네트워크 침입탐지를 위한 인공면역 시스템의 동적 클론선택 연구

김정원(King's College London) 최종욱[u](상명대), 김상진(상명대)

Towards an Artificial Immune System for Network Intrusion Detection: An Investigation of Dynamic Clonal Selection

Jungwon Kim(King's College London) Jong Uk Choi[u] (Sangmyung University) Sang Jin Kim(Sangmyung University)

요 약

인공면역시스템에서 중요한 특징중의 하나는 지속적으로 변화하는 환경에서 자기(self)의 유동적인 패턴을 동적으로 학습하고 비자기(non-self)에 대한 새로운 패턴을 예측하는데 있다. 본 논문은 자기적용(self-adaptation)의 인공면역체계 특성을 기반으로하여 설계된 dynamiCS(동적 클론선택 알고리즘, dynamic clonal selection algorithm)의 역할을 논한다. 시스템의 세가지 중요한 변수인 자기내성 기간(Tolerisation Period), 면역 반응 임계값(activation threshold), 수명(life span)에 따라 변화하는 dynamiCS 의 성능을 네트워크 침입에서 흔히 발견되는 시나리오를 모의실험하여 평가한다.

1. 소개

네트워크 정보 보안 시스템 기술의 개발 노력중 하나로 개발되고 있는 침입탐지시스템은 시스템의 불법적인 오용이나 남용을 탐지하는 시스템을 칭한다. 현재 사용되고 있는 침입탐지 시스템은 대부분 이미 알려진 침입정보를 이용하는 것으로, 새로운 시스템의 헛점을 이용한 알려지진 않은 침입에는 많은 헛점을 드러내고 있다. 이러한 문제점을 극복하기 위한 국내외의 연구노력중 하나로, 외부에서 침입한 병원균을 효과적으로 탐지/파괴하는 인간의 면역 시스템을 응용하여 외부침입 탐지 시스템을 개발하는 연구들이 보고되고 있다 [1].

본 논문에서는 이러한 노력의 일환으로, 새로운 인공면역시스템인 동적클론선택 (Dynamic Clonal Selection) 을 제안한다. 기존의 인공면역시스템이 일정시간 동안 모아진 정적데이타만을 이용하여 탐지자를 생성하였던 바에 비해 [3],[4] 동적클론선택 알고리즘은 지속적으로 모아지는 데이타를 이용하여 탐지자들을 생성, 교체하는 것으로, 동적으로 변화하는 관찰대상의 정상행위와 비정상행위를 관찰하는 것을 주요 특징으로 한다.

2. 동적 클론선택 (DynamiCS) 알고리즘

동적클론선택 (Dynamic Clonal Selection) 알고리즘은 Hofmeyr[2] 인공면역시스템을 모델로한 새로운 인공면역알고리즘으로, 세개의 다른 탐지자 개체군의 상호작용으로 인공면역반응을 생성한다.

동적클론선택 알고리즘은 관찰대상의 비정상적인 개별행위를 탐지할수 있는 탐지자 개체군을 지속적으로 생성, 갱신하는 것을 주 골자로 운영된다. 처음 무작위로 생성되는 미성숙 탐지자들은 음성선택(Negative Selection)을 통과하는것으로 성숙탐지자가 된다. 음성선택이란 현재 알고리즘이 관찰하고자하는 어떤 행위에 대한 데이타를 항원으로 간주하여, 일정 자기내성 기간 (Tolerisation Period) 동안 관찰된 모든 정상항원 데이터에 대해 탐지 신호를 발산하지 않는 탐지자들만이 성숙탐지자로 변환되는것을 허락하는 선택과정을 칭한다. 첫번째 탐지자 생성 경로인 음성선택(Negative Selection)으로 인하여 탐지자들은 후에 정상행위에 대해 탐지신호를 보내지 않는 자기내성(Self Tolerance)을 갖게된다.

성숙탐지자들은 곧바로 관찰되는 항원데이타들에 대해 탐지과정을 시작한다. 이때 성숙탐지자들이 새로 관찰되는 항원데이터를 비정상행위로 간주하여 탐지 신호를 발산하고 성숙탐지자의 변수인 탐지종합(Match Count)을 하나씩 증가시킨다. 따라서, 새로운 항원데이타들이 각 성숙탐지자들에 의해 비정상행위로 간주될 때마다, 각 해당 성숙탐지자들의 탐지종합은 증가하게된다. 증가된 탐지종합이 사용자가 미리 정의한 면역 반응 임계값 (Activation Threshold)이 되었을 경우, 성숙탐지자들은 최종 비정상행위 탐지 신호를 사용자에게 보내게 된다. 이는 성숙탐지자들이 음성선택을 통해 자기내성을 갖게되었지만, 자기내성기간동안 관찰된 정상행위가 관찰시스템이 보일수 있는 모든 정상행위를 포함할수 없기때문에 초래되는 FP 오류를 줄이기 위한 방안이다.

사용자는 성숙탐지자가 보내온 탐지결과를 분석하여 그 결과가 정확하게 비정상행위를 탐지하였을 경우, 성숙탐지자를 기억탐지자로 변환시키어 새로운 항원데이터 관찰을 위하여 다시 탐지시스템에 보내게 된다. 기억탐지자들은 새로 관찰되는 항원데이타를 비정상행위로 간주할때, 탐지종합의 증가없이 곧바로 비정상행위 탐지신호를 사용자에게 보낸다. 이는 기억탐지자가 성숙탐지자와는 달리 이미 비정상행위를 탐지하여 그 유용성을 검증 받았음으로 성숙탐지자들에 비해 FP 오류가 낮을것으로 기대되기 때문이다.

또하나 주목하여야 할점은 성숙탐지자들은 사용자가 미리 수명(Life Span)을 정의해 주었기 때문에 만일 주어진 수명 기간 이내에 그들의 탐지종합이 임계값을 만족시키지 못한 경우 바로 시스템에서 제거된다. 기억탐지자들은 이와는 달리 무한 수명을 가지고 있어서 한번 생성된 경우 지속적으로 관찰되는 항원들에 대해 탐지활동을 벌인다.

따라서, 무작위로 생성된 하나의 탐지자는 일정 자기내성 기간동안 미성숙탐지자로 음성선택과정을 거친후, 탐지종합이 면역 반응 임계값에 미치기까지 성숙탐지자로의 성숙기간을 마친다. 성숙기간을 마친 성숙탐지자는 사용자의 확인을 받고서는 기억탐지자로 변환되어 탐지과정을 시작하게 된다. 이러한 세단계 과정은 항원데이터가 제공되는한 지속적으로 진행된다. 항원데이터가 제공되는 순간 동적클론선택 알고리즘은 우선 기억탐지자에 의해 비정상행위의 탐지를 시작하고, 아직 생성된 기억탐지자가 없을경우엔 항원데이터는 성숙탐지자에게 제공된다. 이때의 항원데이터에 포함되어 있을 비정상행위에 의해 성숙탐지자의 성숙과정을 진행시킨다. 그러나, 생성된 성숙탐지자도 역시 없을경우 항원데이타는 미성숙탐지자에게로 제공되어 음성선택에 쓰이게 된다. 따라서, 최초의 자기내성 기간동안은 시스템의 자기내성을 갖을수 있는 최초의 성숙탐지자 생성을 위한 훈련과정으로서, 비정상행위가 포함되어 있지 않은 항원데이타만을 제공하는 것을 가정한다.

따라서, 동적클론선택알고리즘 진화와 학습의 한 세대는, 만족할만한 수의 최초의 성숙탐지자가 생성된 이후에 상기에 서

본 논문은 한국과학재단 특정기초연구사업(1999-2-511-001-3)의 지원으로 수행되었음

술된 순서, 즉 기억탐지자의 탐지, 성숙탐지자의 성숙, 미성숙 탐지자의 내성으로 이루어진다.

3. 데이터와 변수설정

실험은 UCI 기계학습 벤치마킹 데이터 모음 사이트에서 제공하는 위스콘신 유방암 데이터를 사용하였다 (ftp://ftp.ics.uci.edu/pub/machine-learning-databases). 이 데이터는 악성종양 (Malignant)과 양성종양 (Benign) 두 그룹으로 나뉘어지는데, 악성종양에 해당되는 데이타를 비정상행위로, 양성종양에 해당되는 데이타를 정상행위로 다루어 동적클론선택 알고리즘에 제공하였다. 악성종양의 경우 240 개의 표본을 갖고 있으며, 양성종양의 경우 460 개의 표본을 갖는다.

동적으로 변화하는 분포를 가지는 항원데이터를 자기내성기간과 성숙기간, 탐지기간중에 제공하기 위해, 정상행위와 비정상행위에 해당하는 데이터를 클러스터링으로 잘 알려진 Expectation Maximization (EM) 알고리즘[5]을 이용하여 각각 3 개의 부군(sub-groups)으로 나누었다. 동적클론선택이 진행되는 매 N 세대동안 오직 세개의 부군중 하나의 부군에 해당하는 항원데이타들의 80%에 해당하는 비정상, 정상의 항원데이터만이 무작위로 선정되어 알고리즘에 제공되었다.

모든 실험은 최대 2000 세대동안 수행되었고, 각 실험은 5 회 수행후의 평균값을 실험결과로 보고한다.

4. 실험 1: 서로 다른 분포의 항원 데이타가 주어지는 경우

첫번째 실험은 N 을 1 로 고정시키고 매 세대마다 다른 분포를 갖는 부군에서 선택된 항원데이타를 제공하였다. 따라서, 이 실험에서 DynamiCS 의 탐지자들은 각 세대에서 오직 전체 항원데이터의 일부분만을 제공받게 된다. 그러나, N 을 1 로 고정시키었기 때문에, 일정세대가 지나면 탐지자들은 세 부군에 속하는 항원데이터를 골고루 경험하게 된다. 이 실험에서는 세가지 변수값을 변화해가면서 DynamiCS 가 세부군에 속하는 항원데이터를 모두 정상과 비정상으로 구분할수 있는지를 평가하여 본다. 이는 침입탐지시스템이 흔히 접하게 되는 상황, 즉 시스템은 각 관찰 시간 단위 동안은 오직 정상행위의 일부분 만을 나타내는 데이터만 제공받게 되지만, 충분한 관찰기간 이후에는 이들 행위들이 골고루 나타나는 경우를 가상 모의 실험하는 경우이다.

4.1 자기내성기간의 영향

자기내성기간(T)을 네개의 다른 값인 {5, 10, 20, 50}으로 설정하여 네가지 다른 실험을 수행하였다. 이 실험에서는 성숙탐지자의 면역반응임계값(A)은 5 로, 수명(L)은 10 으로 고정되었다. 실험이 수행된 2000 세대동안 TP(True Positive) 탐지율과 FP(False Positive) 오류율은 T 값에 관계없이, 주어진 항원데이타의 클러스터가 변화함에 따라 다른 결과를 보이고 있으나, 같은 클러스터가 반복됨에 따라 각각 수렴된 최대값과 최소값을 보이고 있다. (그림 1 참조)

이 실험에서 주목되는 결과는 T 가 증가함에 따라, FP 오류율이 급격히 감소하는 현상이다. 이는 자기내성기간이 인공면역시스템의 정상 항원 데이터에 대한 탐지 오류를 방지하기 위해 제안된 본래의 의도에 부합되는 결과임을 증명하고 있다. 그러나, T 값이 가장 작은 5 인 경우와 가장 큰 값인 20 의 경우 TP 탐지율을 비교해보면 T 값이 클수록 TP 탐지율은 감소함을 발견할 수 있다. 이는 T 값이 증가할수록 미성숙탐지자의 수가 증가하게 되며 정작 비정상 항원데이터를 탐지할수 있는 성숙탐지자의 감소를 초래하고 그로인한 전반적인 탐지 시도의 감소가 그 원인인것으로 설명된다.

4.2 성숙탐지자 면역 반응 임계값의 영향

두번째 실험은 자기내성기간(T)은 5 로, 성숙탐지자의 수명(L)은 10 으로 고정시키고, 성숙탐지자의 면역 반응 임계값(A)을 {5, 10, 20, 50} 변화시켜가면서 TP 탐지율과 FP 오류율을 관찰하였다 (그림 2 참조). 이 실험결과 역시 4.1 의 실험에서와 같이 각각 수렴된 최대값과 최소값을 보이고 있다. 면역반응임계값(A)이 증가함에 따라 FP 오류율이 감소하는 반면 TP 탐지율 역시 함께 감소하는 것을 발견할수 있다. 또한, 성숙탐지자의 면역 반응임계값이 자기내성기간과 함께 추가적으로 사용될때 인공면역시스템의 FP 오류율을 더 큰 폭으로 감소시키는 것을 발견할 수도 있다.

4.3 성숙탐지자 수명의 영향

세번째 실험은 자기내성기간(T)을 5 로, 성숙탐지자의 면역 반응 임계값(A)을 150 으로 설정하고, 성숙탐지자의 수명(L)을 {5, 10, 20, 50} 으로 변화시켜가면서 수행되었다. (그림 3 참조) 이 실험결과 역시 앞선 실험결과와 같이 각각 수렴된 최대값과 최소값을 보이고 있으며, 성숙 탐지자의 수명(L)이 증가함에 따라 TP 탐지율은 큰폭으로 증가하고 FP 오류율은 소폭으로 역시 증가함을 보이고 있다.

5. 실험 2: 항원데이터의 분포를 갑자기 변경하는 경우

실험 2 는 N 을 5, 10, 20, 30 으로 변화시킬 때 관찰되는 탐지율과 오류율을 분석하였다. N 이 커질수록, 생성되는 탐지자들은 가장 최근에 선택된 항원부군에 해당하는 정상행위와 비정상행위만의 분포를 인식하게 된다. 따라서, 비교적 큰값을 갖는 N 세대이후 항원부군을 갑자기 대체하는 것으로 항원데이터의 분포를 바꾸고, 동적클론선택 알고리즘이 새롭게 생성하는 탐지자들이 얼마나 빠르게 새 항원부군의 정상행위와 비정상행위 데이터를 판별할 수 있는지를 관찰, 분석하는것을 이실험의 목표로 한다. 이는 침입탐지시스템이 흔히 접하게 되는 또 다른 상황, 즉 과거 안정적으로 관찰되었던 정상행위가 합법적인 요인들로 인하여 갑작스러운 변화에 대해 모의실험하는 경우이다.

이 실험에서는 자기내성기간(T)은 30, 성숙탐지자의 면역 반응 임계값(A)은 5, 수명(L)은 10 이 사용되었다. 그림 4 에 나타난 결과를 보면, N 이 증가함에 따라, 생성되는 탐지자들은 가장 최근에 선택된 항원부군만의 정상행위와 비정상행위의 분포를 인식하고 있다. N 을 1 로 고정시켰던 실험에서 (그림 1) 자성내성기간이 30 으로 비교적 큰 값이 주어졌을 경우에 언제나 FP 오류율 0 에 가까운 완전한 성능을 보였으나, 그림 4.에서 N 이 증가할수록 비교적 큰값의 자기내성기간이 FP 오류를 만족할만한 수준으로 감소기키지 못하고 있다.

6. 결 론

본 논문에서는 인공면역시스템을 이용한 침입탐지시스템 개발을 위해 동적클론선택 알고리즘을 제안하고, 침입탐지시스템이 흔히 접하게 되는 실제 두가지 상황, 즉 시스템은 관찰시간동안 오직 정상행위의 일부분 만을 나타내는 데이터만 제공받게 되는 경우와, 과거 안정적으로 관찰되었던 정상행위가 합법적인 요인들로 인하여 갑작스러운 변화를 보일경우를 모의 실험하여 그 탐지율과 오류율을 분석하였다. 실험은 기계 학습 벤치마킹에 쓰이는 유방암의 데이타의 악성종양의 경우를 비정상행위로 양성종양의 경우를 정상행위로 간주하여 실시되었다.

첫 번째 실험에서는, DynamiCS 가 각 관찰시간동안 오직 전체적으로 수렴되어 학습될수 있는 정상행위의 일부분만을 나타내는 항원데이터만을 제공받게 되었을때, 점진적으로 모든 정상행위를 학습할 수 있는가를 평가하였다. 특히 이 평가는 DynamiCS 의 성능을 결정하는 세가지 변수인

자기내성기간, 성숙탐지자의 면역반응임계값과 수명의 값을 변화시켜 가면서 그 성능을 분석하였다.

이 실험의 결과로, DynamiCS 는 모든 정상행위를 오직 한세대에 전체 정상항원데이터의 오직 일부분만을 학습하는 것으로도, 전체 정상항원데이터를 학습할수 있었다. 특히, TP 탐지율과 FP 오류율에 의해 측정했던 시스템 성능은 앞서 소개된 세 변수들의 값에 크게 지배되고 있음을 보였다.

자기내성기간을 늘리수록, 성숙탐지자들이 생성되기 어려운 여건은 곧바로 비성숙탐지자들을 더 많이 생성함으로써 FP 오류율을 감소시키는 결과를 보였다. 또한, 성숙탐지자의 면역 반응 임계값과 수명을 감소시킬 수록 DynamiCS 는 증가된 TP 탐지율을 보였다.

두 번째 실험은 비교적 큰값을 갖는 N 세대이후 항원부군을 갑자기 대체하는 것으로 항원데이터의 분포를 바꾸고, 새롭게 생성하는 탐지자들이 얼마나 빠르게 새 항원부군의 정상행위와 비정상행위 데이터를 판별할 수 있는지를 관찰하였다. 이 경우 앞선 실험에서 완전한 FP 오류율을 보여주기에 충분했던 비교적 큰값의 T 를 사용했을 경우에도 만족할만한 수준의 낮은 FP 오류율을 보여주지 못하였다. 이는 비정상 항원데이터 탐지에 관여하는 기억탐지자들이 특정 항원부군에 속하는 항원데이타를 경험하지 못하여, 전체 항원데이타에 대한 완전한 자기내성을 가질 수 없었기 때문이다.

따라서, 현재의 DynamiCS 는 과거 안정적으로 관찰되었던 정상행위가 합법적인 요인들로 인하여 갑작스러운 변화를 보일경우, 새로운 변화를 빠르게 학습하지 못하는 것으로 관찰되었다. 이러한 문제를 보완하기 위해 현재 면역시스템의 기억탐지자군의 수정 메커니즘과 돌연변이를 이용한 빠른 학습메카니즘을 새롭게 보완한 DynamiCS 가 구현되었고, 그 실험결과가 곧 발표될 예정이다.

References

[1] Allen, J. et al, (2000), "State of the Practice of Intrusion Detection Technologies", Technical Report CMU/SEI-99-TR-028, Software Engineering Institute, Carnegie Mellon University.

[2] Hofmeyr, S., (1999) An Immunological Model of Distributed Detection and Its Application to Computer Security, PhD Thesis, Dept of Computer Science, University of New Mexico.

[3]Kim, J. and Bentley, P. J. (2001a), "Evaluating Negative Selection in an Artificial Immune System for Network Intrusion Detection", Proceeding of GECCO-2001, San Francisco, pp.1330 - 1337, July 7-11.

[4]Kim, J. and Bentley, P. (2001b), "The Artificial Immune System for Network Intrusion Detection: An Investigation of Clonal Selection with a Negative Selection Operator", Proceeding of CEC-2001, Seoul, Korea, pp.1244-1252, May 27-30.

[5] Mitchell, T. (1997), Machine Learning, McGraw-Hill.

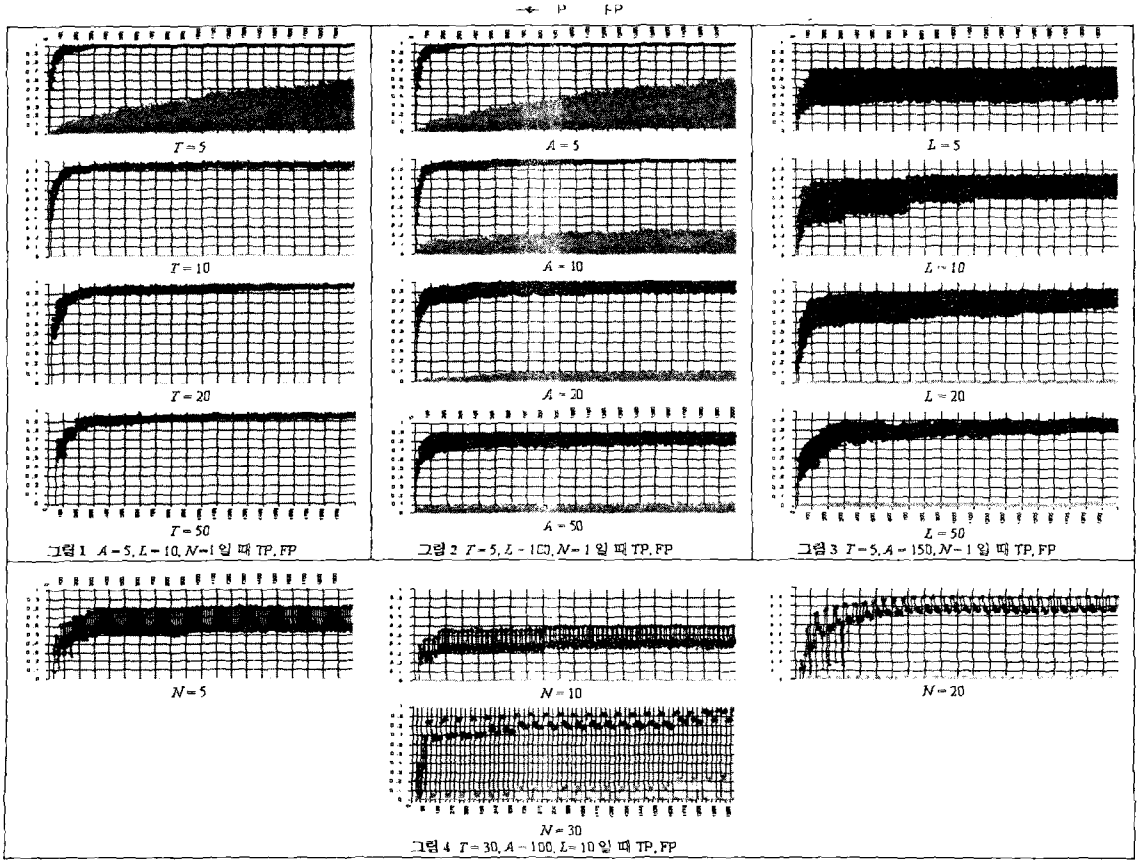

그림 1 $A=5, L=10, N=1$ 일 때 TP, FP

그림 2 $T=5, L=100, N=1$ 일 때 TP, FP

그림 3 $T=5, A=150, N=1$ 일 때 TP, FP

그림 4 $T=30, A=100, L=10$ 일 때 TP, FP