Proceedings of KFIS 2001 Spring Conference, 2001. 5.

인공 면역계를 이용한 자기변경 검사 알고리즘

Self-Change Detection Algorithms using the Artificial Immune System

선상준 · 전호병 · 박세현 · 심귀보
Sang-Joon Sun, Ho-Byung Chun, Se-Hyun Park, and Kwee-Bo Sim

중앙대학교 전자전기공학부
School of Electrical and Electronic Engineering, Chung-Ang University
E-mail : kbsim@cau.ac.kr

요 약

최근 컴퓨터와 인터넷의 급속한 발전과 더불어 컴퓨터의 데이터를 파괴하는 바이러스나 정보를 빼내기 위한 해킹 등이 만연하고 있다. 이에 컴퓨터의 데이터를 보호하기 위한 방법들이 연구 중에 있는데 이 중 외부의 침입물질에 대해 자체적인 보호와 제거기능을 가지는 생체면역시스템을 이용한 컴퓨터면역시스템 구축에 대해 활발히 연구가 진행되고 있다. 생체 면역시스템은 바이러스나 병원균 등의 낯선 외부 침입자로부터 자신을 보호하고 침입자를 제거한다. 본 논문에서는 생체면역시스템의 면역세포 중 하나인 세포독성 T세포의 자기(Self)와 비자기(Nonself)를 구분하는 기능을 이용해 자기변경 검사 알고리즘을 구현하였다. 구현한 알고리즘은 자기로 인식하는 자기파일에서 자기를 구분하는 MHC 인식부를 구성한다. 이렇게 구성한 MHC 인식부는 자기파일을 대표하는 값을 이용하여 변경된 파일을 구분한다. 이 알고리즘을 변경된 자기파일에 적용함으로서 컴퓨터 해킹이나 바이러스에 의한 자기파일의 변경 검사의 유효성을 검증한다.

Abstract

According to the rapid growth of computer and internet recently, A hacking to steal informations and the computer virus to destroy the data in computer are now prevailing in the whole world. A study of methods to protect the data of computer is in progress. One of the study is construction of computer immune system using biological immune system that has ability of removal and protection from external invasion. In this paper, we make a change detection algorithm which is based on ability of distinction between self and nonself in T-cytotoxic cell that is one of biological immune cell. In algorithm, MHC receptors are composed of a part of self-file that is recognized as itself and those shall distinguish self-file from the changed file. As a result of applying this algorithm to the changed self-files, we prove the efficacy of detection of the self-files changed by computer virus and hacking.

Key Words : 생체 면역시스템, 자기-변경 검색 알고리즘, 인공 면역시스템, 매칭 알고리즘

Ⅰ. 서 론

컴퓨터 바이러스는 생물학의 바이러스와 같은 자기 복제와 파괴 능력을 갖고 컴퓨터에서 실행되는 프로그램의 일종으로서 감염 대상인 컴퓨터 프로그램이나 데이터 파일을 파괴한다. 최근 컴퓨터의 사용이 보편화되면서 악의적 사용자에 의해 이러한 컴퓨터 바이러스의 피해가 급속히 증가하고 있으며, 파일의 손상에 그치지 않고 시스템을 파괴하는 바이러스들도 등장하고 있다. 해킹은 주로 다른 사람의 컴퓨터에 침입해 정보를 가져오거나, 그 컴퓨터가 가지고 있는 정보를 없애는 작용으로 인터넷의 지속적인 발전에 의해 하나의 네트워크로 연결된 많은 컴퓨터의 피해가 확산되고 있다. 이렇게 남의 컴퓨터에 침입하는 해킹이나 데이터를 파괴하는 컴퓨터 바이러스에 의한 피해를 막기 위해 최근에 생명체의 면역시스템의 특징을 이용

한 시스템 침입탐지와 바이러스 탐지 및 치료에 대한 연구가 활발히 진행 중에 있다[1-4].

생명체의 면역계는 외부에서 침입해 세포나 장기에 피해를 주는 물질인 항원에 대해서 스스로 자기세포와 구분해 인식하고 제거하는 기능을 가지고 있다. 면역계의 특징들 중의 하나인 항원을 인식하는 기능은 자기세포의 확실한 인식을 가지고 있는 상태에서 자기세포와 다름으로 구분되는 물질로 분류하는 자기/비자기(self/non-self) 인식방법으로 볼 수 있다. 이러한 기능을 가장 잘 보여주는 면역 T세포 중의 하나인 세포독성 T세포(T-cytotoxic Cell)는 자기세포를 인식하는 부분과 항원으로 인식하는 부분으로 구성되어 항원에 의해 감염된 자기세포를 찾아 제거하는 역할을 한다[5].

본 논문에서는 생명체의 면역계에서 중요한 역할을 하는 세포독성 T세포의 자기인식 과정인 Positive Selection과 Negative Selection을 모델링하여 침입에 의한 데이터 변경과 바이러스에 의한 데이터 감염 등을 탐지할 때 가장 중요한 요소인 자기와 비자기의 구분 알고리즘을 구현하고, 이를 이용한 자기변경 탐지(Self-Change Detection) 알고리즘을 이용해 서 컴퓨터 해킹이나 바이러스에 의한 자기파일의 변경 검사의 유효성을 검증한다.

II. 알고리즘 구현

2.1 생체면역 시스템

생명체의 방어체계인 면역계은 박테리아, 기생균, 병원균, 독소, 바이러스 등과 같이 항원이라고 통칭하는 매우 다양한 외부 유기체나 단백질에 대하여 생명체의 세포와 장기를 방어할 수 있는 매우 정교하고 복잡한 시스템이다. 이러한 생명체의 면역계는 중앙처리장치인 뇌의 명령에 따르는 것이 아닌 각 요소의 자율적인 행동이 유기적으로 결합되어 형성된 자율분산 시스템으로 항원을 인식하는 기능, 정보처리 기능, 학습 및 기억능력, 자기와 비자기의 구별능력, 분산시스템으로서 전체의 조화를 유지하는 능력 등을 가지고 있다. 이렇듯 복잡하게 형성된 면역계를 구성하는 기본요소는 두 가지 형태의 림프구이다. 이는 B세포와 T세포로써, B세포는 항원을 죽이는 역할인 항체를 분비하는 체액성 반응을 하며, T세포는 면역에 관련된 세포를 자극 또는 억제하거나 항원에 의해 감염된 자기세포를 죽이는 세포성 반응을 주로 담당한다.

초기 외부의 침입 물질인 항원이 발생하면 대식세포 등과 같은 식세포에 의한 1차 면역반응이 형성된다. 이 과정에서 대식세포는 항원제공세포(Antigen-Presenting Cell, APC)로서 항원의 특정부위의 정보를 수집, 이를 항원의 모습으로 설정하여 제공한다. 이렇게 모여진 정보는 보조 T세포(T-helper Cell)를 자극시켜 정보가 전달된다. 보조 T세포는 전달받은 항원의 특징을 가지는 세포독성 T세포(T-cytotoxic Cell)와 B세포(B-Cell)를 찾아 각각의 세포를 자극한다. 자극 받은 B세포는 항원의 특징을 가지는 항체를 생산하는 Antibody-forming Cell과 항원과 작용하는 B세포를 만들기 위해 혈장세포(Plasma Cell)로 분화한다. 나중에 이 혈장세포는 항원의 특징을 가지는 기억세포가 된다. 침입한 항원의 특징을 가지는 세포독성 T세포는 자신의 세포 중에서 감염된 세포를 찾아서 제거하는 역할을 하게 된다. 항원이 감소하기 시작하면 T세포의 일종인 억제 T세포(T-suppressor Cell)에 의해 B세포와 T세포의 활동이 억제된다. 이러한 일련의 과정이 2차 면역반응이다.

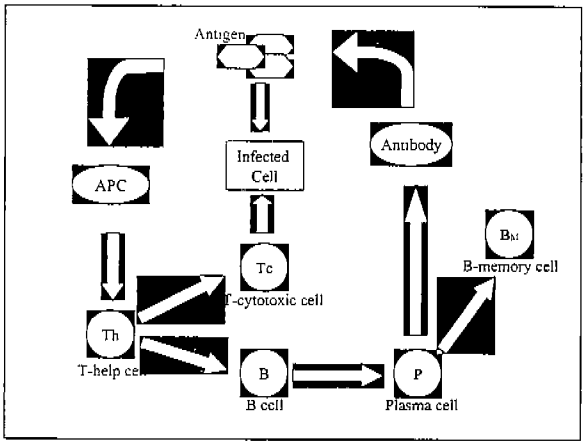

그림 1. 생체 면역시스템의 상호작용도

2.2 Positive Selection과 Negative Selection

각 면역세포는 항원과 자기세포의 수용체를 가지고 있다. 항원과 반응하는 B세포에는 항원수용체(Antigen Receptor)가 존재하여 항체의 모양을 결정하며, T세포 중의 하나인 세포독성 T세포의 경우 항원과 더불어 자신의 세포를 구별해야하므로 항원을 구별하는 항원수용체와 자기세포 판별용 단백질 MHC(Major Histo-compatibility Complex, 주조직 적합성 복합체)를 제한하는 MHC 제한(MHC Restriction) 기능을 가지고 MHC로 인식되며 항원수용체에 수용되는 세포는 감염된 자기세포로 인식하게 된다. 이러한 T세포와 B세포 항원수용체는 MHC 단백질을 항원으로 인식하면 안되며 MHC 제한기능에서는 MHC 단백질을 정확히 인식해야한다. 따라서 각 면역세포들은 초기 생성시 Positive Selection과 Negative Selection을 통해 정상적인 기능을 가진 세포로 구성된다.

Positive Selection은 각 면역세포의 MHC 제한기능을 확인하는 방법이다. 자기세포에서 분비되는 MHC 단백질을 정확히 인지할 수 있는 면역세포만이 사용가능하기 때문에 갓 생성된 면역세포에 MHC 단백질을 결합시켜 긍정적인 선택이 되는 세포들로만 구성하게 된다.

Negative Selection은 항원수용체가 MHC 단백질을 항원으로 인식하지 못하게 하기 위한 방법으로 면역세포에 MHC 단백질을 결합시켰을 때 항원수용체가 부정적인 선택을 하는 세포만으로 구성된다. 이 두 가지 선택을 거친 면역세포는 MHC 단백질을 자신으로 인식하면서 이를 항원으로 인식하지 못하게 구성되어 생명체에서 정상적인 면역반응을 형성한다.

2.3 세포독성 T세포 Modeling

본 논문에서는 항원을 인식하는 항원수용체와 MHC 단백질을 제한하는 MHC 제한기능을 형성해 주는 두 가지 선택법인 Positive Selection과 Negative Selection을 이용해 컴퓨터 상에서 존재하며 자기로 인식해야하는 파일이나 기능에 대해 구별할 수 있는 T세포 기능의 MHC 제한기능을 자기파일의 MHC 인식부로서 모델링하였다. MHC 인식부는 자기파일의 셀이 가지는 위치와 셀의 연속적으로 이루어진 스트링들을 이용해 구성한다. 자기파일의 해킹이나 바이러스에 의한 변화나 자기파일과의 일치성을 검사할 때는 구성된 MHC 인식부들의 데이터를 토대로 파일의 위치에 따른 연속된 부분의 존재여부를 이용해 구분한다.

구현된 알고리즘은 다음과 같다.

[1] 자기파일(컴퓨터 상에서 자신으로 인식해야 하는 파일)을 일정한 크기인 셀(Cell)로 나눈다. 이 셀은 하나의 모델링된 MHC 인식부의 크기가 되며 자기파일 변경검사의 단위가 된다. 셀은 여러 개의 스트링(String)으로 구성되며 각 스트링은 정해진 개수의 값 중 하나의 값을 가진다.

[2] 구성된 셀들을 이용해 셀과 동일한 크기의 MHC 인식부를 구성한다. 각각의 자기파일의 셀에 위치하는 일정한 개수의 연속적인 스트링을 가져와 MHC 인식부의 하나로서 구성한다. 이러한 MHC 인식부 N개가 자기파일의 여부를 검사하는 검사 셀을 이루며 이를 자기파일 변경검사(Change Detection)에 사용한다.

[3] 자기파일 여부의 검사는 구성된 MHC 인식부를 이용하여 이루어진다. 각각의 인식부의 일정한 개수의 연속적인 셀이 자기파일에 존재하는가를 검사하여 인식부를 이루고 있는 연속 셀 모두가 존재하면 해당 인식부에 의해서는 자기파일로 인식한다. 이러한 과정이 검사 셀을 이루는 모든 인식부에서 자기파일로 판명된 경우만을 자기파일로 인식한다.

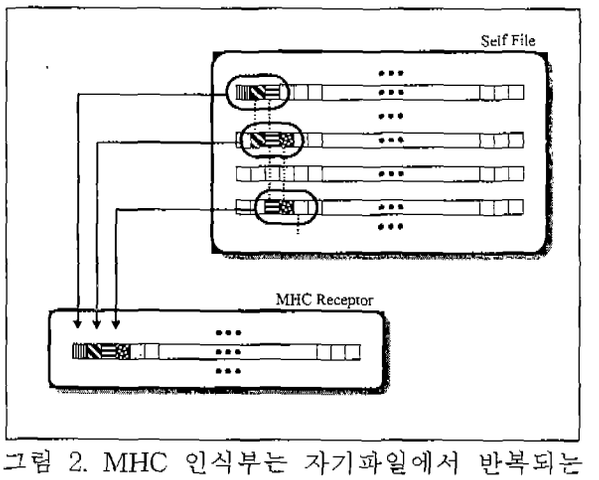

그림 2. MHC 인식부는 자기파일에서 반복되는 연속스트링을 이용하여 구성한다.

III. 자기파일의 변경 검색 시뮬레이션

구성된 MHC 인식부를 이용한 자기파일의 변경탐지에 대한 시뮬레이션은 컴퓨터에서 자기파일을 만든 다음 이를 변경시켜 얻어지는 변형파일의 탐지여부를 이용하여 MHC 인식부의 성능을 평가하였다.

3.1 시뮬레이션 조건

제안한 MHC 인식부에 의한 자기변경 탐색알고리즘의 유효성을 검증하기 위해서 시뮬레이션 조건을 다음과 같이 설정하였다.

자기파일은 컴퓨터에서 자기로 인식되는 파일로 시뮬레이션에서는 일정 크기의 파일을 자기파일로 이용하였다. 자기파일의 각 스트링을 이루는 심벌의 개수는 256개로 2진 8비트의 크기로 나타낸다. 이는 문자를 나타내는 컴퓨터의 단위가 Character의 2진 8비트 코드를 기본으로 형성하기 때문에 이와 비슷한 방법으로 구현하기 위함이다.

셀은 32개의 스트링으로 구성하였으며 총 1600개의 셀로 자기파일을 구성하였다. 각각의 셀 분할로 자기파일은 32개의 위치 정보를 가지게 된다. MHC 인식부는 2개의 연속적인 스트링을 하나의 셀에서 가져와 구성하였다. 따라서 하나의 MHC 인식부는 31개의 자기파일의 셀에서 각 위치에 해당하는 부분으로 이루어졌다. 자기파일의 변경방법은 두 가지를 이용하였다. 하나는 극소의 위치 변경에 의한 MHC 인식부의 자기파일 변경의 검색율을 확인하기 위해 자기파일의 몇 개의 스트링을 변경하는 스트링 변경(String Change)과 자기파일의 일정부분 변경에 따른 검색율을 확인하기 위해 자

기파일의 몇 개의 셀을 변경하는 셀 변경(Cell Change) 방법의 두 가지를 이용하였다. 스트링 변경의 시뮬레이션은 MHC 인식부의 자기파일 변경에 따른 검사의 유효성 검증이며 셀 변경 시뮬레이션은 해킹이나 바이러스 등에 의한 자기파일 일부분의 변경검사에 대한 유효성을 보여주는 것이다.

3.2 시뮬레이션 결과

표 1은 스트링 변경과 MHC 인식부 개수를 변화시켜 얻은 시뮬레이션 결과이다. 결과에서 보듯이 MHC 인식부를 이용한 자기파일의 변경검사가 가능하며 자기파일과 변경된 파일간의 유사도와 인식부의 개수가 인식율에 영향을 주어 낮은 유사도와 많은 개수일 때 인식율이 높아짐을 알 수 있다.

표 1. 스트링변경에 따른 변경된 자기파일 10,000개에 대해서 MHC 인식부가 자기로 잘못 인식한 회수

개수 / 유사도	5	10	20	30
0.99938	9935	9891	9775	9626
0.99690	9754	9450	8912	8308
0.9845	8568	7324	5641	4089
0.9768	7862	6532	3797	2511
0.9695	7311	6113	3233	1759

표 2는 일련의 셀 변경에 따른 MHC 인식부의 인식율을 보여주고 있다. 이 경우 스트링변경 시뮬레이션과 비슷한 유사도를 가지는 변경된 파일에 경우에서도 셀 변경 때와는 다른 높은 인식율을 보여주고 있다. 이는 블록화된 자기파일의 변경부분에 대해 MHC 인식부의 변경검사가 정밀함을 알 수 있다.

표 2. 셀 변경에 따른 변경된 자기파일 10,000개에 대해서 MHC 인식부가 자기로 잘못 인식한 회수

개수 / 유사도	5	10	20	30
0.990	9989	6815	2659	187
0.980	9796	2803	1762	366
0.970	6861	612	0	2
0.960	2400	7	3	0
0.940	2562	2	0	0
0.920	22	0	0	0
0.900	0	0	0	0

Ⅳ. 결론 및 향후 연구과제

본 논문에서는 생체 면역시스템의 면역세포 중의 하나인 세포독성 T세포의 자기를 구분하는 MHC 제한기능을 이용하여 컴퓨터에서 파일의 변경여부를 검사하는 변경 검사 알고리즘을 구현하였다. 이렇게 구현된 MHC 인식부를 이용한 변경된 자기파일에 대한 시뮬레이션의 결과로 자기파일 변경 검사 알고리즘이 상황에 안정적이며 정밀하게 변경 검사를 수행한다는 유효성을 검증하였다. 이에 컴퓨터 면역시스템 구축에 필요한 자기와 비자기 구분 알고리즘의 적용 가능성을 보였다. 아직 자기파일과의 유사도가 작은 변경 검사에서는 그 유효성이 미미하고 변경 검사를 실행할 때 걸리는 시간 등에 대한 알고리즘의 보안이 요구된다.

감사의 글 :

본 연구는 한국산업자원부 2000년 제2차 산업기반기술개발사업(공통핵심/Spin-Off)의 연구비지원으로 수행되었으며 연구비 지원에 감사드립니다.

Ⅴ. 참고문헌

[1] Stephanie Forrest, Lawrence Allen, Alan S. Perelson, Rajesh Cherukuri "Self-Nonself Discrimination in a Computer" *IEEE Symposium on Research in Security and Privacy*, 1994.

[2] Dipankar Dasgupta, "An Immune Agent Architecture for Intrusion Detection", *Genetic and Evolutionary Computation Conference Workshop Program* pp.42 - 44, 2000.

[3] Paul K. Harmer, Gary B. Lamont, "An Agent Based Architecture for a Computer Virus Immune System", *Genetic and Evolutionary Computation Conference Workshop Program* pp. 45 - 46, 2000.

[4] 구자범, 이동욱, 박세현, 심귀보, "생체 면역시스템 기반의 새로운 보안 항체 계층 모델", *한국 퍼지 및 지능시스템학회 논문지* vol. 10, no. 2, pp. 122-128, 2000.

[5] I. Roitt, J. Brostoff, D. Male, *Immunology*, 4th edition, Mosby, 1996.