論文2001-38CI-5-4

THRE-KBANN을 이용한 이상현상탐지모델

(Anomaly Detection Model Using THRE-KBANN)

沈 東 熙 *

(Dong Hee Shim)

요 약

인터넷이 널리 이용되면서 네트워크나 호스트에 대한 불법적인 침입은 많은 위협요소가 되고 있다. 이러한 침입을 탐지하기 위하여 통계적기법, 데이터마이닝기법, 유전자 알고리즘/프로그래밍 기법 등을 이용한 이상현상 탐지모델들이 많이 제안되어 왔으나 새로운 유형의 침입에 대해서는 탐지능력이 떨어지는 단점이 있다. 본 논문에서는 THRE-KBANN을 이용한 이상현상탐지모델을 제안하였는데, 이는 연속학습을 할 수 있도록 지식기반신경망을 개선한 것이다. 이 모델을 실험적 자료에 적용한 결과를 데이터마이닝기법을 적용한 경우와 비교하여 성능평가를 하였다. 그리고 새로운 침입유형을 탐지하기 위한 연속학습에 대한 성능도 평가하였다.

Abstract

Since Internet has been used anywhere, illegal intrusion to a certain host or network become the ciritical factor in security. Although many anomaly detection models have been proposed using the statistical analysis, data mining, genetic algorithm/programming to detect illegal intrusions, these models has defects to detect new types of intrusions. THRE-KBANN (theory-refinement knowledge-based artificial neural network) which can learn continuously based on KBANN, is proposed for the anomaly detection model in this paper. The performance of this model is compared with that of the model based on data mining using the experimental data. The ability of continual learning for the detection of new types of intrusions is also evaluated.

Ⅰ. 서 론

인터넷이 널리 이용되면서 호스트나 네트워크에 대한 불법적인 침입은 보안측면에서 중요한 관심사가 되었다. 자료에 대한 기밀성, 무결성과 가용성이 중시되면서 이러한 불법적인 침입을 탐지하는 것은 시스템에 필수적인 요소가 되었다. 침입이 발생하면 시스템의 상태를 나타내는 자료에 이상현상이 존재하다고 보는 관점인 IDS (Intrusion Detection System,침입탐지시스템)가 1987년에 Denning[1]에 의하여 정의된 이후 이상현상탐지를 위한 많은 연구가 이루어져왔다[2,3,4,5,6,7,8,9]. 그래서 1998년에는 IDSC(Intrusion Detection Systems Consortium)이 결성되었으며 분기마다 포름을 열고 있다[10]. 지금까지 개발된 침입탐지시스템은 모니터링 측면에서 응용기반, 호스트기반, 목표기반, 네트워크 기반으로 분류하며, 시간측면에서 실시간모드, 일괄모드로 분류할 수 있다[11]. 이러한 시스템들이 서로 다른 대상이나 방법으로 침입을 탐지하지만 이 침입탐지가 핵심적인 기능이다. 이런 탐지시스템이 어떤 것을 모니터

* 平生會員, 全州大學校 情報技術 컴퓨터工學部
(Jeonju University, School of Information Technology and Computer Engineering)

接受日字:2000年11月16日, 수정완료일:2001年7月18日

링하든지 침입을 탐지하는 기술적인 방법은 통계적 분석방법, neural networks, Bayesian networks, hidden Markov models, genetic algorithm/programming과 같은 방법들로 대별할 수 있다[4,5,6,7,8,9]. 그리고 이러한 탐지시스템의 성능은 일반적으로 이상현상을 이상현상으로 분류하는 적중율(hit ratio), 이상현상을 정상으로 분류하는 오류율(missing rate), 정상을 이상현상으로 분류하는 부진율(false alarm rate)로 평가한다[2]. 일반적으로 전체적인 성능은 통계적 분석방법이 전체적 평가요소에서 앞서는 것으로 알려지고 있으며, 다른 방법들은 부진율이 낮아 좋지만 적중율이 또한 낮은 것으로 알려져 있다.

그런데 침입은 자꾸 새로운 형태를 취하며 이러한 새로운 침입형태는 과거의 자료에는 없는 특징을 지니기 때문에 지금까지 제안된 침입탐지모델은 기존의 알려진 침입유형에 대해서는 적중율이 높지만 새로운 침입유형에 대해서는 오류율과 부진율이 높은 단점이 있다. 그래서 침입탐지에서의 문제는 새로운 침입유형에 대해서 어떻게 대처하느냐가 중요한 관건이다.

침입탐지모델에서 새로운 침입유형에 대처하려면 새로운 유형에 대한 연속적인 학습(Continual Learning)[12]이 필요하다. 연속학습은 자율적인 에이전트가 동적으로 변하는 환경에서 학습해 나가는 것을 의미하는데 이러한 학습을 하려면 기계학습분야에서 사용하는 기법을 도입해야한다. 기계학습방법 중 지식기반신경망[13]에 기반한 이론정련지식기반신경망(THRE-KBANN, THeory-REfinement-Knowledge-Based Artificial Neural Network)[14]은 영역이론과 사례를 이용하여 영역이론을 정련화함으로써 학습능력이 다른 학습방법보다 성능이 우수하다고 입증되었지만 연속학습의 능력은 보유하고 있지 않다. 본 논문에서는 THRE-KBANN이 연속학습능력을 보유하도록 보완하여 이상현상탐지모델로 사용할 수 있는 방안을 제시하였으며 이에 대한 성능평가를 통하여 다른 모델과 비교하였다. 본 논문의 Ⅱ장에서는 THRE-KBANN을 설명하였으며, Ⅲ장에서는 이의 이용방안을 제시하였고, Ⅳ장에서는 성능평가를 했으며 Ⅴ장에는 결론을 기술하였다.

Ⅱ. 이상현상 탐지모델과 THRE-KBANN

1. 이상현상탐지모델과 기존의 방법

(1) 이상현상탐지모델

이상현상을 탐지하는 모델은 보통 <그림1>과 같이 구성된다[2].

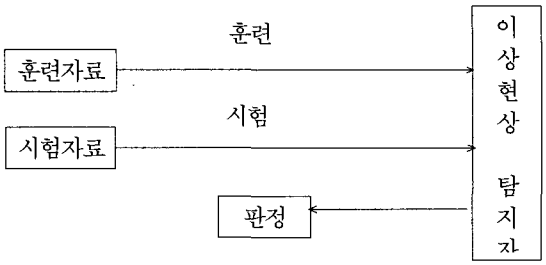


그림 1. 침입탐지모델
Fig. 1. Intrusion Detection Model.

이 그림에서 이상현상탐지자(Anomaly Detector)는 기계학습에서와 같이 훈련자료에 의하여 훈련을 받으며 시험자료를 이용하여 성능평가를 받을 수 있다. 기계학습에서는 이런 학습유형을 비교사학습(Unsupervisor Learning), 교사학습(Supervisor Learning)으로 분류한다. 현재까지 이상현상탐지자가 주로 사용하는 기법은 다음과 같다.

통계적 방법으로 대표적인 침입탐지시스템은 SRI에서 구축한 NIDES이다[6]. 이 NIDES에서는 frequentist라는 탐지자를 사용하는데 이는 빈도를 계산하여 결정하는 방식으로 비교사학습에 해당한다. 한편 데이터마이닝은 규칙성을 발견하거나 결정을 증진시키기 위하여 과거의 자료를 사용하는 기법이며 RIPPER에 기반한 탐지시스템[5], CN2[8,9]에 기반한 탐지시스템[4]이 대표적이며 교사학습에 해당한다. 그리고 GP에 기반한 방법[2]에서는 문제에 대한 해를 GA에서는 비트열로 표현하는데 반해 트리로 표현한 처리한다. 그래서 표현의 다양성이 비트열보다 좋으며, 적합성함수를 이용하여 평가를 하며 교사학습에 해당한다.

2. THRE-KBANN

KBANN에서는 어떤 문제영역에 대한 이론이 명제논리를 이용한 혼절(Horn Clause) 형태의 규칙으로 표현되어 있으면 이 규칙을 신경망으로 변환한다[13]. 그리고 예제에 의거하고 역전파 알고리즘을 이용하여 신경망을 학습시킨다. 그런데 KBANN에서는 규칙들을 신경망으로 변환한 후에는 신경망 구조를 변화시킬 수 없다. 하지만 THRE-KBANN은 신경망 구조의 변화를 통하여 영역이론에 대한 정련의 효율성을 높여주었다

[14]. THRE-KBANN은 오류를 많이 발생시키는 중간층의 노드를 찾아내서 오류를 없앨 수 있는 방법으로 중간층의 노드 구성을 변경해나간다. KBANN, THRE-KBANN은 이론을 먼저 이용하고 다음은 훈련예제를 통하여 학습을 하므로 연역적 학습과 귀납적 학습을 결합한 방법에 해당한다. THRE-KBANN의 알고리즘은 다음에 나타낸 바와 같다.

① 훈련예제를 훈련집합, 조정집합1, 조정집합2, 시험집합으로 임의로 분류한다.

② 훈련집합을 이용하여 훈련된 KBANN을 생성한다.

③ 조정집합1을 이용하되 다음의 절차에 의하여 신경망을 정련화한다.

ⓐ 각 노드의 음부제(false negative example)와 양부제(false positive example)의 값을 0으로 초기화한다.

ⓑ 조정집합1에서 각 부제에 대하여 각 노드에서의 양부제, 음부제 여부를 판단하여 해당값을 증가시킨다.

ⓒ 양부제와 음부제의 합이 가장 큰 노드를 선정한다. 같은 경우는 양부제나 음부제의 비율이 편중된 노드, 입력계층에 가까운 노드 순으로 선정한다.

ⓓ 노드 추가방법에 의거하여 노드를 추가하여 신경망을 생성한다.

④ 새로운 신경망을 조정집합2를 이용하여 훈련시키고 오류율이 이전의 신경망보다 높으면 위의 ⓒ단계로 되돌아간다.

⑤ 시험집합을 이용하여 새로운 신경망의 오류율이 중지조건을 만족하면 이를 출력하고 만족하지 않으면 ③으로 간다.

3. THRE-KBANN의 귀납적 학습

THRE-KBANN은 영역이론에 근거하여 훈련예제를 이용하지만, 영역이론이 없이 훈련예제만 있어도 귀납적 학습을 할 수 있다. 귀납적 학습에서는 영역이론이 없으므로 많은 훈련예제를 필요로 하는데 THRE-KBANN은 훈련예제로부터 신경망을 형성하고 다시 훈련예제를 통하여 영역이론을 정련한다.

Ⅲ. THRE-KBANN을 이용한 이상현상탐지모델

침입탐지모델에서 사용되는 훈련예제에서는 침입을 의미하는 자료인지 정상적인 자료인지를 나타내는 영역이론이 없으며 많은 훈련예제만 있고, 이것이 침입인지 정상인지만을 나타내고 있다. 따라서 THRE-KBANN을 적용하기 위해서는 <그림2>와 같이 먼저 훈련예제의 형식을 이용하여 초기 KBANN을 형성해야 한다. 다음은 다시 훈련예제를 이용하여 은닉노드를 적절하게 포함하는 초기 KBANN을 완성해야한다. 그리고 이 신경망을 THRE-KBANN을 이용하여 훈련예제를 학습시켜 영역이론정련을 함으로써 KBANN을 완성한다. 다음에 새로운 유형이 도착하면 THRE-KBANN을 이용하여 연속학습을 위한 훈련을 한다.

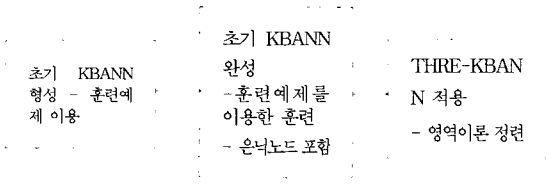


그림 2. THRE-KBANN의 처리절차
Fig. 2. The procedure sequence for THRE-KBANN process.

1. 훈련예제의 형식을 이용한 초기의 KBANN 형성

다음과 같은 절차를 이용하여 초기의 KBANN을 형성한다.

① 출력노드를 생성하는데 출력노드수는 분류하는 클래스 수가 정상 아니면 침입이므로 출력노드는 1개로 한다.

② 입력노드를 생성하는데 입력노드수는 입력을 구성하는 속성수에 의해 결정된다. 또한 속성마다 속성이 갖는 값의 수에 따라 노드수를 결정한다.

③ 중간층노드를 생성한다. 이 노드수는 1개로 한다.

④ 각 노드간의 가중치는 임의의 작은 수로 한다.

2. 초기 KBANN 완성

다음과 같은 알고리즘에 따라 KBANN의 중간노드수를 확장하여 초기의 KBANN을 완성한다. 여기서는 중간노드를 하나씩 증가해서 KBANN을 생성하여 이중 오류율이 가장 적은 것을 선택한다. 이 알고리즘은 K개의 자료를 유지하는 측면에서 beam 탐색과 유사하다.

① 훈련예제를 훈련집합, 조정집합, 시험집합으로 같은 수로 임의로 분류한다.

② 훈련집합을 이용하여 KBANN을 훈련시키고 시험집합을 이용하여 오류율을 평가한다.

③ 다음과정을 반복한다.

ⓐ 은닉노드수가 입력노드 수보다 크면 단계④로 간다.

ⓑ 은닉노드를 1개 추가하고 조정집합을 이용하여 이를 훈련시킨다.

ⓒ 시험집합을 이용하여 오류율을 계산한다. 이 KBANN을 저장한다.

ⓓ ⓐ단계로 간다.

④ 저장된 KBANN 중 오류율이 가장 적은 KBANN을 출력한다.

위에서 은닉노드의 수는 입력노드 수로 제한을 하였는데 이는 은닉노드가 많다고 무조건 효율적인 것은 아니기 때문에 휴리스틱하게 제한을 하였다.

3. THRE-KBANN의 적용

이제 KBANN이 생성되었으므로 앞서 2장에서 소개한 THRE-KBANN 알고리즘을 적용하여 영역이론을 정련함으로써 오류를 최소화한다. 기존의 유형에 대해서는 THRE-KBANN을 이용하여 정련화된 KBANN이 이상현상탐지기능을 잘 수행할 수 있다.

4. 연속학습을 위한 THRE-KBANN

새로운 유형의 특징이 나타나면 기존의 다른 방법의 학습을 통하여 훈련을 지속적으로 시켜나가야 한다. 새로운 유형의 특징은 먼저 입력의 새로운 특징, 출력의 새로운 특징이 있을 수 있는데 이는 훈련예제에 명시적으로 나타나며, 이는 입력노드의 추가, 출력노드의 추가를 통하여 신경망의 구조를 변경하고 훈련을 시켜야 한다. 그러나 입력이나 출력에의 특징 이외에 중간층의 개념추가와 같은 유형변화는 입출력노드의 변화없이 훈련을 통해 학습을 시켜야 한다. 이러한 새로운 훈련예제가 발생하면 이 새로운 예제와 기존의 예제를 이용하여 훈련을 한다. 새로운 유형에 대하여 이 같은 훈련을 지속적으로 해나가면 이것은 바로 연속학습(Continual Learning)[12]과 유사한 개념이 된다. 여기서는 입출력특징의 변화는 고려하지 않고 다른 특징의 변화만을 가정하여 이를 처리하기로 한다.

새로운 유형의 훈련예제들을 새로운 집합으로 만들고 다음과 같이 처리한다.

① 기존의 훈련예제 중 새로운 예제 수 만큼의 예제를 제거하고 남은 예제를 조정집합1, 시험집합으로 같은 예제수로 분류한다.

② 다음의 절차에 의하여 신경망을 생성한다.

ⓐ 각 노드의 음부제와 양부제의 값을 0으로 초기화한다.

ⓑ 새로운 집합에서 각 부제에 대하여 각 노드에서의 양부제, 음부제 여부를 판단하여 해당값을 증가시킨다.

ⓒ 양부제와 음부제의 합이 가장 큰 노드를 선정한다. 같은 경우는 양부제나 음부제의 비율이 편중된 노드, 입력계층에 가까운 노드 순으로 선정한다.

ⓓ 노드 추가방법에 의거하여 노드를 추가하여 신경망을 생성한다.

③ 새로운 신경망을 조정집합1과 새로운 집합을 이용하여 훈련시키고 오류율이 이전의 신경망보다 높으면 위의 ⓒ단계로 되돌아간다.

④ 시험집합과 새로운 집합을 이용하여 새로운 신경망의 오류율이 중지조건을 만족하면 이를 출력하고 만족하지 않으면 ②단계로 간다.

1) 기존 훈련예제의 제거

새로운 집합으로 편입된 예제수 만큼을 기존의 훈련예제에서 삭제한다. 이와 같이 훈련예제를 유지하면 모든 예제의 수는 일정크기가 유지된다. 그래서 각 훈련예제는 예제로 편입된 시간을 기록하여 이를 선입선출의 방법에 따라 제거하도록 하여 가장 새로운 유형의 예제를 포함하도록 한다.

2) 새로운 집합

THRE-KBANN에서 새로운 집합은 새로운 훈련예제를 포함하는 집합이다. 이 집합에 포함되는 예제수는 전체 훈련예제의 일정비율이하로 제한한다. 최대 이 비율은 1/3이어야 바람직하다. 왜냐하면 기존의 훈련예제는 두개의 집합으로 나뉘어 이용되므로 최대 이 집합의 크기와 같도록 한다.

Ⅳ. 성능평가

1. 기존유형에 대한 실험

(1) 이용자료

성능평가에 이용한 자료는 Cinnamon[15]에서 생성한 자료를 이용하였다. 이 자료는 2.5백만개의 레코드로 구성되어 있는데 알파벳 크기는 6바이트를 이용했다. 이 자료는 규칙지수(Regurarity Index)를 포함하고 있는데 규칙지수란 자료순서에 있어서의 순차적 종속성을 의미하며 이를 엔트로피로 측정하여 나타내고 있다. 규칙지수가 0이면 완벽하게 규칙적인 것을 의미하며, 1이면

규칙성이 전혀없이 랜덤하다는 것을 의미한다. 이 자료에는 이 규칙지수가 0.0부터 0.1 단위로 1.0까지 11개의 자료집합이 있다. 실험의 적절성을 위하여 규칙지수가 양단에 치우치지 않는 규칙지수 0.3부터 0.6의 자료를 이용하였다.

(2) 실험방법

정상과 이상을 포함하는 각 자료를 훈련집합, 조정집합, 시험집합과 같은 3가지 집합으로 40%, 30%, 30% 씩 할당하여 설정하여 초기 KBANN을 형성하였다. 그리고 훈련집합, 조정집합1, 조정집합2, 시험집합으로 각각 40%, 20%, 20%, 20% 씩 나누어 THRE-KBANN으로 정련시켰다. 그리고 이와 같은 실험을 5회 반복하였다.

(3) 성능평가기준

성능평가기준으로는 침입탐지모델에서 많이 사용하는 적중율, 부진율을 사용하였다. 그리고 기계학습분야에서 성능평가기준으로 많이 사용되는 범위율(recall 또는 coverage)과 정확성(precision또는 correctiveness)[16]이 있다. 범위율은 양의 예제(number of positive examples)중 올바르게 양으로 판단된 예제(number of correct positive examples)의 비율을 의미하는데 이상현상을 양으로 간주하면 범위율은 적중율과 같은 의미다. 정확성은 양으로 판단된 예제(number of positive predictions)중 올바르게 양으로 판단된 예제의 비율을 의미한다. 침입탐지모델에서 정확성은 이상현상으로 판단된 예제중 이상현상의 비율을 의미하는데 이 정확성도 평가기준으로 사용하였다.

(4) 성능평가결과

<표2>에는 THRE-KBANN을 이용하여 실험한 결과의 적중율과 오류율, 정확성을 나타냈다. 이 표에 나타낸 결과중 데이터마이닝 기법은 Ali의 방법[2]에 따라서 측정한 것이다. 데이터마이닝에서는 부진율이 모든 규칙지수에 대하여 0.0에 근사하였는데 THRE-KBANN에서는 적은 비율이지만 데이터마이닝보다는 높은 부진율을 나타내 나쁜 결과를 보여주었다. 그리고 정확성의 경우 데이터마이닝은 1에 근접하였고 THRE-KBANN은 데이터마이닝의 경우보다 다소 나쁜 결과를 보여주었다. 이 정확성은 부진율과 관계가 있는데 부진율에서 나쁜 결과는 정확성에서도 나쁘게 나타나게 된다. 그러나 적중율은 THRE-KBANN이 데이터마이닝 기법보다 규칙지수가 높은 경우에는 비슷한 수준을 보였지만 보통의 규칙지수에서는 더 높은 적중율을 나타냈다.

표 2. 실험 결과의 비교표

Table 2. The comparison of experiment results.

규칙지수	기법	0.3	0.4	0.5	0.6
적중율	데이타마이닝	0.781	0.752	0.684	0.720
적중율	THRE-KBANN	0.811	0.792	0.739	0.721
부진율	THRE-KBANN	0.031	0.022	0.022	0.013
정확성	데이타마이닝	0.999	0.999	0.999	0.999
정확성	THRE-KBANN	0.982	0.987	0.988	0.991

2. 신경망모델과의 비교

침입탐지모델을 위하여 역전파알고리즘을 이용한 신경망 모델 NNID(Neural Network Intrusion Detector)[8]와도 비교해보았다. 여기서는 비교의 용이를 위하여 NNID에서 사용한 동일한 자료를 이용하였다. 그런데 NNID에서는 사용자의 과거 사용명령을 학습하여 사용자가 누구인지 맞추는 문제에 적용하였다. 이 모델에서의 결과는 사용자를 밝히는 것이었으므로 THRE-KBANN의 출력노드수도 같은 수로 조절하였다. NNID에서의 적중율은 0.96 이었는데 THRE-KBANN에서는 0.98로 나타났으며, 부진율은 NNID에서는 0.07이었는데 반해 THRE-KBANN에서는 0.05로 나타났으며, 정확성은 NNID는 0.94 , THRE-KBANN에서는 0.96으로 나타나 대체적으로 THRE-KBANN이 NNID보다 높은 성능을 나타냈다.

3. 연속학습을 위한 새로운 유형에 대한 실험

(1) 일부의 새로운 유형 포함시

기본실험에서 사용한 자료를 이용하되 하나의 규칙지수를 이용하여 학습을 시키고 여기에 규칙지수를 변화시킨 자료의 20%를 임의로 추출하여 실험하였다. 이 실험결과는 <표 3>에 나타낸 바와 같은데 규칙지수 0.1의 변화에서는 적중율이나 부진율이 거의 차이가 없

표 3. 새로운 유형에의 실험 결과

Table 3. Experimental Result of New Feature Type.

규칙지수변화	0.3→0.4	0.4→0.5	0.5→0.6	0.3→0.5	0.4→0.6
적중율	0.781	0.733	0.713	0.712	0.702
부진율	0.022	0.018	0.023	0.032	0.034
정확성	0.962	0.970	0.966	0.962	0.960

었으며 규칙지수 0.2의 변화에서는 적중율은 0.02정도 낮게 나타났으며, 부진율은 0.02정도 높게 나타났다. 이와 같은 변동은 어느 정도의 변화에 대한 적응력을 나타낸다고 볼 수 있다.

(2) 모든 새로운 유형 포함시

새로운 유형이 기존의 유형을 모두 교체한 경우에 대하여 실험을 하였는데 <표 4>에는 교체비율에 따른 적중률, 부진율 그리고 전확성을 나타냈으며 마지막 행에는 두 규칙지수의 모두를 포함한 경우의 적중율과 부진율을 나타냈다. 이 표에서 보면 전제적으로 새로운 유형의 비율이 100%에 가까워지면 <표 2>에 나타낸 원래의 비율에 근접해감을 보여주고 있다. 그리고 이 때의 적중율은 두 규칙지수의 모두를 합쳐놓은 경우의 적중율보다는 다소 낮은 비율을 보이고 있지만 부진율과 정확성에서는 좋은 결과를 보여주고 있다. 이러한 결과는 연속학습의 효과라고 말할 수 있겠다.

표 4. 유형 비율 변화에 따른 적중율/부진율/정확성의 변화

Table 4. Hit ratio, false alarm rate and precision according to ratio of new type.

새로운 유형 비율	0.3 -> 0.4	0.4 ->0.5	0.5->0.6	0.3->0.5	0.4->0.6
20 %	0.781/0.022 /0.965	0.733/0.018 /0.969	0.713/0.023 /0.967	0.712/0.032 /0.964	0.702/0.034 /0.963
40 %	0.780/0.023 /0.966	0.734/0.018 /0.971	0.716/0.022 /0.968	0.716/0.031 /0.965	0.704/0.030 /0.965
60 %	0.779/0.022 /0.964	0.734/0.018 /0.972	0.718/0.020 /0.965	0.722/0.029 /0.972	0.707/0.026 /0.971
80 %	0.783/0.022 /0.965	0.735/0.019 /0.971	0.720/0.018 /0.971	0.732/0.027 /0.973	0.712/0.020 /0.966
100 %	0.785/0.022 /0.966	0.736/0.019 /0.970	0.722/0.015 /0.975	0.732/0.026 /0.972	0.714/0.015 /0.976
두 집합시의 비율	0.790/0.053 /0.958	0.732/0.022 /0.968	0.720/0.018 /0.970	0.734/0.027 /0.971	0.715/0.035 /0.965

V. 결론 및 향후과제

지금까지 많은 침입탐지모델들이 제안되어 그 성능이 평가되었는데 적중율과 부진율 측면에서는 진전이 많이 있었지만 새로운 침입유형에 대해서는 어려운 점이 있었다. 이러한 것은 침입은 자꾸 새로운 특징을 지니게 되는데 침입탐지모델은 이러한 새로운 침입의 특징에 대응할 학습능력이 떨어지기 때문이다. 본 연구에서는 새로운 유형에 대한 적응력을 갖게 하기 위해 연속학습이 가능하도록 THRE-KBANN의 이용방안을 제안하였다. 이는 이론정련지식기반신경망의 훈련방법의 훈련예제의 구성을 달리하여 연속학습효과를 높이는 방법이다. 이 모델은 기존유형의 자료에 대해서도 적중율과 부진율의 측면에서 데이터마이닝기법을 이용하는 경우와 비교하여 그 성능이 떨어지지 않음을 실험을 통하여 보여줬다. 그리고 간단한 실험을 통하여 침입유형의 변화에도 적응력을 보여줌을 확인해 연속학습능력을 보유함을 실험하였다.

이 논문에서는 다루지 못한 침입에 발생하는 새로운 입력특성, 출력특성에 대한 처리방법도 개선시킬 필요가 있다. 또한 이론정련지식기반신경망이 여러 측면에서 성능이 다소 좋지만 향후, 이를 실세계에서 구현하려면 실시간에 적용할 수 있는 연구접근이 필요하다.

참 고 문 헌

[1] Dorothy E. Denning, "An intrusion-detection model", IEEE Transactions on Software Engineering, SE Vol. 13, No. 2, pp. 222~232, February, 1987.

[2] Shahzad Ali, Adventures in Anomaly Detection, Technical Report, Carnegie Mellon University, December, 1999.

[3] Salvatore J. Stolfo, Wenke Lee, Data Mining Approaches for Intrusion Detection, Technical Report, Columbia University, 1998.

[4] Alfonso Valdes, Harold S. Javitz, The NIDES Statistical Component: Description and Justification, Technical Report, SRI International, March, 1993.

[5] Ludovic Me, Genetic Algorithms, an Alternate Tool for Security Audit Trails Analysis, Technical Report, Supelec, France, 1992.

[6] Robin Boaswell, Peter Clark, "Rule Induction with cn2: Some Recent Improvements," 1Machine Learning - Fifth European Conference, pp. 151~163, 1991.

[7] Tim Niblett, Peter Clark, "The CN2 Induction Algorithm', Machne Learning Journal, Vol. 3, No 4, pp. 261~283, 1989.

[8] J. Ryan, M.J. Lin and R. Miikkulainen, Intrusion Detection with Neural Networks,

Advanced in Neural Information Processing Systems 10, Cambridge, MA, MIT Press, 1998.

[9] Terran Lane, Machine Learning Techniques for the Domain of Anomaly Detection for Computer Security, Tecinical Report, Purdue University, 1998.

[10] http://www.icsa.net/html/communities/ids/White Papers/Intrusion1.pdf

[11] http://www-rnks.informatik.tu-cottbus.de/~sobirey/ids.html

[12] M. Ring, "CHILD : A First Step towards Continual Learning", Machine Learning, Vol. 28 No 1, pp. 77~104, July, 1997.

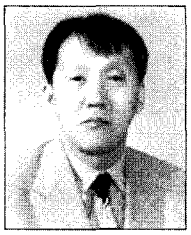
[13] G.G. Towell, "Symbolic Knowledge and Neural Networks:Insertion, Refinement, and Extraction", Ph.D thesis, University of Wisconsin-Madison, 1991.

[14] 심동희, "지식기반신경망에서 은닉노드 삽입을 이용한 영역이론정련화", 정보처리학회논문지, 제3권 제7호, pp. 1773-1780, 12월, 1996년

[15] http://www.cs.cmu.edu/~maxion/invictus/cinnamon.html

[16] Mark Craven, Sean Slattery and Kamal Nigam, "First-Order Learning for Web Mining", 10th European Conference on Machine Learning, 1998

저 자 소 개



沈 東 熙(平生會員)

1980년 2월 : 서울대학교 산업공학과 졸업. 1982년 2월 : 서울대학교 대학원 졸업(공학석사). 1994년 2월 : 고려대학교 대학원 전산과학과 졸업(이학박사). 1990~현재 : 전주대학교 정보기술컴퓨터공학부 교수. <주관심분야> 기계학습, 네트워크보안, 게임공학