진화신경망을 이용한 프로그램 행위학습 및 비정상행위탐지

한상준○, 조성배
연세대학교 컴퓨터과학과
{sjhan, sbcho}@sclab.yonsei.ac.kr

Anomaly Detection and Learning of Program Behaviors with Evolutionary Neural Networks

Sang-Jun Han and Sung-Bae Cho
Dept. of Computer Science, Yonsei University

요 약

시스템 호출 감사자료기반 기계학습기법을 사용한 프로그램 행위 학습방법은 효과적인 호스트기반 침입탐지 방법이며, 특히 신경망은 기존 연구중 가장 좋은 성능을 보였다. 하지만 보통의 신경망은 그 구조를 찾기 위한 방법이 알려져 있지 않아 침입탐지에 효과적인 구조를 찾기 위해서는 많은 시간이 요구된다. 본 논문에서는 기존 신경망 기반 침입탐지시스템의 단점을 보완하고 성능을 향상시키기 위해 진화신경망을 이용한 방법을 제안한다. 진화 신경망은 신경망의 구조와 가중치를 동시에 학습하기 때문에 일반 신경망보다 빠른 시간내에 더 좋은 성능의 신경망을 얻을 수 있다는 장점이 있다. 1999년의 DARPA IDEVAL자료로 실험한 결과 기존의 연구보다 좋은 성능을 보여 진화신경망이 침입탐지에 효과적임을 확인할 수 있었다.

1. 서론

호스트기반 비정상행위 탐지에는 프로그램의 행동을 분석하는 방법이 많이 사용되고 있다. 정상 프로그램의 행동을 학습하고 이와는 상이한 행동을 침입으로 잡아내는 문제는 일반적인 인공지능의 이진분류문제로 바꾸어 볼 수 있어 규칙 학습, 신경망, 통계적 방법, 은닉 마크로프 모델 등의 기계학습 방법이 많이 사용되어 좋은 성능을 보였다.

그중에서도 신경망은 호스트기반 침입탐지 방법 중 가장 좋은 성능을 보였다. 그러나 감사자료의 특성상 학습데이터의 크기가 매우 커서 대부분의 기계학습 학습알고리즘으로 많은 계산량이 소요되기 때문에 정상행위 모델링 과정에 있어서 많은 시간을 필요로 하는 단점이 있다. 또한 분류기의 구조와 설정에 따라 성능이 좌우되기 때문에 적합한 가중치, 은닉 노드 수, 위상 구조 등을 설정하는 것이 매우 중요하다. 하지만 적합한 구조에 대한 많은 연구가 진행되었음에도 불구하고 이를 결정하는 정형화된 방법은 알려져 있지 않다[1]. 따라서 대부분의 경우 유사한 응용 분야에서 사용했던 경험에 기반하여 시도와 오류 과정의 반복을 통해서 설계되기 때문에, 기계학습 기법을 이용한 침입탐지는 학습단계에서 매우 많은 시간이 소요되는 단점이 있다.

본 논문에서는 기존 기계학습 기반 침입탐지기법의 단점을 극복하기 위하여 진화신경망을 사용하였다. 진화신경망은 분류기의 구조와 내부의 가중치를 동시에 학습하기 때문에 일반적인 기계학습방법보다 빠른 시간 내에 좋은 성능의 분류기를 얻을 수 있다는 장점이 있다.

2. 관련연구

대부분의 침입은 프로그램의 버그를 이용해 오동작을 유도함으로써 이루어지기 때문에 공격을 받은 프로그램은 정상적인 실행과는 다른 행동을 하게 된다. 따라서 정상적인 프로그램을 학습한 후 이와 다른 행동을 보이는 프로그램을 침입으로 간주하는 방식은 효과적인 비정상행위 탐지 방법이 될 수 있다. 프로그램의 행동을 관찰하는 방법에는 여러 가지가 있지만 호스트기반 침입탐지시스템에서는 주로 프로그램이 사용한 시스템 호출을 기록한 감사자료가 많이 사용되며, 정상적인 프로그램 실행에서 생성된 일정크기의 시스템 호출 시퀀스 데이터를 수집하여 이와는 다른 시스템 호출 시퀀스를 보이는 프로그램을 침입으로 간주한다.

이와 같은 방법을 사용한 연구 중 가장 좋은 성능을 보인 것은 A.K. Ghosh 등의 신경망을 사용한 방법이다[2]. 전통적인 전방향 오류 역전파 알고리즘을 사용하는 다층 신경망과 Elman recurrent 신경망이 사용되었는데 1998년과 1999년의 DARPA IDEVAL 데이터를 사용하여 실험한 결과 Elman 신경망의 성능이 더 뛰어나 신경망의 구조가 침입탐지 성능에 큰 영향을 미치는 것을 확인할 수 있었다. 그러나 이 경우에도 많은 수의 신경망을 학습시킨 후 가장 좋은 것을 선택하는 시행착오에 의한 방법이 사용되어 정상행위 학습에 많은 시간이 소요된다.

3. 진화신경망을 이용한 침입탐지

본 논문에서는 기존 신경망 기반 침입탐지시스템의 단점을 보완하고 성능을 향상시키기 위해 진화신경망을 이용한 방법을 제안한다. 초기 신경망 자동 설계에 관한 연구에서는 다양한 컨스트럭티브(constructive) 알고리즘과 가지치기(pruning) 알고리즘이 사용되었다[1]. 하지만 두 방식 모두 신경망의 전체적인 구조 영역을 검색하는 것이 아니라 주어진 환경에서 제한된 영역만을 탐색하므로 최적화된 신경망을 찾기 어렵다.

이런 한계를 극복하기 위하여 진화 알고리즘이 도입되었다. 진화 알고리즘은 일반적인 모든 탐색 문제에 적용될 수 있으며, 초기 조건에 덜 민감한 전역 탐색 능력을 가진다. 진화 신경망은 진화 알고리즘을 신경망 설계 과정에 도입해서 자동으로 신경망을 결정하는 방법으로 신경망의 가중치, 위상 구조, 은닉 노드 수 등 신경망 학습 시 결정해야 하는 인자들을 여러 세대 진화를 통해 찾아서 최적의 신경망을 결정한다. 그림 1은 진화신경망을 사용한 침입탐지 시스템의 개요를 보여준다.

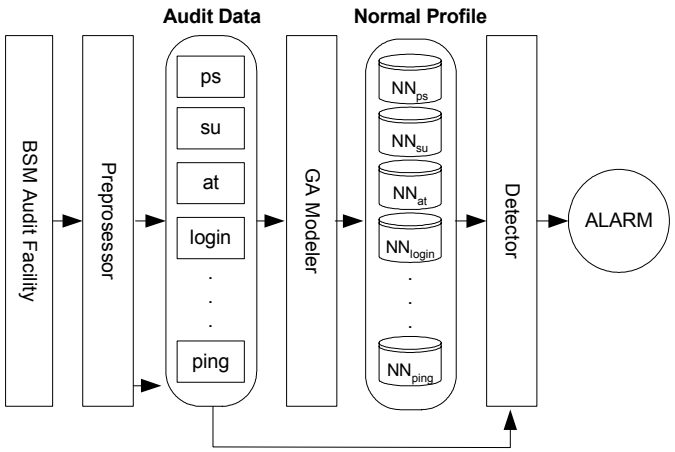

그림 1. 제안하는 방법의 개요

3.1 프로그램 행위 학습

본 논문에서는 시스템 호출 감사자료를 사용하여 프로그램 행동을 관찰하였다. 프로그램 행동학습과 시스템 호출 시퀀스 데이터를 통한 침입탐지는 다음과 같이 정리될 수 있다. 어떤 프로그램이 N개의 시스템 호출 이벤트를 사용하였을 때 모든 이벤트의 집합을 P라고 하고, 시간 t에서 길이 L의 크기로 P를 윈도윙(windowing) 하여 만들어낸 시퀀스의 집합을 S_t라 할 때 P와 S_t는 다음과 같이 표현된다.

$$P = (s_1, s_2, \mathrm{K}, s_N)$$
$$S_t = (s_{t+1}, s_{t+2}, \mathrm{K}, s_{t+L}), t \le N - L$$

여기에서 R_t를 S_t에 대한 시퀀스 평가함수 $eval$을 통해 나온 결과값 이라 할 때, $R_t = eval(S_t)$의 값이 정해진 임계값보다 높은 경우 현재 프로세스는 침입으로 판단된다.

$$alarm(R_t) = \begin{cases} normal & \text{if } R_t \ge threshold \\ attack & \text{if } R_t < threshold \end{cases}$$

프로그램 행위를 학습하기 위해 사용된 신경망의 입력층은 10개의 노드로 이루어져 있으며 여기에는 길이 10으로 윈도윙된 시스템 호출 시퀀스가 입력된다. 출력층은 각각 침입, 정상을 나타내는 2개의 출력노드로 이루어져 있으며 은닉 노드는 모두 15개가 사용되었는데 노드들 사이의 연결 관계는 진화 알고리즘을 이용해서 설정된다.

신경망의 유전자형 표현방법으로는 행렬기반의 표현을 사용하였다. N개의 노드를 가진 신경망은 $N \times N$ 크기의 정방행렬에 연결 정보와 가중치를 동시에 표시하여 나타내어진다. 행렬의 우상단은 노드간 연결 정보를 1과 0으로 표시하고, 각 연결 정보에 대칭하는 좌하단은 가중치를 나타낸다. 그림 2는 4개의 노드와 4개의 연결로 구성된 신경망의 행렬기반 표현의 예를 보여준다. 이 표현방식은 간단하면서도 N개의 노드를 가지는 모든 경우의 신경망을 표현할 수 있고 유전연산자를 적용하기 쉬운 장점이 있다.

유전연산자로는 교차와 돌연변이가 사용되었다. 교차연산은 임의의 은닉노드를 하나 선택한 후 그 노드를 중심으로 두 신경망의 구조를 교환하며, 돌연변이 연산은 임의의 노드를 추가 또는 삭제하는 형태로 이루어진다.

이렇게 표현된 신경망을 학습 데이터로 테스트해 올바르게 분류한 샘플이 많은 신경망이 높은 적합도를 가지도록 인식률을 사용하여 적합도를 계산하였다.

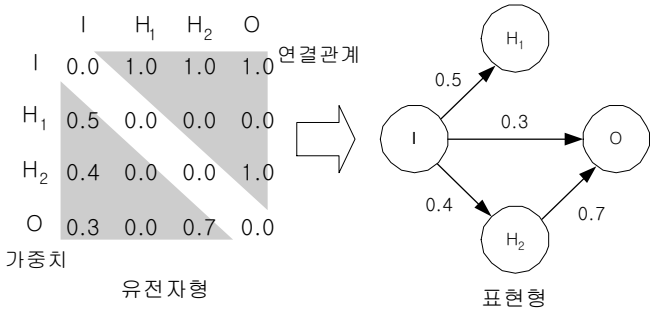

그림 2. 신경망의 표현

3.2 비정상행위 탐지

신경망은 한 개의 시퀀스에 대한 정상, 비정상 여부를 제공하지만 프로세스 전체의 정상, 비정상 여부를 판단해야한다. 이를 위해서는 침입발생시 일어나는 지역적이며 연속적인 평가값 추이의 변화를 탐지해내는 것이 중요하다. 그러기 위해서는 현재 시퀀스의 평가 값 뿐만 아니라 이전 시퀀스의 평가 값도 같이 반영하는 것이 필요한데 본 논문에서는 이를 위해 다음과 같은 방법으로 시퀀스의 평가값을 결정하였다. o_t^1은 침입을 나타내는 출력 노드의 값, o_t^2는 정상을 나타내는 출력 노드의 값, w_1, w_2, w_3는 각 값의 가중치를 나타낼 때, 시간 t의 시퀀스의 평가 값 r_t는 다음과 같은 식에 의해 결정된다.

$$r_t = w_1 \cdot r_{t-1} + w_2 \cdot o_t^1 + w_3 \cdot o_t^2$$

각 프로그램별로 다른 신경망이 사용되므로 침입과 정상행위의 결정경계가 모두 다르다. 따라서 하나의 임계값을 전체 신경망 집합에 사용하는 것은 문제가 있는데 본 논문에서는 이를 해결하기 위하여 통계적인 방법을 사용하여 각 신경망의 평가 값을 정규화하였다. m은 학습데이터 평가 값의 평균, d는 표준편차라 할 때 정규화된 평가 값 R_t는 다음과 같이 계산된다. 이렇게 계산된 R_t값이 정해진 임계값을 넘으면 해당 프로세스는 침입으로 간주된다.

$$R_t = eval(S_t) = \frac{R_t - m}{d}$$

4. 실험 및 결과

BSM 감사자료에는 약 280여개의 시스템 호출 이벤트가 들어있다. 하지만 이를 모두 다 사용할 경우 문제의 복잡도가 너무 커지므로 자주 사용되는 46개의 시스템 호출로 축약하여 사용하였다. 제안하는 기법의 성능을 시험하기 위해 MIT Lincoln Lab에서 제공하는 1999년 DARPA IDEVAL데이터를 사용하였다[3]. 이 데이터는 denial-of-service(DoS), probe, remote-to-local (R2L), user-to-root (U2R)의 4가지 종류의 공격을 담고 있는데 본 논문에서는 프로그램의 오동작을 일으켜 비정상적인 프로그램 행동을 유도하는 U2R공격을 탐지하는데 초점을 두어 실험하였다. 따라서 본 논문에서는 U2R공격의 주된 공격 대상이 되는 SETUID권한을 가지는 프로그램만의 실행을 모니터링 하였는데 모니터되는 프로그램의 수는 총 51가지이다.

1999년 IDEVAL 데이터는 총 5주 분량의 감사자료를 제공하는데 그중 1-3주는 학습 데이터이고 4-5주는 테스트 데이터이다. 본 논문에서는 침입이 들어 있지 않은 1, 3주 데이터를 학습데

이터로 사용하였고 4, 5주를 테스트데이터로 사용하였다. 테스트 데이터에는 4가지종류의 U2R공격이 총 11번 포함되어 있다.

그림 3은 진화신경망의 진화과정을 보여준다. 세대가 거듭될수록 신경망의 적합도가 증가하여 진화알고리즘이 좀 더 좋은 신경망의 구조를 찾아낼 수 있음을 확인하였다. 최대 적합도는 0.9에서 수렴하여 학습데이터를 90%정도 인식률로 분류할 수 있음을 알 수 있었다.

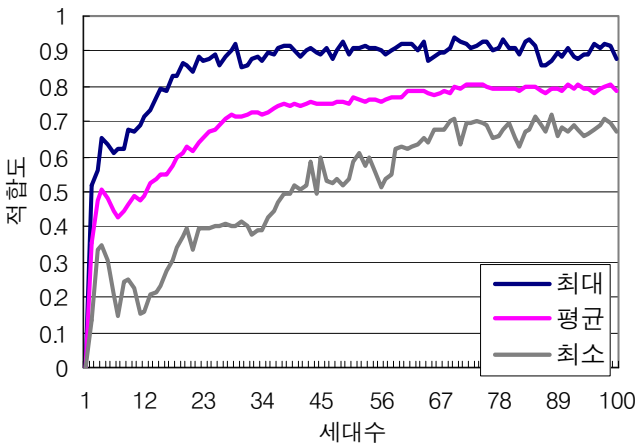

그림 3. 신경망의 진화 과정

일반적인 MLP와 진화신경망의 학습시간을 비교하여 보았다. 실험은 Intel Pentium Zeon 2.4GHz Dual 프로세서, 1GB RAM의 하드웨어와 솔라리스9 운영체제 하에서 10번 실행한 후 평균값을 취하였다. MLP의 경우 은닉노드수를 10부터 60개까지 변화시키며 5000epoch까지 학습시켰고 진화신경망의 경우 15개의 은닉노드를 가지는 20개체의 신경망을 100세대까지 진화시켜보았다. 사용한 데이터는 login프로그램의 학습데이터로 총 1905개의 시퀀스로 이루어져 있다.

표 1. 진화신경망과 일반적인 MLP의 학습시간 비교

종류	은닉노드 수	소요시간(초)
MLP	10	235.5
	15	263.4
	20	454.2
	25	482
	30	603.6
	35	700
	40	853.6
	50	1216
	60	1615
진화신경망	15	4460

실험결과(표 1) 기존의 방법과 같이 각 신경망을 10개씩 학습시킨 후 그중 가장 좋은 것을 선택하는 방법을 쓸 경우 약 17시간 50분이 걸리게 된다. 그러나 진화신경망을 사용한 경우는 약 1시간 14분밖에 걸리지 않았다. 진화알고리즘을 통한방법이 구조를 최적화시킬 수 있는 장점을 가지면서도 학습시간면에서도 기존의 방법보다 나은 것을 알 수 있었다.

그림 4에서는 테스트 결과를 탐지/오경보 그래프로 나타내었다. 100% 탐지율에서 하루에 평균 0.7개의 false alarm을 나타내었다. 1999년 DARPA IDEVAL 데이터를 사용한 연구 결과 중 U2R공격 탐지에 가장 좋은 성능을 보인 것은 A.K. Ghosh 등의 시스템 호출 감사자료와 Elman 신경망을 사용한 방법이었다[4]. 이 탐지 시스템은 100% 탐지율에서 하루에 3개의 false alarm을 보였다[2]. 이와 비교해 보았을 때 진화 알고리즘을 이용해 신경망의 구조를 결정하는 것이 시행착오를 통해서 결정하는 것보다 더 짧은 시간 안에 효과적인 구조를 찾아낼 수 있음을 확인하였다.

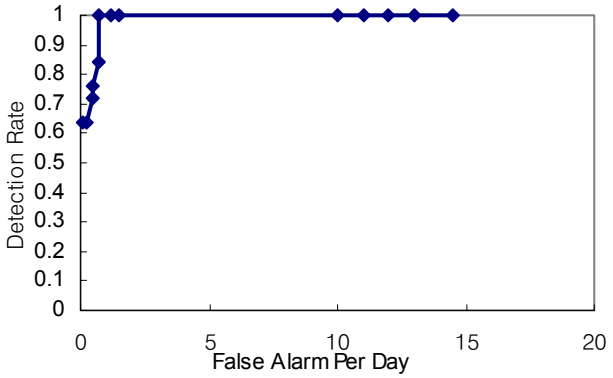

그림 4. 제안한 탐지 방법의 성능

5. 결론

본 논문에서는 기존의 신경망 기반 비정상행위탐지 방법의 단점을 극복하기 위하여 진화 신경망을 사용하는 방법을 제안하였다. 제안한 침입탐지 방법은 분류기의 구조와 가중치가 진화 알고리즘에 의해 동시에 학습되므로 기존의 고정된 구조를 사용하는 방법보다 더 좋은 성능을 기대할 수 있는데 실제 벤치마크 데이터에 의한 테스트에서 기존의 방법보다 좋은 결과를 보였다. 향후 연구로는 진화된 신경망의 구조를 분석하여 침입탐지에 좋은 구조가 어떤 것인지 밝혀내는 작업이 필요하겠다. 또한 종분화 방법에 의해 진화된 상호보완적인 다중 신경망을 결합하는 방법을 이용하면 좀 더 좋은 성능을 기대할 수 있을 것이다.

감사의 글

본 연구는 대학 IT 연구센터 육성/지원사업의 연구결과로 수행되었음.

참고 문헌

[1] X. Yao, “Evolving Artificial Neural Networks,” *Proceedings of the IEEE*, vol. 87, no. 9, pp. 1423-1447, 1999.

[2] A. K. Ghosh, C. C. Michael, and M. A. Schatz, "A Real-Time Intrusion Detection System Based on Learning Program Behavior," *Proc. of the Third Int. Workshop Recent Advances in Intrusion Detection*, pp. 93-109, 2000.

[3] MIT Lincoln Laboratory, "DARPA Intrusion Detection Evaluation", Available from <http:://www.ll.mit.edu/IST/ideval/index.html>

[4] R. Lippmann, J. Haines, D. Fried, J. Korba, and K. Das, "The 1999 DARPA Off-Line Intrusion Detection Evaluation," *Computer Networks*, vol. 34, no. 4, pp. 579-595, 2000.