지능형 IPS 프레임워크

An Intelligent IPS Framework

이동민[a], 김광백[a], 박충식[b], 김성수[b], 한숭철[c]

[a] *신라대학교 컴퓨터정보공학부 컴퓨터공학전공*

부산광역시 사상구 신라대학길 100번지

gavin82@naver.com, gbkim@silla.ac.kr

[b] *영동대학교 컴퓨터공학과*

충북 영동군 영동읍 설계리 산12-1

leciel@youngdong.ac.kr, indielazy@hotmail.com

[c] *지모컴㈜*

서울특별시 송파구 문정동 76-1

hansc@zimocom.com

Abstract

컴퓨터 네트워크 모니터링에 의한 보안장비는 많은 트래픽 자료를 분석하여, 이상유무를 판단하고, 대응해야 한다. 기존의 보안장비들은 이미 알려진 패턴에 대한 규칙을 이용하는 오용탐지방법(misuse detection)과 의미를 파악하기 어려운 많은 자료들을 제시하고 있는데 머물고 있다. 보다 나은 보안을 위해서는 정상적인 동작에서 벗어나는 이상징후를 탐지하여 침입을 탐지하는 이상탐지방법(anomaly detection)의 채용이 필요하고, 보안장비에서 제시되는 많은 트래픽 자료들은 보안전문가의 전문적인 분석이 필요하다.

본 연구에서는 데이터마이닝 기법을 이용한 이상탐지방법과 보안전문가의 전문적인 보안지식에 의한 분석, 대응, 관리를 위한 지식처리 기법을 사용할 수 있는 지능형 IPS(Intrusion Detection System) 프레임워크를 제안한다.

Keywords

침입방지시스템, 데이터마이닝, 규칙기반시스템, 오용탐지, 이상탐지, intrusion prevention system, anomaly detection, misuse detection

1. 서론

컴퓨터 네트워크 모니터링에 의한 보안장비는 많은 트래픽 자료를 분석하여, 이상유무를 판단하고, 대응해야 한다. 기존의 보안장비들은 이미 알려진 패턴에 대한 규칙을 이용하는 오용탐지방법(misuse detection)과 의미를 파악하기 어려운 많은 자료들을 제시하고 있는데 머물고 있다. 보다 나은 보안을 위해서는 정상적인 동작에서 벗어나는 이상징후를 탐지하여 침입을 탐지하는 이상탐지방법(anomaly detection)의 채용이 필요하고, 보안장비에서 제시되는 많은 트래픽 자료들은 보안전문가의 전문적인 분석이 필요하다.

규칙을 이용하는 오용탐지방법(misuse detection)은 미리 전문가들에 의하여 작성되면 정확히 탐지할 수 있지만 그 외의 것은 당연히 탐지할 수 없다. 이에 비하여 정상적인 동작에서 벗어나는 이상징후를 탐지하여 침입을 탐지하는 이상탐지방법(anomaly detection)은 정의상 기존에 있는 경우 또는 모든 새롭게 등장하는 경우에 상관없이 침입으로 탐지할 수 있으나 정상적인 동작을 정확하게 파악하기가 어려울 뿐 아니라 모든 이상징후가 침입은 아니기 때문에 잘못 탐지하는 경우(False Positive)가 많이 생긴다.

이러한 이상징후를 적절히 정의할 수 있는 이상탐지모델을 생성하기 위하여 많은 양의 트래픽자료를 이용하는 데이터마이닝 기법이 이용되고 있다. 그러나 데이터마이닝 기법을 이용하여 해당 네트워크 환경의 변화하는 상황에서 이상탐지모델을 생성하는 것은 학습을 위한 자료를 준비하고 처리하는 과정은 많은 시간과 노력이 필요하기 때문에 본 연구에서는 경제적으로 운영될 수 있는 데이터마이닝 기법을 이용하고, 지식처리시스템을 채용하여 이의 관리와 운영을 자동화 할 수 있도록 하였다.

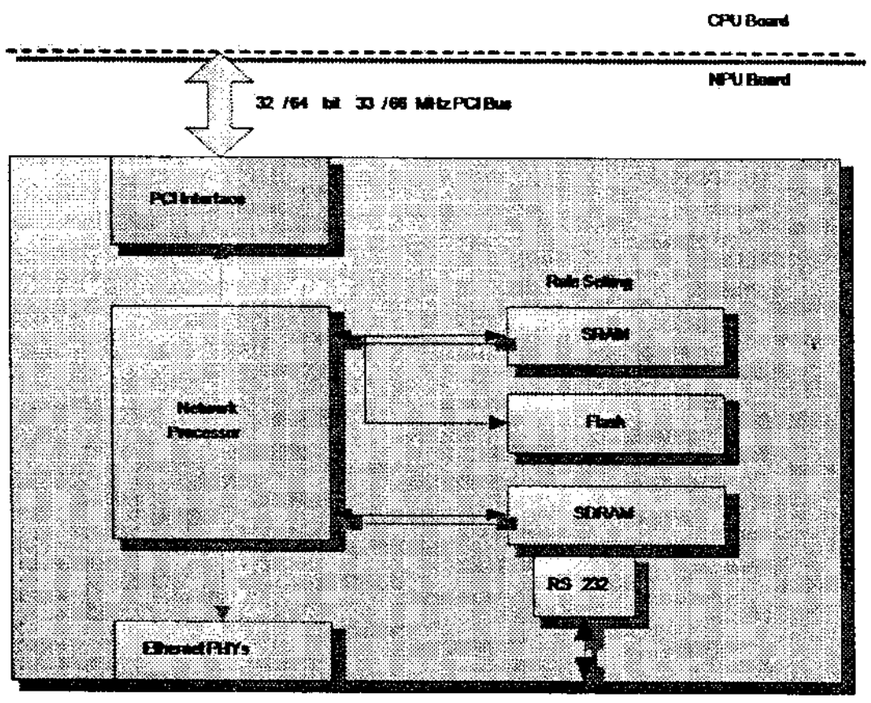
또한 기존의 보안장비들이 다양한 트래픽 자료에 대한 여러 통계적 자료를 시계열에 따라 제시하는 기능을 가지고 있지만 그 의미는 많은 경험을 가진 보안전문가들만이 분석하고 대응할 수 있다. 본 연구에서는 이러한 보안전문가의 전문지식을 수용하여 처리할 수 있는 규칙기반의 지식처리시스템을 채용함으로써 트래픽 자료의 분석과 그에 대한 대응을 자동화하도록 하였다.

본 연구에서 제안하는 지능형 IPS는 기존의 오용탐지 와 원 방지 규칙 패턴에 의한 접근통제가 고속으로 이루어지는 네트워크 프로세서 기반의 고속 보안장비 위에 수행되는 지능형 보안처리를 위한 프레임워크로 제안되는 것이다.

2. 네트워크 보안을 위한 자료 수집

본 연구에서는 오용탐지방법을 지원하는 IPS(Intrusion Detection System) 장비에서 시스템의 이상탐지 모델을 생성을 위하여 유지관리가 용이한 센서정보를 이용하고

운영관리를 자동화하여 경제적으로 시스템을 유지할 수 있도록 데이터마이닝 기법과 보안전문가의 휴리스틱한 전문지식을 이용할 수 있는 지능형 관리 기술을 이용할 수 있는 지능형 IPS(Intrusion Detection System) 프레임워크를 제안하는 것이다. 이러한 지능형 IPS 프레임워크의 원활한 동작을 위해서는 고속으로 패킷을 처리할 뿐만 아니라 데이터마이닝 처리와 지식 처리를 위한 계산능력이 확보되어야 한다. 지능형 IPS 프레임워크는 <그림. 1>와 같은 고속패킷처리를 가능하게 하는 네트워크프로세서에 기반한 하드웨어 위에 구성된다. 본 연구의 지능형 IPS 프레임워크는 <그림. 1>에서 보는 바와 같이 고속패킷처리를 NPU보드 가 전담할 수 있기 때문에 CPU보드에서 데이터마이닝 이상탐지처리와 지식처리를 위한 계산자원을 확보할 수 있는 것이다.



<그림 1> 고속패킷처리를 위한 네트워크프로세서 기반의 하드웨어

트래픽 자료의 속성은 가상적인 센서측정값으로 정의하여 네트워크 종류, 방향, 측정대상, 측정단위 등에 의하여 이루어지고 그 종류는 현재 보안장비의 네트워크 종류인 INT1, INT2, EXT1, EXT2, WAN, LAN, DMZ 등과 인바운드, 아웃바운드의 방향, 측정대상으로써 프레임 크기별(<64, <128, <256, <512, <1024, <1519, >1519, 등) 트래픽양과 비율, 프로토콜별(IP, ARP, TCP, UDP, ICMP, IGMP, 등) 트래픽양과 비율, TCP flag 트래픽양과 비율, 시스템(CPU, 메모리, HDD) 양 등의 최대값, 최소값, 평균, 값, 등을 PPS, BPS, % 등의 측정단위로 측정된다.
센서 측정값은 많은 대량의 패킷으로 이루어지기 때문에 5분 간격 측정값을 현재값의 간주하고, 저장되는 측정값은 5분 간격의 현재값으로부터 1시간 간격 정보로 저장한다. 이러한 저장값으로부터 필요에 따라 원하는 값을 네트워크, 방향, 측정대상의 종류, 통계수식(평균, 최소, 최대, 표준편차), 측정기간(10분간, 1시간, 3시간, 6시간, 12시간, 하루, 3일, 1주일, 2주일, 한달, 등), 측정시점(현재부터, 특정시간지정) 등에 의하여 지정되어 얻어질 수 있도록 한다.

3. 이상탐지 모델을 생성을 위한 데이터마이닝

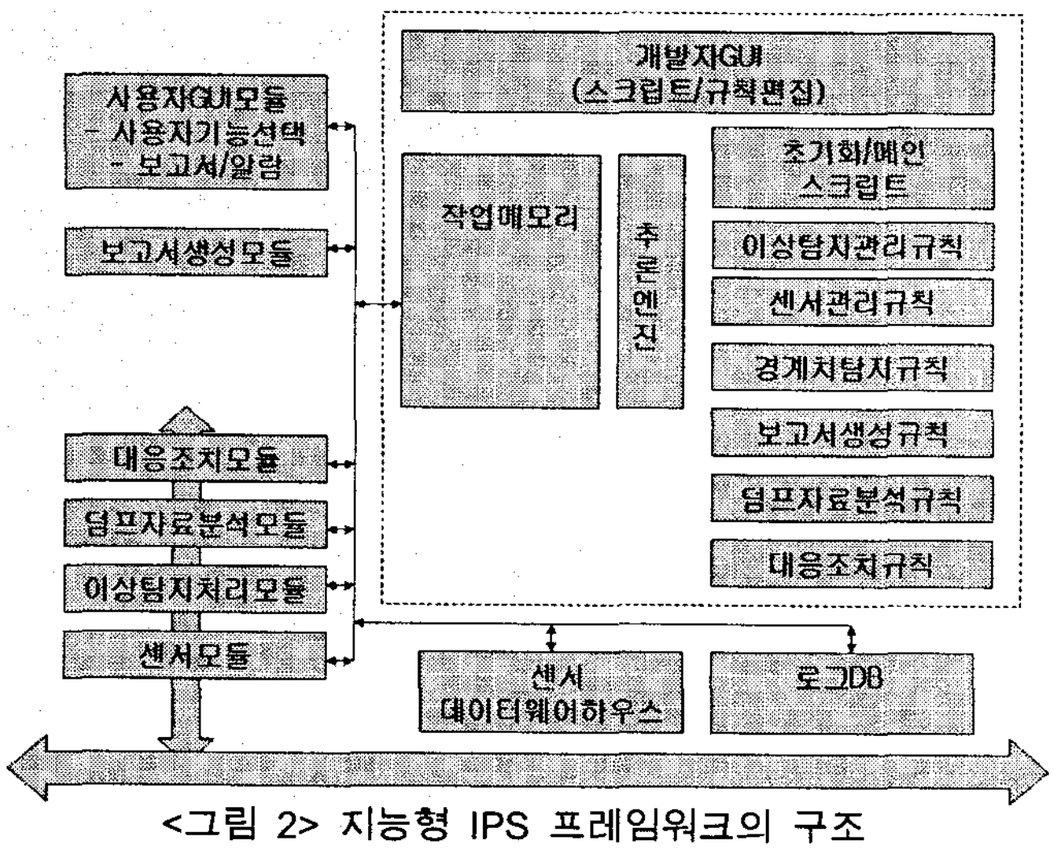
계속적으로 갱신이 가능한 이상탐지 모델을 만들기 위해서는 축적된 네트워크 트래픽 자료를 조직적으로 유지, 관리하여 데이터웨어 하우스를 유지하고, 데이터마이닝 기술을 이용하여 정기적으로 이상탐지모델을 생성하는 것이다. 이때 데이터마이닝 기법을 이용하여 이상탐지모델을 만들기 위해서는 훈련에 필요한 정상자료와 비정상자료를 준비(데이터라벨링)해야 하는데 시스템이 운영되고 있는 상황에서는 매우 힘든 일이다[1,2,3,4,5]. 이러한 이유로 검증을 위해 사용되는 공인된 자료들은 있지만 환경과 시간에 따라 변하는 현실적인 상황을 침입모델에 반영하기 어렵다. 때문에 본 연구에서는 정상 자료와 비정상 자료를 별도로 준비하지 않고도 훈련이 가능한 방법을 모색하였다.
비정상 자료는 정상자료에 비해 매우 드물게 나타나며 매우 다른 특성을 가지고 있다고 가정할 수 있다면 정상 자료와 비정상 자료를 따로 준비할 필요가 없어진다. 실제로 비정상적인 행동은 드물고 알려진 공격의 비정상인 자료도 규칙에 의한 오용탐지 시스템이 찾아 준다면 정상적인 자료에 대하여 통계적으로 매우 작은 경우일 것이며 통계적인 특성도 매우 상이할 것이다[6].
클러스터링의 기본적인 아이디어는 클러스터의 공집합으로부터 시작하여 자료 집합으로부터 한번에 처리로 클러스터를 만들 수 있다. 학습을 위한 자료 집합으로부터 얻어진 새로운 각각의 자료에 대하여 알고리즘은 각 자료의 거리와 클러스터의 각 클러스터의 센트로이드(centroid)와의 거리를 계산한다. 가장 가까운 거리를 가진 클러스터가 선택되고, 그 거리가 어떤 상수 W(클러스터의 폭)보다 작으면 그 자료는 그 클러스터에 할당된다. 그렇지 않으면 그 자료를 중시으로 하는 새로운 클러스터가 생성된다. 그 알고리즘은 다음과 같이 진행된다.
계산값을 M으로 고정하고 클러스터 폭 상수를 W로 가정하자. C가 클러스터이고 d가 자료일 때 dist(C, d)를 C와 d의 거리로 정의한다. 클러스터의 자료는 그 클러스터의 중심을 정의하는 특징벡터(feature vector)가 된다. 그 자료는 센트로이드라고 할 수 있다.
1) 클러스터 S를 공집합으로 초기화 한다.
2) 학습 자료 집합으로부터 자료의 거리(특징벡터)를 구한다. 만약 S가 공집합이면 d를 클러스터로 생성하고 S에 추가한다. 그렇지 않으면 그 자료에 가장 가까운 S의 클러스터를 찾는다. 환언하면 S에서 S의 모든 C1에 대하여 dist(C, d) <= dist(C1, d)인 클러스터 C를 찾는다.
3) 만약 dist(C, d) <= W이면 클러스터 C와 d를 연결한다. d는 그렇지 않으면 d는 S의 어떤 클러스터로부터 W이상이고, Cn은 정의된 자료로 d의 클러스터일 때 S <- S U {Cn}인 새로운 클러스터가 생성된다.
4) 학습 집합의 모든 자료에 대하여 2)단계와 3)단계를 반복한다.
일단 학습집합으로부터 클러스터들이 생성되면 시스템은 침입 탐지를 수행할 준비가 된 것이다.
1) d를 생성된 클러스터로부터 생성된 훈련 집합의 통계적 정보를 근거로 d를 변환한다. d'는 변환후의 자료라고 하자.
2) d'와 가장 근접한 클러스터를 찾는다.(즉, 클러스터 집합의 클러스터 C는 S의 모든 C'는 dist(C, d) <= dist(C', d')이다.
3) C의 라벨(label)에 따라 d'를 분류한다(정상이거나 비정상).

환언하면 d에 가장 근접한 클러스터를 찾고, 그 클러스터의 분류를 할당하는 것이다.
본 연구에서는 이러한 점에 착안한 이상탐지기술을 채용하여 침입방지 시스템이 최소한의 노력으로 운영될 수 있도록 인공지능의 지능화 기술을 이용하여 시스템의 운영을 최대한 자동화할 수 있도록 하였다.

4. 지능형 지식처리를 위한 지식처리 시스템

네트워크 보안관련 자료의 분석과 대응은 보안 전문가의 보안지식이 필요하기 때문에 이에 관련 지식을 인공지능의 지식처리 기술을 사용하여 자동화함으로써 보안기능의 고도화를 이룰 수 있다. 보안전문가들은 네트워크 트래픽 모니터링을 통하여 이상징후를 탐지하고 그를 바탕으로 추적해야 할 또 다른 트래픽 자료를 찾고 그에 대한 원인을 파악하고 대응조치를 취하게 된다.
그러한 예의 가상 시나리오를 생각해보면 (1) 트래픽 시간별 추이량 변화의 모니터링을 통하여 bps가 평소보다 급격히 올라가서 지속되면 호스트 탑 10을 조사하고, (2) 해당 호스트들의 프로토콜별 트래픽 양을 조사함으로써 과도한 트래픽을 내보는 호스트 탐지하고, (3) 해당 호스트의 상대 호스트를 조사하고 트래픽 캡쳐를 통하여, (4) P2P 트래픽임을 알아낸다. (5) 해당 트래픽을 차단한 후 네트워크 정상화를 확인하게 된다.
이러한 과정은 지식처리시스템과 동적인 네트워크 트래픽 측정 기능, 네트워크에 대한 처리기능을 연동함으로써 자동화할 수 있다.
대개의 네트워크 모니터링뿐만 아니라 데이터마이닝 기법을 이용하는 이상탐지 모델 생성의 과정도 지식처리 시스템을 이용하여 자동화함으로써 이상탐지 모델의 구성과 관리를 경제적이고도 효율적으로 운영할 수 있다.

5. 지능형 IPS 프레임워크의 구조



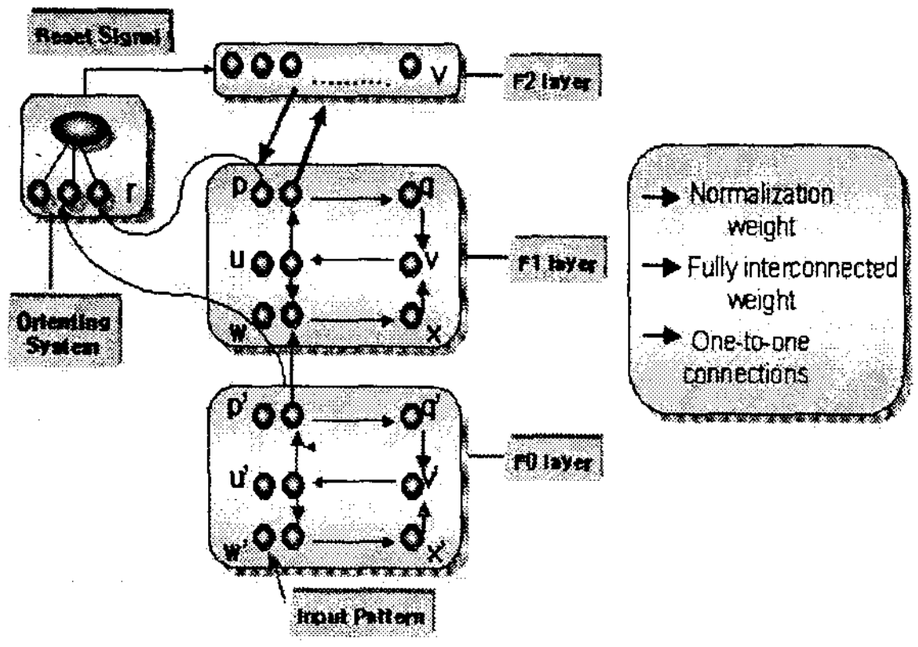
<그림 2> 지능형 IPS 프레임워크의 구조

전문적인 지능형 IPS 프레임워크는 보안장비의 운용과 관리에 다양한 보안기술을 운용하는 보안전문가의 전문적인 능력을 적용할 수 있도록 하는 것이다. 이러한 목적에 부응하기 위해서 지능형 IPS프레임워크는 보안전문가의 전문적인 능력을 표현할 수 있는 지식처리 시스템이 필요하고, 지식처리 시스템에 의하여 운용/관리될 수 있는 다양한 보안관련 기능모듈들이 필요하다.
이러한 보안관련 기능모듈들은 지식처리시스템의 지시에 따라 네트워크로부터 필요에 따른 정보를 능동적으로 수집하여 전달하거나, 지시에 따라 이상탐지 모델을 구성하기 위한 정보 처리, 모델 학습, 모델 적용, 결과 분석 등의 작업을 수행하거나, 지시에 따라 대응조치, 보고 등을 수행하는 등의 모듈 들로 이루어진다.
지능형 IPS 프레임워크는 규칙처리를 위한 지식처리시스템 부분(점선 내부)와 기존의 침입방지 시스템과의 연동하여 수행되는 부분(점선 외부)으로 나누어 볼 수 있다. 규칙처리를 위한 지식기처리시스템은 자체 개발한 NEO라는 스크립트 기반의 인공지능 추론엔진으로써 보안시스템에서 통상적으로 쓰이는 규칙과는 다른 구조의 인공지능 지식처리 시스템이다.
기존의 침입방지 시스템과 연동하면서 수행되는 여러 모듈들은 기존의 침입방지 시스템의 기능과는 다른 지능적인 모니터링과 탐지 기능을 위한 것이다. 외부의 모든 모듈들은 기존의 침입방지시스템으로부터 자료를 받아서 처리하면서도 지식처리시스템과 연동하여 지능적인 분석과 관리를 적용할 수 있도록 하였다.
이상탐지처리 모듈은 NPU 보드를 통하여 들어오는 패킷을 분석하여 이상탐지를 위한 알고리즘을 수행한다. 이러한 수행을 통한 자료의 분석은 지식처리시스템에 의하여 수행되고, 이어지는 후속조치들은 대응조치 모듈, 덤프자료분석 모듈, 센서모듈 등에 의하여 수행된다. 센서 모듈은 통상적인 자료수집외에 필요에 따라 규칙기반 시스템의 추론에 의하여 지식되는 정보를 동적으로 수집할 수 있도록 제어될 수 있다. 덤프자료분석 모듈은 필요에 따라 해당 순간의 필요한 자료를 덤프하여 규칙기반의 지식처리시스템이 분석할 수 있도록 하는 기능을 제공한다. 대응조치 모듈은 센서모듈, 덤프자료분석 모듈에 의하여 제공되는 자료를 통하여 이루어지는 면밀한 분석을 이후에 필요한 조치를 기존의 침입방지시스템에 전달하여 수행하는 역할을 수행한다. 보고서생성 모듈은 기존의 보고기능에 추가하여 전문가들의 분석지식을 규칙으로 지식화하여 좀 더 심도있는 보고기능이 가능하도록 하는 것이다. 사용자 GUI 모듈은 시스템의 지능형 기능을 사용하고 관리할 수 있는 기능에 대한 인터페이스를 제공한다. 센서 데이터웨어하우스와 로그 DB 는 패킷 자료와 로그분석을 위한 저장소의 역할을 한다.

5.1. 이상탐지 모듈

이상탐지를 위한 클러스터링의 자료는 2장에서 기술한 바와 같은 센서측정값을 세션이나 플로우 정보로 재구성하여 사용한다[7, 8].
비정상 자료는 정상자료에 비해 매우 드물게 나타나며 매우 다른 특성을 가지고 있다고 가정할 수 있다면 정상 자료와 비정상 자료를 따로 준비할 필요가 없어진다. 실제로 비정상적인 행동은 드물고 알려진 공격의 비정상인 자료도 규칙에 의한 오용탐지 시스템이 찾아 준다면 정상적인 자료에 대하여 통계적으로 매우 작은 경우일 것이며 통계적인 특성도 매우 상이할 것이다. 이러한 가정하에 재구성된 입력값으로 ART2 신경망 알고리즘을 이용하여 클러스터링하여 네트워크 상태를 판별한다.
ART2 신경망은 임의의 입력 패턴에 대해 이미 학습된

패턴을 잊지 않고 새로운 학습 패턴을 학습할 수 있는 안정성(stability)과 적응성(plasticity)을 가지면서 실시간 학습이 가능하여 저속 및 고속 학습을 지원할 뿐만 아니라 지역 최소화(local minima)문제가 발생하지 않는 장점을 갖는다. ART2 신경망 알고리즘은 F1레이어, F2레이어, orienting mechanism의 3개의 메인 컴포넌트로 구성 되어 있는 self-organizing신경망이다. ART2신경망 알고리즘은 복잡한 템플릿 저장과 계속적으로 학습하기 위해 디자인된 복잡한 구조를 가진다. ART2 학습 프로세스를 통해, 각각의 출력 노드는 입력 패턴의 특별한 카테고리에 들어간다. 특히, 각각의 출력 노드는 입력 패턴의 그룹과 함께 정의된 요소들을 공유하는 템플릿 패턴을 저장된다. 우선, 네트워크는 F1 레이어안에 입력 패턴을 받는다. 그 다음에 네트워크는 F2레이어 안에 있는 저장된 모든 템플릿을 비교하고, 하나의 템플릿은 입력 패턴과 가장 공통된 요소와 함께 선택되어진다. 그리고 orienting-mechanism을 경유한 입력 패턴과 선택된 템플릿은 더 가깝게 얼마나 잘 매치되는지를 결정하기 위해 비교된다. 마지막으로, 만약 템플릿이 잘 매치되었다면 이것은 입력 패턴을 더 잘 받아들이기 위해 수정되고, 네트워크는 이것의 입력을 카테고리화 한다. 템플릿이 매치되지 않으면 두번째 단계가 고려사항이나 reset으로부터 제한된 현재의 템플릿과 함께 반복된다. 이상탐지를 위한 ART2 구조도는 <그림 2>과 같고 ART2 알고리즘은 다음과 같다.



<그림 3> 이상탐지를 위한 ART2의 구조

Step 1. k 번째 입력 벡터 X_k 를, 신경회로망의 i 번째 클러스터의 중심 벡터를 W_i 라 정한다.

Step 2. 새로운 입력 벡터 X_k 에 대해 최소 거리(minimum distance)를 가지는 클러스터 $j*$ 을 승자 클러스터로 선택한다. 일반적으로 입력 벡터와 클러스터 중심 벡터 사이의 거리는 유클리디안 거리로 계산한다.

$$\|X_k - W_{j*}\| = \min\|X_k - W_i\|$$

Step 3. 입력 벡터에 대한 Vigilance Test를 수행한다. 만약 입력 벡터와 승자 클러스터의 중심 벡터 사이의 거리가 반경 ρ (vigilance parameter) 이내에 들어오면 이 입력 패턴은 승자 클러스터와 유사한 패턴임을 의미하여 이 입력 벡터를 승자 클러스터에 포함시키고 그 클러스터의 중심 벡터를 수정한다.

$$W_{j*}^{t+1} = \frac{X_k + W_{j*}^t \bullet n_j}{n_{j*} + 1}$$

여기서, n_j 는 j 번째 클러스터에 포함된 입력 벡터의 개수이다. 만약 입력 벡터와 승자 클러스터의 중심 벡터 사이의 거리가 반경 ρ 보다 크면 이 입력 패턴은 기존의 클러스터와는 상이한 패턴임을 의미하며 이 입력 벡터로 새로운 클러스터를 생성한다.

Step 4. 모든 입력이 제시될 때까지 Step 1에서 부터 Step 3의 과정을 반복 수행한다.

Step 5. 지정된 회수의 학습을 반복 수행하거나 신경망의 클러스터 중심 벡터가 각각 변함이 없으면 학습을 종료한다.

5.2. 규칙기반 지식처리 시스템

지능형 IPS 프레임워크 는 기본적으로 자체 개발된 NEO 시스템[8]이라는 스크립트기반 인공지능 규칙처리 추론엔진을 기반으로 한 NEO-IAS으로 이루어진다.

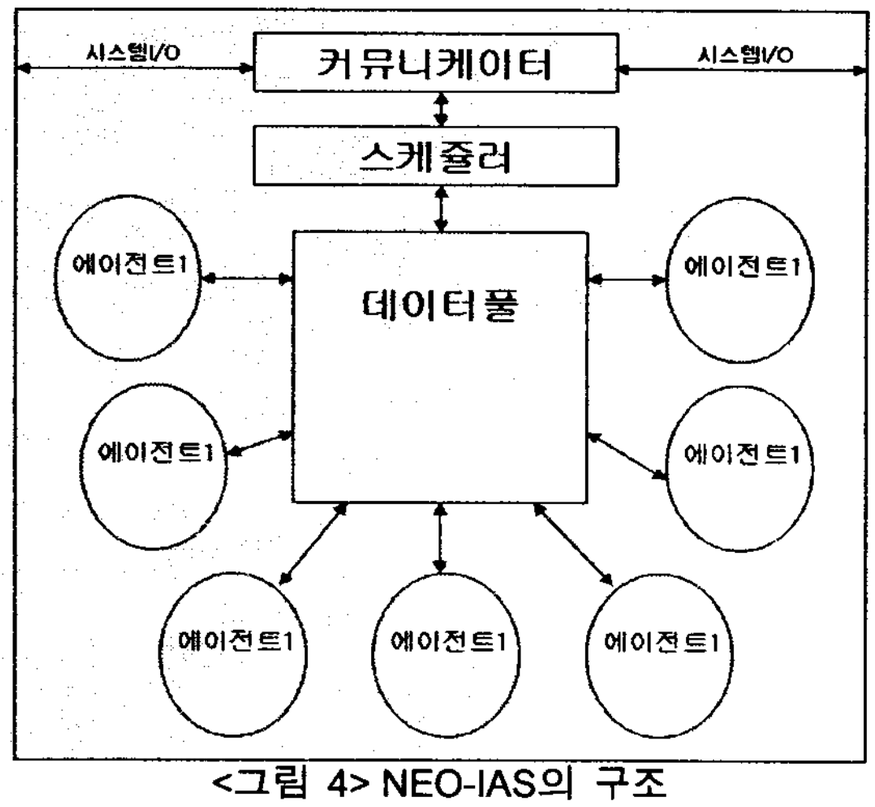
가. NEO 시스템

NEO 시스템은 인공지능 프로그램을 개발하기 위한 소프트웨어 도구이다. NEO 시스템에서는 모든 개체는 리스트로 이루어져 있다. 리스트는 문자나 숫자로 이루어진 구성요소를 나열한 것이며, 그렇게 이루어진 구성요소도 또 다른 리스트의 구성요소가 될 수 있다.

NEO 시스템은 함수언어 기능, 객체지향 기능, 규칙 추론 기능 등을 지원하지만 이러한 기능을 이루는 함수, 객체, 속성, 메소드, 사실, 규칙 등 모든 구성요소가 리스트 형태로 표현되고, 관리된다. 모든 구성요소가 리스트로 구성, 관리되는 이유는 시스템의 모든 자원을 투명하고 일관성 있게 처리하기 위해서 이다. NEO 시스템의 수행방식이나 함수언어 기능은 LISP과 유사하지만, 내부적으로 처리되는 방식과 내장 함수들은 서로 다르며, 객체 지향 기능이나 규칙 추론 기능, 진리치 유지 기능은 지식기반 시스템 개발을 위한 환경이 된다.

NEO의 핵심 기능은 DLL형태로 이루어져 있기 때문에 인공지능 프로그램을 개발할 때 내장하여 이용할 수 있으며, 자체의 GUI를 Visual Basic이나 Visual C++를 이용하여 구현할 수 있다. NEO의 개발환경은 Window95/NT에서 수행되는 명령어 인터프리터 형태로 되어있는데 이 또한 NEO의 DLL을 이용하여 만들어 진 것이다.

나. NEO IAS(Intelligent Agent System)

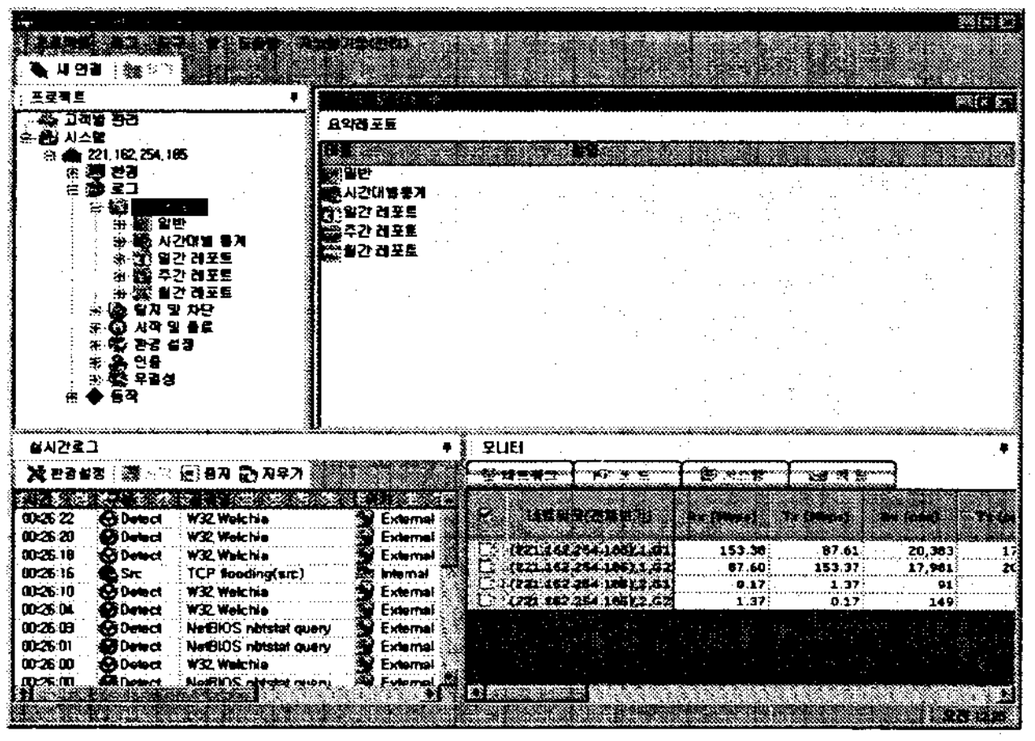


<그림 4> NEO-IAS의 구조

NEO IAS의 에이전트는 목적, 활성화조건, 내부변수, 내부함수들, 메인 프로시듀어로 이루어진다. 내부함수는 자체정의함수, 외부언어함수호출이 가능하고, 이를 통하여 규칙기반모듈, 신경망모듈, 유전자모듈, 외부처리모듈 등을 이용할 수 있다. 각 에이전트는 자신의 목적에 부합되는 활성화 조건이 갖추어 지면 정의된 내부변수/함수를 이용하여 메인 프로시듀어를 구동한다. 활성화 조건은 직접호출, 데이터 풀의 상태, 등에 따라 결정된다. 에이전트는 스케쥴러에 의하여 사이클별로 처리되기 때문에 물리적으로 순차처리되지만 계산적으로는 병렬처리된다. 하드웨어의 구조에 따라서 병렬처리가 가능하다. 커뮤니케이터는 외부 환경에 대한 시스템 입출력을 처리함으로써 시스템의 유일성(아이덴티티)를 유지한다. 그러나 시스템 내부의 에이전트들도 자체의 입출력 기능을 가질 수 있다. 데이터 풀은 객체지향형태로 유지되는 공통 정보 공간이며, 시스템 입출력 정보의 저장공간이며, 임의 조건에서 임의의 에이전트들이 정보를 교환할 수 있는 정보전달공간(버스)의 역할을 한다. NEO-IAS 에서 에이전트의 사용방법은 다음 예시와 같다.

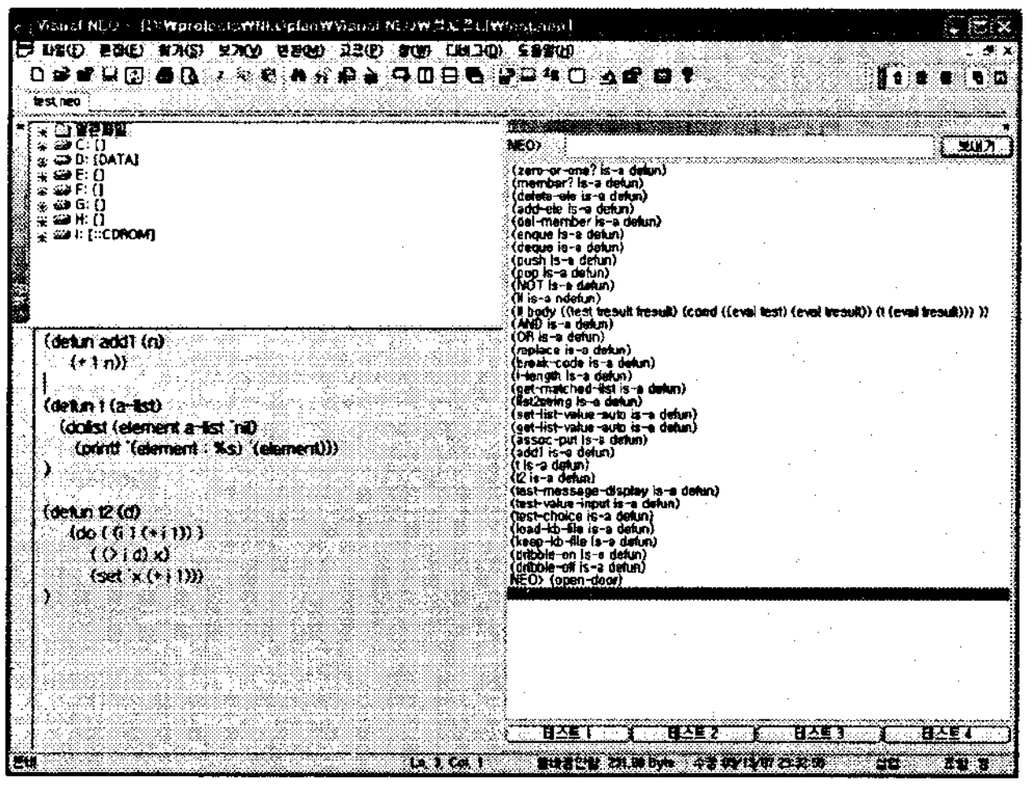
```
(app-agent is-a agent)
(app-agent rule-system rule-system1)
(rule-system1 is-a rule-system)
(rule-system1 rule-set rule-set1 rule-set2)
(rule-set1 is-a rule-set)
(rule-set rule r1 r2 r3 r3)
(r1 is-a rule)
(r1 if (?x is-a bird))
(r1 then (?x is-a animal)
(app-agent method (:set-height ?value) (
                    (printf  "previous height => %s"
'((get-list self  'height)))
                    (put-list self  height  ?value)
          (printf  "current height => %s" '((get-list
self  'height)))
                    )
)
(app-agent1 is-instance-of app-agent)
(app-agent1 height 24)
(app-agent1 :get-height) =>
(app-agent1 :set-height 32) =>
```

5.3. 사용자 GUI 모듈



<그림 5> 지능형 기능의 메뉴

사용자 GUI모듈은 현재 사용되고 있는 GUI에 메뉴를 추가하여 프로토타입 형태로 구성하였다. 메뉴는 [지능형기능(관리)]라는 이름으로 만들어져 있으며, [보고서생성], [이상탐지모델관리], [스크립트명령]의 3가지 부메뉴로 구성하였다. 현재 일부기능만으로 메뉴 형태로 제공하고, 그 외 기능들은 NEO 시스템의 스크립터 명령어 다이어로그 박스를 통하여 이루어진다. 차후 용이한 사용을 위하여 다양한 메뉴를 개발할 예정에 있다.



<그림 6> 스크립트 명령 다이어로그 박스(NEO 시스템)

6. 결론 및 향후 연구

본 연구는 기존의 IPS 보안장비[9]에 데이터마이닝 기법을 이용한 이상탐지방법과 보안전문가의 전문적인 보안지식에 의한 분석, 대응, 관리를 위한 지식처리 기법을 사용할 수 있는 지능형 IPS 프레임워크를 제안하였다. 향후 여러 보안 상황에서 필요한 보안지식과 경험을 지식화하고, 다양한 네트워크환경에서 여러 자료에 의해 효용성을 검증할 수 있는 실험을 수행할 예정이다.

참고문헌

1. R. Heady, G. Luger, A. Maccabe, and M. Servilla. The Architecture of a Network Level Intrusion Detection System. Technical report, Department of Computer

Science, University of New Mexico, August 1990.
2. T. F. Lunt, Ann Tamaru, Fred Gilham, R. Jagannathan, Caveh Jalali, H. S. Javitz, A. Valdes, P. G. Neumann, and T. D. Garvey. A Real-Time Intrusion Detection Expert System (IDES), Final Technical Report. Technical report, Computer Science Laboratory, SRI International, Menlo Park, California, February 1992.
3. Henry S. Teng, Kaihu Chen, and Stephen C Lu. Security Audit Trail Analysis Using Inductively Generated Predictive Rules. In Proceedings of the Sixth Conference on Artificial Intelligence Applications, pages 24-29, Piscataway, New Jersey, March 1990. IEEE.
4. Kevin L. Fox, Ronda R. Henning, Jonathan H. Reed, and Richard Simonian. A Neural Network Approach Towards Intrusion Detection. In Proceedings of the 13th National Computer Security Conference, pages 125-134, Washington, DC, October 1990.
5. R. Jagannathan and Teresa Lunt. System design document: Next generation intrusion detection expert system (NIDES). SRI report, SRI International, Menlo Park, California, March 9, 1993.
6. Leonoid Portnoy, Eleazar Eskin, and Sal Stolfo, Intrusion Detection with Unlabeled data Using, Clustering,
7. 김명섭, 원영준, 이형조, 호원기, Flow 기반의 인터넷 응용 트래픽 특성분석, KROM review, Vol. 7, No. 1, August 2004, pp.20-31이종엽, 윤미선, 이훈, DoS공격의 유형분석 및 탐지방법,
8. NEO 시스템 매뉴얼, 2006
9. 지모컴, 원브레이커 매뉴얼, 2007