韓國컴퓨터情報學會 論文誌
第14卷 第10號, 2009. 10.

2009-14-10-3-7

유전 알고리즘 기법을 이용한 HA 모델 설계

신 미 예*, 전 승 흡**, 이 상 호***

A Hybird Antibody Model Design using Genetic Algorithm Scheme

Mi-yea Shin*, Seoung-heup Jeon**, Sang-ho Lee***

요 약

자연면역 시스템은 여러 신체 부위에서 다양한 기능으로 외부침입에 민감하게 대응할 뿐만 아니라 기존에 감염된 정보를 기억하는 기능을 수행한다. 그러나 자연 면역 시스템의 원리를 적용한 컴퓨터 보안 시스템에서는 자연면역 시스템이 갖는 기능을 충분히 제공하지 못하는 문제점이 있다. 이 논문에서는 자연면역 시스템의 네거티브 셀렉션을 적용한 항체와 임의의 비정상 시스템 콜 시퀀스를 선택하여 유전자 알고리즘을 적용한 항체를 결합하여 자연면역 시스템과 유사한 기능을 제공하는 하이브리드 모델을 제안한다. 제안된 모델은 긍정적 결함과 부정적 결함을 줄이기 위해 임의의 비정상 시스템 콜 시퀀스를 이용한다. 실험에 사용된 데이터는 UNM(University of New Maxico)에서 제공된 샌드메일 데이터이며 실험 결과 제안 모델은 기존 네거티브 셀렉션보다 비정상 시스템 콜을 정상 시스템 콜로 판정하는 부정적 결함이 평균 0.55% 낮게 나타났다.

Abstract

A nature immunity system responds sensitively to an external invasion with various functions in a lot of bodies, besides it there is a function to remember information to have been currently infected. we propose a hybrid model similar to immune system which combine with the antibody which applied genetic algorithm as select antibody and the arbitrary abnormal system call sequence that applied negative selection of a nature immunity system. A proposed model uses an arbitrary abnormal system Kol sequence in order to reduce a positive defect and a negative defect. Data used to experiment are send mail data processed UNM (University of New Maxico). The negative defect that an experiment results proposal model judged system call more abnormal than the existing negative selection to normal system call appeared 0.55% low.

• 제1저자 : 신미예 교신저자 : 이상호
• 투고일 : 2009. 08. 31, 심사일 : 2009. 09. 10, 게재확정일 : 2009. 10. 09.
* 충북대학교 전자계산학과 * 충북대학교 전자계산학과
** 충북대학교 전기전자컴퓨터공학부 컴퓨터공학전공 교수

▸ Keyword : 인공면역 시스템(Articial Immune System), GA(Genetic Algorithm), 시스템 보안 (System Security)

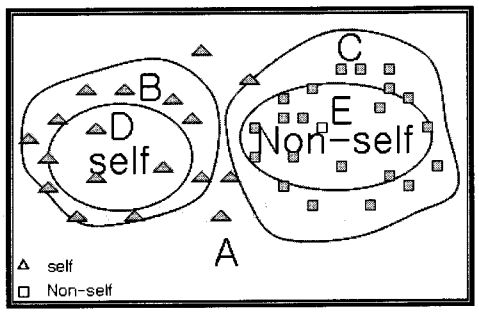
Ⅰ. 서 론

자연면역시스템(NIS:Natural Immune System)은 박테리아, 바이러스, 기생충, 독소 등 위험한 외부 병원균들로부터 동물들을 보호하는 역할을 수행한다[1,2]. 이 자연면역 시스템은 다계층 보호, 분산 탐지, 탐지 능력의 다양성, 불완전한 탐지, 기존에 감염된 정보를 기억하는 기능, 새로운 외부 패턴들에 대해 민감하게 대응하는 특징을 갖고 있다[2]. 신체 내 면역 시스템의 역할은 컴퓨터 시스템의 시스템 보호와 유사하여 현재까지 다양한 모델들이 광범위하게 제안되었다.

ARTIS(Artificial Immune System)는 1987년 Cohen에 의해 "Computer Virus"라는 용어로 처음 소개되었다[3]. 1994년 멕시코 대학의 Forrest 교수는 흉선에서 항체 T-cell이 생성될 때 몸 안에 있는 항체와 같은 것은 선택하지 않는 'negative selection'을 적용하여 컴퓨터에서 비정상적으로 실행되는 것을 탐지하기 위한 항체 생성 알고리즘을 제안했다. 이 알고리즘은 change detection 알고리즘으로 정상적인 이진수 집합 x와 임의로 생성된 이진수 집합 y사이의 match(x,y)는 적어도 r개의 이진수가 연속해서 일치되는지를 판단하게 된다[4].

네거티브 셀렉션은 정상적인 시스템 콜 시퀀스(system call sequence)를 self로 정의하고, 이 self를 이용하여 항체를 생성한다. 네거티브 셀렉션은 항체를 생성할 때 수집되지 않은 정상적인 시스템 콜인 self를 비정상적인 시스템 콜인 non-self로 판단하는 긍정적 결함률(false positive rate)과 non-self를 self로 판단하는 부정적 결함률(false negative rate)이 높게 나타난다.

네거티브 셀렉션과 시스템 콜 시퀀스를 고려한 기존 방법들은 탐지자(detector)의 크기가 정상적인 시스템 콜의 진(gene)의 크기와 같게 하는 특징은 있지만 알려지지 않은 새로운 침입을 판단하기가 어려운 문제점이 존재한다. 여기서 진은 시스템 콜 시퀀스를 일정 크기로 나눈 집합을 의미한다.



A : self와 non-self 전체 집합
B : 실제 self data C : non-self data
D : 수집된 self data E : 수집된 non- self data

그림 1. self와 nonself
Fig. 1 self and nonself

네거티브 셀렉션에서 self와 r-contiguous개 비교하여 동일하지 않은 진을 선택할 때, 그림 1에서와 같이 A, B, C가 non-self임을 보장할 수 없다. 그 이유는 self와 non-self가 모두 존재하는 전체 집합 A에서 negative selection을 위한 self를 정의하기가 매우 어렵기 때문이다. negative selection을 위한 self로 B 부분의 self를 얻지 못한다면 탐지자는 충분하지 못한 self로 생성되게 된다.

이 논문에서는 자연면역 시스템의 네거티브 셀렉션을 적용한 항체와 임의의 비정상 시스템 콜 시퀀스를 선택하여 유전자 알고리즘을 적용한 항체를 결합하여 자연 면역 시스템과 유사한 기능을 제공하는 하이브리드 항체(Hybrid Antibody) 모델을 제안한다. 제안된 모델은 긍정적 결함과 부정적 결함을 줄이기 위해 임의의 비정상 시스템 콜 시퀀스를 이용한다.

이 논문의 구성은 다음과 같다. 2장에서는 면역 시스템과 시스템 콜 시퀀스를 이용한 탐지 모델을 기술하고 3장에서는 임의의 시스템 콜 시퀀스를 선택하여 GA에 적용한 항체 생성 모델을 제안한다. 4장에서는 negative selection과 제안 모델을 false positive rate와 false negative rate를 비교분석한다. 마지막으로 5장에서는 결론 및 향후 연구에 대해서 기술한다.

Ⅱ. 관련연구

2.1 자연면역 시스템과 인공면역 시스템

자연 면역 시스템(natural immune system)은 박테리아, 바이러스, 기생충, 독소 등을 포함한 위험한 외부 병원균

으로부터 동물들을 보호한다. 자연면역 시스템에서 보여준 몇 가지 중요한 속성들을 갖는 컴퓨터 면역 시스템을 디자인함으로써 컴퓨터 보안 시스템의 개선을 이루었고 침입 탐지 방법과 분산처리 가능한 체인지 디텍션 알고리즘을 이용한다[1].

자연면역 시스템은 내재면역(innate immune system)과 적응면역(adaptive immune system) 단계로 이루어진다. 내재면역은 감염에 대한 일차 방어선으로 대식세포 및 중성구들과 같은 식세포들, 피부와 같은 장벽들, 체내의 항생물질 등이 내재면역에 중요한 역할을 한다. 적응면역의 특징은 항원들 사이의 미묘한 차이점을 구별할 수 있게 하는 항원에 대한 특이성, 분자들을 인식하는데 있어서 엄청난 다양성을 생성할 수 있어서 외부 항원들 사이의 수십억 개의 독특한 구조들을 인식하는 다양성과 일단 면역 시스템이 어떤 항원을 인식하고 반응하고 나면 그 정보를 기억하고 있다가 동일한 항원을 다음에 접촉하게 되면 면역 반응을 빠르게 하는 면역기억 등이 있다[5].

인공 면역 시스템은 자연 면역 시스템에서 이루어지는 면역체계가 비정상 침입 탐지시스템 과정과 매우 유사하므로 이를 적용한 시스템이다. 골수에서 생성되는 항체는 본래의 유전자와 비교하여 일치하지 않는 유전자를 항체로 선택한다. 이를 negative selection이라 부른다. 이와 같은 메커니즘을 컴퓨터 면역 시스템에 적용한 시스템에서는 항체를 생성할 때 임계치를 기준으로 negative selection을 수행 하였다. 그러나 실제로 인간의 면역체계에서는 본래의 유전자와 완벽하게 일치되는 유전자를 제외시키는 것은 물론 완전히 일치되지 않는 유전자도 제외시키는 메커니즘을 이용하고 있다.

2.2 유전 알고리즘

유전 알고리즘(Genetic Algorithm, GA)은 최적화 문제를 해결하는 기법의 하나로, 전역 최적화 기법이다[6]. GA는 생물의 진화를 모방한 기법인 진화 연산의 대표로서, 생명체에 적용되는 많은 방식을 차용하여, 선택, 교차(교배), 변이(돌연변이), 대치 연산 등이 존재한다.

선택은 유전자에 조작을 가한 후 제대로 형질전환이 일어난 것만 골라내는 것을 의미한다. 선택 방법에는 균등 비례 룰렛휠 선택, 토너먼트 선택, 순위 기반 선택 등이 있다.

교차는 두 염색체 사이에서 일정 점을 중심으로 정보를 상호 치환하는 과정을 의미한다. 일반적으로 교차에서는 두 개의 해가 교배를 해서 다음 세대의 해를 생성하게 되며, 새로운 해는 각각의 부모 해로부터 서로 겹치지 않는 위치의 유전체를 받아 새로운 유전자를 구성하게 된다. 이때 염색체가 재조합되는 과정에서 부모 염색체의 일부분이 특정 위치를 기준으로 서로 바뀌어 결합되는 경우가 있다. 유전 알고리즘에서는 이 교차 현상을 의도적으로 이용, 부모 해를 교차시켜서 자식 해를 만들어낸다.

돌연변이는 염색체의 한 부분이 결실되었거나 다른 염색체에 더 붙는 것을 의미한다.

대치는 교차·변이 등을 거쳐서 만들어진 새로운 해를 해집단에 추가하고 기존 해 중 열등한 해를 가려내서 제외시키는 연산이다. 가장 품질이 나쁜 해를 대치하는 방법, 새로운 해의 부모 해중에서 새로운 해와 가장 비슷한 해를 대치시키는 방법(해집단의 다양성을 유지하기 위함) 등이 있다.

2.3 negative selection에서 r-contiguous bit를 이용한 탐지

Negative selection에서 r-contiguous bit를 이용한 탐지는 흉선에서 T-세포가 생성되는 negative selection 알고리즘을 이용하여 정상적인 system call을 적당한 크기의 윈도우로 분류한 후 탐지자로 사용하고, 이 탐지자에 해당되지 않은 system call은 비정상으로 판단하는 방법이다. 이 방법은 Negative Selection을 적용하여 바이러스 침입[7], 시스템 콜의 시퀀스 이상[8], 네트워크 트래픽[9] 이상을 탐지하도록 탐지자의 크기를 self의 크기와 동일하게 사용한다.

(식 1)은 한 개의 진(gene)을 구성하는 문자열의 개수가 l개일 때 연속적으로 r개 매치될 가능성을 의미한다.

$$P_M \approx m^{-r}[(l-r)(m-1)/m+1] \quad \text{(식 1)}$$

m : 알파벳 심볼의 수
l : 문자열 안에 있는 심볼의 수(문자열의 길이)
r = 연속적으로 매치되는 수

예를 들어, (식 1)에 사용된 파라미터의 값을 m = 2, l = 10, r = 6로 가정하였을 경우 P_M은 0.09375와 같은 결과를 도출한다.

(식 2)는 negative selection하기 전 초기 탐지자의 크기를 의미한다. (식 2)에 사용된 파라미터는 N_{R_0}, N_R, N_S 그리고 P_M등이 사용되며 각 파라미터의 의미는 다음과 같다.

$$N_{R_0} = \frac{-\ln P_f}{P_M \times (1 - P_M)^{N_S}} \quad \cdots\cdots\cdots\cdots \text{(식 2)}$$

N_{R_0} = 초기 탐지자(detector) 문자열의 수(센서가 만들어지기 전)

N_R = 센서가 만들어진 후 탐지자 문자열의 수

N_S = 정상적인 문자열의 수

P_M = 2개의 임의의 문자열 사이의 일치 가능성

독립적인 탐지자를 생성하기 위한 확률 P_f는(식 3)과 같이 N_R 탐지자에 의해 얻어질 수 있다.

$$P_f \approx (1 - P_M)^{N_R} \quad \cdots\cdots\cdots\cdots \text{(식 3)}$$

(식 3)의 P_M이 매우 작고, N_R이 크다면, 탐지자 문자열 수는 (식 4)와 같다.

$$N_R \approx \frac{-\ln P_f}{P_M} \quad \cdots\cdots\cdots\cdots \text{(식 4)}$$

따라서, 탐지자 집합은 N_S의 크기에 영향을 받고 탐지자의 크기는 self 크기와 같다[1, 10].

2.4 System call sequence를 이용한 탐지

System call sequence를 이용한 탐지는 모든 system call에 대하여 윈도우 크기에 맞추어 sequence를 고려하여 탐지자를 생성한다. 표 1은 정상적인 시스템 호출 순서를 진 크기 3으로 맞춘 탐지자이다. 시스템에서 처리되어 지는 시스템 콜 시퀀스로 만들어진 진과 표 1의 탐지자를 비교하여 불일치률을 구한다. 이 경우, 탐지자의 크기는 진의 크기와 시퀀스의 길이를 이용한 (식 5)와 같다.

$$k(L-k) + (k-1) + (k-2) + \cdots + 1$$
$$= k(L-(k+1)/2) \quad \cdots\cdots\cdots\cdots \text{(식 5)}$$

k : 진의 크기(call, position1, position2, position3)
L : 시스템 콜 시퀀스의 길이

open, read, mmap, open, open, getrlimit, mmap, close 등의 시스템 콜이 발생한 경우 표 2는 프로세스 호출 순서가 불일치되는 과정을 보여주고 있다.

표 1. 시스템 콜의 순서
Table. 1 sequence of system calls

call	position1	position2	position3
open	read	mmap	mmap
	getrlimit		close
read	mmap	mmap	open
mmap	mmap	open	getrlimit
	open	getrlinit	mmap
	close		
getrlimit	mmap	close	
close			

표 2. 프로세스 호출 순서 예제
Table. 2 sequence of system calls examples

순서	시퀀스	불일치한 위치
1	open->read->mmanp->open	position 3
2	read->mmap->open->open	position2
3	mmap->open->open->getrlinit	position2
4	open->open->getlimit->mmap	position2
5	open->gerrlimit->mmap->close	
6	getrlimit->mmap->close	

시스템 콜 시퀀스의 불일치 정도는 순서 ① ② ③ ④에서 4개가 발생한다. 표 1을 통해 진의 크기와 시퀀스의 길이가 각각 3과 8이고, (식 5)을 통해 데이터 베이스의 크기는 18이 되어 불일치 정도는 22%가 된다[11].

III. HA(Hybrid Antibody) 모델

이 절에서는 임의의 비정상 시스템 콜 시퀀스를 선택하여 유전 알고리즘을 적용한 항체와 자연면역 시스템의 네거티브 셀렉션을 적용한 항체를 결합한 HA(Hybrid Antibody) 모델을 제안한다. 제안 모델은 비정상적인 시스템 콜 시퀀스에 교배와 돌연변이를 적용하여 정상적인 시스템 콜 시퀀스와 탐지자와의 유사도는 낮추고 비정상적인 시스템 콜 시퀀스와 탐지자와의 유사도는 높여서 긍정적 결함율과 부정적 결함율을 낮춘다. 또한, 제안 모델은 긍정적 결함률과 부정적 결함률을 줄이기 위하여 탐지자의 수를 결정하는 (식 4)를 이용하여 self의 크기와 비례한 비정상 시스템 콜 시퀀스의 진을 선택한다.

3.1 개요

이 절에서는 negative selection 알고리즘으로 생성된 탐지자와 임의의 비정상 시스템 콜 시퀀스를 추출하여 GA를 적용한 탐지자를 그림2에서 보여주고 있다.

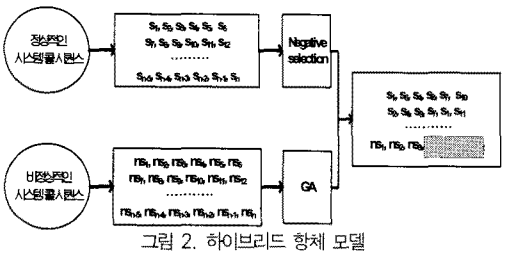


그림 2. 하이브리드 항체 모델
Fig 2. Hybrid Antibody model

그림 2는 정상적인 시스템 콜 시퀀스의 진과 비정상적인 시스템 콜 시퀀스의 진으로 구성된다. 정상적인 시스템 콜 시퀀스는 탐지자를 생성할 때 negative selection에 의하여 탐지자가 생성되고, 비정상적인 시스템 콜 시퀀스는 정상적인 시스템 콜 시퀀스의 일정 크기의 비율로 GA를 적용한 탐지자를 생성한다. 그림 2의 GA는 임의의 비정상 시스템 콜을 선택하여 크기 6인 진을 생성하여 진의 일부분에 교배 및 변이를 일으켜 탐지자의 진들과 비교 후 동일한 진이 없으면 탐지자로 선택된다.

3.2 용어정의

HA 모델에서 사용하는 주요 용어를 정의하면 표 3과 같다.

표 3. 파라미터
Table 3. Parameter

Notaion	Definitions
R	문자열의 개수
N	윈도우의 크기
$gene$	시스템 콜 시퀀스를 N으로 나눈 크기
$T_{\max}$	연속된 R개가 매치될 최대값
$T_{\min}$	연속된 R개가 매치될 최소값
$detector$	탐지자
GG	진 생성자
GA	유전 알고리즘
NS_i	i번째의 비정상 시스템 콜 시퀀스
$self$	정상적인 시스템 콜 시퀀스
$non-self$	비정상적인 시스템 콜 시퀀스

3.3 negative selection을 이용한 항체 생성 과정

기존 연구에서는 자연 면역에서 성숙한 항체 T-cell이 흉선에서 생성되어 신체의 각 부분으로 방출될 때 유전자 조합을 하여 self 세포와 비교 후 완전히 일치하거나 완전히 일치하지 않아도 항체로 채택되지 않는 negative selection을 이용한다[4, 8]. negative selection에 의해 생성되는 탐지자는 그림 3과 같이 크게 2개의 과정으로 구분한다. 1단계에서는 정상적인 시스템 콜 시퀀스를 GG에서 N의 크기로 진을 생성한다.

그림 3의 1단계에서 GG는 정상적인 시스템 콜 데이터를 윈도우 크기 6으로 진들을 생성한다. 만약 시스템 콜 시퀀스가 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15와 같이 발생된다면 진은 1, 2, 3, 4, 5, 6의 진, 7, 8, 9, 10, 11, 12의 진 그리고 13, 14, 15의 진이 생성된다.

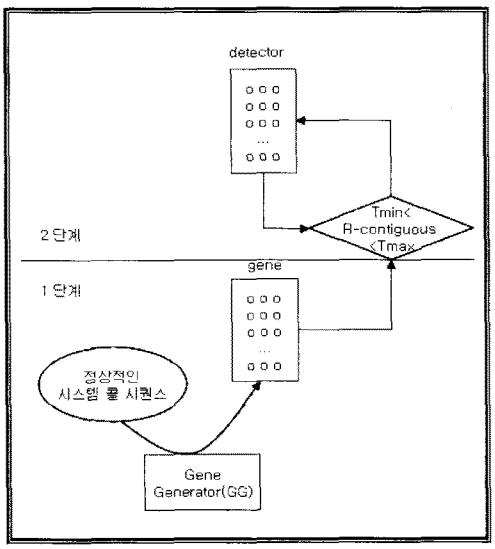


그림 3. GA 기법을 이용한 항체 생성
Fig 3. Antibody Generation using GA Scheme

1단계가 끝난 후 2단계에서는 임의의 정상 시스템 콜을 선택하여 윈도우 크기 6인 1개의 진을 생성한다. 그리고 새로 생성된 진은 1단계에서 정상적인 시스템 콜로 생성된 진들과 중복되지 않고, r-contiguous 방법으로 비교하여 최소 임계치($T_{\min}$) 보다 크고, 최대 임계치($T_{\max}$)보다 작은 범위이면 탐지자로 선택한다.

3.4 임의의 non-self에 GA를 적용한 항체 생성 과정

정상적인 시스템 콜 시퀀스를 이용한 탐지자는 self의 수집 능력에 따라 긍정적 결함과 부정적 결함이 달라진다. 이를

보완하기 위해 HA 모델에서는 GA를 이용하여 탐지자를 생성한다. 진으로 생성된 비정상 시스템 콜 시퀀스에서 임의의 진을 선택한다. 임의의 비정상 진을 선택하여 GA를 적용한 과정은 그림 4와 같다. 그림 4의 비정상 시스템 콜 시퀀스로 생성된 진은 탐지자의 크기와 일정하게 비례하여 임의로 선택한다. 임의로 선택된 진의 뒷부분을 GA를 적용하여 새로운 진을 생성한다. 새로운 진은 그림 3의 1단계 과정을 수행하여 적절한 진을 탐지자로 선택 한다.

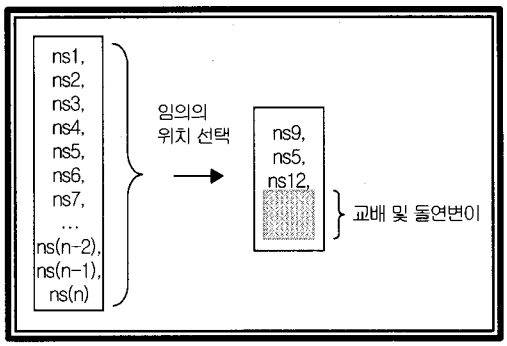


그림 4. 비정상 진의교배와 돌연변이
Fig 4. crossover and mutate of non-self 진

그림 4의 교배 및 돌연변이 과정은 비정상 시스템 콜 시퀀스를 임의로 선택하여 윈도우 크기 6인 진을 생성한다. 윈도우 크기 6으로 생성된 진의 뒤 3자리는 교배연산을 통해 임의의 다른 시스템 콜 번호로 치환되고, 윈도우 크기 6에 맞추어지지 않은 진은 돌연변이 연산으로 시스템 콜이 추가되게 된다. 그림 4의 교배 및 돌연변이 과정을 통해 생성된 진은 탐지자의 모든 진들과 비교 후 동일한 것이 없으면 탐지자로 선택되게 된다.

Ⅳ. 평가

이 장에서는 임의의 비정상 진을 선택 후 교배와 돌연변이를 통해 새로운 후보 항체를 생성하여 제안하는 HA모델을 실험 및 분석한다.

4.1 실험 환경

표 4는 HA모델을 실험 평가하기 위한 실험 환경을 나타내고 있다. HA모델의 유용성 검증을 위해 실험 데이터는 UMN의 가공된 샌드메일 데이터를 참조하였다. 이 데이터는 143개의 정상적인(normal) 프로세스의 system call sequence가 기록되어 있으며, 3개의 비정상적인(abnormal) 프로세스의 system call sequence가 기록되어 있다. 각각의 프로세스에 대한 system call sequence은 N = 6으로 진을 생성하고, R=3, T_{max} = 6, T_{min} = 0으로 실험한다[12].

표 4. 실험 환경
Table 4. Experimental Environment

구 분	내 용
컴파일러	Visual C++ 6.0
메모리	1 GB
CPU	Pentium 4 2.4GHz Processor
OS	Windows XP SP2
데이터	UNM(University of New Maxico)의 가공된 샌드메일 데이터

4.2 실험 방법

홍선에서 T-cell이 생성되는 알고리즘을 적용한 negative selection 방법으로 정상적인 프로세스의 system call sequence로 항체를 생성한다. 생성된 항체의 긍정적 결함 율과 부정적 결함 율을 알아보기 위해서 10CV로 70% 항체(탐지자)와 30% test용 self로 분류한다. 분류된 항체를 이용한 실험에서는 첫째, 70%의 항체가 30%의 self와 모든 non-self의 진을 평가하는 실험을 하고 둘째, 임의의 non-self를 GA를 적용한 새로운 진을 항체 크기에 비례하여 생성한 후 70%의 항체에 추가하여 self와 non-self를 판단하는 실험을 한다.

4.3 실험 결과

이 절에서는 negative selection에 의해 생성된 항체로 self와 non-self 진을 판단하는 실험과 임의의 비정상 시스템 콜 시퀀스의 진에 의해 생성된 항체로 self와 non-self 진을 비교평가하고 있다.

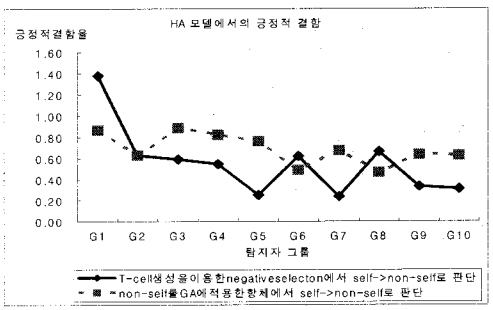


그림 5.긍정적 결함 비교
Fig 5. compare false positive rate

그림 5는 negative selection과 non-self를 적용한 항체의 긍정적 결함을 보여주고 있다. 그림 5의 negative selection 항체는 10CV에 의해 정상적인 시스템 콜 시퀀스의 70%를 항체로 사용하고, non-self를 적용한 항체에서는 negative selection 항체 크기에 비례한 임의의 non-self를 선택한다.

negative selection은 탐지자의 변화에 따라 긍정적 결함률의 차이가 크게 나타나지만 non-self를 적용한 항체는 탐지자의 변화와 상관없이 긍정적 결합률의 차이가 일정하게 나타났다. 전체적인 긍정적 결합률에서는 두 모델이 0.6과 0.65로 0.05의 근소한 차이로 비슷한 결함률을 나타내고 있다.

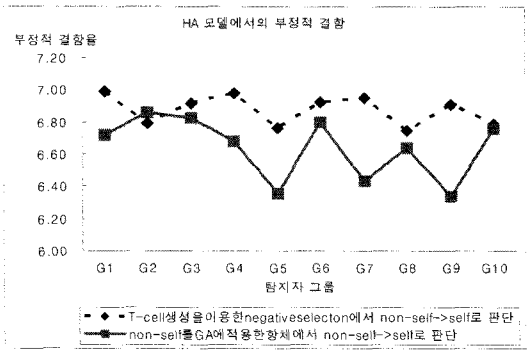


그림 6. 부정적 결함 비교
Fig 6. compare false negative rate

그림 6은 negative selection과 non-self를 적용한 항체에서의 부정적 결함을 보여주고 있다. 그림 6에서 non-self를 self로 판단하는 false negative rate는 non-self에 GA를 적용할 경우가 negative selection보다 0.55% 더 결합률이 낮아졌다. 또한 임의 비정상 시퀀스를 이용한 탐지자의 선택률의 변화는 false negative rate에 많은 영향을 미치지 않는다.

V. 결론

기존 네거티브 셀렉션은 긍정적 결함과 부정적 결합이 있고, self를 이용한 모델로 새로운 침입을 탐지할 수 없는 단점이 있다. 이 논문에서는 이러한 문제점을 개선하기 위해서 system call sequence에 의한 탐지자 생성에 관한 고찰 및 이를 보완하기 위한 HA 모델을 제안하였다. 제안된 HA모델에서는 새로운 침입을 탐지하기 위해서 임의의 non-self를 GA에 적용하여 추가한 항체가 기존 방법보다 평균 0.55% 더 결함률을 낮추었다. 향후 연구는 system call arguments 중에서 time 정보를 이용하여 system call sequence만으로 탐지 할 수 없는 침입을 탐지하기 위한 연구를 수행할 계획이다.

참고문헌

[1] S. Forrest, S. Hofmeyr and A. Somayaji, "Computer Immunology(review article)," In Communications of the ACM Vol. 40, No. 10, pp. 176-177, 2007.

[2] A. Somayaji, S. Hofmeyer, and S.Forrest, "Principles of a Computer Immune System," Proc. of new Security Paradigms Workshop pp. 75-81,Sep, 1997.

[3] F. Cohen. *"Computer viruses,"* Computer & Security, 6:22-35, 1987.

[4] S.Forrest, A. S Perelson, L. Allen and R. Cherukuri, "Self-nonself discrimination in a computer," In Proceedings of the IEEE Symposium on Research in Security and Privacy, IEEE Computer Society Press, Los Alamotos, CA, pp. 202-212, 1994.

[5] 강호영외 12인역, *"Kuby 면역학,"* 월드 사이언스

[6] 위키백과, *http://ko.wikipedia.org/*

[7] Rodney A., "A Biologically inspired immune system for computers," Artificial Life IV, Proceedings on the Fourth International Workshop on Synthesis and Simulation of Living Systems, pp. 130 - 139, 1994.

[8] S. Forrest, Steven A. Hofmeyr, Anil Somayaji, Thomas A. Longstaff, "A Sense of Self for Unix Process," In Proceedings of the 1996 IEEE Symposium on Research in Security and Privacy, Los Alamos, CA, pp. 120-128. IEEE Computer Society Press., 1996.

[9] J. Balthrop, S. Forrest and M. R. Glickman, "Revisition LISYS : parameters and Normal Behavior," In the proceedings of the special sessions on artificial immune systems in the 2002 congress on Evolutionary Computation, 2002 IEEE World Congress in Computational Intelligence, Honolulu, Hawaii, 2002.

[10] Patrik D'haeseleer, Stephanie .Forrest, Paul Helman, "An Immunological Approach to Change Detection:Algorithms, Analysis and Implications," 96

IEEE, pp.120-128, Jun, 1999.

[11] S.A. Hofmeyer, A. Somayaji and S.Forrest, "Intrusion Detection Using Sequences of System Calls," Journal of Computer Security Vol. 6, pp. 151-180, 1998.

[12] Kymic M.C., Tan and Roy A. Maxion, "why 6?" Defining the Operational Limits of stide. an Anomaly-Based Intrusion Detector," Procedings of the 2002 IEEE Symposium on Security and Privacy, pp. 188-201, May 12-15, 2005.

저 자 소 개

신 미 예(Mi-yea Shin)

1990년 :
한발대학교 전자계산학과 이학사
1998년 :
충북대학교 전자계산학과 이학석사
2001년 ~ 현재 :
충북대학교 전자계산학과
관심분야 : 네트워크보안, 인공지능, 정보검색

전 승 흡(Seoung-heup Jeon)

1989년 :
한발대학교 전자계산학과 공학사
1998년 :
한남대학교 전자계산학과 이학석사
2000년 ~ 현재 :
충북대학교 전자계산학과
관심분야 : 네트워크보안, 유비쿼터스, 정보검색

이 상 호 (Sang-ho Lee)

1972년 3월~1976년 2월
숭실대학교 전자계산 공학사
1979년 3월~1981년 2월
숭실대학교 시뮬레이션공학석사
1985년 3월~1989년 2월
숭실대학교 컴퓨터네트워크 공학박사
관심분야 : Protocol Engineering, Network Security, Network Management, Network Architecture