Self-Organizing Feature Maps 기반 IP 패킷의 웜 탐지에 관한 연구

민동옥° 손태식 문종섭
고려대학교 정보보호기술연구센터
{eieshine°, tssohn, jsmoon}@cist.korea.ac.kr

A Study on the Worm Detection in the IP packet based on Self-Organizing Feature Maps

Dong-Og Min° Taeshik Shon Jong-Sub Moon
CIST, Korea University

요 약

급증하고 있는 인터넷 환경에서 정보보호는 가장 중요한 고려사항 중 하나이다. 특히, 인터넷의 발달로 빠르게 확산되고 있는 웜 바이러스는 현재 바이러스의 대부분을 차지하며, 다양한 종류의 바이러스들과 악성코드들을 네트워크에 전파시키고 있다. 지금 이 순간도 웜 바이러스가 네트워크를 통해 확산되고 있지만, 웜 바이러스의 탐지가 응용레벨에서의 룰-매칭 방식에 근거하고 있기 때문에 신종이나 변종 웜 바이러스에 대해서 탐지가 난해하고, 감염된 이후에 탐지를 할 수 밖에 없다는 한계를 가지고 있다. 본 연구에서는 신종이나 변종 웜 바이러스의 탐지가 가능하고, 네트워크 레벨에서 탐지할 수 있는 신경망의 인공지능 모델 중 SOFM을 이용한 웜 바이러스 탐지 방안을 제시한다.

1. 서 론

인터넷의 빠른 확장과 성능 향상으로 기존의 디스크를 옮겨 다니던 바이러스는 네트워크의 취약성과 e-mail등을 이용해 스스로 전파하는 바이러스로 발전하게 되었다. 웜 바이러스라 부르는 자가 복제 및 중식 능력이 있는 이 코드들은 감염된 호스트에서 다음 목표를 찾아서 바이러스를 감염시키는 일련의 동작들을 행한다. 감염된 호스트의 피해는 그리 크지 않지만, 감염된 호스트의 속도저하, 감염된 호스트가 속한 네트워크의 속도저하 등 피해가 확산되면, 네트워크 전체를 다운시킬 수 있을 정도의 위력을 지닌다. 최근 웜 바이러스의 침투기법이 다양해지면서, 운영체제 취약점을 이용한 버퍼 오버 플로우 기법, e-mail 첨부파일을 이용한 기법 외에도 윈도우의 파일공유를 통한 기법, 특정 응용프로그램 취약점을 통한 기법, 그리고 위에 열거한 여러 가지 침투를 동시 다발적으로 시도하는 하이브리드 기법들이 생겨났다.

웜 바이러스는 현재 응용레벨에서 특정 문자열이나 룰을 매치시켜서 탐지하는 방법이 일반적이다. 그러나 이러한 탐지 방법은 첫째, 신종이나 변종 바이러스를 탐지하지 못하고 둘째, 응용레벨에서 탐지하기 때문에 바이러스가 감염된 이후에 탐지가 된다는 단점이 있다. 본 논문에서는 이러한 단점을 극복하기 위해 TCP/IP 헤더에 신경망 SOM을 적용하여 웜 바이러스를 네트워크 레벨에서 탐지하는 모델을 제시한다.

본 논문의 구성은 다음과 같다. 2장에서는 SOM의 특징 및 개요에 대해서 설명하고, 3장에서는 SOM에 적용하기 위한 IP 헤더의 ID 필드에 있는 특성 데이터의 전처리 과정을 설명한다. 4장에서는 SOM과 전처리된 데이터를 이용한 웜 바이러스 탐지방안을 제시하고, 5장에서는 SOM을 통한 실험을 수행한다. 그리고, 마지막 6장에서는 본 논문의 결론 및 향후 연구과제에 대해서 제시한다.

2. Self-organizing Feature Maps (SOM)

2.1 SOM 개요

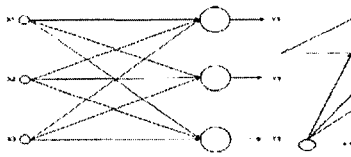
SOM은 Self Organizing Map 의 약자로 헬싱키 공과대의 튜보 코호넨(Teuvo Kohonen)에 의해 제안되었다. SOM은 자기조직화(self-organizing)라는 말 그대로, 주어진 입력 패턴에 대한 정확한 해답을 미리 주지 않고 자기 스스로 학습할 수 신경망 모델이다. 이 모델은 음성인식, 문자인식, 구문분석 등 다양한 분야에 응용되며, 입력 Layer와 출력 Layer로만 구성되는 순방향(Feed-forward) 신경망이다. SOM 신경망 모델은 다음과 같은 장점을 갖는다.

- SOM은 백프로퍼게이션 모델과는 달이 여러 단계의 피드백이 아닌 단 하나의 feed forward를 사용하기 때문에, 트레이닝이나 클러스터링의 수행이 상당히 빠르다. 그렇기 때문에 잠재적으로 여타의 신경망에서는 불가능했던, 실시간 학습처리를 할 수 있는 모델이다.
- SOM은 연속적인 학습이 가능하므로, 시간에 따라 입

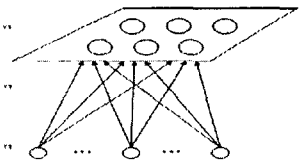
력데이터의 통계적 분포가 변한다고 하더라도 자동적으로 변화에 적응이 가능하다.

- SOM은 자기조직화를 통해 아주 정확히 통계적인 모델이기 때문에 출력 결과에 대한 신뢰도가 높다.

SOM의 구조는 간단하게 2 Lyaer 구조로 되어있으며, 입력 레이어 x1, x2, ... , xn 이 있고, 출력 레이어 y1, y2, ... , ym 이 존재한다. 그리고, 입력 레이어와 출력 레이어 연결 강도 벡터 W가 존재한다. 구조상 1차원 배열과 2차원 배열의 구조가 있고, 2차원 배열에는 사각형 배열과 육각형 배열 방식이 있다. 본 논문에서는 좀 더 정확한 분류를 위해 2차원 배열방식의 육각배열 방식을 사용하였다.



[그림 1] SOM의 1차원 배열



[그림 2] SOM의 2차원 배열

SOM을 본 연구에 도입한 이유는, 첫째 네트워크 구조상 수행이 빠르며 단 한 개의 feed-forward만 존재하기 때문에 잠재적으로 실시간 학습을 처리할 수 있고, 둘째 연속적인 학습이 가능하므로 입력데이터의 통계적 분포가 시간적으로 변하면 자동적으로 이러한 변화에 적응할 수 있으며, 셋째 자기조직화를 통한 정확한 통계적 모델이기 때문에 입력 데이터 분포에 대한 정확한 분류가 가능하기 때문이다.

2.2 분류를 위한 SOM

본 절에서는 SOM을 통한 분류를 위한 기본개념을 알아본다. SOM은 경쟁학습(competitive learning)방식을 취하며, 승자독점(winner take all) 형태이다. 입력 벡터 x와 가장 연결강도 벡터가 가까운 뉴런이 승자가 된다. 입력 벡터 x와 출력 뉴런 사이의 거리인 연결강도 벡터는 다음의 (식 1)로 구하게 된다.

$$d_j = \sum_{i=0}^{N-1} (x_j(t) - w_{ij}(t))^2 \qquad \text{(식 1)}$$

(식 1)에서 $x_i(t)$는 시각 t에서의 i번째 입력벡터이고, $w_{ij}(t)$는 시각 t에서 i번째 입력벡터와 j번째 출력 뉴런 사이의 연결강도이다. (식 1)에서 구한 연결강도 벡터가 가장 작은 즉, 최소거리인 출력뉴런이 승자뉴런이 되며, 이 승자 뉴런과 인접한 이웃 뉴런들만이 제시된 입력벡터에 대한 학습이 허용된다. 승자 뉴런과 인접한 이웃 뉴런들의 학습은 연결강도 벡터의 크기를 조정하게 되며, 이 규칙은 다음 식으로 표현된다.

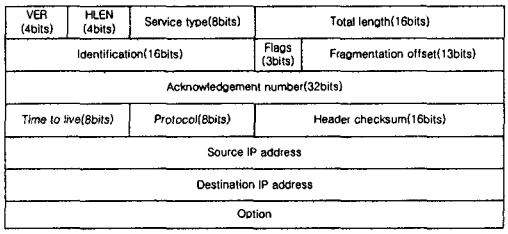
$$w_{ij}(t+1) = w_{ij}(t) + a(x_i(t) - w_{ij}(t)) \qquad \text{(식 2)}$$

(식 2)에서 $w_{ij}(t)$는 입력벡터 i 에서 출력뉴런 j 사이의 조정되기 이전의 연결강도 벡터이며, $w_{ij}(t+1)$는 입력벡터 i 에서 출력뉴런 j 사이의 조정된 후의 새로운 연결강도 벡터이고, $x_i(t)$는 i 번째 입력패턴 벡터이며, a는 학습상수이다. 승자 뉴런의 연결강도 벡터는 기하학적으로 입력벡터에 가장 가깝다. SOM에서의 학습은 단순히 연결강도 벡터와 입력벡터의 차이를 구한다음 그것의 일정한 비율을 원래의 연결강도의 벡터에 더하는 것이다. 이때, 승자 뉴런만이 연결 강도 벡터를 조정하는 것이 아니라 그 이웃 반경에 드는 모든 뉴런들도 유사한 조정을 하게 된다. 이웃은 2차원 배열일 경우, 정해진 크기의 사각형 배열 혹은 육각형 배열 안에 드는 뉴런들을 가리킨다.

3. SOM적용을 위한 전처리

본 장에서는 웜 바이러스 탐지를 위한 IP 패킷의 전처리 과정을 설명한다. 전처리의 목적은 첫째, IP 패킷에서 실험결과에 영향을 미치는 특성 데이터를 추출하는 것이고 둘째, 패킷을 SOM에 적용하기 위한 형식을 맞추기 위해서이다.

IP 프로토콜은 현재 인터넷에 사용되는 기본적인 프로토콜이며, 다양한 기능을 가지고 있다. 본 논문에서는 그 중에서도 IP 프로토콜의 헤더 부분을 이용하여 웜 바이러스를 탐지하는 방안을 연구하였다. 아래의 [그림 3]에는 IP헤더의 구조가 나타나 있다.



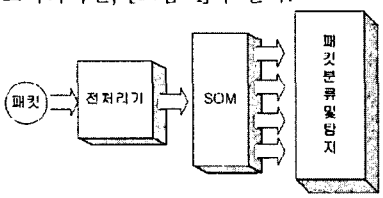
[그림 3] IP 헤더 구조

IP 헤더의 많은 필드 중 옵션 필드들은 재조합 후 그 값이 변화되거나 패킷 필터링을 통해 데이터가 드러날 수 있다는 문제점을 가진 것에 비해, ID 필드와 같은 필수 필드는 패킷 재조합 과정에 의해 변화되지도 않을뿐더러, 패킷 필터링에 의해 노출될지라도 드러난 값은 통신과정에 쓰이는 비트들의 조합일 뿐 특별한 의미를 부여하지 않는다. 그러므로 본 논문에서는 IP 통신에 필수적으로 사용되는 ID 같은 필드를 분석하여 웜 바이러스를 효율적으로 탐지하는데 사용한다.

전처리는 탐지율의 향상을 위해 두 가지 모드로 하게 된다. 특성데이터 추출과 관련하여 패킷으로부터 10바이트씩 뽑아내서 구성하는 것과 16바이트씩 뽑아내서 구성하는 것이 그것이다.

4. 웜 바이러스 탐지방안

본 장에서 제안하는 탐지방안은 IP헤더의 ID필드의 특성 데이터를 입력벡터로 하는 SOM 신경망을 학습시켜 웜 바이러스와 정상 패킷을 분류하는데 초점을 두었다. 웜 바이러스 패킷은 네트워크 레벨에서 실시간으로 탐지하는데에 그 의미를 두었기 때문에, 전처리 시 패킷들의 순서나 재조합을 고려하지 않았다. 제안한 탐지방안을 간략하게 도식화하면, [그림 4]와 같다.



[그림 4] 웜 바이러스 탐지방안

앞서, 2장에서 설명한대로 SOM은 학습을 유도하지 않고 통계학적 특성에 의해 자가조직화하는 방식이므로, 분류된 패킷의 확인을 위해서는 SOM 학습 이후에 기록된 Feature Maps에 이름을 붙이는 것이 필요하다.

5. IP헤더 웜 바이러스 탐지실험 및 결과

IP헤더의 웜 바이러스 탐지 실험을 위해 먼저 SOM을 학습시키기 위한 학습 데이터 집합과 테스트 데이터 집합을 구성하였다. 이때 사용되는 정상데이터는 tcpdump를 사용하여 수집하였으며, 웜 바이러스 데이터는 수집된 웜 바이러스 소스를 통해 독립된 네트워크를 구축하여 수집하였다.

Field	feature 개수	Feature Description
Identification	1	ID(16)
	3	ID(16) + Flag, Offset(16) + IP Header checksum(16)

[표 1] IP헤더의 ID필드 특성데이터

수집된 데이터는 3장에서 설명한 것과 같이 IP헤더의 ID필드에서 특성데이터가 1개인 것과 특성데이터가 3개인 것으로 나누어 실험 하였다. 실험조건은 학습상수 a는 0.3으로 초기값을 주고, 육각형 모델의 이웃반경 r은 3칸으로 정했다. SOM의 입력 벡터로 들어가는 데이터 셋은 5,000개의 패킷으로 5셋을 1000회 학습하였다. 그리고, 약 50,000 개의 정상 패킷을 사용하여 실험하였다.

특성데이터가 1개인 경우에 100회 학습하였을 경우, 같은 웜 바이러스 셋의 탐지율은 97.949769 %로 false detection은 거의 일어나지 않았다. 정상패킷에 대한 시뮬레이션은 32189(정상)/48103(총 패킷수)의 실험으로 약 65.045839 % 즉, 약 35%의 false detection을 일으켰다. 또, 1000회 이상 학습하였을 경우 32689(정상)/48003(총 패킷수)로 68.097827 %의 성능을 보였으며, false detection은 약 32%였다.

특성데이터가 3개인 경우에 웜 바이러스 셋의 탐지율은 100.00 %며, 정상 패킷에서의 탐지율은 100회 학습에 59.817475%, 1000회 이상 학습에 60.732179%의 성능을 보였다.

DataSet / Features	탐지율 바이러스 셋	오용 탐지율(%)	Map Size	학습횟수(회)
1	97.969769%	35 / 32	100	100 / 1000
3	100.00%	41 / 40	100	100 / 1000

[표 3] SOM을 이용한 웜 바이러스 탐지율

6. 결론 및 향후 연구방향

웜 바이러스의 탐지가 감염된 이후 치유하기 위해서는 응용레벨에서의 탐지와 치료가 타당하다. 그러나 감염된 후의 치료는 호스트가 이미 감염되어서 네트워크에 전파를 하였거나, 혹은 감염에 대한 피해를 입었을 가능성이 크다. 그러므로, 웜 바이러스가 발견된 즉시 빠르게 치료하는 것도 중요하지만, 웜 바이러스를 네트워크 레벨에서 탐지/차단 시켜 바이러스의 감염을 사전에 예방하는 것이 더욱 중요하다. 그러한 관점에서 본 연구는 웜 바이러스를 탐지하는 새로운 기법에 대해 하나의 방안을 제시하고 있다.

고정된 환경과 한정된 데이터로 인한 실험을 통해 실제적인 적용에 잠재적인 문제점을 내포할 수 있고, 더 좋은 성능을 내기위한 학습상수나 네트워크 크기의 확장, 이웃반경의 결정, 배열모양의 결정 등 학습과 관련된 최적성능 파라메터가 입증되지 않았다. 특히, features를 3개 사용했을 때의 효율은 실제 네트워크에서 성능이 더 떨어진다고 봤을 때, 만족할 만한 탐지율을 내지 못하고 있다. 이것은 자기 형상화 지도의 크기가 데이터의 분류 가지에 비해 작아서 생긴 결과라고 생각되며, 이후 다양한 패킷과 실제 네트워크와 같은 실험환경에서 대단위의 학습과 분류실험을 통해 최적성능 파라메터와 Map의 크기를 결정하는 것이 필요하겠다.

7. 참고문헌

[1] Teuvo Kohonen, Self-Organizing Maps, 1995
[2] Winkler, J, R. A UNIX Prototype for Intusion and Anomaly Detection in Secure Networks. In Proceedings of the 13th National Computer Security Conference, pages 115-124, Oct. 1990.
[3] Tarun Khanna, Foundations of Neural Networks, Addsom-Wesley, 1990.
[4] Nagano, 입문과 실습 NeuroComputer, 기술평론사, 1990.
[5] 조성배, 신경망 기법의 현실적 적용을 위한 개선 전략, KAIST석사논문,1990.
[6] W. Richard Stevens, TCP/IP Illustrated, Volume 1
[7] Vicki Irwin , Hal Pomeranz ,Intrusion Detection and Packet Filtering How It works