# RBF신경망을 이용한 IDS에서의 학습데이터 결정 알고리즘

박일곤*, 문종섭*

*고려대학교 정보보호대학원

# Train Data Mining Algorithm for RBF-IDS

Il-Gon Park*, Jong-Sub Moon*

*GSIS, CIST, Korea Univ.

## 요 약

현재 침입탐지 시스템은 인터넷의 확장과 더불어 네트워크 보안을 보장하기 위한 광범위한 수단으로 이용되고 있다. 이러한 탐지 시스템중 신경망의 적용은 분산된 네트워크와 다양한 공격환경하의 오용탐지와 비정상행위 탐지에 좋은 응용이 되고 있다. 본 연구에서는 RBF-신경망을 이용한 침입탐지 시스템이 가지고 있는 단점 중 하나인 학습데이터의 공격과 정상의 비율에 따라 탐지 율의 차이가 큰 것에 착안, 보다 자동화되고 안정된 학습을 위한 데이터 결정 알고리즘을 제안한다.

## I. 서론

침입탐지시스템(IDS)은 광범위한 네트워크에의가용성과 기밀성, 무결성을 보장하기 위한 수단으로 널리 사용되고 있는 도구이다. 침입탐지시스템은 보호하고자 하는 대상시스템(사용자계정, 파일 시스템, 시스템커널 등)의 종류에 따라 네트워크 기반과 호스트 기반으로 분류되며, 탐지 방법에 따라 오용탐지(misuse detection)와 비정상행위 탐지(anomaly detection)로 구분된다[1][2]. 오용탐지란 사전에 알려진 공격행위에 대한 정보를 룰 집합으로 구성, 탐지시스템에서 룰과 실제 네트워크 정보의 매칭을 통하여 침입을 탐지하는 방식을 말한다. 비정상행위 탐지란 정상적인 시스템 혹은 네트워크의 정보를 기준으로, 이에 벗어나는 행위를 탐지하는 방식을 말한다. 대부분의 침입탐지시스템은 전자인 오용탐지 방식을 사용하고 있으나 단순 패턴 매칭을 통한 침입탐지 방식은 침입의 증가에 비례하여 설정해야 할 룰 또한 증가하게 되므로, 저장매체의 제약과 알려지지 않은 공격에 대한 적응력이 부족한 단점을 가지고 있다.

### 1. 신경망을 이용한 침입탐지시스템

신경망은 정상과 공격데이터로 학습데이터를 구성하여 오용탐지와 비정상행위 탐지를 동시에 수행하는 분류를 위한 알고리즘이다. 패턴매칭 시스템의 룰과 비교되는 학습이라는 방법을 통해 정상데이터를 일반화하여, 이에 벗어나는 범주를 탐지하는 비정상행위 탐지와 비정상행위들을 일반화하여, 이에 속하는 범주를 탐지하는 오용탐지, 모두를 수행할 수 있다.

신경망을 이용한 침입탐지시스템은 다음과 같은 장점을 가져올 수 있다.

· 범위성과 효율성: 범위성이란 환경변화에 따른 제약사항에 비교적 강하다는 뜻이다. 신경망은 기존 탐지 시스템에서 행하여지는 알려진 공격에 대한 룰 설정을 대체 할 수 있으며, 이에 따른 부가적인 정보의 저장이 필요 없기 때문에, 공격 환경의 변화에 따른 영향을 덜 받는 장점을 가지고 잇다.

· 공격에 대한 적응력과 편의성: 신경망은 새로운 공격의 발견에 따른 업데이트의 필요성을 학습을 통한 일반화로 해결한다. 그러므로 수동적인 업데이트로 인한 부가비용이 들지 않으며, 공격의 탐지를 위하여 오용탐지와 비정상행위 탐지, 두 가지 방식 모두를 수행할 수 있으므로 공격의 탐지를 위한 대처능력과 적응력이 우수하다.

반면, 신경망의 학습을 통해 이뤄지는 일반화는 학습데이터의 구성에 영향을 많이 받게 된다. 즉, 정상과 공격데이터의 비율에 따라 false alarm성도가 크게 차이가 나며, 적정 수준의 학습 성도를 경험적으로 찾아야하는 어려움이 존재한다. 이에 본 연구에서는 RBF-신경망에서 학습데이터의 적절한 비율과 수를 조절할 수 있는 알고리즘을 제안한다.

2장에서는 본 연구의 동기를 제공한 선행 연구사항에 대하여 알아보며, 3장에서는 RBF신경망의 기본 학습과 구조에 대하여 서술하며, 4장에서는 본 연구에서 제안한 학습데이터 결정알고리즘과 그 효율성에 관해 알아본다. 5장에서는 결론 및 향후과제에 대하여 언급한다.

## II. 선행 연구

본 연구의 선행연구로서 RBF-신경망을 이용한 침입탐지시스템이 제안되었다[4]. 이는 다양한 특성을 보유한 공격자의 속성과 분산된 네트워크 환경에서의 알려지지 않은 공격에 대한 침입탐지를 위하여 우회공격도구인 fragrouter를 이용하여 실험하였으며, 네트워크의 가용성 증가에 따른 다량의 데이터 수용의 문제를 결정계수(R-square)값의 측정을 통하여 해결하려고 시도하였다.

선행연구에서 제안된 침입탐지시스템의 구조는 다

음과 같다.

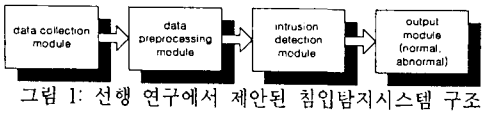


그림 1: 선행 연구에서 제안된 침입탐지시스템 구조

제안된 침입탐지시스템은 데이터 수집, 결정계수를 이용한 데이터 선 처리, 침입 탐지, 출력모듈로 구성되었으며, 우회도구 공격의 탐지를 위한 실험 결과, 96%이상의 높은 탐지 율을 보여주었으나, 비정상을 정상으로 판별하는 false positive가 높은 단점이 존재하였다. 이는 RBF에서 사용되는 학습데이터의 비율과 양의 판단이 수동적인 경험적 요소에 의해 결정되는 문제점을 제기하였다.

## III. RBF-신경망 침입탐지시스템

RBF는 빠른 훈련과정과 일반화 능력, 구조적인 단순함으로 다양한 분야에서 연구가 진행 중이다. 불명확한 입력에 대한 일반화 능력이 우수하며, 일반적으로 복잡하다고 인식되는 분류 문제에 효과적이어서 침입탐지시스템으로의 응용은 전망 있는 분야 중 하나이다[4][5]. 또한 빠른 훈련과정으로 시스템의 자원소모를 최대한 줄일 수 있으며, 사용의 간편함으로 탐지시스템의 유지와 설정, 업데이트로 인한 부가 비용이 필요 없다는 장점을 가지고 있다.

RBF는 구조는 다음과 같다.

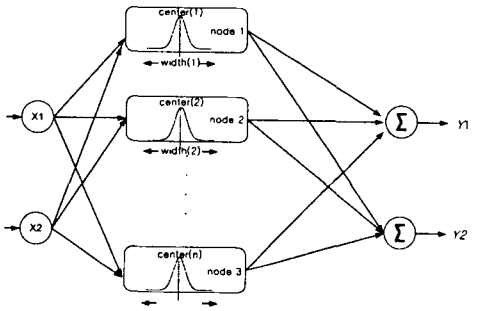


그림 2: RBF의 구조

RBF의 구조는 적용 될 데이터의 입력을 받는 입력 층과 가우시안 함수가 적용되는 은닉 층, RBF의 결과를 출력하는 출력 층으로 구성되는, 신경망에서 가장 널리 쓰이고 있는 feed-forward구조를 가지고 있다[6]. 모든 입력 값들은 normalize를 통해 은닉 층으로 전달되며 식(1)의 가우시안 함수를 통해 식(2)와 같은 형태로 출력 층으로 전달된다.

$$h_{j(x)} = \exp\left(\frac{-\|x-u\|^2}{\sigma_j^2}\right) \quad (1)$$

$x$ :입력 벡터, $u_j$ :가우시안중심

$\sigma_j$ : *receptivefield*의 *width*

$$f(x) = \sum_{j=1}^{m} w_j h_j(x),\ m : \text{은닉층의 갯수} \quad (2)$$

$w_j$ :가중치 행렬, $h_j(x)$ :은닉층의 출력값

RBF는 오용탐지 방식의 패턴매칭 침입탐지시스템의 룰과 비교되는 다음과 같은 학습이 사용된다.

1. 가우시안 함수의 중심위치 학습

가우시안 함수의 중심위치와 가우시안 함수의 영향력을 의미하는 receptive field크기의 선정은 많은 논의의 대상이 되고 있다.

다음은 K-means clustering을 이용한 중심위치 선정 방법을 보여준다.

1) 초기 센터의 위치를 랜덤하게 생성
2) 각 센터 별 입력벡터와 초기 센터와의 Euclcadian distance(ED)값 계산
3) 최소 ED값을 기준으로 중심 값 업데이트
4) 1)-3)을 반복 수행

receptive field의 폭은 각 클러스터별 상대적인 위치 값에 대한 평균값을 계산하여, 적용하게 된다.

2. 은닉 층의 가중치 행렬 학습

가우시안 중심과 receptive field의 크기 학습이 끝난 후에 교사 학습에 의해 히든노드의 가중치 행렬을 최적화시키는 작업이다. 이는 다음과 같은 순서로 진행된다.

1) 은닉 층의 가중치 값을 랜덤하게 생성
2) 학습에 사용 할 입력 값을 RBF의 입력 층에 적용
3) (1)식을 통해 은닉 층의 가우시안 값을 계산
4) (2)식을 통해 출력 층 값을 계산 한 후 목표 벡터 t와의 에러 차를 계산, 다음과 같은 식을 통해 가중치 값을 업데이트 한다.

$$w_{ij}(n+1) = w_{ij}(n) + \eta(t_i - y_i)x_i \quad (3)$$

$w_{ij}$ :은닉층 $i$번째노드와출력층 $j$번째노드사이의가중치

$t_j$ :출력층 $j$번째노드의목표값

$y_i$ :출력층 $j$번째노드의 *RBF*에 의한 실제 출력

$\eta$ :가중치의 학습률을 나타내는 상수 값

5) 학습에 사용 할 모든 데이터들에 대해 1)-4)과정을 반복
6) 사용자에 의해 입력된 최소 에러 값에 도달 시 종료

그림 3은 위에서 서술한 가우시안 중심위치와 은닉 층의 가중치 행렬학습을 기화학적인 모형으로 보여준다.

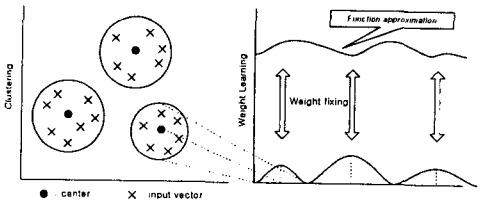


그림 3: RBF 학습방식의 기하학적 위상

## IV. RBF 학습데이터 결정 알고리즘

본 연구에서는 RBF의 침입탐지시스템으로의 적용시 학습데이터의 양에 따른 탐지 율과 false alarm 정도의 변화에 따른 수동적인 학습 방법의 단점을 보완하기 위하여 RBF의 내부 변수를 사용하여 학습데이터의 정상, 공격데이터 비율과 그 수를 결정할 수 있는 학습데이터 결정 알고리즘을 제안한다.

RBF를 사용한 침입탐지시스템에서 알고리즘이 적용되는 위치는 다음 그림 4와 같다.

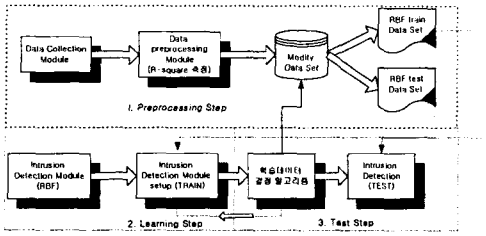


그림 4: 학습데이터 결정알고리즘의 위치 구성도

RBF 학습데이터 결정알고리즘은 모든 학습데이터를 2장에서 언급한 학습방법과 동일하게 1회 실행 후 적용된다. 먼저 1회 학습을 함으로서 은닉 층에 대한 가우시안 센터와 receptive field 크기가 계산되며, 이를 학습데이터 결정알고리즘의 입력 값으로 대입, 출력으로는 새로운 학습데이터를 구성하게 된다. 이를 다시 RBF를 이용해 학습시킨 후 시험데이터를 적용하여 정상, 비정상 판별 실험을 하게 된다.

그림 5는 학습데이터 결정알고리즘을 보여준다.

그림 5: 학습데이터 결정알고리즘

학습데이터 결정알고리즘은 은닉 층의 가우시안 중심을 기준으로 1회 학습을 통해 결정된 receptive field의 크기에 벗어나는 학습데이터를 제거하는 목적으로 만들어졌다. 이렇게 제거되는 데이터는 그림 3

Input: Gausian center, width, train data set
Output: To remove train data

Procedure:
1) compute max, min center
2) compute (max center - min center)/2
3) For each train data
if( $\Sigma$|max - min)/2 - a train data|
< width)
remove a train data
4) Create new train set

RBF 학습의 기화학적 위상에서 보듯이 센터를 기준으로 한 반경을 벗어남으로서 학습 수행 시 저해가 되는 요소로 작용된다. 이는 학습의 효율성과 일반화된 결과의 신뢰성을 떨어뜨리게 된다. 그러므로 이러한 요소들의 제거를 통하여 결정된 학습데이터를 RBF를 이용한 침입탐지 시스템에 적용되는 입력 값으로 사용하여 학습함으로서, 실제 시험데이터를 이용하여 실험 시 나타나는, 실제 침입이 아닌데도 불구하고 침입으로 판정하는 false positive와 실제 침입임에도, 이를 탐지하지 못하는 false negative의 정도를 현실적으로 줄일 수 있을 것이다. 이는 전체적인 탐지 율에도 영향을 미칠 수 있을 것이다.

## V. 결론 및 향후과제

본 연구에서는 RBF-신경망을 이용한 침입탐지시스템에서 학습 시 적용될 수 있는 학습데이터 결정알고리즘을 제안하였다.

학습데이터 결정알고리즘을 통해 기대되는 효과는 다음과 같다.

- RBF-신경망 학습데이터의 정상, 공격데이터 비율에 따른 탐지 율의 false alarm를 줄일 수 있다.
- 불필요한 학습데이터를 자동적으로 제거함으로서, 학습의 자동화와 데이터 처리성능의 증대를 가져올 수 있다.

위의 기대효과를 실질적으로 확인하기 위하여 본 연구의 향후과제로, 실험을 통한 알고리즘의 평가와 분석이 요구된다.

## VI. 참고문헌

[1] Anup K. Ghosh, Aaron Schwartzbard, "A study in using neural network for anomaly and misuse detection." In Proceedings of the 8th USENIX Security Symposium, August 1999.

[2] Kumar, S., Spafford, E. "A Software Architecture to Support Misuse Intrusion Detection", Department of Computer Sciences,Purdue University; CSD-TR-95-009, 1995.

[3] 박일곤, 문종섭, "원시데이터 축약알고리즘을 이용한 신경망의 침입탐지시스템으로의 접근", 한국정보과학회, 2002년 11월.

[4] P.A Porras, R.A Kemerer, "Penetration state transition analysis - a rule-based intrus ion detection approach." In Eighth Annual Computer Security Applications Conference, pages 220-229. IEEE Computer Society Press, November 1992.

[5] R. Heady, G. Luger, A. Maccabe, M. Servilla. "The architecture of a network level intrusion detection system. Technical report", Computer Science Department, University of New Mexico, August 1990.

[6] Fox, Kevin L., Henning, Rhonda R., Reed, Jonathan H. "A Neural Network Approach Towards Intrusion Detection.", In Proceedings of the 13th National Computer Security Conference, 1990.