International Journal of Fuzzy Logic and Intelligent Systems, vol. 4, no. 1, June 2004 pp. 7-11

A Biologically Inspired New Hardware Fault Detection : immunotronic and Genetic Algorithm-Based Approach

Sanghyung Lee, Euntai Kim and Mignon Park

Dept. of Electrical and Electronic Engr., Yonsei Univ.,
ICS Lab., Dept. of Electrical and Electronic Engr.,
Yonsei Univ., Shinchon-dong 134, Seodaemun-gu, Seoul, Korea

Abstract

This paper proposes a new immunotronic approach for the fault detection in hardware. The suggested method is, inspired by biology and its implementation is based on genetic algorithm. Tolerance conditions in the immunotronic system for fault detection correspond to the antibodies in the biological immune system. A novel algorithm of generating tolerance conditions is suggested based on the principle of the antibody diversity and GA optimization is employed to select mature tolerance conditions in immunotronic fault detection system. The suggested method is applied to the fault detection for MCNC benchmark FSMs (finite state machines) and its effectiveness is demonstrated by the computer simulation.

Key words : Immunotronic system, hardware fault detection, tolerance conditions, antibody diversity

1. Introduction

Fault detection for hardware is an important technique in the fault tolerant hardware and many researches for fault detection have been developed. Especially, fault detection is indispensable to the system the hand of the person cannot reach such as spacecraft system or nuclear power reactor. Yinong Chen proposed a fault detection system using n-modular redundancy [1], S. Dutt proposed error-detecting and correcting code [2] and P.K Lala suggested self-checking logic circuit [3].

Over the last decade, a new techniques inspired by the biological immune system, called the artificial immune system, has been extensively studied and applied to various fields such as computer security [4][5], virus protection [4], and anomaly detection [6]. D. Dasgupta brought the immune principles into multi-agent system [7]. S. Hofmeyr gave an immune system model used for distributed detection [8].

Particularly, the immunotronic system has proven to be useful in the fault detection system for hardware. In contrast to the previous methods, imperfect matching is fully utilized in the immunotronic system for hardware fault detection. Imperfect matching enables the system to detect nonselfs though they are not known to the system and faults can be detected by tolerance conditions which are generated from the information of selfs by negative selection algorithm. Tolerance conditions in the immunotronic system correspond to antibodies in the biological immune system and the most important problem in designing the immunotronic system for hardware fault detection is how to generate tolerance conditions effectively and to distinguish nonselfs from selfs.

As a pioneering work, Bradley et al. suggested immunotronics(electronics + immune system) for FSM fault detection [9]. To generate tolerance conditions, they adopted negative selection algorithm proposed by S. Forrest [6] and greedy detector generating algorithm [10] and a matching method for these algorithms is c-contiguous matching one.

But the previous immunotronic system imitated the biological immune system in a superficial manner. Actual biological aspect of the immunological matching was not fully exploited. That's, the previous immune-based algorithms did not take into account the principle of antibody diversity which is one of the most important concepts in the biological immune system. This paper proposes a new immunotronic system for fault detection. A novel algorithm of generating tolerance conditions is suggested. GA is employed to select the mature tolerance conditions.

The rest of the paper is organized as follows : The biological immune system and the immunotronic system for fault detection are compared in Section 2. In Section 3, the new algorithm of generating tolerance conditions which is superior to the previous generation and matching algorithms is proposed and in section 4, the new algorithm applied to FSMs is demonstrated by the computer simulation. The paper concludes with some discussions in Section 5.

2. Problem Formulation

A. The biological immune system

The biological immune system protects body from the attack of invaders or antigens such as virus and bacteria. The biological immune system consists of two types of lymphocytes : B cells and T cells. B cells generate antibodies

Manuscrip received Apr. 6, 2004; revised May. 28, 2004.
This work was supported by the Ministry of Commerce, Industry and Energy of Korea.

which destroy the antigens. T cells are divided into T-helper cells which help B cells to generate antibodies and T-cytotoxic cells which kill the antigens directly. In general, the immune operation of B cells is called humoral immunity and the immune operation of T-cells is called cell mediated immunity. Interaction of the biological immune system is shown in Fig. 1.

B. The immunotronic system

In this paper, a new immunotronic system is proposed for the fault detection in FSMs. The relationship between the biological immune system and the immunotronic system for fault detection is listed in Table 1.

In the immunotronic system for fault detection, a set of tolerance conditions is generated using known selfs through negative selection algorithm so that the set detects the nonselfs. Tolerance conditions in the immunotronic system correspond to antibodies in the biological immune system and how to generate a set of tolerance conditions is the most crucial problem in the fault detection for hardware. In this paper, the new algorithm taking into account the principle of antibody diversity, the important concept in the biological immune system, is proposed. The proposed algorithm adopts the way the biological immune system works more than the previous immunotronics [9]. Mature tolerance conditions are generated automatically through genetic algorithm just as the mature antibodies are chosen by clonal selection, recombination and mutation in the biological immune system.

3. Generation of Tolerance Conditions

A. The principle of antibody diversity

Scientists long wondered how the biological immune system generates the proper antibodies against many antigens with a limited number of genes. The answer is that antibody genes are pieced together from widely scattered bits of DNA when they are generated by recombination and mutation. For this reason, antibodies can have the extreme diversity and the immune system has the capacity to recognize and response to about 10^7 different antigens. This is called the principle of antibody diversity [11]. As in the biological immune system, the principle of antibody diversity can play an important role in the immunotronic system. The process of antibody generation considering the principle of antibody diversity is shown in Fig. 2. In the immunotronic system, to cope with diverse antigens and achieve the excellent fault detection with a limited number of tolerance conditions, we have to design the tolerance conditions such that the distances between tolerance conditions are maximized. That is the immunotronic version of the principle of antibody diversity.

To detect more nonselfs, we need more tolerance conditions. If we have the same number of tolerance conditions as nonselfs, we can detect all the nonselfs. But the memory of the fault detection system is limited, so the smaller the number of tolerance conditions is, the more effective the system is. The implementation of the principle of antibody diversity could be the solution to the problem. It could help the effective detection of nonselfs with a limited number of tolerance conditions.

Table 1. The biological immune system vs. the immunotronic system

Biological immune system	Immunotronic system for fault detection
Self	Valid state transition
Nonself	Invalid state transition
To create antibody	Generating of tolerance conditions
Antibody	Set of tolerance conditions (Detectors)
Antibody/antigen binding	Pattern matching

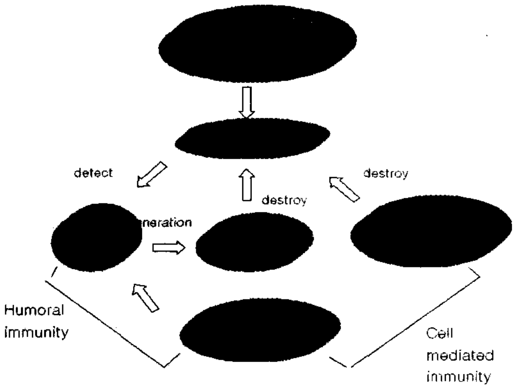


Fig.1 Interaction of the biological immune system

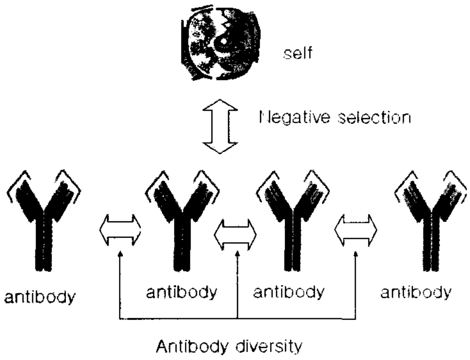


Fig. 2 The Process of Antibody Generation

To generate tolerance conditions which are diverse as possible, we choose the following function Eq.(1) :

$$Fitness = \sum_{i=1}^{N_r} (\min{}_{j=0}^{n} (H(\sigma_j, \tau_i))) + \sum_{i=1}^{N_r} \sum_{j=1}^{N_r} H(\tau_i, \tau_j) \qquad (1)$$

n: *the number of self strings*
N_r; *the number of tolerance conditions*
σ_j; *jth self string*$(1 \le j \le n)$
τ_i; *ith tolerance condition*$(1 \le i \langle N_r)$

$$H(X, Y) = \sum_{i=1}^{N} (x_i \oplus y_i) \quad X, Y \in \{0, 1\}: \ Hamming\ Distance$$

The first component of the fitness function Eq.(1) corresponds to negative selection and prohibits the undesired binding of the selfs. The second component is aimed at the proper allocation of tolerance conditions to achieve the antibody diversity

B. GA Optimization

Genetic algorithm is the optimization algorithm based on evolution mechanism of nature [12]. In the previous section, the fitness function for selecting mature tolerance conditions is designed based on the antibody diversity and negative selection.

In this section, binary GA optimization is employed to maximize the fitness function Eq. (1) and determine the suboptimal tolerance conditions. N_r tolerance conditions are generated through mutation, crossover of GA, which is very similar to the biological immune system. N_r tolerance conditions are coded into a chromosome. The length of a tolerance condition (same as the length of a self) is p bits and the size of a chromosome is $p\times N_r$ bits. The structure of the chromosome is shown in Fig. 3.

GA involves two basic genetic operators of crossover and mutation. The crossover operator explores the search space by exchanging some parts of the chromosome. In our problem, in order to select the individuals for crossover, stochastic universal selection is performed and single point crossover is used. The mutation operator introduces the diversity into a population and avoids its premature convergence to local minima. The parameters of genetic operators used in this simulation are shown in Table 2.

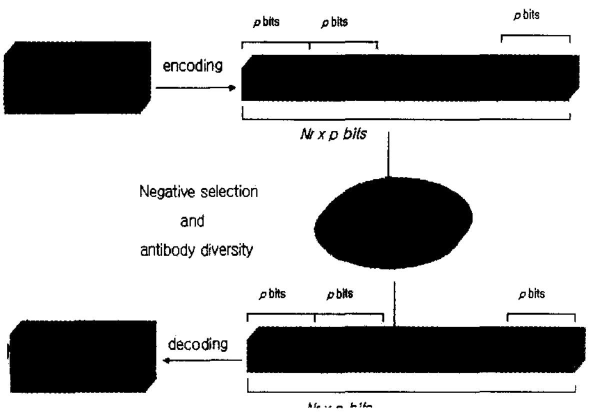


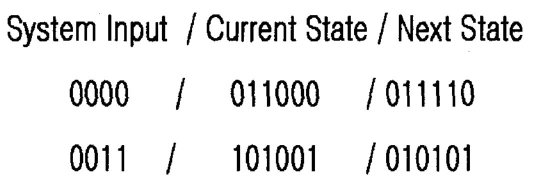
Fig 3.The Process of Antibody Generation

Table 2 Genetic Parameters

Parameter	Value
The Number of Individual	1000
The Number of Generation	10000
The Size of Chromosome	$p\times N_r$
Mutation Probability	$0.7/\,p\times N_r$
Crossover Probability	0.7

4.Simulation

The algorithm suggested in this paper is applied to a decade counter, a typical example of FSM [9] and MCNC benchmark FSMs [13]. An individual string is formed from the combination of a user input and previous and current sta the stn



System Input / Current State / Next State

0000 / 011000 / 011110

0011 / 101001 / 010101

Fig.4 The Structure of selfs

A. A decade counter

This example is taken from [9]. There are forty valid transitions in a decade counter and the number of selfs is forty. Tolerance conditions are generated by the suggested method. For the various number of tolerance conditions, the simulation is performed fifty times and the nonself detection rates are shown in Table 3. The results are compared to the results of greedy detecting algorithm [9] in Table 4 and Fig. 5.

The fault detection system using tolerance conditions which are generated by the proposed method shows the improved the nonself detection rates than the previous method. Especially when the number of tolerance conditions is small, the suggested method shows better performance than the previous method. The reason might be that tolerance conditions are widely spread due to the principle of antibody diversity and cover wider area in the state space.

Table 3. Nonself detection rates(The number of runs :50)

Detector Set Size	Best	Worst	Average
25	78.12 %	75.32 %	77.74 %
50	93.13 %	90.31 %	92.37 %
75	96.50 %	95.22 %	96.13 %
100	98.08 %	97.98 %	98.01 %
125	99.35 %	99.12 %	99.22 %

Table 4. Nonself detection rates comparison between proposed algorithm and greedy detector

Detector Set Size	Proposed Algorithm	Greedy Detector
25	77.74 %	46.25 %
50	92.37 %	70.01 %
75	96.13 %	81 %
100	98.1 %	88 %
125	99.2 %	91 %

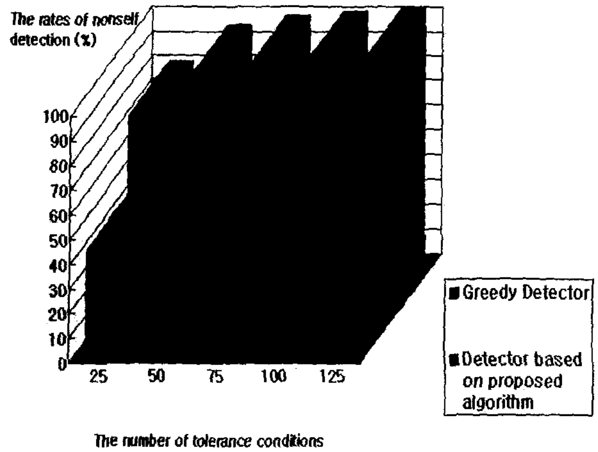


Fig. 5 The rates of nonself detection

B. MCNC benchmark FSMs

In this subsection, the suggested algorithm is applied to MCNC benchmark FSMs. The MCNC FSMs are a standard set of FSMs and are used for fault detection in numerous research papers [13].

The simulation is performed fifty times. In this problems, the number of tolerance conditions is set to a half of the number of selfs and this number is the pertinent to show the performance of the proposed algorithm. The average nonself detection rates are shown in Table 5. It can be seen in Table 5 that the suggested method shows good average nonself detection rates for MCNC FSMs. Especially, the larger are the difference between the number of selfs and the number of nonselfs, the better is the performance of the proposed algorithm.

Table 5. Average nonself detection rates for MCNC benchmark state machines

FSM name	The number of selfs	String length	The number of TCs	Average nonself detection rates
bbara	160	12	80	91.08 %
dk16	108	12	54	81.2 %
ex6	248	11	124	73.2 %
lion9	29	10	14	85.1 %
s8	20	10	10	86.75 %
train11	25	10	12	75.12 %

5. Conclusion

This paper proposes a new immunotronic approach to the fault detection in hardware based on the principle of antibody diversity and GA optimization. The suggested method resembles the generation of the antibodies in the actual biological immune system. The suggested method is applied to the fault detection for the various FSMs (a decade counter and MCNC benchmark FSMs) and its effectiveness is demonstrated by computer simulation. In a decade counter, the fault detection system using tolerance conditions which are generated by the proposed method shows the improved nonself detection rates than the previous method. In MCNC benchmark FSMs, the fault detection system also shows good average nonself detection rates. For the future study, its probabilistic analysis is required in this algorithm.

Reference

[1] Y. Chen and T. Chen, "Implementing fault-tolerance via modular redundancy with comparison," *IEEE Transactions on Reliability*, Volume: 39 Issue: 2 , Jun 1990, pp. 217 -225

[2] S. Dutt and N.R Mahapatra, "Node-covering, error-correcting codes and multiprocessors with very high average fault tolerance," *IEEE Trans. Cput.*, Vol. 46, Sep.1997, pp.997-1914

[3] P.K. Lala, Digital Circuit Testing and Testablilty, New York: Academic, 1997

[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] S. Forrest, S.A. Hofmeyr, A. Somayaji, and T.A. Longstaff, "A Sense of Self for Unix Processing," Proc.*IEEE Symp. Computer Security and Privacy*, May, 1996, pp.120-128

[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] D. Dasgupta, "An artificial immune system as a multi-agent decision support system," Proc. *IEEE Int. Conf. Systems, Man and Cybernetics*, Oct. 1998, pp.3816-3820

[8] S.A Hofmeyr and S. Forest, "Architecture for an artificial immune system," *Evol.Comput.*,vol.8 no.4, 2000, pp.443-473

[9] 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

[10] 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

[11] R.A. Goldsby, T.J. Kindt, and B.A Osborne, Kuby Immunology, 4th ed. W.H Freeman and Company: New York, 2000

[12] D.E Goldberg, Genetic Algorithms in Search, Optimization and Matching Learning,

Addison-Wesley:MA 1989

[13] S.Yang "Logic Synthesis and Optimization Benchmarks User GuideVersion 3.0," *Technical report*, Microelectronics Center of North Carolina, Jan. 1991

Sanghyung Lee

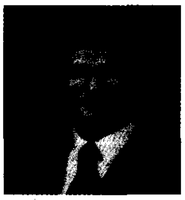
He received the B.S. and M.S. degree in electronic engineering from Yonsei University, Seoul, Korea, in 1996 and 1999, respectively. He is currently a Ph.D. candidate of Dept. of Electrical and Electronic engineering in Yonsei University. His research interests include the genetic algorithm, artificial immune system, evolvable hardware, and fuzzy control.

Phone : +82-2-2123-2868
Fax : +82-2-312-2333
E-mail : lsh@yeics.yonsei.ac.kr

Euntai Kim

Euntai Kim was born in Seoul, Korea, in 1970. He received the B.S. (summa cum laude) and the M.S. and the Ph.D. degrees in electronic engineering, all from Yonsei University, Seoul, Korea, in 1992, 1994 and 1999, respectively. From 1999 to 2002, he was a full-time lecturer in the Department of Control and Instrumentation Engineering at Hankyong National University, Kyonggi-do, Korea. Since 2002, he has joined the faculties of the Department of Electrical and Electronic Engineering at Yonsei University, where he is currently an assistant professor.

Phone : +82-2-2123-2863
E-mail : etkim@yonsei.ac.kr



Mignon Park

He received the B.S. degree and M.S. degree in electronics from Yonsei University, Seoul, Korea, in 1973 and 1977, respectively. He received the Ph.D. degree in University of Tokyo, Japan, 1982. He was a researcher with the Institute of Biomedical Engineering, University of Tokyo, Japan, from 1972 to 1982, as well as at the Massachusetts Institute of Technology, Cambridge, and the University of California Berkeley, in 1982. He was a visiting researcher in Robotics Division, Mechanical Engineering Laboratory Ministry of International Trade and Industry, Tsukuba, Japan, from 1986 to 1987. He has been a Professor in the Department of Electrical and Electronic Engineering in Yonsei University, since 1982. His research interests include fuzzy control and application, robotics, and fuzzy biomedical system.

Phone : +82-2-2123-2868
Fax : +82-2-312-2333
E-mail : mignpark@yonsei.ac.kr