2003년도 대한전자공학회 하계종합학술대회 제26권 제1호

하드웨어 테스트를 위한 새로운 인공 면역 시스템

이상형, 김은태, 박민용

연세대학교 전기 전자공학과
전화 : 02-2123-2868

A New Artificial Immune Approach to Hardware Test Based on The Principle of Antibody Diversity

Sanghyung Lee, Euntai Kim, Mignon Park

Dept . Of Electrical and Electronic Eng, Yonsei University
E-mail : lsh@yeics.yonsei.ac.kr

Abstract

This Paper proposes a new artificial immune approach to hardware test. A Novel Algorithm of generating tolerance conditions is suggested based on the principle of the antibody diversity. Tolerance conditions in artificial immune system correspond to the antibody in biological immune system. The suggested method is applied to the on-line monitoring of a typical FSM (a decade counter) and its effectiveness is demonstrated by the computer simulation.

I. 서론

온라인 하드웨어 테스트는 전자 시스템에서 매우 중요한 요소 중의 하나이며 특히 인간의 손이 닿기 힘든 우주선이나 원자로 등에서는 반드시 필요한 기능이다. 지금까지 하드웨어 테스트를 위해서 여러 가지 이론들이 연구되어 왔으며 그 중에서도 인간의 면역계를 모사한 인공면역 시스템이 최근에 연구되어 왔다. 초창기 연구로 S. Forrest 는 컴퓨터 바이러스와 네트웍 침입의 검출을 위한 Negative Selection algorithm 을 제안하였다. Negative selection 은 기존의 알려진 self pattern 에 대해서 항체를 생성하는 방식이다. 그리고 D'haeseleer 는 greedy detector generating algorithm 을 제안하였다. 이 알고리즘은 기존의 negative selection 알고리즘을 향상시켜 좀 더 나은 검색 영역을 가진다.

하지만 기존에 연구된 인공 면역 시스템은 생체 면역 시스템을 피상적으로 모방했을 뿐 실제적인 생체 면역 시스템과는 거리가 있는 시스템이며 생체면역 시스템의 중요한 개념중의 하나인 antibody diversity 원리를 구현하지 않았다. 따라서 본 논문에서는 antibody diversity 원리를 구현하여 하드웨어 테스트를 위한 새로운 인공 면역 시스템 알고리즘을 제안한다.

본 논문의 2 장에서는 생체 면역 시스템과 하드웨어 디자인을 위한 인공 면역 시스템에 대해서 설명하고 3 장에서 tolerance condition 생성을 위한 새로운 인공 면역 알고리즘을 제안한다. 4 장에서 컴퓨터 모의 실험을 통해서 본 알고리즘의 우수성을 검증한 후 5 장에서 결론을 맺는다.

본 논문은 Korea Institute of Industrial Technology (ITEP)에 의해 지원되었습니다.
(Next Generation new technology development program)

II. 면역 시스템

A. 생체 면역 시스템

생체 면역 시스템은 외부의 바이러스나 박테리아의 침입에 대하여 생체를 보호하는 시스템이다. 즉 외부의 침입에 대해 자기 (self)와 비자기 (nonself)를 구분하여 항원(antigen)이 생성되며 이러한 항원에 대해 항체(antibody)가 생성된다 이 생성된 항체가 해당 항원을 파괴함으로써 외부의 침입으로 생체를 보호하게 되는 것이다.

실제 생체 면역 시스템은 임파구로 구성되어 있다. 임파구는 다시 B cell 과 T cell 로 구분되며 B cell 은 항체를 생성함으로써 항원을 파괴하는 역할을 하며, T cell 은 B cell 의 항체 생성을 돕는 t-helper cell 과 직접 항원을 파괴하는 t-cytotoxic cell 로 나누어진다. 생체 면역 시스템의 상호작용은 그림 1 과 같다.

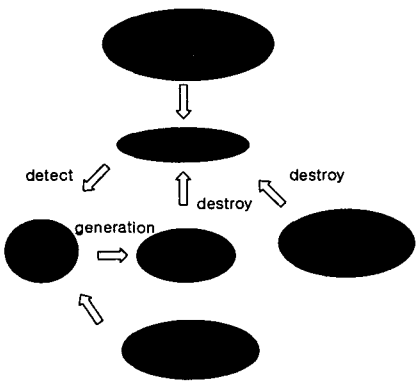

그림 1 생체 면역계의 상호작용

B. 하드웨어 디자인을 위한 인공 면역 시스템

일반적으로 하드웨어는 *finite state machine*(FSM)의 집합으로 표현될 수 있다. FSM은 state와 state사이의 transition을 가진다. 생체 면역 시스템과 하드웨어 테스트 시스템은 표 1과 같은 연관관계를 가진다.

면역시스템	하드웨어 테스트 시스템
Self	유효한 스테이트
Nonself	유효하지 않은 스테이트
항체 생성	Tolerance condition 생성
항체	Set of tolerance conditions (Detectors)
Antibody/antigen binding	Pattern matching

표 1 면역 시스템과 하드웨어 테스트 시스템

하드웨어 테스트를 위한 인공 면역 시스템에서는 알려진 self 에 대해서 tolerance condition 을 생성한 후 에러 state (nonself) 발생시 에러를 검출 해낸다.

III. Antibody diversity 원리에 의한 Tolerance Condition 생성

과학자들은 제한된 유전자의 수로써 어떻게 수많은 항원들에 대한 다양한 항체들을 생성해낼 수 있는지에 대해서 지속적으로 연구해왔다. 이는 항체 생성시 DNA 가 가능한 서로 멀리 떨어져 있도록 생성함으로써 다양한 항체들을 생성하게 되는 것이다. 이러한 원리를 antibody diversity 라고 부른다. 생체 면역 시스템과 마찬가지로 인공면역 시스템에서도 *antibody diversity* 원리는 중요한 역할을 한다. 더 많은 nonself 를 탐지하기 위해서는 더 많은 tolerance condition 들이 필요하다. 만약 nonself 와 같은 수의 tolerance condition 이 존재한다면 모든 nonself 를 탐지할수 있다. 그러나 시스템의 기억공간은 한계가 있고 따라서 tolerance condition 의 수를 줄일수록 더 효율적인 하드웨어 시스템을 구현할 수 있게 된다. 이 때문에 antibody diversity 원리를 구현하는 것은 중요하다.

본 논문에서는 antibody diversity 를 구현하기 위해 새로운 알고리즘을 제안한다. 이 알고리즘은 인간의 면역 시스템을 거의 유사하게 흉내낸 알고리즘이다.

실제로 인간이 항체를 생성하는 것과 유사한 방식으로 유전자 알고리즘을 이용하여 tolerance condition 을 생성한다. 일단 tolerance condition 을 염색체로 코딩한다. 유전자 알고리즘을 통해서 tolerance condition 을 생성하기 위해서는 두 가지 점을 고려해야 한다. 첫번째는 tolerance condition 은 self 와 멀리 떨어져 있어야 하고 두 번째는 tolerance condition 들끼리 서로 멀리 떨어져 있어야 한다. 이 두 번째 고려사항이 바로 antibody diversity 의 원리이다. 이렇게 antibody diversity 의 원리를 구현함으로써 더 작은 수의 tolerance condition 만으로 더 많은 수의 nonself 를 self 와 구분해낼 수 있다. 본 알고리즘에서의 거리는 hamming distance 가 사용되었다.

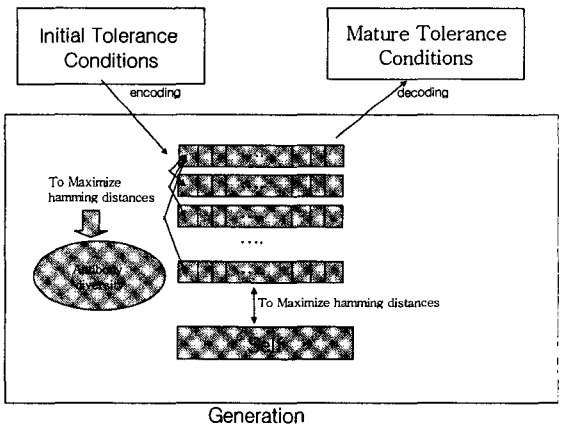

그림 2 제안된 알고리즘

IV. 모의 실험

본 논문에서 제안된 알고리즘을 십진 카운터에 적용함으로써 그 성능을 확인한다. Self 문자열의 구조는 표 2 와 같다.

Function	0 to 9 counter
States	10
Size (bits)	4
Operation	Incremental count (CEN=1,RST=0) Hold (CEN=0, RST=0) Reset (CEN=X, RST=1)

표 2 Self String 의 구조

십진 카운터에서 적절한 self string 의 개수는 40 개가 된다 (40 x 10 bits). Tolerance condition 의 적합도를 평가하기 위한 함수는 다음과 같이 구성된다.

Fitness
= the hamming distances
(between self and tolerance conditions)
+ the hamming distances
(between tolerance conditions)

Tolerance condition 의 개수를 각각 25, 50, 75, 100 개로 정한 후 nonself 탐색율을 구한 결과는 표 3 과 같다. 기존의 greedy detector 에 비해서 더 나은 효율을 보여준다.

Detector Set Size (Tolerance Conditions Size)	Nonself Strings Detectable (Proposed Algorithm)	Nonself Strings Detectable (Greedy Detector)
25	77.74 %	46.25 %
50	92.37 %	70 %
75	96.13 %	81%
100	98.17 %	88 %
125	99.22 %	91 %

표 3 제안된 알고리즘과 greedy detector 의 nonself 탐색율 비교

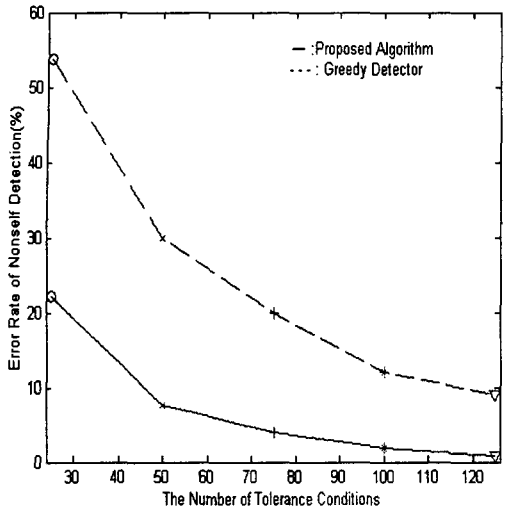

그림 3 nonself 검출시 에러율

V. 결론

본 논문에서는 on-line 하드웨어 테스트를 위한 새로운 인공 면역 알고리즘을 제안하였다. 이 알고리즘은 생체 면역 시스템에서 가장 중요한 개념 중 하나인 antibody diversity 원리를 기반으로 구현되었기 때문에 본 알고리즘에 의해 생성된 tolerance condition 은 실제 생체면역 시스템에서의 항체 생성 방식과 유사하다. 제안된 알고리즘을 컴퓨터 모의 실험을 통해 실제 FSM 의 가장 일반적인 예인 십진 카운터에 적용하여 기존의 greedy detector 에 비해 더 나은 성능을 보임을 확인하였다. 추후 과제로는 본 알고리즘에 대한 좀더 확률적인 분석이 요구된다.

References

[1] S.Forrest, L.Allen, A.S. Perelson, and R.Cherukuri, "Self-Nonself Discrimination In A Computer," *Proceedings of IEEE Symposium on Research in Security and Privacy,* 1994, pp.202-212

[2] Y. Chen and T. Chen, "Implemneting Fault-Tolerance Via Modular Redundancy With Comparison," *IEEE Transactions on Reliability*, Volume: 39 Issue: 2 , Jun 1990, pp. 217 –225

[3] D.W. Bradley and A.M. Tyrrell, "Immunotronics-Novel Finite-State-Machine Architectures With Built-In Self-Test Using Self-Nonself Differentiation," *IEEE Trans. On Evolutionary Computation*, Vol.6, No. 3, June 2002, pp. 227-238

[4] P. K. Harmer, P. D.Williams, G. H. Grunsch, and G. B.Lamont, "An Artificial Immune System Architecture For Computer Security Applications," *IEEE Transactions on Evolutionary Computation,* Vol.6, No.3, June 2002, pp. 252-280

[5] D.Dagupta, Ed., Artificial Imune Systems and Their Applications, Heidelberg, Germany:Springer-Verlag, 1999

[6] S.Forrest, L.Allen, A.S. Perelson, and R.Cherukuri, "Self-Nonself Discrimination In A Computer," *Proceedings of IEEE Symposium on Research in Security and Privacy,* 1994, pp.202-212

[7] P.D'haeseller, S. Forrest, P. Helman, "An Immunological Approach to Change Detection : Alogorithms, Analysis and Implications," *Proc. Of IEEE Symp. On Security and Privacy*, 1996