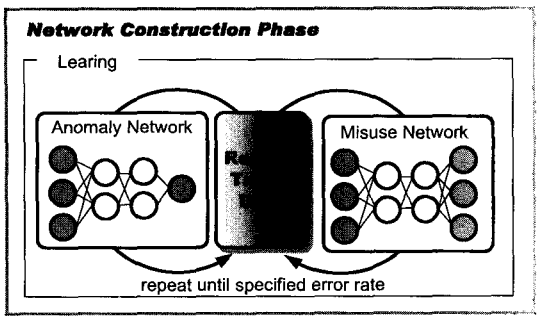
네트워크 생성부는 침입 탐지 시스템의 엔진에 해당하는 네트워크들을 생성하는 역할을 수행한다. 신경망의 네트워크 구성은 네트워크 위상의 설계와 설계된 위상에서의 학습의 두 가지 부분으로 나누어 생각할 수 있고, 설계 및 학습에 있어 다음과 같이 몇 가지 고려사항들이 있다.

(1) 네트워크 생성부의 동작

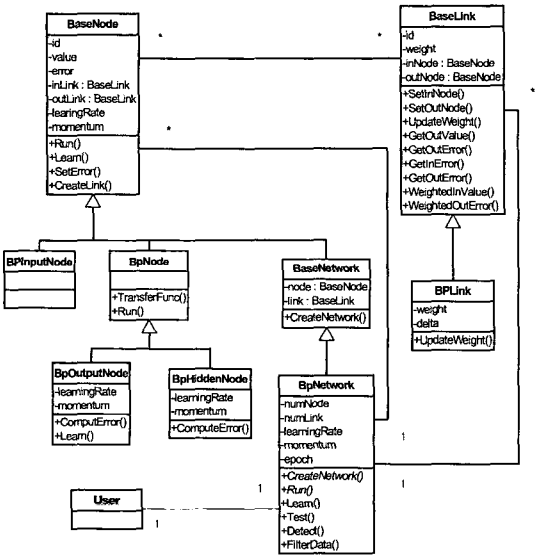
네트워크 생성부의 주요 역할은 비정상 탐지와 오용 탐지를 위한 역전파 네트워크를 학습 하는데 있다. 사용자의 입력을 기반으로 비정상 탐지와 오용 탐지 네트워크가 생성되고, 데이터 전처리부를 통해서 생성된 훈련 데이터를 통해서 학습을 수행하게 된다. 이러한 학습은 전체 입력에 대해서 지정된 에러율 이하의 오차가 나올 경우 종료 하게 된다.[그림 6]

(2) 네트워크의 구성

역전파 알고리즘에서, 입력 노드와 출력 노드의 개수는 주어지는 데이터에 따라서 결정될 수 있으나 은닉 노드 개수는 비선형 분리를 위한 하이퍼 플레인(Hyper Plane)의 개수와 관계가 있다. 분류하고자 하는 패턴의 분포가 복잡할수록 더 많은 하이퍼플레인이 필요하며 너무 많은 수의 하이퍼플레인을 나누게 되면 과적합(overfitting)의 문제점 때문에 패턴의 분포에 맞는 은닉층 노드 개수 설정이 중요하다. 본 논문에서는 데이터 집합에 대한 패턴의 분포를 알 수 없으므로 반복적인 실험으로 적절한 노드의 수를 구성 하였다.



〈그림 6〉 네트워크 생성부의 동작



〈그림 7〉 네트워크 구성에 대한 클래스 다이어그램

네트워크의 구성은 각 노드와 객체를 그림 7과 같이 객체지향적으로 설계하였다. 네트워크의 모든 노드는 BaseNode() 클래스를 상속 받으며, 모든 링크는 BaseLink() 클래스를 상속 받아 구현된다. 각 노드는 다수의 입력 링크와 출력 링크 객체를 소유하고 네트워크를 통한 노드의 출력 값을 가진다. 각 링크는 하나의 입력 노드와 출력 노드를 가지고 있으며, 가중치값을 가진다. 네트워크를 구성하는 클래스도 BaseNode() 클래스를 상속받아서 구성되며, 이러한 구성은 다수의 노드의 연결과 동일한 방법으로 다수의 네트워크 연결을 가능하게 한다. 네트워크는 사용자로부터 입력 받은 네트워크 내부의 계층수, 각 계층별 노드수, 학습율, 관성 값을 기준으로 네트워크 위상을 구성하게 된다. 이러한 객체 지향적인 구조는 다양한 변형이 가능하며 다양한 형태의 신경망 알고리즘을 네트워크 생성에 이용할 수 있다.

(3) 네트워크에서의 학습

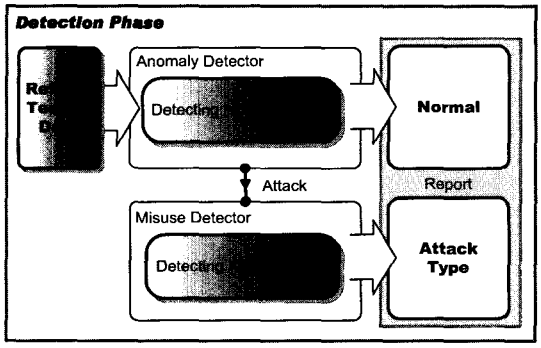
네트워크를 구성한 후 각 네트워크는 역전파 알고리즘을 이용하여 훈련 과정을 거치게 되며, 아래와 같은 훈련 절차를 가진다.

① 입력층에 데이터 패턴을 위치한다.
② 은닉층에서는 입력층의 데이터를 받아 가중치를 곱하여 출력층으로 전파한다.
③ 출력층 노드들은 모든 입력 값을 종합하여 출력값을 결정한다.
④ 출력 노드에서의 기대치와 출력값과의 차를 구하여 출력층에서의 δ 값을 구한다.
⑤ 출력층에서의 δ 값을 입력된 모든 링크에대해 가중치를 곱하여 은닉층으로 역전파 한다.
⑥ ⑤에서의 δ 값을 기준으로 출력층으로 향하는 링크에 대한 가중치를 조절한다.
⑦ ⑤에서 받은 모든 δ 값을 더함으로 인해 해당 은닉층 노드의 에러값을 구할 수 있다.
⑧ ⑦에서의 에러값을 가지고 은닉층 노드에서의 δ 를 구한다.
⑨ ⑧에서 구한 δ 값으로 입력층에 이르기 까지 모든 은닉층에 대해 ⑤~⑦의 과정을 반복 수행한다.
⑩ ①~⑨까지의 과정이 학습에서의 한번의 반복이 된다. 모든 입력에 대한 에러가 지정된 경계값(threshold)에 보다 작을 때까지 이러한 과정을 반복하게 되면 학습이 종료된다.

이렇게 비 정상 탐지와 오용 탐지에 대해 학습된 네트워크를 연결하여 최종적으로 탐지 시스템의 엔진을 구성하게 된다.

3.2.3 침입 탐지부 (Detection Phase)

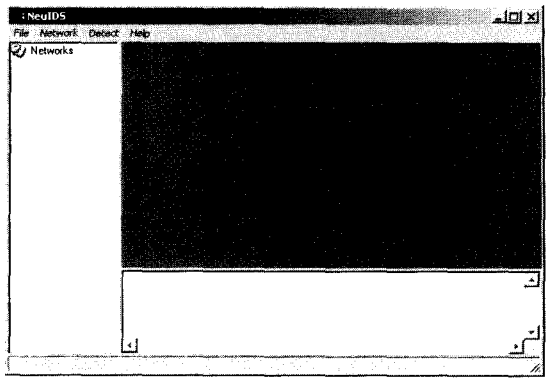
침입 탐지부는 네트워크 생성부에서 생성된 비정상 탐지 네트워크와 오용 탐지 네트워크를 연결하여 구성하고, 데이터 전처리부에서 정제된 데이터 중 시험 데이터를 가지고 탐지 시뮬레이션을 수행한다. 시험 데이터는 먼저 비정상 탐지 네트워크를 통해 테스트가 이루어 지며 여기서 공격과 정상 여부를 판단하게 된다. 만약 정상인 패턴이 입력 되었을 경우 이를 인식하여 정상 패턴 카운트가 증가 한다. 반대로 공격 패턴임을 탐지 하게 되면 해당 패턴은 오용 탐지 네트워크로 보내어 진다. 오용 탐지 네트워크에서는 공격에 해당 하는 패턴이 어떠한 공격 유형에 해당하는지 분석하고 최종적으로 발견된 공격 유형을 제시하게 된다.[그림 8]



〈그림 8〉 침입탐지부 동작

4. 시스템 구현

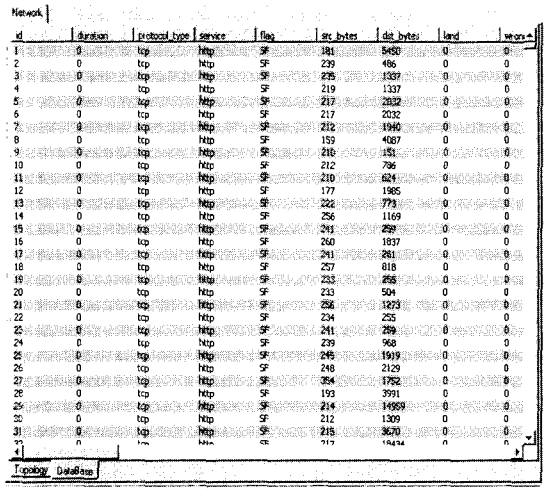
시스템의 구현은 설계에서와 마찬가지로 3가지 구성부로 나누어 질 수 있으며 각 구성부를 중심으로 실제 구현된 시스템을 기반으로 설명 한다. 그림 9는 시스템을 처음 시작시의 초기화면이다. 왼쪽에는 트리 컨트롤을 두어 새롭게 생성하거나 확장된 네트워크의 구조를 나타내었고, 하단에는 텍스트 컨트롤을 두어 시스템에서 발생하는 이벤트에 대한 로그를 출력한다. 이외의 모든 시스템의 출력은 메인 윈도우와 팝업창을 통해서 이루어진다.



〈그림 9〉 시스템 초기 화면

4.1 감사 데이터 처리

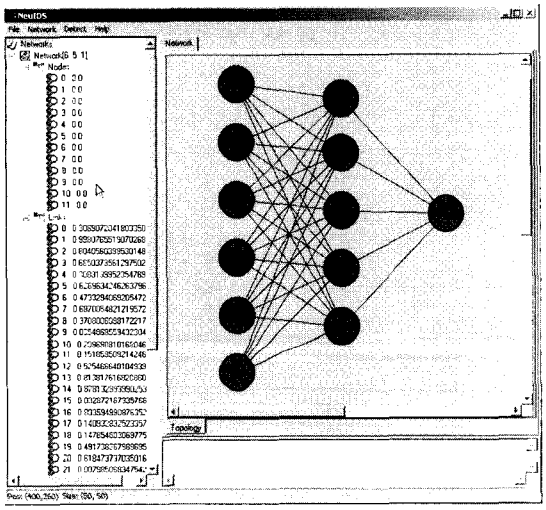
감사 데이터는 시스템과는 별개의 전처리 과정을 거쳐서 데이터베이스에 저장된다. 본 시스템은 학습을 위해 훈련 데이터 집합을, 탐지 시뮬레이션을 위해서 시험 데이터 집합을 가지고 있다. 두 가지 데이터는 모두 동일한 41개의 필드를 가지고 있으며, 방대한 데이터에 대한 용이한 접근과 분석을 위해서 질의를 통해 데이터베이스에 접근하여 결과를 확인할 수 있게 하였다. 아래 그림 10은 시스템에서 전체 훈련 데이터의 집합을 호출한 결과이다.



〈그림 10〉 훈련 데이터 집합

4.2 네트워크의 생성 및 탐지

네트워크를 생성하기 위해서는 생성하려는 네트워크의 계층 수와 각 계층마다의 노드수, 학습율, 관성계수를 입력으로 받는다. 이렇게 네트워크에 대한 구성 정보를 입력하면 그림 11과 같이 해당되는 네트워크가 생성 된다.

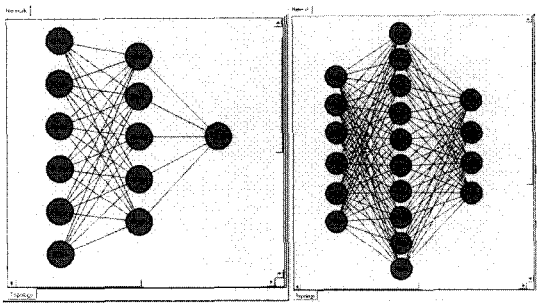


〈그림 11〉 네트워크의 생성

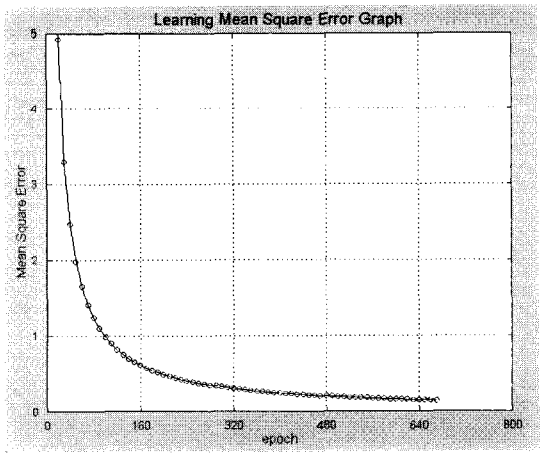
이 시스템은 비정상 탐지와 오용탐지 두 가지의 네트워크 위상이 필요하므로 그림 12와 같이 위상을 구성하였다. 두개의 네트워크 모두 6개의 입력을 사용하고 비 정상 탐지의 경우 5개의 은닉층 노드를 오용탐지의 경우 10개의 은닉층 노드를 사용하였다. 이렇게 은닉층 노드의 차이를 두는 이유는 비정상 탐지의 경우 정상과 공격 두 가지 출력에 대한 분류만을 하는데 비해서 오용탐지는 12가지의 분류를 필요로 하므로 더 많은 하이퍼플레인이 요구되기 때문이다.

출력 노드는 비정상 탐지의 경우 공격과 정상만을 구별하기 위하여 한 개의 노드를 사용하였고, 오용탐지의 경우는 12개의 공격 형태를 분류하기 위해 4개의 출력 노드를 사용하였다. 생성된 네트워크의 가중치 값은 모두 0~1사이의 임의의 수가 설정 되어있다.

다음에 수행해야 할 과정은 생성된 네트워크를 학습시키는 것이다. 네트워크의 학습은 훈련 데이터를 가지고 수행한다. 모든 학습이 종료 되면 학습이 종료되었다는 메시지와 함께 학습을 위해 반복된 횟수와 에러값을 나타낸다.



〈그림 12〉 비 정상 탐지와 오용탐지의 네트워크 위상



〈그림 14〉 학습에서의 Mean Square Error 그래프

본 논문에서는 학습이 진행되는 과정에서 매 10번의 반복마다 반복 회수와 에러값을 저장하여 학습이 종료 되었을 때 그래프 형태로 제시하였다[그림 13]. 그래프의 X축은 반복 횟수를 Y축은 MSE(Mean Square Error)를 의미한다. 이 그래프는 1000개의 훈련 데이터를 기반으로 660번의 반복 학습 동안의 에러값의 변화를 보여준다. 이 그래프를 통한 학습의 특징은 반복회수가 거듭될수록 0으로 수렴하는 로그

그래프의 성격을 가지고 있다는 것이다. 이는 특정 회수 이상의 반복 후에는 학습을 반복해도 더 이상의 성능 향상이 이루어지지 않음을 의미하며 이 시점에서 학습을 종료해야 한다. 이렇게 학습된 네트워크를 기반으로 탐지 시스템의 엔진이 구성되며 시험 데이터를 가지고 탐지 시뮬레이션 과정을 수행하게 된다. 탐지 시뮬레이션 과정은 구성된 네트워크의 입력으로 시험데이터를 제공함으로써 수행되며, 최종적으로 발생한 에러율을 가지고 네트워크의 성능을 측정할 수 있다.

5. 결 론

본 논문에서는 다양한 최근의 침입에 대한 경향을 분석하고 이를 해결하기 위한 여러 가지 방안들을 살펴보았다. 그리고 이러한 문제를 해결하기 위한 방안으로써 신경망 기반의 침입 탐지 시스템을 설계·구현하였다. 본 연구의 특징은 다음과 같이 요약해 볼 수 있다.

첫째, 신뢰성 있는 시뮬레이션 데이터를 통한 침입 패턴의 분석 및 실험을 수행하였다. KDD Cup '99의 데이터를 통한 실험 결과는 실생활의 감사 데이터를 처리할 때와 비슷한 결과를 산출할 것을 예상할 수 있다. 둘째, 대표적인 두 가지 형태의 침입 탐지 방법론을 모두 수용하는 모델을 구현하였다. 비정상 행위 탐지와 오용 탐지에서의 단점들을 해결하고 장점들을 부각시키기 위해서 두 가지 방법론을 병용하는 방법을 사용하였다. 셋째, 과적합을 방지하기 위하여 모든 공격 유형에 대해 통합적인 네트워크를 구성하였으며, 훈련 데이터와 시험 데이터를 신경망의 입출력에 맞게 가공하였다. 또한 객체 지향적인 네트워크 설계를 통해서 본 논문에서 사용된 역전파 알고리즘 이외의 알고리즘도 쉽게 적용이 가능하며, 데이터 전처리부의 교체를 통한 실제 데이터 처리도 가능하다.

현재 신경망을 적용한 침입 탐지 시스템에 대한 연구가 활발하게 진행되고 있지만 신경망 자체가 가지고 있는 내부의 처리 과정을 설명할 수 없다는 단점은 보다 효율적인 네트워크 구성에 있어서 어려움을 주고 있다. 설계에서 잠시 언급하였던 노드의 개수와 계층에 따른 수학적인 분석들이 보다 현실화 될 때 신경망을 이용한 침입 탐지 시스템의 활용도는 더욱 높아 질 수 있을 것이다.

본 논문에서 사용된 데이터는 상당히 많은 양을 가지고 있어 모든 데이터에 대한 학습에 있어서 상당히 많은 시간이 요구되었다. 최적의 결과를 내는 네트워크를 발견하기 위해서는 다양한 네트워크를 구성하고 반복적인 실험이 요구되지만 시간상의 제약으로 인해 향후 연구 과제로 남겨 두기로 한다. 마지막으로 신뢰적인 데이터를 사용하기는 했지만 실제 네트워크 데이터와는 다른 점들이 존재하므로 네트워크 상의 원형의 감사 데이터들을 수집/가공 하여 시스템에 적용하기 위한 연구가 요구된다.

참 고 문 헌

[1] Canegie Mellon Software Engineering Institute CERT Coordination Center. available at http://www.cert.org.

[2] Korea Computer Emergency Response Team Coordination Center. available at http://www.certcc.or.kr.

[3] CERT Coordination Center, "Overview of Attack Trends," Carnegie Mellonn University, April 8, 2002. http://www.cert.org/archive/pdf/attack_trends.pdf.

[4] Julia H. Allen, "CERT Guide to System and Network Security Practices," Addison-Wesley, 2001.

[5] J. Ghosh, Wanken, F. Charron, "Detecting anomalous and unknown intrusions against programs," In Proceedings of the 1998.

[6] J. Cannady, "Artificial Neural Networks for Misuse Detection," Proceedings of the 1998 National Information Systems Security Conference (NISSC'98), 1998.

[7] G. Giacinto, F. Roli , "Intrusion Detection in Computer Networks by Multiple Classifier Systems,"

Proc. 16th International Conference on Pattern Recognition, Quebec City, Canada, Page 9, 2002.

[8] D.E. Denning, "An Intrusion Detection Model," IEEE Transactions on Software Engineering, vol. SE-13, pp. 222-232, February 1987.

[9] T. F. Lunt, "A survey of intrusion-detection techniques," Computers & Security, 12(4):405–418, June 1993.

[10] T. Verwoerd, R. Hunt, "Intrusion Detection Techniques and Approaches," Computer Communications, Elsevier, UK, Vol 25, No 15, pp. 1356-1365, September 2002.

[11] IDS Intrusion detection system, available at http://www.linuxfocus.org/English/May2003/article292.shtml.

[12] E. Biermann, "A comparison of Intrusion Detection Systems," Computers & Security, pp. 676-683, 20(2001).

[13] W. Lee, S. J. Stolfo, "A Framework for Constructing Features and Models for Intrusion Detection Systems,". ACM Transactions on Information and System Security, 3(4):227-261, 2000.

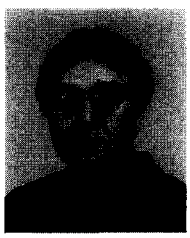
[14] S. Mukkamala, G. Janoski, A. H. Sung, "Intrusion Detection Using Neural Networks and Support Vector Machines," Proceedings of IEEE International Joint Conference on Neural Networks, pp. 1702-1707, 2002.

[15] A. M. Cansian, E. S.Moreira, A.C.P.L.F. Carvalho, and Jr, J.M.B., "Network Intrusion Detection using Neural Networks." In Proceedings of the International Conference on Computational Intelligence and Multimedia Applications, pp. 276-280, 1997.

[16] H. Debar, M. Becker and D. Siboni, "A Neural Network Component for an Intrusion Detection System." in : Proc. IEEE Symp. on Research in Computer Security and Privacy, pp.240-250, 1992.

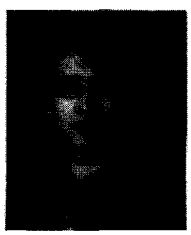
[17] http://www.shef.ac.uk./psychology/gurney/notes14/14.html.

◐ 저 자 소 개 ◑



우 종 우

1978년 서울대학교 농생물학과 졸업(학사)
1983년 Minnesota State University at Mankato 전산학과 졸업(석사)
1991년 Illinois Institute of Technology 전산학과 졸업(박사)
1994～현재 국민대학 컴퓨터학부 교수
관심분야 : 인공지능, 에이전트, 정보보호
E-mail : cwwoo@kookmin.ac.kr



김 상 영

2002년 국민대학교 전산과학과 졸업(학사)
2004년 국민대학교 대학원 전산학과 졸업(석사)
2004～현재 시그널 스펙트럼 재직
관심분야 : 인공지능, 정보보호, etc.
E-mail : reborn@neozone.net