원시데이터 축약 알고리즘을 이용한 신경망의 침입탐지시스템으로의 접근

박 일 곤O, 문 종 섭*

*고려대학교 정보보호기술연구센터

{cist_gon, jsmoon}@korea.ac.kr

Neural network with audit data reduction algorithm for IDsystem

Il-gon Park, Jong-sub Moon

*CIST, Korea Univ

요 약

현재 인터넷의 발달에 인한 다양한 공격의 가능성의 이유로 침입 탐지 시스템(IDsystem, IDS)의 중요성은 날로 커지고 있으며 네트워크의 보안을 보장하기 위한 방안으로서 널리 이용되고 있다. 그러나 작은 네트워크 환경에서도 IDsystem에 적용되는 audit data의 양이 많아짐으로서 시간당 처리속도와 IDsystem의 설정을 위한 시간이 더욱더 요구되며 전체적인 효율성이 감소하게 된다. 본 연구에서는 IDsystem으로 빠른 훈련과정과 일반화 능력, 구조적인 단순함으로 다양한 분야에서 연구가 진행 중인 신경망 모델 중 하나인 Radial Basis Function(RBF)를 사용하였으며, 효율성 제고를 위하여 RBF에 적용 할 입력 값들의 중요성을 선 처리 단계에서 판별하여 불필요한 입력 값들을 축약하기 위해 결정계수(R-square)값을 측정, 알려지지 않은 공격과 알려진 공격들을 판별 할 수 있는 IDsystem을 제안하였다.

I. 서론

침입 탐지 시스템는 광범위한 네트워크의 가용성과 기밀성, 무결성을 보장하는 수단으로 널리 사용되고 있는 도구이다. 초기 침입을 막기 위한 기술들은 패스워드를 이용한 유저 인증과 프로그램 자체의 버그 방지, 암호화를 통한 정보보호와 같은 방법이 주류를 이루었다. 그러나 단순한 침입 방지만으로는 인터넷의 발전으로 인한 네트워크 가용성의 증가와 다량의 데이터를 수용하기에는 역부족이었으며, 그에 따른 침입의 증가에 대응하기에는 충분치 않았다. 이에 대한 보완의 필요성에 의해 침입 탐지 시스템이 대두되었다.

현재 악의를 가진 공격자의 침입을 탐지하는 기술로 크게 오용 탐지(misuse detection)와 비정상 행위 탐지(anomaly detection)로 나눌 수 있다[1][2]. 오용탐지란 사전에 여러 시스템들의 알려진 취약점들을 이용하여 공격하는 행위들에 대한 정보를 DB화하여 침입 탐지 시스템에 적용, 탐지하는 방법을 말하며, 비정상 행위 탐지란 정상적인 시스템 사용에 관한 프로파일이나 상태정보를 이용하여 이것에 벗어난 행위들을 탐지하는 방법을 말한다. 현재 대부분의 침입 탐지 시스템에서는 단순한 오용 탐지방식의 패턴 매칭이 자주 사용되고 있으나 다양한 특성을 보유한 공격자의 속성과 분산된 네트워크 환경 하에서의 침입 탐지와 알려지지 않은 공격에는 실제 침입이 아닌데도 불구하고 침입으로 판정하는 false positive와 실제 침입을 정상적인 행위로 탐지하는 false negative의 정도가 높은 실정이며 탐지에 큰 효과를 보지 못하고 있는 게 사실이다.

본 연구에서는 이러한 침입 탐지에의 어려움에 착안하여 패턴인식과 분류의 문제에 좋은 효과를 보여주는 신경망 알고리즘 중 하나인 Radial Basis Function(RBF)을 사용하여 알려지지 않은 다양한 공격에의 탐지를 위하여 비정상 행위 탐지방식으로 실험을 진행하였으며, 보다 효율적인 데이터 처리를 위하여 변수 선택 알고리즘 중 하나인 결정계수(R-square)값을 측정하여 선택된 변수를 RBF의 입력 값으로 사용하였다.

본 논문의 구성은 다음과 같다. 2장에서는 기존의 신경망을 이용한 침입 탐지 시스템들의 연구 상황을 알아보고 3장에서는 본 연구에서 제안한 침입 탐지 시스템의 모듈들을 살펴본다. 4장에서는 실험과 결과분석을 서술하였으며, 5장에서는 결론 및 향후연구 과제를 기술하였다.

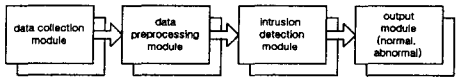
II. 관련 연구

침입 탐지 시스템은 분산된 네트워크와 다양한 공격의 현실을 고려 해 볼 때 탐지기법으로 비 정상행위 탐지 기술 방향으로 많은 연구가 진행 중이며 다양한 모델이 제안되고 있다. 본 연구에서처럼 침입 탐지의 오용 탐지나 비정상 행위 탐지를 위한 신경망의 응용은 전망 있는 기술 중에 하나로 볼 수 있다.

현재 신경망을 이용한 침입 탐지에 대한 연구를 살펴보면 Georgia Technical Research Instituite의 Multi layer Perceptron(MLP)를 이용한 ISS scan, SATAN scan, SYN Flooding 공격 탐지, MIT의 Lincoln lab의 Unix 호스트와 root계정에 위협을 주는 공격을 탐지하기 위한 MLP를 이용한 오용탐지, UBILAB의 SOM를 이용한 네트워크 클러스트링을 이용한 공격탐지 등의 연구가 이루어 졌다.

III. 침입 탐지 시스템

본 연구에서는 IDsystem 우회도구인 fragrouter를 이용한 공격을 탐지하기 위한 모델을 제안한다. 다음은 본 연구에서 제안된 탐지 모듈의 구성이다.



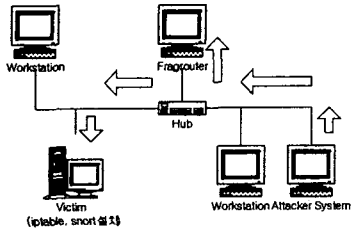
〔그림 1〕 침입탐지 시스템 구성

제안된 침입 탐지 시스템은 데이터 수집, 데이터 선 처리, 침입 탐지, 출력

모듈로 구성된다. 그 중 결정계수(Coefficient of Determination; R^2)값을 이용하여 정상과 비정상에 영향을 미치는 입력변수를 선택하는 방법인 데이터 선 처리과정과 침입 탐지 모듈인 RBF가 공격을 탐지하기 위한 본 연구의 핵심이다.

3.1 데이터 수집

본 연구에서는 IDsystem 우회도구 탐지를 위하여 다음 그림과 같은 실험 환경을 구축하여 데이터를 추출하였다.



[그림 2] 데이터 추출을 위한 실험 환경

가상공격 시뮬레이션을 설정하여 LAN을 통해 TCP/IP 덤프데이터를 수집하였으며 그 종류 및 공격 특성은 다음 표1과 같다.

[표 1] fragrouter를 이용한 공격

사용 fragrouter옵션	공격 내용 및 특성
frag-1	비정상적으로 작게 fragment된 tiny fragmentation공격
frag-3	tiny fragmentation공격 + fragmentation의 순서변경을 통한 공격
frag-4	tiny fragmentation공격 + teardrop공격
frag-5	tiny fragmentation공격 + 패킷의 순서 변경 공격 + teardrop공격
frag-6	tiny fragmentation공격 + 마지막 fragmentation을 가장 먼저 보내는 공격
frag-7	tiny fragmentation공격 + NULL data를 이용한 teardrop공격

3.1.1 fragrouter를 이용한 IDsystem우회

fragrouter는 기존의 패턴 매칭 IDsystem의 탐지 알고리즘의 단점을 이용하여 우회하는 방법을 제공하는 도구로서 공격자 시스템으로부터 입력되는 모든 패킷을 표1에서 정의 한 공격 유형에 따라 단편화한 다음, 침입 탐지 시스템이 보호하는 영역의 네트워크로 패킷을 전달하는 역할을 한다. 본 연구에서는 fragrouter통한 비정상적인 ping데이터를 이용한 우회를 탐지하는 실험을 4장에서 논의한다.

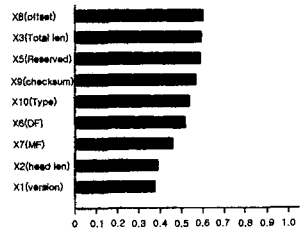
3.2 데이터 선 처리

데이터 선처리라 함은 tcpdump를 통해 취득한 데이터를 침입 탐지 시스템(RBF)의 입력 값으로 사용 될 변수로 바꾸는 과정을 일컫는다. 이 과정은 침입 탐지 시스템의 방대한 데이터 처리로 인한 오류와 탐지 모듈의 정상과 비정상 판별에의 효율성을 위한 것으로, 너무 많은 변수의 사용은 공격과 정상의 판별의 모호성을 제공 할 소지가 있다. 따라서 본 연구에서는 경험적으로 정상/비정상 판별에 영향을 주는 변수 군을 선택한 후 입력 변수와 목표변수(정상/비정상)간의 결정계수(R^2)를 이용하여 최종 입력 변수를 선정하는 방법을 사용하였다. 결정계수란 목표 변수의 분산 중 입력 변수에 의해 설명되는 분산의 비율을 의미하는 것으로 식(1)과 같다.

$$R^2_p = \frac{SSR_p}{SST} \qquad (1)$$

SST:총변동, SSR_p:p변수의변동의크기

이 값은 0에서 1까지의 값을 가지며, 1에 가까울수록 입력 변수가 목표 변수에 대한 기여도가 높다는 것을 의미하며, 모든 가능한 변수에 대한 R^2값을 계산한 후 그 값에 대한 증가폭이 그다지 크지 않은 시점에서 입력 변수를 선택하는 것이 바람직하다. 이와 같은 변수 선택의 결과에 근거하여 침입 탐지 모듈의 입력 값으로 사용 할 요소를 추출 한 결과와 변수들의 R^2값은 다음과 같다.



[그림 3] 추출된 입력변수의 R^2값

[표 2] 최종 선택된 입력변수의 형태 예제

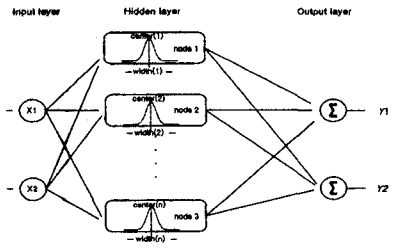
입력변수	입력 값
IP version	4
Header length	5
Total length	68
Reserved	0
DF	0
MF	1
fragment offset	8
IP checksum	3246
ICMP Type	8

위의 결과는 IP, ICMP프로토콜 헤더의 12개 변수 중 최종 입력변수로 선택된 결과를 나타내고 있다.

3.3 침입 탐지 모듈(RBF)

침입 탐지를 위한 모델로서 빠른 훈련과정과 일반화 능력, 구조적인 단순함으로 다양한 분야에서 연구가 진행 중인 신경망 모델 중 하나인 RBF를 사용하였다. 불명확한 입력에 대한 일반화 능력이 우수하며[3][4], 일반적으로 복잡하다고 인식되는 분류 문제에 효과적이어서 fragrouter와 같이 알려지지 않은, linear하게 구분 할 수 없는 복잡한 형태의 공격을 탐지하기에 적합하고 빠른 훈련과정으로 시스템의 자원소모를 최대한 줄일 수 있으며, 사용의 간편함으로 IDsystem의 유지와 설정, 업데이트 등의 부가 비용이 필요 없다는 것에 착안하여 선택하게 되었다.

RBF의 구조는 적용 될 데이터의 입력을 받는 입력 층과 Gaussian basis function이 적용되는 은닉 층, RBF의 결과를 출력하는 출력 층으로 구성되는 신경망에서 가장 널리 쓰이고 있는 그림 4와 같은 feedforward구조를 가지고 있다[5].



[그림 4] RBF의 구조

모든 입력 값들은 normalize화를 통해 은닉 층으로 전달되며 식(2)의 함수의 결과를 바탕으로 식(3)과 같은 형태로 출력 층으로 전달된다.

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

x : 입력 벡터, u_j : 가우시안센터

σ_j : *receptivefield*의 *width*

$$f(x) = \sum_{j=1}^{m} w_j h_j(x),\ m : \text{은닉노드의 갯수} \qquad (3)$$

w_j : 가중치 행렬, $h_j(x)$: 은닉노드의 출력값

IV. 실험 및 결과 분석

앞서 소개된 데이터수집과 선 처리과정을 거친 입력벡터들을 RBF의 입력노드에 적용, 그 결과로서 각 패킷 당 정상은 1, 비정상은 0이라는 클래스 라벨 값을 통하여 정상과 비정상을 판별하였다.

RBF의 학습을 위하여 정상 데이터 1000개와 비정상 데이터1000개를 구성, 총 2000개의 데이터를 사용하였으며, 테스트를 위해 정상과 비정상 패킷 각 50개를 구성하여 실험을 진행하였다. 다음 표3은 침입탐지의 결과를 보여준다.

[표 3] 침입 탐지 결과

테스트 결과	실험1	실험2
RBF학습용 데이터 수	2000 (1000/1000)**	2000 (1000/1000)
RBF테스트용 데이터 수	100 (50/50)	100 (50/50)
입력 변수의 수	12	9
변수 선택 알고리즘	·	결정계수
잘못된 분류의 수	2	4
정확도	98%	96%

**(정상/비정상)

상기 표는 히든노드의 개수를 바꾸어가며 100회의 실험 후, 평균적인 탐지 정확도를 나타낸 것으로 실험1은 축약 알고리즘을 적용하지 않은 12차원의 입력벡터를 사용한 것이고 실험2는 R-square알고리즘을 통해 선택된 9차원의 입력벡터를 RBF에 적용한 경우이다. 전체적으로 비슷한 성능을 가지며, 데이터 축약이라는 선 처리 작업이 많은 양의 데이터를 처리하는 탐지 시스템에 적용될 수 있는 가능성을 보여준다.

잘못된 분류는 실험1, 실험2 모두 비정상을 정상으로 판별하는 false positive였으며 이는 RBF의 학습을 위한 데이터 양이나 비율의 적절한 조절로 줄일 수 있을 것으로 보인다.

V. 결론 및 향후과제

본 연구에서는 원시데이터의 축약을 응용, 신경망을 이용한 침입 탐지 시스템을 제안하였다. 정상과 공격에 영향을 미치는 의미 있는 입력벡터들을 사용하여, 탐지 시스템을 위한 설정 시간을 줄였으며, 잘 알려진 공격의 변형을 통해, 단순 패턴 매칭 시스템을 우회하는 공격도구를 탐지하기 위하여 빠른 훈련과정과 분류능력이 뛰어난 RBF를 사용하여 높은 탐지 율을 보여주었다.

그러나, RBF의 학습을 위해 사용되어지는 데이터 양의 판단이 수동적으로 이루어짐으로서 false positive가 높아지며, 적절한 학습데이터 양의 판단이 힘든 경향을 실험에서 보여주었다. 이에 향후 과제로서 학습데이터의 양을 자동적으로 판단해 주는 알고리즘을 통해 false positive를 낮추는 연구를 할 것이며, 우회공격뿐만 아니라 DOS와 같은 여러 공격들에 대한 실험을 병행할 것이다.

VI. 참 고 문 헌

[1] Anup K. Ghosh and 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] P.A Porras and R.A Kemmerer. Penetration state transition analysis - a rule-based intrusion detection approach. In Eighth Annual Computer Security Applications Conference, pages 220-229. IEEE Computer Society Press, November 1992.

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

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